DOI 10.36622/VSTU.2022.25.1.010
УДК 004.056.55.

ИСПОЛЬЗОВАНИЕ МЕТОДА АУТЕНТИЧНОГО ШИФРОВАНИЯ ДЛЯ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ ОБЛАЧНОГО ХРАНИЛИЩА ДАННЫХ

О.В. Трубиенко, В.В. Филинов, П.И. Карасев, Д.А. Головченко

Аутентичное шифрования (когда проводится одновременное выполнение функций шифрования и взаимозависимостей) предназначено для обеспечения конфиденциальности, контроля целостности и достоверности данных. Стороны, которые имеют общие ключи, могут организовать не только шифрованный обмен сообщениями, но и осуществлять контроль целостности путем добавления имитовставок до сообщения, что позволяет убеждаться в приеме достоверного сообщения. Аутентичное шифрование обеспечивает определенную функциональную нить: ключи могут обновляться в процессе обработки данных; есть возможность шифровать только отдельные части сообщения или чередовать шифрованные и открытые сообщения; имитовставки могут отсутствовать или, наоборот, случаться несколько раз. Преимущественно алгоритмы аутентичного шифрования строят на базе блочных криптосистем, некоторые из них симулируют классический подход, исключая использование двух ключей, другие являются оригинальными конструкциями.

Ключевые слова: шифрование, защищенность, облачное хранилище, аутентичное шифрование.

Альтернативным подходом к построению алгоритмов аутентичного шифрования является использование конструкций типа *sponge* [1-2]. Конструкции *sponge* являются относительно новыми криптографическими способами, которые могут быть использованы для построения разнообразных криптографических алгоритмов. *Sponge*-функции относятся к *LRX*-классу криптографических преобразований и могут эффективно и с большей скоростью реализоваться на программируемых логических интегральных схемах, потому что в них задействованы только логические операции (*L*), циклические сдвиги (*R*) и XOR (*X*), что является интересным при современных скоростях телекоммуникаций [3-4].

В работе [5] предложена интересная *sponge*-функция *Bash-f*. Исследование и оценка новых решений в сфере криптографии, в частности алгоритмов аутентичного шифрования на базе *sponge*-функций, всегда являются актуальными в связи с возможным их применением для задач безопасности современного киберпространства.

Методы и средства криптографической защиты информации занимают важное место в системе обеспечения безопасности киберпространства. К современным средствам криптозащиты выдвигают определенные требования, прежде всего обоснованную устойчивость и быстродействие, которая отвечает современным требованиям. Все новые решения в области криптографии, которые предлагаются для практического использования, должны пройти соответствующие исследования.

На настоящее время в работах отечественных и зарубежных ученых не исследовались вопросы устойчивости в стандартных атак алгоритма аутентичного шифрования, на базе *sponge*-функции *Bash-f*. Целью статьи является исследование устойчивости алгоритма аутентичного шифрования с использованием *sponge*-функции *Bash-f*, а именно, получение оценки устойчивости криптоалгоритма к атакам, направленных на расшифровку шифротекста (восстановление ключа шифрования), и атак, направленных на нарушение целостности (подделки имитовставки).

Использование итерационных конструкций типа sponge является альтернативным подходом в построении алгоритмов аутентичного шифрования. В их основе лежит sponge-функция, которая определяет сложное биактивное преобразование над внутренним состоянием $S \in \{0,1\}^b$ конструкции. В состоянии S выделяют две части

$$S_r \in \{0,1\}^r \text{ и } S_c \in \{0,1\}^c,$$

такие что $b = r + c$ и $S = S_r \| S_c$. Часть S_r может быть известна как часть конструкции, а часть S_c держится в секрете. Различные значения r и c определяют компромисс между скоростью обработки данных и стойкостью конструкции: увеличение r с одновременным уменьшением c приводит к увеличению скорости и снижению устойчивости.

В работе [3] для sponge-алгоритмов предполагается, что ключ K сохраняется в тайне и выбирается случайно из вероятного множества $\{0,1\}^{|K|}$ и определены следующие требования безопасности (где A – открытые данные/заголовок, C – шифротекст, M– открытый текст, T – имитовставка):

Невозможность восстановления ключа. Вероятность нахождения нападающим ключа в атаке, в которой он может проверить n ключей, не превышает $n \cdot 2^{|K|}$.

Невозможность подделки имитовставки. При условии невозможности восстановления ключа вероятность успешного определения нападающим имитовставки для какой-либо пары (A,M) равна $2^{-|T|}$, даже когда нападающему известен шифротекст C, который соответствует (A,M), и выходным значениям (C_i,T_i) для адаптивно избираемых им входных значений (A_i,M_i), где $(A_i,M_i) \neq (A,M)$.

Невозможность восстановления открытого текста. Для нападающего наиболее эффективным методом получения какой-либо информации об M (за исключением информации о длине) по выходным значениям (C, T), соответствуют входные значения (A, M), где A выбирается нападающим, а M – неизвестная переменная, которая является восстановлением ключа, даже если нападающему известны выходные значения (C_i, T_i) для соответствующих им входных значений (A_i, M_i), где $A_i \neq A$.

Отметим, что требования относительно невозможности восстановления открытого текста базируется на том, что для фиксированного ключа не должно быть двух входов (A', M') и (A, M), где $A' = A''$ и $M' \neq M''$. Уникальность открытых данных для того же самого ключа является критическим с точки зрения криптографической стойкости.

Оценку устойчивости будем проводить в допущении, что базовое преобразование $\boldsymbol{F}$ *sponge*-функции *Bash-f* не отличается от случайного.

Основными параметрами, по которым оценивают алгоритм шифрования, как правило, является его устойчивость к атакам, направленных на расшифровку шифротекста (восстановление ключа шифрования), и быстродействие процесса шифрования. В итоге с алгоритмом аутентичного шифрования добавляется еще оценка его устойчивости относительно атак направлен на нарушение целостности (подделки имитовставки).

В основном оценивают устойчивость алгоритма как в известных атаках общего назначения (например, полный перебора ключевого пространства или *tradeoff*-атаки [6-8]), так и в базовых атаках, что разрабатываются специально под алгоритм.

Условия атаки относительно расшифровки (восстановление ключу шифрования) заключаются в том, что нападающий должен отличить случайную входную последовательность от зашифрованного на секретном ключе текста, при этом нападающий может обращаться как к генератору расшифровки (на вход генератора запрещено подавать входную последовательность, которую нужно отличить), так и к *sponge*-функции.

Условия атаки по нарушения целостности (подделки имитовставки) состоят в том, что нападающий должен подделать имитовставку заданного входного сообщению, при этом он может обращаться к генератору выработки имитовставки (нужно

подавать на вход исходное сообщение) или к *sponge*-функции.

Для оценки устойчивости аутентичного шифрования надо доказать, что нападавший не имеет существенных преимуществ в условиях проведения определенной атаки.

В случае, когда аутентичное шифрование используется для зашифрования известного открытого текста, то оно может рассматриваться как текущий алгоритм, который формирует гамму по блокам.

Tradeoff-атака относится к эффективным универсальным атакам на алгоритмы поточного шифрования [9]. Эта атака используется для обращения односторонней функции, то есть для обозначения неизвестного прообраза по известному образу. Такие односторонние функции отражают внутреннее состояние или ключ и синхронизацию алгоритма в выходную последовательность, которая называется префиксом [6]. Длина нужного префикса зависит от класса атаки. Если атака направлена на восстановление внутреннего состояния, то длина префикса должна равняться сумме длин ключа и синхронизации. Префиксы, которые используются в атаке, могут соответствовать тому самому ключу или разным ключам.

Атака состоит из двух этапов [7]:

– этап предварительных вычислений, на котором злоумышленник изучает алгоритм и в соответствии с ним создает определенные таблицы;

– этап реального времени (этап поиска решения), на котором отслеживаются выходные префиксы и восстанавливается внутреннее состояние или ключ с помощью таблиц созданных на первом этапе.

Tradeoff-атака характеризуется следующими параметрами [8]:

N – мощность множества внутренних состояний и ключей (мощность пространства поиска или размер области поиска);

P – время для этапа предварительных вычислений;

M – размер памяти, необходимый для хранения предварительно вычисленных таблиц (объем памяти, доступный злоумышленнику);

T – время для этапа реального времени;

D – количество префиксов, необходимых для проведения атаки;

ψ – вероятность успеха атаки.

Для того чтобы атака была успешной, параметры должны соответствовать определенному уравнению, которое зависит от класса атаки. Обычно рассматривают решение для уравнения с вероятностью успеха атаки $\psi = 0{,}63$.

Проведем анализ устойчивости алгоритма аутентичного шифрования к наиболее эффективным *tradeoff*-атакам.

Целью атаки является определение секретного ключа $K \in \{0,1\}^l$, где $l \in \{128,256\}$ – уровень устойчивости. Будем считать, что проводиться атака на алгоритм шифрования при известном открытом тексте (то есть при известной гамме). В таком случае нападающему будет неизвестна только часть $S(1571-2l...) \in \{0,1\}^{2l-8}$ пространства поиска $S \in \{0,1\}^{1563}$. В случае успешного восстановления значения пространства поиска S в некоторый момент времени t, легко можно и сам ключ.

В работе [9] рассмотрена *BG*-атака (Brute-Force атака или атака методом «грубой силы»), основанная на переборе всех возможных вариантов пароля и направленная на восстановление начального состояния. Уравнение компромисса *BG*-атаки имеет вид:

$$TM = N$$

где $M = D$, $P = M = N/D$. Одним из возможных решений уравнения есть

$$T = M = D = P = N^{1/2}.$$

В работе [10] предложена модификация классической *tradeoff*-атаки (обозначим ее как *BS*-атака). Данная атака направлена на восстановление первоначального состояния алгоритма. Уравнения *BS*-атаки имеет вид:

$$T \cdot M^2 \cdot D^2 = N^2,$$

где $P = N / D$, $1 \le D^2 \le T$, N – сочетание множества ключей. Одним из возможных решений для данного уравнения является

$$T=M=N1/2,\ D=N1/4,\ P=N3/4.$$

Атаки *BG* и *BS* направлены на восстановление внутреннего состояния. В случае, когда сумма длин ключа и синхронизации менее чем размер внутреннего состояния, применяются более

эффективные модификации таких атак. Например, в работе [6] предложена модификации атак *BG* и *BS*, которые направлены на восстановление ключа по префиксам, полученных на одном ключе, но на разных синхронизациях (данные атаки обозначим через *HBG* и *HBS*, соответственно). При длине ключа *k*, длине синхронизации *v* и мощности множества ключей *N* решениями для данных модификаций является:

$$(P, D, M, T) = (N^{1/2}, N^{1/2}, N^{1/2}, N^{1/2}), \quad (1)$$

где $P = 2^{(k+v)/2} < 2^k$ для $k > v$;

$$(P, D, M, T) = (N^{2/3}, N^{1/3}, N^{1/3}, N^{2/3}), \quad (2)$$

где $P = 2^{(k+v)/3} < 2^k$ для $k > 2v$;

$$(P, D, M, T) = N^{3/4}, N^{1/4}, N^{1/2}, N^{1/2}, \quad (3)$$

где $P = 2^{(k+v)/4} < 2^k$ для $k > 3v$.

Формулы (1) и (2) соответствуют *HBG*-атаке, а (3) – *BS*-атаке.

В работе [7] описана модификация *BS*-атаки (назовем ее *DK*-атака), которая направлена на восстановление ключа по префиксах, полученных на разных ключах и одинаковой синхронизации. Уравнения компромисса для такого вида атаки:

$$T \cdot M^2 \cdot D^2 = N^2$$

где $1 \le D^2 \le T$, $P=N/D$, N - мощность множества ключей. Одними из возможных решений для этого уравнения является:

$$(P, D, M, T) = (N^{2/3}, N^{1/3}, N^{1/3}, N^{2/3});$$
$$(P, D, M, T) = N^{3/4}, N^{1/4}, N^{1/2}, N^{1/2}).$$

В табл. 1 и 2 приведены характеристики некоторых *tradeoff*-атак в отношении исследуемого алгоритма для уровня устойчивости l = 128 и l = 256. Для *HBG*-атаки длина синхронизации v = l/2.

Таблица 1

Характеристики tradeoff-атак для уровня устойчивости l=128

Атака	*N*	*T*	*M*	*D*	*P*
BG	2248	2124	2124	2124	2124
BS	2248	2124	2124	262	2186
HBG	2192	296	296	296	296
DK	**2128**	**285.3**	**242.7**	**242.7**	**285.3**

Таблица 2

Характеристики tradeoff-атак для уровня устойчивости l=256

Атака	*N*	*T*	*M*	*D*	*P*
BG	2504	2252	2252	2252	2252
BS	2504	2252	2252	2126	2378
HBG	2384	2192	2192	2192	2192
DK	**2256**	**2170.7**	**285.3**	**285.3**	**2170.7**

Из приведенных данных видно, что наилучшие характеристики имеет *DK*-атака. Несмотря на то, что вычислительная сложность *DK*-атаки меньше, чем атаки «грубой силы», необходимые объемы памяти и количество префиксов для проведения успешной атаки являются достаточно большими. Поэтому его применение на практике является маловероятным.

Теперь рассмотрим устойчивость алгоритма по отношению к базовым атакам.

В работе [3] исследованы устойчивые *sponge*-функции относительно базовых атак, в которых априори нет никаких предположений относительно возможных атак на функцию $\boldsymbol{F}$.

В исследовании предполагалось, что нападающий может выполнить не более, чем β обращений к $\boldsymbol{F}$ (в т.ч. к $\boldsymbol{F}^{-1}$, если $\boldsymbol{F}$ является функцией). Устойчивость алгоритма была рассмотрена соответственно в таких базовых атаках:

– *Поиск путей*. Необходимо найти такой строку, которая после фазы ‘впитывания’ алгоритма получает заданное внутреннее состояние. Вероятность успеха атаки составляла $\beta^2 / 2^{c+2}$, если $\boldsymbol{F}$ – биекция.

– *Нахождение циклов*. Проводится поиск циклов в выходных последовательностях при корректных входных данных. Вероятность успеха атаки составляла $\beta^2 / 2^{c+r+1}$, если $\boldsymbol{F}$ – не биекция.

– *Восстановление состояния*. Для заданной строки Z проводится восстановление соответствующего состояния S. Вероятность успешной атаки составила $\beta / 2^c$.

– *Связывание выхода*. Для заданной строки Z производится поиск такого состояния S, который выдает соответствующий выход. При этом не гарантируется, что такое состояние

существует. Вероятность успешной атаки составила $\beta / 2^{|Z|-r}$.

– *Внутренняя коллизия.* Проводится поиск таких двух строк, что в результате совершения этапа «впитывания» получается одинаковые внутренние состояния (внешние состояния могут отличаться). Вероятность успеха атаки составила $\beta^2 / 2^{c+1}$.

Уязвимость *sponge*-функции в таких атаках обусловлена тем, что состояние конечные, поэтому атаки не способны к внешнему воздействию. Вероятность успеха базовых атак задают оценки сверху на устойчивость *sponge*-функции. Минимальное число β обращений к $\boldsymbol{F}$ для одной успешной атаки составляет $O(2^{c+2})$.

Для режимов, что зависит от ключа, рассматриваются следующие атаки.

– *Прогнозирование гаммы.* После завершения успешной атаки по восстановлению текущего состояния по известной части исходной гаммы прогнозируется другая часть гаммы. Ожидаемое число обращений к $\boldsymbol{F}$ составила $2^{c/2}$, а при $l \le c$ атака вообще не несет угрозы.

– *Подделка имитовставки*. После успешного проведения атаки по восстановлению текущего состояния может быть проведена подделка имитовставки для нового сообщения при наблюдении наборов пар «сообщения+имитовставка» – «имитовставка». Ожидаемое число обращений к $\boldsymbol{F}$ составляла $2^{r+c-n}/(m+1)$, где m – число наблюдательных сообщений, а n – длина имитовставки. При $l \le c - \log_2(m)$ атака не представляет угрозы. При $m = 2^{c/2}$ получена оценка $c \ge 2l$. Другой способ подделки имитовставки заключается в поиске внутренней коллизии ключевой sponge-функции. Ожидаемое число наблюдательных блоков составляет $2^{c/2}$. После определения внутренней коллизии имитовставки могут быть легко рассчитаны.

Полученные результаты об устойчивости исследуемого алгоритма аутентичного шифрования как универсальной *tradeoff*-атаки, так и базовых атак для конструкций *sponge* подтверждают, что он является устойчивым. Учитывая полученные ранее оценки быстродействия реализации этого алгоритма [10], можно утверждать, что этот класс алгоритмов базы *sponge*-функции $\boldsymbol{F}$ может быть перспективным для использования при создании защищенного киберпространства.

Список литературы

1. Митяков А.В. Разработка методологий ориентированных на архитектуру облачных хранилищ данных / А.В. Митяков, Ю.С. Татаринов // Информационные технологии моделирования и управления. 2011. № 2. С. 221-227.

2. Земцов И.А. Использование семантической сети для выбора знаний с целью обеспечения информационной безопасности интеллектуальных систем / И.А. Земцов, О.Г. Иванова, Ю.В.Минин, С.В. Данилкин // Информация и безопасность. 2020. Т. 23. Вып. 2. С. 261–268.

3. Гомаш М. Генерация Пуасонновского ключа с помощью криптосистемы для безопасности облачного хранилища данных / М. Гомаш, С. Прасанна // Журнал перспективных исследований в области динамических систем и систем управления. 2018. №10. С. 804–817.

4. Громов Ю.Ю. Размещение узлов сетевой информационной системы с комбинаторной топологией с целью повышения эффективности защиты информации в условиях неопределенности / Ю.Ю. Громов, Ю.В. Минин, С.А. Копылов // Информация и безопасность. 2019. Т. 22. Вып. 2. С. 272–279.

5. Максимовский А.Ю. О выборе параметров автоматных моделей мониторинга информационной безопасности сетевых объектов (часть 2) / А.Ю. Максимовский // Информация и безопасность. 2020. Т. 23. №. 3. С.327-336.

6. Хан К. Смена обмена данными по безопасности и эффективности для облачного хранилища / К. Хан, К. Ли, З. Дэн // Хаос. 2016. № 86. С. 107–116.

7. Арки О. Многоагентная среда безопасности для облачного хранилища данных / О. Арки, А. Зитуни //

Мультиагентные и сетевые системы. 2017. №14 (4). С. 357–382.

8. Громов Ю.Ю. Построение непрерывных законов распределения для оценки рисков в информационных системах / Ю.Ю. Громов, Ю.В. Минин, В.Е. Дидрих, Н.Г. Шахов, С.А, Копылов // Информация и безопасность. 2019. Т. 22. Вып. 1. С. 86–91.

9. Громов Ю.Ю. Формализованное представление и классификация конфликтов тренажной подготовки операторов эрготехнических радиоэлектронных средств / Ю.Ю. Громов, И.Н. Ишук, А.Н. Потапов // Приборы и системы. Управление, контроль, диагностика. 2019. Вып. 2. С. 44–50.

10. Симановский Е.А. Метод повышения безопасности передачи данных в сети интернет / Е.А. Симановский, М.А.Макаров // Информатизация образования и науки. 2021. № 2. С. 22–36.

МИРЭА – Российский технологический университет
MIREA – Russian Technological University

Поступила в редакцию 20.11.2021

Информация об авторах

Трубиенко Олег Владимирович – канд. техн. наук, доцент, МИРЭА – Российский технологический университет, e-mail: trubienko@mirea.ru

Филинов Владимир Викторович – д-р техн. наук, профессор, МИРЭА – Российский технологический университет, e-mail: filinov@mirea.ru

Карасев Павел Игоревич – канд. техн. наук, МИРЭА – Российский технологический университет, e-mail: karasev@mirea.ru

Головченко Дарья Андреевна – аспирант, МИРЭА – Российский технологический университет, e-mail: golovchenko@mirea.ru

USING THE AUTHENTIC ENCRYPTION METHOD TO INCREASE THE SECURITY OF CLOUD DATA STORAGE

O.V. Trubienko, V.V. Filinov, P.I. Karasev, D.A. Golovchenko

Authentic encryption (the simultaneous execution of encryption functions and mutual dependencies is carried out) is designed to ensure confidentiality, control the integrity and reliability of data. The parties who have shared keys can organize not only an encrypted message exchange, but also carry out integrity control by adding imits before the message, which allows you to make sure that a reliable message is received. Authentic encryption provides a certain functional thread: keys can be updated during data processing; it is possible to encrypt only individual parts of the message or alternate encrypted and open messages; there may be no extensions or, conversely, occur several times. Mostly authentic encryption algorithms are built on the basis of block cryptosystems: some of them simulate the classical approach, excluding the use of two keys, others are original designs.

Keywords: encryption, security, cloud storage, authentic encryption.

Submitted 20.11.2021

Information about the authors

Oleg V. Trubienko – Candid. Sc. (Technical), MIREA – Russian Technological University, e-mail: trubienko@mirea.ru

Vladimir V. Filinov – Dr. Sc. (Technical), professor, Tambov State Technical University, e-mail: filinov@mirea.ru

Pavel I. Karasev – Cand. Sc. (Technical), MIREA – Russian Technological University, e-mail: karasev@mirea.ru

Daria A. Golovchenko – postgraduate., MIREA – Russian Technological University, e-mail: golovchenko@mirea.ru