УДК 003.26

КВАНТОВИЙ КРИПТОАНАЛІЗ ГЕШ-ФУНКЦІЇ «КУПИНА»

А. С. Ткаченко[1,a]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

Проаналізовано криптографічну геш-функцію «Купина», яка визначена національним стандартом України ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функції гешування». Досліджено компоненти побудови геш-функції: схема Меркла-Дамгора, структура Девіса-Мейєра та схема Івена-Мансура.

Отримано результати по застосуванню алгоритму Гровера до геш-функції «Купина». Версія геш-функції, що використовує вхід довжини 512 біт, є вразливою у квантовій моделі. Стійкість версії геш-функції, що використовує вхід довжини 1024 біт, є відкритим питанням, враховуючи наявні порогові константи NIST.

Ключові слова: геш-функція «Купина», алгоритм Гровера

Вступ

У 2015 році геш-функція «Купина» прийнята в якості національного стандарту України ДСТУ 7564:2014 [1]. Геш-функція «Купина» позиціонується як стійка до атак у квантовій моделі. Але поява нових напрямків у створенні квантових алгоритмів під задачі криптоаналізу та вразливості деяких компонент геш-функції ставить під питання її стійкість у квантовій моделі.

1. Опис геш-функції «Купина»

Структура геш-функції «Купина» складається з ряду компонент, які необхідно проаналізувати для розуміння роботи криптопримітиву в цілому.

Структура Меркла-Дамгора

Структура Меркла-Дамгора [2], зображена на рис. 1, є методом побудови геш-функції, що має властивості:

- стійкість функції стиснення до атак колізії;
- стійкість до колізій в цілому.

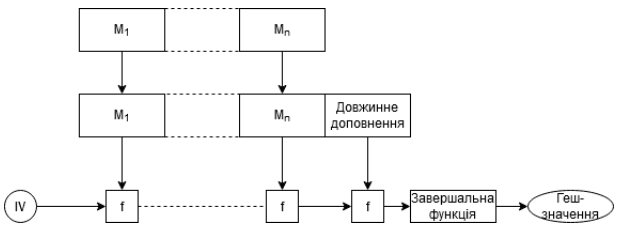

Рис. 1. Конструкція Меркла-Дамгора

Перед початком роботи потрібно доповнити повідомлення M до необхідної довжини. Після цього, доповнене повідомлення M' розбивається на умовлену кількість блоків однакової довжини. На кожній ітерації функція стиснення $f : V_l \to V_l$, де V_l – векторний простір розмірності l, приймає на вхід поточний блок повідомлення та результуючий блок із попередньої ітерації. Завершальним етапом є довжинне доповнення, що кодує довжину вхідного повідомлення M.

В кінці схеми, для кращого змішування та достатнього рівня лавинного ефекту, результат подається на обробку завершальній функції.

Структура Девіса-Мейєра

Структура Девіса-Мейєра – це одностороння функція стиснення [3, стор. 341], що будується на основі блокового шифру. Схема складається з блокового шифру E, на вхід якому подається блок повідомлення m_i та геш-значення H_{i-1} в якості ключа і блоку відкритого тексту відповідно. Геш-значення H_i обчислюється за формулою:

$$H_i = E_{m_i}(H_{i-1}) \oplus H_{i-1}$$

Робота схеми зображена на рис. 2.

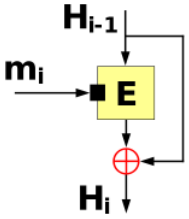

Рис. 2. Одностороння функція стиснення Девіса-Мейєра

[a] a123.tkachenko@gmail.com

Схема Івена-Мансура

Схема Івена-Мансура [4], що зображена на рис. 3, є стійким режимом блокового шифрування із мінімальною конструкцією. Під мінімальністю розуміється кількість елементів у схемі шифру, а під стійкістю – формально вірну оцінку знизу складностей атак на цей шифр.

Припустимо, задано множини $\mathcal{P}$, що є множиною відкритих текстів, та $\mathcal{C}$ – множина шифротекстів. Нехай є деяка обрана підстановка π із множини $S_{|\mathcal{P}|}$ ($S_{|\mathcal{P}|}$ – це множина всіх можливих підстановок над множиною $\mathcal{P}$) та визначена обернена підстановка π^{-1}. Перестановка будь-якого елементу із множини $\mathcal{P}$ та обернена перестановка будь-якого елементу із $\mathcal{C}$ легко обчислюється просто як значення відповідних підстановок.

Множини $\mathcal{P}$ та $\mathcal{C}$ задаються як двійкові послідовності довжини n: $\mathcal{P} \equiv \mathcal{C} = \{0,1\}^n$, а множина ключів, як двійкові вектори довжини $2n$: $\mathcal{K} = \{0,1\}^{2n}$. Особливість побудови схеми – це представлення секретного ключа K у вигляді кортежу із підключів $K = \langle K_1, K_2 \rangle$. Підключі обираються із імовірністю $\frac{1}{2^n}$ із множини $\{0,1\}^n$.

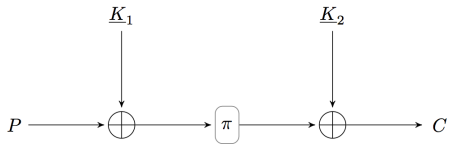

Рис. 3. Схема Івена-Мансура

Процедура шифрування відкритого тексту P з секретним ключем $K = \langle K_1, K_2 \rangle$ та підстановки π визначається формулою:

$$E_K(P) = E(P, \langle K_1, K_2 \rangle) = \pi(P \oplus K_1) \oplus K_2,$$

а розшифрування шифротексту C з секретним ключем K та оберненої підстановки π^{-1} визначається формулою:

$$D_K(C) = D(C, \langle K_1, K_2 \rangle) = \pi^{-1}(C \oplus K_2) \oplus K_1.$$

Опис геш-функції «Купина»

Геш-функція «Купина» – це ітеративна геш-функція, що побудована на основі структури Меркла-Дамгора, схеми Івена-Мансура та схеми Девіса-Мейєра.

На вхід подається повідомлення M у двійковому форматі. Нехай N – довжина повідомлення M. На початку роботи перевіряється чи N кратне l, де l – довжина блоків на які розбивається M. l обирається в залежності від довжини геш-значення n:

$$l = \begin{cases} 512, 8 \le n \le 256, \\ 1024, 256 < n \le 512, \end{cases}$$

де $n \in \{8 \cdot s \,|\, s = 1, 2, \ldots, 64\}$. Якщо N не кратне l, то M доповнюється до кратної довжини: $1 + d + bin(len(N))$, де $d = (-N - 97) \mod n$ нульових бітів, $bin(len(N))$ – це 96 бітів, що кодує довжину N. Після цього, доповнене повідомлення $M^{'}$ розділяється на k блоків: $M^{'} = M_0 || M_1 || \ldots || M_{k-1}$.

Геш-значення обчислюється за ітеративним алгоритмом:

1. $CV_0 \leftarrow IV$,
2. $CV_{i+1} \leftarrow CF(CV_i, M_i), i = \overline{0, k-1}$,
3. $h = Trunc(T_l^{\oplus}(CV_k) \oplus CV_k)$,

де $CF(CV_i, M_i)$ – функція стиснення, яка обчислюється за формулою:

$$CF_l(CV_i, M_i) = T_l^{\oplus}(CV_i \oplus M_i) \oplus T_l^{+}(M_i) \oplus M_i;$$

IV – вектор ініціалізації довжиною l біт, що залежить від l: $IV = 1 \ll 510$ при $l = 512$, $IV = 1 \ll 1023$ при $l = 1024$ $Trunc$ – функція, яка повертає n значущих біт із вхідного блоку повідомлення довжиною l ($l < n$), а результат записується в молодші n біт обчисленого значення.

У функції стиснення використовуються перестановки $T_l^{\oplus}$, T_l^{+} [1, стор. 6]. Перестановки є бієктивними відображеннями виду $T_l^{\oplus}, T_l^{+} : V_l \to V_l$, де $l = \{512, 1024\}$. Кожне відображення – це композиція функцій, що приймають в якості аргументу $x \in V_l$ матрицю розміром 8×8 ($l = 512$), або 16×16 ($l = 1024$). Елементи матриці належать полю $\mathbf{GF}(2^8)$ [1, стор. 5].

Робота геш-функції схематично представлена на рис. 4.

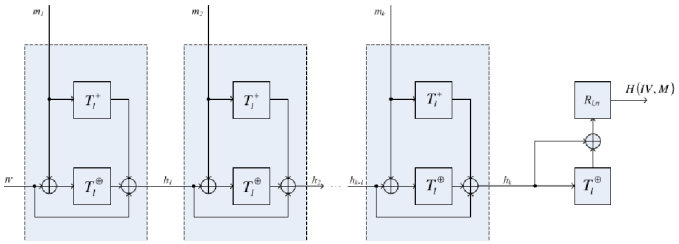

Рис. 4. Геш-функція «Купина»

2. Застосування алгоритму Гровера для криптоаналізу геш-функції «Купина»

Розглянемо задачу, яку розв'язує алгоритм Гровера [5] і проаналізуємо отримані результати по застосуванню даного алгоритму до геш-функції «Купина».

Алгоритм Гровера

Алгоритм Гровера – це алгоритм квантового пошуку. Алгоритм розв'язує *задачу пошуку*, що формулюється наступним чином.

Задача пошуку. Функція $f : \{0,1\}^n \to \{0,1\}$ визначена так: якщо $x \in \{0,1\}^n$ є розв'язком задачі пошуку, то $f(x) = 1$, інакше $f(x) = 0$. Необхідно знайти розв'язок x. У класичній моделі складність пошуку складає $\mathcal{O}(2^n)$. Тоді як у квантовій моделі, за допомогою алгоритму Гровера, задача розв'язується

за $\mathcal{O}(2^{\frac{n}{2}})$ запитів та $\mathcal{O}(n)$ пам'яті. Пошук за алгоритмом Гровера покращує складність розв'язку квадратично.

Результати застосування алгоритму Гровера до геш-функції «Купина»

Результати застосування алгоритму Гровера до геш-функції «Купина» оцінювалися за допомогою метрики NIST [6]. Криптопримітив вважається вразливим, якщо виконується нерівність:

$$GateCount \cdot MaxDepth \leq SecurityLevelConstant,$$

де $GateCount$ – це кількість використаних вентилів у схемі, $MaxDepth$ – максимальна глибина схеми. Константа $SecurityLevelConstant$ визначається в залежності від обраного рівня стійкості [6].

Для оцінки складності досліджувалось застосування алгоритму Гровера до одної ітерації геш-функції «Купина»:

$$CF(CV, M) = T_l^{\oplus}(CV \oplus M) \oplus T_l^{+}(M) \oplus M.$$

Основними компонентами складності є перестановки $T_l^{\oplus}$, T_l^{+}. Метод обчислення складностей перестановок представлений у роботі [7, стор. 56].

Застосовність алгоритму Гровера до геш-функції «Купина» визначалась за формулою:

$$\mathcal{O}(GateCount_l^{1round}) \times \mathcal{O}(MaxDepth_l^{1round}) \times \mathcal{O}(2^{\frac{n}{2}}),$$

де

- $\mathcal{O}(GateCount_l^{1round}) \times \mathcal{O}(MaxDepth_l^{1round})$ – складність реалізації одної ітерації геш-функції для входу довжини l,
- $\mathcal{O}(2^{\frac{n}{2}})$ – кількість викликів оракулу Гровера.

Отримані результати часової складності застосування алгоритму Гровера до геш-функції «Купина»:

- Вхід довжини 512 біт: $\mathcal{O}(2^{307.6})$,
- Вхід довжини 1024 біт: $\mathcal{O}(2^{566.6})$.

За цими результатами можна зробити висновки:

1) Версія геш-функції «Купина» із довжиною входу 512 біт є вразливою у квантовій моделі.
2) Вразливість геш-функції «Купина» із довжиною входу 1024 біт у квантовій моделі є відкритою проблемою, бо NIST не вводив значень $SecurityLevelConstant$ для такої довжини входу.

Висновки

Досліджено стійкість геш-функції «Купина» у квантовій моделі обчислень, використовуючи алгоритм Гровера. Отримані результати показують, що версія геш-функції «Купина» із довжиною входу 512 біт вразлива у квантовій моделі обчислень. NIST не вводив значення порогової константи $SecurityLevelConstant$ для довжини входу 1024 біт. Відповідно до цього, стійкість версії із довжиною входу 1024 біт поки є відкритим питанням.

Перелік використаних джерел

1. Інформаційні технології. Криптографічний захист інформації. Функція ґешування ДСТУ 7564:2014 / А. Бойко, І. Горбенко, Ю. Горбенко, О. Дирда, В. Долгов, О. Казимиров, О. Кузнецов, Р. Олійников, А. Пушкарьов, В. Руженецев. — 2014. — 35 с.
2. *Merkle R. C.* Secrecy, Authentication, and Public Key Systems. — 1979. — 182 с. — URL: http://www.ralphmerkle.com/papers/Thesis1979.pdf.
3. *Menezes A., Oorschot P. van, Vanstone S.* Handbook of Applied Cryptography. — 1996. — 815 с.
4. *Dunkelman O., Keller N., Shamir A.* Minimalism in Cryptography: The Even-Mansour Scheme Reviseted. — 2011. — URL: https://eprint.iacr.org/2011/541.pdf.
5. *Grover L. K.* A fast quantum mechanical algorithm for database search. — 1996. — arXiv: https://arxiv.org/abs/quant-ph/9605043.
6. *Langenberg B., Pham H., Steinwandt R.* Reducing the Cost of Implementing AES as a Quantum Circuit. — 2019. — URL: https://eprint.iacr.org/2019/854.pdf.
7. *Ткаченко А.* Квантовий криптоаналіз геш-функції «Купина». — 2021. — URL: https://ela.kpi.ua/bitstream/123456789/44256/1/Tkachenko_bakalavr.pdf.