УДК 681.3

СПОСОБЫ ОТРИЦАЕМОГО ШИФРОВАНИЯ С РАЗДЕЛЯЕМЫМ КЛЮЧОМ

Е. В. Морозова,
канд. техн. наук, ученый секретарь НТС
НИИ «Вектор», г. Санкт-Петербург
Я. А. Мондикова,
аспирант
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
Н. А. Молдовян,
доктор техн. наук, заведующий лабораторией
Санкт-Петербургский институт информатики и автоматизации РАН

Предложены критерии построения алгоритмов отрицаемого шифрования для реализации механизмов защиты информации типа обманных ловушек и представлены разработанные алгоритмы данного типа. Новыми реализованными требованиями являются неотличимость от вероятностного шифрования и идентичность процедуры расшифрования и использования всех битов криптограммы для всех возможных значений ключа. Предложенные способы отрицаемого шифрования обеспечивают высокую производительность и перспективны для расширения арсенала криптографических механизмов защиты информации, используемых в комплексных системах компьютерной безопасности.

Ключевые слова *— компьютерная безопасность, криптография, отрицаемое шифрование, хэш-функции, блочные шифры, вероятностное шифрование, криптограмма.*

Введение

Понятие отрицаемого шифрования (ОШ) [1] связывается с задачей обеспечения стойкости шифрования информации в условиях возможности так называемых атак с принуждением. Данные виды атак подразумевают наличие у атакующего таких ресурсов воздействия на отправителя и (или) получателя сообщений, которые вынуждают отправителя и (или) получателя раскрыть параметры процесса зашифрования (принуждающая атака на отправителя сообщения) или расшифрования (принуждающая атака на получателя сообщения), например, ключ шифрования и случайные значения, использованные в процессе шифрования. Если предполагается, что атакующий может потребовать предоставления ему параметров как зашифрования, так и расшифрования, то имеет место двухсторонняя принуждающая атака. Стойкость к таким атакам обеспечивается алгоритмами и протоколами ОШ тем, что выходной шифртекст (криптограмма) может быть получен из различных осмысленных исходных сообщений и (или) из криптограммы могут быть получены различные расшифрованные осмысленные тексты. Атакующему передаются параметры шифрования, которые связывают криптограмму с некоторым фиктивным осмысленным текстом. Атакующий проверяет то, что использование предоставленных ему параметров шифрования действительно приводит к преобразованию фиктивного сообщения в заданную криптограмму и (или) к расшифрованию последней в фиктивное сообщение. Если результат проверки является положительным и атакующий не может доказать неполноту раскрытого текста, то алгоритм (протокол) ОШ считается стойким.

В известной литературе основное внимание исследователей направлено на способы ОШ, относящиеся к криптосхемам с открытым ключом. Такие способы основаны на использовании алгоритмов открытого шифрования или протоколов открытого распределения ключей [2—4]. При этом предполагается, что отправитель и получатель не имеют общей секретной информации (разделяемого секретного ключа), а восстановление фиктивного/настоящего сообщения зависит от применяемых случайных значений.

Интерес к алгоритмам и протоколам ОШ связан с перспективами их применения в защищенных распределенных вычислениях и системах тайного электронного голосования [5, 6]. Одно из ограничений практического использования процедур ОШ состоит в их низкой производительности, особенно характерной для криптосхем с открытым ключом. Поиск новых алгоритмов и протоколов ОШ привел к разработке более производительных способов ОШ [7, 8], однако практика требует дальнейшего повышения скорости работы криптоалгоритмов, особенно в случаях применения способов ОШ как специального механизма защиты информации в комплексных средствах компьютерной безопасности, основанного на обманных ловушках [9].

В отличие от схем ОШ на основе асимметричных алгоритмов шифрования, ОШ, основанное на схемах с разделяемым ключом, подразумевает наличие общего секрета (общего секретного ключа), позволяющего восстановить настоящее сообщение, как у отправителя, так и у получателя. В данной работе решается задача разработки производительных алгоритмов отрицаемого шифрования при одновременном обеспечении высокой стойкости к двухсторонней атаке с принуждением на основе ОШ с разделяемым секретом. Сочетание производительности и стойкости снимает существенные ограничения к практическому применению алгоритмов ОШ для защиты информации в средствах обеспечения информационной безопасности. При этом формулируются специальные требования к алгоритмам ОШ, связанные с использованием ОШ для реализации механизмов защиты типа обманных ловушек. Предложенные новые требования не удовлетворяются известными в литературе алгоритмами ОШ с разделяемым секретом [1].

Требования к алгоритмам отрицаемого шифрования с разделяемым секретом

Реализация механизмов защиты информации типа обманных ловушек основана на использовании способов ОШ, обеспечивающих возможность достаточно быстрого совместного зашифрования двух или более различных сообщений на двух или более различных ключах конечной длины. Одно из сообщений является фиктивным и зашифровывается на фиктивном секретном ключе, к которому организуется контролируемый доступ со стороны нарушителя. При расшифровании соответствующим образом составленного фиктивного сообщения нарушитель оказывается введенным в заблуждение (дезинформированным). Однако следует предполагать, что нарушитель знает алгоритм расшифрования, используемый санкционированным пользователем, и может проанализировать криптограмму и ее применение при выполнении процедуры расшифрования по фиктивному ключу. Это не должно дать ему обоснованных подозрений, что кроме полученного им фиктивного ключа имеется еще и другой ключ, расшифровывающий криптограмму в другое осмысленное сообщение. Другими словами, алгоритм ОШ должен обладать такими свойствами, которые не позволят атакующему отличить ОШ от вероятностного шифрования по криптограмме, по фиктивному сообщению и фиктивному ключу. Это определяет следующие требования к алгоритмам ОШ:

1) неотличимость по криптограмме от вероятностного шифрования;

2) одинаковость процедур расшифрования для различных используемых ключей;

3) равноправность (идентичность использования) всех битов криптограммы для всех возможных значений ключа расшифрования.

Эти требования накладываются на требование использовать ключи конечного размера и обеспечивать достаточно высокую производительность. Они фактически являются продолжением принципа Керхкоффа, сформулированного для симметричных алгоритмов шифрования: шифр должен быть стойким при условии, что все детали процедуры шифрования известны атакующему. Для алгоритмов ОШ этот принцип разумно дополнить требованиями вычислительной неотличимости от вероятностного алгоритма шифрования при известной процедуре расшифрования и известной криптограмме. Смысл этого расширения принципа Керхкоффа состоит в том, чтобы атакующий не смог обоснованно утверждать (подозревать), что в криптограмме содержится какое-то другое сообщение, кроме сообщения, полученного с помощью имеющегося у него ключа расшифрования. Из трех сформулированных ранее требований к алгоритмам ОШ второе и третье являются вспомогательными. Однако несоблюдение этих требований служит источником предположений о том, что кроме фиктивного сообщения криптограмма содержит и другую информацию. Сформулированные требования выполняются, если можно указать алгоритм вероятностного шифрования, который преобразует фиктивное сообщение по фиктивному ключу в криптограмму, полученную с помощью алгоритма ОШ. При этом алгоритм расшифрования задается некоторой математической формулой, в которую криптограмма и ключ расшифрования входят в качестве параметров преобразования.

Способ отрицаемого шифрования с использованием блочных преобразований

Пусть дана хэш-функция F_H. Шифрование сообщения T, представленного в виде последовательности u-битовых знаков $\{t_1, t_2, ..., t_i, ..., t_z\}$, выполним путем подбора k-битовых значений $R=\{r_1, r_2, ..., r_i, ..., r_z\}$, где $k > u$, таких, что выполняется соотношение

$$F_H(K, r_i) \bmod 2^u = t_i \quad (1)$$

или

$$F_H(K, i, r_i) \bmod 2^u = t_i, \quad (2)$$

где K — ключ шифрования, для всех значений $i=1, 2, ..., z$. На каждом шаге зашифрования значения r_i выбираются по случайному закону, т. е. эта процедура является вероятностной. Заданному исходному тексту соответствует большое число различных криптограмм. Расшифрование каждой возможной криптограммы приводит к получению одного и того же исходного текста. Расшифрование криптограммы выполняется как последовательная подстановка знаков криптограммы R в формулу (1) или (2).

Очевидно, что размер значений r_i должен превышать размер значений t_i. В результате последнего размер криптограммы больше размера исходного сообщения. Данный способ вероятностного шифрования является интересным благодаря следующим особенностям:

— универсальность (любая хэш-функция или блочное преобразование может быть использовано для реализации вероятностного шифрования по этому способу);

— полное совпадение формул зашифрования и расшифрования;

— возможность выполнения одновременного зашифрования двух и более сообщений.

Смысл шифрования по формуле (2) состоит в том, что включение счетчика в аргумент хэш-функции приводит к получению хороших статистических свойств шифртекста (криптограммы) даже при сравнительно малых значения k и u. Например, можно использовать значения $k=16$ и $u=4$ при шифровании по формуле (2), тогда как при шифровании по формуле (1) достаточная стойкость достигается при $k \geq 24$ и $u \geq 8$.

Шифрование двух сообщений T и M, представленного в виде последовательности знаков $\{m_1, m_2, ..., m_i, ..., m_z\}$, выполним путем подбора k-битовых значений $\{r_1, r_2, ..., r_i, ..., r_z\}$ знаков таких, что выполняется пара соотношений

$$F_H(K_1, r_i) \bmod 2^u = t_i \text{ и } F_H(K_2, r_i) \bmod 2^u = m_i$$

или

$$F_H(K_1, i, r_i) \bmod 2^u = t_i \text{ и } F_H(K_2, i, r_i) \bmod 2^u = m_i.$$

Очевидно, что размер значений r_i должен превышать сумму разрядностей значений t_i и m_i. Причем это должно обеспечить достаточно малое значение вероятности того, что для данной пары значений t_i и m_i не будет найдено подходящее значение r_i. Например, можно задать значения $k=32$ и $u=8$.

Вместо хэш-функции F_H можно использовать алгоритм блочного шифрования E_K. Тогда шифрование пары сообщений T и M выполняется по формулам

$$E_{K_1}(r_i) \bmod 2^u = t_i \text{ и } E_{K_2}(r_i) \bmod 2^u = m_i$$

или

$$E_{K_1}(i, r_i) \bmod 2^u = t_i \text{ и } E_{K_2}(i, r_i) \bmod 2^u = m_i.$$

Включение счетчика в аргумент в случае использования алгоритмов блочного шифрования также обосновывается улучшением статистических свойств ОШ. Преимуществом использования блочных шифров по сравнению с использованием хэш-функций состоит в том, что выходное значение имеет меньшую длину, благодаря чему может быть достигнута более высокая производительность алгоритма ОШ. Представляет интерес использование 64-битовых блочных шифров, а также специально разработанных хэш-функций с u-битовым выходным значением.

Описанный выше способ вероятностного шифрования может обеспечить скорость преобразования входного сообщения, равную $1—10^3$ Мбит/с, а построенный на его основе алгоритм ОШ — скорость зашифрования, равную $10—10^4$ Кбит/с (в режиме расшифрования производительность равна производительности алгоритма вероятностного шифрования). В ряде практических случаев применения ОШ для защиты информации такой производительности достаточно, однако расширение областей применения ОШ связано с существенным повышением скорости совместного шифрования двух сообщений. В следующем разделе предлагается вариант решения данной задачи.

Способ скоростного отрицаемого шифрования

Совместное шифрование двух различных осмысленных сообщений по ключам (K_1, m_1) и (K_2, m_2), где K_1 и K_2 — ключи некоторого блочного шифра E с v-битовым входом; m_1 и m_2 — взаимно простые числа, можно выполнить, разбив их на блоки данных размером v бит и последовательно преобразуя пары блоков данных следующим путем.

1. Используя алгоритм блочного шифрования E и ключ K_1, зашифровать блок M первого сообщения: $C_M=E_{K_1}(M)$.

2. Используя блочный шифр E, зашифровать блок T второго сообщения по ключу K_2: $C_T=E_{K_2}(T)$.

3. Используя дополнительные секретные значения m_1 и m_2, которые являются взаимно простыми, вычислить блок криптограммы, содержащий информацию об обоих исходных текстах T и M и являющийся решением следующей системы сравнений:

$$\begin{cases} C \equiv C_M \bmod m_1 \\ C \equiv C_T \bmod m_2 \end{cases}, \qquad (3)$$

где выходные блоки C_T и C_M функции шифрования E интерпретируются двоичными числами; m_1 и m_2 — секретные взаимно простые значения, имеющие разрядность $v+1$ бит. Размер выходного шифртекста C на два бита больше суммы размеров шифртекстов C_T и C_M. Для чисел m_1 и m_2 может быть задано и большее значение разрядности, например $v+\delta$, однако это приведет к увеличению размера криптограммы на $2(\delta - 1)$ бит по сравнению с рассматриваемым случаем. Решение системы линейных сравнений (3) описывается формулой

$$C=[C_M m_2(m_2^{-1} \bmod m_1)+ \\ +C_T m_1(m_1^{-1} \bmod m_2)] \bmod m_1 m_2.$$

Вычисление значений $m_2(m_2^{-1} \bmod m_1)$ и $m_1(m_1^{-1} \bmod m_2)$ может быть выполнено на этапе генерации секретных ключей, поэтому основной вклад в трудоемкость вычисления значения C вносит операция деления значения в квадратных скобках на модуль $m_1 m_2$. При использовании скоростных блочных шифров данный способ ОШ обеспечивает высокую производительность (в 10^2—10^3 раз более высокую по сравнению со способом ОШ, описанным в предыдущем разделе). Другим его достоинством является то, что размер криптограммы существенно меньше по сравнению с вышеописанным способом ОШ.

Для практического использования алгоритмов ОШ в системах компьютерной безопасности, предусматривающих реализацию защиты информации в режиме прозрачного шифрования данных на встроенном носителе информации [10], предпочтительным является случай равенства размера шифртекста C сумме размеров шифртекстов C_T и C_M. Для реализации такого требования при одновременном получении более высокого быстродействия может быть применен способ ОШ, аналогичный рассмотренному, но отличающийся тем, что формирование блока криптограммы осуществляется путем решения следующей системы линейных сравнений, в которых модулями являются многочлены:

$$\begin{cases} C \equiv E_{K_1}(M) \bmod \mu(x) \\ C \equiv E_{K_2}(T) \bmod \lambda(x) \end{cases}, \qquad (4)$$

где $\mu(x)$ и $\lambda(x)$ — взаимно простые двоичные многочлены степени v; выходные значения блочного алгоритма шифрования интерпретируются двоичными многочленами степени $v-1$. При формировании криптограммы C выполняются вычисления в конечных кольцах двоичных многочленов. Решение этой системы сравнений представляет собой двоичный многочлен степени $2v-1$, который вычисляется по формуле

$$C=[E_{K_1}(M).\lambda(x)(\lambda^{-1}(x) \bmod \mu(x))+ \\ +E_{K_2}(T).\mu(x)(\mu^{-1}(x) \bmod \lambda(x))] \bmod \mu(x)\lambda(x).$$

Так же как и для предыдущего способа ОШ, вычисление значений $\lambda^{-1}(x) \bmod \mu(x)$ и $\mu^{-1}(x) \bmod \lambda(x)$ может быть выполнено заранее, чтобы ускорить процесс шифрования. Для увеличения производительности алгоритма шифрования можно выбирать двоичные трехчлены (не обязательно, чтобы многочлены были неприводимы). Значение k может выбираться равным 64, 128, 256, 512 бит и более. При этом могут использоваться как известные блочные шифры, так и разрабатываемые специально для реализации данного способа ОШ. Алгоритмы ОШ, описанные в настоящем разделе, относятся к алгоритмам блочного шифрования. При шифровании с их помощью сообщений произвольной длины последние должны быть разбиты на блоки, которые могут шифроваться в режиме электронной кодовой книги, в режиме сцепления блоков шифра или в других известных и применяемых для блочных шифров режимах [11—13], которые должны быть соответствующим образом адаптированы для случая ОШ.

Соответствие предложенным требованиям

Способ ОШ, основанный на использовании хэш-функций или блочных преобразований и описанный в разделе «Способ отрицаемого шифрования с использованием блочных преобразований», обеспечивает выполнение трех требований к алгоритмам ОШ, сформулированным в разделе «Требования к алгоритмам отрицаемого шифрования с разделяемым секретом». Это непосредственно видно из описания алгоритмов, реализованных на основе этого способа.

Алгоритмы ОШ, описанные в предыдущем разделе, с очевидностью удовлетворяют второ-

му и третьему требованиям. Покажем, что они удовлетворяют также и требованию неотличимости от вероятностного шифрования. Для этого укажем алгоритм вероятностного шифрования, который по фиктивному ключу преобразует фиктивное сообщение в криптограмму. Данный алгоритм будем называть ассоциируемым алгоритмом вероятностного шифрования.

Рассмотрим алгоритм ОШ, включающий решение системы сравнений (3). Пусть фиктивным ключом является пара значений (K_2, m_2), а фиктивным сообщением — T. Ассоциируемый алгоритм вероятностного шифрования описывается следующим образом.

1. Зашифровывается сообщение T с использованием блочного алгоритма шифрования по формуле $C' = E_{K_2}(T)$.

2. Генерируется случайное значение $R < 2^v$ и простое случайное значение $2^v < r < 2^{v+1}$.

3. Вычисляется криптограмма C как решение следующей системы сравнений:

$$\begin{cases} C \equiv C' \bmod m_2 \\ C \equiv R \bmod r \end{cases}. \qquad (5)$$

Заданная криптограмма C может быть получена с помощью ассоциированного алгоритма вероятностного шифрования при различных парах значений $R < 2^v$ и $r < 2^{v+1}$. Выберем произвольное простое число $2^v < r < 2^{v+1}$. По формуле $C \equiv R \bmod r$ вычислим значение R, которое вместе с выбранным r образует пару значений, при которых решение системы (5) совпадает с заданной криптограммой C. Это означает, что заданная криптограмма может быть получена при выполнении шифрования фиктивного сообщения T с использованием процедуры вероятностного шифрования по фиктивному ключу (K_2, m_2). Для доказательства того, что криптограмма была получена с использованием алгоритма ОШ, атакующему требуется вычислить ключ (K_1, m_1) и расшифровать сообщение M. Однако даже при известном фиктивном ключе и известном фиктивном сообщении это является не проще взлома алгоритма блочного шифрования E. Действительно, если известно секретное значения m_1, то тогда можно вычислить шифртекст, формируемый на выходе функции блочного шифрования E при шифровании сообщения M по ключу K_1, т. е. в результате этого получаем стандартные условия, при которых блочные шифры должны быть стойкими.

Заключение

В настоящей статье рассмотрено применение алгоритмов ОШ с разделяемым секретным ключом в качестве механизма защиты информации и сформулированы требования к алгоритмам такого типа, ориентированные на применение в механизмах защиты, позволяющих реализовать обманные ловушки. Данный механизм защиты информации является новым для применения в комплексных системах информационной и компьютерной безопасности. Описаны разработанные способы и конкретные алгоритмы ОШ, удовлетворяющие сформулированным требованиям. Одним из сформулированных требований является неотличимость криптограммы, полученной с помощью процедуры ОШ, от криптограммы, полученной с помощью процедуры вероятностного шифрования. Соответствие разработанных алгоритмов этому требованию обосновывается указанием ассоциированного вероятностного шифра, для которого процедура расшифрования совпадает с процедурой расшифрования фиктивного сообщения по фиктивному ключу. Приведенные ассоциированные вероятностные шифры интересны тем, что в процессе расшифрования криптограммы случайные значения, использованные при выполнении процедуры зашифрования, не восстанавливаются однозначно, тогда как для известных вероятностных блочных шифров в процессе расшифрования использованные случайные значения восстанавливаются однозначно [10, 14]. Это определяет самостоятельный интерес к рассмотренным алгоритмам вероятностного шифрования. Также самостоятельной исследовательской задачей является разработка достаточно быстрых алгоритмов ОШ, обладающих коммутативными свойствами. Наши предварительные результаты свидетельствуют в пользу возможности решения последней задачи с использованием механизма формирования криптограммы на основе решения системы сравнений, предложенного в данной работе. Рассмотренные алгоритмы относятся к случаю одновременного шифрования двух сообщений, однако они легко расширяются на случай одновременного шифрования трех и более сообщений.

Литература

1. **Canetti R., Dwork C., Naor M., Ostrovsky R.** Deniable Encryption // Advances in Cryptology – CRYPTO 1997: Proc. P. 90–104.
2. **Ibrahim M. H.** A Method for Obtaining Deniable Public-Key Encryption // Intern. J. of Network security. 2009. Vol. 8. N 1. P. 1–9.
3. **Ibrahim M. H.** Receiver-Deniable Public-Key Encryption // Intern. J. of Network security. 2009. Vol. 8. N 2. P. 159–165.
4. **Klonowski M., Kubiak P., Kutyłowsk M.** Practical Deniable Encryption // Theory and Practice of Com-

puter Science: 34th Conf. on Current Trends in Theory and Practice of Computer Science SOFSEM 2008, Nový Smokovec, Slovakia, Jan. 19–25, 2008. P. 599–609.
5. **Canetti R., Gennaro R.** Incoercible multiparty computation // Proc. of the 37th Annual Symp. on Foundations of Computer Science FOCS, Oct. 14–16, 1996 // IEEE Computer Society, Washington, DC. P. 504.
6. **Bo Meng.** A Secure Internet Voting Protocol Based on Noninteractive Deniable Authentication Protocol and Proof Protocol that Two Ciphertexts are Encryption of the Same Plaintext // J. of Networks. 2009. Vol. 4. N 5. P. 370–377.
7. **Bresson E., Catalano D., Pointcheval D.** A simple public key cryptosystem with a double trapdoor decryption mechanism and its applications // Proc. of the Aciacrypt 2003 Conf. LNCS 2894. Berlin: Springer-Verlag, 2003. P. 37–54.
8. **Bo Meng, Jiang Qing Wang.** A Receiver Deniable Encryption Scheme // Proc. of the 2009 Intern. Symp. on Information Processing (ISIP'09), Huangshan, P. R. China, Aug. 21–23, 2009. P. 254–257.
9. **Березин А. Н., Биричевский А. Р., Молдовян Н. А., Рыжков А. В.** Способ отрицаемого шифрования // Вопросы защиты информации. 2013. № 2. С. 18–21.
10. **Алексеев Л. Е., Молдовян А. А., Молдовян Н. А.** Алгоритмы защиты информации в СЗИ НСД «СПЕКТР-Z» // Вопросы защиты информации. 2000. № 3. С. 63–68.
11. **Pieprzyk J., Hardjono Th., Seberry J.** Fundumentals of Computer Security. – Berlin: Springer-Verlag, 2003. – 677 p.
12. **Смарт Н.** Криптография. – М.: Техносфера, 2005. – 528 с.
13. **Menezes A. J., Vanstone S. A.** Handbook of Applied Cryptography. – CRC Press, 1996. – 780 p.
14. **Молдовян А. А., Молдовян Н. А., Гуц Н. Д., Изотов Б. В.** Криптография: скоростные шифры. – СПб.: БХВ-Петербург, 2002. – 495 с.