Math-Net.Ru

Общероссийский математический портал

В. В. Гусев, Легальные сообщения для некоторых функций имитозащиты блочных шифров, *Матем. вопр. криптогр.*, 2018, том 9, выпуск 1, 27–46

DOI: <https://doi.org/10.4213/mvk243>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 52.87.193.239

26 апреля 2023 г., 12:40:53

**Легальные сообщения для некоторых функций
имитозащиты блочных шифров**

В. В. Гусев

Технический комитет по стандартизации (ТК 26), Москва

Получено 11.V.2017

Аннотация. Для некоторых способов имитозащиты блочных шифров показано, что сторонние лица, не имеющие секретного ключа, могут навязывать законным пользователям шифртексты, которые после расшифрования будут восприниматься как истинные.

Ключевые слова: легальное сообщение, имитовставка, функция имитозащиты

Legal messages for some message authentication functions in block ciphers

V. V. Gusev

Technical Committee for Standardization TC 26, Moscow

Abstract. It is shown that for some message authentication functions in block ciphers the adversary having no knowledge of secret key may construct new messages which will be accepted by the legal user as correct ones.

Key words: legal message, message authentication code, authentication function

Введение

Имитовставка используется в блочных шифрах с секретным ключом как средство проверки целостности переданного сообщения. Имитовставка представляет собой значение некоторой функции, зависящее от ключа и открытого (или зашифрованного) текста. Эту функцию будем называть имитозащитной функцией или функцией имитозащиты.

При анализе криптографической стойкости функции имитозащиты, зависящей от открытого текста, решаются традиционные задачи построения прообраза, второго прообраза, коллизии и некоторые другие схожие по смыслу задачи (см., например, [1 – 2]). При этом, как правило, игнорируются вопросы, связанные с возможностью построения искаженных зашифрованных сообщений, которые воспринимались бы как неискаженные. Иногда только вскользь упоминается о возможности построения таких зашифрованных сообщений в блочных шифрах для режима гаммирования.

В этой работе рассматриваются способы навязывания (имитации) для различных режимов блочного шифрования, а именно способы формирования зашифрованных сообщений (без знания ключа), которые при расшифровании в соответствующем режиме и вычислении имитовставки идентифицируются пользователем, имеющим ключ, как истинные, соответствующие некоторым открытым сообщениям. Стойкость функции имитозащиты определяется как вероятность совпадения двух имитовставок, полученных после расшифрования двух текстов. Нам не известны какие-либо публикации, в которых стойкость функции имитозащиты оценивалась с таких позиций.

Введем обозначения, определения и опишем некоторые функции имитозащиты для блочных шифров с секретным ключом.

Пусть V_n — множество всех n -мерных двоичных векторов, $E_K(x)$ — отображение $V_N \times V_n$ в V_n ($K \in V_N$, $x \in V_n$), которое является подстановкой на V_n при любом фиксированном значении K .

Будем предполагать, что ключ K является секретным.

Опишем три типовых режима шифрования для блочных шифров, построенных на основе отображения $E_K(x)$: простая замена, гаммирование, гаммирование с обратной связью (по шифртексту).

Перед выполнением шифрования в любом из режимов открытые данные X разбиваются на блоки длиной n бит в каждом

$$X = (x_0, x_1, \dots, x_{L-1}), \quad x_i \in V_n.$$

Режим простой замены

Результатом зашифрования X на ключе K является последовательность

$$Y = (y_0, y_1, \dots, y_{L-1}), \quad \text{где } y_i = E_K(x_i), \quad i = \overline{0, L-1}.$$

Для расшифрования данных $Y = (y_0, y_1, \dots, y_{L-1})$ используется преобразование

$$E_K^{-1}: x_i = E_K^{-1}(y_i), \quad i = \overline{0, L-1}.$$

Режим гаммирования

В режиме гаммирования вырабатывается гамма наложения γ_i ($i = \overline{0, L-1}$), которая зависит от случайно генерируемой синхропосылки S и известной константы C длиной n бит каждая:

$$\gamma_i = E_K(S_i), \quad \text{где } S_i = (E_K(S) + (i+1) \cdot C) \bmod 2^n. \quad (1)$$

Результатом зашифрования X на ключе K является последовательность

$$Y = (y_0, y_1, \dots, y_{L-1}), \quad \text{где } y_i = x_i \oplus \gamma_i, \quad i = \overline{0, L-1}.$$

Другой вариант формирования последовательности S_i и γ_i выглядит следующим образом:

$$\gamma_i = E_K(S_i), \quad S_i = E_K(S) \oplus \alpha_i, \quad (2)$$

где $\alpha_0, \alpha_1, \alpha_2, \dots$ — известная последовательность из V_n .

Для расшифрования данных $Y = (y_0, y_1, \dots, y_{L-1})$ по синхропосылке S и последовательности $\alpha_0, \alpha_1, \dots$ вычисляются

$$S_i \quad \text{и} \quad x_i = y_i \oplus \gamma_i, \quad i = \overline{0, L-1}.$$

Режим гаммирования с обратной связью

В режиме гаммирования с обратной связью вырабатывается гамма наложения γ_i ($i = \overline{0, L-1}$), которая зависит от случайно генерируемой синхропосылки S длины n бит и открытых данных X . Последовательно от $i = 0$ до $i = L-1$ вычисляются

$$\gamma_i = E_K(y_{i-1}), \quad y_i = x_i \oplus \gamma_i, \quad \text{где } y_{-1} = S.$$

Результатом зашифрования открытых данных X на ключе K является последовательность $Y = (y_0, y_1, \dots, y_{L-1})$.

Для расшифрования данных Y (используя синхропосылку S) последовательно от $i = 0$ до $i = L-1$ вычисляются

$$\gamma_i = E_K(y_{i-1}), \quad x_i = y_i \oplus \gamma_i.$$

Режим выработки имитовставки

Для обеспечения защиты открытых данных $X = (x_0, x_1, \dots, x_{L-1})$ вырабатывается дополнительный блок IM (зависящий от X и K) из n^* бит, $1 \leq n^* < n$. Отображение прямого произведения множества открытых данных и множества ключей в пространство V_{n^*} — функция имитозащиты. Значение этой функции — имитовставка.

Итеративно формируется последовательность $\{R_i\}$:

$$\begin{aligned} R_i &= E_K(x_i \oplus R_{i-1}), & i = \overline{0, L-2}, \\ R_{L-1} &= E_K(x_{L-1} \oplus R_{L-2} \oplus \xi), \end{aligned} \quad (3)$$

где $R_{-1} = b_0$ — известная константа, а для константы ξ возможны два варианта: либо $\xi = 0$, либо ξ неизвестно.

Имитовставка IM равна $IM = f(R_{L-1})$, где $f : V_n \rightarrow V_{n^*}$ — известная функция.

Возможен другой опосредованный способ защиты открытых данных, зависящий от шифрованных данных. В формулах (3) x_i заменяются на y_i :

$$\begin{aligned} R_i &= E_K(y_i \oplus R_{i-1}), & i = \overline{0, L-2}, \\ R_{L-1} &= E_K(y_{L-1} \oplus R_{L-2} \oplus \xi), \end{aligned} \quad (4)$$

и $IM = f(R_{L-1})$.

Идентификация соответствия шифрованных данных $Y = (y_0, y_1, \dots, y_{L-1})$ открытым данным $X = (x_0, x_1, \dots, x_{L-1})$ (полученным после расшифрования) с помощью имитовставки IM проверяется пользователем, обладающим ключом K , следующим образом. Возможны два варианта.

Первый. Принятые данные $Y = (y_0, y_1, \dots, y_{L-1})$ расшифровываются в соответствующем режиме, и по полученным открытым данным X по формулам (3) вычисляется имитовставка $\tilde{IM}$, которая сравнивается с принятой IM . Только в случае совпадения имитовставок полученные в результате расшифрования блоки открытых данных X считаются истинными.

Второй. Имитовставка $\tilde{IM}$ вычисляется по формулам (4) и шифрованным данным; в случае совпадения $\tilde{IM}$ с принятой имитовставкой IM считается, что целостность шифрованных данных $Y = (y_0, y_1, \dots, y_{L-1})$ не нарушена, и расшифрованный после этого текст признается истинным.

О п р е д е л е н и е. Любое сообщение $(S; Y; IM)$ назовем *легальным*, если вычисленная с помощью ключа K имитовставка $\tilde{IM}$ для расшифрованных открытых данных $X = (x_0, x_1, \dots, x_{L-1})$ либо для зашифрованных данных $Y = (y_0, y_1, \dots, y_{L-1})$ (в зависимости от варианта (3), (4) режима выработки имитовставки) совпадает с имитовставкой IM .

Здесь $S \in V_n$ — синхропосылка (в режиме простой замены отсутствует).

Пользователь, обладающий ключом K , всегда формирует легальные сообщения. Пользователь, который не имеет ключа K , не знает полностью подстановку E_K и поэтому, формально, не обладает такой возможностью. В его распоряжении есть определенная информация в виде зашифрованных текстов и имитовставок к ним, а также ему известна часть переходов $(x, E_K(x))$ в подстановке E_K . Поэтому он может попытаться сформировать сообщение (отличное от переданных ранее на этом ключе), которое с определенной вероятностью p^* окажется легальным. Величина p^* — это вероятность успешного навязывания. Для краткости слово «успешное» будем опускать.

Ниже для различных режимов шифрования и функций имитозащиты данных (3), (4) будут приведены примеры сообщений $(S; Y; IM)$ и оценены вероятности p^* навязывания.

Обратим внимание на один существенный момент, который используется при построении легальных сообщений. Преобразование

$$E : V_N \times V_n \rightarrow V_n$$

и секретный ключ K — одни и те же в режимах шифрования и режиме выработки имитовставки.

1. Легальные сообщения для режима простой замены

1.1. Имитозащита открытых данных (3) ($b_0 = 0, \xi = 0$)

Пусть имеется несколько открытых и соответствующих им зашифрованных текстов, зашифрованных с помощью неизвестного ключа K , из которых можно сформировать два множества

$$X^{(0)} = \{x_0, x_1, \dots, x_{L-1}\}$$

и

$$Y^{(0)} = \{y_0, y_1, \dots, y_{L-1}\},$$

где все x_i различны и $y_i = E_K(x_i)$.

Предположим, что существуют такие x_i и x_j ($i < j$), что $x_i \oplus x_j \in Y^{(0)}$. Это означает, что для некоторого $x^{(0)} \in X^{(0)}$

$$x_i \oplus x_j = E_K(x^{(0)}). \quad (5)$$

Значения $E_K(x_i)$, $E_K(x_j)$, $E_K(x^{(0)})$ известны.

Формируем сообщение $(Y; IM)$, где

$$Y = (E_K(x^{(0)}), E_K(x_i)), \quad IM = f(y_j).$$

Лицо, обладающее секретным ключом K , получив сообщение $(Y; IM)$, расшифровывает его: $X = (x^{(0)}, x_i)$, последовательно вычисляет

$$\tilde{R}_0 = E_K(x^{(0)}),$$

$$\tilde{R}_1 = E_K(x_i \oplus E_K(x^{(0)})),$$

$$I\tilde{M} = f(\tilde{R}_1),$$

убеждается, что $I\tilde{M} = IM$ (в силу равенства (5)), и признает открытые данные $X = (x^{(0)}, x_i)$ истинными.

Оценим вероятность выполнения равенства (5) в предположении, что $0 \notin Y^{(0)}$. Будем считать, что элементы множества

$$X^{(0)} = \{x_0, x_1, \dots, x_{L-1}\}$$

выбираются из V_n по равновероятной схеме выбора без возвращения. Как некоторое приближение можно рассмотреть следующую вероятностную модель размещения частиц по ячейкам. Пару (x_i, x_j) ($i < j$) можно интерпретировать как частицу, попадающую в ячейку с номером $(x_i \oplus x_j) \neq 0$. В качестве еще одного приближения будем считать значения

$$(x_i \oplus x_j), \quad 1 \leq i < j < L,$$

независимыми и имеющими равновероятное распределение на множестве $\{1, 2, \dots, L-1\}$.

Тогда вероятность того, что (x_i, x_j) не попадет ни в одну из отмеченных ячеек $y_0, y_1, \dots, y_{L-1}$, равна $(1 - L/(2^n - 1))$. А вероятность p_0 непопадания в отмеченные ячейки всех $L(L-1)/2$ частиц равна

$$p_0 = \left(1 - \frac{L}{2^n - 1}\right)^{L(L-1)/2}.$$

Отсюда получаем, что при $0 \notin Y^{(0)}$ в рамках вероятностной модели случайного и равновероятного размещения частиц по ячейкам вероятность выполнения равенства (5) составит

$$p_1 = 1 - \left(1 - \frac{L}{2^n - 1}\right)^{L(L-1)/2}.$$

Для случая $0 \notin Y^{(0)}$ при выполнении условия (5) вероятность навязывания равна единице.

Отметим, что легальным будет также сообщение, которое получается из $(Y; IM)$ перестановкой индексов i и j .

Для случая когда $E_K(x^{(0)}) = 0$ при некотором $x^{(0)}$, легальным будет сообщение $(Y; IM)$, где

$$Y = (0, E_K(x_i)), \quad IM = f(y_i)$$

при любом значении i . Можно считать, что вероятность q_1 выполнения условия $0 \in Y^{(0)}$ равна $q_1 = L/2^n$.

Сделаем два замечания, которые будут касаться почти всех рассматриваемых ниже случаев.

Первое. Может так оказаться, что приведенные выше сообщения $(Y; IM)$ могли быть уже случайно переданы пользователем, обладающим ключом K . Такую ситуацию будем игнорировать.

Второе. В рассмотренных далее случаях возможность построения легальных сообщений иногда будет зависеть от выполнения некоторых условий, накладываемых на имеющуюся информацию (в настоящем подпункте это равенство (5)). Чтобы корректно вычислять вероятность навязывания, необходимо определить действия в случае, когда эти условия не выполняются. Будем считать, что в таком случае при навязывании выдается любое случайно сформированное сообщение, соответствующее данному режиму шифрования и имитозащите, и вероятность того, что оно будет легальным, равна $1/2^{n^*}$.

Конкретно в этом подпункте вероятность p^* навязывания сообщения, сформированного либо как $(Y; IM)$ (в случае выполнения условия $0 \in Y^{(0)}$ или равенства (5)), либо как случайное, равна

$$p^* = q_1 + (1 - q_1) \left(p_1 + p_0 \frac{1}{2^{n^*}} \right).$$

1.2. Имитозащита открытых данных (3) ($b_0 = 0, \xi$ неизвестно)

Сначала рассмотрим случай, когда известен один открытый текст

$$X = (x_0, x_1, \dots, x_{L-1}) \quad (L \geq 3)$$

и соответствующее ему легальное сообщение $(Y; IM)$, сформированное обладателем секретного ключа K :

$$Y = (y_0, y_1, \dots, y_{L-1}), \quad \text{где } y_i = E_K(x_i),$$

имитовставка IM выработана в соответствии с (3).

Будем считать, что все x_i различны.

Зафиксируем значение $y_0 \oplus x_1$ и рассмотрим два варианта формирования легальных сообщений.

Первый вариант. Предположим, что существует такое x_{i_0} ($0 \leq i_0 \leq L-1$), что $y_0 \oplus x_1 = x_{i_0}$, т. е.

$$E_K(x_0) \oplus x_1 = x_{i_0}. \quad (6)$$

Формируем сообщение

$$(\tilde{Y}; IM), \quad \text{где } \tilde{Y} = (y_{i_0}, y_2, \dots, y_{L-1}).$$

Пользователь, имеющий секретный ключ K , получив сообщение $(\tilde{Y}; IM)$, расшифровывает его:

$$X = (x_{i_0}, x_2, \dots, x_{L-1}).$$

Затем по формулам (3) вычисляет последовательность $\tilde{R}_0, \tilde{R}_1, \dots, \tilde{R}_{L-2}$ для полученного текста $X = (x_{i_0}, x_2, \dots, x_{L-1})$.

В силу равенства (6)

$$\tilde{R}_0 = E_K(x_{i_0}) = E_K(x_1 \oplus E_K(x_0)) = E_K(x_1 \oplus R_0) = R_1.$$

Далее,

$$\tilde{R}_1 = E_K(x_2 \oplus \tilde{R}_0) = E_K(x_2 \oplus R_1) = R_2.$$

Отсюда следует, что

$$\tilde{R}_2 = R_3,$$

...

$$\tilde{R}_{L-2} = R_{L-1},$$

$$IM = f(\tilde{R}_{L-2}) = f(R_{L-1}) = IM.$$

Поэтому сообщение $\tilde{Y}$ является легальным.

Второй вариант. Предположим, что существуют такие

$$x_{i_0}, y_{j_0} \quad (0 \leq i_0, j_0 \leq L-1; i_0 \neq 1, j_0 \neq 0),$$

что $y_0 \oplus x_1 = y_{j_0} \oplus x_{i_0}$, т. е.

$$E_K(x_0) \oplus x_1 = E_K(x_{j_0}) \oplus x_{i_0}. \quad (7)$$

Формируем сообщение

$$(\tilde{Y}; IM), \quad \text{где} \quad \tilde{Y} = (y_{j_0}, y_{i_0}, y_2, \dots, y_{L-1}).$$

После расшифрования пользователь, имеющий ключ K , получает текст

$$X = (x_{j_0}, x_{i_0}, x_2, \dots, x_{L-1})$$

и по формулам (3) вычисляет последовательность $\tilde{R}_0, \tilde{R}_1, \dots, \tilde{R}_{L-1}$ для этого текста.

Сначала $\tilde{R}_0 = E_K(x_{j_0})$, затем (в силу равенства (7))

$$\tilde{R}_1 = E_K(x_{i_0} \oplus \tilde{R}_0) = E_K(x_{i_0} \oplus E_K(x_{j_0})) = E_K(x_1 \oplus E_K(x_0)) = R_1,$$

и далее

$$\tilde{R}_2 = R_2,$$

...

$$\tilde{R}_{L-1} = R_{L-1},$$

$$IM = f(\tilde{R}_{L-1}) = f(R_{L-1}) = IM.$$

Поэтому сообщение $\tilde{Y}$ признается легальным.

Оценим вероятность выполнения хотя бы одного из равенств (6), (7).

Будем считать, что совокупность блоков

$$E_K(x_j) \oplus x_i \quad (i \neq 1, j \neq 0)$$

является независимой случайной и равновероятной выборкой из V_n .

При этом предположении вероятность выполнения хотя бы одного из равенств (6), (7) равна

$$p_1 = 1 - \left(1 - \frac{1}{2^n}\right)^{(L-1)^2 + L}.$$

С учетом второго замечания из подпункта 1.1 вероятность p^* навязывания сообщения $(\tilde{Y}; IM)$, которое формируется либо в соответствии с (6) или (7), либо случайно, если (6) и (7) не выполняются, равна

$$p^* = p_1 + p_0 \frac{1}{2^{n^*}}, \quad \text{где} \quad p_0 = \left(1 - \frac{1}{2^n}\right)^{(L-1)^2 + L}.$$

Пусть известно несколько открытых текстов (для простоты — одинаковой длины)

$$X^{(j)} = (x_0^{(j)}, x_1^{(j)}, \dots, x_{L-1}^{(j)}) \quad (j = \overline{0, s-1}, L \geq 3)$$

и соответствующих им легальных сообщений $(Y^{(j)}; IM^{(j)})$, сформированных обладателем секретного ключа K :

$$Y^{(j)} = (y_0^{(j)}, y_1^{(j)}, \dots, y_{L-1}^{(j)}), \quad \text{где } y_i^{(j)} = E_K(x_i^{(j)}).$$

Будем считать, что все $x_i^{(j)}$ различны.

Если не все $s(s \geq 2)$ значений сумм $E_K(x_0^{(j)}) \oplus x_1^{(j)}$ различны, например

$$E_K(x_0^{(j_0)}) \oplus x_1^{(j_0)} = E_K(x_0^{(j_1)}) \oplus x_1^{(j_1)},$$

то легальным будет сообщение $(\tilde{Y}; \tilde{IM})$, где

$$\tilde{Y} = (y_0^{(j_1)}, y_1^{(j_1)}, y_2^{(j_0)}, \dots, y_{L-1}^{(j_0)}), \quad \tilde{IM} = IM^{(j_0)}.$$

Вероятность этого события можно считать равной

$$q_1 = 1 - q_0, \quad \text{где } q_0 = \left(1 - \frac{1}{2^n}\right) \left(1 - \frac{2}{2^n}\right) \dots \left(1 - \frac{s-1}{2^n}\right). \quad (8)$$

Если все s значений двоичной суммы $c_j = E_K(x_0^{(j)}) \oplus x_1^{(j)}$ ($j = \overline{0, s-1}$) различны, то зафиксируем это множество: $\{c_0, c_1, \dots, c_{s-1}\}$.

Как и выше ($s = 1$), проверяем выполнение одного из условий (для всех $j = \overline{0, s-1}$), аналогичных (6), (7):

$$E_K(x_0^{(j)}) \oplus x_1^{(j)} = z \quad \text{или} \quad E_K(x_0^{(j)}) \oplus x_1^{(j)} = E_K(z_0) \oplus z_1, \quad (9)$$

где $z, z_0, z_1 \in \bigcup_{i=0}^{s-1} X^{(i)}$, а $X^{(i)}$ здесь понимается как множество блоков открытого текста $X^{(i)}$.

Вычислим вероятность выполнения хотя бы одного из равенств (9) при условии, что все $E_K(x_0^{(j)}) \oplus x_1^{(j)}$ различны.

Будем предполагать, что блоки z_0 и z_1 пары (z_0, z_1) (которую мы ассоциируем со значением $E_K(z_0) \oplus z_1$, а также блок z из (9) выбраны независимо, случайно и равновероятно из V_n .

Число пар (z_0, z_1) равно $(sL)^2$. Из них мы исключаем s пар $(x_0^{(j)}, x_1^{(j)})$, $j = \overline{0, s-1}$, так как все $c_0, c_1, \dots, c_{s-1}$ различны.

Рассмотрим три варианта.

а) $z_0 = x_0^{(j)}, z_1 \neq x_1^{(j)}$ ($j = \overline{0, s-1}$). Пара (z_0, z_1) заведомо не может привести к значению c_j , так как все $x_\alpha^{(\beta)}$ различны. Число таких пар равно $s(sL-1)$. При нашем предположении вероятность того, что ни одна из этих пар не породит элемент множества $\{c_0, c_1, \dots, c_{s-1}\}$, равна

$$\left(1 - \frac{s-1}{2^n-1}\right)^{s(sL-1)}.$$

б) $z_0 \notin \{x_0^{(0)}, \dots, x_0^{(s-1)}\}, z_1 = x_1^{(j)}$ ($j = \overline{0, s-1}$). Пара (z_0, z_1) заведомо не может привести к значению c_j . Число таких пар равно $s(sL-s)$. При нашем предположении вероятность того, что ни одна из этих пар не породит элемент множества $\{c_0, c_1, \dots, c_{s-1}\}$, равна

$$\left(1 - \frac{s-1}{2^n-1}\right)^{s(sL-s)}.$$

в) $z_0 \notin \{x_0^{(0)}, \dots, x_0^{(s-1)}\}, z_1 \notin \{x_1^{(0)}, \dots, x_1^{(s-1)}\}$. Число таких пар равно $(sL-s)^2$. При нашем предположении вероятность того, что ни одна из этих пар не породит элемент множества $\{c_0, c_1, \dots, c_{s-1}\}$, равна

$$\left(1 - \frac{s}{2^n}\right)^{(sL-s)^2}.$$

Обратимся теперь к первому равенству в (9). Вероятность того, что ни один $z \in \{X^{(0)}, \dots, X^{(s-1)}\}$ не попадет в множество $\{c_0, c_1, \dots, c_{s-1}\}$, равна

$$\left(1 - \frac{s}{2^n}\right)^{sL}.$$

Итого получаем, что при нашем предположении вероятность создать легальное сообщение (определяемое равенствами (9)) при условии, что все значения $c_0, c_1, \dots, c_{s-1}$ различны, равна

$$p_1 = 1 - p_0, \quad \text{где} \quad p_0 = \left(1 - \frac{s-1}{2^n-1}\right)^{s(2sL-s-1)} \left(1 - \frac{s}{2^n}\right)^{(sL-s)^2+sL}. \quad (10)$$

Окончательно получаем, что вероятность p^* навязывания равна

$$p^* = q_1 + q_0 \left(p_1 + p_0 \frac{1}{2^{n^*}}\right),$$

где входящие в формулу параметры определены равенствами (8) и (10).

Данный приближенный расчет вероятности p^* может уточняться.

1.3. Имитозащита шифрованных данных (4) (b_0 известно, $\xi = 0$)

Пусть известны множество попарно различных открытых блоков

$$X^{(0)} = \{x_0, x_1, \dots, x_{L-1}\}$$

и соответствующие им шифрованные блоки

$$Y^{(0)} = \{y_0, y_1, \dots, y_{L-1}\} \quad (L \geq 1), \quad \text{где} \quad y_i = E_K(x_i),$$

полученные в результате шифрования на неизвестном ключе K .

Сформируем последовательность $z_0, z_1, \dots, z_{s-1}$ ($s \geq 1$), определяемую следующим рекуррентным законом. Выберем произвольный блок $x^{(0)} \in X^{(0)}$. Для всех $i = 0, 1, \dots, s-1$ положим

$$z_i = E_K(x^{(i)}) \oplus x^{(i+1)},$$

где $x^{(i+1)}$ — произвольный блок из $X^{(0)}$. Формируем сообщение $(\tilde{Y}; IM)$:

$$\tilde{Y} = (x^{(0)} \oplus b_0, z_0, z_1, \dots, z_{s-1}),$$

$$IM = f(y^{(s)}), \quad \text{где} \quad y^{(s)} = E_K(x^{(s)}).$$

Все элементы последовательности $\tilde{Y}$ известны, так как $x^{(0)}, x^{(1)}, \dots, x^{(s)} \in X^{(0)}$.

Пользователь, имеющий секретный ключ K , получив сообщение $(\tilde{Y}; IM)$, вычисляет имитовставку от $\tilde{Y}$ по формулам (4):

$$\tilde{R}_0 = E_K((x^{(0)} \oplus b_0) \oplus b_0) = E_K(x^{(0)}),$$

$$\tilde{R}_1 = E_K(z_0 \oplus \tilde{R}_0) = E_K(z_0 \oplus E_K(x^{(0)})) = E_K(x^{(1)}),$$

...

$$\tilde{R}_s = E_K(z_{s-1} \oplus \tilde{R}_{s-1}) = E_K(z_{s-1} \oplus E_K(x^{(s-1)})) = E_K(x^{(s)}) = y^{(s)},$$

$$IM = f(y^{(s)}).$$

Так как вычисленная имитовставка $\tilde{IM}$ совпадает с IM , то критерий целостности шифрованного текста выполняется и сообщение $(\tilde{Y}; IM)$ признается легальным.

Число сформированных таким образом сообщений длины $(s+1)$, вообще говоря, может равняться L^{s+1} , и для любого из них вероятность навязывания p^* равна единице.

1.4. Имитозащита шифрованных данных (4)

(b_0 известно, ξ неизвестно)

Пусть известно одно легальное сообщение $(Y; IM)$, сформированное обладателем секретного ключа K , где

$$Y = (y_0, y_1, \dots, y_{L-1}),$$

и имитовставка IM выработана в соответствии с (4).

Пусть также известна одна пара значений $(x^{(0)}, y^{(0)})$, связанная соотношением

$$y^{(0)} = E_K(x^{(0)}).$$

Формируем сообщение $(\tilde{Y}; IM)$, где

$$\tilde{Y} = (x^{(0)} \oplus b_0, y^{(0)} \oplus b_0 \oplus y_0, y_1, \dots, y_{L-1}),$$

в котором известны все компоненты.

Обладатель ключа K , получив сообщение $(\tilde{Y}; IM)$, вычисляет имитовставку $\tilde{IM}$ от $\tilde{Y}$:

$$\tilde{R}_0 = E_K((x^{(0)} \oplus b_0) \oplus b_0) = E_K(x^{(0)}) = y^{(0)},$$

$$\tilde{R}_1 = E_K((y^{(0)} \oplus b_0 \oplus y_0) \oplus \tilde{R}_0) = E_K(y_0 \oplus b_0) = R_0,$$

...

$$\tilde{R}_L = R_{L-1},$$

$$\tilde{IM} = f(\tilde{R}_L) = f(R_{L-1})$$

и, убедившись, что она совпадает с IM , признает сообщение легальным.

Вероятность p^* навязывания сообщения $(\tilde{Y}; IM)$ равна единице.

2. Легальные сообщения для режима гаммирования

2.1. Имитозащита открытых данных (3) (модульное формирование синхропосылок (1), b_0 известно, $\xi = 0$)

Пусть известны открытая последовательность

$$X = (x_0, x_1, \dots, x_{L-1}),$$

шифрованная последовательность

$$Y = (y_0, y_1, \dots, y_{L-1})$$

и синхроросылка S , связанные соотношениями ($i = \overline{0, L-1}; L \geq 2$)

$$y_i = x_i \oplus \gamma_i,$$

$$\gamma_i = E_K(S_i),$$

$$S_i = (E_K(S) + C_i) \mod 2^n,$$

где

$$C_i = ((i+1) \cdot C) \mod 2^n.$$

Формируем сообщение $(S; \tilde{Y}; IM)$, где

$$\tilde{Y} = (S \oplus b_0 \oplus \gamma_0, C_j \oplus \gamma_1),$$

$$IM = f(\gamma_j) \quad (0 \leq j \leq L-1).$$

Пользователь, имеющий ключ K , получив сообщение $(S; \tilde{Y}; IM)$, расшифровывает его: $\tilde{X} = (S \oplus b_0, C_j)$, последовательно вычисляет

$$\tilde{R}_0 = E_K((S \oplus b_0) \oplus b_0) = E_K(S),$$

$$\tilde{R}_1 = E_K(C_j \oplus E_K(S)),$$

$$I\tilde{M} = f(\tilde{R}_1).$$

Вычисленная имитовставка $I\tilde{M}$ заведомо совпадает с IM , если

$$C_j \oplus E_K(S) = (C_j + E_K(S)) \mod 2^n.$$

Вероятность p_1 этого события несложно подсчитать, если предположить, что неизвестное $E_K(S)$ случайно равномерно выбирается из V_n и что в известном $C_j \in V_n$ содержится R_1 единиц. Вероятность p_1 равна $1/2^{R_1}$, если старший бит у C_j равен нулю, и $1/2^{R_1-1}$, если старший бит у C_j равен единице. За счет выбора значения j в допустимом диапазоне от 0 до $(L-1)$ эту вероятность можно максимизировать.

В случае когда модульное сложение не совпадает с бинарным, будем предполагать, что событие $I\tilde{M} = IM$ выполняется с вероятностью $1/2^{n^*}$. Тогда вероятность p^* навязывания сообщения $(S; \tilde{Y}; IM)$ равна

$$p^* = p_1 + (1-p_1) \frac{1}{2^{n^*}}.$$

2.2. Имитозащита открытых данных (3) (бинарное формирование синхросылок (2), b_0 известно, $\xi = 0$)

Пусть известны открытая последовательность $X = (x_0, x_1, \dots, x_{L-1})$, шифрованная $Y = (y_0, y_1, \dots, y_{L-1})$ и синхросылка S , связанные соотношениями ($i = 0, L-1; L \geq 2$)

$$\begin{aligned} y_i &= x_i \oplus \gamma_i, \\ \gamma_i &= E_K(S_i), \\ S_i &= E_K(S) \oplus \alpha_i, \end{aligned}$$

где α_i — известная последовательность из V_n .

Формируем сообщение $(S; \tilde{Y}; IM)$, где $\tilde{Y} = (\tilde{Y}_0, \tilde{Y}_1, \dots, \tilde{Y}_{r-1})$,

$$\begin{aligned} \tilde{Y}_0 &= (S \oplus b_0 \oplus \gamma_0, \alpha_{j_0} \oplus \gamma_1), \\ \tilde{Y}_1 &= (S \oplus \gamma_{j_0} \oplus \gamma_2, \alpha_{j_1} \oplus \gamma_3), \\ &\dots \\ \tilde{Y}_{r-1} &= (S \oplus \gamma_{j_{r-2}} \oplus \gamma_{2(r-1)}, \alpha_{j_{r-1}} \oplus \gamma_{2(r-1)+1}), \\ IM &= f(\gamma_{j_{r-1}}). \end{aligned}$$

Здесь j_i — любые ($0 \leq j_i \leq L-1$), $2r < L$. В тексте $\tilde{Y}$ известны все элементы.

Завершив расшифрование, лицо, располагающее ключом K , получит текст $\tilde{X} = (\tilde{X}_0, \tilde{X}_1, \dots, \tilde{X}_{r-1})$, где

$$\begin{aligned} \tilde{X}_0 &= (S \oplus b_0, \alpha_{j_0}), \\ \tilde{X}_1 &= (S \oplus \gamma_{j_0}, \alpha_{j_1}), \\ \tilde{X}_2 &= (S \oplus \gamma_{j_1}, \alpha_{j_2}), \\ &\dots \\ \tilde{X}_{r-1} &= (S \oplus \gamma_{j_{r-2}}, \alpha_{j_{r-1}}), \end{aligned}$$

затем последовательно вычислит

$$\begin{aligned} \tilde{R}_0 &= E_K(S), \quad \tilde{R}_1 = \gamma_{j_0}, \\ \tilde{R}_2 &= E_K(S), \quad \tilde{R}_3 = \gamma_{j_1}, \end{aligned}$$

$$\dots \quad \tilde{R}_{2(r-1)} = E_K(S), \quad \tilde{R}_{2(r-1)+1} = \gamma_{j_{r-1}}$$

и $I\tilde{M} = f(\gamma_{j_{r-1}})$.

Так как $I\tilde{M} = IM$, то сообщение $(S; \tilde{Y}; IM)$ с вероятностью $p^* = 1$ оказывается легальным.

2.3. Имитозащита открытых данных (3) (бинарное формирование синхропосылок (2), b_0 известно, ξ неизвестно)

Пусть известны два легальных сообщения $(S^{(j)}; Y^{(j)}; IM^{(j)})$ ($j = 0, 1$), сформированных владельцем секретного ключа K , и открытые тексты $X^{(j)} = (x_0^{(j)}, x_1^{(j)}, \dots, x_{L_j}^{(j)})$, соответствующие шифрованным текстам $Y^{(j)} = (y_0^{(j)}, y_1^{(j)}, \dots, y_{L_j}^{(j)})$; пусть $L_1 \geq L_0 + 2$ и $(i = \overline{0, L_j - 1}, j = 0, 1)$

$$\begin{aligned} y_i^{(j)} &= x_i^{(j)} \oplus \gamma_i^{(j)}, \\ \gamma_i^{(j)} &= E_K(S_i^{(j)}), \\ S_i^{(j)} &= E_K(S^{(j)}) \oplus \alpha_i. \end{aligned}$$

Имитовставки $IM^{(j)}$ выработаны в соответствии с (3):

$$\begin{aligned} R_{-1}^{(j)} &= b_0, \\ R_i^{(j)} &= E_K(x_i^{(j)} \oplus R_{i-1}^{(j)}), \quad i = \overline{0, L_j - 2}, \\ R_{L_j-1}^{(j)} &= E_K(x_{L_j-1}^{(j)} \oplus R_{L_j-2}^{(j)} \oplus \xi), \\ IM^{(j)} &= f(R_{L_j-1}^{(j)}). \end{aligned}$$

Формируем сообщение $(S^{(1)}; \tilde{Y}; IM^{(0)})$, где

$$\begin{aligned} \tilde{Y} &= (S^{(0)} \oplus b_0 \oplus \gamma_0^{(1)}, \alpha_{i_0} \oplus \gamma_1^{(1)}, x_0^{(0)} \oplus b_0 \oplus \gamma_{i_0}^{(0)} \oplus \gamma_2^{(1)}, Y'), \\ Y' &= (x_1^{(0)} \oplus \gamma_3^{(1)}, x_2^{(0)} \oplus \gamma_4^{(1)}, \dots, x_{L_0-1}^{(0)} \oplus \gamma_{L_0+1}^{(1)}), \end{aligned}$$

и i_0 — любое $(0 \leq i_0 \leq L_0 - 1)$. В тексте $\tilde{Y}$ все элементы известны.

После расшифрования пользователь, имеющий ключ K , получит текст

$$\tilde{X} = (S^{(0)} \oplus b_0, \alpha_{i_0}, x_0^{(0)} \oplus b_0 \oplus \gamma_{i_0}^{(0)}, x_1^{(0)}, x_2^{(0)}, \dots, x_{L_0-1}^{(0)}),$$

затем последовательно вычислит

$$\begin{aligned} \tilde{R}_0 &= E_K(S^{(0)}), & \tilde{R}_1 &= E_K(\alpha_{i_0} \oplus E_K(S^{(0)})) = \gamma_{i_0}^{(0)}, \\ \tilde{R}_2 &= E_K(x_0^{(0)} \oplus b_0) = R_0^{(0)}, & \tilde{R}_3 &= R_1^{(0)}, \dots, \\ \tilde{R}_{L_0+1} &= R_{L_0-1}^{(0)}, & \tilde{IM} &= f(R_{L_0-1}^{(0)}) = IM^{(0)}. \end{aligned}$$

Сообщение $(S^{(1)}; \tilde{Y}; IM^{(0)})$ с вероятностью $p^* = 1$ является легальным.

2.4. Имитозащита открытых данных (3) (модульное формирование синхропосылок (1), b_0 известно, ξ неизвестно)

В этом случае используются те же начальные данные, то же сообщение $(S^{(1)}; \tilde{Y}; IM^{(0)})$, что и в подпункте 2.3, только параметр α_i заменяется на

$$C_i = ((i+1) \cdot C) \bmod 2^n.$$

Вычисленная имитовставка $\tilde{IM}$ заведомо совпадет с $IM^{(0)}$, если при вычислении $\tilde{R}_1 = E_K(C_{i_0} \oplus E_K(S^{(0)}))$ значение $C_{i_0} \oplus E_K(S^{(0)})$ совпадет с

$$(C_{i_0} + E_K(S^{(0)})) \bmod 2^n.$$

Поэтому можно считать, что вероятность p^* навязывания сообщения $(S^{(1)}; \tilde{Y}; IM^{(0)})$ равна

$$p^* = p_1 + (1 - p_1) \frac{1}{2^{n^*}},$$

где значение p_1 взято из подпункта 2.1.

2.5. Имитозащита шифрованных данных (4) (бинарное формирование синхропосылок (2), b_0 известно, ξ неизвестно или $\xi = 0$)

Пусть известны одно легальное сообщение $(S; Y; IM)$ и один блок открытого текста x_{i_0} , связанный с блоком шифрованного сообщения соотношением $y_{i_0} = x_{i_0} \oplus \gamma_{i_0}$, где

$$\gamma_{i_0} = E_K(S_{i_0}),$$

$$S_{i_0} = E_K(S) \oplus \alpha_{i_0},$$

$$Y = (y_0, y_1, \dots, y_{L-1}), \quad L \geq 2.$$

Имитовставка IM выработана в соответствии с (4). Метод построения легального сообщения такой же, как и в подпункте 2.3.

Формируем сообщение $(S; \tilde{Y}; IM)$, где

$$\tilde{Y} = (S \oplus b_0, \alpha_{i_0}, y_0 \oplus b_0 \oplus \gamma_{i_0}, y_1, y_2, \dots, y_{L-1}).$$

Обладатель ключа K , получив сообщение $(S; \tilde{Y}; IM)$, вычисляет имитовставку $\tilde{IM}$ от $\tilde{Y}$:

$$\tilde{R}_0 = E_K(S), \quad \tilde{R}_1 = E_K(\alpha_{i_0} \oplus E_K(S)) = \gamma_{i_0},$$

$$\tilde{R}_2 = E_K(y_0 \oplus b_0) = R_0, \quad \tilde{R}_3 = R_1, \dots,$$

$$\tilde{R}_{L+1} = R_{L-1}, \quad \tilde{IM} = f(R_{L-1}) = IM.$$

Сообщение $(S; \tilde{Y}; IM)$ с вероятностью $p^* = 1$ оказывается легальным.

3. Легальные сообщения для режима гаммирования с обратной связью

3.1. Имитозащита открытых данных (3) (b_0 известно, ξ неизвестно или $\xi = 0$)

Пусть известно одно легальное сообщение $(S; Y; IM)$, полученное на ключе K . Имитовставка IM выработана в соответствии с (3).

Открытый $X = (x_0, x_1, \dots, x_{L-1})$ и шифрованный $Y = (y_0, y_1, \dots, y_{L-1})$ тексты связаны соотношением ($i = 0, L-1; L \geq 2$)

$$y_i = x_i \oplus E_K(y_{i-1}), \quad \text{где } y_{-1} = S.$$

Пусть известен только один блок x_0 в тексте X .

Формируем сообщение $(S; \tilde{Y}; IM)$, где

$$\tilde{Y} = (x_0 \oplus b_0, y_1, y_2, \dots, y_{L-1}).$$

Пользователь, имеющий ключ K , получив такое сообщение, расшифровывает его, получает текст

$$\tilde{X} = (y_0 \oplus b_0, y_1 \oplus E_K(x_0 \oplus b_0), x_2, \dots, x_{L-1}),$$

вычисляет имитовставку

$$\begin{aligned} \tilde{R}_0 &= E_K((y_0 \oplus b_0) \oplus b_0) = E_K(y_0), \\ \tilde{R}_1 &= E_K(y_1 \oplus E_K(x_0 \oplus b_0) \oplus E_K(y_0)) = E_K(x_1 \oplus R_0) = R_1, \\ \tilde{R}_2 &= R_2, \\ &\dots \\ \tilde{IM} &= IM \end{aligned}$$

и признает его легальным.

Текст $\tilde{Y}$ может совпасть с Y только при $E_K(S) = b_0$. В этом случае легальным будет сообщение $(S; \tilde{Y}; IM)$, где

$$\tilde{Y} = (S, y_0, y_1, y_2, \dots, y_{L-1}).$$

При расшифровании получается текст

$$\tilde{X} = (S \oplus b_0, x_0, x_1, \dots, x_{L-1}).$$

Таким образом, с вероятностью $p^* = 1$ сообщение $(S; \tilde{Y}; IM)$ (текст $\tilde{Y}$ выбирается в зависимости от $E_K(S)$) оказывается легальным.

3.2. Имитозащита шифрованных данных (4)

(b_0 известно, ξ неизвестно или $\xi = 0$)

Пусть известно одно легальное сообщение $(S; Y; IM)$, полученное на ключе K , где $Y = (y_0, y_1, \dots, y_{L-1})$. Имитовставка IM выработана в соответствии с (4). Пусть известен один блок x_{i_0} в тексте X , $0 \leq i_0 \leq L-1$.

Тогда

$$\gamma_{i_0} = E_K(y_{i_0-1}) = x_{i_0} \oplus y_{i_0}$$

— известная величина.

Формируем сообщение $(\tilde{S}; \tilde{Y}; IM)$, где $\tilde{S}$ выбираем произвольно, а

$$\tilde{Y} = (y_{i_0-1} \oplus b_0, \gamma_{i_0} \oplus y_0 \oplus b_0, y_1, y_2, \dots, y_{L-1}).$$

Обладатель ключа K , получив сообщение $(\tilde{S}; \tilde{Y}; IM)$, вычисляет имитовставку $\tilde{IM}$ от $\tilde{Y}$:

$$\tilde{R}_0 = E_K(y_{i_0-1}) = \gamma_{i_0},$$

$$\tilde{R}_1 = E_K(\gamma_{i_0} \oplus y_0 \oplus b_0 \oplus \gamma_{i_0}) = R_0,$$

$$\tilde{R}_2 = E_K(y_1 \oplus \tilde{R}_1) = R_1,$$

...

$$\tilde{R}_L = R_{L-1},$$

$$\tilde{IM} = f(R_{L-1}) = IM.$$

Сообщение $(\tilde{S}; \tilde{Y}; IM)$ с вероятностью $p^* = 1$ оказывается легальным.

4. Заключение

Представленные в работе способы формирования сообщений позволяют сторонним лицам без знания секретного ключа K навязывать обладателям ключа K шифрованные тексты, которые идентифицируются как истинные по имитовставке. Для различных режимов шифрования и функций имитозащиты в зависимости от известной исходной информации и ее объема возможны с определенной вероятностью подмена сообщений (переданных пользователями, которые имеют ключ K) или формирование легальных сообщений с заданным значением имитовставки.

Автор благодарен П. Л. Гутееву за замечания, позволившие улучшить стиль изложения результатов статьи.

Список литературы

- [1] Лось А. Б., Нестеренко А. Ю., Рожков М. И., *Криптографические методы защиты информации*, учебник для академического бакалавриата, 2-е изд., испр., М. : Юрайт, 2016, 473 с.
- [2] Матюхин Д. В., Шишкин В. А., “Некоторые методы анализа функций хэширования и их применение к алгоритму ГОСТ Р 34.11-94”, *Математические вопросы криптографии*, **3**:1 (2012), 71–90.