УДК 681.322

И.В. ЛЫСЕНКО

Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Украина

ИСПОЛЬЗОВАНИЕ ПРИНЦИПА ДИВЕРСНОСТИ ДЛЯ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ СООБЩЕНИЙ В РАМКАХ СОВРЕМЕННОЙ КРИПТОГРАФИИ

Проведен анализ возможности использования принципа диверсности (многоверсионности) для решения задачи криптографической защиты данных. Дано концептуальное описание моделей обеспечения конфиденциальности передаваемых сообщений в соответствии с подходами, основанными на целостной и блочной диверсности, а также межсеансовой и внутрисеансовой диверсности

диверсность, конфиденциальность, криптоалгоритм

Введение

Проблема обеспечения конфиденциальности данных, передаваемых по открытым каналам, не потеряла своей актуальности, при том что в рамках современной криптографии были достигнуты значительные результаты. Задача повышения защищённости сообщений, передаваемых по компьютерным сетям, традиционно решается путём разработки новых и совершенствования существующих криптографических алгоритмов [1]. К примеру, что касается несимметричной криптографии, основанной на преобразованиях в кольцах и полях целых чисел, практически единственным методом защиты от существующих методов криптоанализа является увеличение размерности параметров криптоалгоритмов (несколько тысяч бит для алгоритмов класса RSA и Эль Гамаля), что сопряжено с увеличением времени выполнения крипто преобразований. В то же время, как отмечается в [2], при использовании несимметричных криптоалгоритмов, основанных на преобразованиях в группах точек эллиптических кривых, для достижения того же уровня криптостойкости можно использовать параметры, размерность которых на порядок меньше, и при этом не возрастает сложность (а, соответственно, и время) выполняемых преобразований. Что касается симметричных криптоалгоритмов, использующих меньшую длину ключа (до 200 бит), то они часто подвергаются специфическим для симметричной криптографии методам криптоанализа.

В этой связи нам представляется, что для решения задачи обеспечения конфиденциальности сообщений может быть использован многоверсионный подход (принцип диверсности), который традиционно используется для обеспечения заданного уровня надёжности и гарантоспособности компьютерных и компьютеризированных систем и отдельных их компонент [3].

Принцип диверсности и проблема обеспечения безопасности передаваемых сообщений

В рамках диверсного подхода к обеспечению безопасности информации может, например, рассматриваться задача выбора протоколов защиты согласно уровням модели TCP/IP. Более того, существующие комбинированные криптосистемы (например, PGP [2, 4]), в которых одновременно используются достоинства симметричных и несимметричных криптоалгоритмов, могут считаться реализацией *естественной* диверсности, обусловленной необходимостью решения специфических задач практической криптографии.

Также специфика построения некоторых блочных симметричных криптоалгоритмов свидетельст-

вует о присутствии в них элементов естественной (тривиальной) диверсности. К примеру, криптоалгоритм RC5 характеризуется переменной длиной ключа, переменной длиной блока шифруемого сообщения, варьируемым числом раундов криптопреобразований; криптоалгоритм Blowfish также допускает варьирование длины ключа, а в криптоалгоритме CAST, наряду с возможностью варьировать длиной ключа, переменной является образующая функция сети Фейстеля [2].

Кроме того, по-видимому, есть смысл говорить и о так называемой *нетривиальной* диверсности (в отличие от естественной), под которой может подразумеваться такая организация криптосистемы, при которой варьируются не только используемые криптоалгоритмы (в том числе и в различных сеансах взаимодействия пользователей сети), но и параметры, структура и режимы применения этих алгоритмов. Примерами такого вида диверсности могут быть [4]:

– многопроходные блочные шифры, где каждый блок информации шифруется последовательно несколькими алгоритмами или одним алгоритмом, но с разными ключами (примером такого алгоритма является TripleDES);

– технология каскадного шифрования, при которой всё сообщение в целом шифруется несколькими различными алгоритмами с использованием независимых ключей;

– использование независимых ключей в каждом из раундов криптопреобразований блочных симметричных криптоалгоритмов в отличие от стандартного подхода, заключающегося в формировании в каждом раунде ключей из основного ключа шифрования по известному правилу.

Также объединение нескольких блочных криптоалгоритмов по какому-либо правилу тоже может быть отнесено к некоторой разновидности диверсного похода при шифровании сообщения. Например, сначала генерируется строка случайных бит R того же размера, что и сообщение M (1 этап), затем первым алгоритмом шифруется R (2 этап), а вторым – результат операции XOR между M и R (3 этап); при этом шифртекст сообщения представляет собой объединение результатов этапов 2 и 3.

Что касается поточных симметричных криптоалгоритмов, то с точки зрения диверсного подхода могут рассматриваться ситуации, когда результирующая шифрующая последовательность бит (гамма шифра), накладываемая (например, с помощью операции XOR) на исходный текст, формируется за счёт объединения по определённому правилу (например, тоже по XOR) битовых последовательностей. При этом в одном случае эти битовые последовательности формируются по одной и той же схеме (алгоритму), например, на основе линейных рекуррентных регистров сдвига с обратными связями (ЛРСОС), но с различными параметрами, например, с использованием различных примитивных полиномов (как одной степени, так и разных степеней), ассоциированных с ЛРСОС. В другом же случае битовые последовательности могут формироваться в соответствии с различными схемами (алгоритмами), например, одна – на основе ЛРСОС, другая – на основе сдвиговых регистров с обратной связью по переносу, третья – на основе регистра сдвига с нелинейными обратными связями и т.д.

Представляется также, что применение принципа диверсности позволяет строить надёжные криптосистемы на основе криптоалгоритмов, надёжность которых недостаточна с точки зрения предъявляемых сегодня требований. Идейной основой, на наш взгляд, здесь может выступать хорошо известный в теории надёжности принцип фон Неймана о построении надёжных систем из ненадёжных элементов. Например, практически не используемые сегодня криптоалгоритмы типа алгоритма Меркли-Хеллмана, основанные на труднорешаемой задаче об укладке рюкзака (такие алгоритмы, как замечается в [4], оказались доступными для взлома в середине 80-х годов прошлого столетия), могут послужить основой для создания криптосистемы, компрометация которой уже не представляет собой три-

виальную задачу. Например, может быть использован подход, когда в качестве шифрования разных блоков исходного текста используется не один сверхвозрастающий вектор чисел (секретный ключ), а заранее подготовленный набор таких векторов. При этом этот набор может быть как жёстко фиксированным, так и обновляться с той или иной периодичностью от сеанса к сеансу в соответствии с определённым правилом, а выбор конкретного вектора из этого набора для шифрования каждого блока исходного сообщения в свою очередь также может быть обусловлен определённой процедурой. В этой же связи можно также говорить и, например, о классическом DES с 56-битовым ключом, алгоритме, криптостойкость которого явно недостаточна для многих практических приложений. Например, это может выражаться в том, что вместо использования классической структуры ети Фейстеля из двух ветвей реализуется несколько структур из четырёх ветвей [5]. При этом в разных сеансах обмена зашифрованными данными могут использоваться разные структуры, выбор которых осуществляется по определённому правилу (*межсеансовая* диверсность). Кроме того, возможно, является практически реализуемой ситуация, когда в конкретном сеансе обмена зашифрованными данными в различных раундах шифрования используются различные структуры сети Фейстеля (*внутрисеансовая* диверсность).

Очевидно, что для симметричных криптоалгоритмов в отношении применения принципа диверсности, по-видимому, может иметь место потребность в некоторой модификации стандартного алгоритма, обусловленная особенностями конкретной модели реализации принципа диверсности.

Модель обеспечения конфиденциальности сообщений на основе целостной диверсности

В данной модели используется принцип комбинирования симметричных и несимметричных криптоалгоритмов для шифрования сообщения и ключа шифрования сообщения соответственно. При этом используемые симметричный и несимметричный алгоритмы шифрования не фиксированы – существуют множества симметричных алгоритмов $ME_c = \{E_{ci}\}$, $i = 1,\ldots,d$, и несимметричных алгоритмов $ME_{нс} = \{E_{cj}\}$, $i = 1,\ldots,h$. Выбор конкретных алгоритмов для каждого сеанса осуществляется с помощью генератора случайного (для криптоаналитика) выбора элементов множеств алгоритмов (симметричных и несимметричных) и соответствующих ключей. Данный генератор представляет собой некоторую функцию, которая передается от одного участника информационного обмена другому участнику в начале каждого сеанса в зашифрованном виде (шифрование функции осуществляется с помощью алгоритма с открытым ключом). Таким образом, чтобы взломать сообщение, злоумышленнику необходимо узнать не только ключ секретный несимметричного алгоритма шифрования $K_{нс}$ сообщения (т.е. взломать несимметричный криптоалгоритм), но и используемый в данном сеансе симметричный алгоритм шифрования исходного сообщения. Очевидно, что данная модель реализуется в рамках *межсеансовой* диверсности.

Модель обеспечения конфиденциальности сообщений на основе блочной диверсности

Отличие данной модели от предыдущей состоит в том, что исходное сообщение разбивается на блоки определенной длины, каждый из которых шифруется с помощью криптоалгоритма E_{ci}. При этом выбор криптоалгоритма для шифрования каждого блока m_r исходного сообщения осуществляется генератором случайного выбора элементов множеств ME_c и MK_c, где MK_c – множество ключей.

В результате перечисленных операций на выходе появляются n блоков, зашифрованных различными (в общем случае) криптоалгоритмами ($n = N/l$, где N – длина исходного сообщения, l – длина блока). Оче-

видно, что возможна и ситуация, когда $n > d$, т.е. когда число алгоритмов, используемых для шифрования блоков исходного сообщения, меньше числа самих блоков. В таком случае, например, разбитое на блоки сообщение можно рассматривать как совокупность групп блоков, в пределах каждой из которых выбор того или иного криптоалгоритма E_{ci} осуществляется по тому или иному правилу (например, в порядке очерёдности следования во множестве ME_c).

Восстановление исходного сообщения происходит следующим образом: шифрованные блоки дешифрируются каждый отдельно, при этом выбор криптоалгоритма и ключа для дешифрования производит функция, аналогичная функции на стороне отправителя сообщения.

Очевидно, что данная модель реализуется в рамках *внутрисеансовой* диверсности.

В сравнении с моделью на основе целостной диверсности данная модель обладает тем достоинством, что при постоянной длине передаваемого сообщения время шифрования и дешифрования можно варьировать, изменяя длину блока исходного сообщения. Однако при этом следует помнить, что чем больше длина блока, тем, очевидно, ниже криптостойкость и наоборот, чем выше мы хотим обеспечить криптостойкость, тем меньшую длину блока необходимо задать при шифровании. Это, разумеется, также связано с увеличением времени выполнения криптопреобразований.

Представляется, что увеличение криптостойкости в соответствии с данной моделью может быть достигнуто использованием в алгоритме переменной длины блока, вычисляемой по определенному правилу, как в пределах одного сеанса связи пользователей, так и в различных сеансах. По сути, это есть расширение применения принципа диверсности при обеспечении конфиденциальности сообщений. Разумеется, что при этом увеличивается ключевая информация (правило определения длины блока должно быть известным взаимодействующим пользователям ещё до начала сеанса), а также снижается быстродействие криптоситемы.

Заключение

В результате анализа возможности применения принципа диверсности для обеспечения конфиденциальности сообщений установлено, что могут иметь место различные подходы (модели) использования методов криптографии, учитывающие различные аспекты и особенности структуры существующих криптографических алгоритмов.

В качестве направления дальнейших исследований видится целесообразным рассмотрение в рамках данного подхода возможностей построения моделей реализации других свойств защиты данных (аутентичности, целостности и др.), а также других функций информационной безопасности, обеспечиваемых за счёт применения соответствующих криптопротоколов (аутентификация пользователей, распределение сеансовых ключей и др.).

Литература

1. Чмора А.Л. Современная прикладная криптография. – М.: Гелиос АРВ, 2001. – 256 с.

2. Столлингс В. Криптография и защита сетей. Принципы и практика. – К.: Вильямс, 2001. – 669 с.

3. Многоверсионные системы, технологии и проекты / Харченко В.С. и др.; Под ред. В.С. Харченко. – Х.: Мин. образования и науки Украины. – 2003. – 528 с.

4. Шнайер Б. Прикладная криптография: протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 815 с.

5. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с.

Поступила в редакцию 9.03.2006

Рецензент: д-р техн. наук, проф. В.С. Харченко, Харьковский национальный аэрокосмический университет «ХАИ», Харьков.