УДК 681.3

А. А. Молдовян, А. В. Муравьев
Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Д. Н. Молдовян
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Способ блочного шифрования в режиме исправления ошибок

Предложен способ блочного шифрования в режиме исправления ошибок, включающий предварительное шифрование блоков данных с последующим совместным преобразованием промежуточных блоков шифртекста и меток, вносящих избыточность, выполняемым в зависимости от секретного ключа. Для практического применения предлагается использовать метод, который в своей реализации использует две и более метки избыточности. Первая метка используется для снижения вероятности ложного декодирования, а вторая – для снижения числа перебираемых вариантов потенциально возможных ошибок. В результате формируются выходные блоки преобразованных данных, имеющие увеличенный размер. Для корректирования ошибок достаточно восстановить только метку. Устранение необходимости восстановления блоков промежуточных шифртекстов и блоков исходных данных до исправления ошибок обеспечивает повышение скорости процедуры расшифровывания в сравнении с известным способом-аналогом.

Блочное шифрование, секретный ключ, исправление ошибок, кодирование, декодирование, криптокодирование, псевдовероятностное шифрование

Как правило, алгоритмы шифрования с разделяемым секретным ключом применяются для защиты информации, передаваемой по незащищенным каналам связи, от несанкционированного доступа. В частности, для выполнения симметричного криптографического преобразования широко используются блочные шифры (БШ) [1]–[3], обладающие сильным лавинным эффектом и требующие помехоустойчивого кодирования шифртекста при передаче последнего по каналам с ошибками. Благодаря выраженному лавинному эффекту БШ применяются для построения хеш-функций, для защиты информации в побочных каналах (использование шифрования по известному ключу), для обеспечения гарантированного уничтожения информации на магнитных носителях [4] и для построения случайных латинских квадратов большого размера [5].

Сравнительно новым применением БШ является их использование для исправления ошибок, возникающих при передаче сообщений по каналам с шумом [6], при одновременном обеспечении защиты передаваемой информации. Способ использования БШ в режиме исправления ошибок, предложенный в [6], обладает следующими интересными для практического применения свойствами: 1) совмещение шифрующих и кодирующих свойств в едином алгоритме преобразования; 2) возможность обнаружения и исправления ошибок различной природы (инверсии, пропуски и вставки бит); 3) возможность реализации способа на основе многих известных БШ, например описанных в [7], [8]. Данные свойства во многом определяются выраженными рассеивающими свойствами БШ. Совмещение шифрующих свойств с возможностью исправления ошибок позволяет называть преобразования такого типа криптокодированием. Более раннее применение рассеивающих преобразований [9] относится к реализации на их основе процедур обнаружения ошибок.

В способе криптокодирования [6] информационная избыточность вносится присоединением к исходным блокам данных заранее известной метки, а исправление ошибок выполняется переборным путем в виде многократного выполнения процедуры расшифровывания блока шифртекста до тех пор, пока восстановленный блок исходных

данных не будет содержать указанную метку. Недостатком способа [6] является сравнительно низкая скорость процедуры расшифровывания при наличии ошибок в блоках шифртекста.

В настоящей статье описывается новый способ реализации криптокодирования с использованием блочных шифров. Способ состоит в выполнении блочного преобразования исходных данных, результатом которого является получение промежуточных блоков шифртекста, и внесении избыточности посредством совместного преобразования промежуточных блоков шифртекста и меток избыточности. Рассмотрены варианты реализации предложенного способа, в которых один блок промежуточного шифртекста преобразуется совместно с одной или с двумя метками. Во втором варианте достигается существенное снижение вычислительной сложности процедуры расшифровывания.

Использование блочных шифров в режиме криптокодирования. В способе криптокодирования [6] шифруемый *n*-битовый двоичный вектор формируется конкатенацией блока данных T размером $n-\mu$ бит и некоторой специфицированной μ-битовой метки избыточности. Если количество ошибок, вносимых в *n*-битовый блок шифртекста при его передаче по каналу с помехами, сравнительно мало (например, возникает от одной до трех ошибок на один переданный блок шифртекста), то ошибки исправляются в процессе перебора возможных комбинаций одиночных битовых ошибок. В принятом блоке шифртекста корректируется предполагаемая комбинация ошибок, после чего выполняется процедура расшифровывания. Если в восстановленном *n*-битовом двоичном векторе присутствует метка избыточности, то считается, что с достаточно большой вероятностью ошибки исправлены правильно. Перебор возможных комбинаций ошибок рекомендуется выполнять, начиная от одиночных ошибок в сторону увеличения числа предполагаемых ошибок, приходящихся на один блок шифртекста. Выполнить процедуру исправления ошибок может только санкционированный получатель сообщения, поскольку для этого необходимо знать ключ шифрования.

Переборный механизм коррекции ошибок определяет универсальность режима криптокодирования, т. е. возможность исправления ошибок различной природы (битовых инверсий, пропусков и вставок бит), включая случай исправления комбинаций одиночных ошибок различного типа, внесенных в один и тот же блок шифртекста. В частном случае исправления однотипных ошибок, а именно битовых инверсий, блочное шифрование в режиме исправления ошибок имеет следующие особенности [6]:

1. При условии $2^{\mu} >> C_n^k$ вероятность ложного восстановления блока данных с k ошибками можно грубо оценить значением $2^{-\mu}C_n^k$ (C_n^k – число сочетаний по k из n).

2. Если для выполнения процедуры шифрования использован такой ключ, при котором при зашифровывании всех $2^{n-\mu}$ возможных входных блоков T наблюдаются только выходные разности, содержащие не менее k единичных бит, то в режиме исправления ошибок гарантированно исправляются k ошибок.

Практическое применение режима криптокодирования связывается со случаем сравнительно небольших значений k ($k << n$), хотя может быть исправлено и сравнительно большое число ошибок. Однако с ростом значения k быстро возрастает вычислительная трудоемкость процедуры расшифровывания. При этом вероятность ошибочного восстановления блока исходного текста приближается к единице.

Способ криптокодирования с меткой в качестве ключевого элемента. Пусть задан некоторый *n*-битовый алгоритм блочного шифрования $E_K(*)$ с ключом K и хеш-функцией $h(*)$ разрядности $m > \mu$. Промежуточный блок шифртекста C_T получим шифрованием блока данных T размером n бит по формуле $C_T = E_K(T)$. К значению C_T присоединяется метка M длины μ и формируется блок выходного шифртекста C по следующей формуле:

$$C = \left(C_T \,\|\, M\right)^{2^{-1} \bmod \left(2^{n+\mu}-1\right)} \bmod \delta(x), \qquad (1)$$

где знак $\|$ обозначает операцию конкатенации; $\delta(x)$ – неприводимый двоичный многочлен степени $n+\mu$, являющийся известным параметром алгоритма криптокодирования; значения C и $C_T \,\|\, M$ рассматриваются как двоичные многочлены, причем метка M вычисляется как битовая цепочка, представляющая двоичное число $M = h(K \,\|\, i) \bmod 2^{\mu}$, зависящее от ключа шифрования K и порядкового номера текущего шифруемого блока данных.

Таким образом, в рассматриваемом способе значение метки избыточности является ключевым элементом, что вносит дополнительный вклад в стойкость алгоритма криптокодирования. Отправитель передает блок шифртекста C, а получатель получает блок C', в котором предположительно имеется несколько одиночных битовых ошибок. Как и в способе криптокодирования, описанном ранее, осуществляется перебор возможных комбинаций ошибок, для каждой из которых выполняется процедура расшифровывания блока C'', полученного коррекцией предполагаемых ошибок в блоке C'. В результате восстанавливается значение

$$C''_T \,\|\, M'' = C^2 \bmod \delta(x). \qquad (2)$$

Если для текущего блока C'' выполняется равенство $M'' = M$ (значение M получатель вычисляет по ключу K и номеру i текущего блока шифртекста), то исходный восстановленный блок данных вычисляется по значению C'': $T = E_K^{-1}(C''_T)$, где E_K^{-1} – функция расшифровывания.

За счет того, что для восстановления значения метки по скорректированному блоку шифртекста C'' достаточно выполнить одно модульное возведение в квадрат и не требуется многократно расшифровывать соответствующий блок промежуточного шифртекста C'', снижается вычислительная сложность переборной процедуры восстановления ошибок.

Аналогичный способ криптокодирования может быть реализован с использованием вычислений, задаваемых следующими двумя формулами, которые, в свою очередь, соответствуют выражениям (1) и (2):

$$C = \left(C_T \,\|\, M\right)^{3^{-1} \bmod \varphi(R)} \bmod R,$$

$$C''_T \,\|\, M'' = C^3 \bmod R,$$

где $\varphi(R)$ – значение функции Эйлера от числа R; переменные трактуются как двоичные числа; в качестве модуля R используются значения разрядности $n + \mu + 1$ бит, для которых $\varphi(R)$ не делится на 3.

Способ криптокодирования с двумя метками информационной избыточности. Если в канале связи возникают только ошибки типа битовых инверсий, может быть применен способ криптокодирования, в котором существенно сокращается или практически устраняется необходимость перебора возможных вариантов комбинаций одиночных ошибок. Эта возможность обеспечивается использованием в рамках описанного ранее способа еще одной дополнительной метки M_S разрядности μ_S и формированием таких передаваемых блоков шифртекста S, которые сравнимы со значением указанной второй метки по модулю некоторого специфицированного двоичного многочлена $\rho(x)$ степени μ_S.

Блок шифртекста S, имеющий разрядность $n + \mu + \mu_S$, формируется отправителем сообщения как решение системы из двух линейных сравнений следующего вида:

$$\begin{cases} S \equiv C \bmod \delta(x), \\ S \equiv M_S \bmod \rho(x). \end{cases}$$

Значение S может быть вычислено по формуле

$$S = \Big[C\rho(x)\left(\rho^{-1}(x) \bmod \delta(x)\right) \oplus$$

$$\oplus M_S \delta(x)\left(\delta^{-1}(x) \bmod \rho(x)\right)\Big] \bmod \rho(x)\delta(x),$$

где знак $\oplus$ обозначает операцию сложения двоичных многочленов (поразрядное суммирование по модулю 2). Получатель принимает блок шифртекста S' с ошибками, который может быть выражен через блок S и вектор ошибок ω, имеющий длину $n + \mu + \mu_S$ бит, по формуле $S' = S \oplus \omega$, из которой имеем

$$\left(S' \bmod \rho(x)\right) = \left(S \bmod \rho(x)\right) \oplus \left(\omega \bmod \rho(x)\right). \qquad (3)$$

Из (3) имеем

$$\left(\omega \bmod \rho(x)\right) = M'_S \oplus M_S, \qquad (4)$$

где $M'_S = \left(S' \bmod \rho(x)\right)$ – двоичный многочлен, вычисленный как остаток от деления двоичного многочлена S' на многочлен $\rho(x)$. По принятому блоку шифртекста с ошибками может быть вычислена разность $B = M'_S \oplus M_S$, которой соответствует некоторое подмножество векторов ошибок (будем называть ее вектором смещения). Мощность этого подмножества зависит от числа битовых инверсий (одиночных ошибок) k, при котором требуется обеспечить возможность правильного исправления ошибок. Исправление k ошибок соответствует рассмотрению всех возможных векторов ошибок ω, содержащих не более k единичных разрядов, т. е. имеющих вес

Хемминга, не превышающий значения k. Мощность множества таких векторов ошибок равна $\#\{\omega\} = C^1_{n+\mu+\mu_S} + C^2_{n+\mu+\mu_S} + \ldots + C^k_{n+\mu+\mu_S}$.

Каждому из 2^b возможных значений вектора смещения B (b – битовая разрядность вектора B) соответствует некоторое подмножество векторов ошибок. Подмножество векторов ошибок, соответствующее значению $B_j = j\left(j = 0, 1, \ldots, 2^b - 1\right)$, будем обозначать как $\{\omega\}_j$. Используя (4), для каждого вектора ошибок ω можно вычислить значение вектора смещения и для каждого значения j сгруппировать в виде подмножества $\{\omega\}_j$ все векторы ошибок, обусловливающих смещение B_j. В результате получим таблицу, позволяющую значительно ускорить процедуру исправления ошибок за счет существенного сокращения числа перебираемых возможных комбинаций ошибок.

B_j	0	1	2	⋯	2^b-1
$\{\omega\}_j$	$\{\omega\}_0$	$\{\omega\}_1$	$\{\omega\}_2$	⋯	$\{\omega\}_{2^b-1}$

Процедура расшифровывания полученного блока шифртекста включает следующие шаги:

1. Вычисляется значение $M'_S = S' \bmod \rho(x)$.

2. Определяется значение $M'_S \oplus M_S = B_j$.

3. Используя таблицу, в которой задается подмножество перебираемых комбинаций одиночных ошибок по вычисленному значению вектора смещения, устанавливается подмножество потенциально возможных векторов ошибок $\{\omega\}_j$. (Предполагается, что для нескольких практически важных случаев комбинаций значений n, μ, μ_s и k заранее вычисляются таблицы такого типа и в ходе протокола криптокодирования они имеются в наличии.)

4. Для каждого вектора $\omega \in \{\omega\}_j$ выполняются следующие 4 шага:

4.1. Вычисляется битовая строка $S = S' \oplus \omega$.

4.2. Находится битовая строка $C = S \bmod \delta(x)$.

4.3. Определяется битовая строка $C''_T \,\|\, M'' = C^2 \bmod \delta(x)$.

4.4. При получении значения $M'' = M$ осуществляется переход к шагу 5.

5. Вычисляется значение блока исходных данных $T = E_K^{-1}\left(C''_T\right)$.

В среднем мощность подмножества $\{\omega\}_j$ равна:

$$U = \#\{\omega\}_j = \frac{\#\{\omega\}}{2^b} = \frac{C^1_{n+\mu+\mu_S} + C^2_{n+\mu+\mu_S} + \ldots + C^k_{n+\mu+\mu_S}}{2^b}.$$

Таблица не зависит от выбранного значения M_S, поэтому значение этой метки можно (как и метку M) использовать в качестве ключевого элемента. По сравнению со способом криптокодирования, описанным ранее, в рассматриваемом способе число перебираемых вариантов возможных комбинаций ошибок уменьшается в среднем в $\#\{\omega\}/U = 2^b$ раз.

Следует отметить, что при выборе некоторых комбинаций значений n, μ, μ_s и k может быть получено значение U, меньшее единицы. Этот случай соответствует наличию пустых подмножеств в таблице (в том числе возможен случай, когда подавляющему числу различных значений вектора смещения будут соответствовать пустые подмножества).

Способ псевдовероятностного криптокодирования. Для защиты информации от несанкционированного доступа в ряде случаев применяется вероятностное шифрование. Оно представляет собой криптографическое преобразование, в ходе которого используются случайные значения, влияющие на значение генерируемого шифртекста. При вероятностном шифровании фиксированному входному сообщению соответствует большое число различных шифртекстов, по каждому из которых при выполнении процедуры расшифровывания однозначно восстанавливается указанное входное сообщение. Размер шифртекста, полученного в результате вероятностного шифрования, превышает размер входного сообщения, что, безусловно, является недостатком. Однако, несмотря на это, вероятностное шифрование находит применение, поскольку в принципе обеспечивает дополнительную защищенность от использования предполагаемым нарушителем некоторых непредвиденных слабостей базового детерминистического алгоритма шифрования. Например, при использовании блочных шифров предложен достаточно простой режим вероятностного

шифрования [10], состоящий в том, что шифруемое сообщение разбивается на блоки размером меньше, чем размер входного блока алгоритма блочного шифрования. При этом входной блок данных формируется присоединением случайной битовой строки к блоку сообщения.

В способе вероятностного шифрования [10] дополнительная стойкость шифрования может быть получена также и при генерации битовой строки, присоединяемой к блоку сообщения, по псевдослучайному закону в зависимости от секретного ключа. Для предложенного способа криптокодирования с двумя метками избыточности режим псевдовероятностного преобразования можно задать так, чтобы это не приводило к увеличению размера шифртекста по сравнению с описанным исходным алгоритмом, который является детерминистическим. Таким образом, возникает возможность потенциального повышения стойкости криптокодирования без увеличения размера шифртекста. Режим псевдовероятностного криптокодирования реализуется следующим образом. В предложенном алгоритме криптокодирования метка избыточности используется в качестве фиксированного ключевого элемента, а таблица, связывающая возможные значения векторов ошибки со значениями наблюдаемого вектора смещения B, не зависит от значения метки избыточности. Последнее позволяет использовать для преобразования каждого нового входного блока новое значение M_{Si} метки избыточности при условии, что закон изменения значения метки известен получателю шифртекста. Изменение значения метки избыточности M_{Si} при переходе от одного входного блока к другому по псевдослучайному закону фактически задает режим псевдовероятностного криптокодирования.

Для задания возможности расшифровывания блоков шифртекста в произвольном порядке удобно задать текущее значение метки избыточности в зависимости от исходного значения метки M_S, являющегося ключевым элементом, и от номера i текущего преобразуемого входного блока данных. Псевдослучайный закон изменения значения метки M_S, например, может быть задан следующей формулой:

$$M_{Si} = h(M_S \| i) \bmod \rho(x),$$

в которой выходное значение хеш-функции h рассматривается как двоичный многочлен.

Предложены 2 способа построения алгоритмов криптокодирования, обеспечивающих повышение производительности процедуры расшифровывания по сравнению с известными в литературе аналогами. Для практического применения более интересным является способ, использующий две метки информационной избыточности. Первая метка обеспечивает достаточно низкую вероятность ложного декодирования, а вторая – возможность существенного снижения среднего числа перебираемых потенциально возможных комбинаций ошибок, за счет чего может быть значительно снижена вычислительная сложность восстановления исходного блока данных по блоку шифртекста с ошибками. Показана возможность задания режима псевдовероятностного криптокодирования на основе предложенного алгоритма преобразования с использованием двух меток избыточности.

Представляет интерес модернизация второго способа, которую можно связать с использованием двух и более меток, по каждой из которых вычисляются внесенные ошибки, а затем результаты вычислений сопоставляются, обеспечивая снижение числа комбинаций ошибок, которые требуется перебирать в процессе расшифровывания блока шифртекста. Самостоятельный интерес представляет также и разработка алгоритмов криптокодирования на основе блочных псевдовероятностных шифров, предложенных в [11].

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-57-54002-Вьет_а.

СПИСОК ЛИТЕРАТУРЫ

1. Bac Do Thi, Minh Hieu Nguyen. A high speed block cipher algorithm // Intern. J. of Security and its applications. 2013. Vol. 7, № 6. P. 43–54.

2. Информационная технология. Криптографическая защита информации. Блочные шифры // Национальный стандарт РФ ГОСТ Р 34.12–2015. М.: Стандартинформ, 2015. 25 с.

3. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров // Национальный стандарт РФ ГОСТ Р 34.13–2015. М.: Стандартинформ, 2015. 42 с.

4. Мирин А. Ю. Метод и алгоритм гарантированного уничтожения информации, хранимой на магнитных дисках: автореф. дис. … канд. техн. наук /

С.-Петерб. гос. ун-т информ. технологии, механики и оптики. СПб., 2005. 20 с.

5. Молдовян Н. А., Нгуен Ле Минь, Хо Нок Зуй. Синтез поточных шифров на основе блочных преобразований: метод латинских квадратов // Вопр. защиты информации. 2008. № 1. С. 27–34.

6. Moldovyan N., Levina A., Taranov S. Symmetric Encryption for Error Correction // Proc. of the 20th FRUCT'20 Conf. Saint Petersburg: Saint Petersburg Electrotechnical University «LETI» and Technopark of ITMO University, 2017. P. 290–295.

7. Moldovyan N. A., Moldovyan A. A. Data-driven block ciphers for fast telecommunication systems. New York; London: Auerbach Publications. Talor & Francis Group, 2008. 185 p.

8. Pieprzyk J., Hardjono Th., Seberry J. Fundumentals of Computer Security. Berlin: Springer-Verlag, 2003. 677 p.

9. Klove T., Korzhik V. Error detecting Codes. Netherlands: Kluwer Academic Publishers, 1995.

10. Moldovyan N. A., Moldovyan A. A. Innovative cryptography. USA, Boston: Charles River Media, 2006. 485 p.

11. Морозова Е. В., Мондикова Я. А., Молдовян Н. А. Способы отрицаемого шифрования с разделяемым ключом // Информационно-управляющие системы. 2013. № 6. С. 73–78.

A. A. Moldovyan, A. V. Muravyev
Saint Petersburg Institutefor Informatics and Automationof the Russian Academy of Sciences

D. N. Moldovyan
Saint Petersburg Electrotechnical University «LETI»

METHOD FOR BLOCK ENCRYPTION IN THE ERROR-CORRECTING MODE

There is proposed a method for block encryption in the error-correcting mode, which includes preliminary encryption of data blocks followed by simultaneous key-dependent transformation of the intermediate ciphertext blocks and labels that introduce redundancy. For practical applications there is proposed implementation of the method, in which two or more redundancy labels are used. The first label is used for reducing probability of the falls decoding. The second label is used for reducing the number of checking variants of potentially possible errors. The error-correcting block ciphering produces the output ciphertext blocks having increased size. To correct errors it is sufficient to compute only the value of the label. Recovering the intermediate ciphertext blocks and source data blocks are not required prior performing the error correction. Due to the last in the proposed method the performance of the decryption procedure is higher than in the known method-analog.

Block encryption, secret key, error correcting, encoding, decoding, error-correcting ciphering, pseudo-probabilistic encryption