УДК 519.1

ОБ ОЦЕНКЕ СТОЙКОСТИ AEAD-КРИПТОСИСТЕМЫ ТИПА GCM

А. Ю. Зубов

Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия

Обсуждается методика доказуемой стойкости криптосистем, обеспечивающих конфиденциальность и аутентичность информации. Предлагается упрощённый вариант известной оценки доказуемой стойкости AEAD-криптосистемы GCM с вектором инициализации фиксированной длины. В тех же условиях получена оценка доказуемой стойкости модификации GCM. Приводится сравнительный анализ криптосистем.

Ключевые слова: *AEAD-криптосистема, GCM, доказуемая стойкость.*

DOI 10.17223/20710410/32/4

ON THE SECURITY OF AEAD-CRYPTOSYSTEM OF THE GCM TYPE

A. Yu. Zubov

Lomonosov Moscow State University, Moscow, Russia

E-mail: Zubovanatoly@yandex.ru

A provable security methodology for the cryptosystems ensuring information privacy and authenticity is discussed. A simplified version of the well-known estimates for the provable security of the AEAD-cryptosystem GCM with an initialization vector of fixed length is proposed. Under the same conditions an estimate for the provable security of GCM modification is obtained. A comparative analysis of the considered cryptosystems is provided.

Keywords: *AEAD-cryptosystem, GCM, provable security.*

1. Необходимые сведения

Пусть $G = \{f : S \to A\}$ — семейство функций, $|S| = k$, $|A| = n$, $n < k$, $|G| = b$. Назовём G $(b; k, n)$-*семейством функций*. Нас будет интересовать свойство функций f из G иметь коллизии, под которыми понимается совпадение $f(s_1)$ и $f(s_2)$ для различных элементов s_1, s_2 из S.

Определение 1. Пусть $A = \{0,1\}^n$; $(b; k, n)$-семейство G называется εXOR-*универсальным* (кратко — εXU-*семейством*), если для любых $s_1, s_2 \in S$ и любого $a \in A$ справедливо неравенство

$$|\{f \in G : f(s_1) \oplus f(s_2) = a\}| \leqslant \varepsilon b.$$

Система MAC типа Wegman — Carter (WC-MAC) основана на εXU-семействе функций. Известно большое число таких систем. Нам понадобятся введённые в [1] системы $WC[G]$ и $WC[G, F]$.

Определение 2. Пусть $G = \{f : S \to \{0,1\}^n\}$ — семейство функций и $P = p_1, p_2, \ldots$ — случайная равновероятная строка векторов $p_i \in \{0,1\}^n$. Пусть cnt — целочисленная переменная (счётчик). Система $WC[G]$ снабжает сообщение $s \in S$ на ключе $\{f, P\}$ меткой $\tau = (cnt, p_{cnt} \oplus f(s))$. Для проверки аутентичности сообщения (s, τ), где $\tau = (i, r)$, вычисляется сумма $p_i \oplus f(s)$, которая сравнивается с r. Совпадение — критерий аутентичности.

Определение 3. Пусть $F : \{0,1\}^k \times \{0,1\}^l \to \{0,1\}^n$ и $G = \{f : S \to \{0,1\}^n\}$ — семейства функций. Пусть cnt — целочисленная переменная (счётчик). Система $WC[G, F]$ снабжает сообщение $s \in S$ меткой $\tau(s) = (cnt, F_K(cnt) \oplus f(s))$, где cnt — текущее значение счётчика, $K \in \{0,1\}^k$, $f \in G$. Ключом служит пара (K, f). При аутентификации каждого следующего сообщения алгоритм генерации MAC увеличивает значение cnt и проверяет условие $cnt < 2^n - 1$. Если неравенство не выполняется, то изменяется значение ключа. Если выполняется, то вычисляется метка по указанной формуле. Для верификации сообщения $(s, \tau(s))$, где $\tau(s) = (i, r)$, проверяющий вычисляет сумму $F_K(i) \oplus f(s)$ и сравнивает её с r. Равенство — критерий аутентичности.

Реализуемые системами $WC[G]$ и $WC[G, F]$ семейства функций можно рассматривать как псевдослучайные семейства функций (PRF). Мерой их псевдослучайности служит свойство неотличимости случайно выбранного представителя семейства от случайной функции по входам-выходам. *Случайной* называется функция, значение которой от любого аргумента выбирается случайно и равновероятно из её области значений. Другими словами, это функция, выбранная из семейства функций $\mathrm{Rand}^{S \to A}$ всех функций $S \to A$ случайно равновероятно. В рассматриваемом случае $A = \{0,1\}^n$. Количественно указанное свойство неотличимости произвольного семейства функций $\Phi = \{f : S \to A\}$ определяется следующим образом. Проводится атака различения, в которой принимают участие *различитель* и *оракул*. Различитель $\mathbf{A}$ (вероятностный алгоритм) может обращаться к оракулу O^{φ} функции $\varphi : S \to A$ с запросами относительно выбранных аргументов x из S, получая от оракула значения $\varphi(x)$. На основании полученных ответов $\mathbf{A}$ решает, какая гипотеза имеет место:

— W_0 : функция φ выбрана случайно равновероятно из $\mathrm{Rand}^{S \to A}$;
— W_1 : функция φ выбрана случайно равновероятно из Φ.

Выбор W_0 или W_1 произведён заранее, до начала обмена вопросами и ответами.

Результатом работы алгоритма $\mathbf{A}$ является различающий бит d, равный 0, если $\mathbf{A}$ делает выбор в пользу W_0, и 1 в противном случае. Эффективность работы различителя $\mathbf{A}$ определяется величиной $\mathrm{Adv}^{\mathrm{prf}}_{\Phi,\mathbf{A}}$, называемой *prf-преимуществом* семейства Φ для различителя $\mathbf{A}$. Она определяется формулой

$$\mathrm{Adv}^{\mathrm{prf}}_{\Phi,\mathbf{A}} = \left|\mathsf{P}\left[d = 1 | W_0\right] - \mathsf{P}\left[d = 1 | W_1\right]\right|, \tag{1}$$

представляющей собой модуль разности условных вероятностей того, что различающий бит равен 1, при условии, что имеет место гипотеза W_0 или W_1.

При теоретико-информационном подходе затраты различителя не учитываются.

Определение 4. Семейство функций Φ называется *ε-псевдослучайным*, если величина

$$\mathrm{Adv}^{\mathrm{prf}}_{\Phi} = \max_{\mathbf{A}} \left\{\mathrm{Adv}^{\mathrm{prf}}_{\Phi,\mathbf{A}}\right\},$$

в которой максимум берётся по всем различителям $\mathbf{A}$, удовлетворяет неравенству $\mathrm{Adv}^{\mathrm{prf}}_{\Phi} \leqslant \varepsilon$. Величина $\mathrm{Adv}^{\mathrm{prf}}_{\Phi}$ называется *prf-преимуществом семейства* Φ.

При теоретико-сложностном подходе величина prf-преимущества зависит от объёма затрат. К ним относятся число запросов к оракулу, их общий объём и время работы, под которым понимается действительное время выполнения алгоритма.

Определение 5. Для любых $t, q, \mu \in \mathbb{N}$ prf-преимущество семейства Φ — это максимум

$$\mathrm{Adv}_{\Phi}^{\mathrm{prf}}(t, q, \mu) = \max_{\mathbf{A}} \left\{ \mathrm{Adv}_{\Phi, \mathbf{A}}^{\mathrm{prf}} \right\}$$

по всем различителям $\mathbf{A}$, имеющим временную сложность t и использующим не более q запросов к оракулу, суммарная длина которых не превосходит μ битов. Φ называется $\varepsilon(t, q, \mu)$-*псевдослучайным*, если выполняется неравенство $\mathrm{Adv}_{\Phi}^{\mathrm{prf}}(t, q, \mu) \leqslant \varepsilon$. Чем меньше ε (при допустимом объёме затрат), тем «более псевдослучайным» является семейство Φ (и тем более стойким к атаке различения).

Аналогично определяется *prp-преимущество* $\mathrm{Adv}_{\Phi}^{\mathrm{prp}}$ семейства подстановок Φ.

Замечание 1. Prf-преимущество семейства функций определяется как prf-преимущество «лучшего» различителя. Если для некоторого различителя выражение под модулем в (1) отрицательно, то для различителя, который принимает противоположный различающий бит, это выражение будет положительным. Второй различитель «лучше» первого. Поэтому, оценивая преимущество семейства функций, можно опускать модуль в определении (1), что обычно и делается.

Замечание 2. Различитель характеризуется набором вероятностей принять различающий бит 1 для каждой последовательности запросов $\overline{x}$ и последовательности $\overline{y}$ ответов на них. Для семейства Rand всех функций для каждого $\overline{x}$ допустим какой угодно $\overline{y}$. «Хороший» различитель семейства Φ ограничивает для каждого $\overline{x}$ число вариантов $\overline{y}$, для которых указанная вероятность отлична от нуля. Поэтому гипотезам W_1 и W_0 отвечают разные распределения вероятностей, P_U и P_V, принять различающий бит 1 на множестве M возможных пар $(\overline{x}, \overline{y})$. Пусть для «лучшего» различителя такими распределениями $\mathsf{P}_U, \mathsf{P}_V$ на (конечном) множестве M определены случайные переменные U и V. Тогда, как показано, например, в [2], преимущество «лучшего» различителя можно записать в виде

$$\max_{f: M \to \{0,1\}} \left| \mathsf{P}\left[f(U) = 1\right] - \mathsf{P}\left[f(V) = 1\right] \right| = 0{,}5 \sum_{m \in M} \left| \mathsf{P}_U(m) - \mathsf{P}_V(m) \right|,$$

где максимум берётся по всем отображениям из M в $\{0, 1\}$. Правая часть этого равенства называется *расстоянием по вариации* (или *статистическим расстоянием*) между распределениями $\mathsf{P}_U, \mathsf{P}_V$. Это равенство даёт другое представление о понятии преимущества.

Определение 6. Система MAC называется ε-*стойкой*, $0 < \varepsilon < 1$, если противник, наблюдая ряд аутентифицированных (на одном ключе, выбранном случайно равновероятно) сообщений, может составить новое аутентифицированное (на том же ключе) сообщение с вероятностью, не превосходящей ε.

Утверждение 1. Пусть G — это εXU-семейство функций. Тогда система MAC $WC[G]$ является ε-стойкой.

Доказательство. Пусть противник имеет сообщения $(s_1, \tau_1), \ldots, (s_q, \tau_q)$, где τ_i — метки, полученные системой $WC[G]$ при использовании ключа (f, P). Оценим вероятность того, что противник сможет составить новое сообщение s^* и снабдить его меткой τ^*, полученной на том же ключе для подходящего значения счётчика — i^*.

Противник обязан произвести значение счётчика — i^*. При этом имеется две возможности: $i^* \leqslant q$ и $i^* > q$. Если $i^* > q$, то p_{i^*} — случайный вектор, не коррелирующий с наблюдаемыми значениями. Поэтому сумма $p_{i^*} \oplus f(s^*) = \tau^*$ также представляет собой вектор, выбранный случайно. Значение τ^* противник может лишь угадать с вероятностью 2^{-n}. Пусть $i^* \leqslant q$. Это означает, что противник выбирает значение счётчика, использованное ранее при вычислении метки τ_{i^*} сообщения s_{i^*}. Теперь ему нужно произвести $s^* \neq s_{i^*}$ и τ^*, такие, что

$$\tau^* = f\left(s^*\right) \oplus p_{i^*} = f\left(s_{i^*}\right) \oplus p_{i^*} = \tau_{i^*}.$$

Из этих соотношений получаем равенство $f(s^*) \oplus f(s_{i^*}) = \tau^* \oplus \tau_{i^*}$.

Пусть $c = \tau^* \oplus \tau_{i^*}$. Поскольку G образует εXU-семейство, имеем неравенство

$$\mathsf{P}\left[f\left(s^*\right) \oplus f\left(s_{i^*}\right) = c\right] \leqslant \varepsilon.$$

Таким образом, и искомая вероятность не превосходит ε. ■

Усилим утверждение 1, предоставив противнику возможность аутентифицировать адаптивно подобранные сообщения и проверить корректность их меток.

Утверждение 2. Пусть G — это εXU-семейство функций. Тогда при использовании не более чем q запросов к оракулу проверки метки и к оракулу генерации метки система $WC[G]$ является εq-стойкой.

Доказательство. В серии подделок (s_i, τ_i), $i \geqslant 1$, успех в атаке определяется путём запросов к оракулу проверки метки. Перед каждым таким запросом допускаются запросы к оракулу генерации метки относительно подобранных сообщений.

Пусть U_i — событие, означающее неуспех в подделке при i-м запросе к оракулу проверки метки. Если имеет место событие $U_1 \cap \ldots \cap U_i$, то, согласно утверждению 1, вероятность успеха следующей подделки ограничена ε. Поэтому имеет место неравенство

$$\mathsf{P}\left[U_{i+1} \middle| \left(U_1 \cap \ldots \cap U_i\right)\right] \geqslant 1 - \varepsilon.$$

Поскольку

$$\mathsf{P}\left[U_1 \cap \ldots \cap U_l\right] = \mathsf{P}\left[U_l \middle| \left(U_1 \cap \ldots \cap U_{l-1}\right)\right] \cdot \mathsf{P}\left[U_{l-1} \middle| \left(U_1 \cap \ldots \cap U_{l-2}\right)\right] \cdot \ldots \cdot \mathsf{P}\left[U_1\right]$$

и каждый сомножитель в правой части не меньше $1 - \varepsilon$, получаем неравенство

$$\mathsf{P}\left[U_1 \cap \ldots \cap U_q\right] \geqslant (1 - \varepsilon)^q.$$

Таким образом, вероятность успеха атаки не превосходит величины

$$1 - (1 - \varepsilon)^q \leqslant \varepsilon q.$$

Утверждение доказано. ■

2. AEAD-криптосистемы, GCM

В последние годы уделяется большое внимание построению и исследованию новых режимов блочного шифрования, обеспечивающих конфиденциальность и аутентификацию данных [3–7]. В связи с этим возникли новые термины, соответствующие названиям новых режимов шифрования: *Authenticated Encryption* (кратко — AE) и *Authenticated Encryption with Associated Data* (AEAD). В AEAD-системах (в отличие от AE-систем) используются так называемые *ассоциированные данные* (*associated*

data). Это — дополнительные сведения, которые при передаче должны быть аутентифицированы, но не зашифрованы. Пример — заголовок сетевого пакета, по которому можно определить характер информации, содержащейся в зашифрованном пакете.

AEAD-криптосистема GCM основана на блочном шифровании в режиме счётчика (CTR) и системе аутентификации типа $WC[G, F]$, разработана в 2004 г. [8]. Система GCM стандартизована NIST в документе SP800-38D, имеет доказуемую стойкость, эффективную программную и аппаратную реализацию, широко используется в популярных криптографических протоколах IPSec, MACSec, P1619.1, TLS.

Алгоритм GCM имеет четыре входа:

— ключ K;
— вектор инициализации iv длины до 2^{64} битов (рекомендуется iv длины 96 битов);
— открытый текст P длины до $(2^{32} - 2)\, n$ битов (n — длина блока шифрования);
— ассоциированные данные A длины до $2^{n/2}$ битов.

Алгоритм GCM имеет два выхода:

— шифртекст C, длина которого совпадает с длиной открытого текста;
— метка аутентификации T длины до n битов; длина метки обозначается τ.

Вектор iv должен меняться с каждым открытым текстом. Не требуется, чтобы iv был случайным или непредсказуемым. Он передаётся вместе с шифртекстом. Открытый текст и ассоциированные данные разбиваются на n-битовые блоки:

$$P = P_1||\ldots||P_{m-1}||P_m^*, \quad A = A_1||\ldots||A_{r-1}||A_r^*.$$

Блоки P_m^* и A_r^* могут быть неполными. Шифртекст имеет вид $C = C_1||\ldots||C_{m-1}||C_m^*$, где длина блока $l\,(P_m^*) = l\,(C_m^*)$. Пусть

$$l(P) = (m-1)n + u,\ 1 \leqslant u \leqslant n; \quad l(A) = (r-1)n + v,\ 1 \leqslant v \leqslant n.$$

Схема алгоритма GCM изображена на рис. 1.

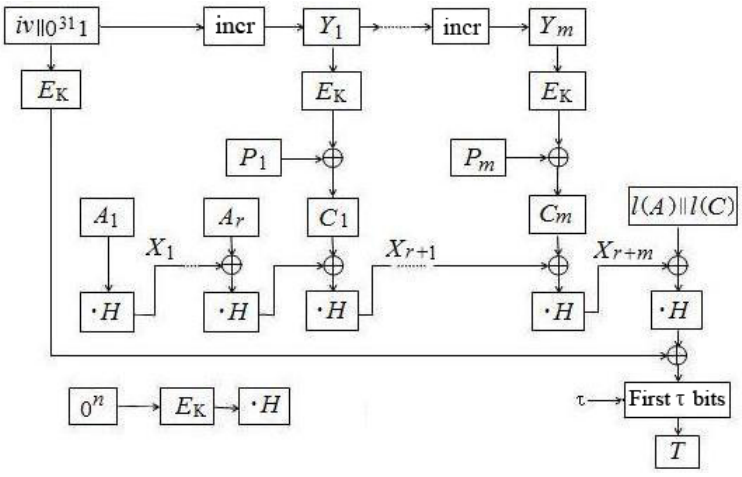

Рис. 1. Схема алгоритма GCM

Алгоритм использует счётчиковую последовательность $Y = Y_0||Y_1||\ldots$, в которой $Y_i = \mathrm{incr}\,(Y_{i-1})$. Функция $\mathrm{incr}(Y)$ изменяет младшие 32 бита Y, добавляя единицу по модулю 2^{32} :

$$\mathrm{incr}\,(L||R) = L||\,(R+1) \bmod 2^{32}.$$

Алгоритм GCM состоит в выполнении следующих операций:

— $H = E_K(0^n)$;

— $Y_0 = \begin{cases} iv||0^{31}1, & \text{если } l(iv) = n - 32, \\ GHASH(H, \{\}, iv) & \text{в противном случае;} \end{cases}$

— $Y_i = \operatorname{incr}(Y_{i-1}),\ i = 1, \ldots, m$;

— $C_i = P_i \oplus E_K(Y_i),\ i = 1, \ldots m - 1$;

— $C_m^* = P_m^* \oplus MSB_u(E_K(Y_m))$;

— $T = MSB_\tau(GHASH(H, A, C) \oplus E_K(Y_0))$.

В описании алгоритма $MSB_t(Z)$ обозначает старшие t битов вектора Z, $\{\}$ — пустую строку, $E_K(Z)$ — результат зашифрования Z на ключе K. Зашифрованное сообщение передаётся в виде вектора (iv, A, C, T). Функция $GHASH$ определяется формулой

$$GHASH(H, A, C) = X_{m+r+1},$$

в которой $X_i,\ i = 0, 1, \ldots, m + r + 1$, задаются рекуррентным соотношением

$$X_i = \begin{cases} 0, & \text{если } i = 0, \\ (X_{i-1} \oplus A_i) \cdot H, & \text{если } i = 1, \ldots, r - 1, \\ (X_{r-1} \oplus (A_r^*||0^{n-v})) \cdot H, & \text{если } i = r, \\ (X_{i-1} \oplus C_{i-r}) \cdot H, & \text{если } i = r + 1, \ldots, m + r - 1, \\ (X_{m+r-1} \oplus (C_m^*||0^{n-u})) \cdot H, & \text{если } i = m + r, \\ (X_{m+r} \oplus (l(A) \oplus l(C))) \cdot H, & \text{если } i = m + r + 1, \end{cases} \tag{2}$$

где операции сложения и умножения выполняются в поле $\mathrm{GF}(2^{128})$, порождённом над полем $\mathrm{GF}(2)$ неприводимым многочленом $x^{128} + x^7 + x^2 + x + 1$.

3. Стойкость GCM

Оценка стойкости GCM, как и других AE-систем, проводится с позиции *доказуемой стойкости* (*provable security*). Известна иерархия понятий доказуемой стойкости, отражающих как статистический (или теоретико-информационный), так и теоретико-сложностной подходы [3, 6, 9, 10]. Второй подход предпочтительнее, поскольку позволяет регулировать выбор параметров криптосистем, обеспечивающих требуемый уровень стойкости. В связи с такой возможностью используется термин *практически-ориентированная доказуемая стойкость* (*practice-oriented provable security*) [9].

В 2004 г. было показано [10], что для AE-систем оценка стойкости типа (IND-CPA)+(AUTH) является адекватной мерой стойкости в смысле различных понятий доказуемой стойкости. Понятие (IND-CPA)+(AUTH)-стойкости означает следующее.

Стойкость шифрования системы оценивается стойкостью к атаке различения на основе подобранного открытого текста. Стойкость аутентификации системы оценивается стойкостью к активной атаке на основе подобранного открытого текста, в которой атакующий имеет доступ к оракулу генерации метки и оракулу проверки метки. Запросы к оракулам можно как угодно чередовать по усмотрению атакующего. После серии запросов и получения ответов на них атакующий вырабатывает «подделку» — пару текст — метка, в которой текст отличен от всех текстов, используемых в запросах. Атака достигает успеха, если метка признаётся корректной. Мерой стойкости служат значения функции преимущества, введённой в определениях 4 и 5 и прокомментированной в замечаниях 1 и 2. В [8] для оценки стойкости GCM использован именно такой

подход. Приведём доказательство оценки стойкости GCM в случае, когда $l(iv) = n - t$, где 2^t — максимальное число сообщений, которые можно зашифровать на одном ключе (для GCM $n = 128$, $l(iv) = 128 - 32$). В этом случае фактор наличия коллизий функций семейства $GHASH$ можно не учитывать, что упрощает получение оценки. Этот упрощённый вариант доказательства мы приводим с целью иллюстрации методики.

Теорема 1. Пусть $\mathcal{C}$ — противник, имеющий преимущество $\mathcal{C}_{\mathrm{GCM}}$ в атаке различения семейства функций, реализуемого GCM, или в активной атаке против GCM, при числе запросов к оракулам, не превосходящем q. Пусть для каждого запроса (iv, A, P) выполняются условия $l(C) + l(A) < l$ и $l(iv) = n - t$. Тогда существует различитель $\mathcal{B}$ базового шифра E, имеющий преимущество $\mathcal{B}_E$, где

$$\mathcal{C}_{\mathrm{GCM}} \leqslant \mathcal{B}_E + q \left\lceil \frac{l}{n} + 1 \right\rceil 2^{-\tau} + \frac{q(q-1)}{2^{n+1}}.$$

Доказательство. Оценим сначала стойкость аутентификации.

Рассмотрим базовый шифр E как псевдослучайное семейство функций (PRF). Пусть $\mathcal{C}$ — противник, имеющий преимущество $\mathcal{C}_{\mathrm{GCM}}$ в активной атаке против GCM. Используем $\mathcal{C}$ для построения различителя $\mathcal{B}$ семейства E. В получении ответов на свои запросы $\mathcal{C}$ будет использовать $\mathcal{B}$, направляя ему значения счётчиковой последовательности и получая от него необходимые результаты зашифрования. В свою очередь, $\mathcal{B}$ будет получать эти ответы от оракула зашифрования.

Пусть W_1 и W_0 — события, соответствующие использованию в атаке различения для $\mathcal{B}$ семейства функций E или случайной функции. После серии запросов $\mathcal{C}$ строит подделку. Если $\mathcal{C}$ достигает успеха в подделке, то $\mathcal{B}$ делает выбор в пользу W_1, иначе — в пользу W_0.

Выразим преимущество $\mathcal{B}_{\mathrm{PRF}} = \mathrm{Adv}^{\mathrm{prf}}_{E,\mathcal{B}}$ различителя $\mathcal{B}$ через преимущество $\mathcal{C}_{\mathrm{GCM}} = \mathrm{Adv}^{\mathrm{prf}}_{\mathrm{GCM},\mathcal{C}}$ противника $\mathcal{C}$. Согласно (1) и замечанию 1,

$$\mathcal{B}_{\mathrm{PRF}} = \mathsf{P}\left[d^{\mathcal{B}} = 1 | W_1\right] - \mathsf{P}\left[d^{\mathcal{B}} = 1 | W_0\right], \tag{3}$$

где $d^{\mathcal{B}}$ — различающий бит, вырабатываемый $\mathcal{B}$. Из описания действий $\mathcal{B}$ и определения преимущества $\mathcal{C}_{\mathrm{GCM}}$ следует, что

$$\mathcal{C}_{\mathrm{GCM}} = \mathsf{P}\left[d^{\mathcal{B}} = 1 | W_1\right]. \tag{4}$$

Оценим вероятность $\mathsf{P}\left[d^{\mathcal{B}} = 1 | W_0\right]$.

Лемма 1. $G = GHASH$ образует $\lceil l/n + 1 \rceil 2^{-\tau} XU$-семейство функций, где τ — длина метки и l определяется неравенством $l(A) + l(C) \leqslant l$.

Доказательство. Напомним, что $GHASH\,(H, A, C) = X_{m+r+1}$, где X_i определяется формулой (2). Рассмотрим два различных входа (A, C), (A', C') и оценим вероятность события

$$G(H, A, C) \oplus G(H, A', C') = a||z, \tag{5}$$

где a — фиксированная τ-битовая строка; z — $(n - \tau)$-битовая переменная (отсекаемая часть выхода).

Согласно описанию алгоритма GCM, строки A, C, A', C' разбиваются соответственно на r, m, r', m' n-битовых блоков. Последние блоки имеют длины v, u, v', u' соответственно. Пусть $h = \max\{m + r, m' + r'\}$ — число блоков в более длинном входе.

Определим блоки:

$$D_i = \begin{cases} A_i, & \text{если } i = 1, \ldots, r-1, \\ A_r^* || 0^{n-v}, & \text{если } i = r, \\ C_{i-r}, & \text{если } i = r+1, \ldots, r+m-1, \\ C_m^* || 0^{n-u}, & \text{если } i = r+m, \\ l(A) || l(C), & \text{если } i = r+m+1, \\ 0^n, & \text{если } i = r+m+2, \ldots, h+1. \end{cases}$$

Аналогично определим блоки D'_i для пары (A', C').

Равенство (5) можно записать в виде $R(H) = 0$, где R — многочлен степени, не превосходящей $h+1$, над полем $\mathrm{GF}(2^n)$:

$$R(H) = (a||z) \oplus \sum_{i=1}^{h} (D_i \oplus D'_i) \cdot H^i.$$

Поскольку $A||C \neq A'||C'$, многочлен R — ненулевой и, следовательно, имеет не более $h+1$ корней. Если H выбирать случайно и равновероятно из $\mathrm{GF}(2^n)$, то вероятность того, что $R(H) = 0$, не превосходит $(h+1)2^{-n} \leqslant \lceil l/n + 1 \rceil 2^{-n}$ при условии, что суммарная длина входов ограничена l битами.

Нетрудно видеть, что имеется взаимно-однозначное соответствие между блоками D и парами (A, C). Поэтому вероятность того, что $R(H) = 0$, для любых двух данных пар (A, C), (A', C') и данного вектора $a||z$ равна вероятности события (5). А так как имеется $2^{n-\tau}$ различных значений z, событие (5) выполняется с вероятностью, не превосходящей

$$\lceil l/n + 1 \rceil 2^{-n} 2^{n-\tau} = \lceil l/n + 1 \rceil 2^{-\tau}$$

для любых пар $(A, C), (A', C')$ и $a \in \{0,1\}^\tau$, что и требуется. ■

Вернёмся к доказательству теоремы. Заметим, что при условии W_0 система MAC типа $WC[G, E]$ модифицируется в систему MAC типа $WC[G]$, поскольку E заменяется случайной функцией. Такая система MAC, согласно утверждению 1 и лемме 1, является $\lceil l/n + 1 \rceil 2^{-\tau}$-стойкой.

Из утверждения 2 получаем неравенство

$$\mathsf{P}\left[d^{\mathcal{B}} = 1 | W_0\right] \leqslant q \lceil l/n + 1 \rceil 2^{-\tau}. \tag{6}$$

Следующее утверждение, известное под названием PRF-PRP-switching lemma [11], связывает $\mathcal{B}_{\mathrm{PRF}}$ и $\mathcal{B}_{\mathrm{PRP}} = \mathcal{B}_E$.

Лемма 2. Пусть $\mathcal{A}_{\mathrm{PRF}}(\mathcal{A}_{\mathrm{PRP}})$ — преимущество различителя блочного шифра с n-битовым блоком и случайной функции (случайной подстановки). Пусть различитель использует не более чем q запросов к оракулу. Тогда

$$\mathcal{A}_{\mathrm{PRF}} \leqslant \mathcal{A}_{\mathrm{PRP}} + \frac{q(q-1)}{2^{n+1}}. \tag{7}$$

Утверждение теоремы о стойкости аутентификации следует из (2), (4), (6) и (7):

$$\mathcal{C}_{\mathrm{GCM}} = \mathcal{B}_{\mathrm{PRP}} + \mathsf{P}\left[d^{\mathcal{B}} = 1 | W_0\right] \leqslant \mathcal{B}_{\mathrm{PRP}} + q \lceil l/n + 1 \rceil 2^{-\tau} \leqslant$$
$$\leqslant \mathcal{B}_E + q \lceil l/n + 1 \rceil 2^{-\tau} + \frac{q(q-1)}{2^{n+1}}.$$

Получим теперь оценку стойкости шифрования схемы. Пусть $\mathcal{C}$ — различитель семейства функций, реализуемых GCM, имеющий преимущество $\mathcal{C}_{\mathrm{GCM}}$. Построим различитель $\mathcal{B}$ семейства функций E. Для получения ответов на свои запросы $\mathcal{C}$ будет использовать $\mathcal{B}$, направляя ему соответствующие блоки счётчика и получая от него необходимые результаты зашифрования. В свою очередь, $\mathcal{B}$ будет получать эти результаты от оракула зашифрования. Если после серии запросов $\mathcal{C}$ принимает бит 1, то и $\mathcal{B}$ принимает бит 1.

Пусть W_1 и W_0 — события, соответствующие использованию в атаке различения для $\mathcal{B}$ семейства функций E и случайной функции, а U_1 и U_0 — события, соответствующие использованию в атаке различения для $\mathcal{C}$ семейства функций GCM и случайной функции. Согласно (1) и замечанию 1, преимущество $\mathcal{C}$ выражается формулой

$$\mathcal{C}_{\mathrm{GCM}} = \mathsf{P}\left[d^{\mathcal{C}} = 1|U_1\right] - \mathsf{P}\left[d^{\mathcal{C}} = 1|U_0\right]. \tag{8}$$

В свою очередь, преимущество $\mathcal{B}$ выражается формулой (3).

Из описания действий различителя $\mathcal{C}$ следует, что

$$\mathsf{P}\left[d^{\mathcal{C}} = 1|U_1\right] = \mathsf{P}\left[d^{\mathcal{B}} = 1|W_1\right]. \tag{9}$$

Оценим вероятность $\mathsf{P}\left[d^{\mathcal{C}} = 1|U_0\right]$.

Каждый запрос различителя использует счётчиковую последовательность $Y_0, Y_1, \ldots$ Обозначим через Q событие, означающее, что значения счётчика во всех запросах различны, а через R — событие, означающее, что $\mathcal{C}$ не достигает успеха.

Лемма 3. Справедливо неравенство

$$\mathsf{P}\left[d^{\mathcal{B}} = 1|\,(W_0 \cap Q)\right] \cdot \mathsf{P}\left[Q|W_0\right] \leqslant \mathsf{P}\left[d^{\mathcal{C}} = 1|U_0\right]. \tag{10}$$

Доказательство. Событие $W_0 \cap Q$ означает, что в атаке реализуется система S, которая получается из GCM заменой функции шифрования случайной функцией, и счётчиковые последовательности в запросах $\mathcal{C}$ не имеют коллизий. Поскольку выход S равносилен выходу случайной функции, событие $\left(d^{\mathcal{C}} = 1|\,(U_0 \cap Q)\right)$ означает, что $\mathcal{C}$ принимает случайную функцию за GCM. Отсюда и из того, что $\mathsf{P}\left[U_0\right] = \mathsf{P}\left[W_0\right] = 0{,}5$, получаем следующие соотношения:

$$\mathsf{P}\left[d^{\mathcal{B}} = 1|\,(W_0 \cap Q)\right] \cdot \mathsf{P}\left[Q|W_0\right] = \frac{\mathsf{P}\left[\left(d^{\mathcal{B}} = 1\right) \cap W_0 \cap Q\right] \cdot \mathsf{P}\left[W_0 \cap Q\right]}{\mathsf{P}\left[W_0 \cap Q\right] \cdot \mathsf{P}\left[W_0\right]} =$$

$$= \frac{\mathsf{P}\left[\left(d^{\mathcal{B}} = 1\right) \cap W_0 \cap Q\right]}{\mathsf{P}\left[W_0\right]} = \frac{\mathsf{P}\left[\left(d^{\mathcal{C}} = 1\right) \cap U_0 \cap Q\right]}{\mathsf{P}\left[U_0\right]} = \mathsf{P}\left[\left(d^{\mathcal{C}} = 1\right) \cap Q|U_0\right] \leqslant \mathsf{P}\left[d^{\mathcal{C}} = 1|U_0\right].$$

Отсюда следует неравенство (10). ■

Выразим $\mathcal{B}_{\mathrm{PRP}}$ через $\mathcal{C}_{\mathrm{GCM}}$. С учётом (8)–(10) имеем

$$\mathcal{B}_{\mathrm{PRP}} = \mathsf{P}\left[d^{\mathcal{C}} = 1|U_1\right] - \mathsf{P}\left[d^{\mathcal{B}} = 1|W_0\right] =$$

$$= \mathsf{P}\left[d^{\mathcal{C}} = 1|U_1\right] - \mathsf{P}\left[\left(d^{\mathcal{B}} = 1\right) |\,(W_0 \cap Q)\right] \cdot \mathsf{P}\left[Q|W_0\right] - \mathsf{P}\left[\left(d^{\mathcal{B}} = 1\right) |\,\left(W_0 \cap \overline{Q}\right)\right] \cdot \mathsf{P}\left[\overline{Q}|W_0\right] \geqslant$$

$$\geqslant \mathsf{P}\left[d^{\mathcal{C}} = 1|U_1\right] - \mathsf{P}\left[d^{\mathcal{C}} = 1|U_0\right] - \mathsf{P}\left[\left(d^{\mathcal{B}} = 1\right) |\,\left(W_0 \cap \overline{Q}\right)\right] \cdot \mathsf{P}\left[\overline{Q}|W_0\right] =$$

$$= \mathcal{C}_{\mathrm{GCM}} - \mathsf{P}\left[\left(d^{\mathcal{B}} = 1\right) |\,\left(W_0 \cap \overline{Q}\right)\right] \cdot \mathsf{P}\left[\overline{Q}|W_0\right] \geqslant \mathcal{C}_{\mathrm{GCM}} - \mathsf{P}\left[\overline{Q}|W_0\right] \geqslant$$

$$\geqslant \mathcal{C}_{\mathrm{GCM}} - \mathsf{P}\left[\overline{Q}|W_0\right] - \mathsf{P}\left[\overline{R}|W_0\right].$$

Поскольку условия исключают возможность коллизий в счётчиковых последовательностях, событие $\overline{Q}$ невозможно, и из последних соотношений получаем неравенство

$$\mathcal{B}_{\mathrm{PRP}} \geqslant \mathcal{C}_{\mathrm{GCM}} - \mathsf{P}\left[\overline{R}|W_0\right]. \tag{11}$$

Заметим, что в условиях W_0, $l(iv) = n - t$ работает система S, для которой можно использовать утверждение 2, согласно которому вероятность $\mathsf{P}\left[\overline{R}|W_0\right]$ не превосходит εq, а ε оценивается в лемме 1. С учётом этого, из (11) и леммы 2 получаем нужную оценку: $\mathcal{C}_{\mathrm{GCM}} \leqslant \mathcal{B}_{\mathrm{PRP}} + q\left\lceil l/n+1\right\rceil 2^{-\tau} \leqslant \mathcal{B}_E + q\left\lceil l/n+1\right\rceil 2^{-\tau} + \dfrac{q(q-1)}{2^{n+1}}$.

Теорема доказана. ■

Приведём числовой пример, иллюстрирующий полученную оценку. Базовым алгоритмом шифрования для GCM является AES. При этом $l(iv) = 96$, $\tau = 96$, $n = 128$. Пусть размер сообщения не превышает 1500 байтов (т. е. $l \leqslant 12000$). Тогда из теоремы 1 следует, что если AES неотличим от случайной подстановки при защите не более чем 2^{32} сообщений на одном ключе (т. е. при этом $\mathcal{B}_E$ практически равно 0), то преимущество атакующего AES-GCM не превосходит $5{,}17 \cdot 10^{-18}$.

4. Оценка стойкости модификации GCM

Рассмотрим модификацию GCM, в которой система MAC типа $WC[G, F]$ заменяется другой системой WC-MAC. В таких системах вместо εXU-семейства G может использоваться семейство функций с более слабым требованием к свойству иметь коллизии.

Определение 7. $(b; k, n)$-семейство функций G называется *ε-универсальным* (εU-семейством), если для любых s_1, s_2 из S, $s_1 \neq s_2$, и положительного числа ε справедливо неравенство $|\{f \in G : f(s_1) = f(s_1)\}| \leqslant \varepsilon b$.

Определение 8. Пусть $G = \left\{f : S \to \{0,1\}^l\right\}$ и $R = \mathrm{Rand}^{l \to n}$. Ключом системы MAC $FH[G]$ служит пара (f, ρ), $f \in G$, $\rho \in R$, а меткой сообщения $s \in S$ — значение $\rho(f(s))$.

Определение 9. Пусть $G = \left\{f : S \to \{0,1\}^l\right\}$ и $F : \{0,1\}^r \times \{0,1\}^l \to \{0,1\}^n$ — семейства функций. Ключ системы $FH[G, F]$ — пара (f, F_K), $f \in G$, $K \in \{0,1\}^r$. Меткой сообщения $s \in S$ служит $F_K(f(s))$.

Утверждение 3. Пусть G — это εU-семейство функций и q — максимальное число сообщений, которые можно аутентифицировать на одном ключе. Тогда система MAC $FH[G]$ является $\varepsilon q(q+1)/2$-стойкой.

Доказательство. Пусть противник наблюдает сообщения $(s_1, \tau_1), \ldots, (s_q, \tau_q)$, где τ_i — метки, полученные с помощью $FH[G]$ при использовании ключа (f, ρ). Оценим вероятность того, что противник сможет снабдить новое сообщение s^* корректной меткой τ^*.

Пусть $\Phi = \{f(s_1), \ldots, f(s_q)\}$, $T = \{\tau_1, \ldots, \tau_q\}$. Если $f(s^*) \notin \Phi$, то $\rho(f(s^*))$ с равной вероятностью может принимать любое из 2^n значений (так как ρ — случайная функция). Поэтому вероятность того, что для некоторого τ^* выполняется равенство $\tau^* = \rho(f(s^*))$, равна 2^{-n}. Таким образом, вероятность $p_{\mathrm{усп}}$ успеха атаки равна

$$p_{\mathrm{усп}} = 2^{-n}. \tag{12}$$

Рассмотрим случай, когда $f(s^*) \in \Phi$. В этом случае τ^* должно принадлежать T. Тогда в рассматриваемых условиях

$$p_{\text{усп}} = \mathsf{P}\Big[\bigcup_{(i,j)} (\tau^* = \tau_j | f(s^*) = f(s_i))\Big] = \sum_{i \leqslant j} \mathsf{P}\left[\tau^* = \tau_j | f(s^*) = f(s_i)\right].$$

В свою очередь,

$$\mathsf{P}[\tau^* = \tau_j | f(s^*) = f(s_i)] = \mathsf{P}[\tau^* = \tau_j | f(s^*) = f(s_i), f(s_i) = f(s_j)] \cdot \mathsf{P}[f(s^*) = f(s_i) = f(s_j)] + \\ + \mathsf{P}\left[\tau^* = \tau_j | f(s^*) = f(s_i), f(s_i) \neq f(s_j)\right] \cdot \mathsf{P}\left[f(s^*) = f(s_i) \neq f(s_j)\right].$$

Поскольку

$$\mathsf{P}\left[\tau^* = \tau_j | f(s^*) = f(s_i), f(s_i) = f(s_j)\right] = 1,$$
$$\mathsf{P}\left[\tau^* = \tau_j | f(s^*) = f(s_i), f(s_i) \neq f(s_j)\right] = 0,$$

получаем формулу

$$p_{\text{усп}} = \sum_{i \leqslant j} \mathsf{P}\left[f(s^*) = f(s_i) = f(s_j)\right]. \tag{13}$$

Пусть D_i — событие, означающее первое появление коллизии функции f в последовательности аргументов $s_1, \ldots, s_{i-1}, s^*$ на i-м месте. Поскольку f выбирается случайно из εU-семейства функций, из (13) получаем соотношения

$$p_{\text{усп}} \leqslant \sum_{i=1}^{q+1} \mathsf{P}\left[D_i\right] \leqslant \sum_{i=1}^{q+1} (i-1)\,\varepsilon = \varepsilon \sum_{i=0}^{q} i = \varepsilon q(q+1)/2.$$

Поскольку $2^{-n} \leqslant \varepsilon \leqslant q(q+1)/2$, в любом случае из (12) и (13) получаем оценку $p_{\text{усп}} \leqslant \varepsilon q(q+1)/2$. ■

Усилим утверждение 3, предоставив противнику возможность аутентифицировать адаптивно подобранные сообщения и проверять корректность их меток. Эти условия могут повысить шансы противника на успех. Покажем, что на самом деле указанные преимущества не позволяют улучшить оценку стойкости, полученную в утверждении 3.

Утверждение 4. Пусть G — это εU-семейство функций. Тогда при использовании не более чем q запросов к оракулу проверки метки и к оракулу генерации метки система $FH[G]$ является $\varepsilon q(q-1)/2$-стойкой.

Доказательство. В серии подделок (s_i, τ_i), $i = 1, 2, \ldots, q$, успех в атаке определяется путём запросов к оракулу проверки метки. Пусть $q = q_1 + q_2$, где q_1 — число запросов к оракулу генерации метки; q_2 — число запросов к оракулу проверки метки.

Пусть U_i — событие, означающее неуспех при i-м запросе к оракулу проверки метки, и p_i — число запросов к оракулу генерации метки, произведённое перед i-м запросом к оракулу проверки метки. Если имеет место событие $U_1 \cap \ldots \cap U_i$, то, согласно утверждению 3, вероятность успеха в следующей подделке ограничена числом $\varepsilon p_{i+1}(p_{i+1}+1)/2$. Это означает, что имеет место неравенство

$$\mathsf{P}\left[U_{i+1} | (U_1 \cap \ldots \cap U_i)\right] \geqslant 1 - \frac{\varepsilon p_{i+1}(p_{i+1}+1)}{2}.$$

Поскольку

$$\mathsf{P}\left[U_1 \cap \ldots \cap U_i\right] = \mathsf{P}\left[U_i | U_1 \cap \ldots \cap U_{i-1}\right] \cdot \mathsf{P}\left[U_{i-1} | U_1 \cap \ldots \cap U_{i-2}\right] \cdot \ldots \cdot \mathsf{P}\left[U_1\right],$$

получаем неравенство

$$\mathsf{P}\left[U_1 \cap \ldots \cap U_{q_2}\right] \geqslant \left(1 - \frac{\varepsilon p_1 (p_1+1)}{2}\right)\left(1 - \frac{\varepsilon p_2 (p_2+1)}{2}\right)\ldots\left(1 - \frac{\varepsilon p_{q_2} (p_{q_2}+1)}{2}\right).$$

Поскольку $p_{i+1} \geqslant p_i$ и $p_{q_2} \leqslant q_1$, вероятность $1 - \mathsf{P}\left[U_1 \cap \ldots \cap U_{q_2}\right]$ успеха атаки не превосходит величины

$$1 - \left(1 - \frac{\varepsilon q_1 (q_1+1)}{2}\right)^{q_2},$$

которая, в свою очередь, меньше $\varepsilon q_1(q_1+1)q_2/2$.

Так как $q_1 + q_2 = q$, $q_1 \leqslant q-1$ и функция $q_1(q_1+1)(1-q_1)$ принимает максимальное значение при $q_1 = q-1$, получаем отсюда, что вероятность успеха атаки не превосходит $\varepsilon q(q-1)/2$, что и требуется доказать. ■

Рассмотрим AE-систему GCM', которая отличается от GCM лишь тем, что на шаге вычисления метки сумма $GHASH(H, A, C) \oplus E_K(Y_0)$ заменяется результатом зашифрования $E_K(GHASH(H, A, C))$. Это соответствует замене системы $WC[G, F]$ системой $FH[G, F]$.

Как и в теореме 1, ограничимся случаем, когда вектор iv имеет фиксированную длину. В этих условиях имеет место следующий аналог теоремы 1.

Теорема 2. Пусть $\mathcal{C}$ — противник, имеющий преимущество $\mathcal{C}_{\text{GCM'}}$ в атаке различения семейства функций, реализуемого GCM', или в активной атаке против GCM', при числе запросов к оракулам, не превосходящем q. Пусть для каждого запроса (iv, A, P) выполняются условия $l(A) + l(C) \leqslant l$ и $l(iv) = n - t$. Тогда существует различитель $\mathcal{B}$ базового шифра E, имеющий преимущество $\mathcal{B}_E$, где

$$\mathcal{C}_{\text{GCM'}} \leqslant \mathcal{B}_E + \frac{q(q+1)}{2^{n+1}}\left\{\left\lceil \frac{l}{n} + 1\right\rceil 2^{n-\tau} + 1\right\}.$$

Доказательство. Воспользуемся схемой доказательства теоремы 1. Получим сначала оценку стойкости аутентификации. Пусть $\mathcal{C}$ — противник, имеющий преимущество $\mathcal{C}_{GCM'}$ в активной атаке против GCM', и $\mathcal{B}$ — различитель семейства функций E, построенный так же, как в доказательстве теоремы 1. Преимущество $\mathcal{B}_{\text{PRF}}$ определяется формулой (3). Из описания действий различителя $\mathcal{B}$ следует, что $\mathcal{C}_{\text{GCM'}}$ выражается формулой (4).

При получении оценки вероятности $\mathsf{P}[d^{\mathcal{B}} = 1|W_0]$ заметим, что при условии W_0 реализуется система MAC $FH[G]$. Согласно лемме 1, $G = GHASH$ образует εXU-семейство функций (следовательно, и εU-семейство), где $\varepsilon = \lceil l/n+1\rceil 2^{-\tau}$; $l(A)+l(C) \leqslant l$.

Из утверждения 4 получаем неравенство

$$\mathsf{P}\left[d^{\mathcal{B}} = 1|W_0\right] \leqslant \left\lceil \frac{l}{n} + 1\right\rceil \frac{q(q-1)}{2^{\tau+1}}.$$

Теперь из (8) и (9), с учётом леммы 2, получаем соотношения

$$\mathcal{C}_{\text{GCM'}} = \mathcal{B}_{\text{PRF}} + \mathsf{P}\left[d^{\mathcal{B}} = 1|W_0\right] \leqslant \mathcal{B}_{\text{PRF}} + \frac{\lceil l/n+1\rceil\, q(q-1)}{2^{\tau+1}} \leqslant$$
$$\leqslant \mathcal{B}_E + \frac{\lceil l/n+1\rceil\, q(q-1)}{2^{\tau+1}} + \frac{q(q-1)}{2^{n+1}},$$

откуда следует искомое неравенство.

Оценка стойкости шифрования GCM' получается так же, как в теореме 1, с той лишь разницей, что в (12) ссылка на утверждение 2 заменяется ссылкой на утверждение 4. ■

Проиллюстрируем полученную оценку. Пусть длина каждого сообщения не превосходит 12000 битов, $l(iv) = 96$, $\tau = 96$, $n = 128$. Тогда преимущество атакующего GCM' не превосходит $1{,}1 \cdot 10^{-8}$, если базовый блочный шифр неотличим от истинно случайной подстановки при защите не более чем 2^{32} сообщений на одном ключе (т. е. если при этом $\mathcal{B}_E$ практически равно нулю).

Отметим, что аналогичную оценку стойкости криптосистемы GCM' в общем случае (когда вектор iv имеет произвольную длину) можно получить, используя подход, предложенный в [12].

Как видим, оценку стойкости GCM' можно считать удовлетворительной, хотя она уступает оценке стойкости GCM. Вместе с тем GCM' защищена от атаки Фергюсона [13], которая, по мнению ряда специалистов, представляет собой основную известную угрозу для GCM. Это делает криптосистему GCM' интересной для дальнейшего изучения.

ЛИТЕРАТУРА

1. *Black J.* Message authentication codes. PhD Dissertation. Dept. of Comp. Sciences, US Davis, 2000. 126 p. `http://www.cs.colorado.edu/~jrblack/`
2. *Stinson D.* Universal hash families and the leftover hash lemma, and applications to cryptography and computing // J. Combin. Math. Combin. Comput. 2001. V. 42. No. 3. 29 p.
3. *Bellare M. and Namprempre C.* Authenticated encryption: relations among notions and analysis of the composition paradigm // Asiacrypt 2000. LNCS. 2000. V. 1976. P. 541–545.
4. CAESAR: competition for authenticated encryption: security, applicability, and robustness. 2012. `http://competitions.cr.yp.to/caesar.html`
5. *Chakraborty D. and Sarkar P.* On modes of operations of a block cipher for authentication and authenticated encryption. Cryptology ePrint Archive: report 627/14. 2014. 51 p.
6. *Rogaway P.* Authenticated-encryption with associated-data. ACM CCS, ACM Press, 2002. 10 p.
7. *Svenda P.* Basic Comparison of Modes for Authenticated-Encryption (IAPM, XCBC, OCB, CCM, EAX, CWC, GCM, PCFB, CS). 2005. 16 p. `https://www.fi.muni.cz/~xsvenda/docs/AE_comparison_ipics04.pdf`
8. *McGrew D. A. and Viega J.* The security and performance of Galois/Counter mode of operation // LNCS. 2004. V. 3348. P. 343–355.
9. *Bellare M.* Practice-oriented provable-security // LNCS. 2003. V. 1561. P. 1–15.
10. *Shrimpton T.* A characterization of authenticated-encryption as a form of chosen-ciphertext security. Cryptology ePrint Archive: 2004/272. 2004. 7 p.
11. *Bellare M., Kilian J., and Rogaway P.* The security of the cipher block chaining // LNCS. 1994. V. 839. P. 341–358.
12. *Iwata T., Ohashi K., and Minematsu K.* Breaking and repairing GCM security proofs // Crypto 2012. LNCS. 2012. V. 7417. P. 31–49.
13. *Ferguson N.* Authentication weaknesses in GCM. Public Comments to NIST. `http://csrc.nist.gov/CryptoToolKit/modes/comments`, May 2005.

REFERENCES

1. *Black J.* Message authentication codes. PhD Dissertation. Dept. of Comp. Sciences, US Davis, 2000. 126 p. `http://www.cs.colorado.edu/~jrblack/`

2. *Stinson D.* Universal hash families and the leftover hash lemma, and applications to cryptography and computing. J. Combin. Math. Combin. Comput., 2001, vol. 42, no. 3. 29 p.
3. *Bellare M. and Namprempre C.* Authenticated encryption: relations among notions and analysis of the composition paradigm. Asiacrypt 2000, LNCS, 2000, vol. 1976, pp. 541–545.
4. CAESAR: competition for authenticated encryption: security, applicability, and robustness. 2012. `http://competitions.cr.yp.to/caesar.html`
5. *Chakraborty D. and Sarkar P.* On modes of operations of a block cipher for authentication and authenticated encryption. Cryptology ePrint Archive: report 627/14. 2014. 51 p.
6. *Rogaway P.* Authenticated-encryption with associated-data. ACM CCS, ACM Press, 2002. 10 p.
7. *Svenda P.* Basic Comparison of Modes for Authenticated-Encryption (IAPM, XCBC, OCB, CCM, EAX, CWC, GCM, PCFB, CS). 2005. 16 p. `https://www.fi.muni.cz/~xsvenda/docs/AE_comparison_ipics04.pdf`
8. *McGrew D. A. and Viega J.* The security and performance of Galois/Counter mode of operation. LNCS, 2004, vol. 3348, pp. 343–355.
9. *Bellare M.* Practice-oriented provable-security. LNCS, 2003, vol. 1561, pp. 1–15.
10. *Shrimpton T.* A characterization of authenticated-encryption as a form of chosen-ciphertext security. Cryptology ePrint Archive: 2004/272. 2004. 7 p.
11. *Bellare M., Kilian J., and Rogaway P.* The security of the cipher block chaining. LNCS, 1994, vol. 839, pp. 341–358.
12. *Iwata T., Ohashi K., and Minematsu K.* Breaking and repairing GCM security proofs. Crypto 2012, LNCS, 2012, vol. 7417, pp. 31–49.
13. *Ferguson N.* Authentication weaknesses in GCM. Public Comments to NIST. `http://csrc.nist.gov/CryptoToolKit/modes/comments`, May 2005.