УДК 519.1, 514.128

https://orcid.org/0000-0002-3232-1787
https://orcid.org/0000-0002-2138-2357

О.С. ПУСТОВІТ, В.О. УСТИМЕНКО

ПРО НОВІ ПОТОКОВІ АЛГОРИТМИ СТВОРЕННЯ ЧУТЛИВИХ ДАЙДЖЕСТІВ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

Анотація. *Для прийняття обґрунтованих планових рішень у суспільно-економічній сфері спеціалісти повинні користуватися перевіреними документами. До засобів перевірки документів належать криптографічно стабільні алгоритми компресії великого файлу в дайджест визначеного розміру, чутливий до будь-якої зміни символів на вході. Пропонуються нові швидкі алгоритми компресії, криптографічна стабільність яких пов'язується зі складними алгебраїчними проблемами, такими як дослідження систем алгебраїчних рівнянь великої степені та задача розкладу нелінійного відображення простору за твірними. Запропоновані алгоритми створення чутливих до змін дайджестів документів будуть використані для виявлення кібератак та аудиту усіх файлів системи після зареєстрованого втручання.*

Ключові слова: *кібербезпека, хеш-функції, аудентифікаційні коди повідомлень, гомоморфізм компресії, високо нелінійна криптографія від багатьох змінних, некомутативна криптографія.*

DOI: 10.35350/2409-8876-2019-16-3-18-35

Вступ

У статті пропонується новий швидкий метод формування компресованого дайджесту великих електронних документів, представлених у бінарному алфавіті у вигляді меншого бінарного файлу, розмір якого визначається користувачем. Створений дайджест виявився чутливим до змін. Так, зміна поєдиного символу в оригінальному документі приводить до зміни більше ніж 98% символів у дайджесті. Алгоритм є симетричним та залежним від ключа, що задовольняє вимогам криптографічної стабільності. Вважаємо, що розробка може бути ефективно використана для розв'язання наступних двох задач:

1. Захисту великих сховищ даних від кібератак за наступним алгоритмом: створюються дайджести як закодованих, так і не закодованих електронних документів в обраний початковий час. В поточний момент часу створюються нові дайджести та порівнюються з початковими. Присутність будь-яких змін означає ушкодження файлів (кібератака, комп'ютерний вірус, відмова апаратури, помилка персоналу та інше).

2. Перевірка цілісності електронних документів при пересиланні. Кореспондент створює дайджест оригінального файлу та цього ж файлу у зашифрованому вигляді. Після пересилання створюється дайджест отриманого файлу та декодованого документа. Кореспонденти порівнюють дайджести та роблять висновок щодо наявності пошкодження.

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 витік 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].

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-функцією (MAC), використовують символ HMAC. Коли користувачі хочуть безпечно обмінятися кореспонденцією, перевіряючи хто є дійсним автором листа, так і відсутність змін при пересилці, вони разом обирають спільний MAC. При цьому користуються спільною схемою симетричного шифрування.

Крім криптографічної стабільності дуже важлива швидкодія та високий показник аваланч ефекту. Цей ефект вимірюється таким чином. Обчислюється HMAC для генерованого файлу, змінюється довільний його біт та обчислюється HMAC для зміненого файлу, після цього робиться побітове порівняння отриманих дайджестів. Для практичного вживання MACу потрібно, щоб статистичні дослідження показали, що поєдина зміна символу приводить до зміни 40% бітів HMACу незалежно від розміру файлів, що генеруються [9].

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 (див. [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 напівгрупи 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 Гамаля. У випадку коротко представленого вище підходу до використання спеціальних підгруп афінних методик напівгрупи Кремони некомутативної криптографії у симетричній криптографії, таких як розробка потокових шифрів (див. [6, 34] та інші

посилання) і конструкції HMAC (див., наприклад, [35], де використовувалися спеціальні лінійні групи), ми використовуємо 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 (див. [13, 14] і розділ 6 нижче). Інші застосування теорії графів до криптографії розглядаються в [31].

Дослідження HMAC (і пов'язаних з ними HMACами) – гаряча галузь. Повний огляд опублікованих результатів з розробки цих засобів та їх криптоаналізу просто не можливий, 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 HMAC; отриманий алгоритм MAC називається HMAC-MD5 або HMAC-SHA-1 відповідно. Криптографічна ефективність HMAC залежить від криптографічної ефективності основної хеш-функції, розміру її хеш-виходу, а також від розміру і якості ключа.

4. Математичне підгрунтя хеш-функції, що пропонується

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

Наш алгоритм ґрунтується на наступному математичному твердженні.

Теорема [3]. Для кожного натурального m≥2 існує гомоморфне відображення $\psi : F'(K) \to S(K^m)$ 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 добутки обмежені числом 3. Ця група вже вживалася для побудови криптографічних алгоритмів з приватним ключем ([5, 6] та подальші посилання) та протоколів обміну ключами [4, 7, 10, 11].

Для створення MACу [9] було використано не саму групу G, а відображення ψ, що її визначає, разом з афінними A та B перетвореннями

групи Кремони за правилом $g: x \to A\psi(x)B$. 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 (розділ 6).

5. Пришвидшення алгоритмів

У цьому розділі 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» процедури обчислення значень гомоморфізму з теореми 1 попереднього розділу. Конструктивне визначення гомоморфізму ψ буде описане у розділі 6 у термінах відомих алгебраїчних графів з екстремальними властивостями. При цьому використана концепція лінгвістичних родин графів, що дозволяє вивчати спеціальні напівгрупу та групу, пов'язані з графами заданими системами алгебраїчних рівнянь.

Нехай $(a_1, a_2, ..., a_n)$ – 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 $i(1), i(2), ..., i(m-1)$ та невиродженої матриці M, складеної з елементів кільця лишків Z_{256}. Вони утворюють вектор $u = (v_1, v_2, ..., v_m)$, де $v_1 = a_1 + a_2 + ... + a_n, ..., v_j = v_{j-1} - a_{i(j-1)}$. Потім обчислюється кубічне відображення $F = \psi_m(a_1, a_2, ..., a_n)$, яке кореспонденти застосовують до вектора u. Отриманий вектор-рядок $F(u)$ множиться на матрицю M. Вектор $w = F(u)M$ вважаємо дайджестом документа.

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 $(a_1, a_2, ..., a_n)$ у вигляді конкатенації скінченної кількості слів $z_1, z_2, ..., z_t$ парної довжини. Потім обрати послідовність слів вигляду $u_1, u_2, ..., u_k$, де $u_i \in \{z_1, z_2, ..., z_t\}$ таку, що кожне z_i у цій послідовності зустрічається не менше ніж один раз. Далі обчислюється значення у добутку $u_1, u_2, ..., u_k$ 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 аффінної 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 файлу векторі. Зрозуміло, що розбиття а 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 (див. розділ 7) 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 родинами алгебраїчних графів з екстремальними властивостями.

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

Відсутні визначення теорії графів, які з'являються у даній статті, 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)◦V(G), і запишемо v G u для суміжних вершин u і v (чи сусідніх).

Позначимо |{ x ϵ V(G)| xGv }| 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. Ми будемо ідентифікувати I з простим графом цього відношення інцидентності або дводольного графа. Пара x, y, x ϵ P, yє 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 $x = (x_1, x_2,\ldots, x_s, x_{s+1}, x_{s+2}, \ldots, x_{s+m})$ належить прямій $y = [y_1, y_2, \ldots, y_r, y_{r+1}, y_{r+2}, \ldots, y_{r+s}]$ тоді і тільки тоді, коли виконується співвідношення:

$$a_1x_{s+1}+b_1\mathbf{y}_{r+1}=f_1(x_1, x_2,\ldots, x_s, y_1, y_2, \ldots, y_r)$$
$$a_2x_{s+2}+b_2\mathbf{y}_{r+2}=f_2(x_1, x_2,\ldots, x_s, x_{s+1}, y_1, y_2, \ldots, y_r, y_{r+1})$$

…

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

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, визначені нескінченним числом рівнянь.

У випадку лінгвістичного графа Г 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,..., 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 $i \in \{1,2,..m\}$.

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 $p_{2i} I l_{2i+1}$ 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 скейтбордах).

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

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

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

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

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

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

Лема 1. Відображення $\boldsymbol{\psi}={}^{I}\boldsymbol{\psi}$**:** ${}^{s}BS_r(K)\rightarrow S(K^n)$ є гомоморфізмом напівгруп.

Посилаємося на ${}^{I}\boldsymbol{\psi}({}^{s}BS_r(K))={}^{I}SR(K)$ як напівгрупу ланцюгових перетворень лінгвістичного графа I.

Ми визначаємо піднапівгрупу ${}^{s}S_r(K)$ гладких стрічок як сукупність смугастих стрічок $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_6,\ldots, H_{t-1}, H_t)$ z ${}^{s}BS_r(K)$ з $H_0=E_0$, $G_1=G_2$, $H_3=H_4$, $G_5=G_6,\ldots$, $H_{t-1}=H_t$. Будемо називати образ цієї напівгрупи ${}^{I}\boldsymbol{\psi}({}^{s}S_r(K)={}^{I}SW(K)$ 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 $Rev(u)=(H_{t-1}(H_t^{-1}), G_{t-2}(H_t^{-1}), G_{t-3},(H_t^{-1}), H_{t-4}(H_t^{-1}), H_{t-5}{}^{1}(H_t), \ldots, G_2(H_t^{-1}), G_1(H_t^{-1}), H_0(H_t^{-1}), H_t^{-1})$.

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

Лема 2. Гомоморфне зображення ${}^{I}\boldsymbol{\psi}({}^{s}BC_r(K))=IR_I(K)$ – підгрупа групи Кремони $C(K^n)$.

Дійсно, ${}^{I}\psi(u\cdot Rev(u)), u \in {}^{s}BC_r(K)$ – тотожне відображення.

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

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

7.1. Деякі означення екстремальної теорії графів

Обхват графа Г, позначаємо g = g(Г), – довжина найкоротшого циклу у Г. Діаметр d= d(Г) графа Г – максимальна довжина найкоротшого проходу між двома його вершинами.

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

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

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

Назвемо сімейство регулярних простих графів $Г_i$ ступеня k і порядку v_i як сімейство графів з великим індикатором циклу, якщо $Cind(Г_i) \ge \log_k(v_i)$ 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 (див. [15] та подальші посилання).

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 $K = F_q$ позначатимемо 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 відрізняти 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 їй алгебри Лі, що належить до класу алгебр Каца-Муді.

Вершини D(K) – нескінченні розмірні кортежі над K, ми запишемо їх наступним чином $(p)=(p_{0,1}, p_{1,1}, p_{1,2}, p_{21}, p_{22}, p'_{22}, p_{23}, \dots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \dots)$, $[l]=[l_{1,0}, l_{1,1}, l_{1,2}, l_{21}, l_{22}, l'_{22}, l_{23}, \dots, l_{i,i}, l'_{i,i}, l_{i,i+1}, l_{i+1,i}, \dots]$. 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 $i \ge 1$, ($p'_{1,1} = p_{1,1}$, $l'_{1,1} = l_{1,1}$).

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_{21}, p_{22},, p_{23}, …, $p_{i,i}$, $p_{i,i+1,...}$).

[l] = [$l_{1,0}$, $l_{1,1}$,$l_{1,2,,}$ l_{21}, l_{22}, l_{23}, … ,$l_{i,i}$, $l_{i,i+1,...}$] 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), … , (i-1, i), (i, i),… } є підмножиною D={(1, 0), (0; 1), (1, 1), (1, 2), (2; 2), (2, 2)',…, (i- 1, i); (i; i - 1); (i, i); (i, i)',…}. 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 ≥ 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 Δ(m) на вершинах графу D(m, K), посилаючись на його точку (p)є$K^{D(m)-\{(1,0)\}}$, обмежену у D(m)∩A-{(1,0)}, і його пряму [l] є$K^{D(m)-\{(0,1)\}}$, обмежену у D(m)∩A-{(0,1)}. Це відображення є гомоморфізмом D(m, K) на A(n, k), n=|D(m)∩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,… є сімейством великого обхвату для кожного параметра q, q>2 (див. [16] і подальші посилання). 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,…сімейством великого обхвату?» залишається відкритим.

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

Всі графи, визначені у 2 розділі, належать до класу L лінгвістичних графів Γ=Γ(K) типу (1, 1, n-1), nєN або n=∞. 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, … ,p_n)єP_n і [l]=[l_1, l_2, … , l_n]єL_n. утворює ребро Γ, якщо виконуються наступні умови ${}^{2}ap_2$ – ${}^{2}bl_2$=${}^{2}f(l_{1,}$ $p_1)$, ${}^{3}ap_2$–${}^{3}bl_2$=${}^{3}f(p_{1,}$ p_{12}, l_1 , l_2), … , ${}^{n}ap_n$ –${}^{n}bl_n$=${}^{n}f(p_{1,}$ p_2, …, p_n , l_1, $l_{2,\ ...}$, l_n), де ${}^{i}a$ і ${}^{i}b$, i≥2 елементи мультиплікативної групи K*, f_i поліноми від багатьох змінних. Визначимо кольори ρ((p)) і ρ([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 aєK.

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 поліноміальною 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 с. Зауважимо, що для більшості пара f ,g є $C(K^n)$ ступенів r і s їх наборів має ступінь rs. Тому ця проблема складна, вона має сильні криптографічні мотивації.

Розглянемо сукупність St(K) рядків виду $(f_1, f_{2,...}, f_k)$ де f_i є$K[x]$. Позначимо поліном f і відображення $x \to f(x)$ з S(K). Добуток двох послідовностей $(f_1, f_{2,...}, f_k)$ і $(g_1, g_{2,...}, g_t)$ є послідовність $(f_1, f_{2,...}, f_k, g_1(f_k), g_2(f_k), ..., g_t(F_k))$. 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 ∑(K) – підгрупа рядків парної довжини з координатами виду x+c, cєK.

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

Отже, можна визначити наступне символічне обчислення. Візьмемо символічну точку x=(x_1, x_2, …, x_n), де x_i є загальними змінними з K[x_1, x_2, …, x_n] і поліноміальним рядком CєSt'(K), який є кортежем многочленів f_1,, f_2,, ... , f_k, з K[x_1] з парним параметром k. (x=x_1). Утворюємо шлях вершин v_0,=x, v_1 так, що $v_1 I v_o$ 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 $K[x_1, x_2,..., x_n]^n$ графа Г'.

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

Наступні твердження наведені у [14].

Теорема 1. Відображення ${}^{\Gamma}\eta : C \to {}^{\Gamma}H(C)$ є гомоморфізмом St'(K) у напівгрупі Кремони $S(K^n)$.

Ми називаємо ${}^{\Gamma}\eta$ 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 розділі 5. Лі образ ${}^{\Gamma}\eta(St'(K))$ співпадає з напівгрупою ${}^{I}SW(K)$ символічних переходів на лінгвістичному графі I.

Неважко побачити, що ця напівгрупа ∑(K) є ізоморфною напівгрупі F'(K), визначеній у 1 розділі.

Теорема 2. Якщо Г – один з графів D(n, K) і A(n,K), то ${}^{\Gamma}\eta(\sum(K))$ є стабільною підгрупою $C(K^n)$ ступеня 3.

Як наслідок із цього твердження одержуємо теорему з розділу 1. При цьому виникає дві ефективні конструкції гомоморфізму ψ, а саме $\psi = {}^{D(n,K)}\eta$ та $\psi = {}^{A(n,K)}\eta$

Позначимо ${}^{\Gamma}\eta(\sum(K))$ для Г=D(n,K) і Г=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 розділі 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 ${}^{I}\boldsymbol{\psi}({}^{s}BC_{r}(K))=IR_{I}(K)$, 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, cєK. 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.

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 розділі 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.

Таблиця 1 – Швидкодія алгоритму створення дайджестів

Розмір файлу, Мегабайт	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	11,09	14,88	16,99	19,82
38,7	11,60	17,39	23,20	29,03	34,84	40,65	46,46
62,3	18,54	27,80	37,10	46,38	55,68	64,94	74,22
121,3	36,24	54,35	72,52	90,63	108,76	126,89	145,02
174,2	51,22	77,72	103,66	129,40	155,53	181,42	207,34

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

Частину модифікації базового алгоритму, описану у розділі 4, та деякі алгоритми з використанням груп $SIR_l(K)$, визначені у розділі 5, вже імплементовано. Проводяться комп'ютерні експерименти для оптимізації параметрів у відповідних програмах.

Висновки

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 – додатне ціле число. Алгоритми використовують нещодавньо знайдені гомоморфні відображення компресії напівгрупи потенційно нескінченних текстів у алфавіті K на скінченну групу кубічних поліноміальних перетворень m вимірного аффінного 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 $F_2^8, F_2^{16}, F_2^{32}$, кілець 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 аудіофайлів, фільму тощо. Розроблені методи створення дайджестів мають потоковий характер – швидкодія при сталому m лінійно залежить від n. Зростання n збільшує криптографічну стабільність. Імплементація у блоковому режимі можлива, але не вмотивована, бо розмір блоку обмежує кількість змінних системи нелінійних рівнянь.

Необхідність подальших досліджень і технологічних розробок зі створення нових залежних від ключа швидких хеш-функцій пов'язана із викликами кібербезпеки, зростанням глобального інформаційного простору, очікуванням 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 некомутативної криптографії для створення НМАСів. Вважаємо, що потрібна подальша робота з оптимізації побудованих алгоритмів, їх порівняння із відомими раніше НМАСами та криптоаналітичні дослідження.

СПИСОК ЛІТЕРАТУРИ

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 p.
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. Устименко В.А. Об экстремальной теории графов и символьных вычислениях // Докл. НАН Украины, 2012 – №11 – С. 15-21.
5. Пустовіт О., Устименко В., Про застосування алгебраїчної комбінаторики до проблем кодування та криптографії // Математичне моделювання в економіці, № 1-2. – Київ. – 2017. – С. 31-46.
6. Ustimenko V., Roma´nczuk-Polubiec U., Wr´oblewska 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. Устименко В.О., Пустовіт О.С. Про нову концепцію електронного підпису та засоби її реалізації, Колективна монографія за матеріалами XVI Міжнародно-практичної конференції. – м. Київ (Пуща-Водиця). – 2017. – С. 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. Устименко В.О., Пустовіт О.С. Про нові алгоритми аудиту електронних документів, їх імплементацію та застосування у кібербезпеці, Колективна монографія за матеріалами XVII Міжнародно-практичної конференції. – м. Київ (Пуща-Водиця). – 2018. – С. 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 (to appear)
11. U. Roma´nczuk-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. Bollob´as, ”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 (to appear).

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 Mathema Discrete Mathematics, N 43, pp. 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, WeiWang, 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) Difererentiability 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 onHMAC/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.

REFERENCES

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 p.
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 kombinatoryky do problem koduvannia ta kryptohrafii [On the application of algebraic combinatorics to the problems

of coding and cryptography] //Matematychne modeliuvannia v ekonomitsi, № 1-2. – Kyiv. – 2017. – s. 31-46.
6. Ustimenko V., Roma´nczuk-Polubiec U., Wr´oblewska 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 (to appear).
11. U. Roma´nczuk-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. Bollob´as, ”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 (to appear).
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 Mathema Discrete Mathematics, N 43, pp. 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,WeiWang, 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) Difererentiability 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 onHMAC/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.

Стаття надійшла до редакції 06.08.2018.