Способы псевдовероятностного блочного шифрования

Молдовян А. А.
Санкт-Петербургский институт информатики
и автоматизации РАН
Санкт-Петербург, Россия
maa1305@yandex.ru

Татчина Я. А.
Санкт-Петербургский государственный
электротехнический университет «ЛЭТИ»
Санкт-Петербург, Россия
iana.tatchina@gmail.com

Аннотация. **Псевдовероятностное шифрование представлено как новый алгоритмический механизм обеспечения информационной безопасности, реализующий защиту информации в случае атак с принуждением к раскрытию ключа шифрования. Базовым требованием к преобразованиям данного вида является вычислительная неразличимость по шифртексту от вероятностного шифрования. Рассматриваются способы и алгоритмы, выполняющие псевдовероятностное шифрование как одновременное криптографическое преобразование фиктивного и секретного сообщений по двум различным ключам, состоящее в формировании блоков промежуточных шифртекстов и их обратимом отображении в единый расширенный блок выходной криптограммы. Предложены алгоритмы, включающие задание процедуры объединяющего отображения в виде решения систем линейных уравнений и сравнений, в которых в качестве модуля используются числа и двоичные многочлены. Предложенные способы обладают высокой производительностью и представляют значительный интерес для практического применения в системах информационной безопасности.**

Ключевые слова: **криптография, отрицаемое шифрование, псевдовероятностное шифрование, симметричное шифрование, блочные шифры, вероятностное шифрование, криптограмма.**

Введение

Отрицаемое шифрование (ОШ) позволяет обеспечить защиту информации в ситуациях, когда участники сеанса защищенной связи подвергаются атаке с принуждением [1–3]. Такие атаки подразумевают, что у злоумышленника имеются некоторые ресурсы воздействия на получателя и/или отправителя, вынуждающие получателя и/или отправителя раскрыть секретные параметры процедуры зашифровывания или расшифровывания, например, исходное сообщение и секретный ключ.

Практическое значение ОШ определяется тем, что его применение позволяет решить ряд важных нестандартных задач, связанных с информационной безопасностью информационно-телекоммуникационных технологий. Этот вид шифрования применяется для защиты информации в протоколах распределенных вычислений [4], защиты от скупки голосов систем тайного голосования через Интернет [5, 6].

Специальным вариантом ОШ является псевдовероятностное (ПВ) шифрование, которое расширяет класс алгоритмических средств защиты информации, используемых в составе комплексных средств обеспечения информационной безопасности [7]. Стойкость ПВ-шифрования к принуждающим атакам обеспечивается тем, что криптограмма (шифртекст) формируется путем совместного криптографического преобразования двух сообщений – секретного и фиктивного – при выполнении требования вычислительной неразличимости от шифртекста, полученного в процессе вероятностного шифрования фиктивного сообщения по фиктивному ключу. Последние могут быть раскрыты атакующему в случае принуждающей атаки с сохранением требуемого уровня защищенности секретного сообщения. При этом пользователи имеют возможность убедительно утверждать, что они использовали алгоритм вероятностного шифрования для защиты информации. Ранее в рамках данного общего подхода были разработаны протоколы ПВ-шифрования, основанные на коммутативных шифрующих преобразованиях [8], и гибридные ПВ-шифры [9].

В схеме ПВ криптографического преобразования получатель и отправитель сообщения обмениваются двумя ключами шифрования – секретным и фиктивным, по которым выполняется процедура преобразования секретного и фиктивного сообщений, соответственно. При этом формируется единый шифртекст, из которого с использованием одного и того же алгоритма расшифровывания может быть восстановлено секретное или фиктивное сообщение в зависимости от используемого ключа. Такая возможность обеспечивается тем, что размер единого шифртекста больше, чем размер каждого из рассматриваемых двух входных сообщений. В случае вероятностного шифрования имеет место аналогичное увеличение размера шифртекста, что создает принципиальную возможность выполнить требование вычислительной неразличимости по шифртексту ПВ-шифрования от вероятностного [10]. Доказательное выполнение этого требования связано с представлением атакующему алгоритма вероятностного шифрования, которому соответствует такой алгоритм расшифровывания, с помощью которого по фиктивному ключу из шифртекста восстанавливается фиктивное сообщение.

Интерес к способам и алгоритмам ПВ-шифрования обусловливается возможностью реализации на их основе новых механизмов защиты информации, реализуемых в виде криптографически скрытых каналов (криптографических стегоканалов) и криптографических обманных ловушек [11, 12]. Данные защитные механизмы нового типа представляют интерес для практического применения в составе комплексных средств обеспечения информационной безопасности информационно-телекоммуникационных систем, используемых на железнодорожном транспорте.

Настоящая статья построена следующим образом. В первой части описываются основные требования к построению алгоритмов псевдовероятностного шифрования и модель потенциального нарушителя. Во второй части представлены способы блочного ПВ-шифрования с вычислением

блоков шифртекста как двоичных чисел путем решения систем сравнений. В третьей части описываются алгоритмы ПВ-шифрования с формированием блоков выходного шифртекста в виде решения систем линейных уравнений в конечном поле (простом и двоичном).

Требования к алгоритмам блочного псевдовероятностного шифрования

Алгоритмы блочного ПВ-шифрования как частные случаи алгоритмов ОШ с разделяемым ключом ориентированы на обеспечение стойкости к атакам с принуждением к раскрытию ключа шифрования. Принудительная атака представляет собой некоторое обобщение разных потенциальных атак, в ходе которых атакующий получает ключ шифрования. Наиболее характерным для модели принудительной атаки является то, что атакующий после перехвата шифртекста получает значение ключа шифрования, с помощью которого может быть восстановлено исходное сообщение. Принимая такую модель, можно абстрагироваться от конкретных способов действий атакующего, с помощью которых ему становится известным ключ. Такими действиями могут быть установка технических и программных закладок, подкуп, хищение ключевых носителей, перехват ключевой информации по побочным каналам, криптоанализ и др.

При разработке механизмов защиты информации, основанных на обманных криптографических, могут создаваться условия облегченного получения ключа шифрования, например, использование более короткого фиктивного ключа по сравнению с секретным ключом. Для практического использования защитных механизмов, основанных на ПВ-шифровании, следует разработать алгоритмы, обеспечивающие достаточно высокую скорость ПВ-шифрования и отсутствие признаков, по которым нарушитель мог бы определить, что шифрование не является вероятностным.

Для обеспечения последнего положения представляется важным выполнение следующих требований к построению ПВ-шифров, в том числе блочных алгоритмов ПВ-шифрования:

• криптограмма, полученная в процессе ПВ-шифрования, должна быть неотличима от криптограммы, получаемой в ходе процедуры вероятностного шифрования;

• восстановление из криптограммы фиктивного и секретного сообщений должно происходить независимо друг от друга;

• алгоритмы расшифровывания фиктивного и секретного сообщений должны совпадать.

Псевдовероятностное шифрование с вычислением блоков шифртекста из системы сравнений

Рассмотрим способ блочного ПВ-шифрования, реализуемый в виде совместного шифрования двух независимых сообщений – фиктивного M и секретного T, выполняемого по двум независимым ключам в единый шифртекст. Для обеспечения возможности независимого восстановления из последнего каждого из входных сообщений с использованием одного и того же алгоритма зададим разбиение M и T на блоки данных одинаковой длины, равной n бит, и формирование n-битовых блоков промежуточных шифртекстов с использованием некоторого апробированного алгоритма блочного шифрования E.

Полный секретный ключ ПВ-шифрования сформируем в виде секретного (K_1, p_1) и фиктивного (K_2, p_2) ключей, где элементы K_1 и K_2 – это ключи блочного n-битового шифра E, а p_1 и p_2 – пара взаимно простых чисел длины $n + 1$ бит. Совместное криптографическое преобразование сообщений $T = (T_1, T_2, \ldots, T_z)$ и $M = (M_1, M_2, \ldots, M_z)$, представленных в виде последовательностей n-битовых блоков данных, определим как последовательное преобразование соответствующих пар входных блоков T_i и M_i в единый расширенный блок шифр текста C_i (для $i = 1, 2, \ldots, z$) по следующему алгоритму:

1) используя функцию блочного шифрования E и ключ K_1, преобразовать входной блок данных T_i в блок промежуточного шифртекста $C_{Ti} = E_{K1}(T_i)$;

2) используя блочный шифр E и ключ K_1, преобразовать входной блок данных M_i в блок промежуточного шифртекста $C_{Mi} = E_{K2}(M_i)$;

3) используя ключевые элементы p_1 и p_2 и трактуя n-битовые блоки промежуточных шифртекстов C_{Ti} и C_{Mi} как числа, представленные в двоичном виде, вычислить единый блок выходного шифртекста C_i в виде решения системы сравнений

$$\begin{cases} C_i \equiv C_{T_i} \bmod p_1; \\ C_i \equiv C_{M_i} \bmod p_2. \end{cases} \qquad (1)$$

Для записи значения блока единого шифртекста C_i резервируется $2n + 2$ битов, что является достаточным, поскольку при любых значениях p_1 и p_2 имеет место условие $C_i < 2^{2n+2}$. Криптограмма C, содержащая в преобразованном виде оба входных сообщения, представляется в виде последовательности блоков шифртекста C_i: $C = (C_1, C_2, \ldots, C_z)$.

В соответствии с китайской теоремой об остатках решение системы линейных сравнений (1) описывается формулой

$$C_i = [C_{Ti} p_2 (p_2^{\,1} \bmod p_1) + C_{Mi} p_1 (p_1^{\,1} \bmod p_2)] \bmod p_1 p_2,$$

которая и задает вычислительную процедуру отображения пары блоков промежуточных шифртекстов в единый расширенный блок выходного шифртекста. Легко заметить, что значения $p_2 (p_2^{\,1} \bmod p_1)$ и $p_1 (p_1^{\,1} \bmod p_2)$ могут быть вычислены предварительно, что позволит повысить производительность описанного алгоритма блочного ПВ-шифрования.

Стойкость данного ПВ-шифра к принуждающим атакам обеспечивается возможностью правдоподобно утверждать, что шифртекст сформирован путем вероятностного шифрования фиктивного сообщения M по фиктивному ключу (K_2, p_2). Доводом в пользу такой интерпретации является представляемый ассоциированный алгоритм вероятностного шифрования и связанный с ним алгоритм процедуры расшифровывания шифртекста.

Ассоциируемый алгоритм вероятностного шифрования можно описать следующим образом:

1) разбить сообщение M на n-битовые блоки M_i:

$$M = (M_1, M_2, \ldots, M_z);$$

2) зашифровать каждый i-й ($i = 1, 2, \ldots, z$) блок входных данных M_i, выполняя следующие шаги:

2.1) используя n-битовый алгоритм блочного шифрования E, зашифровать блок данных M_i по ключу K_2

$$C_{Mi} = E_{K2}(M_i);$$

2.2) сгенерировать случайное число r, удовлетворяющее условию $2^n < r < 2^{n+1}$ и взаимно простое с p_2;

2.3) сгенерировать случайное число $R < 2^n$;

2.3) вычислить i-й блок криптограммы C_i как решение системы линейных сравнений

$$\begin{cases} C_i \equiv C_{M_i} \bmod p_2; \\ C_i \equiv R \bmod r. \end{cases} \quad (2)$$

Легко показать, что каждый блок C_i криптограммы C мог быть получен в результате вероятностного шифрования блока фиктивного сообщения M_i по фиктивному ключу при использовании представленного алгоритма вероятностного блочного шифрования. Действительно, пусть C_i и $C_{Mi} = E_{K2}(M_i)$ удовлетворяют первому сравнению системы (2). Тогда для любого значения r, которое является взаимно простым с p_2 и удовлетворяет условию $C_i < rp_2$, имеется значение $R = C_i \bmod r$, при котором система (2) имеет своим решением заданное значение C_i. Таким образом, зашифровывание фиктивного сообщения M по фиктивному ключу с использованием ассоциированного алгоритма вероятностного шифрования потенциально может привести к формированию шифртекста, полученного с помощью ПВ-шифрования сообщений M и T.

Алгоритму ПВ-шифрования и ассоциируемому с ним алгоритму вероятностного шифрования соответствует один и тот же алгоритм расшифровывания криптограммы $C = (C_1, C_2, \ldots, C_i, \ldots, C_z)$ по ключу (K_2, p_2), который описывается следующими шагами:

1) каждый i-й ($i = 1, 2, \ldots, z$) блок C_i расшифровать, выполнив следующие два шага:

1.1) вычислить блок промежуточного шифртекста $C_{Mi} = C_i \bmod p_2$;

1.2) расшифровать блок C_{Mi} по ключу K_2, используя функцию блочного расшифровывания $D = E^{-1}$

$$M_i = D_{K2}(C_{Mi});$$

2) объединить все восстановленные блоки M_i в сообщение $M = (M_1, M_2, \ldots, M_i, \ldots, M_z)$.

В случае принуждающей атаки отправитель и получатель криптограммы C предоставляют атакующему ключ (K_2, p_2) и сообщение M в качестве секретных значений. При этом они поясняют, что блочный шифр E использован в режиме вероятностного шифрования (и предоставляют атакующему ассоциированный алгоритм вероятностного шифрования). Применение режима вероятностного шифрования они поясняют желанием повышения стойкости шифрования и защиты от возможных непредвиденных слабостей блочного шифра E.

Секретное сообщение из криптограммы $C = (C_1, C_2, .., C_z)$ восстанавливается также путем выполнения последнего алгоритма, но при использовании секретного ключа (K_1, p_1), что определяет такую последовательность шагов:

1) каждый i-й ($i = 1, 2, \ldots, z$) блок C_i расшифровать, выполнив следующие два шага:

1.1) вычислить блок промежуточного шифртекста $C_{Ti} = C_i \bmod p_1$;

1.2) расшифровать блок C_{Ti} по ключу K_1, используя функцию блочного расшифровывания $D = E^{-1}$

$$T_i = D_{K1}(C_{Ti});$$

2) объединить все восстановленные блоки T_i в сообщение $T = (T_1, T_2, \ldots, T_i, \ldots, T_z)$.

Таким образом, рассмотренный блочный ПВ-шифр удовлетворяет принятым критериям построения, т. е. в нем совпадают алгоритмы восстановления из криптограммы C фиктивного и секретного сообщения. Также они совпадают с алгоритмом расшифровывания криптограммы, полученной с помощью ассоциированного алгоритма вероятностного шифрования.

Псевдовероятностные шифры с вычислением блоков шифртекста из системы уравнений

Рассмотрим построение скоростных алгоритмов псевдовероятностного шифрования с отображением пар промежуточных шифртекстов, реализуемое в виде процедуры решения системы линейных уравнений в простом конечном поле. Так же, как в предыдущем шифре, предполагается предварительное зашифровывание блоков входных сообщений M и T с помощью блочного шифра E на ключах $K = (K_1, K_2)$ и $Q = (Q_1, Q_2)$, соответственно, подключи которых используются также в качестве коэффициентов уравнений, входящих в систему. При этом при генерации подключей K_1, K_2, Q_1 и Q_2 следует обеспечить выполнимость условия $K_1Q_2 - K_2Q_1 \neq 0 \bmod p$ (условие существования единственного решения для системы двух линейных уравнений).

Пусть, например, промежуточное шифрование выполняется с помощью блочного шифра E с размером входного блока $n = 64$ бит и 128-битовым ключом K, представленным в виде пары 64-битовых подключей K_1 и K_2: $K = (K_1, K_2)$. Блочное ПВ-шифрование сообщений T и M, имеющих одинаковый размер, задается следующим алгоритмом:

1) разбить сообщения T и M на 64-битовые блоки T_i и M_i:

$$T = (T_1, T_2, \ldots, T_i, \ldots, T_z);$$

$$M = (M_1, M_2, \ldots, M_i, \ldots, M_z);$$

2) каждый i-й блок T_i и каждый i-й ($i = 1, 2, \ldots, z$) блок M_i зашифровать, выполнив следующие два шага:

2.1) зашифровать блок данных T_i по ключу Q

$$C_{Ti} = E_Q(T_i);$$

2.2) зашифровать блок данных M_i по ключу K

$$C_{Mi} = E_K(M_i);$$

3) для каждого значения $i = 1, 2, \ldots, z$ сформировать 130-битовый блок криптограммы C_i в виде конкатенации двух 65-битовых значений C_i' и C_i'': $C_i = (C_i', C_i'')$, являющихся решением системы линейных уравнений с неизвестными C_i' и C_i'':

$$\begin{cases} K_1C_i' + K_2C_i'' \equiv C_{M_i} \bmod p; \\ Q_1C_i' + Q_2C_i'' \equiv C_{T_i} \bmod p, \end{cases} \quad (3)$$

где p – некоторое специфицированное простое число длиной 65 бит, такое, что операция умножения по модулю p

может быть выполнена без операции арифметического деления на p (например, p = 18446744073709551629; p = = 18446744073709553681).

Ассоциируемый алгоритм вероятностного шифрования описывается следующим образом:

1) разбить сообщение M на 64-битовые блоки M_i

$$M = (M_1, M_2, \ldots, M_z);$$

2) каждый i-й (i = 1, 2, …, z) блок зашифровать, выполнив следующие три шага:

2.1) зашифровать блок данных M_i по ключу K с использованием n-битового блочного алгоритма шифрования E по формуле $C_{Mi} = E_K(M_i)$;

2.2) сгенерировать случайные числа $R < p$ и $r < p$;

2.3) вычислить i-й блок криптограммы C_i как решение системы сравнений

$$\begin{cases} K_1 C_i' + K_2 C_i'' \equiv C_{M_i} \bmod p; \\ C_i' + r_i C_i'' \equiv R \bmod p. \end{cases} \quad (4)$$

При фиксированном ключе K каждый i-й блок C_i криптограммы в общем случае может быть получен с помощью ассоциированного алгоритма вероятностного шифрования при различных парах значений R и r. Действительно, выбор произвольного числа r однозначно определяет значение R, при котором второе уравнение в (4) будет выполняться для фиксированного значения C_i.

Вместо (4) в ассоциируемом алгоритме вероятностного шифрования можно задать систему линейных уравнений, в которой второе уравнение имеет более простой вид:

$$\begin{cases} K_1 C_i' + K_2 C_i'' \equiv C_{M_i} \bmod p; \\ C_i' \equiv r_i C_i'' \bmod p. \end{cases}$$

Расшифровывание криптограммы $C = (C_1, C_2, \ldots, C_i, \ldots, C_z)$ по фиктивному ключу $K = (K_1, K_2)$ выполняется следующим образом:

1) каждый i-й (i = 1, 2, …, z) 130-битовый блок C_i представить в виде конкатенации двух 65-битовых подблоков C_i' и C_i'' и расшифровать его, выполнив следующие два шага:

1.1) вычислить 64-битовый блок промежуточного шифртекста

$$C_{M_i} \equiv K_1 C_i' + K_2 C_i'' \bmod p;$$

1.2) расшифровать блок C_{Mi} по ключу K, используя функцию блочного расшифровывания $D = E$ [1]:

$$M_i = D_K(C_{Mi});$$

2) объединить все восстановленные 64-битовые блоки данных M_i в сообщение

$$M = (M_1, M_2, \ldots, M_i, \ldots, M_z).$$

Раскрытие секретного сообщения из криптограммы C = = (C_1, C_2, …, C_z) выполняется по этому же алгоритму при использовании секретного ключа $Q = (Q_1, Q_2)$:

1) каждый i-й (i = 1, 2, …, z) 130-битовый блок C_i расшифровать, выполнив следующие два шага:

1.1) вычислить 64-битовый блок промежуточного шифртекста $C_{T_i} \equiv Q_1 C_i' + Q_2 C_i'' \bmod p$;

1.2) расшифровать блок C_{Ti} по ключу Q, используя функцию блочного расшифровывания $D = E$ [1]:

$$T_i = D_Q(C_{Ti});$$

2) объединить все восстановленные 64-битовые блоки данных T_i в сообщение $T = (T_1, T_2, \ldots, T_z)$.

Подблоки C_i' и C_i'' имеют размер, равный 65 бит, а блок C_i – 130 бит. Это на 2 бита больше, чем суммарная длина блоков входных данных. Чтобы обеспечить равенство размера объединенного блока криптограммы сумме размеров входных блоков данных, следует воспользоваться заданием системы уравнений, аналогичной (3), в конечном поле двоичных многочленов.

Алгоритмы на основе решения систем линейных уравнений в конечных двоичных полях

Пусть требуется выполнить совместное шифрование двух сообщений $T = (T_1, T_2, \ldots, T_z)$ и $M = (M_1, M_2, \ldots, M_z)$, где T_i и M_i – 128-битовые блоки. Произведем промежуточное шифрование каждого блока данных M_i с помощью алгоритма блочного шифрования E с размером входного блока n = = 128 бит и 256-битовым ключом K, представленным в виде пары 128-битовых подключей K_1 и K_2: $K = (K_1, K_2)$. Для промежуточного шифрования блоков T_i также воспользуемся блочным шифром E и другим 256-битовым ключом Q, представленным в виде пары 128-битовых подключей Q_1 и Q_2: $Q = (Q_1, Q_2)$. Генерацию ключей K и Q выполним как генерацию пар равновероятных случайных 128-битовых строк, рассматриваемых как двоичные многочлены и удовлетворяющих условию $K_1 Q_2 - K_2 Q_1 \neq 0 \bmod \eta(x)$, где $\eta(x)$ – неприводимый двоичный многочлен степени 128, являющийся специфицируемым параметром ПВ-шифра.

Блочное ПВ-шифрование сообщений M и T можно задать по следующему алгоритму:

1) каждый i-й 128-битовый блок данных T_i и каждый i-й (i = 1, 2, …, z) блок M_i зашифровать, выполнив следующие два шага:

1.1) зашифровать 128-битовый блок данных M_i по ключу K

$$C_{Mi} = E_K(M_i);$$

1.2) зашифровать 128-битовый блок данных T_i по ключу Q

$$C_{Ti} = E_Q(T_i);$$

2) для каждого значения i = 1, 2, …, z сформировать 256-битовый блок криптограммы C_i в виде конкатенации двух 128-битовых двоичных многочленов C_i' и C_i'': $C_i = (C_i', C_i'')$, являющихся решением системы линейных уравнений с неизвестными C_i' и C_i'':

$$\begin{cases} K_1 C_i' + K_2 C_i'' \equiv C_{M_i} \bmod \eta(x); \\ Q_1 C_i' + Q_2 C_i'' \equiv C_{T_i} \bmod \eta(x). \end{cases} \quad (5)$$

Ассоциируемый алгоритм вероятностного шифрования описывается следующим образом:

1) разбить сообщение M на 128-битовые блоки M_i:

$$M = (M_1, M_2, \ldots, M_z);$$

2) каждый i-й (i = 1, 2, …, z) блок зашифровать, выполнив следующие три шага:

2.1) зашифровать блок данных M_i по ключу Q с использованием 128-битового блочного алгоритма шифрования E по формуле $C_{Mi} = E_Q(M_i)$;

2.2) сгенерировать случайные двоичные многочлены $\lambda(x)$ и $\rho(x)$ степени 127;

2.3) вычислить i-й 256-битовый блок криптограммы $C_i = (C_i', C_i'')$ как решение системы уравнений

$$\begin{cases} K_1 C_i' + K_2 C_i'' \equiv C_{M_i} \bmod \eta(x); \\ C_i' + \lambda(x) C_i'' \equiv \rho(x) \bmod \eta(x). \end{cases} \quad (6)$$

Заданный блок криптограммы C_i может быть получен с помощью ассоциированного алгоритма вероятностного шифрования при фиксированных значениях фиктивного ключа K и блока промежуточного шифртекста C_{Mi} при различных парах значений многочленов $\lambda(x)$ и $\rho(x)$. При этом выбор произвольного многочлена $\lambda(x)$ однозначно определяет значение $\rho(x)$, для которого система уравнений (5) в качестве своего решения будет иметь пару многочленов C_i', C_i'', таких, что $C_i = (C_i', C_i'')$.

Расшифровывание криптограммы $C = (C_1, C_2, \ldots, C_z)$ по фиктивному ключу $K = (K_1, K_2)$ выполняется следующим образом:

1) каждый i-й ($i = 1, 2, \ldots, z$) 256-битовый блок C_i расшифровать, выполнив следующие два шага:

1.1) вычислить 128-битовый блок промежуточного шифртекста по формуле

$$C_{M_i} = K_1 C_i' + K_2 C_i'' \bmod \eta(x);$$

1.2) расшифровать 128-битовый блок C_{Mi} по ключу K, используя функцию блочного расшифровывания $D = E^{-1}$

$$M_i = D_K(C_{Mi});$$

2) объединить все восстановленные блоки M_i в сообщение $M = (M_1, M_2, \ldots, M_i, \ldots, M_z)$.

Раскрытие секретного сообщения из криптограммы $C = (C_1, C_2, \ldots, C_z)$ выполняется по ключу $Q = (Q_1, Q_2)$ следующим образом:

1) каждый i-й ($i = 1, 2, \ldots, z$) 256-битовый блок C_i расшифровать, выполнив следующие два шага:

1.1) вычислить 128-битовый блок промежуточного шифртекста

$$C_{T_i} \equiv Q_1 C_i' + Q_2 C_i'' \bmod \eta(x);$$

1.2) расшифровать 128-битовый блок C_{Ti} по ключу Q, используя функцию блочного расшифровывания $D = E^{-1}$,

$$T_i = D_K(C_{Ti});$$

2) объединить все восстановленные блоки T_i в сообщение $T = (T_1, T_2, \ldots, T_z)$.

В описанном ПВ-шифре в качестве функции блочного шифрования E можно использовать 128-битовый алгоритм блочного шифрования, рекомендуемый стандартом ГОСТ Р 34.12-2015. В общем случае для шифрования сообщений T и M можно использовать блочные шифры с разными размерами входного блока. Например, сообщение T можно разбивать на 64-битовые блоки данных T_i и шифровать последние с помощью 64-битового шифра, а сообщение M – на 128-битовые блоки M_i с последующим их шифрованием с использованием 128-битового блочного шифра. Однако блоки промежуточного шифртекста потребуется объединять путем совместного решения двух линейных уравнений (5), записанных по модулю одного и того же неприводимого двоичного многочлена $\eta(x)$ степени 128. Это приведет к тому, что объединенный блок C_i криптограммы будет иметь размер 256 бит, что превышает сумму размеров блоков T_i и M_i.

Для разбиения сообщений T и M на блоки данных разного размера предпочтительно использовать построение алгоритма ПВ-шифрования с объединением блоков промежуточных шифртекстов путем решения системы из двух уравнений, в которой в качестве модулей можно использовать двоичные многочлены разной степени (например, 128 и 64 бит), за счет чего можно обеспечить равенство размера объединенного блока (192 бит) сумме размеров блоков промежуточных шифртекстов, имеющих различную длину.

Заключение

В настоящей статье показана перспективность применения ПВ-шифрования для построения новых механизмов защиты информации, сформулированы основные требования к ПВ-шифрам, рассмотрены способы построения и предложены конкретные алгоритмы блочного ПВ-шифрования с разделяемым ключом. Выполнимость критерия вычислительной неразличимости по шифртексту блочного ПВ-шифра от блочного вероятностного шифра доказывается наличием ассоциированного алгоритма вероятностного шифрования.

Предложенные способы блочного ПВ-шифрования задают процедуру совместного зашифровывания двух сообщений, однако они легко расширяются для одновременного шифрования трех и более сообщений.

Дальнейшее развитие тематики ПВ-шифрования можно связать с разработкой рандомизированных ПВ-шифров, с поиском новых способов задания взаимно однозначного отображения блоков промежуточных шифртекстов в единый блок выходной криптограммы и ПВ-шифров, включающих процедуру предварительного сжатия входных сообщений.

Литература

1. Dachman-Soled D. On minimal assumptions for sender-deniable public key encryption // Public-Key Cryptography-PKC 2014: 17th Int. Conf. Practice and Theory in Public-Key Cryptography. Lecture Notes Comp. Sci. 2014. Vol. 8383. P. 574-591.

2. Ibrahim M. H. A Method for Obtaining Deniable Public-Key Encryption // Int. J. Network Security. 2009. Vol. 8, № 1. P. 1-9.

3. Canetti R., Dwork C., Naor M., Ostrovsky R. Deniable Encryption // Proc. Advances in Cryptology – CRYPTO 1997. Lectute Notes in Computer Science. Springer – Verlag. 1997. Vol. 1294. P. 90-104.

4. Ishai Yu., Kushilevits E., Ostrovsky R. Efficient non-interactive secure computation // Advances in Cryptology – EUROCRYPT 2011. Lectute Notes in Computer Science. Springer – Verlag. 2011. Vol. 6632. P. 406-425.

5. Meng B. A secure Internet voting protocol based on non-interactive deniable authentication protocol and proof protocol that two ciphertexts are encryption of the same plaintext // J. Networks. 2009. Vol. 4. P. 370-377.

6. Barakat T. M. A New Sender-Side Public-Key Deniable Encryption Scheme with Fast Decryption // KSII Transactions on Internet and Information Systems. 2014. Vol. 8, №. 9. P. 3231-3249.

7. Молдовян Н. А., Биричевский А. Р., Мондикова Я. А. Отрицаемое шифрование на основе блочных шифров // Информационно-управляющие системы. 2014. № 5. С. 80-86.

8. Moldovyan N.A., Shcherbacov A.V., Eremeev M.A. Deniable-encryption protocols based on commutative ciphers // Quasigroups and related systems. 2017. Vol. 25, № 1. P. 95-108.

9. Moldovyan N.A. Berezin A.N., Kornienko A.A., Moldovyan A.A., Bi-deniable Public-Encryption Protocols Based on Standard PKI // Proc. 18th FRUCT & ISPIT Conf., 18-22 Apr. 2016. St. Petersburg. P. 212-219.

10. Moldovyan N.A., Moldovyan A.A., Moldovyan D.N., Shcherbacov V.A. Stream Deniable-Encryption Algorithms // Comput. Sci. J. Moldova. 2016. Vol. 24, № 1 (70). P. 68-82.

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

12. Березин А. Н., Биричевский А. Р., Молдовян Н. А., Рыжков А. В. Способ отрицаемого шифрования // Вопр. защиты информации. 2013. № 2. С. 18-21.

Deniable-encryption Methods Based on Block Ciphers

Moldovyan A. A.
Saint-Petersburg Institute for Informatics and Automation of RAS
St. Petersburg, Russia
maa1305@yandex.ru

Tatchina Ya. A.
Saint-Petersburg State Electrotechnical University "LETI"
St. Petersburg, Russia
iana.tatchina@gmail.com

Abstract. **Pseudo-probabilistic encryption is presented as a new algorithmic mechanism for ensuring information security, which implements information protection in the event of attacks with compelling disclosure of the encryption key. The basic requirement for transformations of this type is the computational indistinguishability of the ciphertext from probabilistic encryption. We consider methods and algorithms that implement pseudo-probability encryption as a simultaneous cryptographic transformation of fictitious and secret messages in two different keys, consisting in the formation of blocks of intermediate ciphertexts and their reversible mapping into a single extended block of the output cryptogram. Algorithms are proposed that include the task of the unifying mapping procedure in the form of solutions of systems of linear equations and comparisons in which numbers and binary polynomials are used as a module. The proposed methods have a sufficiently high productivity and are of considerable interest for practical application in information security systems.**

Keywords: **cryptography, denied encryption, pseudo-probabilistic encryption, symmetric encryption, block ciphers, probabilistic encryption, cryptogram.**

References

1. Dachman-Soled D. On minimal assumptions for sender-deniable public key encryption, *Public Key Cryptography PKC 2014: 17th Int. Con. Practice and Theory in Public Key Cryptography. Lecture Notes Comp. Sci.*, 2014, Vol. 8383, pp. 574-591.

2. Ibrahim M. H. A Method for Obtaining Deniable Public-Key Encryption, *Int. J. of Network Security*, 2009, Vol. 8, no. 1, pp. 1-9.

3. Canetti R., Dwork C., Naor M., Ostrovsky R. Deniable Encryption, *Proc. Advances in Cryptology – CRYPTO 1997. Lectute Notes in Computer Science. Springer – Verlag*, 1997, Vol. 1294, pp. 90-104.

4. Ishai Yu., Kushilevits E., Ostrovsky R. Efficient non-interactive secure computation, *Advances in Cryptology – EURO CRYPT 2011. Lectute Notes in Computer Science. Springer – Ver lag*, 2011, Vol. 6632, pp. 406-425.

5. Meng B. A secure Internet voting protocol based on non-interactive deniable authentication protocol and proof protocol that two ciphertexts are encryption of the same plaintext*, J. Net works*, 2009, Vol. 4, pp. 370-377.

6. Barakat T. M. A New Sender-Side Public-Key Deniable Encryption Scheme with Fast Decryption, *KSII Transactions on In ternet and Information Systems.* 2014, Vol. 8, no. 9, pp. 3231-3249.

7. Moldovyan N. A., Birichevskiy A. R., Mondikova Ya. A. Deniable Encryption Based on Block Ciphers [Otritsaemoe shyfrovanie na osnove blochnyh shyfrov], *Information control systems [Informatsionno upravlyayuschchie sistemy]*, 2014, no. 5, pp. 80-86. (In Russ.)

8. Moldovyan N. A., Shcherbacov A. V., Eremeev M. A. Deniable-encryption protocols based on commutative ciphers, *Quasig roups and related systems*. 2017. Vol. 25, no. 1, pp. 95-108.

9. Moldovyan N. A. Berezin A. N., Kornienko A. A., Moldovyan A. A. Bi-deniable Public-Encryption Protocols Based on Standard PKI. *Proc. 18th FRUCT & ISPIT Conf.*, 18-22 Apr. 2016. St. Petersburg. P. 212-219.

10. Moldovyan N. A., Moldovyan A. A., Moldovyan D. N., Shcherbacov V. A. Stream Deniable-Encryption Algorithms, *Comput. Sci. J. Moldova*, 2016, Vol. 24, no. 1 (70), pp. 68-82.

11. Morozova E. V., Mondikova Ya. A., Moldovyan N. A. Methods for Deniable Encryption with Shared Key [Sposoby otritsaemogo shifrovaniya s razdelyaemym klyuchom]. *Informa tion control systems [Informatsionno upravlyayuschchie sistemy]*, 2013, no. 6, pp. 73-78. (In Russ.)

12. Berezin A. N., Birichevskiy A. R., Moldovyan N. A., Ryzgkov A. V. Method for Deniable Encryption [Sposob otritsaemogo shifrovaniya]. *Items of Information Protection [Voprosy zash chity informatsii]*, 2013, no. 2, pp. 18-21. (In Russ.)