УДК 512.624.5 **DOI** 10.15622/sp.61.5

А.А. Молдовян, Н.А. Молдовян

СПОСОБЫ И АЛГОРИТМЫ ПСЕВДОВЕРОЯТНОСТНОГО ШИФРОВАНИЯ С РАЗДЕЛЯЕМЫМ КЛЮЧОМ

Молдовян А.А., Молдовян Н.А. **Способы и алгоритмы псевдовероятностного шифрования с разделяемым ключом.**

Аннотация. В качестве способа обеспечения секретности сообщений, переданных в зашифрованном виде по открытым каналам связи, при потенциальных атаках с принуждением к раскрытию ключей шифрования предложены алгоритмы и протоколы отрицаемого шифрования, которые разделяются на следующие типы: 1) с открытым ключом; 2) с разделяемым секретным ключом; 3) бесключевые. В статье описываются псевдовероятностные симметричные шифры, представляющие собой специальный вариант реализации алгоритмов отрицаемого шифрования. Обсуждается применение псевдовероятностного шифрования для построения специальных механизмов защиты информации, в том числе стеганографических каналов, носителями которых являются шифртексты. Рассмотрены способы построения поточных и блочных алгоритмов псевдовероятностного шифрования, реализующих совместное шифрование фиктивного и секретного сообщений таким образом, что формируемый шифртекст является вычислительно неразличимым от шифртекста, получаемого в результате вероятностного шифрования фиктивного сообщения. В качестве одного из критериев построения использовано требование неотличимости по шифртексту псевдовероятностного шифрования от вероятностного. Для реализации этого требования в схеме построения псевдовероянностных шифров используется шаг взаимно-однозначного отображения пар блоков промежуточных шифртекстов фиктивного и секретного сообщений в единый расширенный блок выходного шифртекста. Описаны реализации псевдовероятностных блочных шифров, в которых алгоритмы расшифровывания фиктивного и секретного сообщений полностью совпадают. Предложены общие подходы к построению псевдовероятностных протоколов бесключевого шифрования и рандомизированных псевдовероятностных блочных шифров, а также приведены конкретные реализации криптосхем данных типов.

Ключевые слова: криптография, отрицаемое шифрование, псевдовероятностное шифрование, блочный шифр, поточный шифр, фиктивное сообщение, рандомизация шифров, бесключевое шифрование.

1. Введение. Криптографические методы и средства защиты информации широко применяются для защиты информации [1, 2], аутентификации сообщений и пользователей [3, 4] в информационно-телекоммуникационных системах. Они также лежат в основе технологии электронной цифровой подписи [5, 6] и решения задачи обеспечения анонимности пользователей [7] в технологиях тайного электронного голосования и электронных денег. При рассмотрении стойкости криптографических алгоритмов и протоколов обычно принимаются модели потенциального нарушителя, в которых секретный ключ неизвестен. Сравнительно новым направлением в области криптографии является разработка протоколов передачи сообщений, обеспечивающих стойкость к атакам со стороны нарушителя, который принуждает абонентов

сеанса секретной связи раскрыть секретный ключ после того как шифртекст был передан по каналу связи [8-11]. Криптосхемы, обеспечивающие защищенность секретного сообщения при указанных принуждающих атаках, называются протоколами и алгоритмами отрицаемого шифрования (ОШ). Интерес к криптосхемам ОШ связан с решением задач обеспечения информационной безопасности распределенных вычислений [12], защиты технологий тайного электронного голосования от скупки голосов [13, 14] и расширением класса алгоритмических средств защиты информации, используемых в составе комплексных средств обеспечения информационной безопасности [15-17].

Прикладной интерес представляют предложенные недавно реализации схем ОШ на основе механизмов разделения секрета [18, 19] и одноразовых ключей [20], а также протоколы отрицаемой аутентификации [21], ориентированные на применение в системах электронного голосования.

Протоколы ОШ могут быть разделены на следующие три класса: криптосхемы с разделяемым секретным ключом [8, 22], криптосхемы с открытым ключом [23, 24] и бесключевые криптосхемы [25].

В статье [25] впервые рассмотрены протоколы ОШ, основанные на коммутативных функциях шифрования и обсуждается реализация протоколов бесключевого ОШ. Однако предложенная в [25] конкретная реализация протоколов последнего типа не в полной мере соответствует термину «бесключевой», поскольку в ней дополнительно к локальным ключам (которые вырабатываются каждой стороной протокола самостоятельно и не передаются другой стороне) используется вспомогательный ключ, разделяемый получателем и отправителем секретного сообщения.

В рамках первого класса недавно был предложен подход к построению алгоритмов ОШ, в которых выполняется одновременное зашифровывание фиктивного и секретного сообщений в единый шифртекст, вычислительно неразличимый от шифртекста, формируемого как результат вероятностного шифрования фиктивного сообщения [15, 22]. Алгоритмы и протоколы, удовлетворяющие этому критерию, называются псевдовероятностными (ПВ) криптосхемами. В настоящее время известны отдельные публикации, связанные с разработкой алгоритмов ПВ шифрования, однако тематика ПВ шифрования как самостоятельная область прикладной криптографии не была рассмотрена.

В настоящей статье обобщаются известные результаты в области ПВ шифрования, выделяются общие приемы построения криптосхем данного типа, предлагаются новые блочные и поточные ПВ шифры, рассматривается механизм рандомизации ПВ шифров и представ-

лен новый протокол бесключевого ПВ шифрования, в котором устранен недостаток, состоящий в использовании заранее согласованного вспомогательного ключа.

2. Типы псевдовероятностных шифров с разделяемым ключом и модель нарушителя. Известные ПВ криптосхемы с разделяемым ключом делятся на алгоритмы ПВ шифрования следующих типов: поточные [15], блочные [22], алгебраические [25]. Общими моментами, используемыми при их построении, являются:

1) совместное зашифровывание фиктивного и секретного сообщений в единый выходной шифртекст;

2) выполнение критерия вычислительной неотличимости по шифртексту от вероятностного шифрования;

3) предъявление алгоритма вероятностного шифрования, для которого множество шифртекстов, соответствующих фиктивному сообщению, включает шифртекст, полученный в результате ПВ шифрования.

Указанный алгоритм вероятностного шифрования называется ассоциируемым (с алгоритмом ПВ шифрования), поскольку его наличие служит доказательством выполнимости критерия вычислительной неотличимости формируемого шифртекста от криптограммы, вырабатываемой при вероятностном шифровании фиктивного сообщения по фиктивному ключу.

Вероятностное шифрование находит применение как способ повышения стойкости криптографического преобразования, поэтому в случае атаки с принуждением к раскрытию ключа шифрования пользователи, предъявляя атакующему ассоциированный алгоритм, могут правдоподобно утверждать, что при шифровании они использовали криптографическое преобразования с включением случайных значений.

На практике возможны различные варианты потенциальных атак, в рамках которых атакующий получает секретный ключ, использованный для выполнения шифрования. Например, это может произойти в результате подкупа, хищения ключевых носителей, выполнения криптоанализа, предварительной несанкционированной установки программ-закладок и так далее. При рассмотрении протоколов ОШ для обобщения таких атак рассматривается модель принуждающей атаки (или атаки с принуждением), в рамках которой предполагается, что атакующий имеет некоторый ресурс принуждения отправителя сообщения, получателя или одновременно их обоих к раскрытию секретного ключа. При этом принимается предположение, что атакующий перехватил все сообщения, переданные в ходе реализации коммуникационного протокола.

В случае ПВ шифрования как частного случая ОШ стойкость к принуждающим атакам обеспечивается тем, что одновременно зашифровываются два или более сообщения и по крайней мере одно из них

является фиктивным. Атакующему раскрывается ключ, по которому выполнение процедуры восстановления исходного текста по шифртексту приводит к получению фиктивного сообщения. При этом алгоритм расшифровывания не должен содержать признаков, по которым атакующий мог бы сделать обоснованный вывод о возможности восстановления из шифртекста и некоторого другого сообщения. При формулировке требований к алгоритмам ПВ шифрования в качестве указанных признаков рассматриваются следующие признаки:

– неполнота использования шифртекста в ходе выполнения процедуры расшифровывания;

– зависимость процесса расшифровывания от ключа (например, наличие ветвлений в алгоритме расшифровывания, зависящих от ключа);

– неравномерность влияния битов криптограммы на биты восстановленного сообщения.

При разработке алгоритмов ПВ шифрования следует обеспечить отсутствие перечисленных признаков. Потенциально возможны атаки, в которых атакующий может измерить время выполнения процедуры расшифровывания секретного сообщения, а также получить доступ к машинному коду, соответствующему программе алгоритма расшифровывания, или непосредственно к самой программе. Для обеспечения стойкости к атакам последнего типа при разработке алгоритмов ПВ шифрования принимается дополнительный критерий построения, формулируемый следующим образом: *алгоритмы восстановления фиктивного и секретного сообщений должны полностью совпадать.* Этот критерий означает, что один и тот же алгоритм должен восстанавливать фиктивное и секретное сообщения в зависимости от задаваемого ключа расшифровывания.

3. Особенности псевдовероятностного шифрования как механизма защиты информации. Алгоритмы ПВ шифрования позволяют реализовать криптографические обманные ловушки, с помощью которых атакующий направляется на ложный путь. Например, потенциальному нарушителя создаются условия для перехвата (или хищения) фиктивного ключа, с помощью которого из шифртекста восстанавливается фиктивное сообщение. Или размер фиктивного ключа выбирается таким, что атакующий имеет возможность его раскрыть методом полного перебора.

Псевдовероятностное шифрование можно трактовать как способ построения стеганографического канала криптографическими средствами. Действительно, благодаря вычислительной неразличимость по шифртексту алгоритма ПВ шифрования от ассоциированного алгоритма вероятностного шифрования при получении (каким-либо способом) ключа для расшифровывания фиктивного сообщения атакующий не

имеет возможности определить однозначно существование в шифртексте еще одного сообщения.

Само по себе существование способов ПВ шифрования ставит потенциального криптоаналитика перед следующей дилеммой. Предположим, ему удалось восстановить ключ, с помощью которого шифртекст расшифровывается в осмысленное сообщение, однако текущие попытки найти еще один ключ, с помощью которого из шифртекста могло бы быть восстановлено еще одно сообщение, оказываются безуспешными. Следует ли криптоаналитику продолжить вычислительно затратный процесс криптоанализа или принять решение, что перехваченный шифртекст получен в процессе вероятностного шифрования и следует прекратить попытки решения неразрешимой задачи?

Применение алгоритмов вероятностного шифрования, которые могут быть ассоциированы с некоторыми алгоритмами псевдовероятностного шифрования, для защиты передаваемых сообщений (файлов, хранимых в ЭВМ) дает возможность встраивания в отдельные шифртексты дополнительных сообщений (файлов). Прежде чем приступить к раскрытию таких криптографических стегоканалов криптоаналитику требуется решить задачу распознавания шифртекста, допускающего возможность неоднозначного расшифровывания.

В целом ПВ шифры предоставляют возможность разработки и использования новых механизмов защиты информации.

4. Псевдовероятностные блочные шифры. Общим подходом к построению псевдовероятностных блочных шифров, описанных в работах [15, 22], является выполнение следующих трех обобщенных шагов преобразования:

1) разбиение фиктивного и секретного сообщения на блоки данных;

2) независимое зашифровывание пары соответствующих друг другу блоков фиктивного и секретного сообщений на различных ключах;

3) совместное зашифровывание пары блоков промежуточных шифртекстов, полученных на шаге 2, в единый блок выходного шифртекста с помощью обратимой процедуры преобразования.

При этом используемая на шаге 3 процедура зашифровывания задается таким образом, что обратное ей преобразование выполняется как независимое восстановление блоков промежуточных шифртекстов, соответствующих фиктивному и секретному сообщениям, осуществляемое по одним и тем же математическим формулам. Рассмотрим конкретные варианты реализации описанного общего подхода.

Алгоритм ПВ шифрования с использованием процесса решения системы линейных сравнений как процедуры биективного отображения пары блоков промежуточных шифртекстов в единый блок выходного шифртекста описывается следующим образом.

Зададим выполнение совместного шифрования двух различных сообщений $M = (M_1, M_2, \ldots, M_z)$ и $T = (T_1, T_2, \ldots, T_z)$, представленных в виде последовательности n-битовых блоков данных M_i и T_i ($i = 1, 2, \ldots, z$), по ключам (K_1, p_1) и (K_2, p_2) соответственно, причем K_1 и K_2 — ключи некоторого блочного шифра E с n-битовым входом; p_1 и p_2 — взаимно простые числа, удовлетворяющие условиям $2^{n+1} > p_1 > 2^n$ и $2^{n+1} > p_2 > 2^n$:

1. Используя алгоритм блочного шифрования E и ключ K_1, зашифровать i-й блок сообщения T_i: $C_{T_i} = E_{K_1}(T_i)$.

2. Используя блочный шифр E, зашифровать i-й блок сообщения M_i по ключу K_2: $C_{M_i} = E_{K_2}(M_i)$.

3. Используя промежуточные шифртексты C_{T_i} и C_{M_i} и подключи p_1 и p_2, вычислить блок выходного шифртекста C_i как решение следующей системы сравнений:

$$\begin{cases} C_i \equiv C_{T_i} \bmod p_1 \\ C_i \equiv C_{M_i} \bmod p_2 \end{cases}, \tag{1}$$

где выходные блоки C_{T_i} и C_{M_i} функции шифрования E рассматриваются как n-битовые двоичные числа. Криптограмма C, содержащая в себе в скрытом виде сообщения T и M, формируется в виде следующей последовательности блоков шифртекста C_i размером $2n + 2$ бит: $C = (C_1, C_2, \ldots, C_z)$.

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

$$C_i = \left[C_{T_i} p_2 \left(p_2^{-1} \bmod p_1\right) + C_{M_i} p_1 \left(p_1^{-1} \bmod p_2\right)\right] \bmod p_1 p_2.$$

При выполнении вычислений по этой формуле наибольший вклад в вычислительную трудоемкость расчета блока криптограммы C_i вносят две операции инверсии по модулям p_1 и p_2 и операция деления на число $p_1 p_2$. Вычисление значений $p_2\left(p_2^{-1} \bmod p_1\right)$ и $p_1\left(p_1^{-1} \bmod p_2\right)$ может быть осуществлено на этапе генерации секретных ключей. В этом случае основной вклад в трудоемкость вычисле-

ния значения C_i вносит операция деления значения в квадратных скобках на модуль p_1p_2, которую надо выполнять при формировании каждого нового блока криптограммы, объединяющей два текущих блока промежуточных шифртекстов C_{T_i} и C_{M_i}.

С описанным алгоритмом ПВ шифрования ассоциируется следующий алгоритм вероятностного шифрования фиктивного сообщения M:

1. Разбить сообщение M на n-битовые блоки данных M_i: $M = (M_1, M_2, \ldots, M_z)$.

2. Каждый i-й ($i = 1, 2, \ldots, z$) блок зашифровать, выполнив следующие три шага:

2.1. Зашифровать блок данных M_i по ключу K_2 с использованием n-битового блочного алгоритма шифрования E по формуле $C_{M_i} = E_{K_2}(M_i)$.

2.2. Сгенерировать случайное число $R < 2^n$ и простое случайное значение $r \neq p_2$, удовлетворяющее условию $2^n < r < 2^{n+1}$.

2.3. Вычислить i-й блок криптограммы C_i как решение следующей системы сравнений:

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

Легко можно увидеть, что в шифртексте C каждый i-й блок C_i потенциально может быть получен как результат преобразования блока фиктивного сообщения M_i в соответствии с ассоциированным алгоритмом вероятностного шифрования. Причем это реализуется при выборе многих различных пар значений $R < 2^n$ и $r < 2^{n+1}$. Для произвольного простого числа r, удовлетворяющего условию $rp_2 < C_i$, по формуле $R \equiv C_i \bmod r$ находим число R, при котором для пары значений r и R решение системы (2) совпадает со значением C_i. Это показывает, что шифртекст C потенциально может быть получен в результате вероятностного шифрования фиктивного сообщения по фиктивному ключу (K_2, p_2).

Чтобы доказать, что шифртекст C содержит не только фиктивное, но и секретное сообщение T, потенциальному криптоаналитику потребуется вычислить ключ (K_1, p_1) и восстановить по нему из шифртекста C сообщение T. Однако последнее даже при известном значении p_2 не проще взлома алгоритма блочного шифрования E. Действительно, по известному p_2 можно вычислить шифртекст, формируемый

на выходе функции блочного шифрования E при шифровании сообщения T по ключу K_1, то есть имеем стандартные условия, при которых блочные шифры должны быть стойкими.

Расшифровывание криптограммы $C = (C_1, C_2, \ldots, C_i, \ldots, C_z)$ по фиктивному ключу (K_2, p_2) выполняется следующим образом:

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

1.1. Вычислить блок промежуточного шифртекста $C_{M_i} = C_i \bmod p_2$.

1.2. Расшифровать блок C_{M_i} по ключу K_2, используя функцию блочного расшифровывания $D = E^{-1}$: $M_i = D_{K_2}(C_{M_i})$.

2. Объединить восстановленные блоки данных M_i в единое сообщение $M = (M_1, M_2, \ldots, M_i, \ldots, M_z)$.

Для восстановления секретного сообщения T из криптограммы $C = (C_1, C_2, \ldots, C_i, \ldots, C_z)$ используется ключ (K_1, p_1) и тот же алгоритм расшифровывания:

1. Преобразовать каждый i-й блок шифртекста C_i:

1.1. Вычислить значение $C_{T_i} = C_i \bmod p_1$.

1.2. Расшифровать блок промежуточного шифртекста C_{T_i} по формуле: $T_i = D_{K_1}(C_{T_i})$.

2. Объединить восстановленные блоки данных T_i в единое сообщение $T = (T_1, T_2, \ldots, T_i, \ldots, T_z)$.

По аналогии с рассмотренным алгоритмом блочного ПВ шифрования может быть построен ПВ блочный шифр с использованием вычислений над двоичными многочленами (подключи и преобразуемые блоки данных рассматриваются как двоичные многочлены, представленные упорядоченным набором коэффициентов последнего). При таком подходе получаем следующий алгоритм совместного шифрования сообщений T и M по ключам (K_1, η_1) и (K_2, η_2), где подключи η_1 и η_2 — взаимно неприводимые двоичные многочлены степени n:

1. Вычислить n-битовый блок промежуточного шифртекста C_{T_i} по формуле $C_{T_i} = E_{K_1}(T_i)$.

2. Вычислить n-битовый блок промежуточного шифртекста C_{M_i} по формуле $C_{M_i} = E_{K_2}(M_i)$.

3. Сформировать $2n$-битовый блок выходного шифртекста C_i как решение следующей системы сравнений:

$$\begin{cases} C_i \equiv C_{T_i} \bmod \eta_1 \\ C_i \equiv C_{M_i} \bmod \eta_2 \end{cases}, \tag{3}$$

в которой блоки C_{T_i} и C_{M_i} промежуточных шифртекстов трактуются как двоичные многочлены числа, а размер блока шифртекста C_i равен $2n$.

Решение системы линейных сравнений (3) задается формулой:

$$C_i = \left[C_{T_i}\eta_2\left(\eta_2^{-1} \bmod \eta_1\right) \oplus C_{M_i}\eta_1\left(\eta_1^{-1} \bmod \eta_2\right)\right] \bmod \eta_1\eta_2,$$

где $\oplus$ — операция сложения двоичных многочленов (поразрядное суммирование битовых строк по модулю два). Так же как и в случае шифра-налога, вычисление значений $\eta_2\left(\eta_2^{-1} \bmod \eta_1\right)$ и $\eta_1\left(\eta_1^{-1} \bmod \eta_2\right)$ может быть осуществлено на этапе генерации секретных ключей, что позволяет значительно повысить производительность процедуры шифрования.

Заслуживает внимания вариант реализации блочного ПВ шифра с различным размеров входных блоков данных M_i и T_i. Например, для большей степени скрытности криптографического стегоканала секретное сообщение предварительно сжимается с устранением его избыточности и существенным сокращением размера текста $T = (T_1, T_2, \ldots, T_i, \ldots, T_z)$. Если размеры блоков данных задаются равными значениям n_1 и n_2, то, соответственно, следует задать степени многочленов η_1 и η_2 равными n_1 и n_2. Размер блока выходного шифртекста в точности равен сумме $n_1 + n_2$.

Рассмотрим построение блочного ПВ шифра, в котором в качестве процедуры преобразования пар блоков промежуточных шифртекстов в единый блок выходного шифртекста используется решение системы уравнений в конечном поле. В данном случае в отличии от предыдущего алгоритма размер входных блоков M_i и T_i должен быть одинаковым: $n_1 = n_2 = n$. Пусть, например, $n = 128$ и блоки промежуточного шифртекста формируются путем зашифровывания блоков фиктивного и секретного сообщений с помощью 128-битовой функции блочного шифрования E и 256-битовых ключей $K = (K_1, K_2)$ и $Q = (Q_1 , Q_2)$, каждый из которых разбит на два 128-битовых подключа. Генерацию ключей K и Q выполним как генерацию пар равноверо-

ятных случайных 128-битовых строк, рассматриваемых как двоичные многочлены и удовлетворяющих условию $K_1 Q_2 \oplus K_2 Q_1 \neq 0 \bmod \eta$, где η — неприводимый двоичный многочлен степени 128.

Процедуру совместного шифрования сообщений T и M зададим в виде следующих шагов:

1. Разбить сообщения T и M на 128-битовые блоки T_i и M_i.

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

2.1. Зашифровать блок данных T_i по ключу Q: $C_{T_i} = E_Q(T_i)$.

2.2. Зашифровать блок данных M_i по ключу K: $C_{M_i} = E_K(M_i)$.

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

$$\begin{cases} K_1 C'_i \oplus K_2 C''_i \equiv C_{M_i} \bmod \eta \\ Q_1 C'_i \oplus Q_2 C''_i \equiv C_{T_i} \bmod \eta \end{cases}, \tag{4}$$

Ассоциируемый алгоритм вероятностного шифрования имеет вид:

1. Разбить сообщение M на 128-битовые блоки M_i.

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

2.1. Зашифровать блок данных M_i по ключу K: $C_{M_i} = E_K(M_i)$.

2.2. Сгенерировать случайные двоичные многочлены λ и ρ степени 127.

2.3. Вычислить i-й 256-битовый блок шифртекста $C_i = (C'_i, C''_i)$ как решение следующей системы сравнений:

$$\begin{cases} K_1 C'_i \oplus K_2 C''_i \equiv C_{M_i} \bmod \eta \\ C'_i \oplus \lambda C''_i \equiv \rho \bmod \eta \end{cases}. \tag{5}$$

При фиксированном ключе K и фиксированном блоке промежуточного шифртекста C_{M_i} один и тот же блок C_i криптограммы в общем случае может быть получен с помощью ассоциированного алгоритма вероятностного шифрования при различных парах значений многочленов λ и ρ. Действительно, выбор произвольного многочлена λ од-

нозначно определяет значение ρ, при котором 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 $C = (C_1, C_2, \ldots, C_i, \ldots, C_z)$ по фиктивному ключу $K = (K_1, K_2)$ выполняется следующим образом:

1. Каждый i-й ($i = 1, 2, \ldots, z$) 256-битовый блок $C_i = (C'_i, C''_i)$ расшифровать, выполнив следующие два шага:

1.1. Вычислить 128-битовый блок промежуточного шифртекста по формуле $C_{M_i} \equiv K_1 C'_i \oplus K_2 C''_i \bmod \eta(x)$;

1.2. Расшифровать 128-битовый блок C_{M_i} промежуточного шифртекста по ключу K, используя функцию блочного расшифровывания $D = E^{-1}$: $M_i = D_K(C_{M_i})$.

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

Секретное сообщение восстанавливается из шифртекста $C = (C_1, C_2, \ldots, C_z)$ по ключу $Q = (Q_1, Q_2)$ с использованием идентичного алгоритма:

1. Каждый 256-битовый блок $C_i = (C'_i, C''_i)$ расшифровать, выполнив следующие два шага:

1.1. Вычислить 128-битовый блок промежуточного шифртекста по формуле $C_{T_i} \equiv Q_1 C'_i \oplus Q_2 C''_i \bmod \eta$.

1.2. Расшифровать 128-битовый блок C_{T_i} промежуточного шифртекста по ключу Q, используя функцию блочного расшифровывания $D = E^{-1}$: $M_i = D_Q(C_{T_i})$.

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

5. Псевдовероятностные поточные шифры. Алгоритмы поточного шифрования представляют интерес для обеспечения защиты информации, передаваемой по открытым каналам связи [26, 27], поэтому значительный интерес представляет рассмотрение подходов к построению поточных ПВ шифров. В разделе 3 представлены алгоритмы блочного ПВ шифрования, в которых выполняется совместное преобразования двух сообщений. Если сообщения разбить на блоки данных малого размера (например, 4, 8 или 16 бит), рассматриваемых как знаки текста, то эти алгоритмы фактически будут задавать процесс поточного ПВ шифрования. Однако для получения высокого уровня

стойкости требуется решить задачу смены ключей шифрования при переходе от одного шифруемого знака к другому.

За счет смены ключей по псевдослучайному закону стойкое шифрование может быть обеспечено использованием достаточно простых операций при формировании знаков промежуточных шифртекстов. Данная идея детерминистического изменения ключей, используемых для шифрования пар знаков шифруемых сообщений, потенциально обеспечивает существенное повышение скорости шифрования по сравнению с алгоритмами поточного ПВ шифрования [15], в которых используется переборный механизм нахождения текущего знака шифртекста. Так же как и в случае поточных алгоритмов [15], для безопасного шифрования многих пар входных сообщений без изменения базовых секретных ключей K и Q требуется задать зависимость значений сменяемых ключей от несекретного вектора инициализации V, который направляется получателю вместе с шифртекстом.

Последовательно сменяемые ключи будем рассматривать как элементы ключевой гаммы. Пусть дана стойкая функция блочного шифрования E и требуется выполнить совместное шифрование сообщений $M = (m_1, m_2, \ldots, m_i, \ldots, m_z)$ и $T = (t_1, t_2, \ldots, t_i, \ldots, t_z)$, имеющих вид последовательности u-битовых знаков t_i и m_i. Шифрование сообщений M и T зададим, соответственно, по фиксированным секретным ключам K и Q, с помощью которых генерируются следующие две ключевые гаммы:

$$\Gamma = \{(\alpha_1, \beta_1), (\alpha_2, \beta_2), \ldots, (\alpha_i, \beta_i), \ldots, (\alpha_z, \beta_z)\} \text{ и}$$

$$\Gamma' = \{(\alpha'_1, \beta'_1), (\alpha'_2, \beta'_2), \ldots, (\alpha'_i, \beta'_i), \ldots, (\alpha'_z, \beta'_z)\},$$

элементами которых являются пары u-битовых ключевых знаков (α_i, β_i) и (α'_i, β'_i). Ключевые знаки α_i, β_i, α'_i и β'_i используются для совместного преобразования знаков m_i и t_i и вычисляются в зависимости от ключей K и Q, номера i и вектора инициализации V.

Процедуру генерации i-ых пар ключевых элементов (α_i, β_i) и (α'_i, β'_i) зададим следующем виде:

1. Вычислить пару u-битовых ключевых знаков $(\alpha_i, \beta_i) = E_K(V\|i) \bmod 2^{2u}$, где $\|$ — операция конкатенации (присоединения битовых строк); E — блочный шифр с входным блоком данных размером 128 бит и значения V и i задаются в виде 64-битовых строк.

2. Вычислить пару u-битовых ключевых знаков $(\alpha'_i, \beta'_i) = E_Q(V\|i) \bmod 2^{2u}$.

3. Присоединяя слева единичный бит к u-битовому знаку β_i, получить значение $\lambda = (1||\beta_i)$.

4. Добавляя слева единичный бит к u-битовому знаку β'_i, сформировать битовую строку $\eta = (1||\beta'_i)$. Если наибольший общий делитель НОД$(\eta, \lambda) \neq 1$, где битовые строки η и λ интерпретируются как двоичные многочлены, то модифицировать β'_i по формуле $\beta'_i \leftarrow (\beta'_i + 1) \bmod 2^u$, где битовая строка β'_i рассматривается как двоичное число, и вернуться к началу шага 4.

5. Взять пары ключевых знаков (α_i, β_i) и (α'_i, β'_i) в качестве i-ых элементов ключевых гамм Γ и Γ' соответственно.

Поточный алгоритм ПВ шифрования фиктивного сообщения M и секретного сообщения T описывается следующим образом:

1. Каждую i-ю ($i = 1, 2, \ldots, z$) пару знаков m_i и t_i входных сообщений преобразовать в $2u$-битовый знак c_i шифртекста, осуществляя следующие три шага:

1.1. Сгенерировать i-е элементы (α_i, β_i) и (α'_i, β'_i) ключевых гамм Γ и Γ' соответственно.

1.2. Сформировать двоичные многочлены λ и η степени u по формулам $\lambda = (1||\beta_i)$ и $\eta = (1||\beta'_i)$, где ключевые знаки β_i и β'_i трактуются как двоичные многочлены.

1.3. Вычислить $2u$-битовый знак c_i как решение следующей системы линейных сравнений:

$$\begin{cases} c_i \equiv \alpha'_i \oplus t_i \bmod \eta \\ c_i \equiv \alpha_i \oplus m_i \bmod \lambda \end{cases}, \tag{6}$$

где ключевые знаки α_i и α'_i и знаки исходных текстов m_i и t_i трактуются как двоичные многочлены, заданные в виде двоичного вектора. Шаг 4 процедуры генерации элементов ключевых гамм задает выполнимость условия взаимной неприводимости двоичных многочленов η и λ, поэтому система линейных сравнений (6) имеет единственное решение по модулю многочлена, равного произведению $\eta\lambda$, которое представляет собой многочлен, степень которого не превышает значения $2u - 1$, то есть битовую строку длины $2u$. Решение системы (6) находится по следующей формуле:

$$c_i = \left[(\alpha'_i \oplus t_i)\lambda\left(\lambda^{-1} \bmod \eta\right) \oplus (\alpha_i \oplus m_i)\eta\left(\eta^{-1} \bmod \lambda\right)\right] \bmod \eta(x)\lambda(x).$$

2. Объединяя все знаки c_i, сформировать выходной шифртекст $C = (c_1, c_2, \ldots, c_i, \ldots, c_z)$.

Ассоциируемый алгоритм вероятностного шифрования фиктивного сообщения M по фиктивному ключу K и вектору инициализации V выполняется следующим образом:

1. Каждый i-й ($i = 1, 2, \ldots, z$) знак m_i исходного текста M преобразовать в $2u$-битовый знак c_i криптограммы, выполнив следующие три шага:

1.1. Используя 128-битовый блочный шифр E, сгенерировать i-й элемент (α_i, β_i) ключевой гаммы Г по формуле $(\alpha_i, \beta_i) = E_K(V||i) \bmod 2^{2u}$.

1.2. Сгенерировать случайный многочлен ρ, степень которого не превышает значения $(u - 1)$, и случайный многочлен η степени u, такой, что НОД$(\eta, 1||\beta_i) = 1$, где битовая строка $1||\beta_i$ рассматривается как двоичный многочлен.

1.3. Вычислить $2u$-битовый знак c_i как решение следующей системы линейных сравнений:

$$\begin{cases} c_i \equiv \alpha_i \oplus m_i \bmod \lambda \\ c_i \equiv \rho \bmod \eta \end{cases},$$

где $\lambda = 1||\beta_i$.

2. Объединяя все знаки c_i, сформировать выходной шифртекст $C = (c_1, c_2, \ldots, c_i, \ldots, c_z)$.

Алгоритм расшифровывания фиктивного сообщения:

1. Каждый i-й ($i = 1, 2, \ldots, z$) $2u$-битовый знак c_i шифртекста преобразовать в i-й u-битовый знак m_i исходного сообщения M, выполнив следующие два шага:

1.1. Используя 128-битовый блочный шифр E, вычислить i-й элемент ключевой гаммы Г: $(\alpha_i, \beta_i) = E_K(V||i) \bmod 2^{2u}$.

1.2. Вычислить u-битовый знак m_i по формуле $m_i = c_i \oplus \alpha_i \bmod \lambda$, где $\lambda = 1||\beta_i$.

2. Объединяя все знаки m_i, сформировать восстановленное сообщение $M = (m_1, m_2, \ldots, m_i, \ldots, m_z)$.

Расшифровывание секретного сообщения T выполняется по такому же алгоритму с использованием секретного ключа Q:

1. Каждый i-й ($i = 1, 2, \ldots, z$) $2u$-битовый знак c_i шифртекста преобразовать в u-битовый знак t_i исходного сообщения T, выполнив следующие четыре шага:

1.1. Вычислить i-й элемент гаммы Γ': $(\alpha'_i, \beta'_i) = E_Q(V||i) \bmod 2^{2u}$.

1.2. Вычислить i-й элемент гаммы Γ: $(\alpha_i, \beta_i) = E_K(V||i) \bmod 2^{2u}$.

1.3. Если НОД$(1||\beta_i, 1||\beta'_i) \neq 1$, то модифицировать битовую строку β'_i по формуле $\beta'_i \leftarrow (\beta'_i + 1) \bmod 2^u$, где битовая строка β'_i рассматривается как двоичное число, и перейти в начало шага 1.3.

1.4. Вычислить u-битовый знак t_i по формуле $t_i = c_i \oplus \alpha'_i \bmod \eta$, где $\eta = 1||\beta'_i$.

2. Объединяя все знаки t_i, сформировать восстановленное сообщение $T = (t_1, t_2, \ldots, t_i, \ldots, t_z)$.

Сравнение двух последних алгоритмов показывает, что в рассмотренном поточном ПВ шифре не выполняется критерий идентичности алгоритмов расшифровывания криптограммы по фиктивному и секретному ключам, которому удовлетворяют поточные ПВ шифры [15]. Действительно, при восстановлении фиктивного сообщения генерируются только элементы ключевой гаммы Γ, а в случае восстановления секретного сообщения требуется вычислять элементы двух гамм Γ и Γ'. Это связано с тем, что на некоторых шагах процедуры зашифровывания входных знаков t_i и m_i осуществляется модифицирование ключевого знака β'_i (см. шаг 4 процедуры генерации) для реализации условия взаимной неприводимость модулей в системе линейных сравнений (6). При построении скоростных поточных ПВ шифров выполнимость указанного критерия остается открытой задачей.

6. Рандомизация блочных псевдовероятностных шифров. Представленные в разделе 3 блочные алгоритмы ПВ шифрования задают детерминистическое преобразование, поэтому наблюдение со стороны потенциального атакующего повторяющихся шифртекстов (случай выполнения повторного шифрования некоторых входных сообщений) даст ему возможность уличить в обмане отправителя и/или получателя сообщения, утверждающих в момент принуждающей атаки, что ими использовался алгоритм вероятностного шифрования. Для задания изменения шифртекста при повторном шифровании можно использовать рандомизацию процесса ПВ шифрования, то есть задать зависимость шифртекста от случайных значений.

Рандомизация блочных ПВ шифров может быть реализована путем добавления в систему линейных сравнений (линейных уравнений)

дополнительного сравнения (уравнения) со случайными коэффициентами. Это модифицирование схемы совместного шифрования фиктивного и секретного сообщений в целом сохраняет ее исходное построение. Изменения связаны с тем, что в алгоритме зашифровывания добавляется один дополнительный шаг — шаг генерации двух или трех случайных значений, а на шаге вычисления шифртекста решается система из трех сравнений (уравнений) вместо решения систем из двух линейных соотношений в случае детерминистических блочных ПВ шифров.

В случае ПВ шифра с использованием системы сравнений (3) соответствующая ему рандомизированная версия включает формирование блока шифртекста в виде решения следующей системы:

$$\begin{cases} C_i \equiv C_{T_i} \bmod \eta_1 \\ C_i \equiv C_{M_i} \bmod \eta_2 \\ C_i \equiv \lambda \bmod \rho \end{cases},$$

где λ и ρ — случайные двоичные многочлены, такие что ρ является взаимно неприводимым с многочленами η_1 и η_2, а степень λ меньше степени ρ. Размер блока шифртекста увеличивается на число битов, равное степени многочлена ρ.

В случае ПВ шифра с использованием системы уравнений (4) соответствующая ему рандомизированная версия включает формирование блока выходного шифртекста в виде решения следующей системы уравнений:

$$\begin{cases} K_1 C_i' \oplus K_2 C_i'' \oplus K_3 C_i''' \equiv C_{T_i} \bmod \eta \\ Q_1 C_i' \oplus Q_2 C'' \oplus Q_3 C_i''' \equiv C_{M_i} \bmod \eta \\ \lambda_1 C_i' \oplus \lambda_2 C_i'' \oplus C''' \equiv \rho \bmod \eta \end{cases},$$

где λ_1, λ_2 и ρ — случайные двоичные многочлены, степень которых меньше степени η; ключи K и Q имеют вид $K = (K_1, K_2, K_3)$ и $Q = (Q_1, Q_2, Q_3)$. Блок шифртекста имеет вид $C = (C_1, C_2, C_3)$ и его длина увеличивается на число битов, равное степени многочлена η.

7. Псевдовероятностный протокол бесключевого шифрования. Функции коммутативного шифрования (коммутативные шифры) лежат в основе протоколов бесключевого шифрования, которые решают задачу передачи секретного сообщения по открытому каналу связи без выполнения процедуры обмена ключами между получателем и отправителем сообщения. Участники сеанса связи выполняют проце-

дуры коммутативного зашифровывания и расшифровывания по локальным ключам, которые они выбирают произвольным образом без согласования с другой стороной.

При использовании коммутативного шифра, стойкого к атаке на основе известного исходного текста, протоколы бесключевого шифрования при соответствующем выборе параметров алгоритма коммутативного шифрования обеспечивают произвольную наперед заданную стойкость к атакам со стороны пассивного нарушителя. Протоколы данного типа обеспечивают секретность, но не аутентификацию отправителя и получателя сообщения, поэтому они не могут применяться в условиях потенциальной возможности активных атак, когда атакующий может навязать пользователям ложный сеанс секретной связи.

При рассмотрении протоколов ОШ, как правило, оценивается стойкость к принуждающим атакам со стороны пассивного нарушителя. В рамках модели пассивных принуждающих атак, представляет интерес задача построения бесключевого протокола ОШ, то есть протокола безопасной передачи секретного сообщения T по открытому каналу, где не используются предварительно распределенные по защищенным каналам секретные ключи или открытые ключи, подлинность которых подтверждена до осуществления сеанса передачи секретного сообщения.

Построение протокола бесключевого ОШ может быть выполнено в виде схемы ПВ бесключевого шифрования, в которой формируемые шифртексты вычислительно неотличимы от шифртекстов, формируемых в процессе вероятностного бесключевого шифрования. При таком подходе требуется разработать протокол вероятностного шифрования по локальным ключам, который будет ассоциироваться с протоколом ПВ бесключевого шифрования.

Задача построения вероятностного протокола бесключевого шифрования может быть решена путем включения в протокол этапа согласования разового общего секретного ключа, реализуемого в соответствии с широко известной схемой Диффи — Хеллмана. На данном этапе пользователи обмениваются разовыми открытыми ключами, по которым каждый из них может вычислить одно и то же секретное значение Z. Используя данный параметр участники протокола выполняют вероятностное шифрование данных, подлежащих передаче другой стороне на текущем шаге протокола. Поскольку обе стороны знают значение Z, то каждая из них может правильно восстановить направляемые ей сообщения.

Представленная обобщенная схема вероятностного бесключевого шифрования преобразуется в протокол ПВ бесключевого шифрова-

ния путем выполнения дополнительной процедуры зашифровывания и расшифровывания некоторого второго (фиктивного) сообщения M с использованием дополнительных локальных ключей. При этом локальные ключи для шифрования сообщений M и T являются независимыми друг от друга, а шифр тексты, полученные в результате шифрования секретного сообщения T, используются как случайные значения в протоколе вероятностного бесключевого шифрования.

В случае принуждения отправителя и получателя к раскрытию переданных в ходе сеанса связи сообщения и локальных ключей каждый из них раскрывает свой дополнительный локальный ключ и фиктивное сообщение. При этом они заявляют, что в ходе сеанса передачи сообщения M ими использовался протокол вероятностного бесключевого шифрования. Имея в наличии раскрытые параметры, атакующему вычислительно невозможно доказательно опровергнуть последнее утверждение.

В качестве коммутативной функции шифрования целесообразно использовать экспоненциальный шифр, в котором процедуры зашифровывания и расшифровывания представляют собой операцию возведения в степени e и d по простому модулю p достаточно большой разрядности. Зашифровывание сообщения $M < p$ состоит в вычислении шифртекста $C = M^e \bmod p$, и для правильного расшифровывания значения C используется значение ключа расшифровывания d, удовлетворяющее условию $ed = 1 \bmod p - 1$, благодаря чему выполняется равенство $M = C^d \bmod p$, которое справедливо для любого исходного значения $M < p$.

Пусть удаленный пользователь А желает послать секретное сообщение $T < p$ удаленному пользователю В, используя протокол бесключевого шифрования таким образом, что в случае принуждающей атаки, осуществляемой пассивным атакующим после перехвата всех значений, переданных по каналу связи, пользователи могут раскрыть локальные ключи K_A и K_B, сохраняя секретность сообщения T. Для решения этой задачи может быть использован способ шифрования, описываемый в обобщенном виде следующим образом.

1. В соответствии с криптосхемой Диффи — Хеллмана пользователи генерируют сеансовые (разовые) открытые ключи, обмениваются ими и вычисляют разовый (действующий в рамках текущего сеанса связи) общий секретный ключ Z.

2. Пользователь А генерирует фиктивное сообщение $M < p$.

3. Пользователи А и В выполняют процедуру ПВ бесключевого шифрования сообщений T и M одновременно, причем каждый из пользователей использует различные локальные ключи для шифрования сообщений T и M.

При этом формируемые в ходе процедуры бесключевого шифрования шифртексты, которые передаются по открытому каналу, вычислительно неотличимы от шифртекстов, получаемых в ходе вероятностного бесключевого шифрования фиктивного сообщения *M*. Наличие такого вероятностного протокола позволяет пользователям в случае принуждающей атаки раскрыть только локальные ключи, использованные для преобразования фиктивного сообщения. Атакующему вычислительно невозможно уличить пользователей в обмане, поскольку перехваченные им шифртексты могли быть на самом деле получены путем шифрования сообщения *M* по предоставленным ему локальным ключам при определенных значениях случайных параметров вероятностного коммутативного шифрования.

Рассмотрим конкретную реализацию протокола вероятностного бесключевого шифрования сообщения $T < p$:

1. Пользователь A генерирует случайное значение $k_A < p - 1$, играющее роль его разового личного секретного ключа, вычисляет свой разовый открытый ключ $R_A = \alpha^{k_A} \bmod p$ и направляет значение R_A пользователю B.

2. Пользователь B генерирует случайное значение $k_B < p - 1$, играющее роль его разового личного секретного ключа, вычисляет свой разовый открытый ключ $R_B = \alpha^{k_B} \bmod p$ и направляет значение R_B пользователю A.

3. Пользователь A генерирует локальный ключ $K_A = (e_A, d_A)$, где $d_A = e_A^{-1} \bmod p - 1$, вычисляет разовый общий секрет $Z = R_B^{k_A} \bmod p$, генерирует случайное значение ρ_1 и вычисляет шифртекст $C_1 = (C'_1, C''_1)$ как решение следующей системы линейных уравнений относительно неизвестных C'_1 и C''_1:

$$\begin{cases} C'_1 + C''_1 = \rho_1 \bmod p, \\ C'_1 + ZC''_1 = T^{e_A} \bmod p. \end{cases}$$

Затем A направляет шифртекст C_1 пользователю B.

4. Пользователь B генерирует локальный ключ $K_B = (e_B, d_B)$, где $d_B = e_B^{-1} \bmod p - 1$, вычисляет разовый общий секрет $Z = R_A^{k_B} \bmod p$ и значение $S_1 = M^{e_A} \bmod p = \left(C'_1 + ZC''_1\right) \bmod p$, генерирует случайное

значение ρ_2 и вычисляет шифртекст $C_2 = (C'_2, C''_2)$ как решение следующей системы уравнений относительно неизвестных C'_2 и C''_2:

$$\begin{cases} C'_2 + C''_2 = \rho_2 \bmod p, \\ C'_2 + ZC''_2 = S_1^{e_B} \bmod p. \end{cases}$$

Затем B направляет шифртекст C_2 пользователю A.

5. Пользователь A генерирует случайное значение ρ_3, вычисляет значение $S_2 \equiv S_1^{e_B} \equiv \left(C'_2 + ZC''_2\right) \bmod p$ и шифртекст $C_3 = (C'_3, C''_3)$ как решение следующей системы уравнений относительно неизвестных C'_3 и C''_3:

$$\begin{cases} C'_3 + C''_3 = \rho_3 \bmod p \\ C'_3 + ZC''_3 = S_2^{e_A} \bmod p \end{cases}.$$

Затем A направляет шифртекст C_3 пользователю B. Получив значение C_3, пользователь B вычисляет сообщение T:

$$T = \left(C'_3 + ZC''_3\right)^{d_B} \bmod p.$$

С учетом описанного конкретного протокола вероятностного бесключевого шифрования легко составить следующий конкретный протокол ПВ бесключевого шифрования, обеспечивающий секретность сообщения $T < p$ в случае пассивной принуждающей атаки:

1. Отправитель сообщения T генерирует случайный разовый секретный ключ k_A, вычисляет свой разовый открытый ключ $R_A = \alpha^{k_A} \bmod p$ и направляет R_A получателю.

2. Получатель генерирует случайный секретный ключ k_B, вычисляет свой разовый открытый ключ $R_B = \alpha^{k_B} \bmod p$ и направляет значение R_B пользователю A.

3. Отправитель генерирует локальные ключи $K_A = (e_A, d_A)$, где $d_A = e_A^{-1} \bmod p - 1$ и $Q_A = (\varepsilon_A, \delta_A)$, где $\delta_A = \varepsilon_A^{-1} \bmod p - 1$, вычисляет разовый общий секрет $Z = R_B^{k_A} \bmod p$, формирует фиктивное сообщение $M < p$ и вычисляет шифртекст $C_1 = (C'_1, C''_1)$ как решение следующей системы уравнений относительно неизвестных C'_1 и C''_1:

$$\begin{cases} C_1' + Z^2 C_1'' = T^{\varepsilon_A} \bmod p, \\ C_1' + Z C_1'' \quad = M^{e_A} \bmod p. \end{cases}$$

Затем отправитель направляет шифртекст C_1 получателю.

4. Получатель генерирует локальные ключи $K_B = (e_B, d_B)$, где $d_B = e_B^{-1} \bmod p-1$, и $Q_B = (\varepsilon_B, \delta_B)$, где $\delta_B = \varepsilon_B^{-1} \bmod p-1$, вычисляет разовый секрет $Z = R_A^{k_B} \bmod p$, значения $S_1 \equiv M^{e_A} \equiv \left(C_1' + ZC_1''\right) \bmod p$ и $U_1 \equiv T^{\varepsilon_{\mathbf{A}}} \equiv \left(C_1' + Z^2 C_1''\right) \bmod p$. После этого он вычисляет шифртекст $C_2 = (C'_2, C''_2)$ как решение следующей системы уравнений относительно неизвестных C'_2 и C''_2:

$$\begin{cases} C_2' + Z^2 C_2'' = U_1^{\varepsilon_B} \bmod p, \\ C_2' + ZC_2'' \quad = S_1^{e_B} \bmod p. \end{cases}$$

Затем получатель направляет шифртекст C_2 отправителю.

5. По полученному шифртексту C_2 отправитель вычисляет значения $S_2 \equiv S_1^{e_B} \equiv \left(C_2' + ZC_2''\right) \bmod p$ и $U_2 \equiv U_1^{\varepsilon_B} \equiv \left(C_2' + Z^2 C_2''\right) \bmod p$ и шифртекст $C_3 = (C'_3, C''_3)$ как решение следующей системы уравнений относительно неизвестных C'_3 и C''_3:

$$\begin{cases} C_3' + Z^2 C_3'' = U_2^{\delta_A} \bmod p, \\ C_3' + ZC_3'' \quad = S_2^{e_A} \bmod p. \end{cases}$$

Значение C_3 направляется получателю.

По шифртексту C_3 получатель вычисляет сообщения T и M:

$$T = \left(C_3' + Z^2 C_3''\right)^{\delta_B} \bmod p; \quad M = \left(C_3' + ZC_3''\right)^{d_B} \bmod p.$$

Доказательство корректности протокола ПВ бесключевго шифрования состоит в том, что устанавливается справедливость следующих двух соотношений.

1. Восстановление секретного сообщения:

$$\left(C_3' + Z^2 C_3''\right)^{\delta_B} \equiv \left(U_2^{\delta_A}\right)^{\delta_B} \equiv \left(U_1^{\varepsilon_B}\right)^{\delta_A \delta_B} \equiv \left(T^{\varepsilon_A}\right)^{\varepsilon_B \delta_A \delta_B} \equiv T \bmod p.$$

2. Восстановление фиктивного сообщения:

$$\left(C_3' + ZC_3''\right)^{d_B} \equiv \left(S_2^{d_A}\right)^{d_B} \equiv \left(S_1^{e_B}\right)^{d_A d_B} \equiv \left(M^{e_A}\right)^{e_B d_A d_B} \equiv M \bmod p.$$

Подвергаясь принудительной атаке, отправитель и получатель сообщения раскрывают фиктивное сообщение M и ключи k_A, R_A, k_B, R_B, Z, (e_A, d_A) и (e_B, d_B). При этом они заявляют, что для передачи сообщения M они использовали протокол вероятностного бесключевого шифрования. Благодаря наличию такого протокола, ассоциируемого с протоколом бесключевого ОШ, атакующий не имеет практической возможности уличить в обмане хотя бы одну из сторон сеанса защищенной передачи секретного сообщения. Действительно, в рамках ассоциированного протокола раскрытые параметры корректно связаны со всеми значениями, переданными по открытому каналу связи.

Для того чтобы показать отличие значений $\rho_i = \left(C_i' + C_i''\right) \bmod p$ $(i = 1, 2, 3)$ от случайных, требуется вычислить один из локальных ключей Q_A и Q_B, что позволит атакующему восстановить сообщение T. Однако для этого нужно решить задачу дискретного логарифмирования по простому модулю p, который выбирается таким, что решение этой вычислительной задачи является практически неосуществимым.

Таким образом, в описанном протоколе выполнено требование вычислительной неотличимости по шифртексту процедуры ОШ от процедуры вероятностного шифрования, то есть он действительно может быть отнесен к протоколам ПВ шифрования. Построенный протокол вероятностного бесключевого шифрования, ассоциированный с разработанным протоколом, имеет также самостоятельное значение в случаях, когда требуется обеспечить достаточную стойкость к атакам на основе специально подобранных текстов.

Бесключевые протоколы различного типа обеспечивают безопасную передачу сообщений по открытым каналам относительно атак пассивного нарушителя. В случаях, когда требуется обеспечить стойкость к принуждающим атакам со стороны активного нарушителя, выдающего себя за отправителя или получателя секретного сообщения, описанный протокол должен быть дополнен механизмами проверки аутентичности передаваемых в ходе протокола разовых открытых ключей и шифртекстов.

8. Заключение. На основе обобщения результатов в области разработки алгоритмов ПВ шифрования выделены общие приемы их построения и рассмотрены особенности реализации механизмов защи-

ты информации с использованием ПВ шифров. Предложены новые алгоритмы симметричного ПВ шифрования, обладающие существенно более высокой производительностью по сравнению с известными в литературе аналогами, и общий подход к рандомизации ПВ шифров, позволяющей расширить класс ПВ шифров и обеспечивающей повышение стойкости к принуждающим атакам. Показано, что критерий неотличимости по шифртексту от вероятностного шифрования может быть использован также и для построения протоколов бесключевого ПВ шифрования, не требующий наличия у участников протокола заранее согласованных ключей.

Дальнейшее развитие данного направления прикладной криптографии, относящейся к разработке и анализу ПВ шифров, связано с разработкой новых способов алгоритмического задания функций взаимно-однозначного отображения пар блоков промежуточных шифртекстов в блоки выходного шифртекста, включая случай разбиения фиктивного и секретного сообщений на блоки различного размера. Для приложений в области защиты информации также представляет интерес разработка коммутативных ПВ шифров и протоколов бесключевого ПВ шифрования, основанных на вычислительной трудности задачи дискретного логарифмирования на эллиптической кривой.

Литература

1. *Жуков К.Д.* Обзор атак на AES-128: к пятнадцатилетию стандарта AES // Прикладная дискретная математика. 2017. № 35. С. 48–62.
2. *Sirwan A., Majeed N.* New Algorithm for Wireless Network Communication Security // International Journal on Cryptography and Information Security. 2016. vol. 6. no. 3/4. pp. 1–8.
3. *Agievich S.V.* EHE: nonce misuse-resistant message authentication // Прикладная дискретная математика. 2018. № 39. С. 33–41.
4. *Nikolaev M.V.* On the complexity of two-dimensional discrete logarithm problem in a finite cyclic group with efficient automorphism // Математические вопросы криптографии. 2015. Т. 6. № 2. С. 45–57.
5. *Алексеев Е.К., Ошкин И.Б., Попов В.О., Смышляев С.В.* О криптографических свойствах алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 // Математические вопросы криптографии. 2016. Т. 7. № 1. С. 5–38.
6. *Николаев В.Д.* Атаки на схемы электронной подписи, не учитываемые традиционными определениями стойкости, и меры противодействия им // Математические вопросы криптографии. 2016. Т. 7. № 1. С. 93–118.
7. *Verma G.K.* A Proxy Blind Signature Scheme over Braid Groups // International Journal of Network Security. 2009. vol. 9. no 3. pp. 214–217.
8. *Canetti R.*, *Dwork C.*, *Naor M.*, *Ostrovsky R.* Deniable Encryption // Annual International Cryptology Conference. 1997. vol. 1294. pp. 90–104.
9. *Ibrahim M.H.* A Method for Obtaining Deniable Public-Key Encryption // International J. of Network security. 2009. vol. 8. no 1. pp. 1–9.
10. *Dachman-Soled D.* On minimal assumptions for sender-deniable public key encryption // International Workshop on Public Key Cryptography. 2014. vol. 8383. pp. 574–591.

11. *Asif A.M.A.M., Hannan S.* A Review on Classical and Modern Encryption Techniques // International Journal of Engineering Trends and Technology. 2014. vol. 12. no. 4. pp. 199–203.
12. *Ishai Yu. et al.* Efficient non-interactive secure computation // Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2011. vol. 6632. pp. 406–425.
13. *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 // Journal of Networks. 2009. vol. 4. pp. 370–377.
14. *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. no. 9. pp. 3231–3249.
15. *Moldovyan N.A. et al.* Deniability of Symmetric Encryption Based on Computational Indistinguishability from Probabilistic Ciphering // Information Systems Design and Intelligent Applications. 2018. vol. 672. pp. 209–218.
16. *Hong X., Wang B.* A Non-interactive Deniable Authentication Scheme in the Standard Model // Journal of Electrical and Electronic Engineering. 2017. vol. 5. no. 2. pp. 80–85.
17. *Yoon E.J.* Security Analysis of Kar's ID-based Deniable Authentication Protocol // Contemporary Engineering Sciences. 2015. vol. 8. no. 17 pp. 765–771.
18. *Hata M.M., Ali F.H.M., Aljunid S.A.* Secret Sharing Deniable Encryption Technique // International Conference on Information Science and Applications. 2017. vol. 424. pp. 347–357.
19. *Amrutiya V., Baskaran A., Iyengar N.* Deniable Encryption using One Time Pads // Proceedings of the International Conference on Advances in Information Communication Technology & Computing. 2016. 49 p.
20. *Talouki M.A., Dastjerdi A.B.* Anonymous electronic voting protocol with deniable authentication for mobile ad hoc networks // International journal of Multimedia and Unbiquitous Engineering. 2014. vol. 9. no. 1. pp. 361–366.
21. *Moldovyan N.A. et al.* Pseudo-probabilistic block ciphers and their randomization // Journal of Ambient Intelligence and Humanized Computing. 2018. pp. 1–8.
22. *Wang C., Wang J.* A shared-key and receiver-deniable encryption scheme over lattice // Journal of Computational Information Systems. 2012. vol. 8. no. 2. pp. 747–753.
23. *O'Neil A., Peikert C., Waters B.* Bi-deniable public-key encryption // Annual Cryptology Conference. 2011. vol. 6841. pp. 525–542.
24. *Moldovyan N.A., Shcherbacov A.V., Eremeev M.A.* Deniable-encryption protocols based on commutative ciphers // Quasigroups and related systems. 2017. vol. 25. no. 1. pp. 95–108.
25. *Zou M.H. et al.* Scan-based attack on stream ciphers: A case study on eSTREAM finalists // Computer science and technology. 2014. vol. 29. pp. 646–655.
26. *Hwang T., Gope P.* Robust stream-cipher mode of authenticated encryption for secure communication in wireless sensor network // Security and communication networks. 2016. pp. 667-679.

Молдовян Александр Андреевич — д-р техн. наук, профессор, главный научный сотрудник лаборатории безопасности информационных систем, Федеральное государственное бюджетное учреждение науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: компьютерная безопасность, криптография, безопасность компьютерных сетей, управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома. Число научных публикаций —

200. maa1305@yandex.ru; 14-я линия В.О., 39, Санкт-Петербург, 199178; р.т.: +7(812)328–5185.

Молдовян Николай Андреевич — д-р техн. наук, профессор, главный научный сотрудник лаборатории безопасности информационных систем, Федеральное государственное бюджетное учреждение науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: компьютерная безопасность, криптография, симметричные и асимметричные криптосистемы, электронная цифровая подпись, аутентификация, блочные шифры, псевдовероятностные шифры. Число научных публикаций — 250. nmold@mail.ru; 14-я линия В.О., 39, Санкт-Петербург, 199178; р.т.: +7(812)328–5185.

Поддержка исследований. Работа выполнена при финансовой поддержке РФФИ (проект № 18-57-54002-Вьет_а).

DOI 10.15622/sp.61.5

A.A. MOLDOVYAN, N.A. MOLDOVYAN

METHODS AND ALGORITHMS FOR PSEUDO-PROBABILISTIC ENCRYPTION WITH SHARED KEY

Moldovyan A.A., Moldovyan N.A. **Methods and Algorithms for Pseudo-Probabilistic Encryption with Shared Key.**

Abstract. As a method for providing security of the messages sent via a public channel in the case of potential coercive attacks there had been proposed algorithms and protocols of deniable encryption. The lasts are divided on the following types: 1) schemes with public key, 2) schemes with shares secret key, and 3) no-key schemes. There are introduced pseudo-probabilistic symmetric ciphers that represent a particular variant of implementing deniable encryption algorithms. It is discussed application of the pseudo-probabilistic encryption for constructing special mechanisms of the information protection including steganographic channels hidden in ciphertexts. There are considered methods for designing stream and block pseudo-probabilistic encryption algorithms that implement simultaneous ciphering fake and secret messages so that the generated ciphertext is computationally indistinguishable from the ciphertext obtained as output of the probabilistic encryption of the fake message. The requirement of the ciphertext indistinguishability from the probabilistic encryption has been used as one of the design criteria. To implement this criterion in the construction scheme of the pseudo-probabilistic ciphers it is included step of bijective mapping pairs of intermediate ciphertext blocks of the fake and secret messages into a single expanded block of the output ciphertext. Implementations of the pseudo-probabilistic block ciphers in which algorithms for recovering the fake and secret messages coincide completely are also considered. There are proposed general approaches to constructing no-key encryption protocols and randomized pseudo-probabilistic block ciphers. Concrete implementations of the cryptoschemes of such types are presented.

Keywords: cryptography, deniable encryption, pseudo-probabilistic encryption, block cipher, stream cipher, fake message, randomization of ciphers, no-key encryption.

Moldovyan Alexandr Andreevich — Ph.D., Dr. Sci., professor, chief researcher of laboratory of information systems security, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS). Research interests: computer security, cryptography, network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems. The number of publications — 200. maa1305@yandex.ru; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328–5185.

Moldovyan Nikolay Andreevich — Ph.D., Dr. Sci., professor, chief researcher of laboratory of information systems security, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS). Research interests: computer security, cryptography, symmetric and asymmetric cryptosystems, digital signature, authentication, block ciphers, pseudo-probabilistic ciphers. The number of publications — 250. nmold@mail.ru; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7-812-328-5185.

Acknowledgements. This research is supported by the Russian Foundation for Basic Research (project No. 18-57-54002-Viet_a).

References

1. Zhukov K.D. [Review of attacks on AES-128: by the fifteenth anniversary of the AES standard]. *Prikladnaya diskretnaya matematika – Applied discrete mathematics*. 2017. vol. 35. pp. 48–62. (In Russ.).
2. Sirwan A., Majeed N. New Algorithm for Wireless Network Communication Security. *International Journal on Cryptography and Information Security*. 2016. vol. 6. no. 3/4. pp. 1–8.
3. Agievich S.V. [EHE: nonce misuse-resistant message authentication]. *Prikladnaya diskretnaya matematika – Applied discrete mathematics*. 2018. vol. 39. pp. 33–41.
4. Nikolaev M.V. [On the complexity of two-dimensional discrete logarithm problem in a finite cyclic group with efficient automorphism]. *Matematicheskie voprosy kriptografii – Mathematical items of cryptography*. 2015. Issue 6. vol. 2. pp. 45–57.
5. Alexeev E.K., Oshkin I.B., Popov V.O., Smyshlyaev S.V. [On the cryptographic properties of algorithms that accompany the application of standards GOST R 34.11–2012 and GOST R 34.10–2012]. *Matematicheskie voprosy kriptografii – Mathematical items of cryptography*. 2016. Issue 7. vol. 1. pp. 5–38. (In Russ.).
6. Nikolaev V.D. [Attacks on digital signature schemes, which are not taken into account by traditional security definitions, and countermeasures against them]. *Matematicheskie voprosy kriptografii – Mathematical items of cryptography*. 2016. Issue 7. vol. 1. pp. 93–118. (In Russ.).
7. Verma G.K. A Proxy Blind Signature Scheme over Braid Groups. *International Journal of Network Security*. 2009. vol. 9. no. 3. pp. 214−217.
8. Canetti R., Dwork C., Naor M., Ostrovsky R. Deniable Encryption. Annual International Cryptology Conference. 1997. vol. 1294. pp. 90–104.
9. Ibrahim M.H. A Method for Obtaining Deniable Public-Key Encryption. *International J. of Network security*. 2009. vol. 8. no. 1. pp. 1–9.
10. Dachman-Soled D. On minimal assumptions for sender-deniable public key encryption. International Workshop on Public Key Cryptography. 2014. vol. 8383. pp. 574–591.
11. Asif A.M.A.M., Hannan S. A Review on Classical and Modern Encryption Techniques. *International Journal of Engineering Trends and Technology*. 2014. vol. 12. no. 4. pp. 199–203.
12. Ishai Yu. et al. Efficient non-interactive secure computation. Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2011. vol. 6632. pp. 406–425.
13. 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. *Journal of Networks*. 2009. vol. 4. pp. 370–377.
14. 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. no. 9. pp. 3231–3249.
15. Moldovyan N.A. et al. Deniability of Symmetric Encryption Based on Computational Indistinguishability from Probabilistic Ciphering. Information Systems Design and Intelligent Applications. 2018. vol. 672. pp. 209–218.
16. Hong X., Wang B. A Non-interactive Deniable Authentication Scheme in the Standard Model. *Journal of Electrical and Electronic Engineering*. 2017. vol. 5. no. 2. pp. 80–85.
17. Yoon E.J. Security Analysis of Kar's ID-based Deniable Authentication Protocol. *Contemporary Engineering Sciences*. 2015. vol. 8. no. 17. pp. 765–771.
18. Hata M.M., Ali F.H.M., Aljunid S.A. Secret Sharing Deniable Encryption Technique. International Conference on Information Science and Applications. Springer. 2017. vol. 424. pp. 347–357.

19. Amrutiya V., Baskaran A., Iyengar N. Deniable Encryption using One Time Pads. Proceedings of the International Conference on Advances in Information Communication Technology & Computing. 2016. 49 p.
20. Talouki M.A., Dastjerdi A.B. Anonymous electronic voting protocol with deniable authentication for mobile ad hoc networks. *International journal of Multimedia and Unbiquitous Engineering*. 2014. vol. 9. no. 1. pp. 361–366.
21. Moldovyan N.A. et al. Pseudo-probabilistic block ciphers and their randomization. *Journal of Ambient Intelligence and Humanized Computing*. 2018. pp. 1–8.
22. Wang C., Wang J. A shared-key and receiver-deniable encryption scheme over lattice. *Journal of Computational Information Systems*. 2012. vol. 8. no. 2. pp. 747–753.
23. O'Neil A., Peikert C., Waters B. Bi-deniable public-key encryption. Annual Cryptology Conference. 2011. vol. 6841. pp. 525–542.
24. Moldovyan N.A., Shcherbacov A.V., Eremeev M.A. Deniable-encryption protocols based on commutative ciphers. *Quasigroups and related systems*. 2017. vol. 25. no. 1. pp. 95–108.
25. Zou M.H. et al. Scan-based attack on stream ciphers: A case study on eSTREAM finalists. *Computer science and technology*. 2014. vol. 29. pp. 646–655.
26. Hwang T., Gope P. Robust stream-cipher mode of authenticated encryption for secure communication in wireless sensor network. *Security and communication networks*. 2016. pp. 667–679.