MGM2: режим аутентифицированного шифрования, устойчивый к повтору вектора инициализации

Л. Р. Ахметзянова, Е. К. Алексеев, А. А. Бабуева, А. А. Божко, С. В. Смышляев

***Аннотация*—В работе разработан новый режим аутентифицированного шифрования** MGM2**, для которого удается доказать стойкость в усиленных моделях противника, учитывающих возможность повторного использования вектора инициализации для обработки различных сообщений. Рассмотрение таких усиленных моделей является актуальным при использовании схем шифрования в приложениях, в которых отсутствуют технические возможности для обеспечения уникальности вектора инициализации. Более того, стойкость при повторе вектора инициализации также обеспечивает дополнительную защиту от ошибок в реализации, как случайных, так и вызванных противником.**

Режим MGM2 **является модификацией стандартизированного в Российской Федерации режима аутентифицированного шифрования** MGM **(Multilinear Galois Mode). В новом режиме используется то же криптографическое ядро - мультилинейная функция, но изменяется процедура выработки секретных коэффициентов и маскирующих значений с целью уменьшения вероятности коллизий между входами в блочный шифр. Для режима** MGM2 **были доказаны оценки в формально определенных моделях MRAE-integrity и CPA-res. Полученные оценки стойкости демонстрируют, что разработанный режим даже в усиленных моделях обеспечивает больший уровень конфиденциальности и целостности, чем оригинальный режим** MGM **в базовых моделях, которые не учитывают возможность повторного использования вектора инициализации.**

***Ключевые слова*—MGM, AEAD-режим, модель противника, оценки стойкости, повтор вектора инициализации, устойчивость к повтору**

I. Введение

Схемы аутентифицированного шифрования с ассоциированными данными (Authenticated Encryption with Associated Data, AEAD), предназначенные для обеспечения целостности и конфиденциальности данных, используются во многих значимых криптографических протоколах, таких как IPsec и TLS. Поэтому исследование стойкости данных схем является крайне важной задачей. Анализ стойкости AEAD-схем обычно проводится в базовых моделях противника, введенных в работе [1]: IND-CPA для конфиденциальности и INT-CTXT для целостности.

Статья получена 10 декабря 2021

Лилия Руслановна Ахметзянова, МГУ им. М.В. Ломоносова, ООО ”КРИПТО-ПРО”, (email: lah@cryptopro.ru).

Евгений Константинович Алексеев, ООО ”КРИПТО-ПРО”, (email: alekseev@cryptopro.ru).

Александра Алексеевна Бабуева, МГУ им. М.В. Ломоносова, ООО ”КРИПТО-ПРО”, (email: babueva@cryptopro.ru).

Андрей Алексеевич Божко, МГУ им. М.В. Ломоносова, ООО ”КРИПТО-ПРО”, (email: bozhko@cryptopro.ru).

Станислав Витальевич Смышляев, ООО ”КРИПТО-ПРО”, (email: svs@cryptopro.ru).

Одним из примеров таких схем является режим работы блочного шифра MGM, который был принят в качестве национального стандарта в Российской Федерации [2]. Процедура зашифрования в режиме MGM аналогична процедуре зашифрования в режиме CTR2 [3]. Основным элементом процедуры формирования имитовставки в режиме MGM является мультилинейная функция, секретные коэффициенты которой вырабатываются способом, аналогичным процедуре выработки секретных масок для шифрования данных. Целостность и конфиденциальность режима MGM были проанализированы в работе [4] путем построения сведения в базовых моделях противника.

Хотя анализ AEAD-схем в базовых моделях является необходимым и достаточным для использования во многих приложениях, в последнее время все чаще возникает необходимость в рассмотрении усиленных свойств безопасности, например, стойкости при возможности получения открытых текстов, соответствующих некорректным шифртекстам (release of unverified plaintext, RUP [5]), стойкости при обработке сообщений, зависящих от ключа (key dependent message, KDM [6]), и т.д. В настоящей работе рассматривается такое усиленное свойство как стойкость при условии, что одно и то же значение вектора инициализации может использоваться для обработки более одного сообщения (misuse-resistance [7]). Вектор инициализации подается на вход алгоритмам шифрования и расшифрования AEAD-схем, обычно предполагается его однократное использование в рамках одного фиксированного ключа. Обеспечение уникальности вектора инициализации возможно с помощью внутреннего состояния или генерации случайных значений, однако не во всех приложениях есть такие возможности, примером могут служить схемы полнодискового шифрования [8]. Более того, стойкость при повторе вектора инициализации также обеспечивает дополнительную защиту от ошибок в реализации, как случайных, так и вызванных противником.

Модели противника для AEAD-схем, устойчивых к повтору вектора инициализации, впервые были предложены Рогавеем и Шримптоном в работе [7] и далее развиты в работе [9]. Сильная модель противника, называемая MRAE («Misuse-Resistant AE»), была предложена в [7]. Данная модель противника является расширением базовых моделей IND-CPA и INT-CTXT путем предоставления противнику возможности повторять значения вектора инициализации в запросах не только к оракулу расшифрования, но и к оракулу зашифрования.

Модель MRAE аналогична модели противника DAE [7] («Deterministic AE»), которая формализует свойство конфиденциальности следующим образом: шифртекст для каждого *нового* запроса (не только нового вектора инициализации) должен быть неотличим от случайной строки той же длины. Известно, что конфиденциальность, определенная моделью нарушителя MRAE, является достаточно трудно обеспечиваемым свойством. Так, например, любые поточные режимы, к которым относится и режим MGM, не обладают им, а все известные авторам схемы, стойкие в модели MRAE, теряют некоторые эксплуатационные свойства: либо требуют большого количества вызовов блочного шифра [10], либо теряют свойство online-обработки данных [11, 12]. Поэтому в работе [9] вводится более слабое определение безопасности для конфиденциальности, называемое CPA-res («Chosen Plaintext Attack-resilience»). Оно также является расширением базовой модели противника IND-CPA, но подразумевает более слабое в сравнении с MRAE свойство безопасности: конфиденциальность должна быть обеспечена только для корректно обработанных сообщений с использованием уникального значения вектора инициализации.

С точки зрения целостности, определяемой моделью MRAE, режим MGM был проанализирован в работе [13]: была предложена атака, требующая объема обработанных данных не меньше $2^{n/2}$ блоков, где n – битовый размер блока используемого блочного шифра. Данный результат позволяет выдвинуть гипотезу, что режим MGM обладает достаточным уровнем стойкости в модели MRAE-int (целостность). Однако получение нижних оценок стойкости для MGM, необходимое для подтверждения данной гипотезы, все еще остается открытой задачей.

С целью получения оценок стойкости в усиленных моделях в настоящей работе предлагается модификация режима MGM — режим MGM2. Основное различие между двумя режимами заключается в способе создания секретных маскирующих блоков и секретных коэффициентов мультилинейной функции - для режима MGM2 этот процесс выполняется аналогично режиму CTR [3], без предварительного шифрования вектора инициализации. Отметим, что основное криптографическое ядро конструкции, а именно, мультилинейная функция, не изменилось. Были получены оценки стойкости для режима MGM2 в моделях MRAE (целостность) и CPA-res, которые оказались даже лучше, чем оценки для исходного режима MGM в базовых моделях INT-CTXT и IND-CPA, при этом соответствующие доказательства получились существенно проще. Помимо указанных преимуществ, конструкция режима MGM2 также позволяет прозрачно встроить внутреннее преобразование ключа (так же, как это сделано для CTR-ACPKM [14]) для увеличения срока жизни ключа (подробнее см. [15]).

II. Обозначения

Обозначим через $\{0,1\}^u$ множество всех u-битовых строк, и через $\{0,1\}^*$ — множество всех битовых строк конечной длины, в том числе пустую строку. Битовую строку, состоящую из u нулей, будем обозначать через 0^u. Длину битовой строки U будем обозначать через $|U|$. Через $|U|_u = \lceil |U|/u \rceil$ обозначим длину битовой строки U в u-битовых блоках. Через $\{0,1\}^{\leqslant u}$ обозначим множество всех строк, длина которых меньше или равна u.

Для битовой строки U и целого числа $0 < l \leqslant |U|$ через $\mathrm{msb}_l(U)$ ($\mathrm{lsb}_l(U)$) будем обозначать строку, состоящую из l крайних левых (правых) бит строки U. Для целых чисел $l > 0$ и $2^l > i \geqslant 0$ через $\mathrm{str}_l(i)$ будем обозначать l-битовое представление числа i, в котором наименее значащий бит находится справа. Для целого числа $l \geqslant 0$ и битовой строки $U \in \{0,1\}^l$ через $\mathrm{int}(U)$ будем обозначать целое число $i < 2^l$, такое что $\mathrm{str}_l(i) = U$. Для битовых строк $a \in \{0,1\}^n$ и $b \in \{0,1\}^n$ через $a \otimes b$ будем обозначать строку, которая является результатом их перемножения в поле $GF(2^n)$ (здесь строки кодируют полиномы стандартным образом). Также введем функцию $\mathsf{Set1}_r \colon \{0,1\}^n \to \{0,1\}^n$, $\mathsf{Set1}_r(x) = x$ or $(\overbrace{0\ldots0}^{r}1\overbrace{0\ldots0}^{n-r-1})$, $0 \leqslant r < n$.

Для произвольного множества S через $Perm(S)$ обозначим множество всех биективных отображений множества S в себя (перестановок на S), а через $Func(S)$ — множество всех отображений множества S в себя. Под блочным шифром E (или просто шифром) с длиной блока n и длиной ключа k будем понимать произвольное семейство перестановок на множестве $\{0,1\}^n$, параметризованное параметром $K \in \{0,1\}^k$, т.е. $E = \{E_K \in Perm(\{0,1\}^n) \mid K \in \{0,1\}^k\}$. Параметр K в этом семействе E называется ключом шифра. Факт того, что значение s выбрано из некоторого множества S в соответствии с равномерным распределением $\mathcal{U}$, будем обозначать через $s \xleftarrow{\mathcal{U}} S$.

III. Модели противника

В данном разделе вводятся формальные определения моделей, в которых противник может повторять значения вектора инициализации в своих запросах.

Для формализации моделей противника используется алгоритмический подход, в рамках которого определяется порядок взаимодействия между экспериментатором и противником. Экспериментатор и противник моделируются с помощью согласованных интерактивных вероятностных алгоритмов. Экспериментатор моделирует для противника функционирование исследуемой криптосистемы и предоставляет ему доступ к одному или более оракулам (для деталей см. [16]).

Экспериментаторы и противники описываются с помощью псевдокодов, которые используют следующие обозначения. Через $x \leftarrow val$ будем обозначать присваивание значения val переменной x. Аналогично, через $x \leftarrow y$ будем обозначать присваивание значения переменной y переменной x. Для вероятностного алгоритма A через $A \xrightarrow{\$} x$ ($x \xleftarrow{\$} A$) будем обозначать присваивание результата его работы переменной x. В случае, когда требуется подчеркнуть детерминированность алгоритма A, будем использовать обозначение $A \to x$ ($x \leftarrow A$).

Определение III.1. *AEAD-схемой* для множества ключей $\boldsymbol{K}$, множества векторов инициализации $\boldsymbol{N}$, множества открытых текстов $\boldsymbol{P}$, множества ассоциированных данных $\boldsymbol{A}$, множества шифртекстов $\boldsymbol{C}$ и множества имитовставок $\boldsymbol{T}$ является набор алгоритмов $\Pi = \{\Pi.\mathsf{Gen},\ \Pi.\mathsf{Enc},\ \Pi.\mathsf{Dec}\}$, где

– $\Pi.\mathsf{Gen}() \xrightarrow{\$} K$: Вероятностный алгоритм генерации ключа. Результатом работы данного алгоритма является ключ $K \in \boldsymbol{K}$.
– $\Pi.\mathsf{Enc}(K, N, A, P) \to (C, T)$: Детерминированный алгоритм аутентифицированного шифрования, принимающий на вход ключ $K \in \boldsymbol{K}$, вектор инициализации $N \in \boldsymbol{N}$, ассоциированные данные $A \in \boldsymbol{A}$ и открытый текст $P \in \boldsymbol{P}$. Результатом работы данного алгоритма являются шифртекст $C \in \boldsymbol{C}$ и имитовставка $T \in \boldsymbol{T}$.
– $\Pi.\mathsf{Dec}(K, N, A, C, T) \to P$: Детерминированный алгоритм расшифрования с проверкой целостности, принимающий на вход ключ $K \in \boldsymbol{K}$, вектор инициализации $N \in \boldsymbol{N}$, ассоциированные данные $A \in \boldsymbol{A}$, шифртекст $C \in \boldsymbol{C}$ и имитовставку $T \in \boldsymbol{T}$. Результатом работы данного алгоритма является открытый текст $P \in \boldsymbol{P}$ или символ ошибки $\perp$.

Введем модель противника MRAE-int («Misuse-Resistant Authenticated Encryption - integrity»), которая является частью модели MRAE, определенной в [7].

Определение III.2 (MRAE-int)**.** Преимущество противника $\mathcal{A}$ в модели MRAE-int для AEAD-схемы Π определяется следующим образом:

$$\mathsf{Adv}^{\text{MRAE-int}}_{\Pi}(\mathcal{A}) = \Pr\left[\mathbf{Exp}^{\text{MRAE-int}}_{\Pi}(\mathcal{A}) \to 1\right],$$

где эксперимент $\mathbf{Exp}^{\text{MRAE-int}}_{\Pi}$ описан ниже:

$\mathbf{Exp}^{\text{MRAE-int}}_{\Pi}(\mathcal{A})$
$K \xleftarrow{\$} \Pi.\mathsf{Gen}(\,)$
$sent \leftarrow \emptyset$
$win \leftarrow \mathsf{false}$
$\mathcal{A}^{Encrypt, Decrypt}(\,)$
return win

Oracle $Encrypt(N, A, P)$
$(C, T) \leftarrow \Pi.\mathsf{Enc}(K, N, A, P)$
$sent \leftarrow sent \cup \{(N, A, C, T)\}$
return (C, T)

Oracle $Decrypt(N, A, C, T)$
$P \leftarrow \Pi.\mathsf{Dec}(K, N, A, C, T)$
if $(P \neq \perp) \wedge ((N, A, C, T) \notin sent)$:
  $win \leftarrow \mathsf{true}$
return P

Введем модель противника CPA-res («Chosen Plaintext Attack - resilience»), определенную в работе [9].

Определение III.3 (CPA-res)**.** Преимущество противника $\mathcal{A}$ в модели CPA-res для AEAD-схемы Π определяется следующим образом:

$$\mathsf{Adv}^{\text{CPA-res}}_{\Pi}(\mathcal{A}) = \Pr\left[\mathbf{Exp}^{\text{CPA-res-1}}_{\Pi}(\mathcal{A}) \to 1\right] - \\ - \Pr\left[\mathbf{Exp}^{\text{CPA-res-0}}_{\Pi}(\mathcal{A}) \to 1\right],$$

где эксперименты $\mathbf{Exp}^{\text{CPA-res-}b}$, $b \in \{0, 1\}$, описаны ниже:

$\mathbf{Exp}^{\text{CPA-res-}b}_{\Pi}(\mathcal{A})$
$K \xleftarrow{\$} \Pi.\mathsf{Gen}(\,)$
$\mathcal{L}_1, \mathcal{L}_2 \leftarrow \emptyset$
$b \xleftarrow{\$} \mathcal{A}^{O_1, O_2}(\,)$
return b

Oracle $O_2(N, A, P)$
if $N \in \mathcal{L}_1$:
  return $\perp$
$(C, T) \leftarrow \Pi.\mathsf{Enc}(K, N, A, P)$
if $N \notin \mathcal{L}_2$:
  $\mathcal{L}_2 \leftarrow \mathcal{L}_2 \cup \{N\}$
return (C, T)

Oracle $O_1(N, A, P)$
if $N \in \mathcal{L}_1 \cup \mathcal{L}_2$:
  return $\perp$
if $b = 1$:
  $(C, T) \leftarrow \Pi.\mathsf{Enc}(K, N, A, P)$
else :
  $C \parallel T \xleftarrow{\mathcal{U}} \{0, 1\}^{|P|+s}$
$\mathcal{L}_1 \leftarrow \mathcal{L}_1 \cup \{N\}$
return (C, T)

В работе [9] также вводится модель противника CCA-res («Chosen Ciphertext Attack - resilience»). Данная модель отличается от модели CPA-res тем, что она предоставляет дополнительный доступ к оракулу расшифрования, что является более релевантным с точки зрения практики. С помощью техники доказательства, описанной в [17], легко показать, что из стойкости в моделях MRAE-int и CPA-res следует стойкость в модели CCA-res. Поэтому мы рассматриваем только модель CPA-res.

IV. Режим MGM2

В данном разделе определяется AEAD-режим MGM2, который является модификацией режима MGM. Через $\text{MGM2}_{\mathsf{E},r,s}$ будем обозначать режим MGM2, который в качестве параметров использует блочный шифр E (с длиной блока n и длиной ключа k), длину вектора инициализации r, $\frac{n}{2} \leqslant r \leqslant \frac{3n}{4}$, и длину имитовставки s, $1 \leqslant s \leqslant n$.

Режим $\text{MGM2}[\mathsf{E}, r, s]$ определен для следующих множеств: $\boldsymbol{K} = \{0,1\}^k$, $\boldsymbol{N} = \{0,1\}^r$, $\boldsymbol{A} = \boldsymbol{P} = \boldsymbol{C} = \{0,1\}^{\leqslant n(2^{n-r-2}-1)}$, $\boldsymbol{T} = \{0,1\}^s$. Дополнительно на длину открытого текста и ассоциированных данных накладывается следующее ограничение: $0 < |A| + |P| \leqslant n(2^{n-r-2}-1)$. Алгоритмы генерации ключа, шифрования и расшифрования определены на Рис. 1.

Отличия от MGM**.** Главное отличие режима MGM2 от оригинального режима MGM состоит в модификации способа вычисления маскированных значений для процедуры шифрования (Γ_i), коэффициентов мультилинейной функции (H_i) и формирования имитовставки T. В режиме MGM2 входные значения блочного шифра, используемые для различных целей (а именно, для формирования значений Γ_i, H_i, T), не пересекаются за счет фиксации определенных битов. Такая модификация позволяет улучшить оценки стойкости, так как, в отличие от режима MGM, коллизия между входами в блочный шифр возможна только среди значений τ.

A. Целостность

Через $\text{MGM2}_{Perm(n),r,s}$ ($\text{MGM2}_{Func(n),r,s}$) обозначим режим MGM2, который использует случайную подстановку π (случайную функцию ρ) вместо преобразования E_K.

MGM2.Gen()

$K \xleftarrow{\mathcal{U}} \{0,1\}^k$
return K

MGM2.Enc(K, N, A, P)

$h \leftarrow |A|_n, q \leftarrow |P|_n$
$\ell \leftarrow h + q + 1$
$u \leftarrow n - r - 2$
..... Encryption .....
for $i = 1 \dots q$ **do**:
  $Y_i \leftarrow N \| 00 \| \mathrm{str}_u(i-1)$
  $\Gamma_i \leftarrow \mathsf{E}_K(Y_i)$
$\Gamma \leftarrow \mathrm{msb}_{|P|}(\Gamma_1 \| \dots \| \Gamma_q)$
$C \leftarrow P \oplus \Gamma$
..... Padding .....
$a \leftarrow n\lceil |A|_n - |A|$
$c \leftarrow n\lceil |C|_n - |C|$
$L \leftarrow \mathrm{str}_{n/2}(|A|) \| \mathrm{str}_{n/2}(|C|)$
$M \leftarrow A \| 0^a \| C \| 0^c \| L$
..... Tag generation .....
for $i = 1 \dots \ell$ **do**:
  $Z_i \leftarrow N \| 01 \| \mathrm{str}_u(i-1)$
  $H_i \leftarrow \mathsf{E}_K(Z_i)$
$\tau \leftarrow \mathsf{Set1}_r \left(\bigoplus_{i=1}^{l} M_i \otimes H_i \right)$
$T \leftarrow \mathrm{msb}_s(\mathsf{E}_K(\tau))$
return (C, T)

MGM2.Dec(K, N, A, C, T)

$h \leftarrow |A|_n, q \leftarrow |C|_n$
$\ell \leftarrow h + q + 1$
$u \leftarrow n - r - 2$
..... Padding .....
$a \leftarrow n\lceil |A|_n - |A|$
$c \leftarrow n\lceil |C|_n - |C|$
$L \leftarrow \mathrm{str}_{n/2}(|A|) \| \mathrm{str}_{n/2}(|C|)$
$M \leftarrow A \| 0^a \| C \| 0^c \| L$
..... Tag verification .....
for $i = 1 \dots \ell$ **do**:
  $Z_i \leftarrow N \| 01 \| \mathrm{str}_u(i-1)$
  $H_i \leftarrow \mathsf{E}_K(Z_i)$
$\tau \leftarrow \mathsf{Set1}_r \left(\bigoplus_{i=1}^{l} M_i \otimes H_i \right)$
$T' \leftarrow \mathrm{msb}_s(\mathsf{E}_K(\tau))$
if $T' \neq T$: **return** $\perp$
..... Decryption .....
for $i = 1 \dots q$ **do**:
  $Y_i \leftarrow N \| 00 \| \mathrm{str}_u(i-1)$
  $\Gamma_i \leftarrow \mathsf{E}_K(Y_i)$
$\Gamma \leftarrow \mathrm{msb}_{|C|}(\Gamma_1 \| \dots \| \Gamma_q)$
$P \leftarrow C \oplus \Gamma$
return P

Рис. 1. AEAD-режим MGM2

Теорема IV.1. *Для любого* MRAE-int *противника* $\mathcal{A}$*, делающего не более* q_E *запросов к оракулу* $Encrypt$ *и не более* q_D *запросов к оракулу* $Decrypt$*, причем суммарное количество блоков ассоциированных данных в запросах равно* σ_A*, а суммарное количество блоков открытых текстов и шифртекстов равно* σ_P*, справедливо*

$$\mathsf{Adv}^{\text{MRAE-int}}_{\text{MGM2}_{Perm(n),r,s}}(\mathcal{A}) \leqslant \left(\frac{q(q-1)}{2^n} + \frac{q_D}{2^s} \right) \cdot \cdot \left(1 - \frac{\sigma - 1}{2^n} \right)^{-\sigma/2}, \quad (1)$$

где $q = q_E + q_D$ *и* $\sigma = 2\sigma_P + \sigma_A + 2q$.

В частном случае, когда значение σ не превышает $2^{n/2}$ и $n \geq 128$, оценка (1) принимает следующий вид:

$$\mathsf{Adv}^{\text{MRAE-int}}_{\text{MGM2}_{Perm(n),r,s}}(\mathcal{A}) \leqslant 1.7 \left(\frac{q(q-1)}{2^n} + \frac{q_D}{2^s} \right). \quad (2)$$

Заметим, что для оригинального режима MGM, если суммарная длина обработанных данных достигает $2^{n/2}$ блоков, то оценка из работы [4] вырождается. Оценка для режима MGM2 выродится, только если будет обработано $2^{n/2}$ сообщений. Данный результат также позволяет использовать MGM2 как функцию выработки имитовставки путем фиксации N. Далее представлено доказательство Теоремы IV.1.

MGM2-MAC.Gen()

$\rho, \rho' \xleftarrow{\mathcal{U}} Func(n)$
$K \leftarrow (\rho, \rho')$
return K

PreTag(ρ', N, M)

$l \leftarrow |M|_n$
$u \leftarrow n - r - 2$
for $i = 1 \dots \ell$ **do**:
  $H_i \leftarrow \rho'(N \| 01 \| \mathrm{str}_u(i-1))$
$\tau \leftarrow \mathsf{Set1}_r \left(\bigoplus_{i=1}^{l} (M_i \otimes H_i) \right)$
return τ

MGM2-MAC.Tag(K, N, M)

$\tau \leftarrow \mathsf{PreTag}(\rho', N, M)$
$T \leftarrow \mathrm{msb}_s(\rho(\tau))$
return T

MGM2-MAC.Verify(K, N, M, T)

$\tau \leftarrow \mathsf{PreTag}(\rho', N, M)$
$T' \leftarrow \mathrm{msb}_s(\rho(\tau))$
if $T' \neq T$: **return** false
return true

Рис. 2. Схема MGM2-MAC

Доказательство. Доказательство проводится в два этапа. На первом этапе вводится вспомогательный абстрактный режим выработки имитовставки MGM2-MAC$_{r,s}$ и доказывается оценка его стойкости в модели UF-CMA (см. Раздел IV-A1).

На втором этапе показывается, что из стойкости MGM2-MAC$_{r,s}$ в модели UF-CMA следует стойкость режима MGM2$_{Func(n),r,s}$ в модели MRAE-int (см. Раздел IV-A2).

Оценка стойкости режима MGM2$_{Perm(n),r,s}$ напрямую получается из оценки стойкости режима MGM2$_{Func(n),r,s}$, используя результат Бернштейна [18], Theorem 2.3. Согласно данной теореме для любого алгоритма $\mathcal{D}^f$ с оракулом $f\colon \{0,1\}^n \to \{0,1\}^n$, который делает не более q запросов, верно следующее неравенство:

$$\Pr[\mathcal{D}^\pi \to 1] \leqslant \Pr[\mathcal{D}^\rho \to 1] \cdot \left(1 - \frac{q-1}{2^n} \right)^{-q/2},$$

where $\pi \xleftarrow{\mathcal{U}} Perm(n)$ and $\rho \xleftarrow{\mathcal{U}} Func(n)$.

Положив в качестве алгоритма $\mathcal{D}$ алгоритм $\mathbf{Exp}^{\text{MRAE-int}}_{\text{MGM2}_{\cdot,r,s}}(\mathcal{A})$, в котором вместо вызовов блочного шифра осуществляется запрос к оракулу, мы получим искомую оценку. □

1) Стойкость MGM2-MAC*:* Введем вспомогательную схему выработки имитовставки с вектором инициализации MGM2-MAC$_{r,s}$, основанную на схеме MGM2$_{Func(n),r,s}$. Такая схема определяется как набор алгоритмов MAC $= \{\mathsf{MAC.Gen}, \mathsf{MAC.Tag}, \mathsf{MAC.Verify}\}$, для схемы MGM2-MAC$_{r,s}$ данные алгоритмы определены на Рис. 2. Данная схема определена для множества сообщений $\{M = M_1 \| \dots \| M_\ell \colon M_i \in \{0,1\}^n,\ M_\ell \neq 0^n,\ 1 \leqslant \ell \leqslant 2^{n-r-2}\}$ (длина сообщения кратна n, последний блок ненулевой).

Сначала введем модель PRF для схемы выработки имитовставки с вектором инициализации и получим в ней оценку для схемы MGM2-MAC.

Определение IV.1 (PRF)**.** Для схемы MAC преимущество любого противника $\mathcal{A}$ в модели PRF определяется

$\mathbf{Exp}^b(\mathcal{A}),\ b \in \{0,1\}$

$(\rho, \rho') \xleftarrow{\$} \mathsf{MGM2\text{-}MAC.Gen}(\,)$
$bad \leftarrow \mathsf{false}$
$tau, sent \leftarrow \emptyset$
$b' \xleftarrow{\$} \mathcal{A}^{Tag^b}(\,)$
return b'

Oracle $Tag^b(N, M)$

if $(N, M) \in sent$:
  return $\perp$
$\tau \leftarrow \mathsf{PreTag}(\rho', N, M)$
$T \leftarrow \mathrm{msb}_s(\rho(\tau))$
if $\tau \in tau$:
  $bad \leftarrow \mathsf{true}$
  if $b = 0$: $T \xleftarrow{\mathcal{U}} \{0,1\}^s$
$tau \leftarrow tau \cup \{\tau\}$
$sent \leftarrow sent \cup \{(N, M)\}$
return T

Рис. 3. Эксперименты $\mathbf{Exp}^0$ и $\mathbf{Exp}^1$

следующим образом:

$$\mathsf{Adv}^{\mathrm{PRF}}_{\mathsf{MAC}}(\mathcal{A}) = \Pr\left[\mathbf{Exp}^{\mathrm{PRF}-1}_{\mathsf{MAC}}(\mathcal{A}) \to 1\right] - \\ - \Pr\left[\mathbf{Exp}^{\mathrm{PRF}-0}_{\mathsf{MAC}}(\mathcal{A}) \to 1\right],$$

где эксперименты $\mathbf{Exp}^{\mathrm{PRF}-b}_{\mathsf{MAC}}(\mathcal{A}),\ b \in \{0,1\}$, описаны ниже.

$\mathbf{Exp}^{\mathrm{PRF}-b}_{\mathsf{MAC}}(\mathcal{A})$

if $b = 1$:
  $K \xleftarrow{\$} \mathsf{MAC.Gen}(\,)$
$sent \leftarrow \emptyset$
$b' \xleftarrow{\$} \mathcal{A}^{Tag^b}(\,)$
return b'

Oracle $Tag^1(N, M)$

if $(N, M) \in sent$:
  return $\perp$
$\boldsymbol{T} \leftarrow \mathsf{MAC.Tag}(K, N, M)$
$sent \leftarrow sent \cup \{(N, M)\}$
return T

Oracle $Tag^0(N, M)$

if $(N, M) \in sent$:
  return $\perp$
$T \xleftarrow{\mathcal{U}} \{0,1\}^s$
$sent \leftarrow sent \cup \{(N, M)\}$
return T

Лемма IV.1. *Для любого противника $\mathcal{A}$ в модели PRF, делающего не более q запросов к оракулу Tag:*

$$\mathsf{Adv}^{\mathrm{PRF}}_{\mathrm{MGM2\text{-}MAC}_{r,s}}(\mathcal{A}) \leqslant \frac{q(q-1)}{2^n}.$$

Доказательство. Определим эксперименты $\mathbf{Exp}^0$ и $\mathbf{Exp}^1$ (см. Рис. 3), которые отличаются от эксперимента $\mathbf{Exp}^{\mathrm{PRF}-1}_{\mathrm{MGM2\text{-}MAC}_{r,s}}$ следующим образом. На этапе инициализации дополнительно вводится множество tau, которое инициализируется пустым множеством, а также флаг bad, который изначально полагается равным значению false. Во время выполнения эксперимента проверяется, лежит ли очередное значение τ в множестве tau, и если лежит, то флаг bad выставляется равным true, после этого значение τ добавляется в множество. Также, в эксперименте $\mathbf{Exp}^0$ значение имитовставки T выбирается из множества $\{0,1\}^s$ случайно равновероятно, в случае, если $\tau \in tau$ (см. строку в рамке, Рис. 3).

Легко заметить, что эксперимент $\mathbf{Exp}^1$ в точности совпадает с экспериментом $\mathbf{Exp}^{\mathrm{PRF}-1}_{\mathrm{MGM2\text{-}MAC}_{r,s}}$. Более того, для любого противника $\mathcal{A}$ значение $\Pr\left[\mathbf{Exp}^0(\mathcal{A}) \Rightarrow 1\right]$ в точности равно значению $\Pr\left[\mathbf{Exp}^{\mathrm{PRF}-0}_{\mathrm{MGM2\text{-}MAC}_{r,s}}(\mathcal{A}) \Rightarrow 1\right]$. Действительно, в эксперименте $\mathbf{Exp}^0$ все значения T генерируются в соответствии с равновероятным распределением, как и в эксперименте $\mathbf{Exp}^{\mathrm{PRF}-0}_{\mathrm{MGM2\text{-}MAC}_{r,s}}$ по следующим причинам. Для запросов, в которых соответствующее значение τ является новым (т.е. не лежит в текущем множестве tau), к данному новому входу применяется случайная функция ρ и поэтому возвращает равновероятные значения T. Для других запросов значение T явно выбирается случайно равновероятно (см. выделенную в рамки строку на Рис. 3). Поэтому

$$\mathsf{Adv}^{\mathrm{PRF}}_{\mathrm{MGM2\text{-}MAC}_{r,s}}(\mathcal{A}) = \Pr\left[\mathbf{Exp}^1(\mathcal{A}) \Rightarrow 1\right] - \\ - \Pr\left[\mathbf{Exp}^0(\mathcal{A}) \Rightarrow 1\right].$$

Заметим, что до выставления флага bad равным true (обозначим это событие как $bad = \mathsf{true}$) эксперименты $\mathbf{Exp}^0$ и $\mathbf{Exp}^1$ функционируют идентичным образом. Поэтому (согласно Лемме 2, [16]) верно следующее неравенство:

$$\Pr\left[\mathbf{Exp}^1(\mathcal{A}) \Rightarrow 1\right] - \Pr\left[\mathbf{Exp}^0(\mathcal{A}) \Rightarrow 1\right] \leqslant \Pr[bad = \mathsf{true}].$$

Оценим величину $\Pr[bad = \mathsf{true}]$. Без ограничения общности, будем считать, что противник является детерминированным и делает q попарно различных запросов$(N_i, M^i),\ i = 1, \ldots, q$. Будем использовать нотацию coll^i, $i = 2, \ldots, q$, для обозначения события, что флаг bad принял значение true после обработки первых i запросов. Тогда,

$$\Pr[bad = \mathsf{true}] = \sum_{i=2}^{q} \Pr\left[\mathsf{coll}^i \cap \overline{\mathsf{coll}^{i-1}}\right].$$

Оценим вероятность $\Pr\left[\mathsf{coll}^i \cap \overline{\mathsf{coll}^{i-1}}\right]$ для любого $i = 2, \ldots, q$.

Заметим, что каждый i-й запрос является парой (N_i, M^i), где $M^i = M^i_1 \| \ldots \| M^i_{l_i}$, $M^i_j \in \{0,1\}^n$, и определяется значениями $T_1, \ldots, T_{i-1}$, полученными на предыдущих запросах. Без ограничения общности, будем считать, что $l_1 = \ldots = l_i$. Действительно, если это не так, то мы всегда можем дополнить сообщение нулевыми блоками до длины $l := \max(l_1, \ldots, l_i)$. Данное дополнение не повлияет на значение имитовставки, а дополненные сообщения останутся попарно различными, так как $M^j_{l_j} \neq 0^n$. Поэтому значения $T_1, \ldots, T_{i-1}$ однозначно определяют значение l и пары $(N_1, M^1), \ldots, (N_i, M^i)$.

Для фиксированного N_j обозначим через $\widetilde{H}^j_k$, $j = 1, \ldots, i;\ k = 1, \ldots, l$, случайную величину $\widetilde{\rho}'(N_j \| 01 \| \mathrm{str}_{n-r-2}(k-1))$.

Заметим, что $\Pr\left[\widetilde{H}^j_k = B\right] = \frac{1}{2^n}$ для любого $B \in \{0,1\}^n$. Также заметим, что случайные величины $\widetilde{H}^j_k$ и $\widetilde{H}^t_k$ для любых $j \neq t$ и любого k независимы, при этом $\Pr\left[\widetilde{H}^j_k = \widetilde{H}^t_k\right] = 1$ тогда и только тогда, когда $N_k = N_j$.

Для краткости обозначим через $\widetilde{H^j}$ набор случайных величин $(\widetilde{H}^j_1, \ldots, \widetilde{H}^j_\ell)$. Также для набора $H = (H_1, \ldots, H_\ell)$ и сообщения $M = M_1 \| \ldots \| M_\ell$ через $\tau(H, M)$ обозначим

функцию $\mathsf{Set1}_r\left(\bigoplus\limits_{k=1}^{l} H_k \otimes M_k\right)$. Таким образом, мы имеем

$$\Pr\left[\mathsf{coll}^i \cap \overline{\mathsf{coll}^{i-1}}\right] = \sum_{T_1,\ldots,T_{i-1}} \Pr\left[\mathsf{coll}^i \cap \overline{\mathsf{coll}^{i-1}} \cap \{\widetilde{T_j} = T_j\}_{j=1}^{i-1}\right],$$

где через $\widetilde{T_j}$ обозначены случайные величины $\mathrm{msb}_s(\widetilde{\rho}(\tau(\widetilde{H^j}, M^j)))$ и суммирование ведется по всем наборам $(T_1,\ldots,T_{i-1}) \in (\{0,1\}^s)^{i-1}$.

Для фиксированных $(N_1, M^1),\ldots,(N_i, M^i)$ введем следующие условия на множество наборов $H^1,\ldots,H^i$, $H^j := (H^j_1,\ldots,H^j_\ell)$, $j = 1,\ldots,i$:

E_1: $\forall\ j,t,\ 1 \leqslant j < t \leqslant i-1$: $\tau(H^j, M^j) \neq \tau(H^t, M^t)$.

E_2: $\exists\ j,\ 1 \leqslant j \leqslant i-1$: $\tau(H^i, M^i) = \tau(H^j, M^j)$.

Для любых фиксированных $T_1,\ldots,T_{i-1}$ и, следовательно, фиксированных $(N_1, M^1),\ldots,(N_i, M^i)$ событие $\mathsf{coll}^i \cap \overline{\mathsf{coll}^{i-1}}$ возникает тогда и только тогда, когда случайные величины $\widetilde{H^1},\ldots,\widetilde{H^i}$ приняли такие значения $H^1,\ldots,H^i$, для которых выполнены условия E_1 и E_2. Для краткости мы будем обозначать события, что выполнены данные условия, таким же образом, а именно через E_1 и E_2 соответственно.

Заметим, что фиксация значений H^j, $j = 1,\ldots,i$, приводит к фиксации значений $\tau_j := \tau(H^j, M^j)$. Поэтому

$$\Pr\left[\mathsf{coll}^i \cap \overline{\mathsf{coll}^{i-1}}\right] = \sum_{T_1,\ldots,T_{i-1}} \Pr\left[\mathsf{E}_1 \cap \mathsf{E}_2 \cap \{\widetilde{T_j} = T_j\}_{j=1}^{i-1}\right] =$$

$$= \sum_{T_1,\ldots,T_{i-1}} \sum_{\substack{H^1,\ldots,H^i:\\ \mathsf{E}_1\cap\mathsf{E}_2}} \Pr\left[\begin{matrix}\{\widetilde{H^j} = H^j\}_{j=1}^{i}\cap\\ \{\mathrm{msb}_s(\widetilde{\rho}(\tau_j)) = T_j\}_{j=1}^{i-1}\end{matrix}\right] =$$

$$= \sum_{T_1,\ldots,T_{i-1}} \sum_{\substack{H^1,\ldots,H^i:\\ \mathsf{E}_1\cap\mathsf{E}_2}} \Pr\left[\{\widetilde{H^j} = H^j\}_{j=1}^{i}\right] \cdot \Pr\left[\{\mathrm{msb}_s(\widetilde{\rho}(\tau_j)) = T_j\}_{j=1}^{i-1}\right].$$

Здесь, суммирование ведется по всем $H^1,\ldots,H^i,\ H^j \in (\{0,1\}^n)^l$, для которых выполнены условия E_1 и E_2. Последний переход верен в силу того, что величины $\widetilde{\rho}$ и $\widetilde{H^j}$, $j = 1,\ldots,i$, независимы.

Рассмотрим значение $\Pr\left[\{\mathrm{msb}_s(\widetilde{\rho}(\tau_j)) = T_j\}_{j=1}^{i-1}\right]$. Для любых $T_1,\ldots,T_{i-1}$ и $H^1,\ldots,H^{i-1}$, для которых выполнено условие E_1, данная вероятность в точности равна вероятности выбора функции ρ, для которой $i-1$ фиксированным входам соответствуют выходы с фиксированными первыми s битами, а именно $\dfrac{1}{2^{s(i-1)}}$. Таким образом:

$$\Pr\left[\mathsf{coll}^i \cap \overline{\mathsf{coll}^{i-1}}\right] = \sum_{T_1,\ldots,T_{i-1}} \sum_{\substack{H^1,\ldots,H^i:\\ \mathsf{E}_1\cap\mathsf{E}_2}} \Pr\left[\{\widetilde{H^j} = H^j\}_{j=1}^{i}\right] \cdot \frac{1}{2^{s(i-1)}} =$$

$$= \frac{1}{2^{s(i-1)}} \sum_{T_1,\ldots,T_{i-1}} \Pr[\mathsf{E}_1 \cap \mathsf{E}_2] \leqslant \frac{1}{2^{s(i-1)}} \sum_{T_1,\ldots,T_{i-1}} \Pr[\mathsf{E}_2].$$

Теперь рассмотрим $\Pr[\mathsf{E}_2]$ при фиксированных $T_1,\ldots,T_{i-1}$ и, следовательно, при фиксированных $(N_1, M^1),\ldots,(N_i, M^i)$.

$$\Pr[\mathsf{E}_2] = \Pr\left[\exists\ j\colon\ \tau(\widetilde{H^i}, M^i) = \tau(\widetilde{H^j}, M^j)\right] = \Pr\left[\bigcup_{j=1}^{i-1}\left\{\tau(\widetilde{H^i}, M^i) = \tau(\widetilde{H^j}, M^j)\right\}\right] \leqslant \sum_{j=1}^{i-1} \Pr\left[\tau(\widetilde{H^i}, M^i) = \tau(\widetilde{H^j}, M^j)\right].$$

Оценим значение $p := \Pr\left[\tau(\widetilde{H^i}, M^i) = \tau(\widetilde{H^j}, M^j)\right]$ для любых $j = 1,\ldots,i-1$. Рассмотрим два случая:

1) $N_i \neq N_j$ (в данном случае $\widetilde{H^i_k}$ и $\widetilde{H^j_k}$ являются независимыми).
2) $N_i = N_j$ (в данному случае $\widetilde{H^i_k}$ и $\widetilde{H^j_k}$ являются зависимыми).

Первый случай:

$$p = \frac{\#\{H^i, H^j\colon \tau(H^i, M^i) = \tau(H^j, M^j)\}}{2^{2nl}}.$$

$$\#\{H^i, H^j\colon \tau(H^i, M^i) = \tau(H^j, M^j)\} = \#\Big\{H^i, H^j\colon \bigoplus_{k=1}^{l} H^i_k \otimes M^i_k = \bigoplus_{k=1}^{l} H^j_k \otimes M^j_k\Big\} + \#\Big\{H^i, H^j\colon \bigoplus_{k=1}^{l} H^i_k \otimes M^i_k = \bigoplus_{k=1}^{l} H^j_k \otimes M^j_k \oplus \mathsf{Set1}_r(0^n)\Big\}.$$

Так как $M^i_{\ell_i} \neq 0^n$ для любого i, мощность множества равна $2 \cdot 2^{n(2l-1)}$ и $p = \dfrac{2}{2^n}$.

Второй случай:

$$p = \frac{\#\{H^i\colon \tau(H^i, M^i) = \tau(H^i, M^j)\}}{2^{nl}}.$$

$$\#\{H^i\colon \tau(H^i, M^i) = \tau(H^i, M^j)\} = \#\Big\{H^i\colon \bigoplus_{k=1}^{l} H^i_k \otimes (M^i_k \oplus M^j_k) = 0^n\Big\} + \#\Big\{H^i\colon \bigoplus_{k=1}^{l} H^i_k \otimes (M^i_k \oplus M^j_k) = \mathsf{Set1}_r(0^n)\Big\}.$$

Так как для одинаковых векторов инициализации M^i и M^j должны быть различными, существует k, такой что $M^i_k \oplus M^j_k \neq 0^n$. Таким образом, мощность множества равна $2 \cdot 2^{n(l-1)}$ и $p = \dfrac{2}{2^n}$.

В итоге получаем искомую оценку:

$$\Pr[bad = \mathsf{true}] = \sum_{i=2}^{q} \frac{1}{2^{s(i-1)}} \sum_{T_1,\ldots,T_{i-1}} \sum_{j=1}^{i-1} \frac{2}{2^n} = \sum_{i=2}^{q} \frac{i-1}{2^{n-1}} = \frac{q(q-1)}{2^n}.$$

□

Теперь введем стандартную модель UF-CMA для схем выработки имитовставки с вектором инициализации и получим оценку в данной модели для схемы MGM2-MAC.

Определение IV.2. Для схемы MAC преимущество противника $\mathcal{A}$ в модели UF-CMA определяется следующим образом:

$$\mathsf{Adv}^{\text{UF-CMA}}_{\mathsf{MAC}}(\mathcal{A}) = \Pr\left[\mathbf{Exp}^{\text{UF-CMA}}_{\mathsf{MAC}}(\mathcal{A}) \to 1\right],$$

где эксперимент $\mathbf{Exp}^{\text{UF-CMA}}_{\mathsf{MAC}}(\mathcal{A})$ описан ниже:

$\mathbf{Exp}^{\text{UF-CMA}}_{\mathsf{MAC}}(\mathcal{A})$
$K \xleftarrow{\$} \mathsf{MAC.Gen}(\,)$
$sent \leftarrow \emptyset$
$win \leftarrow \mathsf{false}$
$\mathcal{A}^{Tag, Verify}(\,)$
return win

Oracle $Tag(N, M)$
if $(N, M) \in sent$:
  return $\perp$
$T \leftarrow \mathsf{MAC.Tag}(K, N, M)$
$sent \leftarrow sent \cup \{(N, M)\}$
return T

Oracle $Verify(N, M, T)$
$res \leftarrow \mathsf{MAC.Vf}(K, N, M, T)$
if $res \wedge ((N, M) \notin sent)$:
  $win \leftarrow \mathsf{true}$
return res

Используя Предложение 7.3 [16] и Лемму IV.1 легко доказать следующее утверждение.

Следствие IV.1. *Для любого противника $\mathcal{A}$ в модели* UF-CMA*, делающего не более q_T запросов к оракулу Tag и не более q_V запросов к оракулу $Verify$:*

$$\mathsf{Adv}^{\text{UF-CMA}}_{\text{MGM2-MAC}_{r,s}}(\mathcal{A}) \leqslant \frac{q(q-1)}{2^n} + \frac{q_V}{2^s},$$

где $q = q_T + q_V$.

2) Стойкость MGM2 *со случайной функцией:*

Лемма IV.2. *Для любого противника $\mathcal{A}$ в модели* MRAE-int*, делающего не более q_E запросов к оракулу $Encrypt$ и не более q_D запросов к оракулу $Decrypt$, существует противник $\mathcal{B}$ в модели* UF-CMA*, делающий не более q_E запросов к оракулу Tag и не более q_D запросов к оракулу $Verify$, такой что*

$$\mathsf{Adv}^{\text{MRAE-int}}_{\text{MGM2}_{Func(n),r,s}}(\mathcal{A}) \leqslant \mathsf{Adv}^{\text{UF-CMA}}_{\text{MGM2-MAC}_{r,s}}(\mathcal{B})$$

Доказательство. Построим противника $\mathcal{B}$, который использует противника $\mathcal{A}$ в качестве черного ящика. Противник $\mathcal{B}$ (см. Рис. 4) перехватывает запросы противника $\mathcal{A}$ и самостоятельно их обрабатывает с использованием своих оракулов. Для шифрования/расшифрования $\mathcal{B}$ реализует процедуру «lazy sampling» для функции ρ''. Для вычисления/проверки имитовставки противник $\mathcal{B}$ реализует процедуру дополнения и отправляет соответствующие запросы своему оракулу.

Заметим, что противник $\mathcal{B}$ симулирует для противника $\mathcal{A}$ в точности эксперимент $\mathbf{Exp}^{\text{MRAE-int}}_{\text{MGM2}_{Func(n),r,s}}$. Действительно, так как для схемы $\text{MGM2}_{Func(n),r,s}$ входы в случайную функцию в случае 1) вычисления имитовставки, 2) вычисления значения H_i и 3) вычисления значений Γ_i является различными (в силу фиксации битов у входов), использование одной случайной функции абсолютно неотличимо от использования трех различных случайных функций ρ, ρ', ρ'' для этих трех случаев. Также заметим, что сообщения M, формируемые противником $\mathcal{B}$, удовлетворяют условиям на множество сообщений для схемы $\text{MGM2-MAC}_{r,s}$.

$\mathcal{B}^{Tag, Verify}_{\mathcal{A}}$
$\rho'' \xleftarrow{\mathcal{U}} Func(n)$
return $\mathcal{A}^{SEnc, SDec}(\,)$

$SEnc(N, A, P)$
$h \leftarrow |A|_n, t \leftarrow |P|_n$
$u \leftarrow n - r - 2$
..... Encryption .....
for $i = 1 \ldots t$ **do**:
  $Y_i \leftarrow N \| 00 \| \text{str}_u(i-1)$
  $\Gamma_i \leftarrow \rho''(Y_i)$
$\Gamma \leftarrow \text{msb}_{|P|}(\Gamma_1 \parallel \ldots \parallel \Gamma_t)$
$C \leftarrow P \oplus \Gamma$
..... Padding .....
$a \leftarrow n|A|_n - |A|$
$c \leftarrow n|C|_n - |C|$
$L \leftarrow \text{str}_{n/2}(|A|) \parallel \text{str}_{n/2}(|C|)$
$M \leftarrow A \| 0^a \| C \| 0^c \| L$
..... Tag Genetation .....
$T \leftarrow Tag(N, M)$
return (C, T)

Oracle $SDec(N, A, C, T)$
$h \leftarrow |A|_n, t \leftarrow |C|_n$
$u \leftarrow n - r - 2$
..... Padding .....
$a \leftarrow n|A|_n - |A|$
$c \leftarrow n|C|_n - |C|$
$L \leftarrow \text{str}_{n/2}(|A|) \parallel \text{str}_{n/2}(|C|)$
$M \leftarrow A \| 0^a \| C \| 0^c \| L$
..... Tag Verification .....
if $Verify(N, M, T) = 0$:
  return $\perp$
..... Decryption .....
for $i = 1 \ldots t$ **do**:
  $Y_i \leftarrow N \| 00 \| \text{str}_u(i-1)$
  $\Gamma_i \leftarrow \rho''(Y_i)$
$\Gamma \leftarrow \text{msb}_{|C|}(\Gamma_1 \parallel \ldots \parallel \Gamma_t)$
$P \leftarrow C \oplus \Gamma$
return P

Рис. 4. Противник $\mathcal{B}$

Если противник $\mathcal{A}$ успешно формирует подделку, то противник $\mathcal{B}$ также успешно формирует подделку в своем эксперименте $\mathbf{Exp}^{\text{UF-CMA}}_{\text{MGM2-MAC}_{r,s}}(\mathcal{B})$. Действительно, прямой проверкой можно убедиться, что если $\mathcal{A}$ делает нетривиальный корректный запрос (N, A, C, T) к оракулу $Decrypt$, то противник $\mathcal{B}$ делает соответствующий запрос $(N, M = A \| 0^a \| C \| 0^c \| L, T)$ к оракулу $Verify$, который также будет корректным и нетривиальным. □

B. Конфиденциальность

Теорема IV.2. *Для любого противника $\mathcal{A}$ в модели* CPA-res*, делающего не более q_1 запросов к оракулу O_1 и не более q_2 запросов к оракулу O_2, где суммарная длина ассоциированных данных не превосходит σ_A блоков, а суммарная длина открытых текстов не превосходит σ_P блоков,*

$$\mathsf{Adv}^{\text{CPA-res}}_{\text{MGM2}_{Perm(n),r,s}}(\mathcal{A}) \leqslant \frac{\sigma^2}{2^n} + \frac{q(q-1)}{2^{n-1}}, \qquad (3)$$

где $q = q_1 + q_2$ и $\sigma = 2\sigma_P + \sigma_A + 2q$.

Доказательство. Сначала применим результат работы [19] для замены семейства $Perm(n)$ на семейство $Func(n)$ (это даст дополнительный член $\frac{\sigma^2}{2^n}$ в оценке), и далее получим оценку в модели CPA-res для схемы $\text{MGM2}_{Func(n),r,s}$.

Оценку для схемы $\text{MGM2}_{Func(n),r,s}$ можно получить аналогичным Теореме IV.1 образом. Действительно, шифртексты C, полученные от оракула O_1, абсолютно неотличимы от случайных равновероятных строк, так как входы в случайную функцию ρ, используемые для вычисления значений Γ_i, всегда уникальны.

Неотличимость имитовставок T, полученных от оракула O_1, от случайных равновероятных строк можно оценить путем построения двух противников в модели PRF для схемы MGM2-MAC, которые используют противника $\mathcal{A}$ в качестве черного ящика. Таким образом, $\mathsf{Adv}^{\text{CPA-res}}_{\text{MGM2}_{Func(n),r,s}}(\mathcal{A}) \leqslant \frac{q(q-1)}{2^{n-1}}$. □

V. Заключение

В настоящей работе предложен новый режим аутентифицированного шифрования MGM2. Для данного режима были доказаны оценки стойкости в расширенных моделях MRAE-int и CPA-res, которые учитывают возможность повторного использования вектора инициализации. На основе полученных оценок стойкости был сделан вывод, что стойкость режима MGM2 даже в усиленных моделях превышает стойкость режима MGM, на базе которого был разработан режим MGM2, в базовых моделях.

В дальнейших работах мы планируем разработать SIV-конструкцию (см. [12]) на основе режима MGM2 для обеспечения конфиденциальности в модели MRAE. Также нашей целью является внедрение механизмов смены ключей в режим MGM2 для увеличения срока жизни ключа и достижения новых свойств безопасности, таких как устойчивость к утечкам.

Библиография

БИБЛИОГРАФИЯ

[1] M. Bellare и C. Namprempre, «Authenticated encryption: Relations among notions and analysis of the generic composition paradigm», *Advances in Cryptology — ASIACRYPT 2000. ASIACRYPT 2000. Lecture Notes in Computer Science*, т. 1976, 2000.

[2] «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицированное шифрование», *Федеральное агентство по техническому регулированию и метрологии (Росстандарт)*, 2019.

[3] P. Rogaway, «Nonce-Based Symmetric Encryption», *Fast Software Encryption. FSE 2004. Lecture Notes in Computer Science*, т. 3017, 2004.

[4] L. Akhmetzyanova, E. Alekseev, G. Karpunin и V. Nozdrunov, «Security of Multilinear Galois Mode (MGM)», *IACR Cryptology ePrint Archive*, т. 2019/123, 2019.

[5] E. Andreeva и et al, «How to Securely Release Unverified Plaintext in Authenticated Encryption», *Advances in Cryptology – ASIACRYPT 2014. Lecture Notes in Computer Science*, т. 8873, 2014.

[6] J. Black, P. Rogaway и T. Shrimpton, «Encryption-Scheme Security in the Presence of Key-Dependent Messages», *In Revised Papers from the 9th Annual International Workshop on Selected Areas in Cryptography (SAC '02)*, 2002.

[7] P. Rogaway и T. Shrimpton, «A provable-security treatment of the key-wrap problem», *Annual International Conference on the Theory and Applications of Cryptographic Techniques. Lecture Notes in Computer Science*, т. 4004, 2006.

[8] Е. Алексеев, Л. Ахметзянова, А. Бабуева и С. Смышляев, *Прикладная дискретная математика*, т. 49, 2020.

[9] T. Ashur, O. Dunkelman и A. Luykx, «Boosting authenticated encryption robustness with minimal modifications», *Advances in Cryptology – CRYPTO 2017. Lecture Notes in Computer Science*, т. 10403, 2017.

[10] V. Hoang, T. Krovetz и P. Rogaway, «Robust Authenticated-Encryption AEZ and the Problem That It Solves», *dvances in Cryptology – EUROCRYPT 2015. EUROCRYPT 2015. Lecture Notes in Computer Science*, т. 9056, 2015.

[11] T. Shrimpton и R. Terashima, «A modular framework for building variable-input-length tweakable ciphers», *International Conference on the Theory and Application of Cryptology and Information Security. Lecture Notes in Computer Science*, т. 8269, 2013.

[12] S. Gueron и Y. Lindell, «GCM-SIV: full nonce misuse-resistant authenticated encryption at under one cycle per byte», *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015.

[13] A. Kurochkin и D. Fomin, «MGM Beyond the Birthday Bound», *8th Workshop on Current Trends in Cryptology (CTCrypt 2019)*, 2019.

[14] «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования», *Федеральное агентство по техническому регулированию и метрологии (Росстандарт)*, 2018.

[15] L. Akhmetzyanova, E. Alekseev, S. Smyshlyaev и I. Oshkin, «On Internal Re-keying», *Advances in Cryptology – Security Standardisation Research 2020. Lecture Notes in Computer Science*, т. 12529, 2020.

[16] M. Bellare и P. Rogaway, «The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs», *Advances in Cryptology — EUROCRYPT 2006. Lecture Notes in Computer Science*, т. 4004, 2006.

[17] T. Shrimpton, «A Characterization of Authenticated-Encryption as a Form of Chosen-Ciphertext Security», *IACR Cryptology ePrint Archive*, т. 2004/272, 2004.

[18] D. Bernstein, «Stronger Security Bounds for Permutations», 2005. url: http://cr.yp.to/papers.html.

[19] D. Chang и M. Nandi, «A Short Proof of the PRP/PRF Switching Lemma», *IACR Cryptology ePrint Archive*, т. 2008/078, 2008.

[20] «CAESAR competion», url: https://competitions.cr.yp.to/caesar.html.

Misuse-resistant MGM2 mode

Liliya Akhmetzyanova, Evgeny Alekseev, Alexandra Babueva, Andrey Bozhko, Stanislav Smyshlyaev

***Abstract*—We introduce a new AEAD mode – an** MGM2 **mode. For this mode we provide security bounds regarding extended security notions in the nonce-misuse setting. Misuse-resistance is crucial for applications for which there is no way to provide uniqueness of nonces. Moreover, this security property also provides additional protection against implementation errors, both accidental and adversarial.**

The MGM2 **mode was developed basing on the** MGM **(Multilinear Galois Mode) mode that was standardized in the Russian Federation. The main cryptographic core of the construction, namely multilinear function, is not changed. For the new mode we change the way how secret masking blocks and secret coefficients of the multilinear function are produced, decreasing the probability of collision between block cipher inputs. We provide the security bounds for** MGM2 **in the** MRAE**-integrity and** CPA-res **models. The obtained bounds show that the developed mode provides better security properties regarding even extended security notions than the original** MGM **mode provides regarding base security notions (in the nonce-respecting setting).**

***Keywords*—MGM, AEAD mode, security notion, security bounds, nonce-misuse, misuse-resistant**

References

REFERENCES

[1] M. Bellare and C. Namprempre, «Authenticated encryption: Relations among notions and analysis of the generic composition paradigm», *Advances in Cryptology — ASIACRYPT 2000. ASIACRYPT 2000. Lecture Notes in Computer Science*, vol. 1976, 2000.

[2] «Information technology. Cryptographic data security. Authenticated encryption block cipher operation modes», *Federal Agency on Technical Regulating and Metrology*, 2019.

[3] P. Rogaway, «Nonce-Based Symmetric Encryption», *Fast Software Encryption. FSE 2004. Lecture Notes in Computer Science*, vol. 3017, 2004.

[4] L. Akhmetzyanova, E. Alekseev, G. Karpunin, and V. Nozdrunov, «Security of Multilinear Galois Mode (MGM)», *IACR Cryptology ePrint Archive*, vol. 2019/123, 2019.

[5] E. Andreeva and et al, «How to Securely Release Unverified Plaintext in Authenticated Encryption», *Advances in Cryptology – ASIACRYPT 2014. Lecture Notes in Computer Science*, vol. 8873, 2014.

[6] J. Black, P. Rogaway, and T. Shrimpton, «Encryption-Scheme Security in the Presence of Key-Dependent Messages», *In Revised Papers from the 9th Annual International Workshop on Selected Areas in Cryptography (SAC '02)*, 2002.

[7] P. Rogaway and T. Shrimpton, «A provable-security treatment of the key-wrap problem», *Annual International Conference on the Theory and Applications of Cryptographic Techniques. Lecture Notes in Computer Science*, vol. 4004, 2006.

[8] L. Akhmetzyanova, E. Alekseev, A. Babueva, and S. Smyshlyaev, *Prikladnaya diskretnaya matematika*, vol. 49, 2020.

[9] T. Ashur, O. Dunkelman, and A. Luykx, «Boosting authenticated encryption robustness with minimal modifications», *Advances in Cryptology – CRYPTO 2017. Lecture Notes in Computer Science*, vol. 10403, 2017.

[10] V. Hoang, T. Krovetz, and P. Rogaway, «Robust Authenticated-Encryption AEZ and the Problem That It Solves», *dvances in Cryptology – EUROCRYPT 2015. EUROCRYPT 2015. Lecture Notes in Computer Science*, vol. 9056, 2015.

[11] T. Shrimpton and R. Terashima, «A modular framework for building variable-input-length tweakable ciphers», *International Conference on the Theory and Application of Cryptology and Information Security. Lecture Notes in Computer Science*, vol. 8269, 2013.

[12] S. Gueron and Y. Lindell, «GCM-SIV: full nonce misuse-resistant authenticated encryption at under one cycle per byte», *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015.

[13] A. Kurochkin and D. Fomin, «MGM Beyond the Birthday Bound», *8th Workshop on Current Trends in Cryptology (CTCrypt 2019)*, 2019.

[14] «Information technology. Cryptographic data security. Cryptographic algorithms accompanying the use of block ciphers», *Federal Agency on Technical Regulating and Metrology*, 2018.

[15] L. Akhmetzyanova, E. Alekseev, S. Smyshlyaev, and I. Oshkin, «On Internal Re-keying», *Advances in Cryptology – Security Standardisation Research 2020. Lecture Notes in Computer Science*, vol. 12529, 2020.

[16] M. Bellare and P. Rogaway, «The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs», *Advances in Cryptology — EUROCRYPT 2006. Lecture Notes in Computer Science*, vol. 4004, 2006.

[17] T. Shrimpton, «A Characterization of Authenticated-Encryption as a Form of Chosen-Ciphertext Security», *IACR Cryptology ePrint Archive*, vol. 2004/272, 2004.

[18] D. Bernstein, «Stronger Security Bounds for Permutations», 2005. [Online]. Available: http://cr.yp.to/papers.html.

[19] D. Chang and M. Nandi, «A Short Proof of the PRP/PRF Switching Lemma», *IACR Cryptology ePrint Archive*, vol. 2008/078, 2008.

[20] «CAESAR competion», [Online]. Available: https://competitions.cr.yp.to/caesar.html.