УДК 681.322

МОДЕЛИ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ СООБЩЕНИЙ СРЕДСТВАМИ КРИПТОГРАФИИ НА ОСНОВЕ ПРИНЦИПА ДИВЕРСНОСТИ

И.В. Лысенко, Д.А. Филиппов
(Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков)

Проведен анализ возможности использования принципа диверсности (многоверсионности) для решения задачи криптографической защиты данных. Предложены модели обеспечения конфиденциальности передаваемых сообщений в соответствии подходами, основанными на целостной и блочной диверсности.

конфиденциальность сообщений, диверсность, криптографическая защита

Постановка проблемы. Несмотря на многие достижения современной криптографии проблема обеспечения конфиденциальности данных, передаваемых по незащищенным каналам, не потеряла своей актуальности. Задача повышения защищенности сообщений, передаваемых по компьютерным сетям, традиционно решается путем разработки новых и совершенствования существующих криптографических алгоритмов [1]. В рамках несимметричной криптографии, основанной на преобразованиях в кольцах и полях целых чисел, практически единственным методом защиты от существующих методов криптоанализа является увеличение длины ключа (несколько тысяч бит для алгоритмов класса RSA и Эль Гамаля). Использование несимметричных криптоалгоритмов, основанных на преобразованиях в группах точек эллиптических кривых, для достижения того же уровня криптостойкости требует использования ключа длиной на порядок меньше. Симметричные криптоалгоритмы, использующие меньшую длину ключа (до 200 бит), часто подвергаются дифференциальному и другим методам криптоанализа. Для решения указанной задачи можно использовать многоверсионный подход (принцип диверсности), традиционно используемый для успешного решения задачи обеспечения заданного уровня надежности и гарантоспособности компьютеризированных систем [2]. **Цель статьи** – анализ возможности использования принципа диверсности для обеспечения безопасности сообщений и описание результатов исследования разработанных моделей обеспечения конфиденциальности сообщений на основе целостной и блочной диверсности.

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 [3]) могут считаться

реализацией *естественной* диверсности, обусловленной необходимостью решения специфических задач практической криптографии. Также специфика построения некоторых блочных симметричных криптоалгоритмов свидетельствует о присутствии в них элементов естественной (тривиальной) диверсности. Например, это касается таких параметров, как переменная длина ключа (криптоалгоритмы RC2, RC5, CAST, Blowfish); переменная длина блока шифруемого сообщения (RC5); переменное число раундов криптопреобразований (RC5); переменная образующая функция сети Фейстеля (CAST).

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. Примеры такого вида диверсности [3]: многопроходные блочные шифры, где каждый блок информации шифруется последовательно несколькими алгоритмами или одним алгоритмом, но с разными ключами (пример такого алгоритма – TripleDES); технология каскадного шифрования, при которой все 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 размера сообщения 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 счет объединения по определенному 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 надежные криптосистемы на основе криптоалгоритмов, надежность которых недостаточна с точки зрения предъявляемых сегодня требований (здесь, на наш взгляд, имеет место аналогия с хорошо известным в теории надежности принципом фон Неймана о построении надежных систем из ненадежных элементов). Например, практически не используемые сегодня криптоалгоритмы типа алгоритма Меркли-Хеллмана, основанные на трудноразрешаемой задаче об укладке рюкзака (такие алгоритмы оказались доступными для взлома в середине 80-х годов прошлого столетия [3]), могут послужить основой для создания криптосистемы, компрометация которой уже не представляет собой тривиальную 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 жестко фиксированным, так и обновляться с той или иной периодичностью от сеанса к сеансу в соответствии с определенным правилом, а выбор конкретного вектора из этого набора для шифрования каждого блока исходного сообщения в свою очередь также может быть обусловлен определенной процедурой. 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 сети Фейстеля из двух ветвей реализуется несколько структур из 4 ветвей [4]. При этом в разных сеансах обмена зашифрованными данными могут использоваться разные структуры, выбор которых осуществляется по определенному правилу. Кроме того, возможно, является практически реализуемой ситуация, когда в различных раундах шифрования (в классическом DES 16 раундов) используются различные структуры сети Фейстеля.

Таким образом, для симметричных криптоалгоритмов в отношении применения принципа диверсности, по-видимому, могут иметь место два подхода: без модификации стандартного алгоритма; некоторой модификацией стандартного алгоритма, обусловленной 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,…,d, и несимметричных алгоритмов $ME_{нс} = \{E_{cj}\}$, i = 1,…,h. Выбор конкретных алгоритмов для каждого сеанса осуществляется с помощью генератора случайного выбора элементов множеств алгоритмов (симметричных и несимметричных) и соответствующих ключей. Данный генера-

тор 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.

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 мгожеств ME_c и MK_c, где MK_c – множество ключей. В результате перечисленных операций на выходе появляются n блоков, зашифрованных различными общем случае) криптоалгоритмами ($n = N/l$, где N – длина исходного сообщения, l – длина блока). Очевидно, 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 очередности следования во множестве ME_c). Восстановление исходного сообщения происходит следующим образом: шифрованные блоки дешифрируются каждый отдельно, при этом выбор криптоалгоритма и ключа для дешифрации производит функция, аналогичная функции на стороне отправителя сообщения. Данная модель в сравнении с моделью на основе целостной диверсности обладает тем достоинством, что при постоянной длине передаваемого сообщения время шифрования и дешифрования можно варьировать, изменяя длину блока исходного сообщения. Однако чем больше длина блока, тем ниже криптостойкость и наоборот: чем выше мы хотим обеспечить криптостойкость, тем меньшую длину блока необходимо задать при шифровании.

Увеличения криптостойкости в соответствии с данной моделью можно достичь, используя в алгоритме переменную длину блока, вычисляемую по определенному правилу, как в пределах одного сеанса связи пользователей, так и в различных сеансах. По сути, это расширение применения принципа диверсности при обеспечении конфиденциальности сообщений. Разумеется, что при этом увеличивается ключевая информация (правило определения длины блока должно быть известным взаимодействующим пользователям еще до начала сеанса), а также снижается быстродействие криптоситемы.

На базе предложенных моделей разработаны программы (была использована платформа .NET Framework, а в качестве среды разработки использо-

валась Microsoft Visual Studio .NET 2003), позволяющие двум пользователям обмениваться зашифрованными сообщениями. В ходе выполнения тестовых сеансов обмена сообщениями с помощью этой программы, были получены результаты, анализ которых дает возможность оценить влияние длины сообщения, размера блока (при использовании блочной диверсификации), а также производительности вычислительной системы (ВС), на которой производятся криптографические преобразования, на время шифрования/дешифрования сообщения. В результате обобщения полученных данных разработаны рекомендации относительно рациональных параметров передаваемых сообщений и производительности используемых вычислительных средств.

Выводы. В результате тестовых сеансов передачи сообщений для модели, основанной на блочной диверсности, было установлено: а) независимо от числа реализаций эксперимента при малых значениях числа блоков n при заданной длине блока и длине сообщения время шифрования и дешифрования отклоняется менее чем на 0,1%; б) независимо от производительности ВС, время шифрования/дешифрования при малых значениях длины блока (n = 1…5) растет примерно пропорционально росту длины передаваемого сообщения; в) чем меньше длина блока, тем большее время ВС необходимо затратить на шифрование/дешифрование сообщения, однако, следует отметить тот факт, что примерно для $n \geq 5$ время шифрования растет равномерно, а при n = 1…4 время начинает резко увеличиваться (по экспоненциальной зависимости). Эта закономерность проявляется независимо от длины исходного сообщения и производительности ВС.

Характер проанализированных результатов моделирования позволяет предложить рациональный вариант передачи сообщений с помощью данной программы: длина сообщений должна быть не более 5…10 кбайт, размер блока необходимо выбирать 5…10 слов (по 2 байта). Это позволит тратить на передачу сообщения от одного пользователя к другому время, равное сумме времени прохождения зашифрованного сообщения по каналу связи и времени шифрования/дешифрования, которое составит примерно 0,5 секунд при использовании компьютеров с частотой работы процессора не ниже 600 Мгц.

ЛИТЕРАТУРА

1. *Чмора А.Л. Современная прикладная криптография. – М.: Гелиос АРВ, 2001. – 256 с.*
2. *Многоверсионные системы, технологии и проекты / В.С. Харченко и др.; Под ред. В.С. Харченко. – Х.: Мин. образования и науки Украины, 2003. – 528 с.*
3. *Шнайер Б. Прикладная криптография: протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 815 с.*
4. *Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. – С.-Пб.: БХВ – Петербург, 2003. – 752 с.*

Поступила 16.01.2006

Рецензент: доктор технических наук, профессор В.С. Харченко,
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ».