Методи шифрування на основі зміни модулів системи залишкових класів

УДК 004.056.55
Соломія Марчук[1], Mikolaj Karpinski[2], Михайло Касянчук[3]

[1,3]Західноукраїнський національний університет,
[2]University of the National Education Commission, Poland;
[1]sol.marchuk@gmail.com, [2]mikolaj.karpinski@uken.krakow.pl,
[3]kasyanchuk@ukr.net

Ключовими аспектами кібербезбеки є забезпечення конфіденційності, цілісності та доступності інформації [1]. Для шифрування перспективним напрямом є використання непозиційних систем числення. У системі залишкових класів (СЗК) цілі числа представляються як набір залишків від ділення цього числа на попарно взаємнопрості модулі [2]. Метою нашої роботи є розробка методів шифрування на основі зміни модулів СЗК.

У СЗК відкритий текст у вигляді цілого числа N представлений за допомогою невід'ємних залишків b_i від ділення цього числа на модулі p_i:

$$b_i = N \bmod p_i. \tag{1}$$

Попередньо вибрані параметри p_i повинні бути додатними і попарно взаємнопростими. Обов'язковою умовою є те, що їх добуток $P = \prod_{i=1}^{s} p_i$, де s - кількість модулів, повинен перевищувати значення числа N.

Зворотне перетворення в десяткову систему числення здійснюється за допомогою китайської теореми про залишки (КТЗ):

$$N = \left(\sum_{i=1}^{s} m_i M_i b_i \right) \bmod P, \tag{2}$$

де $M_i = \frac{P}{p_i} = p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_s$ - добуток усіх модулів окрім і-го, коефіцієнти m_i є оберненими елементами за відповідними модулями і шукаються з конгруенцій:

$$m_i = M_i^{-1} \bmod p_i = \left(M_i \bmod p_i\right) - 1 \bmod p_i. \tag{3}$$

Із формули обчислення M_i випливає, що

$$(M_i m_i b_i) \bmod p_j = \{0, if\ i \neq j\ b_i, if\ i = j \tag{4}$$

Це означає, що кожен доданок в КТЗ (2) за модулем p_i рівний 0, окрім *i*-го, тому що M_i не містить в собі множника p_i.

В методі шифрування на основі зміни параметра M_{1i} обирається два набори модулів p_{1i} та p_{2i} таким чином, щоб кожен модуль з другого набору був більшим, ніж відповідний модуль з першого. Із цього випливає, що нові модулі

обов'язково більші, ніж залишки, отримані за модулями першого набору. При цьому набір p_{2i} повинен відповідати тим самим умовам, що і p_{1i}.

Для шифрування за допомогою КТЗ використовуються нові значення модулів p_i та параметрів M_i:

$$N' = \left(\sum_{i=1}^{s} m_{1i} M_{2i} b_{1i} \right) \bmod P_2 \quad . \tag{5}$$

При розшифруванні після ділення шифртексту N' на модулі p_{2i} отримуються змінені залишки b'_i. Істинні залишки обчислюються таким чином:

$$b_{1i} = (b'_i (m_{1i} M_{2i})^{-1}) \; mod \; p_{2i}. \tag{6}$$

Щоб отримати відкритий текст, потрібно знову використати КТЗ (2).

Для методу шифрування на основі зміни параметрів M_{1i} та m_{1i} аналогічно до попереднього обирається два набори модулів. Шифртекст отримується за допомогою КТЗ (2) при використанні нових значень p_i, M_i та m_i і набуває наступного вигляду:

$$N' = \left(\sum_{i=1}^{s} m_{2i} M_{2i} b_{1i} \right) \bmod P_2 \quad . \tag{7}$$

Оскільки m_{2i} та M_{2i} отримані з одного набору модулів, то при дешифруванні одразу отримуються значення початкових залишків b_{1i}. Відновлення відкритого тексту за допомогою КТЗ відбувається по модулях p_{1i}.

В методі шифрування на основі зміни одного модуля необхідно також обрати два набори, в яких відрізняється лише один модуль. Якщо перший набір складається із значень $p_{11}, p_{12}, p_{13}, \dots, p_{1s}$, а другий - з $p_{21}, p_{22}, p_{23}, \dots, p_{2s}$, то необхідно, щоб виконувались такі умови: $p_{21} > p_{11}, p_{12} = p_{22}, p_{13} = p_{23}, \dots, p_{1s} = p_{2s}$. Для шифрування рівняння КТЗ (2) набуває наступного вигляду:

$$N' = \left(\sum_{i=1}^{s} m_{2i} M_{1i} b_{1i} \right) \bmod P_2 \quad . \tag{8}$$

З рівності модулів випливає, що співвідношення (4) виконується для всіх елементів, крім першого рядка. Відновлення $b_{12}, b_{13}, \dots, b_{1s}$ відбувається за формулою (2). Значення b_{11} отримується за наступною формулою:

$$b_{11} = \left(\left(\sum_{i=1}^{s} b'_{1i} - \sum_{i=2}^{s} M_{1i} m_{2i} b_{1i} \right) \cdot (M_{11} m_{21})^{-1} \right) \bmod p_{21} \quad . \tag{9}$$

Обчисливши значення початкових залишків, відкритий текст можна відновити за допомогою КТЗ по модулях p_{1i}. Якщо змінити більше одного модуля, то при розшифруванні потрібно буде розв'язати систему діофантових рівнянь, в якій залишки b_i визначаються неоднозначно.

Дослідження підтвердило, що запропоновані методи забезпечують можливість ефективного шифрування та коректного відновлення відкритого тексту за рахунок властивостей КТЗ.

1. Chai, K. Y., & Zolkipli, M. F. (2021). Review on confidentiality, integrity and availability in information security. Journal of Information Security and Applications, 58, 102729.
2. Mohan Ananda P. Residue Number Systems: Theory and Applications. Birkhäuser. 2016. 351 p.

Вплив квантових обчислень на сучасну криптографію: загрози, виклики та напрямки розвитку постквантових алгоритмів

УДК 004.056.55

Михайло Касянчук[1], Юрій-Богдан Петренчук[2]

Західноукраїнський національний університет,
[1]kasyanchuk@ukr.net, [2]petrenchuk.yuriy@gmail.com

Сучасний розвиток квантових обчислень суттєво змінює модель загроз для криптографії. Алгоритми, які вважалися практично незламними для класичних комп'ютерів, можуть стати вразливими. Зокрема, алгоритм Шора забезпечує поліноміальний розв'язок задач факторизації великих чисел і обчислення дискретного логарифма, що створює загрозу для криптосистем RSA, DSA та ECC. Алгоритм Ґровера прискорює пошук у неструктурованих просторах, зменшуючи ефективну стійкість симетричних ключів завдяки квадратичному прискоренню. У результаті традиційні криптографічні підходи можуть втратити необхідний рівень безпеки у квантову епоху.

Вплив квантових обчислень на криптографію є одним із ключових викликів інформаційної безпеки XXI століття. Більшість сучасних криптографічних протоколів, що використовуються в Інтернеті, електронному урядуванні, банківських системах і блокчейн-інфраструктурі, базуються на математичних задачах, складність яких визначається обмеженнями класичних обчислень. Поява масштабованих квантових комп'ютерів змінює цю парадигму криптостійкості [1].

Алгоритм Шора, запропонований у 1994 році, дозволяє ефективно виконувати факторизацію великих чисел і обчислення дискретного логарифма на квантовому комп'ютері. Це означає, що криптосистеми на основі RSA та еліптичних кривих (ECDSA, ECDH) можуть стати вразливими після появи достатньо потужних квантових пристроїв. Дослідження показують, що для зламу RSA-2048 знадобляться тисячі логічних кубітів із корекцією помилок, хоча точні оцінки залежать від розвитку квантового обладнання.

Квантові обчислення впливають і на симетричну криптографію. Алгоритм Ґровера прискорює перебір ключів, зменшуючи складність атаки приблизно з