УДК 519.1, 514.128

О.С. ПУСТОВІТ, В.О. УСТИМЕНКО

ПРО ЗАСТОСУВАННЯ АЛГЕБРАЇЧНОЇ КОМБІНАТОРИКИ ДО ПРОБЛЕМ КОДУВАННЯ ТА КРИПТОГРАФІЇ

Анотація. *У статті подано короткий огляд вітчизняних досліджень із застосувань алгебраїчної комбінаторики до захисту інформації. Розроблена теорія дала змогу побудувати нові нелінійні алгоритми захисту інформації, які можуть бути використані в задачах електронного бізнесу, управління та комерції. Параметри одного з потокових алгоритмів представлено у таблицях. Описано його специфічні властивості. Головною метою статті є огляд застосувань з прикладної алгебраїчної комбінаторики до постквантової криптографії – напрямку, який виник у зв'язку з надіями на появу квантового комп'ютера.*

Ключові слова: *постквантова криптографія, безпека електронного управління, криптографія від багатьох змінних, алгебраїчні графи, комбінаторика.*

Вступ

Метою статті є огляд досліджень з прикладної алгебраїчної комбінаторики – напрямку, який виник як математичне підґрунтя теорії кодування та застосування теорії динамічних систем до криптографії із представленням практичного застосування прикладної алгебраїчної комбінаторики у криптографії. Основними задачами є постановка проблеми дискретного логарифму та симетричні алгоритми з приватним ключем, які використовуються у кодуванні та криптографії.

Роботу присвячено деяким питанням інформаційної безпеки для електронного управління (e-governing) та електронного бізнесу (e-business). В останні десятиліття із зростанням інформаційних технологій завдання інформаційної безпеки в даній області істотно розширилися. Тому сфера інформаційної безпеки стала важливим напрямком активної міжнародної співпраці. При вирішенні завдань електронного управління необхідно захищати банківські електронні платежі, інформаційні мережі, інформаційні системи та багато іншого.

Конфіденційна інформація схильна до погроз недружнього ознайомлення, накопичення, підміни, фальсифікації і тому подібне. Час від часу з'являється сенсаційна інформація про успішні електронні атаки на захищені бази даних як державних, так і корпоративних організацій (wikileaks скандал, просочування інформації Sonny corporation). Розробка ефективних засобів захисту з керованим рівнем безпеки – одна з умов створення успішної моделі системи захисту інформаційних систем та комунікаційних мереж.

Стратегія розвитку глобальних мереж потребує подальшого розвитку теоретичних та технологічних методів захисту інформації. Зокрема, розвиток громадянського суспільства (електронне управління, електронний бізнес та зв'язок тощо) потребує нових криптографічних симетричних та асиметричних алгоритмів, протоколів обміну ключами. Особливу увагу слід приділяти

розвитку методів захисту, які потенційно можуть використовуватися і після появи квантового комп'ютера або ж інших реалізацій ідеї ймовірнісної обчислювальної машини.

У цьому напрямку перспективними є нові методи, що реалізуються на основі символьних перетворень. Протягом 2012 року, оголошеного Міжнародним роком Алана Тюрінга, відбулося декілька міжнародних конференцій, присвячених поліноміальній криптографії від багатьох змінних (Multivariate cryptography). Слід зауважити, що до наукової спадщини Алана Тюрінга належить не тільки концепція сучасного комп'ютера, засади штучного інтелекту, але й видатні приклади практичних криптографічних розробок.

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 Імаі 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 та мережі, інші складні об'єкти.).

У суспільстві виникають потреби захисту інформації, її обробки та зберігання, що вимагає керованості балансу між рівнем безпеки інформації та швидкодією. Потрібні нові програмні продукти, де необхідний баланс може встановлювати користувач. Таких методів 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 зі 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).

Зазначена 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, яка не має 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 доступу 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 системи 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 відеотелефони. 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 й експлуатації електронних мереж.

Все викладене логічно підводить до деталізації питання щодо застосування алгебраїчної комбінаторики до проблем постквантової криптографії. Зокрема, постквантова криптографія призначена для відшукання криптографічних алгоритмів (частіше за все з публічним ключем або алгоритмів 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 підрозділяється 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 (див. [1]), що використовує поліноміальні відображення вільного модуля K^n, визначеного над скінченним 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:

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

що діють на вільному K^n, де $f_i \in K[x_1, x_2, ..., x_n]$, $i = 1, 2, \ldots, n$ 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 den (F) одночленів для многочленів $f f_i$, $i = 1, 2, \ldots, n$.

Будемо говорити, що вираз den (F) і є поліноміальним, якщо цей параметр має розмір $O(n^d)$ для деякої додатної сталої d.

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

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 $(b_1, b_2, \ldots, b_n)$ може бути обчислене за $O(n^{d1+d2+1})$ 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 (див. [1], [2]). Це досить молода дослідницька галузь, якій ще бракує прикладів криптосистем з теоретично оціненою опорністю 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 комутативним 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 Імаі та Мацумото. 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 (див., наприклад, [3] та подальші посилання).

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 із симетричних алгоритмів, що базуються на конструктивних побудовах екстремальної теорії графів та подібної теорії для орієнтованих графів (див. огляди [4], [5]).

Головна ідея – конвертувати алгебраїчний граф у скінченний автомат та використовувати псевдовипадкові прогулянки по графу як знаряддя для кодування. Такий підхід можна також використати для створення протоколів обміну ключів. Нещодавно 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 скінченних 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 значною мірою 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 скінченних полів.

Небієктивні 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 небієктивними поліноміальними кодуючими відображеннями вільного модуля Z_m^n у себе, було презентовано на міжнародній конференції з алгебри, дискретної математики та їх застосувань DIMA 2015 (див. [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 $Z_m[x_1, x_2, \ldots, x_{k-1}]$ та послідовність параметрів l_i, $i = 1, 2, \ldots, k-1$, які є взаємно простими з $\varphi(m)$. Властивості кодуючого відображення в значній мірі залежать від розкладу числа *m* на прості множники.

Це небієктивне кодуюче 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 споводована існуванням дільників нуля для складеного цілого числа *m*. В дійсності ідея "схованого RSA" знайшла реалізацію (див. [10]). Інший алгоритм, що використовує цю ідею, описано в [11].

В останні 15 років 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.

У 2001 році в Києві було відкрито Інститут телекомунікацій і глобального інформаційного простору (ІТГІП Національної академії наук України). Цей інститут займається створенням та розвитком глобальних інформаційних мереж, сучасних телекомунікаційних технологій, знаходженням технічних рішень, гарантуючих безпеку телекомунікаційного зв'язку, створенням і впровадженням автоматизованих інформаційних систем, зокрема, в галузях природоохоронного захисту та збереження природних ресурсів, розвитком сучасних інформаційних технологій у телемедицині. Вже кілька років зусилля інституту сконцентровані на створенні та впровадженні інформаційно-аналітичних засобів підтримки центрального та місцевого урядів. Дуже важливим напрямком Інституту стало впровадження нових методів та інформаційних технологій в середній та вищій освіті, зокрема, співпраця з Малою академією наук України.

ІТГІП продовжує вітчизняні дослідження з прикладної алгебраїчної комбінаторики, що починалися Л. А. Калужніним та А. О. Стогнієм в рамках спільного проекту Інституту кібернетики НАН України та Київського державного університету ім. Т. Г. Шевченка (див. [17], [18], [19], [20] та [21]).

Зокрема, продовжується праця над створенням бібліотеки криптографічного програмного забезпечення на основі властивостей простих і скерованих алгебраїчних графів без малих циклів або комутативних діаграм. Останні теоретичні результати і результати комп'ютерного моделювання представлені на кількох доповідях на міжнародних конференціях з криптології, конференціях АКА (застосування комп'ютерної алгебри) та інших. Ці алгоритми та результати досліджень їх властивостей відображені в публікаціях [22]–[26]. Значна кількість публікацій підготовлена у співпраці з дослідниками університету Марії Кюрі-Склодовської, з яким ІТГІП має міжнародну угоду про співпрацю. Огляд попередніх результатів по криптографічних алгоритмах (1998–2011) читач може знайти в книзі [23], працях Advanced Study NATO Institute, в якому брав участь і Інститут телекомунікацій [24]. Окреслимо теоретичне підґрунтя класу алгоритмів, яким займається відділ. 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 скінченної групи, але в застосуваннях до криптографії група, як правило, є мультиплікативною групою Z_n^* кільця лишків.

Нагадаємо, що теоретико-групова проблема дискретного логарифмування є наступною: знайти натуральне число x, таке що g^X = h, де h і g є обрані елементи скінченної 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 різноманіття, як група матриць над скінченним 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 Sp^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 із симетричної групи Sp^n можна записати у вигляді "публічного правила" g: x_1 переходить до $g_1(x_1, x_2, \ldots, x_n)$, x_2 – відповідно до $g_2(x_1, x_2, \ldots, x_n)$, нарешті x_n змінюється на $g_n(x_1, x_2, \ldots, x_n)$, де g_i – многочлени від багатьох змінних з $F_p[x_1, x_2, \ldots, x_n]$.

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.

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 $g_i(x_1, x_2, \ldots, x_n)$. Сучасна математика не знайшла принципово швидших за метод Гауса 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 стовпчики з простору V, A – невироджена квадратна матриця. Таким чином, існує справжня прірва по складності між лінійністю та нелінійністю.

Проблема дискретного логарифму для циклічної групи, породженої "псевдовипадковим" нелінійним поліноміальним відображенням g із 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” ужите 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 із 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.

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 нескінченності, 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-стовпчики з *V*, *A* – невироджена 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" "pseudorandom" 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), існують 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 скінченні 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).

3. Про властивості одного з потокових симетричних алгоритмів кодування

Завдяки дослідницькій діяльності Інституту телекомунікацій і глобального інформаційного простору було розроблено нові методи шифрування даних. 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. Наші 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. Із самого початку свого розвитку системи інформаційної безпеки розроблялися для військових відомств. Розголошення такої інформації могло призвести 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 лежать 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 $y_2 - x_2 = y_1 x_1$, $y_3 - x_3 = x_1 y_2$, $y_4 - x_4 = y_1 x_3$, $y_5 - x_5 = x_1 y_4$, …, $y_n - x_n = x_1 y_{n-1}$ 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 прикладом послідовності графів $A(n, q)$ є q-регулярне дерево T_q.

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

$x_0 = v$, $x_1 = Dt_1(x_0)$, $x_2 = Dt_2(x_1)$, … , $x_s = Dt_s(x_{s-1})$, де послідовність $t = t_1, t_2, \ldots, t_s$ задовольняє умову t_i та $-t_{i-1}$ різні при $i = 1,2,\ldots, s$. Нехай Dt – відображення, яке переводить v в x_s. Помітимо, що зворотним до нього буде бієкція Dt', де t – послідовність $-t_s, -t_{s-1}, \ldots, -t_1$. Виявляється, що незалежно від вибору послідовності перетворення Dt є поліноміальним перетворенням вигляду $(x_1, x_2, \ldots, x_n) \rightarrow (f_1(x_1, x_2, \ldots, x_n), f_2(x_1, x_2, \ldots, x_n), \ldots, f_n(x_1, x_2, \ldots, x_n))$, де всі многочлени $f_i(x_1, x_2, \ldots, x_n)$, $i=1,2, \ldots, n$, 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 текста" над F_q. Будемо вважати, що відкритий текст x є елементом вибраної долі, наприклад, P. Послідовність $t = t_1, t_2, \ldots, t_s$ кольорів ребер простого шляху в автоматі, відповідного обчислення функції $Dt(x)$, назвемо нескоротним пассвордом. 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 $(b_1, b_2, \ldots, b_n)$. 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 пассворда $t = t_1, t_2, \ldots, t_s$. 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 $-t_s, -t_{s-1}, \ldots, -t_1$. Кубічне перетворення E обчислюємо за допомогою одного із пакетів, реалізуючих символьні перетворення комп'ютерної алгебри. Результатом обчислення буде поліноміальне перетворення $G: (x_1, x_2, \ldots, x_n) \rightarrow (g_1(x_1, x_2, \ldots, x_n), g_2(x_1, x_2, \ldots, x_n), \ldots, g_n(x_1, x_2, \ldots, x_n))$, де всі многочлени $g_i(x_1, x_2, \ldots, x_n)$, $i=1,2, \ldots, n$, є кубічними виразами, записаними у вигляді списку впорядкованих мономів.

Список G буде служити публічним правилом (ключем), так що публічний користувач може за 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 пассворду), q (вибір алфавіту). Помітимо, що найкращий загальний алгоритм знаходження зворотного до G перетворення потребує $3^{O(n)}$ кроків, незалежно від того, використовує він ідеологію базиса Гребнера 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 пассвордам відповідають різні відображення G.

Описаний вище симетричний алгоритм має самостійну цінність як потоковий алгоритм швидкого шифрування. Якщо q – непарне, то з-за зв'язності графа при фіксованих афінних перетвореннях L_i, $i = 1,2$, та змінних нескоротних пассвордах довільної довжини кодування володіє властивістю транзитивності, тобто для довільно вибраних відкритих текстів (файлів однакового розміру) існує пассворд, такий, що відповідне кодуюче 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 пассвордів на множині слів довжини $O(n)$. Кодування при використанні таких обмежень пассвордів 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**.** В такому випадку порядок відображення G співпадає з порядком Dt. Як випливає із наведених 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 зростанні параметра n.

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

Для виміру продуктивності алгоритму, ми проведемо 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 було зроблено 160 вимірів, що представлено в табл. 1 та 2 та візуалізовано на рис. 1 і 2.

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

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

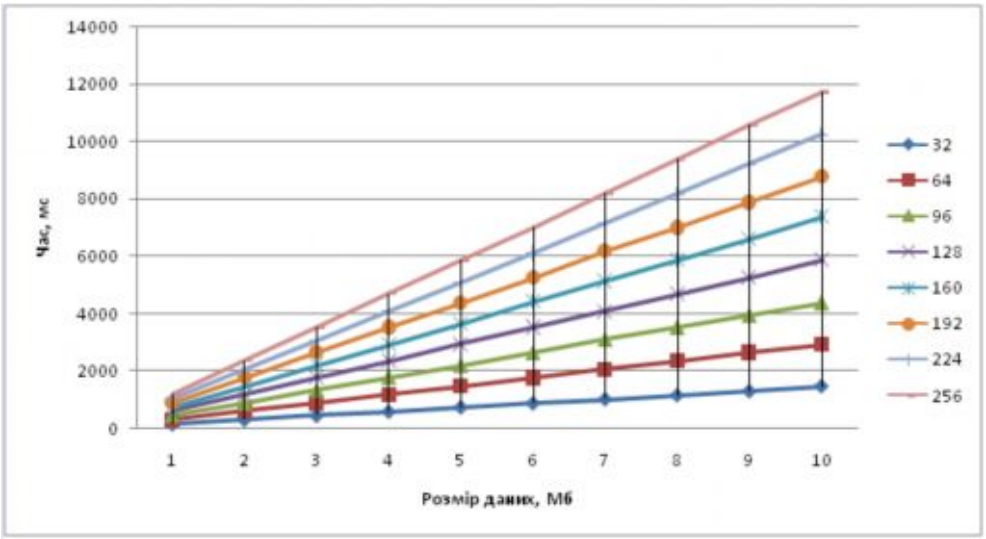

Рисунок 1 – Вимір 1: «Quad core Intel Core 2 Quad E6600 2,40GHz 4Gb RAM»

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

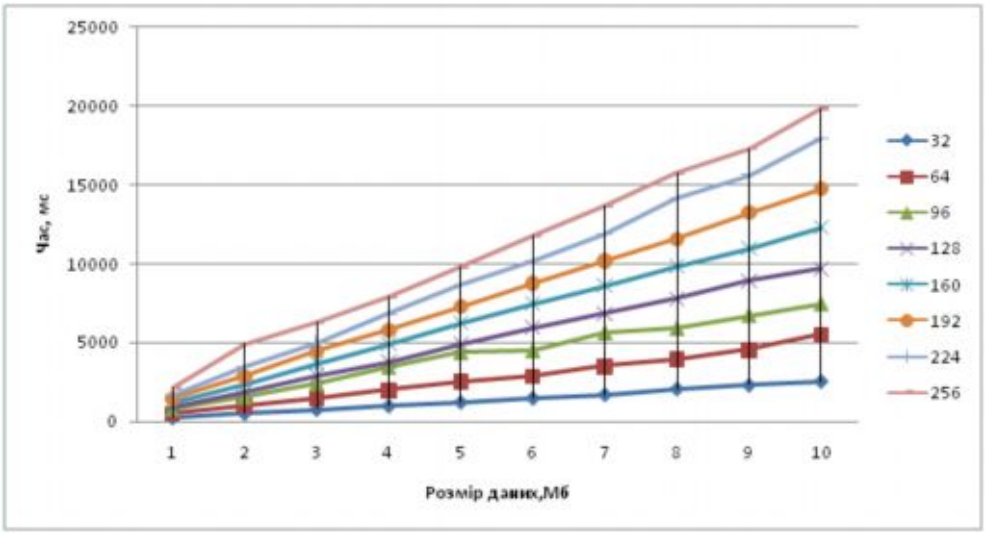

Рисунок 2 – Вимір 2: «Single core AMD Athlon 3GHz 1Gb RAM»

Презентований алгоритм є універсальним і ефективним симетричним алгоритмом шифрування даних. Цей алгоритм забезпечує однорідне шифрування всіх типів даних на основі бінарного алфавіту. 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.

У відділі інформаційної безпеки Інституту телекомунікацій і глобального інформаційного простору здійснюється подальша робота щодо вивчення алгоритмів шифрування на алгебраїчних графах, а також щодо покращення продуктивності наведеного вище алгоритму. Зокрема, у багатоядерних обчислювальних системах із застосуванням паралельних обчислень для шифрування та дешифрування даних алгоритмами, побудованими на алгебраїчних графах.

Висновки

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. Цьому аспекту була присвячена конференція Workshop on Secure Implementation of Post-Quantum Cryptography (Tel Aviv University Israel, Sep 26–27, 2016 (NATO for Science and Peace Security Program).

В Інституті телекомунікацій та глобального інформаційного простору дослідження з поліноміальної криптографії від багатьох змінних ведуться від моменту створення цієї установи. 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 ЛІТЕРАТУРИ

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., Cryptanalisis 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 // Annalles 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., Сущанский 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 AAECC-14 Symposium on Applied Algebra, Algebraic Algorithms and Error Correction Codes, November 2001, pp. 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 p.
25. V. Ustimenko, On K-theory of dynamical systems corresponding to graphs and its applications, Dopovidi NAS of Ukraine, N 8, 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.

Стаття надійшла до редакції 06.01.2017.