calculated according to the recurrent rules. When finding their optimal values, the Bellman principle is followed. The revealed properties of similarity, which are characteristic of the problems of this class, determine their universality, through which they are solved by the same method. Typically, dynamic programming is used to solve these problems. The study and use of this property in combinatorial optimization in the future will allow solving insoluble problems for solvable ones. Examples of some dynamic combinatorial optimization problems are given.

Key words: *combinatorial optimization, combinatorial configuration, dynamic combinatorial optimization problems, similarity of combinatorial optimization problems, objective function.*

Одержано 24.01.2019

УДК 519.1,514.128
DOI: 10.32626/2308-5878.2019-19.174-180

В. О. Устименко*,**, д-р фіз.-мат. наук, професор,
О. С. Пустовіт**

*Університет Марії Кюрі-Склодовської, м. Люблін, Республіка Польща,
**Інститут телекомунікацій і глобального інформаційного простору НАН України, м. Київ

ПРО НОВІ ПОТОКОВІ АЛГОРИТМИ СТВОРЕННЯ ДАЙДЖЕСТІВ ЕЛЕКТРОННИХ ДОКУМЕНТІВ З ВИСОКОРІВНЕВИМ АВАЛАНЧ ЕФЕКТОМ

Пропонується родина залежних від ключа швидких алгоритмів створення дайджестів електронних документів Комп'ютерна симуляція дозволяє дослідити високий рівень аваланч ефекту, що виникає. Нехай K — вільно обране скінчене комутативне кільце, m — додатне ціле число. Алгоритми використовують нещодавно знайдені гомоморфні відображення компресії функцій вільної напівгрупи потенційно нескінчених текстів у алфавіті K на скінчену групу кубічних поліноміальних перетворень m вимірного афінного простору K_m.

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

Для пришвидшення алгоритму дайджестом слова $p = (p_1, p_2, ..., p_n)$, $p_i \in K$ вважатимемо не саме кубічне перетворення $F = \psi(p)$, але його значення $F(w(p))$ на деякому за-

лежному від p векторі $w(p)$ деформоване множенням на псевдовипадкову матрицю M. 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}).

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

Необхідність подальших досліджень і технологічних розробок по створенню нових залежних від ключа хеш-функцій пов'язана із викликами кібербезпеки, зростанням глобального інформаційного простору, очікування появи квантового комп'ютера та розвитком технологій bitcoins, де потрібно хешувати вхідні дані довільного розміру, перетворюючи їх у послідовність бітів, що є дайджестом так званих blockchains. Запропоновані 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, автентифікаційні коди повідомлень, гомоморфізм компресії, високо нелінійна криптографія від багатьох змінних, некомутативна криптографія.*

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

Для задач виявлення кібератак, верифікації та автентифікації документів потрібні так звані залежні від ключів хеш-функції (автентифікаційні коди повідомлень або МАСи) які залежать. від гасла [2 с. 244–257]. 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 сертифіковано загальну хеш-функцію Купина, як новий державний стандарт України [1].

2. Вимоги до дайджесту документів. Криптографічно стабільна функція хешування f має забезпечувати: практичну неможливість вибору пари посилань x та z таким самим значенням хеш-функції. Для дайджесту документа, створеного залежною від ключа хеш-функцію (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.

3. 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 підпівгрупою всіх слів парної довжини. Позначимо $S(K^n)$ скінченну напівгрупу всіх поліноміальних відображень простору K^n в себе.

Наш алгоритм грунтується на наступному математичному твердженні.

Теорема. ([3]) Для кожного натурального $m \geq 2$ існує гомоморфне відображення $\psi : F'(K) \to S(K^m)$ таке, що його образ $\psi(F'(K))$ утворює групу G кубічних поліномів 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, визначе-

них за алгебраїчними графами з екстремальними властивостями [4]. Ці методи дозволяють отримати 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 протоколів обміну ключами [4, 7, 10].

Для створення МАСу [9] 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 — природній 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].

4. Пришвидшення алгоритмів. У доповіді на симпозіумі буде представлено модифікацію описаного алгоритму у випадку $K = Z_{256}$, що дозволяє зберегти (або ж поліпшити) рівень аваланч ефекту при значному підвищенні швидкодії.

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 документу.

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

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

1) можна представити слово $(a_1, a_2, ..., a_n)$ у вигляді конкатенації скінченої 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 y 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 файла векторі. Зрозуміло що розбиття a на підслова z_i та послідовність u_j слід вважати частиною спільного ключа для кореспондентів;
2) можна обчислювати v_1 як добуток виразів $2a_i + 1$ та отримувати v_i діленням v_{i-1} на $2a_{i(j-1)} + 1$;
3) у варіанті 2 можна замінювати v_i на його непарні степені $k, k < 128$. Тоді ці степені слід вважати параметрами ключа.

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

Висновки. Зазначимо, що добрі властивості функції компресії грунтуються на конструкціях гомоморфізмів нескінченної напівгрупи слів парної довжини у напівгрупи Кремони, дискретних динамічних систем, визначених родинами алгебраїчних графів з екстремальними властивостями та комп'ютерних моделях конденсованих систем.

Список використаних джерел:

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. Ustimenko V. On new symbolic key exchange protocols and cryptosystems based on hidden tame homomorphism. *Dopov. Nac. akad. nauk Ukraine.* 2018. N 10. P. 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*. Київ, 2017. № 3. 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. ACSIS*. 2018. Vol. 15. P. 397–405.
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. ACSIS.* 2018. Vol. 15. P. 387–390.
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. Ustimenko V., Klisowski M. On Noncommutative Cryptography with cubical multivariate maps of predictable density. *Proceedings of the 2019 Computing Conference.* London. July, 2019 (to appear).

ON NEW STREAM ALGORITHMS FOR GENERATING DOCUMENTS DIGESTS WITH HIGH AVALANCHE EFFECT

The family of key dependent algorithms for generating digests of electronic documents is proposed. Computer simulation allows to investigate high level of corresponding avalanche effect. Let K be a freely chosen finite commutative ring and m be a positive integer. Algorithm uses recently discovered homomorphic compression maps of free semigroup of potentially infinite texts written in the alphabet K onto finite group of cubic polynomial transformations of affine space K_m.

Cryptographic stability of proposed hash functions is connected with hard algebraic problems such as investigation of systems of algebraic equalities or decomposition of nonlinear map on free module into given generators.

To make algorithm faster instead of cubical transformation $F = \psi(p)$ we take as digest its value $F(w(p))$ on some depending from $p = (p_1, p_2, ..., p_n)$ word $w(p)$ additionally transformed by multiplication on pseudorandom matrix M. The algorithms are implemented in the cases of finite fields $F_2^8, F_2^{16}, F_2^{32}$, commutative ring Z_{256} and Boolean ring $B(32)$ of order 2^{32}.

Proposed algorithms can work with data in the form of texts, audio and video files, files with various extensions such as .avi, .tif, .pdf and etc. Algorithms can generate digests of already encrypted files, this option gives a possibility to check the integrity of files without their decryption. Suggested methods of digest generation have a stream nature, the speed for constant m is linearly dependent on variable n. Growth of n increases the cryptographic stability. The implementation in the form of block by block compression is possible but it has a lack of motivation because the size of the block restricts the number of variables in the system of nonlinear equations.

The necessity of a further research and technological solutions on the constructions of key dependent hash functions is caused by cybersecurity calls, the increase of global information space, expectations of quantum computers appearance and development of bitcoins technology, which requires hashing of data of arbitrary size with its transformation into sequences of bits which form digests of the so called blockchains. Proposed algorithms of generation of sensitive for changes of documents digests will be used for cyberattacks detection and for the auditing of all files after registered intrusion.

Key words: *cybersecurity, hash functions, message authentication codes, homomorphism of compression, highly nonlinear multivariate cryptography, noncommutative cryptography.*

Одержано 27.01.2019

УДК 519.6
DOI: 10.32626/2308-5878.2019-19.180-187

О. М. Хіміч, член-кореспондент НАН України, д-р фіз.-мат. наук,
В. А. Сидорук, канд. фіз.-мат. наук

Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ

ВИКОРИСТАННЯ МІШАНОЇ РОЗРЯДНОСТІ У МАТЕМАТИЧНОМУ МОДЕЛЮВАННІ

У роботі пропонується методика, за допомогою якої можна прискорити час математичного моделювання складних систем, використовуючи мішану розрядність в обчисленнях. Мішана розрядність дозволяє підвищити продуктивність обчислень, а також зекономити пам'ять. Показано застосування такого підходу при побудові алгоритму розв'язання систем лінійних алгебраїчних рівнянь з розрідженими матрицями.

Ключові слова: *математичне моделювання, мішана розрядність, паралельні алгоритми, розріджені матриці.*

Вступ. Проведення обчислень на довільній розрядності — один з основних інструментів підвищення ефективності програм і ідентифікації лінійних систем у комп'ютерному середовищі [1], зокрема,