УДК 681.3.06
DOI: 10.15587/2313-8416.2019.189617

ПРИМЕНЕНИЕ АЛГОРИТМА UMAC НА КРИПТО-КОДОВЫХ КОНСТРУКЦИЯХ В БЛОКЧЕЙН-ТЕХНОЛОГИЯХ

А. А. Гаврилова

Проведен вычислительный эксперимент по возможности использования крипто-кодовых конструкций Мак-Элиса с эллиптическими кодами на алгоритме UMAC для обеспечения реализации основных правил блокчейн-технологии при передаче конфиденциальной информации. Проанализировано результаты вычислений, сделан вывод о целесообразности практической реализации быстрого алгоритма хеширования для повышения уровня защищенности цепочки блоков технологии блокчейн
Ключевые слова: *блокчейн-технология, алгоритм UMAC, хеш-функция, крипто-кодовая конструкция, вычислительный эксперимент, эллиптические коды*

1. Введение

Интенсивное развитие информатизации ведёт к росту числа информационных систем (ИС) различного назначения. Количество зарегистрированных субъектов и объектов в ИС громадно. Такие ИС являются большими информационными системами (БИС). Количество БИС увеличивается. Этому способствует развитие таких технологий, как системы интернета вещей (Internet of Things, IoT) и блокчейн-технологии.

При удалённом электронном взаимодействии важно обеспечить процесс распознавания объекта по предъявленным параметрам (идентификаторам) и связанного с ним процесса аутентификации. Наиболее остро данная задача стоит в системах управления доступом и подтверждения аутентификации и верификации при передаче сообщений [1]. При постоянно увеличивающемся росте кибератак и разного рода мошенничеств, вопросы идентификации отправителя и получателя при их взаимодействии становятся особенно актуальными.

При обеспечении повышения криптостойкости алгоритмов шифрования сообщений для передачи по каналам связи, используются системы симметричного и асимметричного шифрования. Алгоритм RSA, основанный на эллиптических кривых и вычислительной сложности задачи факторизации больших чисел, на сегодня обеспечивает высокую криптостойкость передаваемых сообщений, за счет невозможности за вычислительное время провести расшифровывание этих сообщений. Но данный алгоритм стойкий лишь при существующих вычислительных мощностях, а при появлении высокопроизводительных квантовых компьютеров увеличится риск его взлома.

Поэтому важным направлением в развитии постквантовой криптографии сегодня являются крипто-кодовые системы (конструкции) (ККК). Их формирование основано на использовании алгебраических кодов, замаскированных под так называемый случайный код [2, 3]. ККК позволяют интегрировано реализовать быстрое криптографическое преобразование данных и обеспечить достоверность передаваемых данных на основе помехоустойчивого кодирования [3, 4].

2. Литературный обзор

Мировой опыт применения блокчейн очень полезен для Украины – с помощью блокчейн открываются новые возможности для устранения коррупционной составляющей при оказании услуг [5]. Но известны и другие применения технологии блокчейн в сфере человеческих коммуникаций, а именно: здравоохранение; строительство; банки; искусство; авиаперевозки; кибербезопасность; образование; Интернет вещей; прогнозирование; энергетика; торговля акциями; отслеживание цепочек поставок продуктов; туризм.

Технология блокчейн базируется на использовании хешей, которые предназначены обеспечить безопасность данной технологии. При получении конфиденциальной информации, осуществляя запуск алгоритма хеширования, можно вычислить xtш этих данных и сравнить его с тем, который передал отправитель. В случае несовпадения, можно утверждать, что информация претерпела изменения до ее получения.

Хеши в блокчейнах гарантируют необратимость всей цепочки транзакций. Каждый новый блок транзакций ссылается на хеш предыдущего блока в реестре. Хеш самого блока зависит от всех транзакций в блоке, но вместо того, чтобы последовательно передавать транзакции хеш-функции, они собираются в одно хеш-значение при помощи двоичного дерева с хешами (дерево Меркла) [6]. Таким образом, хеши используются как замена указателям в обычных структурах данных: связанных списках и двоичных деревьях. Свойство неизменности хеша одного блока определяет неизменность всего блокчейна.

Поэтому актуальной задачей на сегодня является повышение скорости криптопреобразований с

обеспечением требуемого уровня криптостойкости данного алгоритма. В работах [7] и [4] рассмотрены практические алгоритмы крипто-кодовых конструкций, которые обеспечивают их практическую реализацию за счет снижения мощности алфавита. Их применение в алгоритме UMAC позволит не только обеспечить требуемый уровень криптостойкости сформированного хеш-кода, но и сохранит его универсальность.

3. Цель и задачи исследования

Целью данной работы является определение возможности использования крипто-кодовых конструкций Мак-Элиса с эллиптическими кодами на алгоритме UMAC для обеспечения реализации основных правил блокчейн-технологии при передаче конфиденциальной информации.

В рамках поставленной цели должны быть решены следующие задачи:

– определены входные данные для реализации вычислительного эксперимента по использованию практического алгоритма UMAC на крипто-кодовых конструкциях при формировании блоков в блокчейн-технологии;

– разработаны этапы реализации алгоритма при формировании блоков в блокчейн-технологии;

– представлены и проанализированы результаты реализации алгоритма.

4. Материалы и методы исследований

В [8, 9] рассмотрена математическая модель аутентификации передаваемого сообщения на основании схемы Мак-Элиса на модифицированных эллиптических кодах с использованием модифицированного алгоритма UMAC.

Для определения целесообразности использования данной модели, необходимо провести вычислительный эксперимент. Проведение вычислительного эксперимента будет базироваться на практическом алгоритме UMAC на крипто-кодовых конструкциях, который представляет собой конечный набор правил, позволяющих осуществить практическую реализацию быстрого алгоритма хеширования с уровнем стойкости в постквантовой криптографии [10]. При этом подразумевается, что начальные исходные данные могут изменяться в определенных пределах, шаги по реализации алгоритма определены однозначно и на каждом шаге известно, что следует считать результатом.

4.1. Входные данные для проведения вычислительного эксперимента:

1 – Y_{L1I} значение универсальной хеш-функции (UHASH-hash) первого уровня хеширования

2 – Y_{L3I} значение хеш-функции (Carter-Wegman-hash) третьего уровня хеширования

3 – *T* блок данных

4 – *Blocklen* длина блока данных (байт)

5 – *Keylen* длина секретного ключа (*32* байта)

6 – *Tag* код контроля целостности и аутентичности

7 – K_{L1I} секретный ключ первого уровня хеширования, состоящий из подключей $K_1, K_2, \ldots, K_n$

8 – Y_{L3I} секретный ключ второго уровня хеширования, состоящий из ключей K_{L31} (подключи $K_1, K_2, \ldots, K_n$) и K_{L32} (подключи $K_1, K_2, \ldots, K_n$)

9 – *M* длина массива передаваемого открытого текста *i*

10 – K' псевдослучайная ключевая последовательность

11 – *Numbyte* длина псевдослучайной ключевой последовательности (количество подключей)

12 – *Index* номер подключа

13 – *I*=11 передаваемый открытый текст (*k*-разрядный информационный вектор над *GF*(*q*))

14 – *Xor* ($\oplus$)побитовое суммирование

15 – $x^3+y^2z+yz^2=0$ алгебраическая кривая над полем $GF(2^2)$

16 – *e*=00100200 **секретный вектор ошибок веса** $w_h(\mathrm{e}) \le \mathrm{t} = \left\lfloor \frac{d-1}{2} \right\rfloor$

17 – $X = \begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix}$ невырожденная $k \times k$ матрица

18 – $P = \begin{bmatrix} 0&1&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 1&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0 \end{bmatrix}$ перестановочная матрица размера $n \times n$

19 – $D = \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 0&2&0&0&0&0&0&0 \\ 0&0&3&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&2&0&0&0 \\ 0&0&0&0&0&3&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&1 \end{bmatrix}$ диагональная матрица, равная 1

20 – $G = \begin{bmatrix} 2&2&3&0&1&3&0&1 \\ 3&3&2&1&0&2&1&0 \end{bmatrix}$ порождающая матрица

21 – *I*=11 передаваемый открытый текст (*k*-разрядный информационный вектор над *GF*(*q*))

22 – Точки алгебраической кривой:

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9
X	0	0	0	1	2	3	1	2	3
Y	1	0	1	2	2	2	3	3	3
Z	0	1	1	1	1	1	1	1	1

23 – *K=0106* секретный ключ

24 – *Taglen* длина кода контроля целостности и аутентичности (достоверности) Pad_{Cx} (4 байта)

25 – *Nonce* **уникальное число для входного сообщения *I* (8 байт)**

26 – *Cx=23023322* криптограмма

$$27 - P^{-1} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \text{ матрица,}$$

обратная перестановочной матрице P (так как ее определитель равен 1, то $P^{-1} = P^T$)

$$28 - D^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \text{ матрица,}$$

обратная диагональной матрице D – унипотентная матрица (квадратная матрица, все собственные значения равны 1), которая сохраняет вес по Хэммингу вектора *e*

$$29 - X^{-1} = \begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix} \text{ матрица, обратная невырожденной матрице } X$$

4.2. Этапы реализации алгоритма

Кодирование открытого сообщения отправителя для передачи по каналам связи выполнялось на основании следующих процедур.

I процедура. Формирование хеш-кода в алгоритме UMAC. Указанные преобразования проводим параллельно с формированием кодограммы. Данная процедура является итеративной и складывается из трехслойной структуры: 1) Y_{L1M} – первый слой, который является значением функции UHASH-hash первого уровня хеширования; 2) Y_{L2M} – второй слой, который является значением функции POLY-hash второго уровня хеширования; 3) Y_{L3M} – третий слой, который является значением функции Carter-Wegman-hash третьего уровня хеширования.

II процедура. Формирование к**риптограммы (C_X) с учетом** одноразового сеансового секретного ключа *e*.

III процедура. Формирование псевдослучайной подкладки/подложки (*Pad*) для обеспечения криптостойкости алгоритма UMAC проводим с помощью функции *PDF*, причем различные части *Pad* можно будет использовать как дополнительный вектор инициализации.

IV процедура. Формирование кода контроля целостности и аутентичности кодограммы *Tag* рассчитывается на основании значений функций Y_{L3M} и *Pad*.

V процедура. Формирование значения суммарного кода достоверности передаваемого текста *(Y)* проведем на основании найденного значения хеш-кода Y_{L3M} и *Tag*.

Верификация хеш-кода на приемной стороне с использованием алгоритма UMAC осуществлялась следующим образом.

I процедура. Строим вектор, который является кодовым словом кода с порождающей матрицей *G*, искаженной не более чем в *t* разрядах.

II процедура. Получаем синдром ошибок S .

III процедура. Находим многочлен локатора ошибок ($\Lambda(x)$) с последующей локализацией ошибок по процедуре Ченя.

IV процедура. Определяем кратности ошибочных позиций, решив систему уравнений (расчет S').

V процедура. Получаем криптограмму C_X^* с учетом вектора ошибок e' .

VI процедура. C_X^* используется в качестве основы для формирования подложки по алгоритму UMAC.

Реализация алгоритма

Формализация показателей и результаты расчетов следующие:

$1 - Y_{L3M} = ((Y_{L1I} \bmod (2^{36} - 5)) \bmod 2^{32}) xor Y_{L32I} = 10000000010$

$2 - C_X = I \times G_X^{EC} + e = 23023322$

$3 - Pad = PDF(K, Nonce, Taglen) = 1101010$

$4 - Tag = Y_{L3M} \oplus Pad = 10001101100$

$5 - Y, Y^{'} = Y_{L3M} \oplus Tag = 1101110$

$6 - C_X^* = C_X \times D^{-1} \times P^{-1} = 22202221$

$7 - S = C_X^* \times H^T = 1,1,1,0,0,0$

$8 - \Lambda(x) = a_{00} + a_{10}x + y = 0 \quad x + y = 0$

$9 - S' = H \times e' = 00020003$

$10 - C_X^{'} = C_X^* + e' = 22222224$

5. Результаты исследований

Значения, полученные при проведении расчетов, согласно алгоритма UMAC на крипто-кодовых конструкциях, показывают, что при сравнении хеш-кодов, сформированных получателем и отправителем, их длины совпадают, а, следовательно, открытый текст получателя поступил к нему в неизменном виде. Поэтому данный механизм определения аутентичности сообщений возможно использовать не только на эллиптических кодах, но и модифицированных (укороченных, и/или удлиненных) эллиптических кодах, а также на ущербных кодах с использованием гибридных крипто-кодовых конструкций. Такой подход позволяет практическую реализацию быстрого алгоритма хеширования с заданным уровнем стойкости в постквантовой криптографии, что

повышает уровень защищенности цепочки блоков технологии блокчейн.

6. Выводы

Результат проведенной работы показал, что предложенный механизм обеспечивает заданный уровень аутентичности сообщений для обеспечения реализации основных правил блокчейн-технологии при передаче конфиденциальной информации.

В рамках поставленной цели были решены следующие задачи:

1) заданы 29 входных параметра, которые участвуют в формировании математической модели и вычислительном эксперименте по использованию практического алгоритма UMAC на ККК при формировании блоков в блокчейн-технологии;

2) определены этапы проведения вычислительного эксперимента по алгоритму при формировании блоков в блокчейн-технологии: **кодирование открытого сообщения отправителя для передачи по каналам связи** и верификация хеш-кода на приемной стороне с использованием алгоритма UMAC;

3) получены и интерпретированы результаты реализации алгоритма UMAC на ККК при формировании блоков в блокчейн-технологии.

Литература

1. Regulation (EU) No 910/2014 of the european parliament and of the council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (2014). Official Journal of the European Union. Brussels, 73–114.

2. Bernstein, D. J., Buchmann, J., Dahmen, E. (2009). Post-Quantum Cryptography. Berlin-Heidleberg: Springer-Verlag, 245. doi: http://doi.org/10.1007/978-3-540-88702-7

3. Кузнецов, А. А., Пушкарев, А. И., Сватовский, И. И., Шевцов, А. В. (2016). Несимметричные криптосистемы на алгебраических кодах для постквантового периода. Радиотехника, 186, 70–90.

4. Yevseiev, S., Kots, H., Minukhin, S., Korol, O., Kholodkova, A. (2017). The development of the method of multifactor authentication based on hybrid crypto-code constructions on defective codes. Eastern-European Journal of Enterprise Technologies, 5 (9 (89)), 19–35. doi: http://doi.org/10.15587/1729-4061.2017.109879

5. Гаврилова, А., Євсеєв, С. (2019). Аналіз стану захищеності блокчейн-проектів на ринку українських сервісів. Інтелектуальні системи та інформаційні технології. Одеса, 62–64.

6. What is a Merkle Tree and How Does it Affect Blockchain Technology References? Available at: https://selfkey.org/what-is-a-merkle-tree-and-how-does-it-affect-blockchain-technology Last accessed: 15.11.2017

7. Hryshchuk, R., Yevseiev, S., Shmatko, A. (2018). Construction methodology of information security system of banking information in automated banking systems. Vienna: Premier Publishing s. r. o., 284. doi: http://doi.org/10.29013/r.hryshchuk_s.yevseiev_a.shmatko.cmissbiabs.284.2018

8. Yevseiev, S., Korol, O., Havrylova, A. (2019). Development of authentication codes of messages on the basis of UMAC with crypto-code McEliece's scheme on elliptical codes. Information protection and information systems security. Lviv: Lviv Polytechnic Publishing House, 86–87.

9. Havrylova, A., Korol, O., Yevseiev, S. (2019). Development of authentication codes of messages on the basis of UMAC with crypto-code McEliece's scheme. International Journal of 3D printing technologies and digital industry, 3 (2), 153–170.

10. Korol, O., Havrylova, A., Yevseiev, S. (2019). Practical UMAC algorithms based on crypto code designs. Przetwarzanie, transmisja i bezpieczenstwo informacji. Vol. 2. Bielsko-Biala: Wydawnictwo naukowe Akademii Techniczno-Humanistycznej w Bielsku-Bialej, 221–232.

Received date 25.11.2019
Accepted date 10.12.2019
Published date 30.12.2019

Гаврилова Алла Андреевна, старший преподаватель, кафедра кибербезопасности и информационных технологий, Харьковский национальный экономический университет имени Семена Кузнеца, пр. Науки, 9А, г. Харьков, Украина, 61166
E-mail: alla.gavrylova@hneu.net