

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ І ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО
ПРОСТОРУ

Кваліфікаційна наукова
праця на правах рукопису

ПУСТОВІТ ОЛЕКСАНДР СЕРГІЙОВИЧ

УДК 519.1 + 519.72

ДИСЕРТАЦІЯ

**ЗАСТОСУВАННЯ ТЕОРІЇ ЕКСТРЕМАЛЬНИХ ГРАФІВ ДО СУЧАСНИХ
ПРОБЛЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

Спеціальність 05.13.06 – Інформаційні технології

Технічні науки

Подається на здобуття наукового ступеня кандидата технічних наук. Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

(О.С.Пустовіт)

(підпис, ініціали та прізвище здобувача)

Науковий керівник

Устименко Василь Олександрович

доктор фізико-математичних наук, професор

Київ – 2021

АНОТАЦІЯ

Пустовіт О.С. Застосування теорії екстремальних графів до сучасних проблем інформаційної безпеки. - Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – Інформаційні технології. – Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України, Київ, 2021.

Дисертаційна робота присвячена вирішенню актуальної науково-практичної проблеми розробки методів захисту інформації, пов'язаних з викликом Великих Даних та появою перших зразків квантового комп'ютера.

У першому розділі розглядаються задачі класичної криптографії від багатьох змінних, що пов'язані зі створенням криптографічних ключів. Коротко оглянуто виники міжнародного тендеру NIST (інституту стандартизації інформаційних технологій Сполучених Штатів Америки) на створення постквантових публічних ключів для розв'язання задач безпечного обміну інформації та постквантових алгоритмів електронного підпису.

Напрямок криптографії від багатьох змінних у цьому тендері конкурує з напрямками алгоритмів, що базуються на решітках, криптосистем, що використовують коди захисту від шумів, криптосистем, що використовують супереліптичні криві та алгоритмів побудованих з використанням хеш функцій.

В липні 2020 року розпочався останній третій раунд цього проекту. Результати відбору в галузі алгоритмів захисту обміну інформації (шифрування) не сприятливі для класичної криптографії від багатьох змінних – жодний з алгоритмів цього класу не залишився у списку кандидатів на переможця.

Зазначимо, що класична криптографія від багатьох змінних використовує відображення простору шифрограм степені 2. Це мотивує дослідження криптосистем від багатьох змінних, що базуються на відображеннях необмеженої степені або таких, що задають взаємно-однозначну відповідність.

Саме цьому напрямку і присвячено перший розділ дисертації. У ньому визначені основні алгебраїчні об'єкти криптографії від багатьох змінних. Це перш за все афінний простір вимірності n над скінченним комутативним кільцем K (алфавітом для текстів).

У другому розділі було імплементовано потоковий алгоритм та детально досліджено вибрану функцію шифрування G з алгоритму, що використовує властивості графів $A(n, K)$.

Було розглянуто інформацію про ці графи та їх проєктивну границю $A(K)$, що використовується в алгоритмі. Граф $A(F_q)$ є нескінченним q – регулярним деревом. Задання графу $A(F_q)$ вирішує проблему презентації графу рівняннями у Гільбертовому просторі F_q .

Важливою категорією інформаційного простору є довіра до документів. Легко побачити, що навіть користування надійними засобами шифрування не забезпечує повної довіри до документів, тому що треба рахуватися із шумами у каналах та проблемами безпечного збереження файлів у електронних сховищах, де документи можуть бути підроблені, пошкоджені комп'ютерними вірусами, технічними помилками в роботі обчислювальної техніки та інше. Останнім часом постійно зростає загроза потужних кібертерористичних атак на сховища, їх наслідки це не тільки виток інформації, але й ушкодження або фальсифікування документів. Зрозуміло, що після виявлення кібератаки потрібно робити аудит усіх файлів системи.

Для задач виявлення кібератак, верифікації та автентифікації документів потрібні так звані залежні від ключів хеш-функції (автентифікаційні коди повідомлень або МАСи) які залежать від гасла. Хеш-функція потрібна для генерації скомпенсованої форми оригінального документа довільно обраного розміру. Таку форму називають хешем або дайджестом документа, її використовують у різних криптографічних застосуваннях. Хеш-функція h працює з файлом довільного розміру n , її значення має фіксований розмір.

Третій розділ присвячено задачам симетричної криптографії, а саме, поточковому шифруванню та створенню чутливих дайджестів електронних документів, що залежать від ключа.

Симетрична криптографія не є частиною постквантової криптографії, але при дослідженні захищеності алгоритмів також потрібно розглядати можливість атак супротивника з використанням квантового комп'ютера. У випадку дайджестів вже визначено поняття постквантової стабільності алгоритму.

Критичним параметром симетричних алгоритмів є швидкодія, тому що розміри інформації для обробки постійно зростають, потрібно рахуватися з викликом Великих Даних. Поточкові алгоритми симетричного шифрування потрібно підтримувати безпечними протоколами обміну ключів. Популярний протокол Діффі-Хеллмана вже не витримує атак з використанням квантового комп'ютера.

Четвертий розділ присвячено побудові криптосистем з публічним ключем криптографії від багатьох змінних, що спираються на відображення необмеженої степені на відміну від першого розділу розглядається випадок бієктивних відображень. Ейлерівські перетворення афінного простору або поліноміальні відображення генеровані за лінгвістичними графами розглядаються окремо, як самостійні методи шифрування.

Використано більш загальні лінгвістичні графи типу $(k, k, n-k)$ вершини яких мають визначений першими k координатами вектору з простору K^n , де K – довільне комутативне кільце.

Визначено напівгрупи та групи $SL(K)$ та $GL(K)$, що відповідають парі лінгвістичних графів $L(K)$ та $L(K[x_1, x_2, \dots, x_n])$. Вони утворені поліноміальними перетвореннями простору K^n , що використовується як простір відкритих текстів над алфавітом K .

Наведено приклади публічних ключів, побудованих на комбінації Ейлерівського перетворення з відображенням лінійної степені, що є побудованим за лінгвістичним графом над комутативним кільцем K .

У п'ятому розділі абстрактні схеми протоколів обміну ключів доводяться до рівня алгоритмів у випадках Подвоєних графів Шуберта, напівгрупи всіх Ейлерівських перетворень та групи визначеною за стабільними кубічними групами $GA(n,K)$. Приведено Tahoma протокол, назва якого походить від tame homomorphism, тобто гомоморфізму який можна обчислити за поліноміальний час.

Детально описується схема для Unbalanced Oil and Vinegar (UOV) систем цифрового підпису. Зазначимо, що UOV один з кандидатів у переможці тендеру NIST PQC. Наводиться модифікація цієї системи, що елімінує багато відомих атак супротивника та підвищує її криптостійкість. Постквантовий статус цього модифікованого цифрового підпису ґрунтується на безпеці Тахома протокола, який можна використовувати для контролю доступу до інформаційної системи (IC).

У роботі пропонуються швидкі, постквантово стійкі алгоритми створення дайджестів електронних документів. Описано нові алгоритми з публічним ключем, визначені перетвореннями від багатьох змінних необмеженої степені. Досліджені властивості нових асиметричних алгоритмів шифрування типу Ель Гамаля, визначених постквантовими протоколами. Запропоновано нові алгоритми цифрового підпису, безпека яких також визначено постквантовими протоколами некомутативної криптографії, визначеними у термінах криптографії від багатьох змінних.

Ключові слова: багатоваріантна криптографія, хеш функція, дайджести, цифровий підпис, протоколи обміну ключів, постквантова криптографія, кібербезпека.

ANNOTATION

Pustovit O.S. Application of theories of extreme graphs to modern problems of information security. - Manuscript.

The dissertation for the degree of a candidate of technical sciences on the specialty 05.13.06 «Information technologies.» Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, Kyiv, 2021.

The dissertation, devoted to the solution of a topical scientific and practical problem, reveals the methods of data protection involved in the Big Data call and the first samples of a quantum computer appear.

In the first section discusses the problems of classical cryptography from many variables associated with the creation of cryptographic keys. The results of the international tender of the NIST (Institute of Information Technology Standardization of the United States of America) for the creation of post-quantum public keys to solve problems of secure information exchange and post-quantum electronic signature algorithms are briefly reviewed.

The direction of cryptography from many variables in this tender competes with the directions of lattice-based algorithms, cryptosystems that use noise protection codes, cryptosystems that use superelliptic curves, and algorithms constructed using hash functions.

In July 2020, the last third round of this project began. The results of selection in the field of algorithms for the protection of information exchange (encryption) are not favorable for classical cryptography from many variables - none of the algorithms of this class remained in the list of candidates for the winner.

Note that classical cryptography of many variables uses the mapping of the space of degree 2 ciphers. This motivates the study of cryptosystems of many variables based on mappings of unlimited degree or those that specify a one-to-one correspondence.

The first section of the dissertation is devoted to this direction. It identifies the basic algebraic objects of cryptography from many variables. This is primarily an affine space of dimension n over a finite commutative ring K (alphabet for texts).

In the second section, the streaming algorithm was implemented and the selected encryption function G from the algorithm using the properties of graphs $A(n, K)$ was investigated in detail.

Information about these graphs and their projective boundary $A(K)$ used in the algorithm was considered. The graph $A(F_q)$ is an infinite q -regular tree. The problem of graph $A(F_q)$ solves the problem of graph presentation by equations in Hilbert space F_q .

An important category of information space is trust in documents. It is easy to see that even the use of reliable encryption tools does not provide complete trust in documents, because you have to take into account channel noise and secure file storage in electronic repositories, where documents can be forged, damaged by computer viruses, technical errors in computing. equipment and more. Recently, the threat of powerful cyber-terrorist attacks on repositories has been growing, the consequences of which are not only information leakage, but also damage or falsification of documents. It is clear that after detecting a cyberattack you need to audit all files in the system.

The tasks of detecting cyberattacks, verifying and authenticating documents require so-called key-dependent hash functions (message authentication codes or MACs) that depend on them. from the slogan. A hash function is required to generate a compensated form of the original document of any size. This form is called a hash or digest of the document, it is used in various cryptographic applications. The hash function h works with a file of arbitrary size n , its value has a fixed size.

The third section is devoted to the tasks of symmetric cryptography, namely, streaming encryption and the creation of sensitive digests of electronic documents that depend on the key.

Symmetric cryptography is not part of post-quantum cryptography, but the study of the security of algorithms should also consider the possibility of enemy attacks using a quantum computer. In the case of digests, the concept of postquantum stability of the algorithm has already been defined.

The critical parameter of symmetric algorithms is speed, because the size of information for processing is constantly growing, you need to take into account the challenge of Big Data. Streaming symmetric encryption algorithms must be supported by secure key exchange protocols. The popular Diffie-Hellman protocol can no longer withstand attacks using a quantum computer.

The fourth section is devoted to the construction of cryptosystems with a public key cryptography of many variables that rely on the display of unlimited degree in contrast to the first section considers the case of bijective mappings. Euler transformations of affine space or polynomial mappings generated by linguistic graphs are considered separately as independent encryption methods.

More general linguistic graphs of type $(k, k, n-k)$ are used, the vertices of which have the first k coordinates of the vector from the space K^n , where K is an arbitrary commutative ring.

The semigroups and groups $SL(K)$ and $GL(K)$ corresponding to the pair of linguistic graphs $L(K)$ and $L(K[x_1, x_2, \dots, x_n])$ are determined. They are formed by polynomial transformations of the space K^n , which is used as a space of open texts over the alphabet K .

Examples of public keys based on a combination of the Euler transformation with a reflection of a linear degree, which is built on a linguistic graph over the commutative ring K , are given.

In the fifth section, abstract schemes of key exchange protocols are brought to the level of algorithms in the cases of Schubert's Double Graphs, a semigroup of all Euler transformations, and a group defined by stable cubic groups $GA(n, K)$. The Tahoma

protocol is given, the name of which comes from tame homomorphism, ie homomorphism that can be calculated in polynomial time.

The scheme for Unbalanced Oil and Vinegar (UOV) digital signature systems is described in detail. Note that UOV is one of the candidates in the winner of the NIST PQC tender. A modification of this system is provided, which eliminates many known enemy attacks and increases its cryptocurrency. The post-quantum status of this modified digital signature is based on the security of the Tahoma Protocol, which can be used to control access to the information system (IS).

The paper proposes fast, post-quantum stable algorithms for creating digests of electronic documents. New algorithms with a public key defined by transformations from many variables of unlimited degree are described. The properties of new asymmetric El Gamal-type encryption algorithms defined by postquantum protocols are investigated. New digital signature algorithms have been proposed, the security of which is also determined by post-quantum protocols of noncommutative cryptography, defined in terms of cryptography from many variables.

Keywords: multivariate cryptography, hash function, digests, digital signature, key exchange protocols, post quantum cryptography, cybersecurity.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, в яких опубліковано основні результати дисертації:

1. V. Ustimenko, **O. Pustovit**, On effective computations in subsemigroups of affine Cremona semigroup and implementations of new postquantum multivariate cryptosystems, Physico-mathematical modelling and informational technologies, Lviv, vol. 32, 2021, pp. 27-31.
2. V. Ustimenko, **O. Pustovit**, On the implementations of new multivariate public keys based on transformations of linear degree, Conference on Mathematical Foundations of Informatics, Kyiv, 2021, pp. 397-420.
3. **O.S. Pustovit**, V.O Ustimenko, A new stream algorithms generating sensitive digests of digital documents, Mathematical modelling in economics, N3, 2019, 18-35.
4. Устименко В. О., **Пустовіт О. С.** Нові потокові алгоритми для створення дайджесту електронних документів з високим рівнем лавинного ефекту. Математичне та комп'ютерне моделювання, Серія: Фізико-математичні науки, Збірник наукових праць. Випуск 19, Київ, 2019, с. 174-180.
5. **О. Пустовіт**, В. Устименко, Про застосування алгебраїчної комбінаторики до проблем кодування та криптографії, Математичне моделювання в економіці, № 1-2, Київ, 2017, с. 31-39.
6. **О. Пустовіт**, Динамічні системи та їх використання до проблем інформаційної безпеки, Журнал для студентів фізико-математичних етюдів, №10, Київ, 2011, 64-67.

Праці, які засвідчують апробацію матеріалів дисертації:

7. Устименко В.О., **Пустовіт О.С.**, On the implementation of postquantum access control protocol based algorithms, 20 Міжнародна науково-практична конференція: Сучасні інформаційні технології управління навколишнім середовищем, природного використання, заходи в надзвичайних ситуаціях, Київ, 2021, с 42-44.

8. V. Ustimenko, **O. Pustovit**, New cryptosystems of Noncommutative cryptography based on Eulerian semigroups of multivariate transformations, Cybersecurity Providing in Information and Telecommunication Systems 2021, Kyiv, 2021, pp. 18-26. (*індексується в Scopus*)

9. V. Ustimenko, **O. Pustovit**, On new stream algorithms generating sensitive digests of computer files, Federated Conference on Computer Science and Information Systems, Sofia, 2021, pp. 131-135 (**List B, IEEE Digital Library**)

10. V. Ustimenko, **O. Pustovit**, On the implementation of public keys with the usage of algebraic maps of unbounded degree, The 13th International Algebraic Conference in Ukraine, Kyiv, 2021, p. 84.

11. V. O. Ustimenko, **O. S. Pustovit**, Dynamical systems based on small world expanding graphs and algorithms to secure big data processing, International conference Modern Stochastics: Theory and Applications V, Kyiv, 2021, pp. 39-40.

12. Устименко В.О., **Пустовіт О. С.**, Про застосування екстремальної теорії графів до створення дайджестів електронних документів з високорівневим аваланч ефектом, 3 Міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS) 2-3 квітня 2020, Taras Shevchenko National University of Kyiv.

13. V. O. Ustimenko, **O. S. Pustovit**, On noncommutative cryptography responds to challenges of quantum computer and secure big data processing, International mathematical conference dedicated to the 60th anniversary of the department of algebra and mathematical logic of Taras Shevchenko National University of Kyiv, Book of abstract, Kyiv 2020, p.83.

14. Устименко В.О., **Пустовіт О. С.**, Про нові постквантові алгоритми електронного підпису, що модифікують алгоритми представлені на другий етап NIST сертифікації, Праці 19-ої Міжнародної науково – практичної конференції «Сучасні інформаційні технології управління екологічною безпекою, природокористуванням, заходами в надзвичайних ситуаціях», 2020р., м. Київ, Петропавлівська Борщагівка.(розділ у колективній монографії), с. 57-59.

15. Устименко В.О., **Пустовіт О.С.**, Покращена безпека для ГІС з використанням N-зв'язної архітектури та нового графу, який базується на основі потокового шифру, 18 Міжнародна науково-практична конференція: Сучасні інформаційні технології управління навколишнім середовищем, природного використання, заходи в надзвичайних ситуаціях, Київ, 2019, с. 92-94.

16. Устименко В. О, **Пустовіт О.С.**, Про екстремальні графи, афінну напівгрупу Кремони та нові рішення постквантової криптографії, Міжнародна алгебраїчна конференція, 2019, с. 121-122, Вінниця.

17. **Пустовіт О.С.**, Устименко В. О. Нові алгоритми аудиту електронних документів, їх впровадження та застосування в кібербезпеці, 17 Міжнародна науково-практична конференція: Сучасні інформаційні технології управління навколишнім середовищем, природокористування, заходи в надзвичайних ситуаціях, Київ, 2018, с. 170-175.

18. В. О. Устименко, **О. С. Пустовіт**, Нова концепція електронного підпису та засоби її реалізації, 16 Міжнародна науково-практична конференція: Сучасні інформаційні технології управління навколишнім середовищем, природокористування, заходи в надзвичайних ситуаціях, Київ, 2017, с. 86-89.

19. В.М. Лахман, **О.С. Пустовіт**, В.О. Устименко, Про реалізацію криптографічного алгоритму, визначеного в рамках груп Кас-Moody над діаграмою $\overline{A_1}$, International mathematical conference Group and Actions: Geometry and Dynamics, Київ, 2016, с. 33

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....	16
ВСТУП.....	17
РОЗДІЛ 1 ЕЛЕМЕНТИ ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ.....	23
1.1. Про Ейлерівські поліноміальні відображення афінного простору (Z_m) ⁿ обмеженої степені.....	23
1.2. Приклад криптосистеми побудованої на відображенні з частково бієктивним розкладом.....	28
1.3. Графи $A(n, Z_m)$ та поліноміальні відображення, що приховують RSA.....	35
1.4. Алгебри Каца-Муді та відповідні автомати Шуберта.....	38
1.5. Про дводольні криптосистеми від багатьох змінних.....	44
1.6. Дводольні криптосистеми над кільцями Z_{p^m}	47
1.7. Автомати Шуберта для систем коренів $A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4, G_2$ над довільним комутативним кільцем.....	49
Висновки до першого розділу.....	55
Список джерел, використаних у першому розділі.....	56
РОЗДІЛ 2 ПРО ЗАСТОСУВАННЯ АЛГЕБРАЇЧНОЇ КОМБІНАТОРИКИ ДО ПРОБЛЕМ КОДУВАННЯ ТА КРИПТОГРАФІЇ.....	60
2.1. Про застосування алгебраїчної комбінаторики до проблем постквантової криптографії.....	60
2.2. Про вибір бази і стабільні підгрупи.....	69
2.3. Про властивості одного з потокових симетричних алгоритмів Кодування.....	71
2.4. Автомати, визначені графами сімейства $A(n, q)$	73
Висновки до другого розділу.....	78
Список джерел, використаних у другому розділі.....	78
РОЗДІЛ 3 ПРО НОВІ ПОТОКОВІ АЛГОРИТМИ СТВОРЕННЯ ЧУТЛИВИХ ДАЙДЖЕСТІВ ЕЛЕКТРОННИХ ДОКУМЕНТІВ.....	82

3.1. Про верифікацію електронних документів.....	82
3.2. Вимоги до дайджесту документів.....	83
3.3. Про некомутативну криптографію та її застосування до задач симетричного шифрування і побудови хеш функцій.....	84
3.4. Математичне підґрунтя хеш функції, що пропонується.....	85
3.5. Пришвидшення алгоритмів.....	86
3.6. Про лінгвістичні графи та пов'язані з ними напівгрупи афінних перетворень.....	88
3.7. Деякі алгебраїчні конструкції екстремальної теорії графів, відповідні гомоморфізми компресії та нелінійні групи перетворень.....	92
3.7.1. Деякі означення екстремальної теорії графів.....	92
3.7.2. Алгебраїчні графи $A(n, K)$ і $D(n, K)$, деякі результати і відкриті питання.....	93
3.7.3. Про лінгвістичні та екстремальні графи і стабільні нелінійні підгрупи афінної групи Кремони.....	95
3.8. Про імплементацію алгоритмів створення дайджесту.....	98
Висновки до третього розділу.....	99
Список джерел, використаних у третьому розділі.....	101
РОЗДІЛ 4 РЕАЛІЗАЦІЯ НОВИХ АЛГОРИТМІВ КРИПТОГРАФІЇ	
ВІД БАГАТЬОХ ЗМІННИХ ЛІНІЙНОЇ СТЕПЕНІ.....	107
ТА ПОЛІНОМІАЛЬНОЇ ГУСТИНИ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ	
4.1. Публічні ключі.....	107
4.2. Про використання афінної напівгрупи Кремони.....	108
4.3. Про явну побудову стійких відображень заданого ступеня та великого порядку.....	109
4.4. Про пари перетворень із проміжком щільності та відповідним відкритим ключем.....	114
4.5. Про Ейлерові перетворення та їх криптографічні додатки.....	115
4.6. Про комбіновані відкриті ключі.....	117
Висновки до четвертого розділу.....	126

Список джерел, використаних у четвертому розділі.....	127
РОЗДІЛ 5 ПРОТОКОЛИ ОБМІНУ КЛЮЧІВ	
НЕКОМУТАТИВНОЇ КРИПТОГРАФІЇ ВІД БАГАТЬОХ	
ЗМІННИХ ТА ЇХ ЗАСТОСУВАННЯ У	
ПОСТКВАНТОВИХ КРИПТОГРАФІЧНИХ АЛГОРИТМАХ.....	132
5.1. Про Постквантову криптографію, криптографію від багатьох	
змінних та некомутативну криптографію.....	132
5.2. Про стабільні підгрупи формальної групи Кремони та	
приватизацію багатовимірних публічних ключів на основі	
відображень обмеженого ступеня.....	134
5.3. Багатовимірний протокол Тахоми для стабільних генераторів	
Кремони та його використання для багатовимірних	
алгоритмів шифрування.....	136
5.4. Про алгоритми багатовимірних цифрових підписів та схему	
їх приватизації.....	140
5.5. Приклади стійких кубічних груп.....	143
5.5.1. Приклад найпростішого графу.....	143
5.5.2. Інші стійкі підгрупи, визначені за допомогою лінгвістичних	
графів.....	147
5.5.3. Спеціальні гомоморфізми лінгвістичних графів та	
відповідних напівгруп.....	151
5.5.4. Приклад стабільних підгруп довільного ступеня.....	152
Висновки до п'ятого розділу.....	155
Список джерел, використаних у п'ятому розділі.....	157
ВИСНОВКИ.....	163
Додаток А Список опублікованих праць за темою дисертації.....	166
Додаток Б Відомості про апробацію результатів дисертації.....	169
Додаток В Акти впровадження результатів дисертаційної роботи.....	172

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ДЛ – дискретний логарифм

ЕЦП – електронний цифровий підпис

ПК – персональний комп'ютер

ПКК – постквантова криптографія

ВСТУП

Обґрунтування вибору теми дослідження. Сучасний стан розвитку суспільства характеризується різким зростанням інформаційних потоків не тільки в засобах масової інформації, але й у сфері виробництва, науки, культури. Стрімке вдосконалювання комп'ютерних технологій позначилося й на принципах побудови захисту інформації.

Проблема захисту інформації з'явилася ще задовго до появи комп'ютерів. З самого початку свого розвитку системи інформаційної безпеки розроблялися для військових відомств. Розголошення такої інформації могло привести до величезних людських жертв, тому конфіденційності в системах безпеки приділялася особлива увага. Очевидно, що надійно захистити повідомлення й дані від розголошення і перехоплення може тільки повне їхнє шифрування.

На сьогоднішній час у галузі захисту інформації має місце велика кількість розробок, для яких відсутній системний аналіз, і тому їх часом неможливо порівняти між собою.

В наш час відбувається криза теорії кібербезпеки викликана неспроможністю сучасних інструментів захисту інформації відповісти зростаючим потребам організацій працюючих у Глобальному Інформаційному просторі.

Одна з таких вимог коротко названа Викликом Великих Даних (Big Data Challenge), вона викликана експоненційним зростом працюючих Інформаційних Систем та обсягами інформації при обробці та потребує значно швидших алгоритмів захисту великих множин даних.

Інший виклик пов'язаний з протидією кібертероризму та кіберагресії. Визнаним фактом є перелік успішних кібертерористичних атак, які підтримуються організаціями з практично необмеженими фінансовими та обчислювальними ресурсами.

Квантові комп'ютери матимуть спроможність вирішувати теоретичні проблеми недоступні сучасним детермінованим комп'ютерам.

Національний Інститут стандартизації технологій Сполучених Штатів Америки оголосив тендер на виявлення найкращих відомих нових алгоритмів асиметричної криптографії з публічним ключем для їх постквантової сертифікації. Такі алгоритми розбиваються на класи криптосистем, що спираються на:

- теорію кодування (Code based Cryptography),
- теорію решіток (Lattice based Cryptography),
- поліноміальні функції від багатьох змінних (Multivariate Cryptography),
- супереліптичні криві (Superelliptic curves),
- функції хешування (Hash functions Cryptography).

В березні 2019 завершився перший раунд цього тендеру, під час другого раунду спеціалісти зі стандартизації виконують дослідження властивостей відібраних у 2019 році алгоритмів.

У липні 2020 року розпочався третій раунд для остаточного подальшого дослідження вже вибраних алгоритмів. В області криптографії від багатьох змінних для подальшого дослідження відбираються лише цифрові підписи на зразок олії та оцту. Їх не можна використовувати як алгоритми шифрування. Цей факт мотивує різні, ніж загальнодоступні напрямки криптографії від багатьох змінних.

На сьогоднішній день питання побудови нових алгоритмів захисту інформації розглядається вітчизняними та багатьма зарубіжними фахівцями та науковцями. Можна назвати дослідників зі Швейцарії (J. Rozenberg , G. Maze , C. Monico), Сполучених Штатів Америки (Т. Shaska, V. Shpilrain, A. Myasnikov, D. Kahrobei та інші), Російської Федерації (D. Moldovjan, A.. Moldovjan, D. Grigoriev, I. Ponomarenko, V. Roman'kov), Великої Британії (S. Blackburn, S Galbraith), Іспанії (J. Lopez Ramos, J. Gutierrez) та інших країн.

В Україні займаються як хеш функціями (І. Горбенко, Р. Олійников., О. Казимиров, В. Руженцев, О. Кузнєцов, Ю. Горбенко та інші) так і теоретичною криптографією з використанням алгебро-комбінаторних об'єктів (В. Устименко, М. Савчук, О. Фаль, В. Задірака, А. Напрієнко, А. Олійник та інші).

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота пов'язана з вирішенням науково-технічних задач, сформульованих в Стратегії кібербезпеки України, затвердженої Указом Президента України №96/2016 від 27.01.2016 р., в Стратегії національної безпеки України, затвердженої Указом Президента України № 287/2015 від 26.05.2015 р., а також в «Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» затвердженому Наказом №660 Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 02.12.2014 р. Дисертаційна робота виконана у рамках науково-дослідних робіт: «Аналіз складних нелінійних динамічних систем, що використовуються у новітніх телекомунікаційних технологіях перетворення, збереження та захисту інформації» (№ держреєстрації: 0112U002714), «Розробка методів захисту інформації що використовують новітні досягнення екстремальної теорії графів» (№ держреєстрації: 0112U007444), «Створення програмно-інформаційних засобів інформаційно-аналітичного забезпечення мережецентричних ситуаційних центрів» (№ держреєстрації: 0221U104666).

Мета і задачі дослідження. Метою дисертаційної роботи є розв'язання нових постквантових задач захисту інформації. А саме:

- розробка і створення унікальних протоколів обміну ключів,
- розробка і створення залежних дайджестів електронних документів для автентифікації нових постквантових криптосистем шифрування,
- розробка і створення нових швидких потокових алгоритмів з відпирністю атак лінеаризації.

Об'єктом дослідження є Марковський процес блукання на алгебраїчних графах та задач дослідження його криптографічних властивостей.

Предметом дослідження є криптографічні прототипи, що будуються за екстремальними графами та графами-експандерами.

Методи дослідження. При вирішенні поставлених задач у дисертаційній роботі було використано методи Екстремальної теорії графів, Теорії скінченних

геометрій та Теорії символічних обчислень разом із методами некомутативної криптографії та прикладної алгебраїчної геометрії.

Для задач симетричної криптографії (потокове шифрування та створення дайджестів електронних документів) використовувались обчислювальні методи. При дослідженні властивостей (швидкодія, степені змішування) вживались статистичні методи.

Наукова новизна одержаних результатів. Новими результатами, отриманими в дисертаційній роботі є:

1) вперше в термінах теорії алгебраїчних графів та графів-експандерів створено криптографічно стійкі постквантові швидкі алгоритми для хешування великих файлів у дайджесту заданих розмірів, який буде чутливим до будь-яких змін символів у файлі;

2) вперше розроблені алгоритми створення чутливих дайджестів електронних файлів для виявлення кібератак на віртуальні організації з покращеним на 45% показником аваланч ефекту;

3) вперше в термінах Алгебраїчної Геометрії запропоновано нову парадигму, в якій теорія алгебраїчних графів та некомутативна алгебра використовується для розробки та впровадження нових несиметричних інструментів криптографії (протоколи, криптосистеми, інструмент контролю доступу), стійких до кібератак супротивника у постквантову епоху;

4) вперше в термінах теорії алгебраїчних графів створено алгоритми використання напівгрупи над скінченними комутативними кільцями для розробки швидких поточкових алгоритмів шифрування зі зростаючим простором відкритих текстів;

5) вперше теорію скінченних геометрій використано для створення алгоритмів електронного підпису криптографії від багатьох змінних, які замість публічних ключів використовують протоколи некомутативної криптографії.

Результати дисертаційних досліджень реалізовані й впроваджені в:

Київському університеті імені Бориса Грінченка в рамках навчальних дисциплін «Методи побудови та аналізу криптосистем», «Математичні методи

криптографії» та впроваджені в програмно-апаратне забезпечення «Центру технологій захисту інформаційних активів» при розгортанні Лабораторії криптографічного та технічного захисту інформації.

ТОВ «Алгоритм –Х» у програмно-апаратне забезпечення при створенні алгоритмів захисту мереж ситуаційних центрів та алгоритмів виявлення кібератак.

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться до захисту, отримані автором самостійно. У статтях написаних у співавторстві з керівником дисертаційної роботи, здобувачу належить: в [2] – імплементація потокового алгоритму шифрування над спеціальними кільцями, дослідження їх властивостей як теоретичними методами, так і з використанням комп'ютерної симуляції, [3] – імплементація потокових алгоритмів створення дайджестів для спеціальних комутативних кілець (скінченні поля, арифметичні кільця за модулем та булевих кілець), вивчення параметрів для цих алгоритмів та рівня відповідного аваланч ефекту, [5] – імплементація публічних ключів визначених за графами, використання комп'ютерної симуляції для дослідження розміру ключа, швидкодії та властивостей змішування, [6] – імплементація протоколів обміну ключами, визначеними за стабільними групами перетворень афінного простору та їх розширень до криптосистеми типу Ель Гамала. Вивчення властивостей нових криптосистем за результатами комп'ютерної симуляції. У працях [7]-[18] – презентація виників комп'ютерної симуляції та теоретичних властивостей запропонованих алгоритмів.

Апробація результатів роботи. Основні положення і результати досліджень доповідалися та обговорювалися на Міжнародних конференціях «Groups and Actions, Geometry and Dynamics», Київ, 2016, «Сучасні інформаційні технології управління навколишнім середовищем, природокористування та заходи в надзвичайних ситуаціях» Київ, 2017, 2018, 2019, 2020, 2021; Міжнародній Алгебраїчній конференції 2019 та 2021.; Міжнародній математичній конференції присвяченій 60-річчю кафедри алгебри та математичної логіки Національного Київського університету ім. Т. Шевченка; 3-й Міжнародній науково-практичній конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем,

Київ, 2020; Міжнародній конференції «Modern Stochastics», Київ, 2021; Federated conference on Computer Science and Information Systems, Sofia, 2021 (digital library); Міжнародній конференції «Cybersecurity Providing in Information and Telecommunication system», Київ, 2021 (індексується в Scopus); Міжнародному науковому симпозиумі «Питання оптимізації обчислень» (ПОО-XLVI), Київ, 2019; Міжнародному науковому симпозиумі «Питання оптимізації обчислень» (ПОО-XLVII), Львів, 2021.

Публікації. За результатами дисертаційної роботи опубліковано 19 наукових праць, 6 наукових статей, написаних у співавторстві й опублікованих у наукових спеціалізованих фахових виданнях України, 1 наукова праця, що входить до наукометричної бази SCOPUS. Разом з тим основні наукові результати додатково відображені у 13 тезах доповідей на науково-практичних конференціях. Із праць, що опубліковано у співавторстві, у дисертаційній роботі використано виключно ті результати, які одержано здобувачем особисто.

Обсяг і структура дисертації. Дисертація складається з анотації, змісту, переліку умовних позначень, вступу, п'яти розділів, загальних висновків, списків використаних джерел (в кінці кожного розділу основної частини дисертації) і має 155 сторінок основного тексту, 9 рисунків, 9 таблиць. Список використаних джерел містить 176 найменувань. Загальний обсяг дисертаційної роботи – 160 сторінок.

РОЗДІЛ 1

ЕЛЕМЕНТИ ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ

1.1. Про Ейлерівські поліноміальні відображення афінного простору $(Z_m)^n$ обмеженої степені

Розглядається задача побудови відображення афінного простору K^n , визначеного над комутативним кільцем K у себе, що не є взаємно однозначним відображення, але його обмеження на $(K^*)^n$ є ін'єктивним. Такі відображення назвемо Ейлерівськими. У випадку $K = Z_m$, де m складене число та довільного $n, n > 2$ будується родина Ейлерівських відображень простору Z_m^n . Пропонується криптосистема, що базується на такій родині. Побудова використовує властивості алгебраїчних графів $D(n, K)$.

1. Нехай K є комутативним кільцем $S(K^n)$ є напівгрупою поліноміальних перетворень афінного простору K^n у себе. Відображення $F \in S(K^n)$ назвемо Ейлерівським, якщо воно не є бієкцією, але його обмеження на $(K^*)^n$ є ін'єкцією. Нехай τ_L є мономіальне перетворення простору K^n , тобто відображення, що задається в обраному базисі $\bar{e}_i, i \in N$ вільного модуля K^n правилом $\bar{e}_i \rightarrow \lambda_i e_{\pi(i)}$, де $\lambda_i \in K^*$ та π є підстановкою на множині $\{1, 2, \dots, n\}$.

Припустимо, що τ_R є загальним бієктивним афінним відображенням вигляду $\bar{x} \rightarrow \bar{x}A + \bar{b}$, де A матриця, що має обернену, $\bar{b}$ – фіксований елемент K^n . Для $F \in S(K^n)$ відображення вигляду $\tau_L F \tau_R$ будемо називати деформацію перетворення F . Очевидно, що деформація Ейлерівського відображення буде Ейлерівським перетворенням. Зауважимо, що F та $\tau_L F \tau_R$ мають однаковий степінь.

Декомпозицію $F = F^{(1)} \cdot F^{(2)} \cdot \dots \cdot F^{k(n)}$ у напівгрупі $S(K^n)$ для Ейлерівського перетворення F назвемо Ейлерівським розкладом, якщо її знання дає змогу

розв'язати рівняння $F(\bar{x}) = b$ відносно невідомого елемента X з $(K^*)^n$ за поліноміальний час $O(n^t)$, де t є сталою.[9, 16, 19]

Неважко побачити, що довільна деформація перетворення з Ейлерівським розкладом також має Ейлерівський розклад.

Теорема 1.1. Нехай $K = (Z_m)^n$, де m є складеним числом. Для довільного поліноміального виразу $K(n)$ від параметру n , що приймає непарні значення, існує нелінійне Ейлерівське відображення $F_{K(n)}$ з Ейлерівським розкладом $F_{K(n)} = F^{(1)} \cdot F^{(2)} \cdot \dots \cdot F^{K(n)}$, що має обмежений степінь d .

Зауваження 1.1. Для довільного натурального s існує відображення степені $d > s$ таке як у теоремі 1.1. Нижче буде представлено конструктивне доведення цієї теореми. Це твердження обґрунтовує наступний алгоритм з ключем публічним.

Аліса обирає параметри $s, n, k(n)$ та складне число m . Вона обирає мономіальне відображення τ_L простору Z_m^m та загальне афінічне відображення τ_R . За поліноміальний час $O(n^r)$ вона генерує поліноміальне перетворення $F_{K(n)}$ та його деформацію $G_n = \tau_L F_{K(n)} \tau_R$ фіксованої степені d , що перевищує s . Аліса має змогу користуватися Ейлерівським розкладами $F_{K(n)} = F^{(1)} \cdot F^{(2)} \cdot \dots \cdot F^{K(n)}$ та $G = \tau_L F^{(1)} F^{(2)} \dots F^{K(n)} \tau_R$, які вона тримає у безпеці. Аліса записує відображення G у стандартному вигляді $x_1 \rightarrow g_1(x_1, x_2, \dots, x_n), x_2 \rightarrow g_2(x_1, x_2, \dots, x_n), \dots, x_n \rightarrow g_n(x_1, x_2, \dots, x_n)$, де поліноми g_i задаються списками їх мономів в деякому фіксованому порядку.

Аліса забезпечує доступ публічного користувача (Боба) до відображень $g_i, i=1, 2, \dots, n$ таких як вище. Вона повідомляє, що простором відкритих текстів буде $(Z_m^*)^n$.

Припустимо, що Боб створив відкритий текст $(p_1, p_2, \dots, p_n) = \bar{p}$. Він обчислив шифрограму $G(\bar{p}) = \bar{c}$ на переслав його Алісі по відкритому каналу зв'язку.

Аліса декодує, виконуючи наступні кроки:

- (1) обчислення $\tau_R^{-1}(\bar{c}) = \bar{b}$
- (2) розв'язання рівняння $F(\bar{z}) = \bar{b}$ з невідомим вектором $\bar{z} = (z_1, z_2, \dots, z_n)$. Нехай $\bar{r} = (r_1, r_2, \dots, r_n) \in \text{розв'язком}$
- (3) обчислення $\tau_L^{-1}(r)$, що дорівнює відкритому тексту $\bar{p}$.

Опишемо тепер конструктивну побудову перетворення F у термінах алгебраїчної теорії графів.

Нехай K є довільне комутативне кільце з одиницею. Розглянемо дводольний граф з множинами точок $P \approx K^n$ та прямих $L = K^n$. Щоб відрізнити точку $(\bar{p}) = (p_1, p_2, \dots, p_n)$ та пряму $[\bar{l}] = [l_1, l_2, \dots, l_n]$ будемо вживати круглі та квадратні дужки.[25]

Вважатимемо, що точка $(\bar{p})$ та пряма $[\bar{l}]$ з'єднані ребром у графі $\psi = \psi(n, k)$ тоді й лише тоді, коли виконуються співвідношення

$$\begin{aligned} p_2 - l_2 &= p_1 l_1, \\ &\dots\dots\dots \\ p_s - l_s &= \varepsilon_s p_1 l_{j(s)} + (1 - \varepsilon_s) l_1 p_{j(s)} \end{aligned}$$

для $s = 2, 3, \dots, n$, де $\varepsilon_s \in \{0, 1\}$, $j(s) < s$

Будемо називати графи з визначеного вище класу двозмінними.

Першу координату p_1 точки $(\bar{p})$ та першу координату l_1 прямої $[\bar{l}]$ будемо називати кольором вершини. Безпосередньо з означення випливає, що для кожної вершини графу існує єдиний сусіда $N_\alpha(v)$ заданого кольору K . З'єднуючи сусідні вершини v_1 та v_2 стрілкою з вагою α , що є кольором вершини v_2 ми перетворимо граф $\psi(n, k)$ у скінченний автомат. Всі стани (вершини) цього автомату будемо вважати припустими (acceptingstates). Зрозуміло, що $N_\alpha(v), \alpha \in K, v \in P \cup L$ можна вважати перехідними функціями такого автомату.[1, 7, 10]

$x_1, x_2, \dots, x_n$. В [6] вдалося довести, що при $chark > 2$ такі умови є достатніми умовами знаходження векторів в одній компоненті зв'язності.

Символічне обчислення вільного двозмінного графу $D(n, k)$ визначається початковим вектором $\bar{x} = (x_1, x_2, \dots, x_n)$ та послідовністю ваг

$f_1(z_1, z_2, \dots, z_l), f_2(z_1, z_2, \dots, z_l), \dots, f_s(z_1, z_2, \dots, z_l)$, де $l = \lfloor \frac{n+2}{2} \rfloor + 1$. Воно задається наступною

процедурою. Для $\bar{x}$ обчислюються вирази

$$\begin{aligned} f_1(x_1, a_1(\bar{x}), a_2(\bar{x}), \dots, a_m(\bar{x})) &= \tilde{f}_1(x), \\ f_2(x_1, a_1(\bar{x}), a_2(\bar{x}), \dots, a_m(\bar{x})) &= \tilde{f}_2(x), \\ &\dots\dots\dots \\ f_m(x_1, a_1(\bar{x}), a_2(\bar{x}), \dots, a_m(\bar{x})) &= \tilde{f}_m(x) \end{aligned}$$

Потім виконуються рекурентні обчислення

$$\begin{aligned} [x_1^1, x_2^1, \dots, x_n^1] &= N_{\tilde{f}_1(\bar{x})}(\bar{x}) \\ (x_1^2, x_2^2, \dots, x_n^2) &= N_{\tilde{f}_2(x)}(x_1, x_2, \dots, x_n) \\ &\dots\dots\dots \\ [x_1^s, x_2^s, \dots, x_n^s] &= N_{\tilde{f}_s(x)}(x_1^{k-1}, x_2^{k-1}, \dots, x_n^{k-1}) \end{aligned}$$

Для спрощення будемо вважати, що параметр s обрано непарним.

Неважко побачити, що відображення $\bar{x} \rightarrow N_{\tilde{f}_s(x)}(x_1^{k-1}, x_2^{k-1}, \dots, x_n^{k-1})$ буде поліноміальним відображенням від багатьох змінних.

Теорема 1.2. Нехай символічне обчислення G графу $D(n, k)$ задається послідовністю ваг $f_1 = f(z_1, z_2, \dots, z_m) + d_1, f_2 = z_1 + d_2, f_{2i+1} = f(z_1, z_2, \dots, z_m) + d_{2i+1}, f_{2i} = z_1 + d_{2i}$ непарної довжини $s = s(n)$. Припустимо, що степінь $f(z_1, z_2, \dots, z_m) \in$ сталою $c, c \geq 1$ параметри $d_i \in$ сталими з кільця K . Тоді степінь відображення G задається сталою $3 \deg \tilde{f}(\bar{x})$.

Теорема 1.3. Нехай $K = Z_m$, де m деяке складене ціле. Припустимо, що символічне обчислення G графу $D(n, k)$ задається послідовністю ваг $f_1, f_2, \dots, f_{2s+1}$,

де $f_{2s+1} = ax_1^r + b(z_2, z_3, \dots, z_m)$, де $a \in K^*$ та $(r, \varphi(m)) = 1$. Тоді відображення G являється перетворенням Ейлерівського типу. [2, 3]

Наслідок 1.1. Нехай G задано символічним обчисленням графу $D(n, Z_m)$, що задовольняє умовам двох попередніх тверджень. Припустимо ще $\deg b(a_1(\bar{x}), a_2(\bar{x}), \dots, a_t(\bar{x})) \in$ сталою c , що перевищує r . Тоді Ейлерівське відображення G має степінь обмежений $3c$.

Твердження 1.1. Нехай G задано символічним обчисленням, що задовольняє умовам двох попередніх теорем. Позначимо через G_i відображення $N_{f_i}(x_1, x_2, \dots, x_n)$ на $P_n \cup L_n$, де $f_1, f_2, \dots, f_{s(n)}$ послідовність символічних ваг. Тоді $G = G_1 \cdot G_2 \cdot \dots \cdot G_s$ являється Ейлерівським розкладом відображення G .

Доведення Обмеження G на P_n можна вважати відображенням з P_n у L_n , що є ізоморфними Z_m^n . Припустимо, що $\bar{x} = (x_1, x_2, \dots, x_n) \in (Z_m^*)^n$. Розглянемо рівняння $G(x) = (d_1, d_2, \dots, d_n) = d$. Зрозуміло, що $d_1 = f_s(x_1, x_2, \dots, x_n)$. Отже маємо умову $ax_1^r + b(a_1(\bar{x}), a_2(\bar{x}), \dots, a_m(\bar{x})) = d_1$. Зауважимо, що $a_i(\bar{x}) = a_i(\bar{d})$. Це означає, що $b(a_1(\bar{x}), a_2(\bar{x}), \dots, a_m(\bar{x})) = b(d_1, d_2, \dots, d_m) = b_1$. Таким чином $x_1^r = \frac{\bar{d}_1 - b_1}{a} = \alpha$.

Нехай r' буде мультиплікативним оберненим до r в групі $Z_{\varphi(m)}$. Тоді $x_1 = \alpha^{r'} = \beta$. Обчислюємо значення $\beta_i = f_i(\beta, d_1, d_2, \dots, d_m), i = 1, 2, \dots, s$. Обчислюємо $\bar{d}_1$ як $N_{\beta_{s-1}}(\bar{d})$, $\bar{d}_2$ як $N_{\beta_{s-2}}(\bar{d}_1), \dots, \bar{d}_{s-1}$ як $N_{\beta_1}(\bar{d}_{s-1})$ та $\bar{d}_s$ як $N_{\beta}(\bar{d}_{s-1})$. Очевидно, що d_s збігається з $(x_1, x_2, \dots, x_n)$. Наведений алгоритм має поліноміальну складність від параметру m . Отже знання розкладу $G = G_1 G_2 \dots G_s$ на символічні перехідні функції дозволяє обчислити прообраз $\bar{d}$ за поліноміальний час.

1.2. Приклад криптосистеми побудованої на відображенні з частково бієктивним розкладом.

Нехай $K = Z_{2^m}$, $Z_{2^m}^*$ мультиплікативна група K , що складається з усіх непарних лишків. У просторі $(Z_{2^m})^n$ розглянемо підмножину $\Omega_n = \{\bar{x} \in K^n \mid x_1 + x_2 + \dots + x_n \in K^*\}$

Теорема 1.4. Існує нескінченна родина поліноміальних відображень $F_n : (Z_{2^m})^n \rightarrow (Z_{2^m})^n$ сталої степені d , яка має частково бієктивний поліноміальний розклад на Ω_n .

Доведення. Розглянемо символічний автомат Шуберта, побудований за родиною графів $D(n, Z_{2^m})$. Нехай $a_1(\bar{x}), a_2(\bar{x}), \dots, a_t(\bar{x}), t = \lfloor \frac{n+2}{4} \rfloor$ буде списком квадратичних інваріантів зв'язності графу. Ми будемо використовувати многочлени f з $Z_{2^m}[u_1, u_2, \dots, u_{t+1}]$. Для такого $f = f(u_1, u_2, \dots, u_{t+1})$ позначимо через $\tilde{f}(z_1, a_1(\bar{z}), a_2(\bar{z}), \dots, a_t(\bar{z}))$. Зрозуміло, що $\tilde{f} \in Z_{2^m}[z_1, z_2, \dots, z_n]$. Для обчислення $\tilde{f}$ маємо ототожнити $(z_1, z_2, \dots, z_n)$ з точкою (прямою) графу $D(n, Z_{2^m})$. Далі будемо використовувати символічне обчислення автомату визначене послідовністю ваг $\alpha_1(\bar{z}) = \tilde{H}(\bar{z}) + \beta_1, \alpha_2(\bar{z}) = z_1 + \beta_2, \alpha_3(\bar{z}) = \tilde{H}(\bar{z}) + \beta_3, \dots, \alpha_{2s}(\bar{z}) = z_1 + \beta_{2s}, \alpha_{2s+1}(\bar{z}) = \tilde{H}(\bar{z}) + \beta_{2s+1}$, де $\beta_i, i = 1, 2, \dots, 2s+1$ являються елементами кільця Z_{2^m} . Нехай $F : Z_{2^m}^n \rightarrow Z_{2^m}^n$ буде поліноміальним відображенням, що генерується цим символічним обчисленням. Нехай многочлен $H(u_1, u_2, \dots, u_{t+1})$ має вигляд $(2R[u_2, u_3, \dots, u_t] + 1)u_1^r + S[u_2, u_3, \dots, u_t]$, де R та S є довільними елементами $K[u_2, u_3, \dots, u_t]$, а число r є непарним з інтервалу $[1, 2^m - 1]$. Розглянемо тепер не вироджене лінійне перетворення $\tau : K^n \rightarrow K^n$ вигляду $x_1 \rightarrow x_1 + x_2 + \dots + x_n, x_2 \rightarrow l_2(x_1, x_2, \dots, x_n), x_3 \rightarrow l_3(x_1, x_2, \dots, x_n), \dots, x_n \rightarrow l_n(x_1, x_2, \dots, x_n)$, де $l_i, i = 2, 3, \dots, n$ довільні лінійні функціонали. Нарешті утворимо композицію $\tau \bullet F = G$. [30, 37]

Нехай тепер $\bar{x} = (x_1, x_2, \dots, x_n)$ належить до Ω_n . Розглянемо $\bar{y} = \tau(\bar{x}) = (y_1, y_2, \dots, y_n)$.

Зрозуміло, що $y_1 \in Z_{2^m}^*$. Покажемо, що прообраз $G(\bar{x})$ визначається однозначно. Розглянемо рівняння $G(\bar{x}) = (b_1, b_2, \dots, b_n)$ для невідомого вектора $\bar{x}$ з Ω_n . Маємо

$$b_1 = (2R[a_1(y_1, y_2, \dots, y_n), a_2(y_1, y_2, \dots, y_n), \dots, a_t(y_1, y_2, \dots, y_n)] + 1)y_1^r + S(a_1(\bar{y}), a_2(\bar{y}), \dots, a_t(\bar{y})) + \beta_{s+1}.$$

Вектори $\bar{y}$ та $\bar{b}$ знаходяться в одній компоненті зв'язності. Тому $a_1(\bar{y}) = a_1(\bar{b}) = \gamma_1, a_2(\bar{y}) = a_2(\bar{b}) = \gamma_2, \dots, a_t(\bar{y}) = a_t(\bar{b}) = \gamma_t$. Таким чином

$$(2R(\gamma_1, \gamma_2, \dots, \gamma_t) + 1)y_1^r + s(\gamma_1, \gamma_2, \dots, \gamma_t) = b_1. \text{ Нехай } r' \in \text{мультиплікативне обернене до } r \text{ в}$$

кільці $Z_{2^{m-1}}$. Можна записати, що $g_1 = \left(\frac{b_1 - s(\gamma_1, \gamma_2, \dots, \gamma_t) - \beta_{2s+1}}{(2R(\gamma_1, \gamma_2, \dots, \gamma_t) + 1)} \right)^{r'} = \alpha$. Знання

параметрів α та $\beta_1, \beta_2, \dots, \beta_t$ дозволяє обчислити всі координати вектора $\bar{y}$.

Справді, обчислимо спочатку нумеричні значення

$$\alpha_{2s} = \alpha + \beta_{2s}, \alpha_{2s-1} = H(\alpha, \gamma_1, \gamma_2, \dots, \gamma_t) + \beta_{2s-1}, \alpha_{2s-2} = \alpha + \beta_{2s-2}, \dots, \alpha_1 = H(\alpha, \gamma_1, \gamma_2, \dots, \gamma_t) + \beta_1, \alpha_0 = \alpha.$$

Значення вектору $\bar{y}$ обчислюємо за наступною рекурсією:

$$\bar{y}^{2s} = N_{\alpha_{2s}}(\bar{b}), \bar{y}^{2s-1} = N_{\alpha_{2s-1}}(\bar{y}^{2s}), \dots, \bar{y}^1 = N_{\alpha_1}(\bar{y}^{(2)}), \bar{y}^0 = N_{\alpha_0}(\bar{y}^1) = (y_1, y_2, \dots, y_n). \text{ Вектор } \bar{x}$$

обчислюється як $\tau^{-1}(y^0)$.

Неважко побачити, що для однозначного обчислення $\bar{x}$ ми використали розклади $G = \tau \cdot F$ та $F(x) = F_1(x) \cdot F_2(x) \cdot \dots \cdot F_{2s+1}(\bar{x})$, де $F_i \in \text{відображенням } \bar{x} \rightarrow N_{\alpha_i(x)}(\bar{x})$ g напівгрупі поліноміальних перетворень простору $(Z_{2^m})^n$. У статті [7] було доведено, що символічне обчислення автомату Шуберта визначене послідовністю ваг $\alpha_i(z)$ як вище при умові $\deg \tilde{H}(z) \geq 1$ має степінь $3 \deg \tilde{H}(z) = c$. Отже й степінь відображення G обмежується цією сталою.[18]

Нехай τ_L буде мономіальним перетворенням простору $Z_{2^m}^n$, що переводить вектор з координатами $(x_1, x_2, \dots, x_n)$ у вектор з координатами $\lambda_i x_{\pi(i)}$, де $\lambda_i \in Z_{2^m}^*$, а π є деякою підстановкою на множині $\{1, 2, \dots, n\}$. Припустимо, що τ_R є бієктивним афінічним перетворенням K^n .

Поліноміальне відображення вигляду $\tau_L F \tau_R$, для F , що задовольняє умовам теореми 1.4 назовемо деформацією F .

Алгоритм з публічним ключем:

Нагадаємо, що не бієктивне відображення $f: Z_m^n \rightarrow Z_m^m$ (m - складне) називається Ейлерівським, якщо рівняння $\tau(x) = \bar{b}, b \in (Z_m^*)^n$ має єдиний розв'язок.

Будемо посилалися на частково бієктивний розклад для F відносно множини $(Z_m^*)^n$ як Ейлерівський розклад.

Деформація Ейлерівського відображення F записується у формі $\tau_L F \tau_R$, де τ_L являється мономіальним перетворенням $x_i \rightarrow \lambda_i x_{\pi(i)}, i = 1, 2, \dots, n, \pi \in S_n$ та τ_R є загальним бієктивним афінним відображенням.

Неважко побачити, що деформація Ейлерівського відображення також буде Ейлерівським перетворенням.

Теорема 1.5. Для кожного складеного m та натурального числа n напівгрупа $S(Z_m^n)$ містить Ейлерівське відображення, що має Ейлерівський розклад та степінь обмежену сталою.[14]

Зауважимо, що функції $H(u_1, u_2, \dots, u_{t+1})$ з конструктивного доведення теореми 1.4 можна надати більш загальний виклад. Наприклад $H(u_1, u_2, \dots, u_{t+1}) = (2R[u_2, u_3, \dots, u_t] + 1) \cdot [(2R_1[u_2, u_3, \dots, u_t] + 1)u_1 + 2S_1(u_2, u_3, \dots, u_t)]^r + S(u_2, u_3, \dots, u_t)$, де R, R_1, S, S_1 обираються довільними елементами кільця $Z_{2^m}[u_2, u_3, \dots, u_t]$. Неважко помітити і множини Ω_n на інші. Наприклад замінити Ω_n на $Z_{2^m}^n - \Omega_n$, змінюючи вираз A у квадратних дужках записаного вище виразу для H на $A+1$. Таким чином доведене наступне твердження.

Теорема 1.6. Існує нескінченна родина поліноміальних відображень $F_n: (Z_{2^m})^n \rightarrow (Z_{2^m})^n$, яка має частково бієктивний розклад на $(Z_{2^m})^n - \Omega_n$.

Розглянемо ідею використання подвійної криптосистеми, що базується на ідеї прихованого RSA.

Аліса вибирає послідовність $F_n: Z_{2^m}^n \rightarrow Z_{2^m}^n$ частково бієктивних на Ω_n відображень з частково бієктивним розкладом теореми 1.4. Вона також

користується послідовністю $G_n : Z_{Z^{2^m}}^n \rightarrow Z_{Z^{2^m}}^n$ з частково бієктивним розкладом, що описується в теоремі 3.[21, 29]

Аліса обирає деформації $F'_n = \tau_L F_n \tau_R$ та $G'_n = \tau'_L G_n \tau'_R$ визначені підстановковими лінійними відображеннями τ_L та τ'_L та загальними афінними перетвореннями τ_R та τ'_R . Вона записує два публічних правила:
 $f_1 \rightarrow f_1(x_1, x_2, \dots, x_n), f_2 \rightarrow f_2(x_1, x_2, \dots, x_n), \dots, f_n \rightarrow f_n(x_1, x_2, \dots, x_n)$ (стандартна символічна форма для F') та $g_i \in Z_{2^m}[x_1, x_2, \dots, x_n]$ (стандартна символічна форма для G'). Ці правила та умова використання F' при $\bar{x} \in \Omega_n$ та G' при $\bar{x} \in Z_{2^m}^n - \Omega_n$ оголошуються публічно.

Публічний користувач (Боб) створює відкритий текст $(p_1, p_2, \dots, p_n) = \bar{p}$, обчислює $\alpha = \sum_{i=1}^n p_i$. При $\alpha \in Z_{2^m}^*$ він відсилає до Аліси вектор $F'(\bar{p}) = \bar{c}$, якщо $\alpha \in Z_{2^m} - Z_{2^m}^*$, то відправляється вектор $G'(\bar{p}) = \bar{c}$.

Аліса декодує, виконуючи такі кроки:

(1) Вона обчислює $\tau_R^{-1}(\bar{c})$.

(2) Розглядає значення $c_1 - s(a_2(\bar{c}), a_3(\bar{c}), \dots, a_t(\bar{c})) = \beta$. Якщо це значення є непарним, то Аліса використає частково бієктивний поліноміальний розклад F' та знаходить $(p_1, p_2, \dots, p_n)$. Якщо β є парним, то Аліса користується частково бієктивним поліноміальним розкладом для G' і знаходить відкритий текст.

Узагальнення на Z_{p^m}

Розглянемо родину графів $D(n, Z_{p^m})$ відповідний їй символічний автомат Шуберта. Нехай послідовність ваг $\alpha_i(x), i = 1, 2, \dots, 2s+1$, що визначається вище залежить від функції $H(u_1, u_2, \dots, u_{t+1})$. Оберемо тепер H , що має вигляд $p(R[u_1, u_2, \dots, u_{t+1}] + \varepsilon_1)[(pR_1[u_1, u_2, \dots, u_t] + \varepsilon_2)u_1 + pS_1(u_1, u_2, \dots, u_{t+1})] + S(u_1, u_2, \dots, u_t)$, де R, R_1, S, S_1 обираються довільними елементами кільця $Z_{p^m}[u_1, u_2, \dots, u_{t+1}]$, $\varepsilon_1, \varepsilon_2 \in \{1, 2, \dots, p-1\}$. Нехай

F_n тепер відображення, що генерується символічним обчисленням, визначеним вище.[8,12,20]

Тоді $G = \tau_L \cdot \tau \cdot F_n \cdot \tau_R$, де τ_L – мономіальне перетворення $(Z_{p^m})^n$, τ задається як невідіржене лінійне перетворення вигляду $x_1 \rightarrow x_1 + x_2 + \dots + x_n, x_2 \rightarrow l_2(\bar{x}), \dots, x_n \rightarrow l_n(\bar{x})$, а τ_R являється загальним афонічним перетворенням, має частково бієктивний поліноміальний розклад відносно множини $\Omega_n = \{\bar{x} \mid \sum x_i \in Z_{p^m}^*\}$.

Змінимо тепер множину Ω_n на її доповнення $\bar{\Omega}_n = Z_{p^m} - \Omega_n$, змінюючи при цьому функцію H заміною виразу A у квадратних дужках на $A+1$. Таким чином отримуємо доведення наступних тверджень.

Теорема 1.7. Існує нескінченна родина поліноміальних відображень $F_n : (Z_{p^m}) \rightarrow (Z_{p^m})$, яка має частково бієктивний поліноміальний розклад на множинах Ω_n .

Теорема 1.8. Існує нескінченна родина поліноміальних відображень $G_n : (Z_{p^m}^n) \rightarrow (Z_{p^m}^n)$, яка має частково бієктивний поліноміальний розклад на множинах $\bar{\Omega}_n = (Z_{p^m})^n - \Omega_n$.

Розглянемо відповідну криптосистему:

1) Аліса вибирає послідовність ваг $\alpha_i(x), i=1,2,\dots,s_n$ обираючи R, R_1, S, S_1 з Z_{p^m} разом зі сталими $\varepsilon_1, \varepsilon_2$ та визначає поліноміальне відображення F_n . Вона обирає афінічні перетворення τ_L, τ та τ_R та обчислює символічну форму $x_i \rightarrow g_i(\bar{x}), i=1,2,\dots,n$ відображення $F_1 = \tau_L \tau \tau_R$. Аліса генерує розклад $F_n = F_1 F_2 \dots F_{s_n}$ та зберігає його безпечним чином.

2) Аліса обирає нову послідовність ваг $\alpha'_i(x), i=1,2,\dots,r_n$ обираючи нові R, R_1, S, S_1 з Z_{p^m} разом зі сталими $\varepsilon_1, \varepsilon_2$ з $\{1,2,\dots,p-1\}$ та визначає поліноміальне відображення G_n , що задовольняє умовам.[22-24]

афінічного простору K^{n+1} . Розглянемо оператор P_α , що переводить ребро $\{(x_1, x_2, \dots, x_n), [y_1, y_2, \dots, y_n]\}$ до ребра $\{(\alpha, z_2, \dots, z_n), [y_1, y_2, \dots, y_n]\}$, де $z_2, z_3, \dots, z_n$ визначається умовою $(\alpha, z_2, z_3, \dots, z_n)[y_1, y_2, \dots, y_n]$. Подібним чином визначено оператор N_β , що переводить ребро $\{(x_1, x_2, \dots, x_n), [y_1, y_2, \dots, y_n]\}$ до ребра $\{(x_1, x_2, \dots, x_n), [\beta, z_2, z_3, \dots, z_n]\}$, де $(z_2, z_3, \dots, z_n)$ визначені умовою .

З'єднаємо два ребра $\bar{l}_1$ та $\bar{l}_2$ напрямленою стрілкою з вагою $(1, \alpha)$, якщо $\bar{l}_2 = P_\alpha(l_1)$. Подібним чином будемо з'єднувати $\bar{l}_1$ та l_2 напрямленою стрілкою з вагою $(-1, \beta)$ якщо $\bar{l}_2 = L_\beta(l_1)$.

Таким чином множину $EA(N, k)$ перетворимо на скінченний автомат, де всі стани прийняті P_α та L_β будуть перехідними функціями цього автомату. Регулярне обчислення автомата визначається початковим станом $\bar{l}$ та послідовністю перехідних функцій вигляду $P_{\alpha_1} L_{\alpha_2} P_{\alpha_3} L_{\alpha_4} \dots P_{\alpha_{2m-1}} L_{\alpha_{2m}}$ або $P_{\alpha_1} L_{\alpha_2} P_{\alpha_3} L_{\alpha_4} \dots L_{\alpha_{2m-2}} P_{\alpha_{2m}}$ або $L_{\alpha_1} P_{\alpha_2} L_{\alpha_3} P_{\alpha_4} \dots L_{\alpha_{2m-1}} P_{\alpha_{2m}}$ або $L_{\alpha_1} P_{\alpha_2} L_{\alpha_3} P_{\alpha_4} \dots P_{\alpha_{2m-2}} L_{\alpha_{2m}}$ (перехідні функції різних типів повинні чергуватися).[38]

Визначимо тепер поняття символічного обчислення, замінивши вирази α_i , елементами кільця $K[x_1, y_1]$. Для спрощення будемо вважати, що символічне обчислення F задається послідовністю $\alpha_1(x_1, y_1), \alpha_2(x_1, y_1), \dots, \alpha_{2m}(x_1, y_1)$ та відповідає набору типу $P_{\alpha_1} L_{\alpha_2} P_{\alpha_3} L_{\alpha_4} \dots P_{\alpha_{2m-1}} L_{\alpha_{2m}}$. Ребро $\{(x_1, x_2, \dots, x_n), [y_1, y_2, \dots, y_n]\}$ ототожнимо з набором $\langle x_1, x_2, \dots, x_n, y_1 \rangle (y_1 = x_{n+1})$. Для обчислення F в точці $\langle p_1, p_2, \dots, p_n, l_1 \rangle = \bar{l}$ потрібно спочатку обчислити $\beta_1 = \alpha_1(p_1, l_1), \beta_2 = \alpha_2(p_1, l_1), \dots, \beta_{2m} = \alpha_{2m}(p_1, l_1)$ та послідовність ребер

$$P_{\beta_1}(\bar{l}) = \bar{l}_1, L_{\beta_2}(\bar{l}_1) = \bar{l}_2, P_{\beta_3}(\bar{l}_2) = \bar{l}_3, L_{\beta_4}(\bar{l}_3) = \bar{l}_4, \dots, P_{\beta_{2m-1}}(\bar{l}_{2m-2}) = \bar{l}_{2m-1}, L_{\beta_{2m}}(\bar{l}_{2m-1}) = \bar{l}_{2m}.$$

Неважко побачити, що F буде поліноміальним відображенням і може бути записаним у вигляді

Значення G в заданій точці може бути обчислене за $O(n^{b+r+5})$ елементарних кроків.

Припустимо тепер, що $K = Z_m, \alpha_{2m-1} = a_1 x_1^{d_1} + b_1$, де $a_1 \in Z_m^*$ та $(d_1, \varphi(m)) = 1$, а $\alpha_{2m} = a_2 x_{n+1}^{d_2} + b_2$, де $a_2 \in Z_m^*$ та $(\alpha_2, \varphi(m)) = 1$

Розглянемо підмножину $P_{n+1} = (Z_m^*)^{n+1}$ в афінічному просторі $(Z_m)^{n+1}$

Твердження 1.4. Розглянемо означене вище відображення F над кільцем Z_m для якого α_i мають вигляд $\alpha x_1^{k_1} x_{n+1}^{k_2} + b, \alpha_{2m-1} = a_1 x_1^{d_1} + b_1, \alpha_{2m} = a_2 x_2^{d_2} + b_2$, де $(a_1, m) = (a_2, m) = 1$ та $(\alpha_1, \varphi(m)) = (\alpha_2, \varphi(m)) = 1$. Нехай τ_L та τ_R являються бієктивним мономіальним та загальним афінічним відображенням простору Z_m^{n+1} та $\Omega_{n+1} = (Z_m^*)^{n+1}$.

Тоді G буде відображенням, що мають частково бієктивний розклад відносно підмножини Ω_{n+1} . Це означає, що G може використати в алгоритмі з публічним ключем за наведеною вище схем.[35]

1.4. Алгебри Каца-Муді та відповідні автомати Шуберта

Узагальненою матрицею Картана $A = (a_{ij}), a_{ij} \in Z, 1 \leq i, j \leq n$ визначається умовами $\forall i a_{ii} = 2, \forall i \forall j a_{ij} \leq 0, (a_{ij} = 0) \Rightarrow a_{ji} = 0$.

Такій матриці відповідає система коренів $\Phi(A)$, що розбивається на додатні та від'ємні корені, що утворюють відповідно множини $\Phi^+ = \Phi^+(A)$ та $\Phi^- = \Phi^-(A)$

Нехай F є полем характеристики нуль Алгебра $L = L_A(F)$ Каца-Муді визначається за парою (A, F) [19]. Вона має розклад $L = L^+ + L_0 + L^-$, де L_0 – її під алгебра Картана, $L^+ = \sum_{\alpha \in \Phi^+} L_\alpha, L^- = \sum_{\alpha \in \Phi^-} L_\alpha, L_\alpha, \alpha \in \Phi$ – однокореневий простір. Розклад визначається системою простих коренів $\alpha_1, \alpha_2, \dots, \alpha_n$. Φ^+ ототожнюється з коренем

вигляду $\sum_{i=1}^n \lambda_i \alpha_i$, де всі λ_i невід'ємні ($\lambda_i \geq 0$), Φ^- містить виключно корені вигляду

$$\sum_{i=1}^n \lambda_i \alpha_i, \text{ де } \forall i \lambda_i \leq 0.$$

Корені спряжені з $\alpha_i, i=1,2,\dots,n$ називаються дійсними, всі інші корені вважаються уявними. Дуальні до α_i елементи α_i^* можна вважати елементами під алгебри Картана. L_0 можна ототожнити з $\langle \alpha_1^*, \alpha_2^*, \dots, \alpha_n^* \rangle$. Нарешті природним чином визначається аналог $L_A(K)$ алгебри $L_A(F)$ над довільним комутативним кільцем K . Підалгебру $L_0 + L^+ = V$ називають під алгеброю Бореля.

В статті [23] визначена геометрія Шуберта для $L_A(K)$. Для $i \in \{1,2,\dots,n\}$ розглянуто многовид $L_i = \sum_{\alpha_i^*(\alpha) > 0} L_\alpha$ та підмножину $\Gamma_i = \{\alpha_i^* + \bar{x} \mid x \in L_i\}$. Геометрія є роздільним об'єднанням $\Gamma_i, i=1,2,\dots,n$. Елементи $\alpha_i^* + \bar{x}$ та $\alpha_j^* + y$ є інцидентними $\alpha_i^* + \bar{x} \mid \alpha_j^* + y$ тоді й лише тоді, коли $[\alpha_i^* + x, \alpha_j^* + y] = 0$.

Нехай l_β це елементи стандартної бази Шевалле при $\beta \in \Phi^+$. Тоді $l_\beta \in L_\beta, [l_\beta \cdot l_\alpha] = \lambda_{\beta,\alpha} l_{\alpha+\beta}$ при $\alpha + \beta \in \Phi^+$ та $[l_\beta \cdot l_\alpha] = 0$ при $\alpha + \beta \notin \Phi^+$. Зазначимо, що $[\alpha_i^*, l_\alpha] = \alpha_i^*(\alpha) l_\alpha$. Наведені вище формули однозначно задають добуток Лі на алгебрі Бореля V_A .

Будемо розглядати випадок, коли ранг матриці Картана дорівнює $n-1$. В цьому випадку система коренів $\Phi(A)$ та групоїд Лі $L_A(K)$ називають афінічним. Відомо, що тоді уявні корені утворюють пряму $\lambda \bar{c}$, де $\lambda \in \mathbb{Z}$, а $\bar{c}$ — мінімальний додатній уявний корінь. Класифікація афінічних систем коренів добре відома кожна така система однозначно задається своєю діаграмою Коксетера-Динкіна. Визначимо апроксимацію $V(\lambda), \lambda \in \mathbb{Z}^+$ алгебри Бореля $L_A(K)$ в афінічному випадку. Для натурального λ розглянемо підмножину $\Phi^+(\lambda)$, яка містить всі додатні корені λ такі, що $\alpha < \lambda c$ у природному лексикографічному порядку на множини Φ^+ .

Вважаємо, що $B(\lambda)$ породжуються елементами $\alpha_i^*, i=1,2,\dots,n$ та $l_\alpha, \alpha \in \Phi^+(\lambda)$. Будемо вважати, що $[\alpha_i^*, l_\alpha] = \alpha_i^*(\alpha)l_\alpha, [l_\alpha, l_\beta] = \lambda_{\alpha,\beta}l_{\alpha+\beta}$ при $\alpha + \beta \in \Phi^+(\lambda)$, $[l_\alpha, l_\beta] = 0$, якщо $\alpha + \beta \notin \Phi^+(\lambda)$. Зафіксуємо матрицю Картана A . За підалгеброю $B(\lambda)$ визначимо наступну систему інциденції. Для $i: 1 \leq i \leq n$ розглянемо множину $L_i(\lambda) = \sum_{\alpha^*(\alpha) > 0, \alpha \in \Phi^+(\lambda)} L_\alpha$. Геометрія $\Gamma_A(\lambda, K)$ є роздільним об'єднанням підмножин $\Gamma_i(\lambda) = \{\alpha_i^* + \bar{x} \mid \bar{x} \in L_i(\lambda)\}$. Елементи $\alpha_i^* + x \in \Gamma_i$ та $\alpha_j^* + y \in \Gamma_j$ будуть інцидентні, коли їх добуток Лі в алгебрі $B(\lambda)$ дорівнює нулю. З означення $\Gamma_A(\lambda, K)$ випливає, що маємо гомоморфізм $\Gamma_A(\lambda+1, K)$ на $\Gamma_A(\lambda, K)$

Твердження 1.5. Проективна границя $\Gamma_A(\lambda, K), \lambda \rightarrow \infty$ збігається із системою $\Gamma_A(K)$.

Максимальний прапор системи інциденції $\Gamma_A(\lambda, K)$ є множиною представників $\alpha_i \in \Gamma_i, i=1,2,\dots,n$ таких, що з $i \neq j$ випливає $\alpha_i \perp \alpha_j$. Будемо вважати, що два максимальні прапори F_1 та F_2 є сусідніми, коли $|F_1 \cap F_2| \geq n-1$.

Многовид максимальних прапорів системи $\Gamma_A(\lambda, K)$ є ізоморфним простору $\sum_{\alpha \in \Phi^+(\lambda)} L_\alpha = L_\lambda$. Зафіксуємо стандартний порядок $\{\alpha_1, \alpha_2, \dots, \alpha_{N_\lambda}\}$ на множині $\Phi^+(\lambda)$. Не обмежуючи загальності будемо вважати, що $\alpha_1, \alpha_2, \dots, \alpha_n$ буде списком простих коренів. Тоді прапор F ототожнюється з вектором $(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{N_\lambda})$ з афінічного простору L_λ . Не важко побачити, що для кожного прапору $F_1 = (x_{\alpha_1}, x_{\alpha_2}, \dots, x_{N_\lambda})$ існує єдиний коректно визначений сусідній до F_1 прапор $F_2 = N_i^t(F_1)$, такий що $F_1 \not\sim F_2$ та $F_2 = (y_{\alpha_1}, y_{\alpha_2}, \dots, y_{\alpha_{N_\lambda}})$, де $y_{\alpha_i} = t, t \in K$. [31-34]

Перетворимо афінічний простір L_λ у скінченний автомат за допомогою з'єднання $\bar{x} = (x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_{N_\lambda}})$ та $\bar{y} = (y_{\alpha_1}, y_{\alpha_2}, \dots, y_{\alpha_{N_\lambda}})$ напрямленою стрілкою з вагою (i, t) . Очевидно, що при $t = x_{\alpha_i}$ виникає петля з вагою (i, x_{α_i}) .

Кожен вектор $\bar{x} \in L_\lambda$ будемо вважати придатним станом (accepting state) цього автомату.

Очевидно, що оператор N_i^t буде перехідною цього автомату. Визначений вище автомат будемо називати автоматом Шуберта системи інциденції $\Gamma_A(\lambda, K)$.

Регулярне обчислення цього автомату задається послідовністю ваг $(i_1, t_1), (i_2, t_2), \dots, (i_m, t_m)$ такою що $i_s \neq i_{s+1}, s = 1, 2, \dots, m-1$ та початковим станом $\bar{p} = (p_{\alpha_1}, p_{\alpha_2}, \dots, p_{\alpha_{N_\lambda}})$. Воно відповідає обчисленню послідовності $\bar{p}_1 = N_{i_1}^{t_1}(p), \bar{p}_2 = N_{i_2}^{t_2}(\bar{p}_1), \dots, \bar{p}_m = N_{i_m}^{t_m}(\bar{p}_{m-1})$. Стан $\bar{p}_m$ вважаємо результатом обчислення.

Визначимо тепер символічний автомат Шуберта системи $FA(\lambda, K)$ шляхом розгляду загального стану $(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_{N_\lambda}})$, де x_{α_i} - змінні, та заміною параметрів $t_1, t_2, \dots, t_m$ у наведеному вище означенні на елементи $f_1(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_{N_\lambda}}), f_2(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_n}), \dots, f_m(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_n})$, де $f_i, i = 1, 2, \dots, m$ належать до комутативного кільця $K[x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_n}]$. Таким чином визначено послідовність поліноміальних відображень $G_{i_1}^{f_{i_1}}, G_{i_2}^{f_{i_2}}, \dots, G_{i_m}^{f_{i_m}}$ таких що $G_{i_s}^{f_{i_s}}(p_{\alpha_1}, p_{\alpha_2}, \dots, p_{\alpha_N}) = N_{i_s}^{t_s}(p_{\alpha_1}, p_{\alpha_2}, \dots, p_{\alpha_{N_\lambda}})$, де $t_s = f_s(p_1, p_2, \dots, p_n)$.

Символічне обчислення автомату Шуберта для $\Gamma_A(\lambda, K)$ є відображення, що є композицією $G_{i_1}^{f_{i_1}(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_n})}, G_{i_2}^{f_{i_2}(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_n})}, \dots, G_{i_m}^{f_{i_m}(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_n})}$. Воно переводить вектор $\bar{x} = (x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_{N_\lambda}})$ до деякого $\bar{y} = (y_{\alpha_1}, y_{\alpha_2}, \dots, y_{\alpha_{N_\lambda}})$, де y_{α_i} є елементами $K[x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_n}]$. Неважко побачити, що $y_{\alpha_{i_m}} = f_m(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_n})$.

Будемо називати функції $f_j(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_n})$ напрямлюючими функціями символічного обчислення G . Символічне обчислення можна записати у стандартному вигляді:

$$\begin{aligned}
x_{\alpha_1} &\rightarrow g_1(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_{N_\lambda}}) \\
x_{\alpha_2} &\rightarrow g_2(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_{N_\lambda}}) \\
&\dots\dots\dots \\
x_{\alpha_n} &\rightarrow g_n(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_{N_\lambda}}) \\
x_{\alpha_{n+1}} &\rightarrow g_{n+1}(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_{N_\lambda}}) \\
&\dots\dots\dots \\
x_{N_\lambda} &\rightarrow g_{N_\lambda}(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_{N_\lambda}})
\end{aligned}$$

де многочлени g_i задані списками своїх мономів, що відповідають певному порядку на змінних $x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_{N_\lambda}}$.

Неважко побачити, що $g_1, g_2, \dots, g_n$ є напрямлюючими функціями, тобто $g_{i_s} = f_{k_s}(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_n})$ де k_s є останньою появою символу s у послідовності $i_1, i_2, \dots, i_m$. Якщо такої появи немає, то $g_{i_s} = x_{i_s}$. Далі будемо вважати, що $\{i_1\} \cup \{i_2\} \cup \dots \cup \{i_m\} = \{1, 2, \dots, n\}$. [13]

Нехай G визначено послідовністю ваг $(i_1, f_1), (i_2, f_2), \dots, (i_m, f_m)$. Розглянемо мономіальне лінійне перетворення τ_L простору K^{N_λ} , що переводить набір $(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_{N_\lambda}})$ до $(\Delta_1 x_{\pi(\alpha_1)}, \Delta_2 x_{\pi(\alpha_2)}, \dots, \Delta_{N_\lambda} x_{\pi(\alpha_{N_\lambda})})$, де π є підстановкою на множині $\{\alpha_1, \alpha_2, \dots, \alpha_{N_\lambda}\}$, а параметри $\Delta_1, \Delta_2, \dots, \Delta_{N_\lambda}$ належать до K^* (мультиплікативної групи кільця K).

Нехай τ_R буде загальним біективним афінічним відображенням простору K^{N_λ} в себе вигляду $\bar{x} \rightarrow \bar{x}A + \bar{b}$, де $\bar{b}$ – фіксований вектор з K^n , а матриця A має обернену.

Перетворення вигляду $\tilde{G} = \tau_L G \tau_R$ будемо називати деформацією символічного обчислення G . Будемо вважати параметр n сталою. Відображення G , яке задається послідовністю ваг $(i_1, f_1), (i_2, f_2), \dots, (i_m, f_m)$ таких що $m = c\lambda$, кількість одночленів в кожному f обмежено сталою c_1 , степені f_i обмежені сталою c_2 будемо називати ручним обчисленням.

Твердження 1.6. Нехай A матриця Картана афінічної алгебри. Тоді ручне обчислення автомату Шуберта системи інциденції $\Gamma_A(\lambda, K)$ є відображенням поліноміальної степені $O(\lambda)$ та поліноміальної густини $O(\lambda^3)$.

Наслідок 1.4. Деформація ручного обчислення автомату Шуберта системи $\Gamma_A(\lambda, K)$ є відображенням поліноміальної степені $O(\lambda)$ та поліноміальної густини $O(\lambda^4)$.

Лема 1.1. Параметр N_λ має розмір $O(\lambda)$.

Нехай тепер $K = Z_t$ та стандартне представлення обчислення G має вигляд

$$\begin{aligned} x_{\alpha_1} &\rightarrow a_1 x_{\alpha_{i_1}}^{r_1} + b_1 \\ x_{\alpha_2} &\rightarrow a_2 x_{\alpha_{i_2}}^{r_2} + b_2 \\ &\dots\dots\dots \\ x_{\alpha_n} &\rightarrow a_n x_{\alpha_{i_n}}^{r_n} + b_n \\ x_{\alpha_{n+1}} &\rightarrow g_{n+1}(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_{N_\lambda}}) \\ x_{\alpha_{n+2}} &\rightarrow g_{n+2}(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_{N_\lambda}}) \\ &\dots\dots\dots \\ x_{\alpha_{N_\lambda}} &\rightarrow g_{N_\lambda}(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_{N_\lambda}}) \end{aligned}$$

де $i_1, i_2, \dots, i_n$ – перестановка символів $1, 2, \dots, n$, де $(r_i, \varphi(t)) = 1, i = 1, 2, \dots, n$ (φ – стандартне означення функції Ейлера). В цьому випадку G будемо називати відображенням Ейлерівського типу.

Теорема 1.10. Нехай G є відображенням Шуберта системи $\Gamma_A(\lambda, K)$, що має Ейлерівський тип, тоді його обмеження на $(Z_t^*)^{N_\lambda}$ є ін'єктивним відображенням.

Наслідок 1.5. Деформація $\tilde{G}$ для G , що задовольняє умові теореми 1.10 є ін'єктивним відображенням. [27, 39]

Приклад криптосистеми

Припустимо, що власник публічного ключа (Аліса) використовує інформацію про символічний автомат Шуберта системи інциденції $\Gamma_A(\lambda, K)$. Вона обрала

У сучасній криптографії деякі відомі системи мають різний розмір простору відкритих текстів та багатовиду шифрограм. Криптосистема Ель Гамала була історично першим прикладом такого типу. Все ж більшість криптосистем використовує той самий простір для множин відкритих текстів та шифрограм. Такий випадок є зручним для користувачів.

Припустимо, що поліноміальне відображення від багатьох змінних F_n простору $(Z_m)^n$ у себе має Ейлерівський розклад $F_n = F^1 \cdot F^2 \cdot \dots \cdot F^{s(n)}$ для множини Ω_n в $(Z_m)^n$. Інше відображення G_n має також Ейлерівський розклад $G_n = G^1 G^2 \dots G^{t(n)}$ для доповнення $\tilde{\Omega}_n = (Z_m)^n - \Omega_n$ множини Ω_n

Припустимо, що $F_n(\Omega_n) \cap G_n(\Omega_n) = \emptyset$, для $n = 2, 3, \dots$. Розглянемо взаємно-однозначне відображення

$$D_n(x) = \begin{cases} F_n(x), \bar{x} \in \Omega_n \\ G_n(x), \bar{x} \in \tilde{\Omega}_n \end{cases}$$

Будемо називати $D_n(x)$ дводольним Ейлерівським відображенням для розбиття $(\Omega_n, \tilde{\Omega}_n)$. [20, 23]

Нехай K буде кільцем Z_{2^m} . Розглянемо розбиття афінічного простору $Z_{2^m}^n$ на дві множини $\Omega_n = \{\bar{x} \in Z_{2^m}^n \mid \sum x_i = 0 \pmod{2}\}$ та його доповнення $\bar{\Omega}_n = Z_{2^m}^n - \Omega_n$. Припустимо, що два відображення P_n та Q_n є такими, що їх обмеження $P_n|_{\Omega_n}$ та $Q_n|_{\bar{\Omega}_n}$ на множини Ω_n та $\bar{\Omega}_n$ являються ін'єктивними перетвореннями та $P_n(\Omega_n) \cap Q_n(\bar{\Omega}_n) = \emptyset$. Тоді правило

$$D_n(\bar{x}) = \begin{cases} P_n(\bar{x}), \bar{x} \in \Omega_n \\ Q_n(x), x \in \tilde{\Omega}_n \end{cases}$$

задає бієктивне відображення афінічного простору $Z_{2^m}^n$ у себе.

Ми можемо створити пару P_n, Q_n , що задає $D_n(x)$ як вище розглянувши $P_n = \tau_L \tau F_n \tau_R$ і $\tau'_L \tau' G_n \tau_R$ зі спеціальними функціями H та H' вигляду

$$H(a_2(x), a_3(x), \dots, a_n(x)) = 2T(a_2(x), a_3(x), \dots, a_t(x))$$

та

$$H'(a_2(x), a_3(x), \dots, a_n(x)) = 2T'(a_2(x), a_3(x), \dots, a_t(x)) + 1$$

Навіть, коли відображення $D_n(x)$ збігається з поліноміальним бієктивним відображенням F вигляду $x_1 \rightarrow f_1(x_1, x_2, \dots, x_n), x_2 \rightarrow f_2(x_1, x_2, \dots, x_n), \dots, x_n \rightarrow f_n(x_1, x_2, \dots, x_n)$ форму F та F^{-1} важко знайти. Зауважимо, що F може бути відображенням необмеженої степені або густини.

Припустимо, що P_n та Q_n як вище, мають частково бієктивні декомпозиції $P_n = P_n^1 \cdot P_n^2 \cdot \dots \cdot P_n^{k(n)}$ та $Q_n = Q_n^1 \cdot Q_n^2 \cdot \dots \cdot Q_n^{r(n)}$ тоді відображення D_n та відповідну криптосистему будемо називати дводольними. Будемо вживати термін дводольна Ейлерівська криптосистема у випадку обраних вище $P_n = \tau_L \tau F_n \tau_R$ та $Q_n = \tau'_L \tau' G_n \tau_R$ які залежать від $H(x)$ та $H'(\bar{x})$. Розглянемо цей випадок з усіма подробицями.

Аліса обирає параметри m та n , що визначають афінічний простір $Z_{2^m}^n$. Вона вибирає функції $H(x)$ та $H'(x)$ і параметри, що визначають обчислення, що генерують перетворення F_n та G_n , що розкладаються у композиції $F^1 F^2 \dots F^{s(n)}$ та $G^1 G^2 \dots G^{r(n)}$. Аліса також обирає афінічні перетворення $\tau_L, \tau'_L, \tau, \tau'$ та перетворення τ_R . Використовуючи ці дані вона генерує дводольне Ейлерівське відображення D_n , що задається множиною Ω_n і відображеннями P_n та Q_n афінічного простору. Воно оголошується публічним правилом для користувачів.

Один з них (Боб) створює своє послання $(p_1, p_2, \dots, p_n)$. Він обчислює $p_1 + p_2 + \dots + p_n = \alpha$. Коли α парне, то він відсилає до Аліси $Q_n(p_1, p_2, \dots, p_n) = \bar{c}$. У випадку непарного α шифрограма $\bar{c}$ обчислюється як $P_n(p_1, p_2, \dots, p_n) = \bar{c}$.

Аліса одержує $\bar{c}$, обчислює $\tau_R(\bar{c}) = (l_1, l_2, \dots, l_n) = \bar{l}$. Якщо l_1 – парне число, то далі Аліса користується частково бієктивним розкладом для $Q_n = \tau'_L \tau' G_n \tau$, де $G_n = G^1 G^2 \dots G^{r(n)}$. Вона обчислює $(G_n)^{-1}(\bar{l}) = \bar{u}$ та початковий текст $\tau_L^{-1}((\tau')^{-1}(\bar{u})) = \bar{p}$. Якщо l_1 непарне, то Аліса обчислює $(F_n)^{-1}(\bar{l}) = \bar{u}$ та $\tau_L^{-1}(\tau^{-1}(u)) = (p_1, p_2, \dots, p_n)$

1.6. Дводольні криптосистеми над кільцями Z_{p^m}

Нехай K буде кільцем Z_{p^m} , $p > 2$. Розглянемо розбиття афінічного простору $(Z_{p^m})^n$ на дві підмножини $\Omega_n = \{x \in (Z_{p^m})^n \mid \sum_{i=1}^n x_i = 0(\bmod p)\}$ та його доповнення $\overline{\Omega}_n = (Z_{p^m})^n - \Omega_n$. Побудуємо два відображення P_n та Q_n такі, що їх обмеження $P_n|_{\Omega_n}$ та $P_n|_{\overline{\Omega}_n}$ на Ω_n та $\overline{\Omega}_n$ будуть ін'єктивними перетвореннями та $P_n(\Omega_n) \cap Q_n(\overline{\Omega}_n) = \emptyset$.

Для цього розглянемо обчислення автомату Шуберта графу $D(n, Z_{p^m})$, що задаються послідовністю ваг

$$\begin{aligned} v_1(x) &= x_1 + \tilde{H}(\bar{x}) + \beta_1, v_2(x) = x_1 + \beta_2, v_3(x) = x_1 + \tilde{H}(\bar{x}) + \beta_3, \dots, \\ v_{2s}(x) &= x_1 + \beta_{2s}, v_{2s+1}(x) = x_1 + \tilde{H}(\bar{x}) + \beta_{2s+1} \end{aligned}$$

Параметр $s = s(n)$ задається деякою поліноміальною функцією від n , функція $\tilde{H}(x) = (R_1(a_1(x), a_2(x), \dots, a_t(x)) [R_2(a_1(x), a_2(x), \dots, a_t(x)) \cdot x_1^r + R_3(a_1(x), a_2(x), \dots, a_t(x))] + R_4(a_1(x), a_2(x), \dots, a_t(x))$

Функції $R_i(x), i=1,2$ мають вигляд $ph(a_1(x), a_2(x), \dots, a_t(x)) + \alpha_i, \alpha_i \in Z_{p^m}^*$, де $h(z_1, z_2, \dots, z_t) \in Z_{p^m}[z_1, z_2, \dots, z_t]$. Функції R_3 та R_4 підібрані як вирази вигляду $p \cdot h(a_1(\bar{x}), a_2(\bar{x}), \dots, a_t(\bar{x}))$. Зауважимо, що всі значення функції $\tilde{H}(x)$ при умові регулярності параметру x_1 будуть регулярними елементами кільця Z_p^m . Будемо вважати, що $\beta_{2s+1} = 0(\bmod p)$. [26]

Позначимо функцію генеровану наведеним вище обчисленням через $F_n : (Z_{p^m})^n \rightarrow (Z_{p^m})^n$.

Побудуємо іншу функцію G_n , що перетворює $(Z_{p^m})^n$, обираючи $\tilde{H}(x)$ у інший спосіб.

Покладемо тепер, що функції $R_i(a_1(\bar{x}), a_2(\bar{x}), \dots, a_t(\bar{x})), i=1,2$ мають вигляд $p \cdot h(a_1(x), a_2(x), \dots, a_t(x)) + 1$. Вирази R_3 та R_4 як і раніше мають вигляд $p \cdot h(a_1(x), a_2(x), \dots, a_t(x))$. Змінимо тепер вираз x_1^r на $(x_1 + 1)$. Параметр β_{2s+1} вибирається як елемент для якого $\beta_{2s+1} = p - 1 \pmod p$. Розглянемо деформації $P_n = \tau_L F_n \tau_R$ та $Q_n = \tau'_L G_n \tau'_R$, де τ_L та τ'_L являються підстановковими лінійними перетвореннями, τ та τ' - бієктивними перетвореннями вигляду $x_1 \rightarrow x_1 + x_2 + \dots + x_n$, $x_2 \rightarrow l_2(x_2, x_3, \dots, x_n), \dots, x_n \rightarrow l_n(x_2, x_3, \dots, x_n)$, де $l_i, i = 2, 3, \dots, n$ є загальними виразами вигляду $a_1 x_1 + a_2 x_2 + \dots + a_n x_n + a_{n+1}$, $a_i \in Z_{p^m}, i = 1, 2, \dots, n+1$.

Розглянемо відповідний до пари родин P_n та Q_n алгоритм кодування з публічним ключем.

Аліса (створювач та власник ключа публічного) генерує функцію $\tilde{H}(x)$ як описаного вище, та створює різні відображення F_n та G_n . Вона обирає трійки τ_L, τ, τ_R та τ'_L, τ', τ'_R та генерує відображення $P_n = \tau_L F_n \tau_R$ та $Q_n = \tau'_L G_n \tau'_R$ у стандартній символічній формі, що є списком одночленів записаних в обраному порядку.

Аліса оголошує публічні правила для побудованих $P = P_n$ та $Q = Q_n$ вигляду $x_1 \rightarrow P^1(x_1, x_2, \dots, x_n), x_2 \rightarrow P^2(x_1, x_2, \dots, x_n), \dots, x_n \rightarrow P^n(x_1, x_2, \dots, x_n)$ та $x_1 \rightarrow Q^1(x_1, x_2, \dots, x_n), x_2 \rightarrow Q^2(x_1, x_2, \dots, x_n), \dots, x_n \rightarrow Q^n(x_1, x_2, \dots, x_n)$ відповідно. Вона зберігає всі дані, що було використано для створення P_n та Q_n у секреті.

Один з публічних користувачів (Боб) створює свій відкритий текст $(p_1, p_2, \dots, p_n)$. Він обчислює $p_1 + p_2 + \dots + p_n = \alpha$. Якщо параметр $\alpha \pmod p$ дорівнює нулю, то він записує шифрограму $Q_n(p_1, p_2, \dots, p_n) = (c_1, c_2, \dots, c_n)$. При умові $\alpha \neq 0 \pmod p$ шифрограма $\bar{c} = (c_1, c_2, \dots, c_n)$ обчислюється як $P_n(c_1, c_2, \dots, c_n)$. Боб відправляє створену шифрограму до Аліси.[7, 11]

Аліса декодує в наступний спосіб. Вона обчислює $\tau_R^{-1}(\bar{c}) = (u_1, u_2, \dots, u_n)$ та розглядає параметр $\beta = u_1 \pmod{p}$. Зауважимо, що заміна τ_R на τ'_R дає те саме значення β .

Якщо $\beta = 0 \pmod{p}$ то Аліса використає розклад $Q_n = \tau'_L \tau' G^{(1)} G^{(2)} \dots G^{2s'+1} \tau'_R$.

Цей розклад є частково бієктивним розкладом Q для множини $\tilde{\Omega}_n$. Аліса використовує $\bar{c}$ та обчислює початковий текст $(p_1, p_2, \dots, p_n)$.

Якщо ж $\beta \neq 0 \pmod{p}$, то Аліса користується розкладом $P_n = \tau_L \tau F^{(1)} F^{(2)} \dots F^{(2s+1)} \tau_R$, що є частково бієктивним розкладом до множини $\tilde{\Omega}_n$ і відновлює $(p_1, p_2, \dots, p_n)$.

Розглянемо, наприклад, випадок $\beta = 0$. Аліса обчислює $\tau'_R(\bar{c}) = v_1, v_2, \dots, v_n = \bar{v}$. Вона обчислює також інваріанти $d_1 a_1(\bar{v}), d_2 a_2(\bar{v}), \dots, d_t a_t(\bar{v})$. Потім Аліса обчислює значення $R_i(d_1, d_2, \dots, d_t) = m_i, i = 1, 2, 3, 4$ та записує рівняння $m_1[m_2(x_1 + 1)^r + m_3] + m_4 + \beta_{2s+1} = v_1$. Роблячи еквівалентні перетворення, вона записує $(x_1 + 1)^r = d$. Знаходить мультиплікативне обернене r' до r в групі $Z_{p^m - p^{m-1}}$. Таким чином $x_1 = d^{r'} - 1 = \gamma$. Аліса обчислює значення параметру $m_1[m_2(\gamma + 1)^r + m_3] + m_4 = h_0$. Після цього розглядається послідовність $\gamma, h_0 + \beta_1, \gamma + \beta_2, h_0 + \beta_3, \dots, \gamma + \beta_{2s}, h_0 + \beta_{2s+1}$. Аліса записує таку послідовність векторів $\bar{v}_{2s}^1 = N_{\gamma + \beta_{2s}}(\bar{v}), \bar{v}_{2s-1}^2 = N_{h_0 + \beta_{2s-1}}(\bar{v}_{2s}^1), \dots, \bar{v}_1 = N_{h_0 + \beta_1}(\bar{v}_2), \bar{v}_0 = N_{\gamma}(\bar{v}_1)$. Неважко побачити, що $\bar{v}_0 = \tau'_L \tau'(\bar{p})$.

1.7. Автомати Шуберта для систем коренів $A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4, G_2$ над довільним комутативним кільцем

Відомо, що для визначення групи Шевалле $A_n(K), B_n(K), C_n(K), D_n(K), E_6(K), E_7(K), E_8(K), F_4(K), G_2(K)$ потрібно розглянути групоїд $Li L_\Phi^Z$, де Φ один з коренів системи $A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4, G_2$, визначений над

кільцем цілих чисел Z . Система коренів ϕ розбивається на множини Φ^+ та Φ^- додатніх та від'ємних коренів, відповідно. Алгебра Лі $L_\phi(K)$ визначається як тензорний добуток $L_\phi(r)$ на кільце K . За алгеброю Лі $L_\phi(K)$ визначається приєднана група $G_\phi(K)$ [25, 26, 28]. Алгебра Лі $L_\phi(K)$ має розклад $L^+ + L_0 + L^-$, де L_0 буде алгеброю Картана у $L_\phi(K)$, $L^+(L^-)$ є сумою однокоренових підпросторів L_α , де α належить списку Φ^+ додатніх коренів (Φ^- від'ємних коренів).

Нехай $U_\phi(K)$ буде уніпотентною підгрупою приєднаної групи $G_\phi(K)$. Нагадаємо, що $U = U_\phi(K)$ являється приєднаною групою під алгебри L^+ . Нехай $U^i = U_{\phi^i}(K)$ це однокоренева підгрупа в $U_\phi(K)$, що відповідає простому кореню $\alpha_i, i = 1, 2, \dots, n$.

Розглянемо наступну систему інциденції $\Gamma(U)$, яка утворюється роздільним об'єднанням множин Γ_i утворених класами суміжності $(U : U_i)$, $i = 1, 2, \dots, n$. Відношення інциденції визначено за правилом : $\alpha \in \Gamma_i$ та $\beta \in \Gamma_j$ є інцидентними $\alpha I \beta$ тоді й лише тоді, коли перетин α та β є непорожнім при $i \neq j$.

Максимальний прапор $\Gamma(U_\phi(K))$ є множиною представників $\alpha_i \in \Gamma_i, i = 1, 2, \dots, n$ таких, що $i \neq j$ впливає $\alpha_i I \alpha_j$.

Будемо вважати, що два максимальні прапори F_1 та F_2 є сусідніми $(F_1 \phi F_2)$, коли $|F_1 \cap F_2| \geq n - 1$.

Многовид максимальних прапорів є ізоморфним алгебрі Лі L^+ , що розкладається в пряму суму однокоренових просторів $L_\alpha, \alpha \in \Phi^+$. Зафіксуємо стандартний порядок $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ на $\Phi^+ (|\Phi^+| = N)$. Не обмежуючи загальності будемо вважати, що $\alpha_1, \alpha_2, \dots, \alpha_n$ буде списком простих коренів. Тоді прапор F ототожнюється з вектором $(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_n})$ афінічного простору L_ϕ^+ . Неважко побачити, що для прапору $F_1 = (x_{\alpha_1} x_{\alpha_2} \dots x_{\alpha_n})$ існує єдиний коректно визначений

сусідній до F_1 прапор $F_2 = N_i(F_1)$, такий що $(F_1 \not\subseteq F_2)$ та $F_2 = (y_{\alpha_1}, y_{\alpha_2}, \dots, y_{\alpha_N})$, де $y_{\alpha_i} = t, t \in K$.

Перетворимо афінічний простір L_Φ^+ у скінченний автомат за допомогою з'єднання $\bar{x} = (x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_N})$ та $\bar{y} = (y_{\alpha_1}, y_{\alpha_2}, \dots, y_{\alpha_N})$ напрямленою стрілкою з вагою (i, t) . Очевидно, що при $t = x_{\alpha_i}$ виникає петля з вагою (i, x_{α_i}) . Кожен вектор $\bar{x} \in L_\Phi^+$ будемо вважати придатним станом (accepting state) цього автомату. Очевидно, що оператор N_i^+ буде перехідною функцією цього автомату, який далі називатимемо автоматом Шуберта типу Φ над комутативним кільцем K . [35]

Регулярне обчислення автомата Шуберта задається послідовністю ваг $(i_1, t_1), (i_2, t_2), \dots, (i_m, t_m)$ такою що $i_s \neq i_{s+1}, s = 1, 2, \dots, m-1$ та початковим станом $\bar{p} = (p_{\alpha_1}, p_{\alpha_2}, \dots, p_{\alpha_N})$. Воно відповідає обчисленню послідовності $\bar{p}_1 = N_{i_1}^{t_1}(\bar{p}), \bar{p}_2 = N_{i_2}^{t_2}(\bar{p}_1), \dots, \bar{p}_m = N_{i_m}^{t_m}(\bar{p}_{m-1})$, стан $\bar{p}_m$ вважаємо результатом обчислення.

Визначимо тепер символічний автомат Шуберта шляхом розгляду загального стану $(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_N})$, де x_{α_i} - змінні, та заміною параметрів $t_1, t_2, \dots, t_m$ у наведеному вище означенні на елементи $f_1(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_N}), f_2(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_N}), \dots, f_m(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_N})$, де $f_i, i = 1, 2, \dots, m$ належать до комутативного кільця $K[x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_N}]$. Таким чином визначено послідовність поліноміальних відображень $G_{i_1}^{f_{i_1}}, G_{i_2}^{f_{i_2}}, \dots, G_{i_m}^{f_{i_m}}$ таких, що $G_{i_s}^{f_{i_s}}(p_{\alpha_1}, p_{\alpha_2}, \dots, p_{\alpha_N}) = N_{i_s}^{t_s}(p_{\alpha_1}, p_{\alpha_2}, \dots, p_{\alpha_N})$, де $t_s = f_s(p_{\alpha_1}, p_{\alpha_2}, \dots, p_{\alpha_N})$. Перехідна функція символічного автомату Шуберта, що відповідає $(i_1, f_1), (i_2, f_2), \dots, (i_m, f_m)$ є відображенням G вектору $\bar{x} = (x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_N})$ у $G_{i_1}^{f_1(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_N})}, G_{i_2}^{f_2(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_N})}, \dots, G_{i_m}^{f_m(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_N})}(\bar{x}) = \bar{y}$. Неважко побачити, що $y_{\alpha_{i_m}} = f_m(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_N})$.

Будемо називати функції $f_j = (x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_N})$ напрямляючими функціями символічного числення G . Символічне обчислення можна задати списком:

$$\begin{aligned}
x_1 &\rightarrow g_1(x_1, x_2, \dots, x_N) \\
x_2 &\rightarrow g_2(x_1, x_2, \dots, x_N) \\
&\dots\dots\dots \\
x_n &\rightarrow g_n(x_1, x_2, \dots, x_N) \\
x_{n+1} &\rightarrow g_{n+1}(x_1, x_2, \dots, x_N) \\
x_{n+2} &\rightarrow g_{n+2}(x_1, x_2, \dots, x_N) \\
&\dots\dots\dots \\
x_N &\rightarrow g_N(x_1, x_2, \dots, x_N)
\end{aligned}$$

де многочлени g_i задані списками своїх мономів, що відповідають певному порядку на змінних $x_1, x_2, \dots, x_n$. Неважко побачити, що $g_1, g_2, \dots, g_n$ є напрямлюючими функціями $g_s = f_{k_s}(x_1, x_2, \dots, x_n)$, де k_s є номер останньої появи символу s у послідовності $i_1, i_2, \dots, i_m$. Далі будемо вважати, що $\{i_1\} \cup \{i_2\} \cup \dots \cup \{i_m\} = \{1, 2, \dots, n\}$.

Нехай G визначено послідовністю символічних ваг $(i_1 f_1), (i_2 f_2), \dots, (i_m f_m)$. Розглянемо мономіальне лінійне перетворення σ_L простору K^N , що переводить набір $(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_N})$ до $(\lambda_1 x_{\pi(\alpha_1)}, \lambda_2 x_{\pi(\alpha_2)}, \dots, \lambda_N x_{\pi(\alpha_N)})$, де π є підстановкою на множині $\{\alpha_1, \alpha_2, \dots, \alpha_N\}$, а параметри $\lambda_1, \lambda_2, \dots, \lambda_N$ належать до K^* (мультиплікативна група кільця K). Нехай τ_R це загальне афонічне відображення простору K^N в себе вигляду $\bar{x} \rightarrow \bar{x}A + \bar{b}$, де $\bar{b}$ - фіксований вектор з K^N , а матриця A має обернену.

Перетворення вигляду $G = \tau_L G \tau_R$ будемо називати деформацією символічного обчислення G .

Відображення G , яке задається послідовністю ваг $(i_1 f_1), (i_2 f_2), \dots, (i_m f_m)$ таких, що $m = c_1 n$, кількість одночленів в кожному f_i обмежена сталою c_2 , степені многочленів обмежені сталою c_3 будемо називати ручним обчисленням.

Твердження 1.7. Нехай Φ є однією з систем коренів A_n, B_n, C_n, D_n . Тоді ручне обчислення є відображенням поліноміальної степені $O(n^{d_1})$ та поліноміальної густини $O(n^d)$.

Наслідок 1.6. Деформація ручного обчислення автомата Шуберта є відображенням поліноміальної степені та поліноміальної густини.

Зауваження 1.2. Поліноміальні степінь та густина відображення з твердження обмежені $O(n^3)$ та $O(n^4)$. [9, 14, 18]

Зазначимо, що відображення G та $\tilde{G}$ мають однакові степені, густина відображення $\tilde{G}$ може бути більшою в n^2 рази від густини G

Нехай тепер $K = Z_t$ та стандартне представлення обчислення G має вигляд

$$\begin{aligned} x_{\alpha_1} &\rightarrow a_1 x_{i_1}^{r_1} + b_1 \\ x_{\alpha_2} &\rightarrow a_2 x_{i_2}^{r_2} + b_2 \\ &\dots\dots\dots \\ x_{\alpha_n} &\rightarrow a_n x_{i_n}^{r_n} + b_n \\ x_{\alpha_{n+1}} &\rightarrow g_{n+1}(x_1, x_2, \dots, x_N) \\ x_{\alpha_{n+2}} &\rightarrow g_{n+2}(x_1, x_2, \dots, x_N) \\ &\dots\dots\dots \\ x_N &\rightarrow g_N(x_1, x_2, \dots, x_N) \end{aligned}$$

де $i_1, i_2, \dots, i_n$ перестановка символів $1, 2, \dots, n$, де $(r_i, \varphi(t)) = 1, i = 1, 2, \dots, n$ φ – функція Ейлера. В цьому випадку G будемо називати відображенням Ейлерівського типу.

Твердження 1.8. Нехай $G \in$ відображенням Шуберта Ейлерівського типу тоді його обмеження на $(Z_t^*)^N$ є ін'єктивним відображенням.

Наслідок 1.7. Деформація $\tilde{G}$ для G обмежена на $(Z_t^*)^N$ є ін'єктивним відображенням. [12]

Приклад криптосистеми

Розглянемо для системи коренів одного з типів A_n, B_n, C_n та D_n ручне обчислення символічного автомату Шуберта, що визначає відображення Ейлерівського типу.

Припустимо, що власник публічного ключа (Аліса) має відомості про символічний автомат Шуберта та напрямляючі функції $f_1, f_2, \dots, f_m$ ручного

Ейлерівського обчислення. Вона обирає мономіальне перетворення τ_L простору Z_t^N та загальне бієктивне перетворення τ_R з афінної групи.

Аліса обчислює стандартну форму H деформації $\tilde{G} = \tau_L G \tau_R$ для G :

$$\begin{aligned} x_{\alpha_1} &\rightarrow h_1(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_N}) = y_{\alpha_1} \\ x_{\alpha_2} &\rightarrow h_2(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_N}) = y_{\alpha_2} \\ &\dots\dots\dots \\ x_{\alpha_N} &\rightarrow h_N(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_N}) = y_{\alpha_N} \end{aligned}$$

Приведене твердження 1.8 гарантує, що це може бути обчислено за поліноміальний час. Аліса оголошує $\tilde{G}$ у наведеному вище вигляді публічним правилом кодування, яке може використатися на просторі відкритих текстів $(Z_t^*)^N$.

Зауважимо, що публічний користувач (Боб) може записати відкритий текст $\bar{p} = (p_{\alpha_1}, p_{\alpha_2}, \dots, p_{\alpha_N})$ з $(Z_t^*)^N$ та обчислити за поліноміальний час $H(\bar{p}) = (c_{\alpha_1}, c_{\alpha_2}, \dots, c_{\alpha_N}) \in (Z_t)^N$.

Декодування. Аліса одержує шифрограму $\bar{c}$. Вона обчислює $\sigma_R^{-1}(\bar{c}) = \bar{u} = (u_{\alpha_1}, u_{\alpha_2}, \dots, u_{\alpha_n}, u_{\alpha_{n+1}}, u_{\alpha_N})$. Після цього Аліса обчислює значення напрямляючих функцій

$$\beta_1 = f_1(u_{\alpha_1}, u_{\alpha_2}, \dots, u_{\alpha_n}), \beta_2 = f_2(u_{\alpha_1}, u_{\alpha_2}, \dots, u_{\alpha_n}), \dots, \beta_m = f_m(u_{\alpha_1}, u_{\alpha_2}, \dots, u_{\alpha_n}).$$

Отже вектор $\bar{u}$ було одержано з невідомого початкового стану $\bar{z} = (z_1, z_2, \dots, z_n, z_{n+1}, z_{n+2}, \dots, z_N)$ регулярним обчисленням автомату Шуберта за послідовністю ваг $(i_1, \beta_1), (i_2, \beta_2), \dots, (i_m, \beta_m)$.

Зазначимо, що

$$\begin{aligned} a_1 z_{\alpha_{i_1}}^{r_1} + b_1 &= u_{\alpha_1} \\ a_2 z_{\alpha_{i_2}}^{r_2} + b_2 &= u_{\alpha_2} \\ &\dots\dots\dots \\ a_n z_{\alpha_{i_n}}^{r_n} + b_n &= u_{\alpha_n} \end{aligned}$$

Крім того $z_{\alpha_{i_1}}, z_{\alpha_{i_2}}, \dots, z_{\alpha_{i_m}}$ належать мультиплікативній групі Z_t^* та множини $\{z_{\alpha_1}, z_{\alpha_2}, \dots, z_{\alpha_n}\}$ та $\{z_{\alpha_{i_1}}, z_{\alpha_{i_2}}, \dots, z_{\alpha_{i_m}}\}$ співпадають. Значення параметрів $z_{\alpha_1}, z_{\alpha_2}, \dots, z_{\alpha_n}$ знаходимо з попередньої системи рівностей.

Аліса розглядає послідовність $(i_1, \beta_1^*), (i_2, \beta_2^*), \dots, (i_m, \beta_m^*)$, де β_s^* є значенням, що відповідає останній появі i_s в послідовності $(i_1, \beta_1), (i_2, \beta_2), \dots, (i_{s-1}, \beta_{s-1})$ якщо $i_s \in \{i_1, i_2, \dots, i_{s-1}\}$, у випадку $i_s \notin \{i_1, i_2, \dots, i_{s-1}\}$ вважаємо, що $\beta_s^* = z_{i_s}$.

Аліса виконує обчислення автомату, що має початковий стан $(u_{\alpha_1}, u_{\alpha_2}, \dots, u_{\alpha_n})$ та визначається послідовністю ваг $(i_m, \beta_m^*), (i_{m-1}, \beta_{m-1}^*), \dots, (i_1, \beta_1^*)$. Результатом цього обчислення буде вектор $\bar{z} = (z_{\alpha_1}, z_{\alpha_2}, \dots, z_{\alpha_n})$. Нарешті Аліса отримує відкритий текст $\bar{p}$ застосовуючи обернене афінне відображення.

Висновки до першого розділу

Запропоновано нові криптосистеми, що будуються за гометріями скінченних простих груп типу Лі та розбиттями многовидів прапорів на клітини Шуберта.

Представлено імплементації кількох алгоритмів шифрування з публічним ключем створених за наступною схемою. Кодуюче відображення F обирається спеціального вигляду $E \cdot G$, де E належить $ES_n(K)$, G є елементом $CG_n(K)$, означає композицію відображень. Ендоморфізм E є відображення степені $\alpha \cdot n$, де $\alpha > 0$. G обирається як елемент малої степені α ($\alpha = 2$ або $\alpha = 3$).

Описано алгоритм генерації елементів $EG_n(K)$ за допомогою спеціальних твірних, так званих генераторів Жордана Гауса. В якості G обирається елемент стабільної підгрупи X степені α у групі $CG_n(K)$, тобто підгрупи, де максимальна степінь автоморфізму дорівнює α .

Визначено основні алгебраїчні об'єкти криптографії від багатьох змінних. Це перш за все афінний простір вимірності n над скінченним комутативним кільцем K (алфавітом для текстів).

Список джерел, використаних у першому розділі

1. Andris Ambainis, Ashwin Nayak, Amnon Ta-Shma, Umesh Vazirani, *Dense quantum coding and quantum finite automata*, Journal of the ACM (JACM), Volume 49, Issue 4 (July 2002), 496 - 511.
2. C. Berrou, A. Glavieux and P. Thitimajshima, *Near Shannon limit error-correcting coding and decoding: turbo-codes*, ICC 1993, Geneva, Switzerland, pp. 1064-1070, May 1993.
3. N.L. Biggs and A.G. Boshier, *Note on the Girth of Ramanujan Graphs*, Journal of Combinatorial Theory, Series B 49, pp. 190–194 (1990).
4. A. Borovik, *Matroids and Coxeter groups*, In: Survey in Combinatorics 2003, London Math Soc. Lect. Notes Ser., vol 307, Cambridge University Press, 2003, 79-114.
5. A. A. Bruen D. L. Wehlau, *Error-Correcting Codes, Finite Geometries and Cryptography*, AMS, 2010.
6. A. Cossidente, M. J. de Ressa, *Remarks on Singer Cycle Groups and Their Normalizers*, Designs, Codes and Cryptography, 32, 97-102, 2004.
7. P. Erdős, M. Simonovits, *Compactness results in extremal graph theory*, Combinatorica 2 (3), 1982, 275-288.
8. V. Futorny, V. Ustimenko, *On Small World Semiplanes with Generalised Schubert Cells*, Acta Applicandae Mathematicae, N4, 2007.
9. W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.
10. Jon-Lark Kim, U. N. Peled, I. Perepelitsa, V. Pless, S. Friedland, *Explicit construction of families of LDPC codes with no 4-cycles*, Information Theory, IEEE Transactions, 2004, v. 50, Issue 10, 2378 - 2388.

11. M. Govorov, Yu Khmelevsky, V. Ustimenko, A. Khorev, *Security Control for Spatial Warehouses*, Proceedings of the 21th International Cartographic Conference (ICC), Durban, South Africa, 2003, 1784-1794.
12. S. Hoory, N. Linial, and A. Wigderson, *Expander graphs and their applications*, Bulletin (New Series) of AMS, volume 43, N4, 439-461.
13. J. Kotorowicz, V. A. Ustimenko, *On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings*, Condensed Matters Physics, Special Issue: Proceedings of the international conferences "Infinite particle systems, Complex systems theory and its application", Kazimierz Dolny, Poland, 2006, 11 (no. 2(54)) (2008) 347–360.
14. F. Lazebnik and V. Ustimenko, *Some Algebraic Constructions of Dense Graphs of Large Girth and of Large Size*, DIMACS series in Discrete Mathematics and Theoretical Computer Science, V. 10 (1993), 75-93.
15. F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *A New Series of Dense Graphs of High Girth*, Bull (New Series) of AMS, v.32, N1, (1995), 73-79.
16. F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *Polarities and $2k$ -cyclefree graphs*, Discrete Mathematics, 197/198, (1999), 503–513.
17. G. A. Margulis, *Explicit construction of graphs without short cycles and low density codes*, Combinatorica, 2, (1982), 71-78.
18. Jose M. F. Moura, Jin Lu, and Haotian Zhang, *Structured LDPC Codes with Large Girth*, IEEE Signal Processing Magazine, vol. 21:1, pp.42-55, January 2004. Included in Special Issue on Iterative Signal Processing for Communications.
19. T. Richardson, R. Urbanke, *Modern Coding Theory*, Cambridge University Press, 2008.
20. J. Seberry, J. Pieprzyk, *Cryptography: An Introduction to Computer Security*, Prentice Hall 1989, 379 p.
21. T. Shaska and V. Ustimenko, *On some applications of graph theory to cryptography and turbocoding*, Special issue of Albanian Journal of Mathematics: Proceedings of the NATO Advanced Studies Institute "New challenges in digital communications", May 2008, University of Vlora, 2008, v.2, issue 3, 249-255.

22. J. A. Thas, *Generalised polygons*, in F. Buekenhout (ed), Handbook in Incidence Geometry, Ch. 9, North Holland, Amsterdam, 1995.
23. A. Touzene, V. Ustimenko, *Graph Based Private Key Crypto System*, International Journal on Computer Research, Nova Science Publisher, volume 13 (2006), issue 4, 12p.
24. V. A. Ustimenko, *On some properties of Chevalley groups and their generalisations*, In: Investigations in Algebraic Theory of Combinatorial objects, Moskow, Institute of System Studies, 1985, 134 - 138 (in Russian), Engl.trans.: Kluwer, Dordrecht, 1992, pp. 112-119
25. V. Ustimenko, *Small Schubert cells as subsets in Lie algebras*, Functional Analysis and Applications, v. 25, no. 4, 1991, pp. 81–83.
26. V. Ustimenko, *CRYPTIM: Graphs as Tools for Symmetric Encryption*, in Lecture Notes in Computer Science, Springer, 2001, v. 2227, 278-287.
27. V. Ustimenko, *Maximality of affine group and hidden graph cryptosystems*, Journal of Algebra and Discrete Mathematics, October, 2004, v.10, pp. 51-65.
28. V. Ustimenko, *On the extremal graph theory for directed graphs and its cryptographical applications* In: T. Shaska, W.C. Huffman, D. Joener and V. Ustimenko, Advances in Coding Theory and Cryptography, Series on Coding and Cryptology, vol. 3, 181-200 (2007).
29. V. A. Ustimenko, *Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, Journal of Mathematical Sciences, Springer, vol.140, N3 (2007) pp. 412-434.
30. V. A. Ustimenko, J. Kotorowicz, *On the properties of Stream Ciphers Based on Extremal Directed graphs*, In "Cryptography Research Perspectives", Nova Publishers, Ronald E. Chen (the editor), 2008.
31. Gilles Van Assche, *Quantum Cryptography and Secret-Key Distillation*, Cambridge University Press, 2006.
32. A. Wroblewska *On some properties of graph based public keys* , Albanian Journal of Mathematics, Volume 2, Number 3, 2008, 229-234.

33. В. А. Устименко, Об экстремальной теории графов и символьных вычислениях // Доповіді НАН України, 2013, N2, с.42-49.

34. V. Ustymenko, A. Wroblewska, On some algebraic aspects of data security in cloud computing // Proceedings of International conference Applications of Computer Algebra, Malaga, 2013, p. 155-160.

35. V. Ustimenko, U. Romanczuk, On regular forests given in terms of algebraic geometry, new families of expanding graphs with large girth and Multivariate cryptographical algorithms // Proceedings of International conference Applications of Computer Algebra, Malaga, 2013, p. 144-147.

36. A. Wróblewska, V. Ustimenko, On new examples of families of multivariate stable maps and their cryptographical applications, Annales of UMCS, Informatica, volume 14 (2014), Special issue "Proceedings of International Conference Cryptography and Security Systems", pp. 19-36.

37. U. Romańczuk-Polubiec, Vasyl Ustimenko, On two windows multivariate cryptosystem depending on random parameters IACR, Cryptology ePrint Archive. 11/2014; Report 2014/964.

38. D. Dudkowski, Yu. Maistrenko, and T. Kapitaniak. "Different types of chimera states: An interplay between spatial and dynamical chaos". Physical Review E 90, 032920 (2014).

39. U. Romanczuk- Polubiec, V. Ustimenko, On two windows multivariate cryptosystem depending on random parameters, Algebra and Discrete Mathematics, Volume 19 (2015). Number 1, pp. 101–129

РОЗДІЛ 2

ПРО ЗАСТОСУВАННЯ АЛГЕБРАЇЧНОЇ КОМБІНАТОРИКИ ДО ПРОБЛЕМ КОДУВАННЯ ТА КРИПТОГРАФІЇ

2.1. Про застосування алгебраїчної комбінаторики до проблем постквантової криптографії

Перші спроби створити безпечну криптосистему від багатьох змінних були пов'язані з різними модифікаціями методу японських дослідників Імаї і Мацумото. Цей напрямок поки не приніс очікуваних результатів - криптоаналітики знайшли методи ефективної протидії. Зараз перспективними вважають спроби використання складних об'єктів, визначених через неалгебраїчні структури (динамічні системи і відповідний хаос, псевдовипадкові графи, інші складні об'єкти).

В суспільстві виникають потреби захисту інформації, її обробки та зберігання в суспільстві, що потребують керованості балансу між рівнем безпеки інформації та швидкодією. Потрібні нові програмні продукти, де необхідний баланс може встановлювати користувач. Такі методи безперечно потребує, зокрема, новий напрямок "Обчислення в хмарах" (Cloud Computing). При використанні техніки обчислень в хмарах користувач отримує віртуальну обчислювальну інфраструктуру для зберігання даних та їх перетворення. Переваги такої ідеології зрозумілі, але виникають нові проблеми теорії безпеки пов'язані з тим, що оператори та користувачі діють в умовах відсутності повної довіри. Це потребує розвитку нових криптографічних алгоритмів з керованою безпекою та методами знаходження відповідного балансу між безпекою та ефективністю обчислень. З іншого боку потрібно знайти безпечні методи віртуального зберігання вразливої приватної інформації (медичні дані, фінансові документи, важлива бізнес інформація).

Одним з важливих напрямків є дослідження з гомоморфного (або ж голоморфного) кодування. Його методи дозволяють оперування з вже

закодованою інформацією. Це може бути достатньо повне оперування (fully-homomorphic encryption) або ж тільки можливість виконання спеціальних операцій, таких як пошук та статистичний (структурний) аналіз.

Ще більш важливим напрямком є розробка залежних від розміру ключа алгоритмів криптографії від багатьох змінних, які дозволяють гнучко керувати рівнем безпеки та швидкодії. Це стосується не тільки обчислень в хмарах, але й вирішення різних задач електронного управління (роботи електронних віртуальних організацій, е-бізнесу, інше).

Для створення ефективних методів захисту системи електронного управління треба зважати на те, що сучасним засобом захисту від загроз для систем управління та корпоративних мереж є створення Інфраструктури публічних ключів (PKI)

Така інфраструктура дозволяє захищати систему електронного парламенту через розв'язання таких задач як:

- аутентифікація (визначення відправника електронного документу)
- цілісність (підтвердження того, що документ не був підроблений)
- незаперечувальність (неможливість відправника заперечувати факт відправки документа.
- безпечне оновлення ключів для алгоритмів захисту.
- конфіденційність (підтвердження того що документ не було прочитано особою не маючої права на доступ до тексту)

Для працюючих систем електронного управління та корпоративних мереж треба визначити декілька рівнів доступу до документів (щонайменше три).

Інфраструктура публічних ключів повинна об'єднати електронні підписи, публічні та приватні ключи і агенцію, що виконує сертифікацію (законодавче визнання електронних підписів, публічних ключів, рівнів доступу).

Для вибору ефективних методів захисту системи електронної віртуальної організації треба зважати на те що сучасним засобом захисту від загроз для систем управління та корпоративних мереж є створення доступ до тексту)

Слід розвивати і новітні методи захисту віртуальних організацій та систем космічного зв'язку від шумів. Новим напрямком має стати створення вітчизняних LDPC кодів та турбокодів (подібних до кодів, що використовує NASA). Зазначимо, що деструктурну атаку на систему електронного уряду можна здійснити не тільки хакерськими методами, але й за допомогою генератора шумів, що може повністю унеможливити урядування та деформувати важливі дані.

Таким чином поряд з традиційними методами захисту (для військової безпеки, боротьби з протиправними діями, державного зв'язку) слід створювати нові інфраструктури захисту інформаційних систем та мереж. При цьому важливо розвивати такі новітні напрямки як постквантова криптографія та теорія кодування, інфраструктури публічних ключів з керованою безпекою, поліноміальні криптографічні систем від багатьох змінних, теорія LDPC кодів та турбокодів. Потрібно створювати власні інженерні та технологічні розробки, що використовують ідеї згаданих вище сучасних напрямків розвитку теорії.

Слід підкреслити, що диверсифікація електронних засобів дуже корисна для електронного управління та експлуатації сучасних інформаційних систем, наприклад, бездротовий зв'язок, онлайн-наради, відеоконференції, та відео телефони. З точки зору процесів, високий рівень безпеки, стандартизація та управління знаннями є обов'язковими для електронного управління та бізнесу, а лише потім іде надання конкретних послуг з акцентом на їх якості. Крім того, створення мережі аутентифікаційних центрів є найважливішою вимогою, тому що користувачі можуть використовувати послуги з їх особистою ідентичністю, і всі операції відображаються в національному центрі управління файлами для захисту електронних документів від будь-яких ушкоджень. З юридичної точки зору, необхідно в законодавчому порядку гарантувати легітимність електронного підпису та електронного документообігу. Нарешті, з точки зору апаратно /

програмного забезпечення популяризація IT-інфраструктурного будівництва має важливе значення для електронного управління, бізнесу і експлуатації електронних мереж.

Все викладене логічно підводить до деталізації питання щодо застосування алгебраїчної комбінаторики до проблем постквантової криптографії. Зокрема, постквантова криптографія призначена для відшукування криптографічних алгоритмів (частіше за все з публічним ключем або алгоритми протоколів обміну ключами), що можуть потенційно бути безпечними для атак, що використовують квантовий комп'ютер.

Популярні в наш час алгоритми ґрунтуються на трьох відомих проблемах:

- проблема факторизації цілих чисел
- проблема логарифму дискретного
- дискретний логарифм для еліптичних кривих

Всі ці проблеми легко розв'язуються на достатньо великому квантовому комп'ютері за допомогою алгоритму Шора.

Сучасна постквантова криптографія підрозділюється на 5 напрямків

- криптографія від багатьох змінних, яка базується на складності розв'язків систем нелінійних рівнянь від багатьох змінних (Multivariate Cryptography)
- решіток (Lattice base Cryptography)
- хаш функцій (Hash based Cryptography)
- корекційних кодів (Code based Cryptography)
- ізогеній супереліптичних кривих (Superelliptic cryptography)

Найстаршим напрямком є Поліноміальна Криптографія від багатьох змінних (Multivariate Cryptography [1], що використовує поліноміальні відображення вільного модуля K^n визначеного над скінченим комутативним кільцем у себе як засіб кодування. Цей напрямок базується на використанні складності знаходження

розв'язку нелінійної системи поліноміальних рівнянь від багатьох змінних. Він використовує нелінійні поліноміальні перетворення вигляду:

$$\begin{aligned}x_1 &\rightarrow f_1(x_1, x_2, \dots, x_n) \\x_2 &\rightarrow f_2(x_1, x_2, \dots, x_n) \\&\dots\dots\dots \\x_n &\rightarrow f_n(x_1, x_2, \dots, x_n)\end{aligned}$$

що діють на вільному K^n , де $f_i \in K[x_1, x_2, \dots, x_n]$, $i=1, 2, \dots, n$ є многочленами записаними у стандартній формі, тобто через список одночленів у заданому порядку. Важливі ідеї і методи в цьому напрямку оглянуті в [2]. Густина відображення F є найбільшим числом $\text{den}(F)$ одночленів для многочленів f_i , $i=1, 2, \dots, n$.

Будемо говорити що вираз $\text{den}(F)$ є поліноміальним якщо цей параметр має розмір $O(n^d)$ для деякої додатньої сталої d .

Степінь $\text{den}(F)$ відображення F є максимальним значенням степенів f_i , $i=1, 2, \dots, n$.

Нехай F буде відображенням K^n у себе яке має поліноміальну густину розміру $C_1 n^{d_1}$ та поліноміальну степінь $C_2 n^{d_2}$.

Тоді значення F на наборі $(b_1, b_2, \dots, b_n)$ може бути обчислене за $O(n^{d_1+d_2+1})$ елементарних операцій кільця.

Актуальною задачею є пошук алгоритмів які є стійкими до криптоаналітичних атак за допомогою звичайної машини Тюрінга. Поліноміальна криптографія від багатьох змінних повинна довести існування практичних криптоалгоритмів які спроможні створити конкуренцію RSA, протоколам Діффі Хелмана та популярним засобам криптографії еліптичних кривих. [1, 2]. Це досить молода дослідницька галузь якій ще не вистачає прикладів криптосистем з теоретично оціненою відпорністю до атак реалізованих на звичайній машині Тюрінга.

Дослідження атак за допомогою машини Тюрінга та квантового комп'ютера повинні робитися різними методами зважаючи на різну природу цих двох машин, детерміністичну та випадкову, відповідно.

Нехай K є коммутативним кільцем, $S(K^n)$ означає афінну напівгрупу Кремони всіх поліноміальних перетворень вільного модуля K^n . Криптографія від багатьох змінних розпочиналася від вивчення можливостей спеціальних квадратичних бієктивних перетворень K^n , де K є розширенням скінченного поля F_q характеристики 2. Одна з перших таких криптосистем була запропонована Імаї та Мацумото, криптоаналітичної такої системи був знайдений Я. Патаріним. Огляд різних модифікацій цих алгоритмів та відповідний криптоаналіз можна знайти в монографії [1]. Багато спроб побудувати працюючий публічний ключ криптографії від багатьох змінних не привели до мети, але дослідження та побудова нових алгоритмів - кандидатів продовжується [3].

Деякі застосування Алгебраїчної Теорії Графів до Поліноміальної Криптографії від багатьох змінних було розглянуто в [4]. Цей огляд присвячено алгоритмам, що базуються на взаємно-однозначних відображеннях вільних модулів у себе. Застосування алгебраїчних графів у криптографії почалися з симетричних алгоритмів що базуються на конструктивних побудовах екстремальної теорії графів та подібної теорії для орієнтованих графів [4, 5].

Головна ідея – конвертувати алгебраїчний граф у скінчений автомат та використовувати псевдовипадкові прогулянки по графу як знаряддя для кодування. Такий підхід може також використатися для створення протоколів обміну ключів. Недавно запропонована ідея "символічних блукань" на алгебраїчних графах коли блукання на графі залежить від параметрів, що є спеціальними многочленами залежними від невідомих координат вектора відкритого тексту дозволила створити кілька нових криптосистем з публічним ключем.

Поряд з екстремальними графами для створення криптографічних алгоритмів можна використати графи інциденції скінчених геометрій та їх систем прапорів. Бієктивні розріджені поліноміальні відображення достатньо великої степені було запропоновано в [5].

Одним з перших застосувань небієктивних відображень у криптографії від багатьох змінних була криптосистема “олії та оцету” запропонована в [6] та піддана аналізу в [7]. В сучасних дослідженнях ця загальна ідея в значній степені підтримана в публікації [8], яка присвячена аналізу прямих атак на модифіковану незбалансовану систему олії та оцету. Цей алгоритм було запатентовано. Виглядає так що ці системи разом із системами веселковоподібних (rainbow like) схем електронного підпису можуть привести до багатообіцяючих систем публічного ключа Криптографії від багатьох змінних для випадку скінчених полів.

Не бієктивні розріджені кодуючі відображення від багатьох змінних степені 3 та ≥ 3 побудовані через блукання на алгебраїчних графах $D(n, K)$ що визначалися над загальним комутативним кільцем [16] та їх гомоморфні образи було запропоновано в [9].

Нові криптосистеми визначені за не бієктивними поліноміальними кодуючими відображеннями вільного модуля Z_m^n у себе було презентовано на міжнародній конференції з алгебри, дискретної математики та їх застосувань DIMA 2015 [10]. Система використовує відкритий текст $(Z_m^*)^n$, де $n=k(k-1)/2$, $k \geq 2$ може бути довільним натуральним числом.

Відкритий ключ сформовано як послідовність загальних многочленів з $Z_m[x_1, x_2, \dots, x_{k-1}]$ та послідовність параметрів l_i , $i=1, 2, \dots, k-1$ які є взаємно простими з $\varphi(m)$. Властивості кодуючого відображення в значній мірі залежать від розкладу числа m на прості множники.

Це небієктивне кодуєче відображення є деформацією спеціального обчислення продукованого автоматом Шуберта для $k-1$ вимірної проективної

геометрії " над Z_m . Цей метод не використовує розбиття змінних на групи, небієктивна природа відображення побудована існуванням дільників нуля для складеного цілого числа m . В дійсності ідея «схованого RSA» знайшла реалізацію [10]. Інший алгоритм що використовує цю ідею описано в [11].

В останні роки алгебраїчна комбінаторика також з успіхом застосовується в криптографії та теорії безпеки мереж - новій галузі теоретичної інформатики, що досліджує рівень комунікаційної безпеки колективу користувачів в розгалужених комунікаційних мережах. Цей міждисциплінарний напрямок розглядає разом з криптографічними проблемами і задачі знаходження та виправлення помилок, захист від шумів та інші аспекти класичної теорії кодування.

Окреслимо теоретичне підґрунття класу алгоритмів. Проблема дискретного логарифма (ДЛ) є відомою NP складною задачею теорії чисел та теорії груп. Ситуація багато в чому подібна до проблеми розкладу цілих чисел на множники. Безпека кількох відомих криптографічних алгоритмів з відкритим ключем ґрунтується на складності цих двох проблем. Наприклад система ElGamal та DSS базуються на ДЛ. Хоча проблема дискретного логарифма формулюється для будь якої скінченої групи, але в застосуваннях до криптографії група, як правило, є мультиплікативною групою Z_n^* кільця лишків.

Нагадаємо, що теоретико-группова проблема дискретного логарифмування є наступною: знайти натуральне число x , таке що $g^x = h$, де h і g є обрані елементи скінченої групи G . У випадках груп $C = Z_p^*$ та $C = Z_{pq}^*$, де p та q - достатньо великі прості числа складність проблеми дискретного алгоритму є обґрунтуванням безпеки класичного алгоритму обміну ключів запропонованого Діффі та Хелманом та криптосистеми RSA. В більшості випадків інших груп складність проблеми дискретного алгоритму є недостатньо дослідженою. Досить часто проблема залежить від вибору бази g та способу представлення інформації про групу. Група може бути визначена за допомогою генераторів і відношень, як група автоморфізмів алгебраїчного різномаїття, як група матриць над скінченим кільцем, група перестановок. вона може визначатися багатьма іншими способами.

Наступний приклад демонструє, важливість способу представлення абстрактної групи.

Мультиплікативна група Z_p^* , де p - просте, є ізоморфною адитивній групі кільця Z_{p-1} . якщо p - "досить велике", то проблема ДЛ є NP-важкою, але ж для адитивної групи кільця лишків Z_{p-1} проблема ДЛ еквівалентна задачі розв'язання лінійного рівняння.

Давайте розглянемо випадок симетричної групи S_{p^n} порядку $p^n!$ представленої як група Кремони всіх бієктивних поліноміальних автоморфізмів векторного простору $V = (F_p)^n$ над простим скінченним полем F_p . Оберемо стандартну базу простору V . Добре відомо, що кожну перестановку π з симетричної групи S_{p^n} можна записати у вигляді "публічного правила" g : x_1 переходить до $g_1(x_1, x_2, \dots, x_n)$, x_2 відповідно до $g_2(x_1, x_2, \dots, x_n)$, нарешті x_n змінюється на $g_n(x_1, x_2, \dots, x_n)$, де g_i - многочлени від багатьох змінних з $F_p[x_1, x_2, \dots, x_n]$.

Зазначимо, що доброї оцінки порядку відображення g не існує. В загальному випадку ступінь нелінійного поліноміального відображення g^k , що відповідає підстановці π^k , росте зі збільшенням k . [17-21]

Обґрунтуємо складність проблеми обчислення порядку "псевдовипадкового" нелінійного відображення g . Почнемо з дуже відомої проблеми знаходження розв'язку нелінійної системи рівнянь $g(x)=b$, з максимальним ступенем d многочленів $g_i(x_1, x_2, \dots, x_n)$. Сучасна математика не знайшла принципово швидших за метод Гаусса способів розв'язання системи. В загальному випадку складність найшвидшого алгоритму становить d^s , $s=O(n^2)$. При умові існування та єдиності розв'язку та деяких додаткових умовах задача розв'язується за d^s , $s=O(n)$ кроків. Тепер перейдемо до більш складної задачі знаходження оберненого перетворення h до відображення g . Зрозуміло, що обчисливши ми знайдемо розв'язок нелінійної системи як $h(b)$. Тому вираз d^s , $s=O(n)$ можна використати як нижню оцінку складності задачі.

Перейдемо до проблеми знаходження порядку t для відображення g . Очевидно, що знаючи t обернене перетворення g обчислимо як g^k , $k=t-1$, тому за нижню оцінку і цієї задачі можна прийняти $d^{O(n)}$, де число d є ступенем для відображення g . Ефективний алгоритм для знаходження g^k , $k=-1$ відомо тільки у випадку, коли ступінь g — одиниця, тобто g є афінним відображенням перетворюючим x у вектор $Ax + b$, де x та b - вектори стовбчики з простору V , A - невироджена квадратна матриця. Таким чином існує справжня прірва по складності між лінійністю та нелінійністю.

Проблема дискретного логарифму для циклічної групи породженою "псевдовипадковим" нелінійним поліноміальним відображенням g з симетричної групи S_p^n , тобто задача знаходження розв'язку рівняння $g^x=b$ виглядає складною. Коли x відомо разом з порядком відображення g , то рівняння можна переписати у вигляді $g^{t-x}=b^{-1}$, але як ми вже бачили обчислення b^k , $k=-1$ потребує щонайменше d^s , $s=O(n^2)$ операцій. Це означає, що у випадку "псевдовипадкової" нелінійної бази g , ми можемо уживати термін схованої символічної проблеми дискретного логарифму, слово "схована" вжите тому, що порядок t циклічної групи невідомий при достатньо великій кількості змінних, термін "символічна" використаний тому, що відображення g та b можна генерувати з використанням методів символьних перетворень таких як популярні "Maple" чи "Matematika", що працюють з символьними перетвореннями або спеціалізованими гнучкими програмами Комп'ютерної Алгебри.

Наведені вище аргументи про складність проблеми ДЛ в симетричній групі S_p^n , справедливі і для більш загального випадку групи Кремони $C(K^n)$ поліноміальних автоморфізмів вільного модуля K^n над загальним комутативним кільцем K . Група $C(K^n)$ є одним з найскладніших об'єктів Алгебраїчної Геометрії. [22-26]

2.2. Про вибір бази і стабільні підгрупи

Зрозуміло, що для вибору нелінійної “псевдовипадкової” бази g у відповідній проблемі ДЛ потрібно використовувати ефективні евристичні алгоритми. Вони повинні генерувати g дуже великого порядку. Якщо поліноміальний ступінь степені g^x в групі Кремони зростає лінійно зі зростанням x , тобто $\deg(g(x))=ax+b$, то x можна обчислити з лінійної рівності $ax+d = \deg b(x)$. Це мотивує наступну концепцію.

Послідовність підгруп G_i у групі $C(K^i)$, де i прямує до нескінченості є родиною стабільних підгруп, якщо поліноміальний ступінь кожного g з G_i обмежений незалежною сталою c . Побудова родин великих стабільних груп G_i є цікавою математичною проблемою, що має важливі застосування в криптографії.

Очевидно що підгрупи $AGL_n(F_p)$ всіх афінних бієктивних відображень з x до $Ax+b$, де x та b – вектори стовбчики з V , A – невідроджена квадратна матриця утворюють родину підгруп стабільного ступеня з $c=1$. Існує легкий спосіб побудови стабільних підгруп через спряження $AGL_l(K)$ (підгрупи всіх автоморфізмів модуля $C(K^l)$ поліноміального ступеня 1) з нелінійним відображенням f з $C(K^l)$. Такі родини природно називати псевдолінійними. Очевидно що ступені многочлена f_i оберненого до нього перевищують 2. Тому при використанні “псевдовипадкових” многочленів f сталого ступеня буде отримано родину стабільного ступеня з $c > 4$.

Саме тому дослідження родин сталого ступеня з $c=2$ або $c=3$ є найцікавішим випадком. Вдалося конструктивно довести наступне твердження:

Для кожного скінченного комутативного кільця, що містить більше двох регулярних елементів (не дільників нуля), існує родини підгруп стабільного ступеня з $c=2$ та $c=3$ такі, що порядок їх представників не обмежений.

На основі цього твердження побудована бібліотека криптографічних алгоритмів і програм, безпека яких ґрунтується на складності проблеми дискретного логарифму у відповідній групі Кремони. Для практичного використання уживано скінчені поля та кільця лишків за модулем n . Розроблено

алгоритми обміну ключів, алгоритми кодування з відкритим ключем (public key), методи цифрового підпису та швидкі симетричні потокові алгоритми кодування (stream ciphers) .

2.3. Про властивості одного з поточкових симетричних алгоритмів кодування

Дані можуть мати будь-який формат, такий як: текст, зображення або звуковий файл. Побудовані симетричні алгоритми не є блочними шифрами. На відміну від блочних шифрів, нові інструменти змінюють всі дані: зміна навіть одного байту інформації, або одного символу ключа призводить до корінної зміни даних всього шифру(змінюється 99 відсотків символів, а не конкретний блок), алгоритми швидкі та їх швидкість лінійно залежить від розміру даних. Якщо супротивник має доступ тільки до зашифрованих даних, то для розшифрування даних йому треба буде використати метод «грубої сили», тобто здійснити перебір всіх можливих варіантів ключа. Математично доведено, що різні ключі виробляють різні шифри, які завжди відрізняються від початкових текстів. Клієнт може вільно обирати довжину ключа, тому опір до атак регулюється розміром простору ключів. Функція шифрування є нелінійною, тому алгоритм стійкий до активної атаки на ключ, у випадку коли супротивник має багато пар оригінальних і зашифрованих даних. Алгоритми можуть бути використані для потокового шифрування, але вони можуть бути перетворені в систему поліноміальних відкритих ключів через алгебраїчний характер базових графів.

Для оцінки якості "удаваного хаосу" теоретично, можна використовувати певні динамічні та стохастичні моделі з теорії складних систем на графах які було зазначено вище. Пропоновані методи засновані безпосередньо на теорії скінченних автоматів (грубо кажучи, графів), використовуваної для шифрування. Виявляється, що алгебраїчні графи великого обхвату є гарним прикладом шифрувальних автоматів.

Проблема захисту інформації з'явилася ще задовго до появи комп'ютерів. З самого початку свого розвитку системи інформаційної безпеки розроблялися для військових відомств. Розголошення такої інформації могло привести до величезних людських жертв, тому конфіденційності в системах безпеки приділялася особлива увага. Очевидно, що надійно захистити повідомлення й дані від розголошення і перехоплення може тільки повне їхнє шифрування.

Стрімке вдосконалювання комп'ютерних технологій позначилося й на принципах побудови захисту інформації. Обчислювальна потужність сучасного домашнього комп'ютера суттєво перевищує потужність деяких суперкомп'ютерів минулого. Тому й деякі інструменти захисту даних зараз можна вважати застарілими адже задачі, що полягають в їх основі більше не є складними обчислювальними задачами.

Принцип побудови сучасного інструменту захисту інформації це пошук оптимального співвідношення між швидкістю шифрування, його стійкістю до активних атак, та можливістю збільшувати довжину ключа. Сучасний інструмент захисту даних повинен мати певний запас міцності, який він може протиставити стрімкому зростанню обчислювальної потужності комп'ютерних систем.

Розроблено теоретичні основи захисту інформації за допомогою алгоритмів на базі алгебраїчних графів, які створили базу для побудови симетричного алгоритму на алгебраїчному графі.

Нехай F_q – скінченне поле порядку q , яке є степінню простого числа. Розглянемо дводольний граф $A(n, F_q) = A(n, q)$, визначений на множині точок $P = F_q^n$ і прямих $L = F_q^n$ через відношення інцидентності I : $x I y$ для $x = (x_1, x_2, \dots, x_n)$ із P та $y = [y_1, y_2, \dots, y_n]$ із L тоді і тільки тоді, коли виконуються співвідношення $y_2 - x_2 = y_1 x_1, y_3 - x_3 = x_1 y_2, y_4 - x_4 = y_1 x_3, y_5 - x_5 = x_1 y_4, \dots, y_n - x_n = x_1 y_{n-1}$ при непарному n і $y_n - x_n = y_1 x_{n-1}$ при парному значенні $n, n > 1$. Круглі та квадратні дужки дозволяють розрізняти точки та прямі.

Граф $A(n, q)$ є дводольним, тому що він не має непарних циклів.

Проективним приділом послідовності графів $A(n, q) \in q$ -регулярне дерево T_q .

2.4. Автомати, визначені графами сімейства $A(n, q)$

Графи $A(n, q)$ були визначені в [14] як гомоморфні відображення графів $D(n, q)$. В цій же публікації вводиться колір вершини (точки або прямої) як значення першої координати вектора вершини. Таким чином, колір являється елементами скінченного поля F_q . У графі $A(n, q)$ кожна вершина v має єдиного сусіда заданого кольору. Розглянемо бієктивне відображення Dt із множини вершин графа $A(n, q)$, яке переводить точку $x=(x_1, x_2, \dots, x_n)$ в її сусіда кольору x_1+t , де t належить полю F_q і переводить пряму $y=[y_1, y_2, \dots, y_n]$ в сусідню з нею точку кольору y_1+t . Простий шлях довжини s в графі з початком у вершині v може бути представлений як послідовність вершин $x_0=v, x_1=Dt_1(x_0), x_2=Dt_2(x_1), \dots, x_s=Dt_s(x_{s-1})$, де послідовність $t=t_1, t_2, \dots, t_s$ задовольняє умову t_i та $-t_{i-1}$ різні при $i=1, 2, \dots, s$. Нехай Dt - відображення, яке переводить v в x_s . Помітимо, що зворотнім до нього буде бієкція Dt' , де t - послідовність $-t_s, -t_{s-1}, \dots, -t_1$. Виявляється, що незалежно від вибору послідовності перетворення Dt є поліноміальним перетворенням вигляду $(x_1, x_2, \dots, x_n) \rightarrow (f_1(x_1, x_2, \dots, x_n), f_2(x_1, x_2, \dots, x_n), \dots, f_n(x_1, x_2, \dots, x_n))$, де всі многочлени $f_i(x_1, x_2, \dots, x_n)$, $i=1, 2, \dots, n$, є кубічними.

Помітивши ребро між сусідніми вершинами v_1 та v_2 різницею їх кольорів, отримаємо скінченний автомат з алфавітом F_q . Сім'ю автоматів $A(n, q)$ можна використати для кодування “потенційно нескінченного тексту” над F_q . Будемо вважати, що відкритий текст x є елементом вибраної долі, наприклад, P . Послідовність $t=t_1, t_2, \dots, t_s$ кольорів ребер простого шляху в автоматі, відповідного обчислення функції $Dt(x)$, назовемо нескоротним паролем. На векторному просторі F_q^n розглянемо два оборотних афінних перетворення L_i , $i=1, 2$, вигляду $x \rightarrow xA_i + b_i$, де A_i є розрідженою матрицею, а b_i - векторами вигляду $(b_1, b_2, \dots, b_n)$. Нагадаємо, що розрідженість матриці означає її

обчисленість за $O(n)$ кроків. Будемо вважати, що персональний ключ складається із пар $A_i, b_i, i=1,2$ і нескоротного пасворда $t=t_1, t_2, \dots, t_s$. Кодуюче відображення E – композиція L_1, Dt та L_2 , оберненим до нього буде відображення $L_2' Dt' L_1'$, де L_i' – обернені до L_i афінні відображення, а t' – послідовність $-t_s, -t_{s-1}, \dots, -t_1$. Кубічне перетворення E обчислюємо за допомогою одного із пакетів, реалізуючих символічних перетворень комп'ютерної алгебри. Результатом обчислення буде поліноміальне перетворення $G: (x_1, x_2, \dots, x_n) \rightarrow (g_1(x_1, x_2, \dots, x_n), g_2(x_1, x_2, \dots, x_n), \dots, g_n(x_1, x_2, \dots, x_n))$, де всі многочлени $g_i(x_1, x_2, \dots, x_n), i=1,2, \dots, n$, є кубічними виразами, записаними у вигляді списку впорядкованих мономів.

Список G буде служити публічним правилом (ключем), так що публічний користувач може з його допомогою кодувати інформацію за не більше ніж $O(n^4)$ кроків. Власник ключа, який має інформацію про сім'ю графів, та персональний ключ може виконувати як кодування так і декодування за час $O(n)$. Помітимо, що він може фактично використовувати генератор публічних ключів, замінюючи параметри n (довжина потенційно нескінченного тексту), s (довжина нескоротного пасворду), q (вибор алфавіту). Помітимо, що найкращий загальний алгоритм знаходження зворотнього до G перетворення потребує $3^{O(n)}$ кроків, незалежно від того, використовує він ідеологію базиса Грьобнера або альтернативні методи. Із визначення сімейства графів з великим цикловим показником випливає, що при умові $s < n$ та фіксованих афінних перетвореннях $L_i, i=1,2$, різним нескоротним пасвордам відповідають різні відображення G .

Описаний вище симетричний алгоритм має самостійну цінність як потоковий алгоритм швидкого шифрування. Якщо q – нерарне то із - за звязності графа при фіксованих афінних перетвореннях $L_i, i=1,2$, та змінних нескоротних пасвордах довільної довжини кодування володіє властивістю транзитивності, тобто для довільно вибраних відкритих текстів (файлів однакового розміру) існує пасворд, такий, що відповідне кодуєчне відображення переводить перший текст в другий.

Помітимо, що для блокових алгоритмів властивість транзитивності не можлива, так як відкритий текст з періодичністю на блоках при будь-якому

кодуванні переходить в новий періодичний текст. Властивість графів малого світу гарантує транзитивність навіть при обмеженні простору паролів на множині слів довжини $O(n)$. Кодування при використанні таких обмежень паролів виконується за $O(n^2)$ кроків.

Важливий частковий випадок відповідає вибору зворотного до L_1 афінного перетворення в якості L_2 . Для простоти припустимо, що s парне. У такому випадку порядок відображення G співпадає з порядком Dt . Як впливає із приведених вище результатів, в такому випадку:

- 1) будь-яка степінь відображення G в симетричній групі $S(F_q^n)$ є або кубічним відображенням векторного простору в себе, чи одиницею;
- 2) якщо $t_1 + t_s$ відмінна від нуля то порядок перетворення G прямує до нескінченності при зростанню параметра n .

Ми продемонструємо вам дослідження цього алгоритму шифрування даних, та його гнучкість і здібність адаптуватись до стрімкого зростання обчислювальної потужності комп'ютерних систем.

Для виміру продуктивності алгоритму, проведено шифрування 10 файлів різного розміру за допомогою 8 ключів різної довжини. Нехай k – розмір даних в кілобайтах, L – довжина ключа в бітах. Позначимо через $t(k, L)$ час в мілісекундах який потрібен для шифрування або розшифрування даних розміру k за допомогою ключа довжини L (алгоритм симетричний). Тоді результати вимірів $t(k, L)$ можна представити як таблиці по одній табличці для кожної тестової конфігурації. Тобто зроблено 160 вимірів та представлено їх двома таблицями табл.2.1 та 2.2, та візуалізовано на рис. 2.1 і 2.2.

Довжина ключа, біт	Розмір даних, Мегабайт									
	1	2	3	4	5	6	7	8	9	10
32	140,63	296,88	437,50	578,13	734,38	875,00	1015,63	1156,25	1296,88	1468,75
64	296,88	593,75	875,00	1171,88	1468,75	1750,00	2046,88	2343,75	2625,00	2906,25
96	437,50	875,00	1312,50	1765,63	2187,50	2625,00	3093,75	3515,63	3937,50	4375,00
128	593,75	1171,88	1765,63	2343,75	2921,88	3515,63	4078,13	4671,88	5250,00	5875,00
160	734,38	1468,75	2203,13	2921,88	3656,25	4406,25	5125,00	5859,38	6609,38	7375,00
192	890,63	1765,63	2640,63	3515,63	4375,00	5265,63	6171,88	7000,00	7875,00	8781,25
224	1031,25	2046,88	3078,13	4109,38	5078,13	6140,63	7156,25	8187,50	9203,13	10265,63
256	1171,88	2343,75	3531,25	4687,50	5859,38	7015,63	8203,13	9390,63	10593,75	11718,75

Таблиця 2.1 – Вимір 1: «Quad core Intel Core 2 Quad E6600 2,40GHz 4Gb RAM»

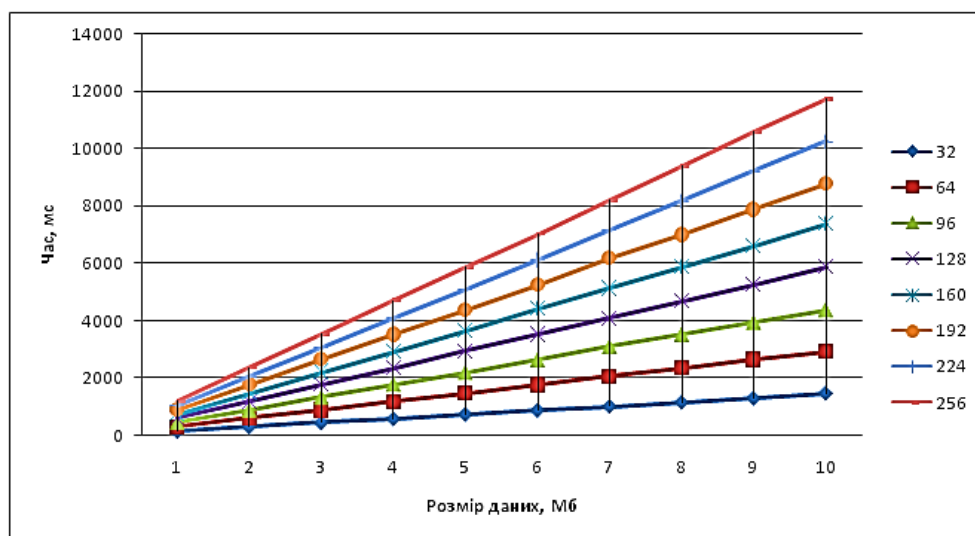


Рис. 2.1 – Вимір 1: «Quad core Intel Core 2 Quad E6600 2,40GHz 4Gb RAM»

Розмір ключа, біт	Розмір даних, Мегабайт									
	1	2	3	4	5	6	7	8	9	10
32	250,00	515,63	765,63	984,38	1218,75	1468,75	1687,50	2046,88	2281,25	2515,63
64	500,00	968,75	1484,38	1968,75	2515,63	2859,38	3484,38	3937,50	4531,25	5500,00
96	781,25	1531,25	2375,00	3421,88	4343,75	4468,75	5593,75	5875,00	6687,50	7421,88
128	953,13	1890,63	2890,63	3812,50	4890,63	5953,13	6828,13	7812,50	8921,88	9671,88
160	1218,75	2390,63	3640,63	4890,63	6234,38	7453,13	8562,50	9796,88	10968,75	12250,00
192	1437,50	2828,13	4437,50	5765,63	7250,00	8734,38	10140,63	11531,25	13203,13	14703,13
224	1640,63	3453,13	4968,75	6812,50	8609,38	10203,13	11906,25	14140,63	15609,38	17937,50
256	2156,25	4937,50	6312,50	7906,25	9765,63	11796,88	13656,25	15750,00	17296,88	19796,88

Таблиця 2.2 – Вимір 2: «Single core AMD Athlon 3GHz 1Gb RAM»

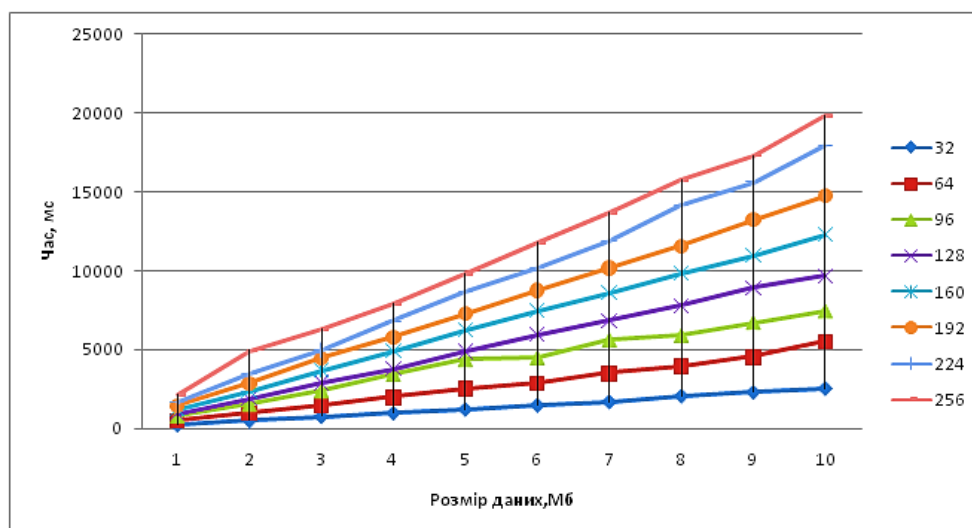


Рис. 2.2 – Вимір 2: «Single core AMD Athlon 3GHz 1Gb RAM»

Презентований алгоритм є універсальним і ефективним симетричним алгоритмом шифрування даних. Цей алгоритм забезпечує однорідне шифрування всіх типів даних на основі бінарного алфавіта. Маючи лінійну складність, алгоритм здійснює обробку даних швидко. Застосування нелінійної функції шифрування робить алгоритм стійким до різних типів атак супротивника. Завдяки

зазначеним перевагам алгоритм може бути основою для нового надійного інструменту забезпечення безпеки даних.

Висновки до другого розділу

Поява квантового комп'ютера в найближчий час є очікуваною подією. Чи буде існувати електронне управління та електронний бізнес у "постквантовий" час? Відповідь залежить від успіхів постквантової криптографії. З іншого боку алгоритми одного з перспективних напрямків постквантових досліджень поліноміальної криптографії від багатьох змінних вже застосовуються для створення струменевих симетричних алгоритмів та алгоритмів цифрового підпису.

Вже розроблені алгоритми постквантової криптографії безпека яких базується на складності схованої проблеми логарифму дискретного. Подальші криптологічні дослідження їх властивостей повинні з'ясувати їх придатність в постквантовий час. Симетричні алгоритми з приватним ключем для створених криптосистем можуть вже зараз використовуватися при розв'язанні практичних задач електронного управління та бізнесу. Їх перевагою є керованість рівня безпеки, що визначається степінню та густиною схованого поліноміального відображення.

Список джерел, використаних у другому розділі

1. Ding J. , Gower J.E., Schmidt D. S., Multivariate Public Key Cryptosystems, - Springer, Advances in Information Security, V.~25, 2006, - 259 p.
2. Goubin L., Patarin J., Bo-Yin Yang, Multivariate Cryptography. Encyclopedia of Cryptography and Security, (2nd Ed.) 2011, pp. 824-828.
3. Porras J., Baena J., Ding J., New Candidates for Multivariate Trapdoor Functions, Revista Colombiana de Matematicas, 2015 (November), vol. 49, No 1, pp 57-76 .

4. Ustimenko V. A., Explicit constructions of extremal graphs and new multivariate cryptosystems // *Studia Scientiarum Mathematicarum Hungarica*, Special issue "Proceedings of The Central European Conference, 2014, Budapest", 2015 (June), Vol. 52, issue 2, pp. 185-204.

5. Ustimenko V., On Multivariate Cryptosystems Based on Computable Maps with Invertible Decompositions // *Annales of UMCS. Informatica*, 2014, Vol. 14, Special issue "Proceedings of International Conference Cryptography and Security Systems", pp.7-18.

6. Patarin J. , The Oil and Vinegar digital signatures, Dagstuhl Workshop on Cryptography, 1997.

7. Kipnis A., Shamir A., Cryptanalysis of the Oil and Vinegar Signature Scheme // *Advances in Cryptology - Crypto 96*, Lecture Notes in Computer Science, Vol. 1462, 1996, pp 257--266.

8. Bulygin S., Petzoldt A. and Buchmann J., Towards provable security of the unbalanced oil and vinegar signature scheme under direct attacks, In Guang Gong and Kishan Chand Gupta, editors, "Progress in Cryptology - INDOCRYPT", Guang Gong and Kishan Chand Gupta, editors, Lecture notes in Computer Science, Vol. 6498, 2010. pp. 17–32.

9. Romańczuk-Polubiec U., Ustimenko V., On two windows multivariate cryptosystem depending on random parameters // *Algebra and Discrete Mathematics*, 2015, Vol. 19, No. 1., pp. 101--129.

10. Ustimenko V., On Shubert cells in grassmanians and new algorithm of multivariate cryptography, *Proceedings of Institute of Mathematics*, Minsk, 2015, Vol. 23, no 2, pp 137-148.

11. Ustimenko V., On algebraic graph theory and non-bijective maps in cryptography, *Algebra and Discrete Mathematics*, 2015, Vol. 20, no 1, pp. 152–170.

12. Ustimenko V., Wroblewska A., On the key exchange with nonlinear polynomial maps of stable degree $\leq d$ // *Annals UMCS Informatica*, 2011, AI XI, no 2, pp. 81-93.

13. Ustimenko V., Romanczuk U., On Dynamical Systems of Large Girth or Cycle Indicator and their applications to Multivariate Cryptography}, // *Artificial Intelligence, Evolutionary Computing and Metaheuristics, In the footsteps of Alan Turing Series: Studies in Computational Intelligence*, Vol. 427, Springer, January , 2013, pp. 257-285.

14. Wroblewska A., On some properties of graph based public keys, *Albanian Journal of Mathematics*, 2008, Vol. 2, no 3, pp. 229-234 (proceedings of NATO Advanced Studies Institute: "New challenges in digital communications").

15. Ustimenko V. A., Maximality of affine group, and hidden graph cryptosystems, *J. Algebra and Discrete Math.*, 2005, no 1, pp. 133-150.

16. V.Ustimenko, Coordinatisation of Trees and their Quotients, in the *Voronoj's Impact on Modern Science*, Kiev, Institute of Mathematics, 1998, vol. 2, 125-152.

17. V. I. Sushchansky , V. A. Ustimenko, On the characterization of types of Boolean functions, in *Calculations in Algebra and Combinatorics*, Kiev, Inst.Cyb., NAN U, 1979, pp. 44{51.

18. L. A. Kaluznin, V.I. Sushchansky, V. A. Ustimenko, Exponentiation in permutation group theory and its applications, *Proceedings of the Sixth Soviet Union Conference on the group theory*, Kiev, IM Ukr. Acad. Sci., 1979, pp. 135{145.

19. L. A. Kaluznin, V. I. Sushchansky, On the system of computer programs for studies of permutation groups, *Proceedings of the Conference on Interactive Systems*, Borjomi, March 1981, Tbilisi, Georgia, USSR, pp. 32{37.

20. L. A. Kaluznin, V.I. Sushchansky, V. Ustimenko, Computer science and its applications to the theory of permutation groups, *Kibernetika*, 1982, no. 6, pp. 63-84.

21. Калужнин Л. А., Суцанский В. И. Преобразования и подстановки, Москва, Просвещение, 1978.

22. V.Ustimenko, CRYPTIM: Graphs as Tools for Symmetric Encryption, Lecture Notes in Computer Science, Springer, LNCS 2227, Proceedings of AAEECC-14 Symposium on Applied Algebra, Algebraic Algorithms and Error Correction Codes, November 2001, p. 278 - 286.

23. T. Shaska, W.C. Huffman, D. Joener and V. Ustimenko (editors), Advances in Coding Theory and Cryptography, Advances in Coding Theory and Cryptography, Series on Coding and Cryptology, vol. 3, (2007).

24. Algebraic Aspects of Digital Communications, IOS Press (Lectures of Advanced NATO Institute 2008), NATO Science for Peace and Security Series - D: Information and Communication Security, v. 24, July 2009, 296 pp.

25. V. Ustimenko, On K-theory of dynamical systems corresponding to graphs and its applications, Dopovidi NAS of Ukraine, N8,2013. pp. 15-21.

26. V. Ustimenko, M. Klisowski, Graph based cubical multivariate maps and their cryptographical applications, in Advances on Superelliptic curves and their Applications, IOS Press, NATO Science for Peace and Security series D: Information and Communication Security, vol 41, 2014, pp. 305 -327.

РОЗДІЛ 3

ПРО НОВІ ПОТОКОВІ АЛГОРИТМИ СТВОРЕННЯ ЧУТЛИВИХ ДАЙДЖЕСТІВ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

3.1. Про верифікацію електронних документів

Спрощену модель глобального інформаційного простору можна уявляти як велику, зростаючу в часі мережу зареєстрованих віртуальних користувачів (фізичні особи або установи) які обмінюються інформацією та можуть її зберігати в електронних сховищах, що розташовані в мережі або знаходяться в ізоляції від неї.

Розмір файлів для обміну (електронних документів) має тенденцію зростати. Важливою категорією інформаційного простору є довіра до документів. Користувачі можуть використати симетричний алгоритм із приватним ключем для шифрування документів та протоколу обміну ключів для підтримки безпеки процедури кодування. Для зміни ключа також можуть використовуватися і сертифіковані алгоритми з публічним ключем. Ці методи забезпечують безпеку каналів обміну.

Легко побачити, що навіть користування надійними засобами шифрування не забезпечує повної довіри до документів, тому що треба рахуватися із шумами у каналах та проблемами безпечного збереження файлів в електронних сховищах, де документи можуть бути підроблені, пошкоджені комп'ютерними вірусами, технічними помилками в роботі обчислювальної техніки та інше.

Зазначимо, що останнім часом постійно зростає загроза потужних кібертерористичних атак на сховища електронної інформації різного призначення, їх наслідки це не тільки виток інформації, але й ушкодження або фальсифікування документів. Зрозуміло, що після виявлення кібератаки на корпоративне сховище інформації потрібно робити аудит усіх файлів системи. Протидія цій загрозі вимагає розробки нових програмних засобів.

Довіра до документів є важливою категорією інформаційного простору. Легко побачити, що навіть користування надійними засобами шифрування не забезпечує повної довіри до документів, тому що треба рахуватися із шумами у каналах та проблемами безпечного збереження файлів у електронних сховищах, де документи можуть бути підроблені, пошкоджені комп'ютерними вірусами, технічними помилками в роботі обчислювальної техніки та інше. Для задач виявлення кібератак, верифікації та автентифікації документів потрібні так звані залежні від ключів хеш-функції (автентифікаційні коди повідомлень або МАСи) які залежать від гасла. [2]. Хеш-функція потрібна для генерації скомпенсованої форми оригінального документа довільно обраного розміру. Таку форму називають хешем або дайджестом документа, її використовують у різних криптографічних застосуваннях. Хеш- функція h працює з файлом довільного розміру n , її значення має фіксований розмір.

Для інших задач захисту інформації потрібна загальна хеш-функція, що не потребує ключа або ж гасла. Нещодавно було сертифіковано загальну хеш-функцію Купина як новий державний стандарт України [1].

3.2. Вимоги до дайджесту документів

Криптографічно стабільна функція хешування f повинна забезпечувати: практичну неможливість вибору пари посилань x та z таким самим значенням хеш-функції. Для дайджесту документа, створеного залежною від ключа хеш-функцію (МАС) використовують символ НМАС. Коли користувачі хочуть безпечно обмінятися кореспонденцією, перевіряючи хто є дійсним автором листа, так і відсутність змін при пересилці, вони разом обирають спільний МАС. При цьому користуються спільною схемою симетричного шифрування.

Крім криптографічної стабільності дуже важлива швидкодія та високий показник аваланч ефекту. Цей ефект вимірюється таким чином. Обчислюється НМАС для генерованого файлу, змінюється довільний його біт та обчислюється НМАС для зміненого файлу, після цього робиться побітове порівняння отриманих

дайджестів. Для практичного вживання МАСу потрібно, щоб статистичні дослідження показали, що поєдина зміна символу приводить до зміни 40% бітів НМАСу незалежно від розміру файлів, що генеруються[9].

3.3. Про некомутативну криптографію та її застосування до задач симетричного шифрування і побудови хеш функцій

Некомутативна криптографія є активною областю криптології, яка досліджує криптографічні примітиви та системи, засновані на алгебраїчних структурах, таких як групи, напівгрупи та некомутативні кільця [18-29]. Одним з найбільш ранніх застосувань некомутативної алгебраїчної структури для криптографічних цілей було використання груп для розробки криптографічних протоколів. Пізніше декілька інших некомутативних структур, таких як групи Томпсона та групи Григорчука, були визначені як потенційні кандидати для криптографічних постквантових додатків. Стандартним способом представлення груп і напівгруп є використання генераторів і зв'язків (Теорія комбінаторних груп), криптографія на основі напівгруп складається із загальних криптографічних схем, визначених у термінах широких класів напівгруп і їх реалізацій для вибраних напівгруп сімей (так звані платформи напівгруп). Звичайна техніка використання пам'яті комп'ютера для представлення групи і напівгрупи заснована на методі генераторів і відношень.

У роботах [3, 14, 30, 32, 33] автори розглядають альтернативний метод представлення групи платформ G як підгрупи афінної напівгрупи Кремони $S(Kn)$ над скінченним комутативним кільцем K всіх поліноміальних перетворень і припускається, що кожен елемент подається у стандартній формі багатовимірної криптографії. Отже, напівгрупа операцій відображень композицій індукує групові операції перетворень. Це спроба поєднати методи некомутативної криптографії та багатовимірної криптографії.

Некомутативну криптографію створено для дослідження проблем асиметричної криптографії, таких як алгоритми відкритих ключів, протоколи обміну ключами та криптосистеми типу Ель Гамала. У випадку коротко

представленого вище підходу до використання спеціальних підгруп афінних методик напівгрупи Кремони некомутативної криптографії у симетричній криптографії, таких як розробку поточкових шифрів [6, 34] і конструкції НМАС [35]. Використовуються нелінійні підгрупи афінних напівгруп Кремони. Метод генерування афінних перетворень у термінах спеціальних графів, заданих рівняннями (так звані лінгвістичні графи), використовується замість методу генераторів і відношень [13, 14]. Інші застосування теорії графів до криптографії розглядаються в [31].

Дослідження НМАС (і пов'язаних з ними НМАСами) - гаряча галузь. Повне спостереження опублікованих результатів з розробки цих засобів та їх криптоаналізу просто неможливо, ми звертаємося лише до декількох останніх робіт [36 - 45].

Зверніть увагу, що будь-яка криптографічна хеш-функція, така як MD5 або SHA-1, може бути використана при обчисленні НМАС; отриманий алгоритм МАС називається НМАС-MD5 або НМАС-SHA-1 відповідно. Криптографічна ефективність НМАС залежить від криптографічної ефективності основної хеш-функції, розміру її хеш-виходу, а також від розміру і якості ключа.

3.4. Математичне підґрунтя хеш функції, що пропонується

Нехай $F(K)$ - простір потенційно нескінченних текстів в алфавіті K , який являє сукупність всіх кортежів виду $(a_1, a_2, \dots, a_k), a_i \in K$ різної довжини k . Будемо вважати, що K є скінченним комутативним кільцем та ототожнювати $F(K)$ з напівгрупою із наступним множенням $(a_1, a_2, \dots, a_k) \circ (b_1, b_2, \dots, b_s) = (a_1, a_2, \dots, a_k, b_1 + a_k, b_2 + a_k, b_s + a_k)$. Нехай $F'(K)$ буде піднапівгрупою всіх слів парної довжини. Позначимо через $S(K^n)$ скінченну напівгрупу всіх поліноміальних відображень простору K^n в себе.

Теорема 3.1. ([3]) *Для кожного натурального $m \geq 2$ існує гомоморфне відображення $\psi: F'(K) \rightarrow S(K^m)$ таке, що його образ $\psi(F'(K))$ утворює групу G кубічних поліноміальних відображень ступеня 3.*

Нагадаємо, що властивість гомоморфного відображення для $\psi = \psi_m$ записується як $\psi(a \circ b) = \psi(a) \circ \psi(b)$.

Відображення, що задовольняє умовам теореми будується конструктивно в термінах теорії дискретних динамічних систем, визначених за алгебраїчними графами з екстремальними властивостями [4]. Ці методи дозволяють одержати таку нижню оцінку порядку конструктивно побудованої групи: $|G| \geq 2^{4n}$. Зазначимо, що твердження визначає рідкісний математичний об'єкт. Суперпозиція двох кубічних відображень з великою ймовірністю буде мати ступінь 9, трьох – 27, чотирьох – 81, а у побудованій групі всі ці добудки обмежені числом 3. Ця група вже вживалася для побудови криптографічних алгоритмів з приватним ключем [5, 6], та протоколів обміну ключами [4, 7, 10, 11].

Для створення МАСу [9] було використано не саму групу G , а відображення ψ , що її визначає, разом з афінними A та B перетвореннями групи Кремони за правилом $g : x \rightarrow A\psi(x)B$. Не важко побачити, що ψ – природний оператор компресії даних, який відображає нескінченну множину $F'(K)$ усіх слів парної довжини в алфавіті K на скінченну множину $S(K^m)$. На вихід подається список координат $g(x)$, до яких двічі застосовано оператор повного диференціалу. Комп'ютерна симуляція дозволила обчислити дуже високий аваланч ефект у межах 97-99%. Для прикладу в МАСу російських дослідників інтервал аваланч ефекту оцінюється як 47-50% [8]. Конструктивна побудова гомоморфізмів компресії визначається у термінах теорії лінгвістичних графів, елементи якої представлені у розділі 5. При цьому застосовуються відомі лінгвістичні графи $A(n, K)$ та $D(n, K)$ побудовані при розв'язанні задач екстремальної теорії графів.

3.5. Пришвидшення алгоритмів

У цьому підрозділі буде представлено модифікацію описаного вище алгоритму, що дозволяє зберегти (або ж поліпшити) рівень аваланч ефекту при значному підвищенні швидкодії. Зазначимо, що алгоритм визначається «за модулем» процедуру обчислення значень гомоморфізму з теореми 3.1

попереднього підрозділу. Конструктивне визначення гомоморфізму ψ буде описане нижче у термінах відомих алгебраїчних графів з екстремальними властивостями. При цьому використана концепція лінгвістичних родин графів, що дозволяє вивчати спеціальні напівгрупу та групу, пов'язаних з графами заданими системами алгебраїчних рівнянь.

Нехай $(a_1, a_2, \dots, a_n)$ документ представлений в алфавіті K після перемішування з деяким псевдовипадковим словом сталої довжини. Будемо вважати, що число n парне. Користувачі обирають розмір дайджесту $m, m < n$ та $m = O(1)$ або ж $m = O(n)$ разом з ключем, що складається зі зростаючої послідовності натуральних чисел $i(1), i(2), \dots, i(m-1)$ та невиродженої матриці M складеної з елементів кільця лишків Z_{256} . Вони утворюють вектор $u = (v_1, v_2, \dots, v_m)$, де $v_1 = a_1 + a_2 + \dots + a_n, \dots, v_j = v_{j-1} - a_{i(j-1)}$. Потім обчислюється кубічне відображення $F = \psi_m(a_1, a_2, \dots, a_n)$, яке кореспонденти застосовують до вектора u . Отриманий вектор-рядок $F(u)$ множиться на матрицю M . Вектор $w = F(u)M$ вважаємо дайджестом документу.

Зазначимо, що значення $F(u)$ обчислюється за допомогою рекурсивного алгоритму, його складність визначається як $O(mn)$ і співпадає зі складністю створення дайджесту.

Цей базовий алгоритм легко модифікувати без змінення складності обчислень. Зокрема:

1) Можна представити слово $(a_1, a_2, \dots, a_n)$ у вигляді конкатенації скінченної кількості слів $z_1, z_2, \dots, z_t$ парної довжини. Потім обрати послідовність слів вигляду $u_1, u_2, \dots, u_k$, де $u_i \in \{z_1, z_2, \dots, z_t\}$ таку, що кожне z_i у цій послідовності зустрічається не менше ніж один раз. Далі обчислюється значення u добутку $u_1, u_2, \dots, u_k$ у розглянутій вище напівгрупі слів $F'(K)$. Алгоритм модифікується заміною кубічного відображення $\psi(a)$ на $\psi(y)$. При умові всім відомого розбиття файлу криптографічна стабільність такого дайджесту буде залежною від проблеми розкладу $\psi(y)$ у добуток перетворень $\psi(z_i)$ з афінної групи Кремони. Зазначимо,

що поліноміального алгоритму для розв'язання цієї проблеми на звичайному або квантовому комп'ютері на сьогоднішній день не знайдено. Насправді ця задача виникає за умов неповної визначеності, бо відоме тільки значення $\psi(y)$ на деякому залежному від файла векторі. Зрозуміло що розбиття a на підслова z_i та послідовність u_j слід вважати частиною спільного ключа для кореспондентів.

2) Можна обчислювати v_1 як добуток виразів $2a_i + 1$ та одержувати v_i діленням v_{i-1} на $2a_{i(j-1)} + 1$.

3) У варіанті 2 можна замінювати v_i на його непарні степені $k, k < 128$. Тоді ці степені слід вважати параметрами ключа.

Імплементовані випадки зручні для їх використання у технології *blockchain*, де потрібні дайджести у вигляді послідовності бітів або ж нулів та одиниць.

Зазначимо, що добрі властивості функції компресії ґрунтуються на конструкціях гомоморфізмів нескінченної півгрупи слів парної довжини у півгрупи Кремони, визначені родинami алгебраїчних графів з екстремальними властивостями.

3.6. Про лінгвістичні графи та пов'язані з ними напівгрупи афінних перетворень

Відсутні визначення теорії графів можна знайти у [12]. Всі графи, які ми розглядаємо, є простими графами, тобто неорієнтованими без петель та кратних ребер. Нехай через $V(G)$ і $E(G)$ позначимо множину вершин та множину ребер G відповідно.

Коли буде зручно, ми будемо ототожнювати G з відповідним антирефлексивним бінарним відношенням на $V(G)$, тобто $E(G)$ є підмножиною $V(G) \circ V(G)$ і запишемо $v G u$ для суміжних вершин u і v (чи сусідніх).

Позначимо $|\{ x \in V(G) \mid x G v \}|$ як ступінь вершини v .

Структура інцидентності є множина V з розділеними множинами P (точок) і L (прямих) і симетричного бінарного відношення I , такого що належність двох елементів означає, що один із них буде точкою, а інший – прямою. Будемо ідентифікувати I з простим графом цього відношення інцидентності або дводольного графа. Пара $x, y, x \in P, y \in L$ така що $x I y$ називається прапором структури інцидентності I .

Нехай K – скінченне комутативне кільце. Позначимо структуру інцидентності з множини точок $P=P_{s,m}=K^{s+m}$ і множини прямих $L=L_{r,m}=K^{r+m}$ як лінгвістичну структуру інцидентності I_m якщо точка $x=(x_1, x_2, \dots, x_s, x_{s+1}, x_{s+2}, \dots, x_{s+m})$ належить прямій $y=[y_1, y_2, \dots, y_r, y_{r+1}, y_{r+2}, \dots, y_{r+s}]$ тоді і тільки тоді коли виконується співвідношення:

$$a_1 x_{s+1} + b_1 y_{r+1} = f_1(x_1, x_2, \dots, x_s, y_1, y_2, \dots, y_r)$$

$$a_2 x_{s+2} + b_2 y_{r+2} = f_2(x_1, x_2, \dots, x_s, x_{s+1}, y_1, y_2, \dots, y_r, y_{r+1})$$

...

$$a_m x_{s+m} + b_m y_{r+m} = f_m(x_1, x_2, \dots, x_s, x_{s+1}, \dots, x_{s+m}, y_1, y_2, \dots, y_r, y_{r+1}, \dots, y_{r+m})$$

де a_j , і $b_j, j=1,2,\dots,m$ не є дільниками нуля, і f_j багатовимірні многочлени з коефіцієнтами з K [13]. Квадратні та круглі дужки дозволяють відрізняти точки від прямих.

Колір $\rho(x)=\rho((x))$ ($\rho(y)=\rho([y])$) точки x (прямої $[y]$) визначається як проекція елемента (x) (відповідно $[y]$) від вільного модуля на його початок s (відносно r) координат. Як випливає із визначення лінгвістичної структури інцидентності для кожної вершини графа існує єдиний сусід вибраного кольору.

Позначимо $\rho((x))=(x_1, x_2, \dots, x_s)$ для $(x)=(x_1, x_2, \dots, x_{s+m})$ і $\rho([y])=(y_1, y_2, \dots, y_r)$ для $[y]=[y_1, y_2, \dots, y_{r+m}]$ як колір точки та колір прямої відповідно. Для кожного $b \in K^r$ і $p=(p_1, p_2, \dots, p_{s+m})$ існує єдиний сусід точки $[l]=N_b(p)$ кольору b . Так само для кожного $c \in K^s$ і прямої $l=[l_1, l_2, \dots, l_{r+m}]$ існує єдиний сусід прямої $(p)=N_c([l])$ кольору c . Потрійні параметри s, r, m визначають тип лінгвістичного графа.

Розглядаються також лінгвістичні структури інцидентності, визначених нескінченним числом рівнянь.

У випадку лінгвістичного графа Γ шлях, що складається з його вершин $v_0, v_1, v_2, \dots, v_k$ однозначно визначається початковою вершиною v_0 , і кольорами $\rho(v_i)$, $i=1, 2, \dots, k$ інших вершин зі шляху. Розглянемо відношення еквівалентності на множинах розбиття такі, що $(p) \approx (p') \ ([l] \approx [l'])$ якщо $p_{i+s} = p'_{i+s} \ (l_{i+r} = l'_{i+r})$ для $i \in \{1, 2, \dots, m\}$.

Визначимо оператор стрибка $J(p, a)$, $a \in K^s$ на множині розбиття P ($J(l, a)$, $a \in K^r$ на множині розбиття L) умовами $J(p, a) \approx (p)$ та $\rho(J(p, a)) = a(J([l], a) \approx [l])$ та $\rho(J([l], a)) = a$.

Оператор обчислення сусіда (чи оператор ковзання) $N(v, a)$, діє на PUL за правилами $N(p, a) = [l]$, де $(p)I[l]$, $\rho([l]) = a$ і $N([l], a) = (p)$, де $(p)I[l]$, $\rho((p)) = a$.

Розглянемо ланцюги ковзання лінгвістичного графа з початковою точкою p яка є послідовністю $(p, p_0, l_1, l_2, p_3, p_4, \dots, l_{t-3}, l_{t-2}, p_{t-1}, p_t)$, $t=4k, k \geq 0$ таке, що $p \approx p_0, l_{2i+1} \approx l_{2i+2}, i \geq 0, p_{2i+1} \approx p_{2i+2}$ і $p_{2i}Il_{2i+1}$ для $i \geq 0$.

Кольори елементів стрічок ковзання і початкова точка визначають цю послідовність. Очевидно, що послідовність обчислюється застосуваннями операторів стрибка J_a і ковзання, що чергуються. Насправді термін ланцюг ковзання вибирається, тому що його обчислення нагадує послідовності стрибків та поверхневих ковзань у фігурному катанні (або ж різних змаганнях на скейт бордах).

Конструкції напівгруп та груп.

Розглянемо напівгрупу $S(K^s)$ і сукупність $S^{s,r}(K)$ відображень вигляду $G: (y_1, y_2, \dots, y_r) \rightarrow (f_1(x_1, x_2, \dots, x_s), f_2(x_1, x_2, \dots, x_s), \dots, f_r(x_1, x_2, \dots, x_s))$. Якщо $H \in S(K^s)$ тоді $G(H)$ для $G \in S^{s,r}(K)$ існує відображення $(y_1, y_2, \dots, y_r) \rightarrow (f_1(H(x_1), H(x_2), \dots, H(x_s)), f_2(H(x_1), H(x_2), \dots, H(x_s)), \dots, f_r(H(x_1), H(x_2), \dots, H(x_s)))$.

Для зручності будемо ототожнювати елементи множини $S(K^s)$ з кортежами у $K[x_1, x_2, \dots, x_s]^s$ і елементи $S^{s,r}(K)$ кортежами у $K[x_1, x_2, \dots, x_s]^r$.

Розглянемо сукупність ${}^sBS_r(K)$ послідовностей виду $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_6, \dots, H_{t-1}, H_t)$, $t=4i$, де $H_k \in S(K^s)$, $G_j \in S^{s,r}(K)$. Будемо називати ${}^sBS_r(K)$ сукупністю смугастих символічних стрічок.

Будемо визначати добуток u з $u'=(H'_0, G'_1, G'_2, H'_3, H'_4, G'_5, G'_6, \dots, H'_{l-1}, H_l)$ як $w=(H_0, G_1, G_2, H_3, H_4, G_5, G_6, \dots, H_{t-1}, H'_0(H_t), G'_1(H_t), G'_2(H_t), H'_3(H_t), H'_4(H_t), G'_5(H_t), G'_6(H_t), \dots, H'_{l-1}(H_t), H'_l(H_t))$.

Легко побачити, що ця операція перетворює ${}^sBS_r(K)$ у напівгрупу з одиничним елементом $(H_0)=(E_0)$ де E_0 – тотожне перетворення з $S(K^s)$.

Розглянемо гомоморфізм групи ${}^sBS_r(K)$ у напівгрупу Кремони $S(K^{s+m})$, визначених у термінах лінгвістичного графа $I=I^m(K)$. Зверніть увагу на те, що ми можемо розглядати граф $I^m(K')$ над розширенням K' кільця K з використанням тих самих рівнянь у визначенні.

Візьмемо кільце $K'=K[x_1, x_2, \dots, x_{m+s}]$ де x_i є формальними змінними і розглянемо нескінченний граф $I^m(K[x_1, x_2, \dots, x_n])$, $n=m+s$ з множинами точок і прямих $P'=K[x_1, x_2, \dots, x_{m+s}]^{m+s}$ та $L'=K[x_1, x_2, \dots, x_{m+s}]^{m+r}$. Після цього беремо смугасту стрічку $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_6, \dots, H_{t-1}, H_t)$ утворену сукупністю поліномів з кільця $K[x_1, x_2, \dots, x_s]$ і точку $(x)=(x_1, x_2, \dots, x_n)$ утворену твірними елементами K' . Ці дані однозначно визначають ланцюг ковзання (x) , $J((x), H_0)=(^1x)$, $N(^1x, G_1)=[^2x]$, $J([^2x], G_2)=[^3x]$, $N([^3x], H_3)=(^4x)$, $J(^4x, H_4)=(^5x)$, ..., $J([^{t-2}x], G_{t-2})=[^{t-1}x]$, $N([^{t-1}x], H_{t-1})=(^tx)$, $J(^tx, H_t)=(^tx)$.

Нехай (^tx) - кортеж $(H_t, F_2, F_3, \dots, F_n)$ де $F_i \in K[x_1, x_2, \dots, x_n]$. Ми визначаємо ${}^1\Psi(u)$ як відображення $(x_1, x_2, \dots, x_n) \rightarrow (H_t, F_2, F_3, \dots, F_n)$, $n=m+s$.

Твердження, наведені нижче [14], випливають з визначення відображення.

Лема 3.1. Відображення $\Psi={}^1\Psi: {}^sBS_r(K) \rightarrow S(K^n)$ є гомоморфізмом напівгруп.

Посилаємося на ${}^I\Psi({}^sBS_r(K)) = {}^ISR(K)$ як напівгрупу ланцюгових перетворень лінгвістичного графа I .

Визначимо піднапівгрупу ${}^sS_r(K)$ гладких стрічок як сукупність смугастих стрічок $u = (H_0, G_1, G_2, H_3, H_4, G_5, G_6, \dots, H_{t-1}, H_t)$ з ${}^sBS_r(K)$ з

$H_0 = E_0$, $G_1 = G_2$, $H_3 = H_4$, $G_5 = G_6, \dots$, $H_{t-1} = H_t$. Будемо називати образ цієї напівгрупи ${}^I\Psi({}^sS_r(K)) = {}^ISW(K)$ напівгрупою символічних переходів на лінгвістичному графі I .

Припустимо, що H_t є бієктивним відображенням і його обернене є поліноміальним відображенням (у випадку нескінченного кільця K). Тоді ми можемо розглядати зворотню бінарну стрічку $Rev(u) = (H_{t-1}(H_t^{-1}), G_{t-2}(H_t^{-1}), G_{t-3}, (H_t^{-1}), H_{t-4}(H_t^{-1}), H_{t-5}^{-1}(H_t), \dots, G_2(H_t^{-1}), G_1(H_t^{-1}), H_0(H_t^{-1}), H_t^{-1})$.

Зверніть увагу, що сукупність бінарних стрічок u з H_t^{-1} поліноміальної природи утворює піднапівгрупу ${}^sBC_r(K)$. Будемо називати її напівгрупою реверсійних бінарних стрічок

Лема 3.2. Гомоморфне зображення ${}^I\Psi({}^sBC_r(K)) = IR_I(K)$ – підгрупа групи Кремони $C(K^n)$.

Дійсно ${}^I\Psi(u \cdot Rev(u))$, $u \in {}^sBC_r(K)$ – тотожне відображення

Назвемо $IR_I(K)$ підгрупою реверсійних символічних переходів лінгвістичного графа I .

3.7. Деякі алгебраїчні конструкції екстремальної теорії графів, відповідні гомоморфізми компресії та нелінійні групи перетворень.

3.7.1. Деякі означення екстремальної теорії графів.

Обхват графа Γ , позначемо $g = g(\Gamma)$, - довжина найкоротшого циклу у Γ . Діаметр $d = d(\Gamma)$ графа Γ – максимальна довжина найкоротшого проходу між двома його вершинами.

Нехай $g_x = g_x(\Gamma)$ – довжина мінімального циклу через вершину x з множини $V(\Gamma)$ вершин графа Γ . Позначимо $Cind(\Gamma) = \max\{g_x, x \in V(\Gamma)\}$ як індикатор циклу графа Γ .

Якщо Γ_i – сім'я k -регулярних зв'язних графів зростаючого порядку зі зростаючим індикатором циклу для якого добре визначено проєктивну границю $\Gamma = \lim \Gamma_i, i \rightarrow \infty$, тоді Γ – дерево, тобто нескінченний зв'язний граф без циклів. Сім'я Γ_i k -регулярних зв'язних графів постійного ступеня є родиною графів малого світу, якщо $d(\Gamma_i) \leq c \log_k(v_i)$, для деякої константи $c, c > 0$.

Нагадаємо, що сімейство регулярних графів Γ_i ступеня k і зростаючого порядку v_i є сім'єю графів великого обхвату, якщо $g(\Gamma_i) \geq c \log_k(v_i)$, для деякої незалежної константи $c, c > 0$.

Назвемо сімейство регулярних простих графів Γ_i ступеня k і порядку v_i як сімейство графів з великим індикатором циклу, якщо $Cind(\Gamma_i) \geq c \log_k(v_i)$ для деякої незалежної константи $c, c > 0$.

Зверніть увагу, що для вершинно-транзитивного графу його обхват та індикатор циклу збігаються. Визначені вище родини відіграють важливу роль в екстремальній теорії графів, теорії LDPC кодів та криптографії. [15].

3.7.2. Алгебраїчні графи $A(n, K)$ і $D(n, K)$, деякі результати і відкриті питання.

Нижче буде визначено сімейства графів $A(n, K)$ і $D(n, K)$, для кожного натурального числа $n, n > 2$ та комутативного кільця K . У випадку $K = F_q$ позначитимемо ці графи як $A(n, q)$ і $D(n, q)$, відповідно. Ці графи виникають як гомоморфні зображення нескінченних дводольних графів $A(K)$ і $D(K)$ для яких

множини точок та прямих P і L ототожнюються з копіями декартової степені K^N , де K – комутативне кільце і N – множина натуральних чисел. Щоб відрізнити точки від прямих будемо використовувати круглі та квадратні дужки. Якщо $x \in V$, тоді $(x) \in P$ і $[x] \in L$.

Опис ґрунтується на побудові цих графів у термінах множини коренів розширеної діаграми Динкіна A_1 та відповідної її алгебри Лі, що належить до класу алгебр Каца-Муді.

Вершини $D(K)$ – нескінченні розмірні кортежі над K ми запишемо їх наступним чином $(p) = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, \dots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \dots)$, $[l] = [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l'_{2,2}, l_{2,3}, \dots, l_{i,i}, l'_{i,i}, l_{i,i+1}, l_{i+1,i}, \dots]$. Будемо вважати, що майже всі компоненти точок і прямих нулі. Умова належності точки (p) і прямої $[l]$ $((p)I[l])$ може бути записана за допомогою переліку нижченаведених рівнянь:

$l_{i,i} - p_{i,i} = l_{1,0} p_{i-1,i}$; $l'_{i,i} - p'_{i,i} = l_{i,i-1} p_{0,1}$; $l_{i,i+1} - p_{i,i+1} = l_{i,i} p_{0,1}$; $l_{i+1,i} - p_{i+1,i} = l_{1,0} p'_{i,i}$. Ці чотири співвідношення визначені для $i \geq 1$, $(p'_{1,1} = p_{1,1}, l'_{1,1} = l_{1,1})$.

Аналогічно, визначимо графи $A(K)$ на множині вершин, що складаються з точок та прямих $(p) = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p_{2,3}, \dots, p_{i,i}, p_{i,i+1}, \dots)$,

$[l] = [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l_{2,3}, \dots, l_{i,i}, l_{i,i+1}, \dots]$ таких, що точка (p) належить прямій $[l]$ $((p)I[l])$, якщо між їх координатами виконуються наступні співвідношення: $l_{i,i} - p_{i,i} = l_{1,0} p_{i-1,i}$; $l_{i,i+1} - p_{i,i+1} = l_{i,i} p_{0,1}$.

Зрозуміло, що множина індексів $A = \{(1; 0), (0; 1), (1; 1), (1; 2), (2; 2), (2; 3), \dots, (i-1; i), (i; i), \dots\}$ є підмножиною $D = \{(1, 0), (0; 1), (1, 1), (1, 2), (2; 2), (2, 2)', \dots, (i-1, i); (i; i-1); (i, i); (i, i)', \dots\}$. Точки і прямі $D(K)$ є функціями від $K^{D-\{(1,0)\}}$ і $K^{D-\{(0,1)\}}$, їхні обмеження на $A-\{(1,0)\}$ і $A-\{(0,1)\}$ визначає гомоморфізм Ψ графа $D(K)$ на $A(K)$.

Для кожного додатного цілого $m \geq 2$ розглядаємо підмножини $A(m)$ і $D(m)$, що містять перші $m+1$ елементів A і D щодо визначених порядків. Обмеження точок і прямих $D(K)$ на $D(m)-\{(1,0)\}$ і $D(m)-\{(0,1)\}$ визначають граф гомоморфізму ${}^D\Delta(m)$

із зображенням, позначеним як $D(n, K)$. Аналогічно обмеження точок і прямих $A(K)$ на $A(m) - \{(1,0)\}$ і $A(m) - \{(0,1)\}$ визначають гомоморфізм ${}^A\Delta(m)$ графа $A(K)$ на граф, визначений як $A(m, K)$.

Розглянемо також відображення $\Delta(m)$ на вершинах графу $D(m, K)$ посилаючись на його точку $(p) \in K^{D(m) - \{(1,0)\}}$ обмеженою у $D(m) \cap A - \{(1,0)\}$ і його прямої $[l] \in K^{D(m) - \{(0,1)\}}$ обмеженою у $D(m) \cap A - \{(0,1)\}$. Це відображення є гомоморфізмом $D(m, K)$ на $A(n, k)$, $n = |D(m) \cap A| - 1$.

Граф $D(q) = D(F_q)$ де q -регулярний ліс. Його частки $D(n, q)$ є крайовими транзитивними графами. Тому їхні зв'язні компоненти є ізоморфними. Символ $D(n, q)$ означає граф, ізоморфний одній з таких зв'язних компонентів.

Сімейство $CD(n, q)$, $n=2,3,\dots$ є сімейством великого обхвату для кожного параметра q , $q>2$ [16]. Питання «Чи є $CD(n, q)$ сімейством графів малого світу?» залишається відкритим. Граф $A(q)$, $q>2$ є q -регулярним деревом. Графи $A(n, q)$ не мають транзитивних вершин.

Вони утворюють сімейство графів з великим індикатором циклу, який q -регулярний сімейства графів малого світу [17]. Питання «Чи є $A(n, q)$, $n=2,3,\dots$ сімейством великого обхвату?» залишається відкритим.

3.7.3. Про лінгвістичні та екстремальні графи і стабільні нелінійні підгрупи афінної групи Кремони

Всі графи, визначені у підрозділі 3.2, належать до класу L лінгвістичних графів $\Gamma = \Gamma(K)$ типу $(1, 1, n-1)$, $n \in \mathbb{N}$ або $n = \infty$. Визначаються над комутативним кільцем K , яке містить дводольні графи з множиною точок $P = K^n$ і множиною прямих $L = K^n$ таких, що $(p) = (p_1, p_2, \dots, p_n) \in P_n$ і $[l] = [l_1, l_2, \dots, l_n] \in L_n$ утворює ребро Γ , якщо виконуються наступні умови ${}^2ap_2 - {}^2bl_2 = {}^2f(l_1, p_1)$, ${}^3ap_2 - {}^3bl_2 = {}^3f(p_1, p_{12}, l_1, l_2)$, $\dots$, ${}^nap_n - {}^nbl_n = {}^nf(p_1, p_2, \dots, p_n, l_1, l_2, \dots, l_n)$, де ia і ib , $i \geq 2$ елементи мультиплікативної групи K^* , f_i поліноми від багатьох змінних. Визначимо кольори $\rho((p))$ і $\rho([l])$

точки (p) і прямої $[l]$ як їх перші координати p_1 і l_1 . Введемо добре визначений оператор $N(v, a)$, який обчислює сусіда вершини v кольору $a \in K$.

Нехай $S(K^n)$ означає напівгрупу Кремони поліноміальних перетворень вільного модуля K^n і $C(K^n)$ – афінна група Кремони обернених елементів $S(K^n)$ з поліноміальної інверсією. Ці алгебраїчні структури є важливими об'єктами алгебраїчної геометрії. Одна зі складних проблем полягає в побудові сімей стабільних підгруп G_n з $C(K^n)$ (чи напівгрупи S_n з $S(K^n)$) групи поліноміальних перетворень з максимальним ступенем, який дорівнює константі s . Зауважимо, що для більшості пара $f, g \in C(K^n)$ ступенів r і s їх наборів має ступінь rs . Тому ця проблема складна, вона має сильні криптографічні мотивації.

Розглянемо сукупність $St(K)$ рядків виду $(f_1, f_2, \dots, f_k)$ де $f_i \in K[x]$. Позначимо поліном f і відображення $x \rightarrow f(x)$ з $S(K)$. Добуток двох послідовностей $(f_1, f_2, \dots, f_k)$ і $(g_1, g_2, \dots, g_t)$ є послідовність $(f_1, f_2, \dots, f_k, g_1(f_k), g_2(f_k), \dots, g_t(f_k))$. Порожній рядок – це одиниця з напівгрупи $St(K)$. Фактично $St(K)$ є напівпрямим добутком вільної напівгрупи над алфавітом $K[x]$ і напівгрупи Кремони $S(K)$. Ми посилаємося на $St(K)$ як напівгрупу поліноміальних рядків. Нехай $St'(K)$ означає напівгрупу рядків парної довжини з $St(K)$ і $\Sigma(K)$ – підгрупа рядків парної довжини з координатами виду $x+c$, $c \in K$.

У випадку лінгвістичного графу $\Gamma = \Gamma(K)$ типу $(1,1,n-1)$ шлях, що складається з його вершин $v_0, v_1, v_2, \dots, v_k$ однозначно визначаються початковою вершиною v_0 , і кольори $\rho(v_i)$, $i=1, 2, \dots, k$ іншими вершинами зі шляху. Ми можемо розглядати граф $\Gamma' = \Gamma(K[x_1, x_2, \dots, x_n])$, визначений тими самими рівняннями з Γ , але над комутативним кільцем $K[x_1, x_2, \dots, x_n]$.

Отже, можна визначити наступне символічне обчислення. Візьмемо символічну точку $x=(x_1, x_2, \dots, x_n)$, де x_i є загальними змінними з $K[x_1, x_2, \dots, x_n]$ і поліноміальним рядком $C \in St'(K)$, який є кортежем многочленів $f_1, f_2, \dots, f_k$ з $K[x_1]$ з парним параметром k . ($x=x_1$). Утворюємо шлях вершин v_0, v_1 так, що $v_1 I v_0$ і $\rho(v_1)=f_1(x_1)$, v_2 так, що $v_2 I v_1$ і $\rho(v_2)=f_2(x_1)$, ..., v_k так, що $v_k I v_{k-1}$ і $\rho(v_k)=f_k(x_1)$. Вибираємо параметр k як парне число. Так v_k – точка з множини $K[x_1, x_2, \dots, x_n]^n$ графа Γ' .

Зауважимо, що обчислення кожної координати v_i залежить від змінних $x_1, x_2, \dots, x_n$ і многочленів $f_1, f_2, \dots, f_k$ потребує лише арифметичних операцій додавання та множення. Як впливає з визначення лінгвістичного графа остання вершина v_k (точка) має координати $(h_1(x_1), h_2(x_1, x_2), h_3(x_1, x_2, x_3), \dots, h_n(x_1, x_2, \dots, x_n))$, де $h_1(x_1) = f_k(x_1)$. Розглянемо відображення ${}^\Gamma H(C): x_i \rightarrow h_i(x_1, x_2, \dots, x_n)$, $i=1, 2, \dots, n$ яка відповідає поліноміальному рядку C .

Наступні твердження наведені у [14].

Теорема 3.2. . Відображення ${}^\Gamma \eta : C \rightarrow {}^\Gamma H(C)$ є гомоморфізмом $St'(K)$ у напівгрупі Кремони $S(K^n)$.

Назвемо ${}^\Gamma \eta$ лінгвістичним відображенням стиснення. Якщо K скінченне, то відображення перетворює сукупність потенційно нескінченних рядків у скінченну напівгрупу.

Неважко побачити, що $St'(K)$ збігається з напівгрупою ${}^s S_r(K)$ гладких стрічок для випадку $s=r=1$, що була визначена у підрозділі 3.5. Лі образ ${}^\Gamma \eta(St'(K))$ співпадає з напівгрупою ${}^I SW(K)$ символічних переходів на лінгвістичному графі I .

Неважко побачити, що ця напівгрупа $\Sigma(K)$ є ізоморфною напівгрупі $F'(K)$.

Теорема 3.3. Якщо Γ один з графів $D(n, K)$ і $A(n, K)$, то ${}^\Gamma \eta(\Sigma(K))$ є стабільною підгрупою $C(K^n)$ ступеня 3.

Як наслідок із цього твердження одержуємо теорему з підрозділу 3.1. При цьому виникає дві ефективні конструкції гомоморфізму ψ , а саме $\psi = {}^{D(n,K)}\eta$ та $\psi = {}^{A(n,K)}\eta$.

Позначимо ${}^\Gamma \eta(\Sigma(K))$ для $\Gamma = D(n, K)$ і $\Gamma = A(n, K)$ як $GD(n, K)$ і $GA(n, K)$. Ці групи вже використовувалися в усіх криптографічних додатках графів $D(n, K)$ і $A(n, K)$.

Таким чином представлений вище алгоритм створення дайджесту, визначений у підрозділі 3.4 «за модулем процедури обчислення гомоморфізму», поповнюється описом цієї процедури. Дві різні версії конструктивного визначення гомоморфізму ψ визначають два різні алгоритмічні пакети створення чутливих дайджестів документів.

Зазначимо, що групи $GD(n,K)$ і $GA(n,K)$ є підгрупами груп ${}^I\psi({}^sBC_r(K)) = IR_I(K)$, $I=D(n,K)$ та $A(n,K)$.

Розглянемо підгрупу $SIR_I(K)$, переходів зсуву групи $IR_I(K)$, реверсійних символічних переходів лінгвістичного графа I , що складається з образів стрічок з координатами вигляду $x+c$, $c \in K$. Елементи груп $SIR_I(K)$, $I=D(n,K)$, $I=A(n,K)$ можна вживати в алгоритмах створення дайджестів замість груп $GD(n,K)$ і $GA(n,K)$. При цьому кольори, що відповідають стрибкам слід вважати елементами гасла.

3.8 Про імплементацію алгоритмів створення дайджесту

Програми імплементовано на мові C++. Час її роботи залежить від параметрів комп'ютера. Ми використали звичайний персональний комп'ютер з процесором Pentium 3.00 GHz, 2GB пам'яті RAM та системи Windows 7. Для провадження комп'ютерних експериментів з базовим алгоритмом, описаним у підрозділі 3.4, було обрано групу $GA(n,K)$, та розширені матриці M , які обчислюються за час $O(m)$, де m – розмір дайджесту.

Для вимірювання аваланч ефекту дайджест представлявся у символах бінарного алфавіту. Швидкодія алгоритму в секундах, виміряна на файлах різного типу подається нижче.

Розмір файлу,	Розмір дайджесту (у бітах)						
	256	384	512	640	768	896	1024
4,0	1,36	2,03	2,74	3,43	4,12	4,81	5,52
16,1	4,94	7,40	9,90	11,0 9	14,88	16,99	19,82
38,7	11,6 0	17,3 9	23,20	29,0 3	34,84	40,65	46,46
62,3	18,5 4	27,8 0	37,10	46,3 8	55,68	64,94	74,22
121,3	36,2 4	54,3 5	72,52	90,6 3	108,7 6	126,8 9	145,02
174,2	51,2 2	77,7 2	103,6 6	129, 40	155,5 3	181,4 2	207,34

Таблиця 3.1 – Швидкодія алгоритму створення дайджестів

Комп'ютерний експеримент показав, що при зміні одного бінарного символу електронного документу змінюється щонайменше 98% символів дайджесту.

Висновки до третього розділу

Поточна робота підприємства, корпорації, фінансової установи потребує довгострокової праці спеціалістів із великою кількістю електронних документів. Для прийняття обґрунтованих планово-фінансових рішень, спеціалісти повинні користуватися перевіреною інформацією. Інструментом перевірки можуть бути

алгоритми компресії великого файлу і дайджест визначеного розміру, чутливий до будь-якої зміни символів на вході.

Запропоновано нову родину залежних від ключа швидких алгоритмів створення дайджестів електронних документів. Комп'ютерна симуляція дозволяє дослідити високий рівень аваланч ефекту, що виникає. Нехай K - вільно обране скінченне комутативне кільце, m -додатнє ціле число. Алгоритми використовують нещодавно знайдені гомоморфні відображення компресії напівгрупи потенційно нескінчених текстів у алфавіті K на скінчену групу кубічних поліноміальних перетворень m вимірного афінного простору K^m .

Криптографічна стабільність функцій хешування пов'язується зі складними алгебраїчними проблемами, такими як дослідження систем алгебраїчних рівнянь великої степені та задача розкладу нелінійного відображення вільного модуля за заданими твірними.

Алгоритми імплементовано у випадках скінченних полів $F_2^8, F_2^{16}, F_2^{32}$, кільця Z_{256} та $B(32)$ (булеве кільце порядку 2^{32}). Комп'ютерна симуляція демонструє, що швидкість алгоритму зростає зі збільшенням розміру базового комутативного кільця.

Пропоновані алгоритми можуть працювати з даними у вигляді тексту, відео та аудіо файлів, фільму тощо. Розроблені методи створення дайджестів мають потоковий характер – швидкодія при сталому m лінійно залежить від n . Зростання n збільшує криптографічну стабільність. Імплементації у блоковому режимі можлива, але не вмотивована, бо розмір блоку обмежує кількість змінних системи нелінійних рівнянь.

Необхідність подальших досліджень і технологічних розробок по створенню нових залежних від ключа швидких хеш-функцій пов'язана із викликами кібербезпеки, зростанням глобального інформаційного простору, очікування появи квантового комп'ютера та розвитком технологій bitcoins, де потрібно хешувати вхідні дані довільного розміру, перетворюючи їх у послідовність бітів, що є дайджестом так званих blockchains. Запропоновані швидкі алгоритми

створення чутливих до змін дайджестів документів вже зараз будуть практично використані для виявлення кібератак та аудиту усіх файлів системи після зареєстрованого втручання. Це перша вдала спроба по застосуванню ідеї не комутативної криптографії для створення НМАСів. Вважаємо, що потрібна подальша робота по оптимізації побудованих алгоритмів, їх порівнянням із відомими раніше НМАСами та крипто аналітичні дослідження.

Список джерел, використаних у третьому розділі

1. Oliynykov R., Gorbenko I., Kazymyrov O., Ruzhentsev V., Kuznetsov O., Gorbenko Yu., Dyrda O., Dolgov V., Pushkaryov A., Mordvinov R., Kaidalov D. Data Security. Symmetric block transformation algorithm. Ministry of Economical Development and Trade of Ukraine. DSTU 7624:2014. National Standard of Ukraine. Information technologies. Cryptographic. –2015.
2. Aumasson J.Ph, Serious Cryptography: A Practical Introduction to Modern Encryption, No Starch Press. – 2017. – 312 pp.
3. V. Ustimenko, On new symbolic key exchange protocols and cryptosystems based on hidden tame homomorphism,. *Dopov. Nac. akad. nauk Ukraine*. –2018, n 10. – pp.26-36.
4. Ustimenko V.A. Ob ekstremalnoy teorii grafov i simvolnyih vyichisleniyah [On extremal graph theory and symbolic calculations] //Dokl. NAN Ukrainyi, 2012 – №11 – s. 15-21.
5. Pustovit O., Ustymenko V., Pro zastosuvannia alhebraichnoi kombinatoriky do problem koduvannia ta kryptohrafii [On the application of algebraic combinatorics to the problems of coding and cryptography] //Matematychnе modeliuvannia v ekonomitsi, № 1-2. –Kyiv. – 2017. – s. 31-46.
6. Ustimenko V, Romańczuk-Polubiec U., Wróblewska A., Polak M., Zhupa E., On the implementation of new symmetric ciphers based on non-bijective multivariate

maps, Proceedings of the 2018 Federated Conference on Computer Science and Information Systems, M. Ganzha, L. Maciaszek, M. Paprzycki (eds). ACSIS, Vol. 15. – pp. 397-405 (2018).

7. Ustymenko V.O., Pustovit O.S. Pro novu kontseptsiiu elektronnoho pidpysu ta zasoby yii realizatsii [A new concept of electronic signature and means of its implementation], Kolektyvna monohrafiia za materialamy XVI Mizhnarodno-praktychnoi konferentsii. – m. Kyiv (Pushcha-Vodytsia). – 2017. – s. 86-89.

8. Krendelev S., Sazonova P., Parametric Hash Function Resistant to Attack by Quantum Computer, Based on Problem of Solving a System of Polynomial Equations in Integers, Proceedings of the 2018 Federated Conference on Computer Science and Information Systems, M. Ganzha, L. Maciaszek, M. Paprzycki (eds). ACSIS. – Vol. 15. –pp. 387 – 390 (2018).

9. Ustymenko V.O., Pustovit O.S. Pro novi alhorytmy audytu elektronnykh dokumentiv, yikh implementatsiiu ta zastosuvannia u kiberbezpetsi [A new algorithms for audit of electronic documents, their implementation and application in cybersecurity], Kolektyvna monohrafiia za materialamy XVII Mizhnarodno-praktychnoi konferentsii. – m. Kyiv (Pushcha-Vodytsia). –2018.–s. 170-174.

10. V. Ustimenko, M. Klisowski, On Noncommutative Cryptography with cubical multivariate maps of predictable density, Proceedings of the 2019 Computing Conference. – London. –July, 2019

11. Romańczuk-Polubiec, V. Ustimenko. On new key exchange multivariate protocols based on pseudorandom walks on incidence structures, Dopovidi NAN Ukrainy, N1, 2015, pp 41-49.

12. B. Bollobás, "Extremal graph theory", Academic Press, London, 1978.

13. V. Ustimenko, Maximality of affine group, hidden graph cryptosystem and graph's stream ciphers, Journal of Algebra and Discrete Mathematics, 2004, v.10, pp 51-65.

14. V. Ustimenko, On desynchronised multivariate algorithms of El Gamal type for stable semigroups of affine Cremona group, Theoretical and Applied Cybersecurity, KPI, N1, 2019.
15. M. Polak, U. Romańczuk, V. Ustimenko A. Wróblewska) On the applications of Extremal Graph Theory to Coding Theory and Cryptography, Electronic Notes in Discrete Mathematics Discrete Mathematics, N 43, p. 329-342.
16. F. Lazebnik, V. Ustimenko, A. J. Woldar, A new series of dense graphs of high girth, Bull. Amer. Math. Soc. (N.S.) 32 (1995), no. 1, 73–79
17. V. Ustimenko. On extremal graph theory and symbolic computations, Dopovidi National Academy of Sci, Ukraine, 2013, N2, pp 42-49.
18. Alexei Myasnikov, Vladimir Shpilrain and Alexander Ushakov (2008), Group-based Cryptography, Berlin: Birkhäuser Verlag.
19. Zhenfu Cao (2012), New Directions of Modern Cryptography. Boca Raton: CRC Press, Taylor & Francis Group. ISBN 978-1-4665-0140-9.
20. Benjamin Fine, et. al. "Aspects of Non abelian Group Based Cryptography: A Survey and Open Problems", arXiv:1103.4093.
21. Alexei G. Myasnikov; Vladimir Shpilrain and Alexander Ushakov (2011), Non-commutative Cryptography and Complexity of Group-theoretic Problems, American Mathematical Society.
22. Alexei G. Myasnikov; Vladimir Shpilrain and Alexander Ushakov (2011), Non-commutative Cryptography and Complexity of Group-theoretic Problems, American Mathematical Society.
23. I. Anshel, M. Anshel and D. Goldfeld, An algebraic method for public-key cryptography. Math. Res. Lett. 6(3–4), 287–291 (1999).

24. S.R. Blackburn and S.D. Galbraith, Cryptanalysis of two cryptosystems based on group actions. In: *Advances in Cryptology—ASIACRYPT '99. Lecture Notes in Computer Science*, vol. 1716, pp. 52–61. Springer, Berlin (1999).
25. K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang and C. Park, New public-key cryptosystem using braid groups. In: *Advances in Cryptology—CRYPTO 2000*, Santa Barbara, CA. *Lecture Notes in Computer Science*, vol. 1880, pp. 166–183. Springer, Berlin (2000).
26. G. Maze, C. Monico and J. Rosenthal, Public key cryptography based on semigroup actions, *Adv.Math. Commun.* 1(4), 489–507 (2007)
27. P.H. Kropholler and S.J. Pride , W.A.M. Othman K.B. Wong, P.C. Wong, Properties of certain semigroups and their potential as platforms for cryptosystems, *Semigroup Forum* (2010) 81: 172–186.
28. A. Lopez Ramos, J. Rosenthal, D. Schipani and R. Schnyder, Group key management based on semigroup actions, *Journal of Algebra and its applications*, vol.16 (to appear in 2019).
29. Gautam Kumar and Hemraj Saini, Novel Noncommutative Cryptography Scheme Using Extra Special Group, *Security and Communication Networks* ,Volume 2017, Article ID 9036382, 21 pages, <https://doi.org/10.1155/2017/9036382>
30. V. Ustimenko, On the families of stable transformations of large order and their cryptographical applications, *Tatra Mt. Math. Publ.*, 70 (2017), 107 =117.
31. Priyadarsini P.L.K., A Survey on some Applications of Graph Theory in Cryptography, *Journal of Discrete Mathematical Sciences and Cryptography*, 18:3, 209-217 (2015)
32. V. Ustimenko, On semigroups of multiplicative Cremona transformations and new solutions of Post Quantum Cryptography, *Cryptology ePrint Archive*, 133, 2019.
33. U. Romańczuk-Polubiec, V. Ustimenko, On Multivariate Cryptosystems Based on Polynomially Compressed Maps with Invertible Decompositions, *Cryptography and*

Security Systems, Third International Conference, CSS 2014, Lublin, Poland, September 22-24, 2014. Proceedings, Communications in Computer and Information Science, 448, p. 23-37.

34. V. Ustimenko, U. Romanczuk-Polubiec, A. Wroblewska, M. Polak, E. Zhupa, On the constructions of new symmetric ciphers based on non-bijective multivariate maps of prescribed degree, Security and Communication Networks, 2019 (to appear)

35. Mathew Cary, Ramarathnam Venkatesam, A Message Authentication Code Based on Unimodular Matrix Groups, Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings, Lecture Notes in Computer Science.

36. Mihir Bellare, Daniel J. Bernstein, and Stefano Tessaro. Hash-function based PRFs:AMAC and its multi-user security. LNCS, pages 566-595. Springer, Heidelberg, 2016.

37. Kan Yasuda. A Double-Piped Mode of Operation for MACs, PRFs and PROs: Security beyond the Birthday Barrier. In Antoine Joux, editor, EUROCRYPT, volume 5479 of Lecture Notes in Computer Science, pages 242-259. Springer, 2009.

38. Xiaoyun Wang, Hongbo Yu, Wei Wang, Haina Zhang, and Tao Zhan. Cryptanalysis on HMAC/NMACMD5 and MD5-MAC. In Antoine Joux, editor, EUROCRYPT, volume 5479 of Lecture Notes in Computer Science, pages 121-133. Springer, 2009.

39. Gaetan Leurent, Thomas Peyrin, and Lei Wang. New Generic Attacks against Hash-Based MACs. In Kazue Sako and Palash Sarkar, editors, Advances in Cryptology-ASIACRYPT 2013, volume 8270, pages 11-20. 2013.

40. Neal Koblitz and Alfred Menezes. Another look at HMAC. Cryptology ePrint Archive, Report 2012/074, 2012.

41. Yevgeniy Dodis, Eike Kiltz, Krzysztof Pietrzak, and Daniel Wichs. Message authentication, revisited. In David Pointcheval and Thomas Johansson, editors,

EUROCRYPT 2012, volume 7237 of LNCS, pages 355-374. Springer, Heidelberg, April 2012

42. Yevgeniy Dodis and John P. Steinberger. Domain Extension for MACs Beyond the Birthday Barrier. In Kenneth G. Paterson, editor, EUROCRYPT, volume 6632 of Lecture Notes in Computer Science, pages 323-342. Springer, 2011.

43. Yevgeniy Dodis, Thomas Ristenpart, John P. Steinberger, and Stefano Tessaro. To Hash or Not to Hash Again? , (In) Differentiability Results for H2 and HMAC. In Reihaneh Safavi-Naini and Ran Canetti, editors, CRYPTO, volume 7417 of Lecture Notes in Computer Science, pages 348-366. Springer, 2012.

44. Pierre-Alain Fouque, Gaetan Leurent, and Phong Q. Nguyen. Full Key-Recovery Attacks on HMAC/NMAC-MD4 and NMAC-MD5. In Alfred Menezes, editor, CRYPTO, volume 4622 of Lecture Notes in Computer Science, pages 13-30. Springer, 2007.

45. Jongsung Kim, Alex Biryukov, Bart Preneel, and Seokhie Hong. On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1 (Extended Abstract). In Roberto De Prisco and Moti Yung, editors, SCN, volume 4116 of Lecture Notes in Computer Science. Springer, 2006.

РОЗДІЛ 4

РЕАЛІЗАЦІЯ НОВИХ АЛГОРИТМІВ КРИПТОГРАФІЇ ВІД БАГАТЬОХ ЗМІННИХ ЛІНІЙНОЇ СТЕПЕНІ ТА ПОЛІНОМІАЛЬНОЇ ГУСТИНИ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

4.1. Публічні ключі

Одним із п'яти напрямків криптографії постквантового публічного ключа є побудова багатоваріантних відкритих ключів. Він був стартував з конструкцій квадратних бієктивних відображень F та приватних алгоритмів пошуку прообразу для $b = F(a)$. [1, 2, 16]. Пізніше деякі небієктивні відображення обмеженого ступеня використовувались у криптографії від багатьох змінних [17-19].

Нещодавно були запропоновані деякі спроби побудови відкритих ключів із відображеннями шифрування необмеженого ступеня та щільності поліномів [12].

Багатовимірні відкриті ключі можна знайти серед кандидатів, обраних для стандартизації NIST. Нагадаємо, що в березні 2019 року NIST опублікував список кандидатів, які потрапили у другий тур процесу Постквантової Криптографії (ПКК) [20, 21]. На сьогодні вже повідомлялося про апаратну ефективність деяких кандидатів у другий тур. Поточні кандидати, відмінні від багатоваріантних криптосистем, розробляються за наступними напрямками ПКК: системи на основі решітки, криптосистеми на основі коду, багатовимірна криптографія, криптографія на основі хешу, дослідження ізогеній для супереліптичних кривих.

Деякі дослідники вивчають можливості, що відрізняються від можливостей криптографії від багатьох змінних криптосистем, визначених за допомогою алгебраїчних об'єктів, цей напрям відомий як пов'язаний з недавнім розвитком некомутативної криптографії [22 - 38]. Важливо, щоб криптозастосування алгебри підтримувалось останніми криптоаналітичними дослідженнями [39] - [48].

4.2. Про використання афінної напівгрупи Кремони

Нехай K - комутативне кільце. Даваймо розглянемо сукупність усіх правил f виду $x_1 \rightarrow f_1(x_1, x_2, \dots, x_n), x_2 \rightarrow f_2(x_1, x_2, \dots, x_n), \dots, x_n \rightarrow f_n(x_1, x_2, \dots, x_n)$, для заданого параметра n та вибраного комутативного кільця K з натуральною операцією композиції. Ми припускаємо, що кожне правило написано у своїй стандартній формі, тобто кожен поліном f_i заданий списком його одночленів, записаним у вибраному порядку. Ми називаємо цю напівгрупу напівгрупою формальних перетворень $SF_n(K)$ вільного модуля K^n . Насправді це сукупність усіх ендоморфізмів кільця $K[x_1, x_2, \dots, x_n]$ з операціями їх суперпозиції. Кожне правило f з $SF_n(K)$ індукує перетворення $t(f)$, яке посиляє кортеж $(p_1, p_2, \dots, p_n)$ у $(f_1(p_1, p_2, \dots, p_n), f_2(p_1, p_2, \dots, p_n), \dots, f_n(p_1, p_2, \dots, p_n))$. Афінна напівгрупа Кремони $S(K^n)$ - це сукупність усіх перетворень виду $t(f)$ [50]. Канонічний гомоморфізм $h: f \rightarrow t(f)$ відображає нескінченну напівгрупу $SF_n(K)$ на скінченну напівгрупу $S(K^n)$, у випадку скінченного комутативного кільця K . Посилаємося на пару (f, f') елементів $SF_n(K)$ такі, що f, f' і $f'f$ є двома копіями однакових правил $x_1 \rightarrow x_1, x_2 \rightarrow x_2, \dots, x_n \rightarrow x_n$ як пари зворотних елементів. Якщо (f, f') є такою парою, то добуток $t(f)t(f')$ є відображенням ідентичності. Розглянемо підгрупу $CF_n(K)$ усіх обернених елементів $SF_n(K)$ (група формальних відображень). Зрозуміло, що образ обмеження h на $CF_n(K)$ є афінною групою Кремони $S(K^n)$ усіх перетворень K^n на K^n , для яких існує зворотний поліном.

Напівгрупа $SF_n(K)$ є важливим об'єктом теорії символічних обчислень або так званої комп'ютерної алгебри [1], яка є потужним інструментом криптографії від багатьох змінних [2, 3]. Будемо вважати, що кожен елемент f цієї напівгрупи записується в однаковій основі в його стандартній формі. Ступінь $\deg(f)$ - це максимальний ступінь багаточленів $f_i, i = 1, 2, \dots, n$. Щільність $\text{den}(f)$ з f - це максимальна кількість одночленів у $f_i(x_1, x_2, \dots, x_n)$.

Кажуть, що сімейство піднапівгруп S_n з $SF_n(K)$ (або $S(K^n)$) стійке ступеня d , якщо максимальний ступінь елементів з S_n є незалежною константою $d, d > 2$. Якщо K скінченне комутативне кільце, тоді стійка напівгрупа повинна бути

скінченною множиною. Коротке спостереження відомих сімей стабільних груп та їх криптографічне застосування можна знайти в [4].

Нехай $f(n)$ - сімейство нелінійних відображень із $SF_n(K)$ ступеня, обмеженого константою d . Кажуть, що $f(n)$ утворюють приручену сім'ю, якщо $SF_n(K)$ є сімейство $g(n)$ із $SF_n(K)$ ступеня, обмеженого константою d' , таке, що $f(n)g(n) = g(n)f(n)$ - тотожність. Нехай $T_1(n)$ і $T_2(n)$ - це два сімейства елементів із групи $AGL_n(K)$ усіх афінних бієктивних перетворень, тобто елементів афінної групи Кремони ступеня 1. Тоді називаємо $f'(n) = T_1(n)f(n)T_2(n)$ як лінійну деформацію $f(n)$. Очевидно, що $f'(n)$ - це також приручене сімейство перетворень, і ступені відображення з цього сімейства також обмежені d . Ступені обернених для $f'(n)$ обмежені d' .

Нехай $G_n < CF_n(K)$ - стійке сімейство підгруп ступеня d , $d > 1$, тоді нелінійні представники $f(n)$ з G_n утворюють приручене сімейство відображень. Неважко помітити, що щільності $f(n)$ та його лінійна деформація $f'(n)$ можуть бути дуже різними. Ми називаємо пару взаємно обернених елементів $f(n)$, $f(n)^{-1}$ із $CF_n(K)$ як пару з розривом щільності, якщо щільність $f(n)$ є поліноміальним виразом у змінній n і щільність $f(n)^{-1}$ обмежена нижче експоненціальною функцією a^n з основою $a > 1$.

Подібним чином ми називаємо пару взаємно обернених елементів $f(n)$, $f(n)^{-1}$ з $CF_n(K)$ як пару зі ступенем, якщо ступінь $f(n)$ є поліноміальним виразом у змінній n , і ступінь $f(n)^{-1}$ обмежена нижче експоненціальною функцією a^n з основою $a > 1$.

4.3. Про явну побудову стійких відображень заданого ступеня та великого порядку

Визначимо подвійний граф Шуберта $DS(k, K)$ над комутативним кільцем K як структуру падіння, визначену як неперервне об'єднання множин розділів $PS = K^{k(k+1)}$, що складається з точок, які є кортежами виду $x = (x_1, x_2, \dots, x_k, x_{11},$

$x_{12}, \dots, x_{kk}$) та $LS = K^{k(k+1)}$, що складається з рядків, які є кортежами типу $y = [y_1, y_2, \dots, y_k, y_{11}, y_{12}, \dots, y_{kk}]$, де $x \in$ інцидентною до y , тоді і тільки тоді, коли $x_{ij} - y_{ij} = x_i y_j$ для $i = 1, 2, \dots, k$ та $j = 1, 2, \dots, k$. Зручно припустити, що індекси виду i, j розміщуються для кортежів $K^{k(k+1)}$ у лексикографічному порядку.

Зауваження 4.1. Вибрано термін Подвійний граф Шуберта, оскільки точки та прямі $DS(k, F_q)$ можна розглядати як підпростори $F_q^{(2k+1)}$ розмірностей $k+1$ і k , які утворюють дві найбільші клітини Шуберта. Нагадаємо, що найбільша комірка Шуберта - це найбільша орбіта групи однокутних матриць, що діють на різноманітність підмножин заданих розмірів [5, 6].

Колір точки $x = (x_1, x_2, \dots, x_k, x_{11}, x_{12}, \dots, x_{kk})$ із PS визначаємо як кортеж $(x_1, x_2, \dots, x_k)$ та колір прямої $y = [y_1, y_2, \dots, y_k, y_{11}, y_{12}, \dots, y_{kk}]$ як кортеж $(y_1, y_2, \dots, y_k)$. Для кожної вершини v з $DS(k, K)$ існує унікальний сусід $y = N_a(v)$ даного кольору $a = (a_1, a_2, \dots, a_k)$.

Символічний колір g із $K[x_1, x_2, \dots, x_k]^{k \times k}$ з v виду $(f_1(x_1, x_2, \dots, x_k), f_2(x_1, x_2, \dots, x_k), \dots, f_k(x_1, x_2, \dots, x_k))$, де f_i -многочлени з $K[x_1, x_2, \dots, x_k]$ визначає сусідню пряму загальної точок $x = (x_1, x_2, \dots, x_k, x_{11}, x_{12}, \dots, x_{kk})$ з кольором $(f_1(x_1, x_2, \dots, x_k), f_2(x_1, x_2, \dots, x_k), \dots, f_k(x_1, x_2, \dots, x_k))$. Подібним чином ми можемо обчислити точку сусіда загальної прямої $[x] = [x_1, x_2, \dots, x_k, x_{11}, x_{12}, \dots, x_{kk}]$ кольору g .

Давайте розглянемо набір символічних кольорів $g^1, g^2, \dots, g^{2t}$ з $(K[x_1, x_2, \dots, x_k]^k)^{2t}$ та відображення f з PS на себе, яке відправляє точку $x = (x_1, x_2, \dots, x_k, x_{11}, x_{12}, \dots, x_{kk})$ в кінець v_{2t} ланцюжка $v_0, v_1, v_2, \dots, v_{2t}$, де $x = v_0$, $v_i \mapsto v_{i+1}, i = 0, 1, 2, \dots, 2t-1$, а колір v_i - це кортеж g_i , елементів з $K[x_1, x_2, \dots, x_k]$. Називаємо f відображенням закритих обчислень "точка-точка" із символічним ключем $g^1, g^2, \dots, g^{2t}$ або просто символічним обчисленням. Як впливає з визначень, $f = f^{g^1, g^2, \dots, g^{2t}}$ - це багатовимірне відображення $K^{k(k+1)}$ до себе. Коли надано символічний ключ, f можна обчислити у стандартній формі за допомогою елементарних операцій додавання та множення кільця $K[x_1, x_2, \dots, x_k, x_{11}, x_{12}, \dots, x_{kk}]$. Нагадаємо, що $(x_1, x_2, \dots, x_k, x_{11}, x_{12}, \dots, x_{kk})$ - це

наша символічна точка графу. Називаємо вираз $f g^{-1}, g^{-2}, \dots, g^{-2t}$ автоматичним поданням f із символічним ключем $g^{-1}, g^{-2}, \dots, g^{-2t}$. Зауважимо, що якщо t (g^{2t}) є елементом афінної групи Кремони $S(K^k)$, то $f g^{-1}, g^{-2}, \dots, g^{-2t}$ є оборотним, і автоматичне подання його зворотного має символічний ключ $g^{-2t} g^{2t-1}, g^{-2t} g^{2t-2}, g^{-2t} g^{2t-3}, \dots, g^{-2t} g^1, g^{-2t}$, де g^{-2t} є оберненим елементом g^{2t} . Обмеження ступенів і щільності багатовимірних відображень $(g g^i)$ від K^k до K^k та розмір параметра t дозволяють визначити поліноміальне відображення f зі ступенем і щільністю поліномів.

Нехай $g^i = (h_1^i, h_2^i, \dots, h_k^i)$, $i=1, 2, \dots, 2t$ є символічним ключем замкнутої точки до обчислення точки $f = f(n)$ символічного автомата $DS(k, K)$. Ми позначаємо елементи g^i як керуючі функції символічного ключа. Покладемо, що $g^0 = (h_1^0, h_2^0, \dots, h_k^0) = (x_1, x_2, \dots, x_k)$. Тоді f - перетворення виду

$$x_1 \rightarrow h_1^{2t}(x_1, x_2, \dots, x_k), \quad x_2 \rightarrow h_2^{2t}(x_1, x_2, \dots, x_k), \quad \dots, \quad x_k \rightarrow h_k^{2t}(x_1, x_2, \dots, x_k),$$

$$x_{11} \rightarrow x_{11} - h_1^1 x_1 + h_1^1 h_1^2 - h_1^2 h_1^3 + h_1^3 h_1^4 + \dots + h_1^{2t-1} h_1^{2t}$$

$$x_{12} \rightarrow x_{12} - h_1^1 x_2 + h_1^1 h_2^2 - h_2^2 h_1^3 + h_1^3 h_2^4 + \dots + h_2^{2t-1} h_1^{2t}$$

...

$$x_{kk} \rightarrow x_{kk} - h_k^1 x_k + h_k^1 h_k^2 - h_k^2 h_k^3 + h_k^3 h_k^4 + \dots + h_k^{2t-1} h_k^{2t}$$

Кажуть, що відображення f замкнутого обчислення від точки до точки є афінним, якщо всі елементи g^i символічного ключа є елементами ступеня < 2 . Називаємо підгрупу G в $S(K^n)$ напівгрупою ступеня d , якщо максимальний ступінь для представника g дорівнює d . Нехай $AGL_n(K)$ - група афінних перетворень K^n , тобто група всіх бієктивних перетворень ступеня 1.

Розглянемо напівгрупу $E_k(K)$, введену в [7], яка складається з усіх перетворень $f h^1, h^2, \dots, h^l, g$, де ступені h^i для $i = 1, 2, \dots, l$ та g обмежені 1, а l непарне число. Зрозуміло, що $E_k(K)$ є стабільною піднапівгрупою ступеня 2.

Група $GL_n(F_q)$ містить цикли Зінгера, тобто елементи порядку $q^n - 1$. [8,9]

Лема 4.1. Нехай $K = F_q$, нехай f - відображення замкнених обчислень від точки до точки $h^1, h^2, \dots, h^l, h$ і h визначає цикл Зінгера з $GL_k(F_q)$. Тоді порядок f дорівнює щонайменше $q^k - 1$.

Лема 4.2. Нехай $K = F_q$ і $f h^1, h^2, \dots, h^l, h$ є елементом напівгрупи $E_k(K)$ таким, що h визначає карту з $GL_k(F_q)$, яка має інваріантний підпростір W розмірності m , і обмеження h на W визначає цикл Зінгера. Тоді стабільна напівгрупа $\langle f \rangle$, породжена f , містить щонайменше $q^m - 1$ елементів.

Розглянемо два символічні обчислення 1C і 2C з керуючими функціями $f^1, f^2, \dots, f^t$ та $g^1, g^2, \dots, g^s$ та відповідними відображеннями $m_1 = m({}^1C)$ та $m_2 = m({}^2C)$. Розглянемо символічне обчислення 1C з керуючими функціями $f^1, f^2, \dots, f^t$ та $g^1(f^1), g^2(f^1), \dots, g^s(f^1)$ як об'єднання 1C та 2C . Неважко помітити, що відображення, що відповідає C , дорівнює $m_2(m_1)$. Отже, $C \rightarrow m(C)$ - це гомоморфізм двох моноїдів.

Давайте розглянемо сукупність $PL = PL(k, K)$ усіх обчислень від точки до точки C з керуючими функціями $f^1, f^2, \dots, f^t$ з останньою, f^t від $K(x_1, x_2, \dots, x_k)$ виду $(l_1(x_1, x_2, \dots, x_k), l_2(x_1, x_2, \dots, x_k), \dots, l_k(x_1, x_2, \dots, x_k))$, де всі вирази l_i мають ступінь 1. Легко помітити, що PL є замкненою множиною щодо операції конкатенації. Ми додаємо порожнє обчислення як формальний нейтральний елемент. Це означає, що відображення виду $m(C)$ з PL утворюють піднапівгрупу $S \setminus^{PL}$ афінна напівгрупа Кремони $S(K^{k(k+1)})$.

Зверніть увагу, що відображення $m(C)$, індуковане обчисленням від точки до точки C з керуючими функціями $f^1, f^2, \dots, f^t$, де f^t має координати, $f_1^t(x_1, x_2, \dots, x_k), f_2^t(x_1, x_2, \dots, x_k), \dots, f_k^t(x_1, x_2, \dots, x_k)$, є оборотним перетворенням $K^{k(k+1)}$, тоді і тільки тоді, коли відображення $x_1 \rightarrow f_1^t(x_1, x_2, \dots, x_k), x_1 \rightarrow f_2^t(x_1, x_2, \dots,$

x_k), ..., $x_k \rightarrow f_k^t(x_1, x_2, \dots, x_k)$, є бієкцією. Зрозуміло, що $m(C)^{-1}$ оберненого відображення з S^{PL} - це також елемент з S^{PL} .

Нехай G^{PL} - група всіх обернених елементів з PL . Визначаємо ступінь керуючої функції f^i , задану кортежем з координатами $f_1^i(x_1, x_2, \dots, x_k)$, $f_2^i(x_1, x_2, \dots, x_k)$, ..., $f_k^i(x_1, x_2, \dots, x_k)$ як максимальний ступінь f_j^i для різних i та j . Зверніть увагу, що $m(C)$ від G^{PL} може бути елементом з дуже великим порядком. Фактично, у випадку $K = F_q$ та довільного переліку керуючих функцій $f^1, f^2, \dots, f^t$ та f^t для даної білінійного відображення $x_1 \rightarrow f_1^t(x_1, x_2, \dots, x_k)$, $x_2 \rightarrow f_2^t(x_1, x_2, \dots, x_k)$, ..., $x_k \rightarrow f_k^t(x_1, x_2, \dots, x_k)$, що є циклом Зінгера, тобто його порядок принаймні $q^k - 1$, порядок $m(C)$ також обмежений знизу $q^k - 1$.

Можемо легко побудувати небієктивні відображення виду $m(C)$ з S^{PL} такі, що підгрупа, породжена цим елементом, складається з більш ніж q^{k-c} елементів для деякої константи $c > 1$. Насправді можна взяти f^t з інваріантним підпростором W розмірності $k-c$, таким чином, що обмеження f^t на W є циклом Зінгера. Нам зручно розглядати кортеж $(x_1, x_2, \dots, x_k)$ як керуючу функцію f^0 символічного обчислення C . Для поліномів f^{2i} , $i = 1, 2, \dots, t/2$, які є кольорами точок з $DS(k, K[x_1, x_2, \dots, x_k])$, розглянемо їх максимальний ступінь d_e . Нехай d_o - максимальний ступінь f^{2i+1} , $i = 1, 2, \dots, t/2$. Зауважимо, що ступінь поліноміального відображення $m(C)$ обмежена зверху $d_e + d_o$. Насправді ступінь цього відображення - це максимум добутків координат f^i та f^{i+1} , $i = 1, 2, \dots, t-1$.

Давайте розглянемо сукупність $S^{rs}(PL)$ відображень $m(C)$ для символічних обчислень, де d_e дорівнює не більше r і не дорівнює не більше s .

Теорема 4.1. *Сукупність $S^{rs}(PL(k, K))$ є стабільною піднапівгрупою афінної напівгрупи Кремони $S(K^{k(k+1)})$ ступеня $r + s$.*

Зрозуміло, що перетин $G^{rs}(PL(k, K))$ з $G(PL)$ та $S^{rs}(PL(k, K))$ є стабільною підгрупою $C(K^{k(k+1)})$ ступеня $r + s$. Зверніть увагу, що $Ek(K)$, представлений у [7], збігається з $S^{11}(PL(k, K))$.

4.4. Про пари перетворень із проміжком щільності та відповідним відкритим ключем

Розглянемо точкове обчислення символічного автомата Шуберта з напівгрупи $S^{m1} (PL (n, K))$ з $m = d (n)$ виду $an = b$, $a > 1$, що відповідає символічному ключу $f^1, f^2, \dots, f^t$ для деякого парного параметра t з елементами f^i , i є непарним, лінійно зростаючого змінного n ступеня та скінченної щільності.

Тоді відповідне перетворення F буде мати ступінь $O (n)$ та лінійну щільність. Припустимо, що f^t – бієктивне відображення. Тоді, в більшості випадків, оберненевідображення F^{-1} , задане символічним ключем, утвореним елементами $f^{t-1} (f^t)$, $f^{t-2} (f^t)$, $\dots$, $f^1 (f^t)$, f^t , де f^{-t} є оберненим для f^t , буде щільністю $O (n^n)$. Отже, пара F, F^{-1} – пара з проміжком щільності.

Пропонується наступний алгоритм відкритого ключа. Аліса вибирає скінченне комутативне кільце K , ціле додатне число n та лінійний вираз $m = d(n)$. Вона працює з подвійним графом Шуберта $DS (n, K)$ та відповідним символічним автоматом. Аліса вибирає непарний параметр t та символічний ключ $f^1, f^2, \dots, f^t$ для зворотного елемента $S^{m1} (PL (n, K))$.

Вона генерує поліноміальне відображення F , що відповідає обчисленням, за допомогою обраного символічного ключа. Стандартну форму цього перетворення можна обчислити за допомогою елементарних операцій $O (n^4)$ (квадратичних за кількістю змінних).

Аліса вибирає бієктивне мономіальне перетворення T з $V = K^{n(n+1)}$, задане мономіальною матрицею розміром $n(n+1)$, помноженому на $n(n+1)$, із $n(n+1)$ ненульовими регулярними записами з K^* (кожен стовпець і кожен рядок містять рівно один ненульовий елемент). Вона приймає афінне бієктивне перетворення T' з V і утворює $G = TFT'$. Для побудови G Аліса повинна обчислити n^2 лінійних комбінацій поліноміального виразу n^2 багатовимірних багаточленів щільності та ступеня $O (n)$. Отже, загальна складність утворення G дорівнює $O (n^6)$ (кубічна за кількістю змінних).

Аліса посилає Бобу стандартну форму G . Зверніть увагу, що G має ступінь $O(n)$ і щільність $O(n^3)$. Боб пише свій відкритий текст p з V і обчислює зашифрований текст $c = G(p)$ у часі $O(n^4)$ (квадратичний час за кількістю змінних).

Процес розшифровки. Припустимо, що Аліса зберігає вже обчислене перетворення $T_1 = T^{-1}$ і $T_2 = T^{-1}$. По-перше, вона обчислює $T_1(c) = b$. Потрібні її елементарні операції $O(n^4)$.

Тепер вона має колір $t = (b_1, b_2, \dots, b_n)$ точки (b) . Аліса шукає проміжний вектор v , утворений координатами точки (v) такий, що $F(v) = c$. Нехай $(r) = (v_1, v_2, \dots, v_n)$ - колір точки (v) . Аліса має обернене f^{-t} бієктивного афінного відображення f^t . Отже, вона обчислює $(r) = f^{-t}(r)$ у часі $O(n^2)$. Тепер Аліса може обчислити значення $f^1, f^2, \dots, f^{t-1}$ на кортежі (r) . Це містить $O(n)$ операцій. Після цього вона обчислює v як кінцевий елемент прогулянки довжиною t з початковою точкою (b) та встановленими кольорами вершин. Це коштує Алісі $O(n^2)$ елементарних операцій. Нарешті, вона отримує відкритий текст через додток $T_2 = T^{-1}$ також у часі $O(n^2)$.

Інші ідеї використання алгебраїчних графів для побудови багатовимірних криптосистем можна знайти в [13-15].

4.5. Про Ейлерові перетворення та їх криптографічні додатки

Можна розглянути засоби шифрування з наступної підгрупи $ES_n(K)$ з $SF_n(K)$ формальних правил G виду:

$$\begin{aligned} x_1 &\rightarrow T_1(x_1, x_2, \dots, x_n), \\ x_2 &\rightarrow T_2(x_1, x_2, \dots, x_n), \quad (4.1) \end{aligned}$$

...

$$x_n \rightarrow T_n(x_1, x_2, \dots, x_n)$$

де T_i - одночлен з $K[x_1, x_2, \dots, x_n]$ з регулярним коефіцієнтом K^* . Таке перетворення зберігає $(K^*)^n$. Ми позначаємо так G як Ейлерову трансформацію. Нехай $EG_n(K)$ - сукупність елементів з $ES_n(K)$, які діють бієктивно на K^* .

Припустимо, що K скінченна і розглянемо кілька перетворень Жордана - Гауса $J_1, J_2, \dots, J_s$ з $EG_n(K)$, тобто перетворення роду

$$x_1 \rightarrow b_1 x_1^{a(1,1)}$$

$$x_2 \rightarrow b_2 x_1^{a(2,1)} x_2^{a(2,2)}$$

...

$$x_n \rightarrow b_n x_1^{a(n,1)} x_2^{a(n,2)} \dots x_n^{a(n,n)},$$

$$\text{де } a(i, j) \in \mathbb{Z}_m, m = |K^*|, (a(i, i), m) = 1.$$

Ми можемо вибрати $s + 1$ мономіальні афінні перетворення ${}^1T, {}^2T, \dots, {}^{s+1}T$ з $AGL_n(K)$ і використовувати

$$G = {}^1T J_1 {}^2T J_2 {}^3T J_3 \dots {}^sT J_s {}^{s+1}T \quad (4.2)$$

Помітно, що знання про декомпозицію (4.2) дозволяють знайти обернену до G за допомогою прямолінійних алгоритмів обчислення обернених J_i та jT .

Говоримо, що τ з виду (4.2) - це обчислювально приручений ейлерів елемент від $EG_n(K)$. Зрозуміло, що τ посиляє змінну x_i на певний одночлен. Розкладання на добуток перетворень Жордана - Гауса дозволяє нам знайти розв'язок рівнянь для x з $(K^*)^n$.

Позначимо ${}^nES(K)$ як Ейлерову напівгрупу формальної напівгрупи Кремони $SF_n(K)$. Припустимо, що порядок K постійний. Як впливає з визначення, обчислення значення елемента з ${}^nES(K)$ для даного елемента K^n оцінюється за

$O(n^2)$. Добуток двох мультиплікативних елементів Кремони можна обчислити за час $O(n^4)$.

Тут не обговорюємо складність обчислення оберненого для загального елемента $g \in {}^nEG(K)$ на машині Тюрінга або квантовому комп'ютері та проблему пошуку оберненого для приручених Ейлерових елементів.

Зауваження 3.2. Нехай G - підгрупа ${}^nEG(K)$, $K \in \{Z_m, F_q\}$, породжена елементами Жордана-Гауса $g_1, g_2, \dots, g_t$. Проблема пошуку слова розкладання $g \in G$ на продукт генератора g_i є складною, тобто поліноміальні алгоритми для її вирішення за допомогою машини Тюрінга або квантового комп'ютера невідомі. Якщо проблему зі словом вирішено, а обернена g_i обчислюється, то визначається обернена до g . Зверніть увагу, що якщо $n = 1$, $K = Z_m$, $m = pq$, де p і q є великими простими числами, а G породжується $g_1 = \mu g_1^a$, то проблема не вирішувана в машині Тюрінга, але її можна вирішити за допомогою квантового комп'ютера.

Тож Аліса може оголосити, що стандартна форма (4.1) з G є загальнодоступним правилом. Кореспонденти працюють із рівнинним простором $(K^*)^n$, який збігся з шифровим простором. Боб використовує G для шифрування. Аліса використовує свої знання щодо розкладання (4.2) для дешифрування.

Поліноміальний алгоритм інвертування G у вигляді (4.1) невідомий.

4.6. Про комбіновані відкриті ключі

Нагадаємо, що щільність елемента F із $SF_n(K)$, задана стандартною формою $x_i \rightarrow f_i(x_1, x_2, \dots, x_n)$, $i = 1, 2, \dots, n$, є загальним числом $den(F)$ одночленів у всіх многочленах f_i . Для досліджень $t(H) \in {}^nES(K)$ без обмеження загальності можна припустити, що $deg(H)$ дорівнює $O(n)$.

Розглянемо склад F елемента H з ${}^nEG(K)$ та елемента G з $SF_n(K)$ щільності $O(n^t)$ та ступеня $O(n^r)$, де t і r - деякі константи. Тоді F має однакову щільність з H та ступінь розміру $O(n^{r+1})$.

Припустимо, що обмеження G на $(K^*)^n$ є ін'єктивним. Зверніть увагу, що відображення $G' \in SF_n(K)$ таке, що GG' фіксує кожен x із $(K^*)^n$, може існувати, але мати не поліноміальну щільність.

Давайте розглянемо наступний тип багатовимірних відкритих ключів. Аліса вибирає $H \in {}^nEG(K)$ з відомим розкладанням виду (2) для цього відображення та G на $(K^*)^n$, як зазначено вище. Припустимо, що вона має алгоритм приватного ключа для обчислення розв'язку для $G(x) = b$, $b \in K^n$ за умови, що $x \in (K^*)^n$. Потім вона обчислює $F = HG$ у стандартній формі та надсилає його Бобу. Йому доводиться працювати з рівнинним простором $(K^*)^n$ та цифровим простором K^n . Тож Боб пише повідомлення $(p) = (p_1, p_2, \dots, p_n) \in (K^*)^n$, обчислює $c = F((p))$ і відправляє його Алісі.

Вона розв'язує $F(y) = c$ для $y \in (K^*)^n$. Нехай $y = (b)$, Аліса використовує свої знання з обраного розкладання H та обчислює відкритий текст як $H^{-1}(b)$. Ми позначаємо цю систему як G , яка базується на багатовимірному відкритому ключі в режимі Ейлера.

Зауваження 4.3. Аліса може взяти багатовимірне публічне правило кандидата ПКК зі списку конкурсу NIST 2019, який утворений бієктивним елементом $F \in SF_n(K)$ ступеня $O(n^r)$ та щільності $O(n^t)$ та алгоритмом приватного ключа для обчислення зображення з F (або раніше відомий вже розбитий багатовимірний кандидат, або потоковий шифр поліноміальної природи). Вона приймає $G = T_1 F T_2$ для деяких $T_1, T_2 \in AGL_n(K)$, $H \in {}^nEG(K)$ і формує G -криптосистему в режимі Ейлера.

Приклад 4.1. Аліса приймає криптосистему, описану в підрозділі 4.3. Оцінка складності процедур для Аліси та Боба рухається вперед.

Приклад 4.2. Насправді можна використовувати небієктивні перетворення K^n , які зберігають K^* , і діяти бієктивно на цей різновид.

Виявляється, що одна з недавньої родини потокових шифрів [49] має багатовимірну природу. Це може бути визначено у випадку довільного

скінченного комутативного кільця K . Основне нелінійне перетворення F з K^n створюється за допомогою графічної процедури, визначеної в термінах прогулянок за відомими регулярними алгебраїчними графами $D(n, K)$ та $A(n, K)$. З'ясовуємо, що F має обмежений ступінь, зберігає різноманітність $(K^*)^n$ та індукує бієктивну перестановку на цій множині.

Таким чином, можемо використовувати це сімейство F в режимі Ейлера та створити криптосистему з перетворенням шифрування ступеня $|K^*|^n$. Випадки булевих кілець $B(n)$ розміром 2^n , скінченних полів та арифметичних кілець Z_m лишків за модулем m цікаві для реалізації.

Перетворення F представлене у стандартній формі $x_i \rightarrow f_i(x_1, x_2, \dots, x_n)$, $i = 1, 2, \dots, n$ та поєднане з двома бієктивними афінними перетвореннями T_1, T_2 , утворюючи $G = T_1 F T_2$ (див. зауваження 4.3).

Розглянемо наступні три випадки. (1) T_1 і T_2 - тотожності, (2) T_1 і T_2 - перетворення типу $x_1 \rightarrow x_1 + a_2 x_2 + a_3 x_3 + \dots + a_n x_n, x_j \rightarrow x_j, j = 2, 3, \dots, n$ (3) $T_j, j = 1, 2$ - матриці з ненульовими записами.

Щільності перетворень шифрування представлені на рис. 4.1 нижче для 2-го випадку для графів $D(n, q)$.

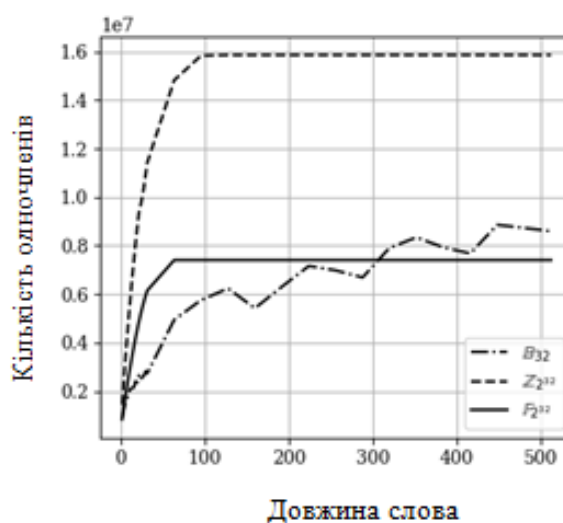


Рис.4.1 Кількість одночленів відображення лінійного ступеня, індукованих графом $(n=128)$ (граф $D(n,k)$, $K=B(32)$, $Z_{2^{32}}$, $F_{2^{32}}$), випадок II

Інші випадки (1) - (3) представлені нижче

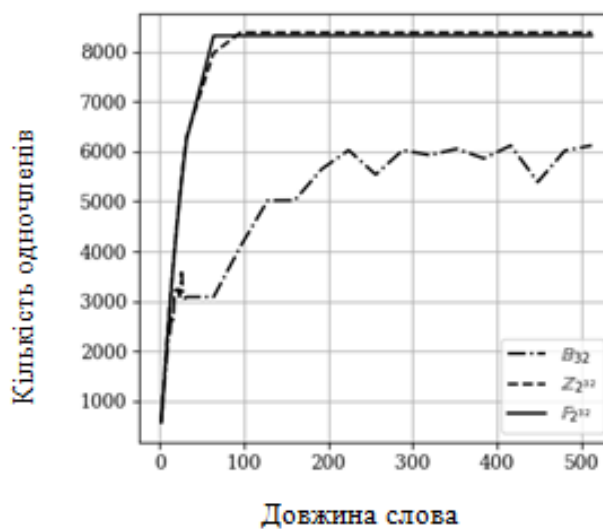


Рис.4.2 Кількість одночленів відображення лінійного ступеня, індукованих графом $(n=128)$ (граф $D(n,k)$, $K=B(32)$, $Z_{2^{32}}$, $F_{2^{32}}$), випадок I

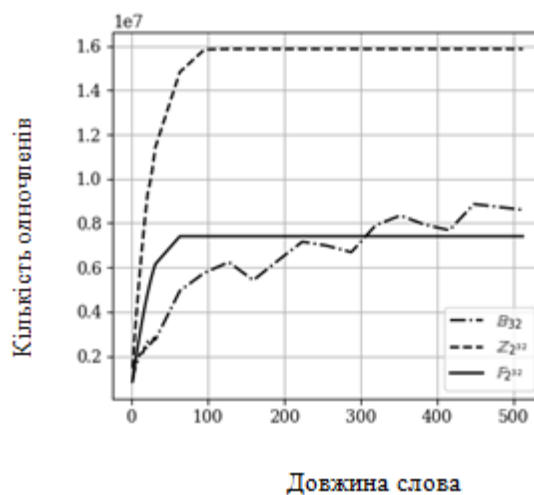


Рис.4.3 Кількість одночленів відображення лінійного ступеня, індукованих графом $(n=128)$ (граф $D(n,k)$, $K=B(32)$, $Z_{2^{32}}$, $F_{2^{32}}$), випадок II

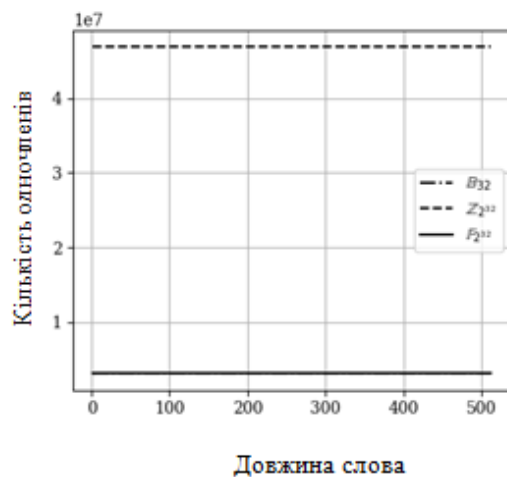


Рис.4.4 Кількість одночленів відображення лінійного ступеня, індукованих графом $(n=128)$ (граф $D(n,k)$, $K=B(32)$, $Z_{2^{32}}$, $F_{2^{32}}$), випадок III

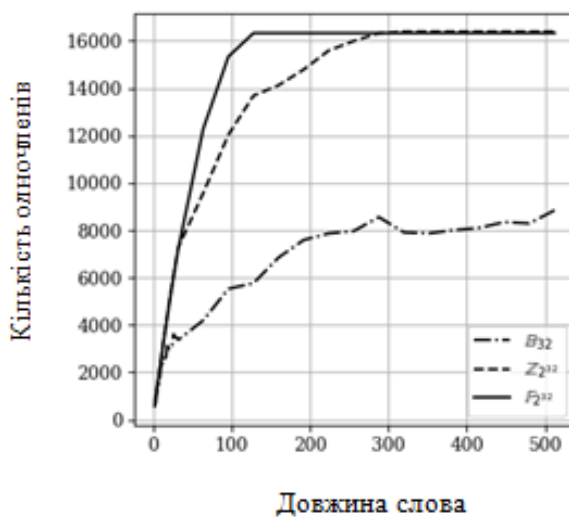


Рис.4.5 Кількість одночленів відображення лінійного ступеня, індукованих графом $(n=128)$ (граф $A(n,k)$, $K=B(32)$, $Z_{2^{32}}$, $F_{2^{32}}$), випадок I

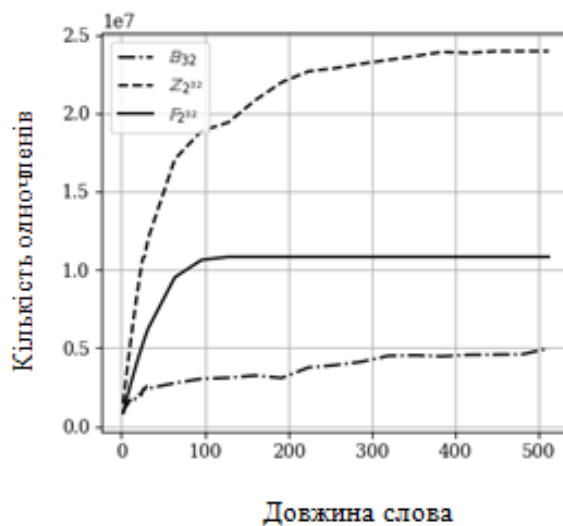


Рис.4.6 Кількість одночленів відображення лінійного ступеня, індукованих графом $(n=128)$ (граф $A(n,k)$, $K=B(32)$, $Z_{2^{32}}$, $F_{2^{32}}$), випадок II

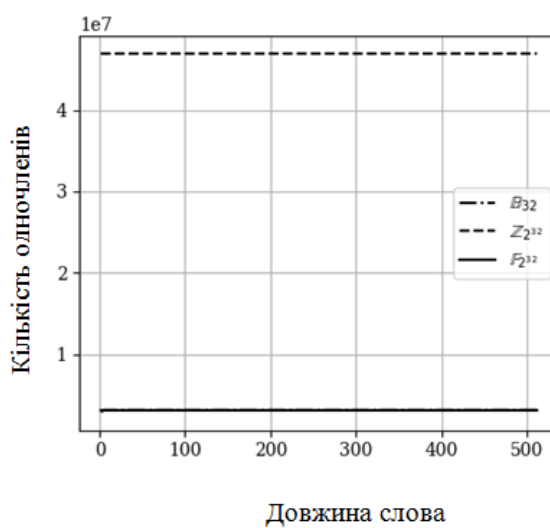


Рис.4.7 Кількість одночленів відображення лінійного ступеня, індукованих графом $(n=128)$ (граф $A(n,k)$, $K=B(32)$, $Z_{2^{32}}$, $F_{2^{32}}$), випадок III

n	Довжина прогулянки				
	16	32	64	128	256
16	145	145	145	145	145
32	544	545	545	545	545
64	1584	2112	2113	2113	2113
128	3664	6240	8320	8321	8321

Таблиця 4.1 Щільність відображення лінійного ступеня, індукованих графом $D(n, F_{2^{32}})$, випадок I

n	Довжина прогулянки				
	16	32	64	128	256
16	3649	3649	3649	3649	3649
32	41355	41356	41356	41356	41356
64	440147	529052	529053	529053	529053
128	3823600	6149213	7405944	7405945	7405945

Таблиця 4.2 Щільність відображення лінійного ступеня, індукованих графом $D(n, F_{2^{32}})$, випадок II

n	Довжина прогулянки				
	16	32	64	128	256
16	6544	6544	6544	6544	6544
32	50720	50720	50720	50720	50720
64	399424	399424	399424	399424	399424
128	3170432	3170432	3170432	3170432	3170432

Таблиця 4.3 Щільність відображення лінійного ступеня, індукованих графом $D(n, F_{2^{32}})$, випадок III

n	Довжина прогулянки				
	16	32	64	128	256
16	250	250	250	250	250
32	770	1010	1010	1010	1010
64	1810	3074	4066	4066	4066
128	3890	7202	12290	16322	16322

Таблиця 4.4 Щільність відображення лінійного ступеня, індукованих графом $A(n, F_{2^{32}})$, випадок I

n	Довжина прогулянки				
	16	32	64	128	256
16	5623	5623	5623	5623	5623
32	53581	62252	62252	62252	62252
64	454375	680750	781087	781087	781087
128	3607741	6237144	9519921	10826616	10826616

Таблиця 4.5 Щільність відображення лінійного ступеня, індукованих графом $A(n, F_{2^{32}})$, випадок II

n	Довжина прогулянки				
	16	32	64	128	256
16	6544	6544	6544	6544	6544
32	50720	50720	50720	50720	50720
64	463542	463542	463542	463542	463542
128	3896521	3896521	3896521	3896521	3896521

Таблиця 4.6 Щільність відображення лінійного ступеня, індукованих графом $A(n, F_{2^{32}})$, випадок III

Щільність залежить від тривалості прогулянки по вершинах основних графів ($A(n, K)$ і $D(n, K)$). Помітний ефект фазового переходу стабілізації щільності зі збільшенням довжини прогулянки.

Результати отримані за допомогою комп'ютерного моделювання. Примітно, що числа одночленних членів многочлена не залежать від вибору комп'ютера. Було використано звичайний ПК для проведення комп'ютерних експериментів.

Висновки до четвертого розділу

Запропоновано алгоритм генерації стійких груп G бієктивних поліноміальних відображень $f(n)$ n -вимірного афінного простору над комутативним кільцем K , тобто групи елементів обмеженого ступеня. Усі відображення наведені в стандартній формі, в якій враховуються ступені та щільності. Метод дозволяє генерувати перетворення $f(n)$ лінійної щільності зі ступенем, заданим заданою лінійною функцією $d(n)$, з експоненціальною щільністю для $f(n)^{-1}$. У випадку $K = F_q$ можна вибрати $f(n)$ експоненціального порядку.

Запропоновано схему генерації відкритого ключа $f(n)$ криптографії від багатьох змінних виду $g(n) = T_1 f(n) T_2$, де T_1 – мономіальне лінійне перетворення K^n і ступінь T_2 – одна із запропонованих. Оцінки складності показують, що час виконання правила шифрування з високим ступенем збігається з часом обчислення значення квадратного багатовимірного відображення. Процедура дешифрування на основі знань алгоритму генерації ще швидша. Захист спирається на ідею удачі ресурсів для противника відновити зворотне відображення експоненціальної щільності та лінійного ступеня та відсутність відомих загальних поліноміальних алгоритмів для вирішення цієї задачі.

Було поєднано Ейлерову трансформацію, яка посиляє кожен змінну в одночлен із запропонованим багатовимірним кільцем, щоб побудувати ще один відкритий ключ небієктивної природи, який використовує рівнинний простір $(K^*)^n$.

Список джерел, використаних у четвертому розділі

1. Machi, A. (2012). *AlgebraforSymbolicComputation*. Springer.
2. Ding, J., J. E. Gower, J. E. & Schmidt, D. S. (2006). *MultivariatePublicKeyCryptosystems*. *AdvancesinInformationSecurity*, V. 25. Springer.
3. Goubin, L., Patarin, J., YangBoYin.(2011). *MultivariateCryptography*. *InEncyclopediaofCryptographyandSecurity*. 2nd Ed. (pp. 824-828). Springer.
4. Ustimenko, V (2017). On the families of stable transformations of large or derane their cryptographical applications. *TatraMt. Math. Publ.*, 70, pp. 107-117.
5. Ustimenko V. (2015). On Schubert cells in grass manian sandnew algorithm of multivariate cryptography. *Tr. Inst. Mat.*, 23, No. 2, pp 137-148.
6. Ustimenko, V. A. (1998). On the varieties of parabolic subgroups, their generalizations and combinatorial applications. *ActaAppl. Math.*, 52, pp. 223-238.
7. Ustimenko, V. (2017). On desynchronised multivariate El Gamal algorithm. *Retrievedfrom*[https:// eprint.iacr.org/2017/712.pdf](https://eprint.iacr.org/2017/712.pdf)
8. Cossidente A. & deRessmine M. J. (2004). Remarkson Singer Cycle Groups and their Normalizers. *DesignsCodesCryptogr.*, 32, pp. 97-102.
9. Kantor W. (1982), Linear groups containing a Singer cycle. *J. Algebra*, 62, pp. 232-234.
10. Ustimenko, V. (2015). On algebraic graph theory and non–bijective maps in cryptography. *Algebra Discrete Math.*, 20, No 1, pp. 152–170.
11. Ustimenko, V. (2017). On new multivariate cryptosystems with nonlinearity gap. *Algebra and Discrete Math.*, 23, No 2, pp. 331–348.
12. Ustimenko, V. (2017). On new multivariate cryptosystems based on hidden Eulerian equations, *Dopov.Nac. Akad.nauk Ukr.*, No. 5, pp. 17-24. doi:<https://doi.org/10.15407/dopovidi2017.05.017>

13. Romańczuk-Polubiec, U. & Ustimenko, V. (2015). On two windows multivariate cryptosystem depending on random parameters// Algebra and Discrete Math., 19, No. 1, pp. 101-129.

14. Ustimenko V. & Romańczuk, U. (2013). On dynamical systems of large girth or cycle indicator and their applications to multivariate cryptography. In Artificial Intelligence, Evolutionary Computing and Metaheuristics (pp. 257-285). Berlin: Springer.

15. Polak, M., Romańczuk, U., Ustimenko, V. & V. Wróblewska, A. (2013). On the applications of extremal graph theory to coding theory and cryptography. Electron. Notes Discrete Math., 43, pp. 329-342.

16. N. Koblitz, Algebraic aspects of cryptography, Springer (1998)., 206 P.

17. Patarin J., The Oil and Vinegar digital signatures, Dagstuhl Workshop on Cryptography, 1997.

18. Kipnis A., Shamir A., Cryptanalysis of the Oil and Vinegar Signature Scheme ,Advances in Cryptology- Crypto 96, Lecture Notes in Computer Science, Vol. 1462, 1996, pp 257-266.

19. Bulygin S., Petzoldt A. and Buchmann J., Towards provable security of the unbalanced oil and vinegar signature scheme under direct attacks, In Guang Gong and Kishan Chand Gupta, editors, "Progress in Cryptology - INDOCRYPT", Lecture notes in Computer Science, Vol. 6498, 2010. pp. 1732.

20. Post-Quantum Cryptography: Call for Proposals: <https://csrc.nist.gov/Project/Post-Quantum-Cryptography-Standardization/Call-for-Proposals>, Post-Quantum Cryptography: Round 2 Submissions.

21. M. Andrzejczak , The Low –Area FPGA Design for the Post – Quantum Cryptography Proposal Round 5, Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS), Cryptography and Security Systems, Leipzig, September, 2019.

22. D. N. Moldovyan, N. A. Moldovyan, A New Hard Problem over Non-commutative Finite Groups for Cryptographic Protocols, International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2010: Computer Network Security pp 183-194.
23. L. Sakalauskas., P. Tvarijonas , A. Raulynaitis, Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problema in Group Representation Level, INFORMATICA, 2007, vol. !8, No 1, 115-124.
24. V. Shpilrain, A. Ushakov, The conjugacy search problem in public key cryptography: unnecessary and insufficient, Applicable Algebra in Engineering, Communication and Computing, August 2006, Volume 17, Issue 3–4, pp 285–289.
25. Delaram Kahrobaei, Bilal Khan, A non-commutative generalization of ElGamal key exchange using polycyclic groups, In IEEE GLOBECOM 2006 - 2006 Global Telecommunications Conference [4150920] DOI: 10.1109/GLOCOM.2006.
26. Alexei Myasnikov; Vladimir Shpilrain; Alexander Ushakov (2008). Group-based Cryptography. Berlin: Birkhäuser Verlag.
27. Zhenfu Cao (2012). New Directions of Modern Cryptography. Boca Raton: CRC Press, Taylor & Francis Group. ISBN 978-1-4665-0140-9.
28. Benjamin Fine, et. al. "Aspects of Non abelian Group Based Cryptography: A Survey and Open Problems". arXiv:1103.4093.
29. Alexei G. Myasnikov; Vladimir Shpilrain; Alexander Ushakov (2011). Non-commutative Cryptography and Complexity of Group-theoretic Problems. American Mathematical Society.
30. Anshel, I., Anshel, M., Goldfeld, D.: An algebraic method for public-key cryptography. Math.Res.Lett. 6(3–4), 287–291 (1999).
31. Blackburn, S.R., Galbraith, S.D.: Cryptanalysis of two cryptosystems based on group actions. In: Advances in Cryptology—ASIACRYPT '99. Lecture Notes in Computer Science, vol. 1716, pp. 52–61. Springer, Berlin (1999).

32. C Ko, K.H., Lee, S.J., Cheon, J.H., Han, J.W., Kang, J.S., Park, C.: New public-key cryptosystem using braid groups. In: *Advances in Cryptology—CRYPTO 2000*, Santa Barbara, CA. *Lecture Notes in Computer Science*, vol. 1880, pp. 166–183. Springer, Berlin (2000)
33. Maze, G., Monico, C., Rosenthal, J.: Public key cryptography based on semigroup actions. *Adv.Math. Commun.* **1**(4), 489–507 (2007)
34. P.H. Kropholler, S.J. Pride, W.A.M. Othman K.B. Wong, P.C. Wong, Properties of certain semigroups and their potential as platforms for cryptosystems, *Semigroup Forum* (2010) 81: 172–186
35. J. A. Lopez Ramos, J. Rosenthal, D. Schipani, R. Schnyder, Group key management based on semigroup actions, *Journal of Algebra and its applications*, 2019, vol.16.
36. Gautam Kumar and HemrajSaini, Novel Noncommutative Cryptography Scheme Using Extra Special Group, *Security and Communication Networks*, Volume 2017, Article ID 9036382, 21 pages, <https://doi.org/10.1155/2017/9036382>
37. V. Ustimenko, Onsemigroups of multiplicative Cremona transformations and new solutions of Post Quantum Cryptography, *Cryptology ePrint Archive*, 133, 2019.
38. R. Wagner, M. R. Magyarik, A Public-Key Cryptosystem Based on the Word N Problem, *Advances in Cryptology, Proceedings of CRYPTO '84*, Santa Barbara, California, USA, August 19-22, 1984.
39. A. G. Myasnikov, A. Roman'kov, A linear decomposition attack, *Groups Complex. Cryptol.* **7**, No. 1 (2015), 81-94.
40. V. A. Roman'kov. Algebraic cryptography. Omsk State University, Omsk, 2013, 136 p..
41. V. A. Roman'kov, Cryptanalysis of some scheme supplying automorphisms. *Prikladnaya Discretnaya Matematika.* **3** (2013), 35-51.

42. V. A. Roman'kov, Essays in algebra and cryptology: Algebraic cryptanalysis. Omsk State University, Omsk, 2018, 207 p.
43. V. A. Roman'kov, A nonlinear decomposition attack, Groups Complex. Cryptol. 8, No. 2 (2016), 197-207.
44. V. Roman'kov, An improved version of the AAG cryptographic protocol, Groups, Complex., Cryptol, 11, No. 1 (2019), 35-42.
45. V. A. Roman'kov, Efficient methods of algebraic cryptanalysis and protection against them, Prikladnaya Discretnaya Matematika, Prilozhenie, 12 (2019), 117-125.
46. V. A. Roman'kov, Efficient methods of algebraic cryptanalysis and protection against them, Prikladnaya Discretnaya Matematika, Prilozhenie, 12 (2019), 117-125.
47. A. Ben-Zvi, A. Kalka and B. Tsaban, Cryptanalysis via algebraic span, In: Shacham H. and Boldyreva A. (eds.) Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part I, Vol. 10991, 255-274, Springer, Cham (2018).
48. B. Tsaban, Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography, J. Cryptol. 28, No. 3 (2015), 601-622.
49. V. Ustimenko, U. Romanczuk-Polubiec, A. Wroblewska, M. Polak, E. Zhupa, On the constructions of new symmetric ciphers based on non-bijective multivariate maps of prescribed degree, Security and Communication Networks, Volume 2019, Article ID 213756.
50. Max Noether, Luigi Cremona, Mathematische Annalen 59, 1904, p. 1-19.

РОЗДІЛ 5

ПРОТОКОЛИ ОБМІНУ КЛЮЧІВ НЕКОМУТАТИВНОЇ КРИПТОГРАФІЇ ВІД БАГАТЬОХ ЗМІННИХ ТА ЇХ ЗАСТОСУВАННЯ У ПОСТКВАНТОВИХ КРИПТОГРАФІЧНИХ АЛГОРИТМАХ

5.1. Про Постквантову криптографію, криптографію від багатьох змінних та некомутативну криптографію

Постквантова криптографія (ПКК) - це відповідь на загрозу, що надходить від повномасштабного квантового комп'ютера, здатного виконати алгоритм Шора. За допомогою цього алгоритму, реалізованого на квантовому комп'ютері, використовувані в даний час схеми відкритих ключів, такі як RSA та криптосистеми еліптичної кривої, більше не захищені. Американський NIST зробив крок до зменшення ризику квантових атак, оголосивши процес стандартизації ПКК [1] для нового алгоритму відкритого ключа. У березні 2019 року NIST опублікував список кандидатів, які потрапили до другого туру процесу стандартизації. Декілька публічних ключів кандидатів імплементовано, наприклад, кандидат під назвою Раунд 5 [2] або класичний алгоритм Мака Еліса [3].

Поточні кандидати розробляються в наступних напрямках ПКК: решітчасті системи, криптосистеми на основі коду, криптографія від багатьох змінних [4], криптографія на основі хешу, дослідження ізогеній для супереліптичних кривих. Існує наступний альтернативний підхід до криптографії з відкритим ключем. Замість загальнодоступного правила шифрування кореспонденти можуть використовувати протокол для опрацювання деякої загальної інформації, яка дозволяє визначити правило шифрування для одного користувача та інструмент дешифрування для його/її партнера. Назвемо такі алгоритми криптосистемою типу Ель-Гамаль. Нагадаємо, що Ель Гамаль запропонував таку криптосистему на основі класичного алгоритму Діффі-Хеллмана над мультиплікативною групою F_p^* .

Розроблені нові криптосистеми в рамках альтернативного підходу ([5-9]) для багатofакторної криптографії з відкритим ключем на основі ідеї модифікованого Діффі-Хеллмана протоколи типу з точки зору некомутативної криптографії для підгруп ендоморфізмів $K[x_1, x_2, \dots, x_n]$. Безпека цих алгоритмів залежить від складності проблеми слова для розкладання заданої багатовимірної відображення на генератори афінної напівгрупи Кремона $End(K[x_1, x_2, \dots, x_n])$ [10]

Нагадаємо, що криптографія від багатьох змінних [4] використовує поліноміальні відображення афінного простору K^n , визначеного над скінченним комутативним кільцем K в себе як інструменти шифрування. Він використовує складність пошуку розв'язання системи нелінійних рівнянь від багатьох змінних. Криптографія від багатьох змінних використовує як інструменти шифрування нелінійні поліноміальні перетворення виду $x_1 \rightarrow f_1(x_1, x_2, \dots, x_n)$, $x_2 \rightarrow f_2(x_1, x_2, \dots, x_n)$, ..., $x_n \rightarrow f_n(x_1, x_2, \dots, x_n)$ перетворюючи афінний простір K^n , де $f_i \in K[x_1, x_2, \dots, x_n]$, $i = 1, 2, \dots, n$ - багатовимірні многочлени, як правило, задані у стандартній формі, тобто через список одночленів у вибраному порядку (нелінійні ендоморфізми $K[x_1, x_2, \dots, x_n]$).

Некомутативна криптографія є активною областю криптології, де криптографічні примітиви та системи базуються на алгебраїчних структурах, таких як групи, напівгрупи та некомутативні кільця [11 - 25]. Важливо, щоб цей напрямок добре підтримувався криптоаналітичними дослідженнями [26-29]. Напівгрупи базуються на криптографії, яка складається із загальних криптографічних схем, визначених у термінах широких класів напівгруп та їх реалізації для вибраних сімейств напівгруп (так званих платформ напівгруп).

Статті [5-9] містять деякі модифікації протоколу Діффі-Хеллмана, коли G задано як підгрупу афінної напівгрупи Кремона $S(K^n)$ над скінченним комутативним кільцем K усіх поліномів перетворення. У цих статтях використовується припущення, що кожен елемент подається у своїй стандартній формі багатовимірної криптографії. Для використання операції напівгрупи

потрібно обчислити склад перетворень. Це була спроба поєднати методи некомутативної криптографії та криптографії від багатьох змінних.

У статті [5, 6] пропонується деяке використання гомоморфізмів піднапівгруп афінних груп Кремони для протоколів та криптосистем, які не є узагальненнями алгоритму Діффі-Хеллмана та його модифікацій типу Ель-Гамала. Деякі приклади наводяться там. Реалізації цих схем з оцінкою щільності перетворених поліноміальних перетворень описані в [7-9]. Елементи стабільних підгруп на основі графів, використані в [7], можуть служити інструментами шифрування поточкових шифрів. [30]

5.2. Про стабільні підгрупи формальної групи Кремони та приватизацію багатовимірних публічних ключів на основі відображень обмеженого ступеня

Нехай $K[x_1, x_2, \dots, x_n]$ є комутативним кільцем усіх поліномів змінних $x_1, x_2, \dots, x_n$, визначеними над комутативним кільцем K . Кожен ендоморфізм $F \in E_n(K)$ однозначно визначається своїми значеннями на формальних утворювачах x_i , $i = 1, 2, \dots, n$. Символ $\text{End}(K[x_1, x_2, \dots, x_n]) = E_n(K)$ означає напівгрупу всіх ендоморфізмів $K[x_1, x_2, \dots, x_n]$. Тож ми можемо ідентифікувати F з формальним правилом $x_1 \rightarrow f_1(x_1, x_2, \dots, x_n), x_2 \rightarrow f_2(x_1, x_2, \dots, x_n), \dots, x_n \rightarrow f_n(x_1, x_2, \dots, x_n)$ де $f_i \in K[x_1, x_2, \dots, x_n]$. Елемент F , природно, індукує перетворення $\Delta(F)$ афінного простору K^n , задане наступним правилом $\Delta(F): (\alpha_1, \alpha_2, \dots, \alpha_n) \rightarrow (f_1(\alpha_1, \alpha_2, \dots, \alpha_n), f_2(\alpha_1, \alpha_2, \dots, \alpha_n), \dots, f_n(\alpha_1, \alpha_2, \dots, \alpha_n))$ для кожного $(\alpha_1, \alpha_2, \dots, \alpha_n) \in K^n$. Луїджі Кремона [31] ввів $\Delta(E_n(K)) = CS(K^n)$, який в даний час називають афінною напівгрупою Кремони. Група всіх обернених перетворень $CS(K^n)$ з інверсією до $CS(K^n)$ відома як афінна група Кремони $CG(K^n)$ (скорочено група Кремони [32, 33]).

Позначимо нескінченну $E_n(K)$ як формальну афінну напівгрупу Кремони. Щільність відображення F - це загальна кількість одночленів у всіх f_i .

Відомо, що зазвичай ступінь ітерації «випадкового» багатовимірної поліноміального перетворення зростає в геометричній прогресії. Це пов'язано з

тим, що склад двох «випадкових» елементів $CS(K^n)$ ступеня d у більшості випадків матиме ступінь d^2 .

Зокрема, це можна побачити в одновимірному випадку (тобто при $n = 1$) експоненціального зростання ступеня ітерацій нелінійного многочлена неминуче. Однак виявляється, що при $n > 1$ ступінь деяких спеціальних перетворень може зростати значно повільніше. Є відкриті приклади перетворень із ступенем, який може зростати поліноміально [34, 35]) або бути навіть не більшою за деяку встановлену константу d . Останній факт означає існування стабільних піднапівгруп/підгруп формальних груп Кремона ступеня d , тобто підгруп ендоморфізмів ступеня щонайменше d . Перший приклад сімей стабільних груп був представлений у [36, 37] з точки зору добре відомих екстремальних графів $D(n, q)$ та їх аналогів $D(n, K)$, визначених над довільним комутативним кільцем K . Однак важливість їхньої стабільності була реалізована пізніше [38, 39]. Формальне доведення того, що ці групи є стабільними ступеня 3, представлено в [40]. Очевидно, напівгрупа перетворень ступеня 1 та загальна афінна група бієктивних перетворень ступеня 1 є прикладами стабільних підгруп та підгруп $E_n(K)$ ступеня 1. В даний час нелінійні сімейства стійких напівгруп та груп відомі для кожного параметра $d \geq 2$, вони мають різні програми для криптографії [8, 9, 41]. Усі ці результати отримані в результаті досліджень «символічних прогулянок» на алгебраїчних графах, тобто графах, визначених системою алгебраїчних рівнянь. Наступне твердження випливає з результатів [8].

Теорема 5.1. *Для кожного натурального числа $n > 1$ і кожного комутативного кільця K і $d \geq 2$ існує сімейство некомутативних стійких підгруп $G_n(K) < E_n(K)$ ступеня d і стабільні напівгрупи $S_n(K) < E_n(K)$ ступеня d такі, що $G_n(K) < S_n(K)$.*

Нехай ${}^iZ = \{{}^ig_1, {}^ig_2, \dots, {}^ig_t\}$ - послідовність наборів елементів із $E_{n(i)}(K)$, де $n(i) > 1$ - зростаюча послідовність натуральних чисел. Кажемо, що iZ є некомутативною системою стабільних генераторів Кремони ступеня d і рангу t , якщо

(1) $\Delta (^i g_k {}^i g_j) \neq \Delta (^i g_j {}^i g_k)$ для довільного $k \neq j$.

(2) ${}^i SZ = \langle {}^i g_1, {}^i g_2, \dots, {}^i g_t \rangle$ є стабільними напівгрупами ступеня d .

Твердження 5. 1. Для кожного комутативного кільця K , послідовності $n(i) = i$, $i \geq 2$ і кожного значення параметрів d і t існує некомутативна система стабільних генераторів Крeмони ступеня d і рангу t .

Кажуть, що ${}^i Z$ - звичайна некомутативна система стабільних генераторів Крeмона, якщо $n(i) = i$ для кожного значення i .

Нехай $n(i)$, $m(i)$, $m(i) \leq n(i)$ - дві зростаючі послідовності природних чисел та ${}^i Z$, ${}^i Z^1$ - відповідні стабільні системи періодів зростання ступенів d і $d' (d' \leq d)$ і рангів t , $t > 1$.

Кажуть, що ${}^i Z' = \{{}^i g'_1, {}^i g'_2, \dots, {}^i g'_t\}$ є часткою стабільної системи Крeмони ${}^i Z$, якщо правило $\varphi (^i g_j) = {}^i g'_j$, $j = 1, 2, \dots, t$ визначає обчислювально приручений гомоморфізм напівгрупи ${}^i SZ$ на ${}^i SZ^1$, тобто гомоморфізм, обчислюваний у часі $O(ni^\alpha)$ для деякої додатної константи α . Називаємо ${}^i Z$ стабільним покриттям некомутативної системи стабільних генераторів Крeмона.

Як випливає з результатів [41], наведене нижче твердження справедливо.

Теорема 5.2. Для кожного скінченного комутативного кільця K і натуральних чисел d , $d > 0$ і t , $t \geq 2$ існує зростаюча послідовність $n(i)$ натуральних чисел і некомутативна система стабільних генераторів Крeмони ${}^i Z = \{{}^i g_1, {}^i g_2, \dots, {}^i g_t\}$ ступеня d і рангу t який має регулярний коефіцієнт ${}^i Z'$.

Кажуть, що стабільна система Крeмони ступеня d елементів має огинаюче сімейство стабільних піднапівгруп $EZ^i(K)$ ступеня d , якщо $E_{(i)}(K) > EZ^i(K) > SZ^i(K)$.

5. 3 Багатовимірний протокол Тахоми для стабільних генераторів Крeмони та його використання для багатовимірних алгоритмів шифрування

Слово тахома позначає тут аббревіатуру «приручений гомоморфізм». Заслугує на увагу те, що Тахома - назва гір у Північній Америці і популярна сукупість в обробці тексту.

Припустимо, що Аліса вибирає некомутативну систему $Z(K)$ стабільних генераторів Кремони ступеня d і рангу t з часткою $Z'(K)$ таку, що існує сімейство обгорт $EZ(K)$ із $Z(K)$ і сімейство обгорт $EZ^1(K)$ із $Z'(K)$.

Аліса вибирає параметр i та бієктивне афінне перетворення T , $\deg(T) = 1$ і T' , $\deg(T') = 1$, діючи на $(K)^{n(i)}$ та $(K)^{m(i)}$. Вона вибирає елементи E та E^1 з $EZ_{n(i)}(K)$ та $EZ'_{m(i)}(K)$. Аліса бере генератори $g_1, g_2, \dots, g_t$ із $SZ_i(K)$ та відповідні зображення $g'_1, g'_2, \dots, g'_t$ у $SZ'_i(K)$.

Отже, вона утворює $a_j = TEg_jE^{-1}T^{-1}$, $j = 1, 2, \dots, t$ і $b_j = T'E'g'_j(E')^{-1}(T')^{-1}$, $j = 1, 2, \dots, t$ записано у стандартній формі $E_{n(i)}(K)$ та $E_{m(i)}(K)$.

Аліса посилає (a_j, b_j) і $j = 1, 2, \dots, t$ Бобу. Він бере алфавіт $\{z_1, z_2, \dots, z_t\}$ і вибирає слово $w(z_1, z_2, \dots, z_t) = z_{i(1)}^{\alpha(1)} z_{i(2)}^{\alpha(2)} \dots z_{i(l)}^{\alpha(l)}$, де $\alpha(j) > 0$, $j = 1, 2, \dots, l$, $l > 1$, і $i(s) \in \{1, 2, \dots, t\}$, і $i(j) \neq i(j+1)$ для $j = 1, 2, \dots, t-1$.

Боб обчислює $b = w(b_1, b_2, \dots, b_t)$ і зберігає це в безпеці для себе. Він утворює $a = w(a_1, a_2, \dots, a_t)$ і відправляє цей елемент $E_{n(i)}(K)$ Алісі.

Вона використовує наступний процес відновлення, щоб отримати $w(b_1, b_2, \dots, b_t)$. Аліса обчислює $E^{-1}T^{-1}aTE = c$. Вона використовує приручений гомоморфізм φ , що відповідає некомутативній системі Z та її коефіцієнту Z^1 , і обчислює $\varphi(c) = c'$. По-друге, вона обчислює $b = w(b_1, b_2, \dots, b_t)$ як $T'E'c^1(E')^{-1}(T')^{-1}$.

Зауваження 5.1. Супротивник повинен розкласти доступне багатовимірне відображення $a = w(a_1, a_2)$ з $E_{n(i)}$ на слово в заданих генераторах $a_1, a_2, \dots, a_t$ при написанні в їхній стандартній формі. Тож безпека спирається на слово проблеми в напівгрупі $E_{n(i)}(K)$ (або стабільна напівгрупа $\langle a_1, a_2, \dots, a_t \rangle$).

Примітно, що завдяки цьому алгоритму кореспонденти Аліса та Боб можуть безпечно розробити колізію квадратичного перетворення $(K)^m(i)$ з обраною розмірністю $m(i)$. У разі регулярного фактора $m(i) = i$.

Отже, кореспонденти мають алгоритм для складання безпечно стабільного відображення зіткнень вибраного ступеня d , що діє на вільний модуль K^l довільно вибраного виміру. Цей варіант піднімає наступне питання.

Чи нам потрібний багатовимірний публічний ключ?

Одним із напрямків досліджень безпеки є класична криптографія від багатьох змінних [42, 43], які представляють приклади старих публічних ключів у вигляді сімейства квадратних елементів nF з $E_n(F_q)$, що індукує бієктивне відображення $\Delta({}^nF)$. Відображення nF подано публічно.

Отже, кожен публічний користувач (і супротивник також) може створити стільки пар $(x, y = \Delta({}^nF)(x))$, де x - обраний відкритий текст із просторового простору F_q^n і отримати відповідний зашифрований текст y як він/вона хоче.

Таким чином, завдяки вищезазначеному протоколу немає необхідності подавати F публічно. Аліса може обрати якусь сім'ю, яка є поточним або минулим (вже зламаним) кандидатом, до безпечного публічного ключа. Отже, у неї є приватний алгоритм розв'язування рівняння $F(x) = b$.

Вона може деформувати nF бієктивними елементами 1T_n і 2T_n від $AGL_n(F_q)$ для використання елементів $G_n = {}^1T_n {}^nF {}^2T_n$. По-друге, Аліса та Боб виконують багатовимірний протокол тахоми для розробки загального елемента $B_n(x)$ із $E_n(F_q)$.

Будемо вважати, що G_n і B_n задані у вигляді кортежів $(g_1, g_2, \dots, g_n)$ та $(b_1, b_2, \dots, b_n)$, де g_i та b_i - елементи F_q $[x_1, x_2, \dots, x_n]$. Нарешті Аліса посилає $(g_1 + b_1, g_2 + b_2, \dots, g_n + b_n)$ Бобу. Він використовує свої знання щодо $B(x)$ та загальновідоме правило додавання для відновлення $G(x)$. Отже, Боб використовує

$G(x)$ як функцію шифрування. Аліса використовує свій приватний алгоритм пошуку повторного зображення $F(x)$ для дешифрування.

Висновок 5.1. Не потрібно давати багатовимірне правило $F(x)$ обмеженого ступеня для публічної аудиторії. Існує безпечний спосіб перенести правило до свого партнера.

Наступне питання: Як довго кореспонденти можуть тримати G в приватному режимі?

Зауваження 5.2. Припустимо, що кореспонденти використовують багатовимірний стабільний протокол, а Аліса безпечно транспортує квадратичне багатовимірне відображення шифрування G на F_q^n (або перетворення постійного ступеня d).

Боб надсилає Алісі кілька елементів типу $G(p_i)$, $i = 1, 2, \dots, l$ через відкритий канал під час їх спілкування.

Якщо параметр l «достатньо великий» ($l = O(n^2)$ для $d = 2$), то супротивник може скористатися його інструментами кібертероризму і перехопить кілька пар (p_i, c_i) , де p_i є відкритим текстом, а c_i - відповідним зашифрованим текстом. Якщо він/вона перехоплює такі пари $O(n^2)$, то він може наблизити G за допомогою поліноміального алгоритму (метод криптоаналітичної лінеаризації), який вимагає елементарної роботи $O(n^5)$ при $d = 2$.

Така діяльність дозволяє супротивнику стати в одному положенні з користувачем Бобом. Він отримує G із приватного сховища кореспондентів. Подібно до випадку, коли противник публічного правила може обчислити $G(p)$ для будь-якого вибраного p .

Звичайно, супротивник також повинен порушити «публічне правило» G , тобто з'ясувати спосіб обчислення його зображення.

Аліса та Боб можуть бути достатньо розумними, щоб використовувати параметр обмеження l (кількість повідомлень) за допомогою деякого виразу $C(n)$, такий що $C(n) \leq \text{den}(G) / (2n)$ (половина середньої щільності zG_i , $i = 1, 2, \dots, n$).

В кінці інтервалу довіри Аліса може вибрати інші кон'югати генераторів системи Зінгера, кореспонденти проводять новий сеанс протоколу. Аліса безпечно пропонує нове правило квадратичного шифрування для Боба.

Висновок 5.2. *Після транспортування багатовимірної правила шифрування $F(x)$ до свого партнера існує можливість періодичного його модифікації. Ця схема дозволяє приватизувати багатовимірні публічні правила, тобто. перехід правила в некомутативну криптосистему типу *El Gamal*, яка використовує протоколи некомутативної криптографії, які приховують алгоритм шифрування від супротивника.*

Практичні аспекти: Замість квазіпублічних правил Аліса може створити обернене квадратичне багатовимірне відображення G щільності $O(n)$ (щільність - це число одночленів у всіх G_i , $i = 1, 2, \dots, n$), що дозволяє обчислити її зображення для $O(n)$ елементарних кроків. Зверніть увагу, що $O(n)$ - це швидкість зчитування рядка з M^n , де M обраний скінченний алфавіт.

Деякі з представлених криптографічних схем приватизації вже реалізовані на рівні прототипів моделей [7, 9]).

5.4. Про алгоритми багатовимірних цифрових підписів та схему їх приватизації

Загальновизнано, що криптографія від багатьох змінних виявилася більш успішною як підхід до побудови схем підписів насамперед тому, що багатовимірні схеми забезпечують найкоротший підпис серед постквантових алгоритмів. Такі підписи використовують систему нелінійних поліноміальних рівнянь

$${}^1p(x_1, x_2, \dots, x_n) = {}^1p_{i,j} \cdot x_i x_j + {}^1p_i \cdot x_i + {}^1p_0$$

$${}^2p(x_1, x_2, \dots, x_n) = {}^2p_{i,j} \cdot x_i x_j + {}^2p_i \cdot x_i + {}^2p_0$$

...

$${}^mp(x_1, x_2, \dots, x_n) = {}^mp_{i,j} \cdot x_i x_j + {}^mp_i \cdot x_i + {}^mp_0,$$

де ${}^kp_{i,j}$, kp_i - елементи вибраного комутативного кільця K .

Квадратичне багатовимірне криптографічне відображення складається з двох бієктивних афінних перетворень, S і T розмірностей n і m , та квадратичний елемент P виду $x_i \rightarrow {}^ip$ формальної групи Кремони, де ip записані над елементами $K[x_1, x_2, \dots, x_n]$. Позначаємо через $\Delta(P^{-1})(y)$ деяке перетворення $= \Delta(P(x))$. Потрійний $\Delta(S)^{-1}$, $\Delta(P)^{-1}$, $\Delta(T)^{-1}$ - це приватний ключ q , також відомий як люк.

Відкритим ключем є композиція S , P і T , яку, за припущенням, важко інвертувати без відома люка. Підписи генеруються з використанням приватного ключа та перевіряються за допомогою відкритого ключа наступним чином. Повідомлення передається до вектора y за допомогою відомої хеш-функції. Підпис $\Delta(T)^{-1}(\Delta(P)^{-1}(\Delta(S)^{-1}(y)))$. Одержувач підписаного документа повинен мати у своєму розпорядженні відкритий ключ P . Він обчислює хеш y і перевіряє, чи підпис x відповідає $\Delta(P)(y) = x$.

Приклад 5.1. Припустимо, що у нас є дві групи змінних $z_1, z_2, \dots, z_r$ та $z'_1, z'_2, \dots, z'_{n-r}$ такі, що підстановка $x_1 = z_1, x_2 = z_2, \dots, x_r = z_r, x_{r+1} = z'_1, x_{r+2} = z'_2, \dots, x_n = z'_{n-r}$ перетворює кожен окремий елемент ip у вираз вигляду $\sum \gamma_{ijk} z_j z'_k + \sum \lambda_{ijk} z'_j z'_k + \sum \zeta_{ij} z_j + \sum \zeta'_{ij} z'_j + \sigma_i$. У цій ситуації ми повинні підписати дане повідомлення y , і результатом буде дійсний підпис x . Коефіцієнти, γ_{ijk} , λ_{ijk} , ζ_{ij} , ζ'_{ij} і σ_i повинні бути обрані таємно. Змінні оцту z'_i вибираються випадковим чином (або псевдовипадково). Отримані лінійні рівняння системи розв'язуються для змінних олії z_i .

Описана вище схема незбалансованої олії та оцту (UOV) - це модифікована версія схеми олії та оцту, розроблена Дж. Патаріном. Обидва протоколи

цифрового підпису. Вони є алгоритмами криптографії від багатьох змінних. Безпека цієї схеми підписів базується на математичній проблемі з жорстким NP. Для створення та перевірки підписів повинна бути вирішена система мінімальних квадратних рівнянь. Вирішення m рівнянь з n змінними є важким для NP. Хоча проблема проста, якщо m або по суті більший, або по суті менший за n , [1] що важливо для криптографічних цілей, вважається, що проблема є складною в середньому випадку, коли m і n майже рівні, навіть при використанні квантового комп'ютера. Схеми множинних підписів були розроблені на основі багатовимірних рівнянь з метою досягнення квантового опору. Припускаємо, що параметр n можна вибрати вільним способом, а параметри n і m пов'язані за допомогою лінійного рівняння $\alpha n + \beta m + b$, де $\alpha \neq 0, \beta \neq 0$. Отже, $m = (n)$. Беремо ціле число k , яке $\geq \max(n, m)$, $k = O(n)$ та комутативне кільце $K[x_1, x_2, \dots, x_n, x_{n+1}, x_{n+2}, \dots, x_k]$ де $x_i, i = 1, 2, \dots, n$ - змінні загальнодоступних рівнянь ${}^i p(x_1, x_2, \dots, x_n), j = 1, 2, \dots, m$ та $x_{n+1}, x_{n+2}, \dots, x_k$ є формальними змінними. Далі може бути використана одна із запропонованих нижче схем.

Схема 5.1. Припустимо, що Аліса вибирає некомутативну систему $Z(K)$ стабільних генераторів Крeмони ступеня $d = 2$ і рангу $t, t > 1$ із регулярним коефіцієнтом $Z'(K)$ такою, що існує сімейство обгорт $EZ(K)$ із $Z(K)$ і сімейство обгорт $EZ^1(K)$ із $Z'(K)$. Припустимо, що $Z(K)$ відповідає послідовності зростаючих цілих чисел $n(i)$ та і збігається з кількістю сумарних змінних k , введених вище. Тож Аліса бере генератори ${}^k g_1, {}^k g_2, \dots, {}^k g_t$ і використовує багатовимірний протокол тахоми. Вона утворює $a_j \in E_{n(k)}(K)$ та $b_j \in E_k(K)$. Вона відправляє їх Бобу. Кореспонденти виконують протокол і розроблений загальний елемент зіткнення $h = (h_1, h_2, \dots, h_k) \in E_k(K)$. Аліса (або Боб) обирає поліноми ${}^i p$ для багатовимірної системи цифрового підпису (б.с.п.). Вона / він приймає h з координатами $h'_1 = {}^i p + h_i, i = 1, 2, \dots, m$ та $h'_i = h_i + f_i, i = m + 1, m + 2, \dots, k$, де f_i - квадратичні «псевдовипадкові» елементи з $K[x_1, x_2, \dots, x_k]$.

Примітно, що користувачі повинні знати формати n та m хешованого вектора та підпису. Тож Боб (Аліса) відновлює $({}^1 p, {}^2 p, \dots, {}^m p)$, а кореспонденти можуть

використовувати систему багатовимірних цифрових підписів у приватному режимі Ель Гамала на основі обраного багатовимірного протоколу тахоми.

Схема 5.2. Аліса (або Боб) може використовувати описану вище схему з $d=3$. Для $f \in K[x_1, x_2, \dots, x_k]$ визначаємо його квадратичне обмеження $r(f)$ як суму мономіальних доданків ступеня не більше 2. Нехай $D = d/dx_1 + d/dx_2 + \dots + d/dx_k$ буде оператором диференціації для елементів $K[x_1, x_2, \dots, x_k]$. Визначаємо деформацію $def(f)$ з f як $D(f) + r(f)$ [5] для ідеї деформованих відображень зіткнень). Тому кореспонденти використовують схему 1 для розробки загального кубічного відображення зіткнення h . Вони продовжують залишати кроки схеми 5.1 з квадратичним $def(h)$ замість h .

5.5. Приклади стійких кубічних груп

5.5.1. Приклад найпростішого графу

Наступне сімейство стабільних груп вже використовується в деяких алгоритмах симетричної криптографії та протоколах комутативної та некомутативної криптографії [44, 45]. Нехай K - комутативне кільце. Визначимо $A(n, K)$ як дводольний граф із набором точок $P = K^n$ і, набором прямих $L = K^n$ (використовуються дві копії декартової степені K). Ми будемо використовувати круглі та квадратні дужки, щоб відрізнити кортежі від P та L . Отже $(p) = (p_1, p_2, \dots, p_n) \in P_n$ та $[l] = [l_1, l_2, \dots, l_n] \in L_n$. Співвідношення інцидентності $I = A(n, K)$ (або відповідний дводольний граф Γ) задається умовою pIl тоді і лише тоді, коли виконуються рівняння наступного виду.

$p_2 - l_2 = l_1 p_1, p_3 - l_3 = p_1 l_2, p_4 - l_4 = l_1 p_3, p_5 - l_5 = p_1 l_4, \dots, p_n - l_n = p_1 l_{n-1}$ для непарних n і $p_n - l_n = l_1 p_{n-1}$ для парних n .

Розглянемо випадок скінченного комутативного кільця K , $|K|=m$. Як миттєво впливає з визначення, порядок нашого дводольного графа $A(n, K)$ дорівнює $2m^n$. Граф є m -регулярним. Насправді сусід даної точки p заданий наведеними вище

рівняннями, де параметри $p_1, p_2, \dots, p_n$ - це фіксовані елементи кільця, а символи $l_1, l_2, \dots, l_n$ - змінні. Неважко помітити, що значення l_1 можна було вибрати вільно. Цей вибір рівномірно встановлює значення для $l_2, l_3, \dots, l_n$. Отже, кожна точка має точно t сусідів. Подібним чином ми спостерігаємо сусідство прямої, яка також містить t сусідів. Ми введемо колір $\rho(p)$ точки p та колір $\rho(l)$ лінії l як параметри p_1 та l_1 відповідно.

Графи $A(n, K)$ із забарвленням ρ належать до класу Γ лінгвістичних графів, розглянутих у [46]. Лінгвістичний граф $\Gamma = \Gamma(K)$ визначається над комутативним кільцем K як дводольний граф із множинами розподілів $L = K^n$ та $P = K^k$ та кольорами K^s та K^r відповідно. Проекція ρ точки $x = (x_1, x_2, \dots, x_n)$ або прямої $y = [y_1, y_2, \dots, y_t]$ на кортеж їх перших координат s і r відповідно визначає кольори вершин. Кожна вершина має унікального сусіда вибраного кольору. Отже $n + r = t + s$. Частота лінгвістичних графів задається системою поліноміального рівняння над кільцем K .

У випадку лінгвістичного графа $\Gamma(K)$ з $s = r = 1$ шлях, що складається з його вершин $v_0, v_1, v_2, \dots, v_k$, однозначно визначається початковою вершиною v_0 та кольорами $\rho(v_i)$, $i = 1, 2, \dots, k$ інших вершин із шляху. Можна розглянути граф $\Gamma = \Gamma'(K[x_1, x_2, \dots, x_n])$, визначений тим самим із рівняннями Γ , але над комутативним кільцем $K[x_1, x_2, \dots, x_n]$.

Тож можна визначити наступне символічне обчислення. Візьмемо символічну точку $x = (x_1, x_2, \dots, x_n)$, де x_i - загальні змінні $K[x_1, x_2, \dots, x_n]$ та символічний рядок C , який є набором поліномів $f_1, f_2, \dots, f_k$ з $K[x_1]$ з парним параметром k . Сформуємо шлях вершин $v_0 = x$, v_1 так, що $v_1 I v_0$ та $\rho(v_1) = f_1(x_1)$, v_2 так, що $v_2 I v_1$ та $\rho(v_2) = f_2(x_1)$, ..., v_k так, що $v_k I v_{k-1}$ і $\rho(v_k) = f_k(x_1)$. Вибираємо параметр k як парне число. Отже, v_k - точка з множини розподілів $K[x_1, x_2, \dots, x_n]^n$ графа Γ' .

Помічаємо, що для обчислення кожної координати v_i залежно від змінних $x_1, x_2, \dots, x_n$ та многочленів $f_1, f_2, \dots, f_k$ потрібні лише арифметичні операції додавання

та множення. Як впливає з визначення лінгвістичного графу кінцева вершина v_k (точка) має координати $(h_1(x_1), h_2(x_1, x_2), h_3(x_1, x_2, x_3), \dots, h_n(x_1, x_2, \dots, x_n))$, де $h_1(x_1) = f_k(x_1)$. Розглянемо відображення $H = \Gamma^\eta(C): x_i \rightarrow h_i(x_1, x_2, \dots, x_n)$, $i = 1, 2, \dots, n$, що відповідає символічному рядку C . Припустимо, що рівняння $b = f_k(x_1)$ має рівно один розв'язок. Тоді відображення $H: x_i \rightarrow h_i(x_1, x_2, \dots, x_n)$, $i = 1, 2, \dots, n$ є бієктивним перетворенням. У випадку скінченного параметра k та скінчених щільностей $f_i(x_1)$, $i = 1, 2, \dots, n$, відображення H також має скінченну щільність. Якщо всі параметри $\deg(f_i(x_1))$ скінченні, то відображення H має лінійний ступінь у змінній n . Ідея символічного обчислення [44] наступна.

Давайте розглянемо сукупність $St = St(K)$ усіх символічних рядків із добутком $(f_1, f_2, \dots, f_r) \cdot (g_1, g_2, \dots, g_s) = (f_1, f_2, \dots, f_s, g_1(f_r), g_2(f_r), \dots, g_s(f_r))$. Неважко помітити, що $St(K)$ - це напівгрупа, для якої порожній рядок служить єдністю.

Можна перевірити, що відображення $\Gamma_\eta = \eta$ є гомоморфізмом напівгрупи $St(K)$ в напівгрупу Кремони $S(K^n)$ для кожного лінгвістичного графа Γ з $r = s = 1$ і набором точок K^n . Ми розглянемо підгрупу $\Sigma = \Sigma(K)$ символічних рядків C виду $(x_1 + a_1, x_2 + a_2, \dots, x_t + a_t)$, де параметр t парний. У випадку лінгвістичних графів з $r = s = 1$ ми ідентифікуємо символічний рядок C з символом відповідний кортеж $(a_1, a_2, \dots, a_t)$. Природним добутком двох рядків, заданих кортежами $C_1 = (a_1, a_2, \dots, a_t)$ і $C_2 = (b_1, b_2, \dots, b_m)$, є рядок $C = C_1 \circ C_2 = (a_1, a_2, \dots, a_t, b_1 + a_t, b_2 + a_t, \dots, b_m + a_t)$. Цей добуток перетворює Σ на напівгрупу. Відображення η' , що посиляє C до $\eta(C)$, є гомоморфізмом Σ в афінну групу Кремони $C(K^n)$. Це обмеження Γ_η на $\Sigma(K)$. Нехай $C = (x_1 a_1, x_1 + a_2, \dots, x_1 + a_s)$ є символічним рядком із напівгрупи $\Sigma(K)$. Ми називаємо $Rev(C) = (x_1 - a_s + a_{s-1}, x_1 - a_s + a_{s-2}, \dots, x_1 - a_s + a_1, x_1 - a_s)$ як зворотний рядок для C . Легко зрозуміти, що $\eta'(C Rev(C))$ - єдиність напівгрупи Кремони.

У випадку лінгвістичних графів $\Gamma = A(n, K)$ сукупність $G(n, K) = \eta'(\Sigma(K))$ є стабільною підгрупою ступеня 3 [44]. Використовуємо позначення ${}^n\eta'$ для обмеження Γ_η , $\Gamma = A(n, K)$ на Σ . Будемо вважати, що $a_0 = 0$, і говорити, що перетворення $\eta'(C)$ незведене, якщо $a_i \neq a_{i+2}$, $i = 1, 2, \dots, t-2$. Якщо $a_1 \neq a_{t-1}$ і $a_2 \neq$

a_t , кажуть, що незведений символічний рядок C і відповідне перетворення $\eta'(C)$ є стандартними елементами. Маємо природний гомоморфізм $G(n+1, K)$ на $G(n, K)$, індукований гомоморфізмом Δ від $A(n+1, K)$ до $A(n, K)$ надісланої точки $(x_1, x_2, \dots, x_n, x_{n+1})$ до $(x_1, x_2, \dots, x_n)$ та прямої $[x_1, x_2, \dots, x_n, x_{n+1}]$ до $[x_1, x_2, \dots, x_n]$. Це означає, що існує чітко визначена проєктивна границя $A(K)$ графів $A(n, K)$ та груп $G(K)$ з груп $G(n, K)$, коли n зростає до нескінченності. Насправді у випадку $K = F_q$, $q > 2$ нескінченний граф $A(F_q)$ - це дерево.

Це означає, що група $G(F_q)$ - це група прогулянок рівною довжиною по q -регулярному дереву, що починається з нульової точки з їх природним додаванням. Стандартний символічний рядок C визначає перетворення ${}^n\eta'(C)$ у кожній групі $G(n, K)$, $n \geq 2$ та $G(K)$. Незведене перетворення $\eta'(C)$ із $G(K)$ має нескінченний порядок.

Будемо використовувати сімейство відображень, представлене нижче.

Нехай $\Delta = \Delta_{n, k}$, $n > k$ - канонічний гомоморфізм $A(n, K)$ на $A(k, K)$, що відповідає процедурі видалення координат з індексами $k+1, k+2, \dots, n$. Це відображення визначає канонічний гомоморфізм $\mu = \mu(n, k)$ групи $G(n, K)$ на $G(k, K)$. Розглянемо схему

$$\begin{array}{ccc} \Sigma(K) & & \\ / & \downarrow & \\ G(k, K) & \leftarrow & G(n, K) \end{array}$$

де вертикальна стрілка відповідає гомоморфізму ${}^n\eta'$ з $\Sigma(K)$, коса лінія відповідає ${}^k\eta'$, а горизонтальна стрілка означає $\mu(n, k)$, $n > k$. Неважко помітити, що ця схема є комутативною.

Як було помічено в [44], підгрупи $G(n, K)$ з $E_n(K)$ утворюють сімейство стійких кубічних відображень. Отже, кореспонденти можуть взяти пару $G(n, K)$ і $G(k, K)$ з $n(k) = k + \gamma$, де параметр γ є додатною константою або додатною лінійною функцією у змінній k .

Аліса може використовувати визначений вище обчислювально приручений гомоморфізм $\mu = \mu(n, k)$, $n > k$ груп $G(n, K)$ та $G(k, K)$.

Вона розглядає сімейство підгруп $G_k = G(n, K)$, $n = n(k)$, $k=2,3$ та сімейство $G'_k = G(k, K)$, $k = 2,3, \dots, n$

Вона вибирає різні рядки $w_1, w_2, \dots, w_t$ парної довжини напівгрупи $\Sigma(K)$ такі, що $w_i w_j \neq w_j w_i$ для різних i та $j \in \{1, 2, \dots, t\}$. З цієї умови випливає, що ${}^s\eta(w_i w_j) \neq {}^s\eta(w_j w_i)$ при $s \geq 2$. Після перевірки некомутативності генераторів Аліса бере генератори ${}^i g_j = {}^{n(i)}\eta(w_j)$, $j = 1, 2, \dots, t$, $i \geq 2$, які утворюють систему Кремони стабільних некомутативних генераторів, що відповідають послідовності $n(2), n(3), \dots$. Позначимо цю систему як Z . Зверніть увагу, що ${}^i SZ = \langle {}^i g_1, {}^i g_2, \dots, {}^i g_t \rangle$ є підгрупою G_i . Отже $G_i(K)$ утворюють сім'ю обгорт Z .

Аналогічно Аліса розглядає генератори ${}^i g'_j = {}^i \eta(w_j)$, $j = 2, 3, \dots, t$, $i \geq 2$ системи Z' . Зверніть увагу, що ${}^i SZ' = \langle {}^i g'_1, {}^i g'_2, \dots, {}^i g'_t \rangle$ є підгрупою $G'_i(K)$

Отже, $G'_i(K)$, $i = 2, 3, \dots$ - це сім'я обгорт Z' .

Неважко помітити, що система Z' є часткою Z , що визначається прирученими гомоморфізмами, які рухають ${}^i g_j$ до ${}^i g'_j$. Тож Аліса бере $i = k$ і запускає стабільний протокол Тахоми з Z та Z' та описує сім'ю обгорт. Отже, вона проводить кроки алгоритму, генерує пари a_i, b_i , $i = 1, 2, \dots, t$ і відправляє їх Бобу. Таким чином, кореспонденти генерують елемент зіткнення h в $E_k(K)$.

Аліса (або Боб) обирає багатовимірне відображення для цифрових підписів (БВП) до Боба (Аліса). Вона/він використовує $def(h)$ і безпечно передає відображення партнеру.

5.5.2. Інші стійкі підгрупи, визначені за допомогою лінгвістичних графів

Розглянемо більш загальні побудови на основі графів напівгруп формальної напівгрупи Кремони $E_n(K)$.

Елемент $x_1 \rightarrow f_i(x_1, x_2, \dots, x_n)$, $i = 1, 2, \dots, n$ цієї напівгрупи буде ідентифікований з набором елементів $(f_1, f_2, \dots, f_n)$, $f_i \in K[x_1, x_2, \dots, x_n]$, коли це зручно.

Розглянемо сукупність ${}^sBS(K)$ послідовностей виду $u = (H_0, G_1, G_2, H_3, H_4, G_5, G_6, \dots, H_{t-1}, H_t)$, $t = 4i$, де $H_k \in E_s(K)$, $G_j \in E_s(K)$. Позначимо ${}^sBS(K)$ як сукупність вільних символічних рядків рангу s . Визначимо добуток u з $u' = (H'_0, G'_1, G'_2, H'_3, H'_4, G'_5, G'_6, \dots, H'_{l-1}, H'_l)$ як $w = (H_0, G_1, G_2, H_3, H_4, G_5, G_6, \dots, H_{t-1}, H'_0(H_t), G'_1(H_t), G'_2(H_t), H'_3(H_t), H'_4(H_t), G'_5(H_t), G'_6(H_t), \dots, H'_{l-1}(H_t), H'_l(H_t))$. Зверніть увагу, що композиції відображень обчислюються в $E_s(K)$.

Неважко помітити, що ця операція перетворює ${}^sBS(K)$ в напівгрупу з єдиним елементом (H_0) , де E_0 є перетворенням тотожності з $S(K^s)$. Елементи роду $(H_0, G_1, G_2, H_3, H_4)$ є генераторами напівгрупи. Ця підгрупа має певну схожість із підгрупою спеціальних ланцюгів у вільному добутку $E_s(K) \cdot E_s(K)$. Називаємо ${}^sBS(K)$ напівгрупою вільних регулярних рядків розмірності s .

Припустимо, що H_t написаного вище $u \in {}^sBS(K)$ – бієктивне відображення, а її обернене – поліномне відображення (у разі нескінченного кільця K). Тоді ми можемо розглянути зворотний лінгвістичний рядок $Rev(u) = (H_{t-1}(H_t^{-1}), G_{t-2}(H_t^{-1}), G_{t-3}(H_t^{-1}), H_{t-4}(H_t^{-1}), H_{t-5}(H_t^{-1}), \dots, G_2(H_t^{-1}), G_1(H_t^{-1}), H_0(H_t^{-1}), H_t^{-1})$ і позначають u як оборотний рядок. Нехай ${}^sBR(K)$ означає напівгрупу оборотних рядків.

Нехай K – скінченне комутативне кільце. Назвемо структуру випадковості з набором точок $P = P_{s,m} = K^s + m$ та набором прямих $L = L_{r,m} = K^r + m$ як структуру лінгвістичної випадковості I_m , якщо точка $x = (x_1, x_2, \dots, x_s, x_{s+1}, x_{s+2}, \dots, x_{s+m})$ інцидентна прямій $y = [y_1, y_2, \dots, y_r, y_{r+1}, y_{r+2}, \dots, y_{r+m}]$ тоді і лише тоді, коли виконуються наступні співвідношення

$$a_1 x_{s+1} + b_1 y_{r+1} = f_1(x_1, x_2, \dots, x_s, y_1, y_2, \dots, y_r)$$

$$a_2 x_{s+2} + b_2 y_{r+2} = f_2(x_1, x_2, \dots, x_s, x_{s+1}, y_1, y_2, \dots, y_r, y_{r+1})$$

...

$$a_m x_{s+m} + b_m y_{r+m} = f_m(x_1, x_2, \dots, x_s, x_{s+1}, \dots, x_{s+m}, y_1, y_2, \dots, y_r, y_{r+1}, \dots, y_{r+m})$$

де a_j і b_j , $j = 1, 2, \dots, m$ не є нульовими дільниками, а f_j - багатовимірні многочлени з коефіцієнтами з K . Круглі та квадратні дужки дозволяють розрізнити точки відпрямих [9].

Колір $\rho(x) = \rho((x))$ ($\rho(y) = \rho([y])$) точки x (прямої $[y]$) визначається як проекція елемента (x) (відповідно $[y]$) із вільного модуля відносно початку (відносно r) координатах. Як випливає з визначення лінгвістичної структури інцидентності для кожної вершини графу інцидентності, існує унікальний сусід вибраного кольору.

Посилаємось на $\rho((x)) = (x_1, x_2, \dots, x_s)$ для $(x) = (x_1, x_2, \dots, x_{s+m})$ та $\rho([y]) = (y_1, y_2, \dots, y_r)$ для $[y] = [y_1, y_2, \dots, y_{r+m}]$ як колір точки та колір прямої відповідно. Для кожного $b \in K^r$ і $p = (p_1, p_2, \dots, p_{s+m})$ існує унікальний сусід точки $[l] = N_b(p) = N((p), b)$ з кольором b . Подібним чином для кожного $s \in K^s$ і рядка $l = [l_1, l_2, \dots, l_{r+m}]$ існує унікальна сусідня пряма $p = N_c([l]) = N([l], b)$ з кольором s . Назвемо оператора прийняття сусіда вершини відповідно вибраного кольору як оператор ковзання. На множинах P і L точок і прямих лінгвістичного графа визначаємо оператори стрибка ${}^1J = {}^1J_b(p) = J((p), b) = (b_1, b_2, \dots, b_s, p_1, p_2, \dots, p_{s+m})$, де $(b_1, b_2, \dots, b_s) \in K^s$ і ${}^2J = {}^2J_b([l]) = J([l], b) = [b_1, b_2, \dots, b_r, l_1, l_2, \dots, l_{r+m}]$, де $(b_1, b_2, \dots, b_r) \in K^r$. Назвемо кортеж (s, r, m) типом лінгвістичного графа $I = I(K)$.

Зверніть увагу, що ми можемо розглянути той самий набір вище вказаних рівнянь із коефіцієнтами з K для змінних x_i та y_i з розширення K' з K та визначити граф ${}^{K'}I = {}^{K'}I(K)$. Нехай $s = r$ і $K' = K[x_1, x_2, \dots, x_n]^n = m + s$. Ми розглядаємо вбудований підграф в I' всіх вершин ${}^{K'}I$ з кольорами з $K[x_1, x_2, \dots, x_s]^s$ (кортежі $K[x_1, x_2, \dots, x_s]^s$)

Формуємо послідовність вершин (прогулянка зі стрибками) графа I з використанням рядка з вільної лінгвістичної напівгрупи ${}^sBS(K)$.

Візьмемо початкову точку $(x) = (x_1, x_2, \dots, x_s, x_{s+1}, x_{s+2}, \dots, x_{s+m})$, утворену загальними змінними K' , і розглянемо ланцюг ковзання

$(x), J((x), H_0) = ({}^1x), N({}^1x, G_1) = [{}^2x], J([{}^2x], G_2) = [{}^3x], N([{}^3x], H_3) = ({}^4x), J(({}^4x), H_4) = ({}^5x), \dots, J([{}^{t-2}x], G_{t-2}) = [{}^{t-1}x], N([{}^{t-1}x], H_{t-1}) = ({}^tx), J(({}^tx), H_t) = ({}^tx).$

Нехай $({}^tx)$ - кортеж $(H_t, F_2, F_3, \dots, F_n)$, де $F_i \in K[x_1, x_2, \dots, x_n]$. Визначимо ${}^1\Psi(u), I = I(K)$ як відображення $(x_1, x_2, \dots, x_n) \rightarrow (H_t, F_2, F_3, \dots, F_n)$ і називаємо це ланцюговим переходом точкового різноманіття.

Викладене нижче твердження впливає з визначення відображення.

Лема 5.1. Відображення $\psi = {}^1\psi: {}^sBS(K) \rightarrow E_n(K)$ - гомоморфізм напівгруп, $\psi({}^sBR(K))$ - група [41].

Позначимо ${}^1\psi({}^sBS(K)) = {}^1CT(K)$ як напівгрупу ланцюгових переходів лінгвістичного графа $I(K)$ і відображення ψ - як лінгвістичне відображення стиснення. Зауважимо, що у випадку скінченного комутативного кільця гомоморфізм композиції $\Delta \psi$ гомоморфізму Δ і ψ відображень у нескінченну напівгрупу у скінченну множину елементів $\Delta({}^1CT(K))$.

Визначимо піднапівгрупу ${}^sGS(K)$ символічних рядків як сукупність дводольних рядків $v_i = (H_0, G_1, G_2, H_3, H_4, G_5, G_6, \dots, H_{t-1}, H_t)$ у ${}^sBS_r(K)$ з $H_0 = E_0, G_1 = G_2, H_3 = H_4, G_5 = G_6, \dots, H_{t-1} = H_t$, де $E_0 \in$ одиницею $E_n(K)$, а ${}^1\psi({}^sGS(K)) = {}^1GCT(K)$ називається напівгрупою переходів ланцюга на лінгвістичному графу I .

У випадку лінгвістичного графа $A(n, K)$ типу $(1, 1, n-1)$ ми можемо розглядати підгрупу $St(K)$ елементів ${}^1GS(K)$ з координатами типу $x_1 + t, t \in K$ і визначити ${}^A(n, K) \psi(St(K))$ із введеною вище групою кубічних ендоморфізмів $GA(n, K)$.

Можна розглянути підгрупу $LSt(K)$ елементів ${}^1BS(K)$ з координатами типу $x_1 + t, t \in K$ і побудувати розширення $Ext(GA(n, K))$ з $G(n, K)$ як ${}^A(n, K) \psi(LSt(K))$. Як було показано у статті [47], елементи стійкої групи $Ext(AG(n, K))$ також є кубічними ендоморфізмами.

Фактично перша родина $GD(n, K)$ стабільних груп ступеня 3 була запроваджена як група перетворюючих бієктивних шифрів потоку багатовимірної природи, визначених за допомогою лінгвістичних графів $D(n, K)$ типу $(1, 1, n-1)$ у [36]. Впровадження цього шифру у випадку $K = F_q$ описано в [37]. Графи $D(n, F_q)$ та їх пов'язані компоненти були введені в [48-50] як сім'я графів великого обгорті теорії екстремальних графів. [51, 52]. Зв'язки між графами $D(n, K)$ та $A(n, K)$ обговорюються в [44].

5.5.3. Спеціальні гомоморфізми лінгвістичних графів та відповідних напівгруп

Нехай $I(K)$ є лінгвістичним графом над комутативним кільцем K і $M = \{m_1, m_2, \dots, m_d\}$ - підмножина $\{1, 2, \dots, m\}$ (множина індексів для рівнянь). Припустимо, що рівняння проіндексовані елементами з M наступного виду

$$a_{m1}x_{m1} - b_{m1}y_{m1} = f_{m1}(x_1, x_2, \dots, x_s, y_1, y_2, \dots, y_r)$$

$$a_{m2}x_{m2} - b_{m2}y_{m2} = f_{m2}(x_1, x_2, \dots, x_s, x_{m1}, y_1, y_2, \dots, y_r, y_{m1})$$

...

$$a_{md}x_{md} - b_{md}y_{md} = f_{md}(x_1, x_2, \dots, x_s, x_{m1}, x_{m2}, \dots, x_{m_{d-1}}, y_1, y_2, \dots, y_r, y_{m1}, y_{m2}, \dots, y_{m_{d-1}})$$

визначають інші лінгвістичні структури інцидентності I_M . Потім натуральні проєкції $\delta_1: (x) \rightarrow (x_1, x_2, \dots, x_s, x_{m1}, x_{m2}, \dots, x_{md})$ та $\delta_2: [y] \rightarrow [y_1, y_2, \dots, y_r, y_{m1}, y_{m2}, \dots, y_{md}]$ вільних модулів визначають натуральний гомоморфізм δ структури інцидентності I на I_M . Використаємо той самий символ ρ для забарвлення лінгвістичного графа I_M .

Зрозуміло, що δ є гомоморфізмом, який зберігає колір структур інцидентності (дводольні графи). Позначимо δ як симплектичний гомоморфізм, а граф I_M як симплектичний коефіцієнт лінгвістичного графа I . У випадку лінгвістичних графів, визначених нескінченною кількістю рівнянь, можемо розглядати симплектичні коефіцієнти, визначені нескінченною підмножиною M

[30], де для побудови криптосистеми був використаний симплектичний гомоморфізм).

Лема 5.2. *Симплектичний гомоморфізм η лінгвістичного графу I типу (r, s, t) на I' , визначений над комутативним кільцем K , індукує гомоморфізм напівгрупи $\eta * {}^I CT(K)$ в ${}^I CT(K)$ та наступна діаграма є комутативною*

$$\begin{array}{ccc} {}^s BS_r(K) & \rightarrow & {}^I CT(K) \\ \downarrow & & / \\ & & {}^I CT(K) \end{array}$$

де горизонтальні та вертикальні стрілки відповідають лінгвістичним стисненням гомоморфізмів ${}^I \psi$ та ${}^I \psi$, а символ $/$ відповідає $\eta *$.

Якщо S є стабільною піднапівгрупою ${}^I CT(K)$ (або $BCT_I(K)$) ступеня d , то $\eta^*(S)$ також є стабільною піднапівгрупою (або підгрупою). Ступінь $\eta^*(S)$ обмежений d . Будемо шукати піднапівгрупу X з ${}^s BS_r(K)$ та лінгвістичні графи $I(K)$ такі, що $\Psi(X)$ є стабільною піднапівгрупою ${}^I CT(K)$.

5.5.4. Приклад стабільних підгруп довільного ступеня

Визначимо Подвійний граф Шуберта $DS(k, K)$ над комутативним кільцем K як структуру інцидентності, визначену як неперервне об'єднання розподілів множин $PS = K^{k(k+1)}$, що складається з точок, які є кортежами виду $x = (x_1, x_2, \dots, x_k, x_{11}, x_{12}, \dots, x_{kk})$ та $LS = K^{k(k+1)}$, що складається з рядків, які є кортежами типу $y = [y_1, y_2, \dots, y_k, y_{11}, y_{12}, \dots, y_{kk}]$, де x є випадковим до y , тоді і тільки тоді, коли $x_{ij} - y_{ij} = x_i y_j$ для $i = 1, 2, \dots, k$ та $j = 1, 2, \dots, k$. Зручно вважати, що індекси виду i, j розміщуються для кортежів $K^{k(k+1)}$ у лексикографічному порядку.

Вибрано термін Подвійний граф Шуберта, оскільки точки та прямі $DS(k, F_q)$ можна розглядати як підпростори $F_q^{(2k+1)}$ розмірностей $k+1$ і k , які

утворюють дві найбільші клітини Шуберта. Нагадаємо, що найбільша клітина Шуберта - це найбільша орбіта групи однокутних матриць, що діють на різноманітність підмножин заданих розмірностей.

Визначаємо колір точки $x = (x_1, x_2, \dots, x_k, x_{11}, x_{12}, \dots, x_{kk})$ з PS як кортеж $(x_1, x_2, \dots, x_k)$ і колір прямої $y = [y_1, y_2, \dots, y_k, y_{11}, y_{12}, \dots, y_{kk}]$ як кортеж $(y_1, y_2, \dots, y_k)$. Для кожної вершини v з $DS(k, K)$ існує унікальний сусід $y = N_a(v)$ даного кольору $a = (a_1, a_2, \dots, a_k)$. Це означає, що графи $DS(k, K)$ утворюють сімейство лінгвістичних графів.

Давайте розглянемо піднапівгрупу ${}^kY(d, K)$ з ${}^kBS(K)$, що складається з рядків $u = (H_0, G_1, G_2, H_3, H_4, G_5, G_6, \dots, H_{t-1}, H_t)$ такою, що максимум параметрів $\deg(H_0) + \deg(G_1), \deg(G_2) + \deg(H_3), \deg(H_4) + \deg(G_5),$

$$\deg(G_6) + \deg(H_7), \deg(G_{t-2}) + \deg(H_{t-1}), \deg(H_t) = 1 \text{ дорівнює } d, d > 1.$$

Теорема 5.3. ([41]). Нехай $I(K)$ - відношення інцидентності Подвійного графа Шуберта $DS(k, K)$. Тоді ${}^1\psi({}^kY(d, K)) = {}^kU(d, K)$ утворюють сімейство стійких напівгруп ступеня d .

Доведення ґрунтується на тому, що ланцюговий перехід u від ${}^kU(d, K)$ переміщує $x_{i,j}$ у вираз $x_{i,j} + T(u)$, де $T(u)$ - лінійна комбінація добутків $f \in K[x_1, x_2, \dots, x_k], g \in K[y_1, y_2, \dots, y_k]$ де $\deg(f) + \deg(g) \leq d$.

Нова напівгрупа ${}^kU(d, K)$ складається з перетворень вільного модуля K^t , $t = (k+1)k$. Якщо $d = 2$, то ${}^kU(d, K)$ містить напівгрупи квадратного перетворення, визначені в [9], які складаються з переходів ланцюга.

Нехай J - підмножина декартового квадрата $M = \{1, 2, \dots, k\}$. Ми можемо ідентифікувати його елемент (i, j) з індексом ij Подвійного графа Шуберта $DS(k, K)$.

Твердження 5.2. Кожна підмножина J з M^2 визначає симплектичний гомоморфізм δ_J з $DS(k, K)$ на лінгвістичному графі $DS_J(k, K)$.

Неважко помітити, що у випадку порожньої множини J зображення відображення є повним дводольним графом із набором вершин $K^k U K^k$.

Висновок 5.3. Нехай $I(J, K)$ є відношенням інцидентності лінгвістичного графа $DS_J(k, K)$. Тоді ${}^{I(J, K)}\psi({}^k Y(d, K)) = {}^k U_J(d, K)$ утворюють сімейство стійких напівгруп ступеня d .

Нехай $f: N \rightarrow R$ - реальна функція в натуральній змінній, а $[,]$ позначає функцію перекриття, тобто $[f(n)]'$ є найближчим до $f(n)$ параметра n таким, що $n' \geq n$.

Аліса містить сімейство ${}^{r(n)}Y(d, K)$, $d = 2$ або $d = 3$, де $r(i) = [i^{1/2}]'$, $i = 2, 3, \dots$. Отже, точка множини ${}^{r(i)}DS(d, K)$ - це вільний модуль розмірності $[i^{1/2}]' + ([i^{1/2}]')^2$, який становить щонайменше $[i^{1/2} + i]'$.

Для кожного i вона може вибрати рядки $u(1) = u(1, i), u(2, i), \dots, u(t, i)$, $t \geq 2$ виду $u(k, i) = ({}^k, {}^i H_0, {}^k, {}^i G_1, {}^k, {}^i G_2, {}^k, {}^i H_3, {}^k, {}^i H_4, {}^k, {}^i G_5, {}^k, {}^i G_6, \dots, {}^k, {}^i H_{t-1}, {}^k, {}^i H_t)$, $k = 1, 2, \dots, t$ такі, що ${}^k, {}^i H_t, {}^j, {}^i H_t \neq {}^j, {}^i H_t, {}^k, {}^i H_t$ для різних k та j .

Остання умова гарантує, що для ${}^I\psi(u(k, i)) = a(k, i)$, $k = 1, 2, \dots, t$ умови $a(k, i) a(j, i) \neq a(j, i) a(k, i)$ виконується, якщо $j \neq k$. Отже, кубічні ендоморфізми $a(l, i) \in E_{r(i)}$, $l = 1, 2, \dots, t$, $i = 2, 3, \dots$ утворюють стабільну кубічну некомутативну систему Кремони Z , що відповідає послідовності $r(i)$. Напівгрупи ${}^{r(i)}U(d, K)$ утворюють сімейство обгорт Z . Аліса може взяти ${}^{r(i)}DS(d, K)$ і підмножину $J(i)$, яка визначає систему інцидентності $I(J, K)$ таку що $|J(i)| = ir(i)$. Отже, точковий набір $I(J(i), K) - K^i$.

Симплектичний гомоморфізм ${}^{r(i)}DS(d, K)$ на $I(J(i), K)$ індукує гомоморфізм $\phi(i, J(i))$ напівгрупи ${}^{r(i)}U(d, K)$ на ${}^i U_{J(i)}(d, K)$. Неважко помітити, що $\phi(i, J(i))(a(k, i)) = a'(k, i)$ утворюють частку Z' системи Z із сімейством обгорт ${}^i U_{J(i)}(d, K)$.

Тож Аліса вибирає багатовимірну систему цифрових підписів з параметрами m і n . Вона приймає $i = k$, що перевищує $\max(m, n)$ для параметрів m і n . Вона генерує $a(k, j)$, $j = 1, 2, \dots, t$ з ${}^{r(k)}U(d, K)$ і розглядає підмножину $J(i)$. Аліса

використовує оборотні елементи напівгруп обгорту ${}^{r(k)}U(d, K)$ та ${}^{k}U_J(d, K)$ разом із біективними афінними перетвореннями вільних модулів $K^{r(k)}$ та K^k . Тому вона використовує багатовимірний протокол Тахоми, генерує пари (a_i, b_i) і відправляє їх Бобу.

Кореспонденти виконують протокол і генерують відображення зіткнень $h = (h_1, h_2, \dots, h_k)$ з $E_k(K)$.

Висновки до п'ятого розділу

Розглянуто варіант збереження багатовимірного загально доступного відображення цифрової системи підпису у «безпечному режимі типу Ель Гамала». Отже, використовується комбінація багатовимірного протоколу Тахома, заснованого на обраній платформі, з багатовимірним цифровим підписом, визначеним у вибраному полі $K = F_q$. База насправді потрібна, яка складається з двох стабільних підмножин груп $S_1(q)$ і $S_2(q)$ з $E_{p(n)}$ та $E_n(F_q)$, а гомоморфізм між ними Відкритого розміру дає формат використовуваних хешованих векторів. Цей номер відомий супротивнику.

Згідно з криптографічними умовами, вся використана комбінація повинна бути відома до деяких прихованих формальних параметрів, які формують ключ алгоритму.

Таким чином супротивник знає поле F_q , розміри n та $p(n)$, пари генераторів (a_i, b_i) , $i = 1, 2$, де $a_i \in E_{p(n)}(F_q)$ та $b_i \in E_n(q)$. Отже, він знає ступінь стабільних піднапівгруп $\langle a_1, a_2, \dots, a_t \rangle$ і $\langle b_1, b_2, \dots, b_t \rangle$, може використовувати гомоморфізм, який переміщує a_i до b_i , але не знає альтернативного ефективного способу обчислення гомоморфізму.

Супротивника повідомляють, що кореспонденти періодично використовують протокол, відображення зіткнень використовується рівно один раз, а багатовимірне відображення використовується для підписів $\leq n$ разів.

Кореспонденти від сеансу до сеансу можуть змінювати набори генераторів без зміни платформи

Він/вона знає тип багатовимірного відображення $P = SP'T$, S і T розмірностей n і m та квадратичний елемент P 'виду $x_i \rightarrow i'p$, $i = 1, 2, \dots, m$, але не знає багатовимірності відображення P сама. Це означає, що супротивник знає, що кореспонденти є послідовниками одного обраного методу. Отже, кореспонденти є послідовниками методу Імай-Мацумото, Оригінального методу олії та оцту за алгоритмами Дж. Патаріна, Rainbow UOV або Lifted UOV алгоритмів.

Зверніть увагу, що криптоаналіз для перших двох методів відомий лише у випадку, коли P оприлюднюється. Супротивник знає, що кореспонденти можуть змінювати відображення S і T та внутрішні параметри P 'у кожному з цих чотирьох випадків. Для простоти ми вважаємо, що кількість рівнянь m , як відомо, суперечлива.

Таким чином, супротивник може спробувати зламати багатовимірний протокол тахоми на основі відомої важкої проблеми NP (робота з розкладання елемента формальної групи Кремони на добуток заданих генераторів, представлений у стандартній формі криптографії від багатьох змінних). Звичайно, якщо він/вона порушить протокол, противник отримує багатовимірний цифровий підпис у публічній формі. Він/вона повинен періодично обчислювати таке розкладання отриманого елемента на генератори, щоб отримати відповідне відображення зіткнень. Отже, у випадку вже порушених класичних схем Імай-Мацумото та Олії та Оцту супротивник може підробити підпис. У випадку з Rainbow and LiftedUOV противник повинен знайти розв'язання відповідної крипто аналітичної задачі. Поточний стан криптоаналізу цих схем можна знайти в [53-55].

Список джерел, використаних у п'ятому розділі

1. Post-Quantum Cryptography: Call for Proposals: <https://csrc.nist.gov/Project/Post-Quantum-Cryptography-Standardization/Call-for-Proposals>, Post-Quantum Cryptography: Round 2 Submissions.
2. M. Andrzejczak, The Low –Area FPGA Desighn for the Post – Quantum Cryptography Proposal Round 5, Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS), Cryptography and Security Systems, Leipzig, 2019.
3. R. J. McEliece, A Public-Key Cryptosystem Based On Algebraic Coding Theo-ry (1978), DSN Progress Report, 44: 114–116.
4. Jintai Ding and Albrecht Petzoldt. Current state of multivariate cryptography. IEEE Securi-ty & Privacy, 15(4):28–36, 2017.
5. V. Ustimenko, On new symbolic key exchange protocols and cryptosystems based on hid-den tame homomorphism. Dopovidi. NAS of Ukraine, 2018, n 10, pp.26-36.
6. V. Ustimenko, On the families of stable transformations of large order and their crypto-graphical applications, Tatra Mt. Math. Publ., 70 (2017), 107-117.
7. V. Ustimenko, M. Klisowski , On Noncommutative Cryptography with cubical multivari-ate maps of predictable density, In “Intelligent Computing” , Proceedings of the 2019 Computing Conference, Londone, Volume 2, Part of Advances in Intelligent Systems and Computing (AISC), volume 998, Springer, pp. 654-674.
8. V. Ustimenko, On desynchronised multivariate algorithms of El Gamal type for stable semigroups of affine Cremona group, Theoretical and Applied Cybersecuri-ty, National Technical University of Ukraine "Igor Sikorsky Kiev Polytechnic In-stitute", Volume 1, No. 1, pp. 22-30 (2019).
9. V. Ustimenko, On the usage of postquantum protocols defined in terms of transformation semigroups and their homomophisms, Theoretical and Applied

Cybersecurity, National Technical University of Ukraine "Igor Sikorsky Kiev Polytechnic Institute", Volume 1, No. 2, pp. 32-44 (2020).

10. R. Wagner, M. R. Magyarik, "A Public-Key Cryptosystem Based on the Word N Problem", *Advances in Cryptology, Proceedings of CRYPTO '84*, Santa Barbara, California, USA, August 19-22, 1984.

11. D. N. Moldovyan, N. A. Moldovyan, A New Hard Problem over Non-commutative Finite Groups for Cryptographic Protocols, *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2010: Computer Network Security*, pp. 183-194.

12. L. Sakalauskas., P. Tvarijonas , A. Raulynaitis, Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problema in Group Representation Level}, *INFORMATICA*, 2007, vol. 18, No 1, 115-124.

13. V. Shpilrain, A. Ushakov, The conjugacy search problem in public key cryptography: unnecessary and insufficient, *Applicable Algebra in Engineering, Communication and Computing*, August 2006, Volume 17, Issue 3–4, pp 285–289

14. Delaram Kahrobaei, Bilal Khan, A non-commutative generalization of ElGamal key exchange using polycyclic groups, In *IEEE GLOBECOM 2006 - 2006 Global Telecommunications Conference* [4150920] DOI: 10.1109/GLOCOM.2006.

15. Delaram Kahrobaei, Bilal Khan, A non-commutative generalization of ElGamal key exchange using polycyclic groups, In *IEEE GLOBECOM 2006 - 2006 Global Telecommunications Conference* [4150920] DOI: 10.1109/GLOCOM.2006.

16. Zhenfu Cao (2012). *New Directions of Modern Cryptography*. Boca Raton: CRC Press, Taylor & Francis Group. ISBN 978-1-4665-0140-9.

17. Benjamin Fine, et. al. "Aspects of Non abelian Group Based Cryptography: A Survey and Open Problems". arXiv:1103.4093.

18. Alexei G. Myasnikov; Vladimir Shpilrain; Alexander Ushakov. Non-commutative Cryptography and Complexity of Group-theoretic Problems. Amer. Math Soc. 2011
19. Anshel, I., Anshel, M., Goldfeld, D.: An algebraic method for public-key cryptography. *Math. Res.Lett.* 6(3–4), 287–291 (1999).
20. Blackburn, S.R., Galbraith, S.D.: Cryptanalysis of two cryptosystems based on group actions. In: *Advances in Cryptology—ASIACRYPT '99. Lecture Notes in Computer Science*, vol. 1716, pp. 52–61. Springer, Berlin (1999).
21. C Ko, K.H., Lee, S.J., Cheon, J.H., Han, J.W., Kang, J.S., Park, C.: New public-key cryptosystem using braid groups. In: *Advances in Cryptology—CRYPTO 2000*, Santa Barbara, CA. *Lecture Notes in Computer Science*, vol. 1880, pp. 166–183. Springer, Berlin (2000)
22. Maze, G., Monico, C., Rosenthal, J.: Public key cryptography based on semigroup actions. *Adv.Math. Commun.* 1(4), 489–507 (2007).
23. P.H. Kropholler, S.J. Pride, W.A.M. Othman K.B. Wong, P.C. Wong, Properties of certain semigroups and their potential as platforms for cryptosystems, *Semigroup Forum* (2010) 81: 172–186.
24. J. A. Lopez Ramos, J. Rosenthal, D. Schipani, R. Schnyder, Group key management based on semigroup actions, *Journal of Algebra and its applications*, vol.16, 2019.
25. Gautam Kumar and Hemraj Saini, Novel Noncommutative Cryptography Scheme Using Extra Special Group, *Security and Communication Networks*, Volume 2017, Article ID 9036382, 21 pages, <https://doi.org/10.1155/2017/9036382>.
26. V. A. Roman'kov, A nonlinear decomposition attack, *Groups Complex. Cryptol.* 8, No. 2 (2016), 197–207.
27. V. Roman'kov, An improved version of the AAG cryptographic protocol, *Groups, Complex., Cryptol.* 11, No. 1 (2019), 35–42.

28. A. Ben-Zvi, A. Kalka and B. Tsaban, Cryptanalysis via algebraic span, In: Shacham H. and Boldyreva A. (eds.) *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference*, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part I, Vol. 10991, 255{274, Springer, Cham (2018).
29. B. Tsaban, Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography, *J. Cryptol.* 28, No. 3 (2015), 601-622.
30. V. Ustimenko, U. Romanczuk-Polubiec, A. Wroblewska, M. Polak, E. Zhupa, On the constructions of new symmetric ciphers based on non-bijective multivariate maps of prescribed degree, *Security and Communication Networks*, Volume 2019, Article ID 2137561, 15pages <https://doi.org/10.1155/2019/2137561>
31. Max Noether, Luigi Cremona , *Mathematische Annalen* 59, 1904, p. 1–19.
32. I.R. Shafarevich, On some infinite dimension groups II, *Izv. Akad. Nauk SSSR Ser. Mat.*, Volume 45, No. 1, pp. 214-226 (1981); *Mathematics of the USSR-Izvestiya*, Volume 18, No. 1, pp. 185-194 (1982).
33. Yu. Bodnarchuk, Every regular automorphism of the affine Cremona group is inner, *Journal of Pure and Applied Algebra*, Volume 157, Issue 1, pp. 115-119 (2001).
34. A. Ostafe, I. E. Shparlinski, On the degree growth in some polynomial dynamical systems and nonlinear pseudorandom number generators, *Mathematics of Computation*, Volume 79, No. 269, pp. 501-511 (2010).
35. A. Ostafe, Multivariate permutation polynomial systems and nonlinear pseudorandom number generators, *Finite Fields and Their Applications*, Vol. 16, 2010, Is.3, pp. 144-154.
36. V. Ustimenko, Coordinatisation of Trees and their Quotients, in the Voronoj's Impact on Modern Science, Kiev, Institute of Mathematics, 1998, vol. 2, 125-152.
37. V. Ustimenko, CRYPTIM: Graphs as Tools for Symmetric Encryption, *Lecture Notes in Computer Science*, Springer, LNCS 2227, Proceedings of AAEECC-14

Symposium on Applied Algebra, Algebraic Algorithms and Error Correction Codes, November 2001, p. 278 - 286.

38. V. Ustimenko, On the graph based cryptography and symbolic computations, *Serdica Journal of Computing*, Proceedings of International Conference on Application of Computer Algebra, ACA-2006, Varna, N1 (2007).

39. V. Ustimenko, On the extremal graph theory for directed graphs and its cryptographic applications, In: T. Shaska, W.C. Huffman, D. Joener and V. Ustimenko, *Advances in Coding Theory and Cryptography*, Series on Coding and Cryptology, vol. 3, 181-200 (2007).

40. A. Wroblewska, On some properties of graph based public keys, *Albanian Journal of Mathematics*, Volume 2, No. 3, pp. 229-234 (2008)

41. V. Ustimenko, On inverse protocols of Post Quantum Cryptography based on pairs of non-commutative multivariate platforms used in tandem, *ePrint Archive*, 897, 2019.

42. J. Ding., J.E. Gower and D.S. Schmidt., *Multivariate Public Key Cryptosystems*, 260. Springer, *Advances in Information Security*, v. 25, (2006).

43. N. Koblitz, *Algebraic aspects of cryptography*, Springer (1998)., 206 P.

44. V. A. Ustimenko, V. A. (2013). On the extremal graph theory and symbolic computations. *Dopov. Nac. akad. Nauk Ukr.*, 2013, No. 2, pp. 42-49.

45. V. Ustimenko, On semigroups of multiplicative Cremona transformations and new solutions of Post Quantum Cryptography, *Cryptology ePrint Archive*, 133, 2019.

46. V. Ustimenko, Maximality of affine group, hidden graph cryptosystem and graph's stream ciphers, *Journal of Algebra and Discrete Mathematics*, 1, 2004, v.10, pp. 51-65.

47. V. Ustimenko, U. Romanczuk-Polubiec, A. Wroblewska, Expanding graphs of the Extremal Graph Theory and expanded platforms of Post Quantum Cryptography,

Position Papers of the 2019 Federated Conference on Computer Science and Information Systems, FedCSIS 2019, Leipzig, Germany, September 1-4, 2019, Annals of Computer Science and Information Systems, No. 19, pp. 41{46 (2019).

48. F. Lazebnik, V. Ustimenko, Some Algebraic Constructions of Dense Graphs of Large Girth and of Large Size, DIMACS series in Discrete Mathematics and Theoretical Computer Science , v. 10, (1993) 75 - 93.

49. F. Lazebnik, V. Ustimenko, New Examples of Graphs without Small Cycles and of Large Size, Europ. J. of Combinatorics(1993) 14, PP. 445-460..

50. F. Lazebnik, V. Ustimenko, Explicit construction of graphs with arbitrary large girth and of large size, Discrete Applied Mathematics 60 (1995), 275-28.

51. F.Lazebnik, V. Ustimenko, A.J.Woldar, A new series of dense graphs of high girth, Bulletin of the AMS 32 (1) (1995), 73-79.

52. F.Lazebnik, V. Ustimenko and A. J.Woldar, A characterisation of the components of the graphs $D(k; q)$, Discrete Mathematics,157 (1996), 271-283.

53. Jintai Ding and Joshua Deaton and Kurt Schmidt and Vishakha and Zheng Zhang, Cryptanalysis of The Lifted Unbalanced Oil Vinegar signature scheme, Cryptology ePrint Archive: Report 2019/1490.

54. Jintai Ding and Joshua Deaton and Vishakha and Bo-Yin Yang, The Nested Subset Differential Attack: A Practical Direct Attack Against LUOV which Forges a Signature within 210 Minutes, ePrint Archive: Report 2020/967.

55. Shuhei Nakamura and Yasuhiko Ikematsu and Yacheng Wang and Jintai Ding and Tsuyoshi Takagi. Shuhei Nakamura and Yasuhiko Ikematsu and Yacheng Wang and Jintai Ding and Tsuyoshi Takagi, New Complexity Estimation on the Rainbow-Band-Separation Attack, ePrint Archive:2020.

ВИСНОВКИ

У дисертації розв'язано задачі оптимізації, імплементації та практичного використання математичних алгоритмів методами теорії алгебраїчних графів. Зокрема, задачі моделювання прикладних алгебраїчних об'єктів (графів, відповідних їм груп та напівгруп перетворень визначених над різними некомутативними кільцями, відповідних динамічних систем) розв'язано методами Алгебраїчної Комбінаторики.

Це дозволило розробити комплекс програм для розв'язання різних проблем сучасного захисту інформації з використанням мов Java, C Sharp та C++. У процесі виконання дисертаційної роботи отримано такі основні результати.

1. Задачу про потокове шифрування розв'язано у термінах динамічних систем, визначених за графами $A(n,K)$ та $D(n,K)$ над обраними скінченними кільцями (скінченні поля, Булеві кільця, арифметичні кільця лишків за модулем натурального числа) таким чином, що функція шифрування гарантує наступну властивість: різним гаслам відповідають різні шифрограми обраного відкритого тексту.

2. За допомогою моделювання та комп'ютерної симуляції підібрано параметри при яких зміна одного символу тексту або гасла призводить до зміни 96-98% символів шифрограми. Показник аваланч ефекту покращено на 16-18%.

3. Методами комп'ютерної симуляції та теорії складності алгоритмів проведено криптографічні дослідження атак лінеаризації. Доведено, що для проведення таких атак супротивник повинен перехопити за $1/8n^3 + O(n^2)$ пар відкритого тексту (відповідна шифрограма). При цій умові успішна атака лінеаризації потребує час $O(n^{10})$. Тобто кореспонденти можуть безпечно використовувати незмінне гасло до $1/8n^3 + O(n^2)$ програм, які працюють з різними типами файлів розширення .txt .jpg, .tyf, .avi та інші.

4. Методами теорії Екстремальних графів побудовано швидкі алгоритми створення залежних від ключа дайджестів електронних документів. Використано методи моделювання та комп'ютерної симуляції дозволили підібрати параметри

для досягнення високого рівня аваланч ефекту (98%), показник аваланч ефекту покращено на 45%, тому дайджест є чутливим інструментом для виявлення кібератак та подальшого аудиту.

5. Методами Алгебраїчної Геометрії над скінченними комутативними кільцями оптимізовано нові алгебраїчні криптосистеми з публічним ключем. Всі такі криптосистеми базуються на алгебраїчних поліноміальних перетвореннях необмеженої степені на відміну від криптосистем розглянутих NIST (степені 2 та 3).

6. Методами теорії складності досліджено властивості криптосистем типу Ель Гамаля, де інструмент шифрування не надається публічно. Обрані криптосистеми використовують методи некомутативної криптографії. Деякі з криптосистем використовують небієктивне відображення необмеженої степені. Параметри (ступінь, густина, період) підбрані так, що відомі методи криптоаналітичних досліджень (бази Ширшова-Грьобнера та інше) не можливо використати.

7. Методами алгебраїчної геометрії оцінено рівень безпеки нових систем електронного підпису, що не спираються на публічні ключі.

8. За рахунок використання генерованих таблиць алгебраїчних операцій швидкодія алгоритмів обміну ключів покращена на порядок. Такі системи використовують складність факторизації нелінійного відображення у добуток відомих генераторів та деякі інші складні проблеми (потенціювання зі спряженості, дискретний логарифм для спеціальних нелінійних перетворень).

ДОДАТКИ

Додаток А Список опублікованих праць за темою дисертації

Праці, в яких опубліковано основні результати дисертації:

1. V. Ustimenko, **O. Pustovit**, On effective computations in subsemigroups of affine Cremona semigroup and implementations of new postquantum multivariate cryptosystems, Physico-mathematical modelling and informational technologies, Lviv, vol. 32, 2021, pp. 27-31.

2. V. Ustimenko, **O. Pustovit**, On the implementations of new multivariate public keys based on transformations of linear degree, Conference on Mathematical Foundations of Informatics, Kyiv, 2021, pp. 397-420.

3. **O.S. Pustovit**, V.O Ustimenko, A new stream algorithms generating sensitive digests of digital documents, Mathematical modelling in economics, N3, 2019, 18-35.

4. Устименко В. О., **Пустовіт О. С.** Нові потокові алгоритми для створення дайджесту електронних документів з високим рівнем лавинного ефекту. Математичне та комп'ютерне моделювання, Серія: Фізико-математичні науки, Збірник наукових праць. Випуск 19, Київ, 2019, с. 174-180.

5. **О. Пустовіт**, В. Устименко, Про застосування алгебраїчної комбінаторики до проблем кодування та криптографії, Математичне моделювання в економіці, № 1-2, Київ, 2017, с. 31-39.

6. **О. Пустовіт**, Динамічні системи та їх використання до проблем інформаційної безпеки, Журнал для студентів фізико-математичних етюдів, №10, Київ, 2011, 64-67.

Праці, які засвідчують апробацію матеріалів дисертації:

7. Устименко В.О., **Пустовіт О.С.**, On the implementation of postquantum access control protocol based algorithms, 20 Міжнародна науково-практична конференція: Сучасні інформаційні технології управління навколишнім середовищем, природного використання, заходи в надзвичайних ситуаціях, Київ, 2021, с 42-44.

8. V. Ustimenko, **O. Pustovit**, New cryptosystems of Noncommutative cryptography based on Eulerian semigroups of multivariate transformations, Cybersecurity Providing in Information and Telecommunication Systems 2021, Kyiv, 2021, pp. 18-26. (*індексується в Scopus*)

9. V. Ustimenko, **O. Pustovit**, On new stream algorithms generating sensitive digests of computer files, Federated Conference on Computer Science and Information Systems, Sofia, 2021, pp. 131-135 (**List B, IEEE Digital Library**)

10. V. Ustimenko, **O. Pustovit**, On the implementation of public keys with the usage of algebraic maps of unbounded degree, The 13th International Algebraic Conference in Ukraine, Kyiv, 2021, p. 84.

11. V. O. Ustimenko, **O. S. Pustovit**, Dynamical systems based on small world expanding graphs and algorithms to secure big data processing, International conference Modern Stochastics: Theory and Applications V, Kyiv, 2021, pp. 39-40.

12. Устименко В.О., **Пустовіт О. С.**, Про застосування екстремальної теорії графів до створення дайджестів електронних документів з високорівневим аваланч ефектом, 3 Міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS) 2-3 квітня 2020, Taras Shevchenko National University of Kyiv.

13. V. O. Ustimenko, **O. S. Pustovit**, On noncommutative cryptography responds to challenges of quantum computer and secure big data processing, International mathematical conference dedicated to the 60th anniversary of the department of algebra and mathematical logic of Taras Shevchenko National University of Kyiv, Book of abstract, Kyiv 2020, p.83.

14. Устименко В.О., **Пустовіт О. С.**, Про нові постквантові алгоритми електронного підпису, що модифікують алгоритми представлені на другий етап NIST сертифікації, Праці 19-ої Міжнародної науково – практичної конференції «Сучасні інформаційні технології управління екологічною безпекою, природокористуванням, заходами в надзвичайних ситуаціях», 2020р., м. Київ, Петропавлівська Борщагівка.(розділ у колективній монографії), с. 57-59.

15. Устименко В.О., **Пустовіт О.С.**, Покращена безпека для ГІС з використанням N-зв'язної архітектури та нового графу, який базується на основі потокового шифру, 18 Міжнародна науково-практична конференція: Сучасні інформаційні технології управління навколишнім середовищем, природного використання, заходи в надзвичайних ситуаціях, Київ, 2019, с. 92-94.

16. Устименко В. О, **Пустовіт О.С.**, Про екстремальні графи, афінну напівгрупу Кремони та нові рішення постквантової криптографії, Міжнародна алгебраїчна конференція, 2019, с. 121-122, Вінниця.

17. **Пустовіт О.С.**, Устименко В. О. Нові алгоритми аудиту електронних документів, їх впровадження та застосування в кібербезпеці, 17 Міжнародна науково-практична конференція: Сучасні інформаційні технології управління навколишнім середовищем, природокористування, заходи в надзвичайних ситуаціях, Київ, 2018, с. 170-175.

18. В. О. Устименко, **О. С. Пустовіт**, Нова концепція електронного підпису та засоби її реалізації, 16 Міжнародна науково-практична конференція: Сучасні інформаційні технології управління навколишнім середовищем, природокористування, заходи в надзвичайних ситуаціях, Київ, 2017, с. 86-89.

19. В.М. Лахман, **О.С. Пустовіт**, В.О. Устименко, Про реалізацію криптографічного алгоритму, визначеного в рамках груп Кас-Moody над діаграмою $\overline{A_1}$, International mathematical conference Group and Actions: Geometry and Dynamics, Київ, 2016, с. 33

Додаток Б Відомості про апробацію результатів дисертації

№ п/п	Назва конференції, конгресу, симпозіуму, школи	Місце проведення	Дата проведення	Форма участі
1	International mathematical conference «Groups and Actions, Geometry and Dynamics»	м. Київ	19-22.12.2016	Очна
2	16 Міжнародна науково-практична конференція «Сучасні інформаційні технології управління навколишнім середовищем, природокористування, заходи в надзвичайних ситуаціях»	м. Київ, Пуща-Водиця	3-4.10.2017	Очна
3	17 Міжнародна науково-практична конференція «Сучасні інформаційні технології управління навколишнім середовищем, природокористування, заходи в надзвичайних ситуаціях»	м. Київ	24-25.09.2018	Очна
4	Міжнародна алгебраїчна конференція	м. Вінниця	02-06.07.2019	Очна
5	Міжнародний науковий симпозіум «Питання оптимізації обчислень» (ПОО-XLVI)	м. Київ	24.27.09.2019	Очна
6	18 Міжнародна науково-практична конференція «Сучасні інформаційні технології управління навколишнім	м. Київ	01-02.10.2019	Очна

	середовищем, природокористування, заходи в надзвичайних ситуаціях»			
7	3 Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно- телекомунікаційних систем» (PCSITS)	м. Київ	02-03.04.2020	Онлайн
8	International mathematical conference dedicated to the 60th anniversary of the department of algebra and mathematical logic of Taras Shevchenko National University of Kyiv	м. Київ	14-17.07.2020	Онлайн
9	19 Міжнародна науково- практична конференція «Сучасні інформаційні технології управління навколишнім середовищем, природокористування, заходи в надзвичайних ситуаціях»	м. Київ	06-07.10.2020	Онлайн
10	Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS'2021)	м. Київ	28.01.2021	Онлайн
11	VI International Conference on Mathematical Foundations of Informatics MFOI-2020	м. Київ	13-15.01.2021	Онлайн
12	International conference Modern	м. Київ	01-04.06.2021	Онлайн

	Stochastics: Theory and Applications V			
13	The 13th International Algebraic Conference in Ukraine	м. Київ	06-09.07.2021	Онлайн
14	Federated Conference on Computer Science and Information Systems	м. Софія, Болгарія	02.09.2021	Онлайн
15	Міжнародний науковий симпозіум «Питання оптимізації обчислень» (ПОО-XLVII)	м. Львів	21-24.09.2021	Онлайн
16	20 Міжнародна науково-практична конференція «Сучасні інформаційні технології управління навколишнім середовищем, природокористування, заходи в надзвичайних ситуаціях»	м. Київ	04-08.10.2021	Онлайн

Додаток В Акти впровадження результатів дисертаційної роботи



ТОВ «Алгоритм-Х»
ЄДРПОУ 41098587
вул. Вікентія Хвойки, 18/14
м. Київ, Україна, 04080
тел.: (067) 431-02-02, (044) 221-74-82
e-mail: info@algoritm-x.com.ua

19 ТРА 2021

№ 1905/2

Акт впровадження

результатів дисертаційного дослідження

Пустовіта Олександра Сергійовича

на тему «Застосування теорії екстремальних графів

до сучасних проблем інформаційної безпеки»,

поданої на здобуття наукового ступеня кандидата технічних наук

зі спеціальності 05.13.06 – інформаційні технології

Цим Актом засвідчуємо, що нижчезазначені наукові розробки, виконані особисто Пустовітом Олександром Сергійовичем у ході проведення ним дисертаційних досліджень, а саме:

- створення криптографічно стійких швидких потокових алгоритмів шифрування великих файлів з визначеним періодом вживання гасла;
- створення чутливих дайджестів електронних файлів з високим показником аваланч ефекту;
- створення постквантових публічних ключів у термінах криптографії від багатьох змінних;
- розробка протоколів обміну ключів в термінах теорії алгебраїчних графів та некомутативної алгебри, стійких до засобів класичного та постквантового криптоаналізу;
- застосування цих протоколів до створення нових асиметричних алгоритмів типу Ель Гамала та до розв'язання задач постквантового електронного підпису та контролю доступу до ресурсів інформаційних систем, -

використані в ТОВ «АЛГОРИТМ-Х» при виконанні науково-дослідної роботи «Розробка окремих структурних елементів захищеної мобільної мультисервісної інфраструктури» (№ держреєстрації 0119U102716).

Акт видано для подання до спеціалізованої вченої ради.

Директор

ТОВ «АЛГОРИТМ-Х»



Б.В.Жовтобрюх

ВИКОНАВЧИЙ ОРГАН КИЇВСЬКОЇ МІСЬКОЇ РАДИ
(КИЇВСЬКА МІСЬКА ДЕРЖАВНА АДМІНІСТРАЦІЯ)

**КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА**

Вул. Бульварно-Кудрявська, 18/2, м. Київ,
Україна, 04053, тел./факс: +380 44 272-19-02
kubg.edu.ua, e-mail: kubg@kubg.edu.ua
ЄДРПОУ 02136554



EXECUTIVE BODY OF KYIV CITY COUNCIL
(KYIV CITY STATE ADMINISTRATION)

**BORYS GRINCHENKO
KYIV UNIVERSITY**

18/2 Bulvarno-Kudriavska St., Kyiv,
Ukraine, 04053, tel./fax: +380 44 272-19-02
kubg.edu.ua, e-mail: kubg@kubg.edu.ua

31.08.2021р. № 28-Н.

На № _____ від _____

АКТ

**про впровадження результатів дисертаційного дослідження
Пустовіта Олександра Сергійовича
на тему «Застосування теорії екстремальних графів
до сучасних проблем інформаційної безпеки»,
поданої на здобуття наукового ступеня кандидата технічних наук
зі спеціальності 05.13.06 – інформаційні технології**

Цим Актом, ґрунтуючись на рішенні кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка (протокол №12 від 24 червня 2021 р.), засвідчуємо, що *нижчеперелічені наукові положення, а саме:*

- криптографічно стійкі швидкі алгоритми для хашування великих файлів у дайджесту заданих розмірів;
- алгоритми створення чутливих дайджестів електронних файлів;
- парадигма, в якій теорія алгебраїчних графів та некоммутативна алгебра використовується для розробки та впровадження нових несиметричних інструментів криптографії (протоколи, криптосистеми, інструмент контролю доступу), стійких до кібератак супротивника у постквантову епоху.
- алгоритми та їх імплементація в задачу електронного підпису для безпеки передавання інформації.

Розроблені особисто Пустовітом Олександром Сергійовичем у ході проведення ним дисертаційних досліджень та *отримали високу оцінку* при обговоренні на засіданнях кафедри інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка.

Зазначені наукові результати:

по-перше, впроваджені в освітній процес Університету у робочих програмах навчальних дисциплін «Методи побудова та аналізу криптосистем» і «Математичні методи криптографії» другого (магістерського) рівня вищої освіти;

по-друге, впроваджені в програмно-апаратне забезпечення «Центру дослідження технологій захисту інформаційних активів» Університету Грінченка при розгортанні Лабораторії систем криптографічного та технічного захисту інформації (навчальний кіберполігон).

Дослідження Пустовіта Олександра Сергійовича відповідає всім вимогам до організації наукового пошуку та дає позитивний результат у практичному застосуванні.

Акт видано для подання до спеціалізованої вченої ради.

Проректор з науково-педагогічної
та міжнародної діяльності



Лілія ГРИНЕВИЧ