УДК 681.322

И.В. ЛЫСЕНКО

Национальный аэрокосмический университет им. М.Е. Жуковского «ХАИ», Украина

МОДЕЛЬ РЕАЛИЗАЦИИ КРИПТОГРАФИЧЕСКОЙ ФУНКЦИИ ХЭШИРОВАНИЯ НА ОСНОВЕ ПРИНЦИПОВ ДИВЕРСНОСТИ И КОМПОЗИТНОСТИ

Предлагается подход к построению криптографической хэш-функции на основе принципов диверсности и композитности с целью повышения стойкости к криптоаналитической атаке, основанной на парадоксе «дня рождения».

дайджест, диверсность, криптостойкость, коллизия, композитность, хэш-функция

Введение

Наряду с конфиденциальностью наиболее важной услугой (функцией) защиты данных, передаваемых по открытым каналам, является целостность. Данная услуга реализуется посредством применения ключевых и бесключевых криптографических хэш-функций (КХФ), осуществляющих однонаправленное (необратимое) криптопреобразование защищаемых данных таким образом, что в его результате формируется дайджест документа (сообщения), длина которого, как правило, существенно меньше сообщения и который выполняет функцию “отпечатков пальцев” данного документа [1, 2].

В настоящее время в системах защиты данных используются такие КХФ, как HAVAL, RIPEMD, MD-5 SHA-1, SHA-2, Whirlpool, относящиеся к классу бесключевых, а также ключевые, формирующие код аутентификации сообщения: UMAC, Rijndael в режиме CBC-MAC, ГОСТ 28147-89 (режим 4) и др.

Среди перечисленных КХФ наиболее распространены в различных приложениях MD-5, SHA-1, RIPEMD. Что касается последнего алгоритма, то, как замечается в [3], он “во многом подобен как MD-5, так и SHA-1, так как за основу всех трёх алгоритмов взят алгоритм MD-4”. Так, например, в [4] отмечается, на долю хэш-функций MD-5 и SHA-1, позволяющих формировать дайджест документа длиной 128 и 160 бит соответственно, приходится 80% хэширований в гражданской криптографии. Однако достижения в области криптоанализа КХФ и рост производительности вычислительных средств привели к формулированию более сильных требований к стойкости хэш-функций. Так, требования международных проектов AES и NESSIE (проводились в 2000–2001 и 2002–2003 г.г. соответственно) предполагают три уровня стойкости КХФ по отношению к криптоанализу, основанному на парадоксе «дня рождения»: вероятность возникновения коллизии должна быть не менее 2^{-128}, 2^{-192} и 2^{-256}, что соответствует длине дайджеста 256, 384 и 512 бит [5].

Как утверждается в статье «Скомпрометированы криптографические хэш-функции» («Компьютеры, сети, программирование», 2007, № 4, с.54, 55), “уже ясно, что слабость MD-5 является фатальной и всем серьёзным программам, на неё опирающимся, пора подыскивать замену”. Известно, что к числу таких “серьёзных программ” относятся PGP и др., а также протоколы информационной безопасности SSL, S/MIME, IPSec и др. В отношении SHA-1 там же говорится, что “израильтяне Эли Бихам и Рафи Чен провели анализ SHA-1, включая отыскание коллизий для сокращённой версии алгоритма … и сумели взломать работу алгоритма на сорока циклах, но уверены, что атаку можно продолжить, правда Би-

хам заметил, что сомнительно, что удастся преодолеть больше сорока шести циклов" и далее делается заключение о том, что "SHA-1 пока вышел сухим из воды, но охотники уже обложили его со всех сторон.

Поэтому ожидается, что вскоре начнётся постепенная миграция криптоприложений к чему-то более сильному".

Несмотря на то, что существует хэш-функция SHA-2, позволяющая формировать дайджест длиной 256, 384 и 512 бит, а также другие хэш-функции с большей, чем у MD-5 и SHA-1 длиной дайджеста [4], предлагаемый подход, возможно, позволит создавать, выражаясь словами авторов вышеупомянутой статьи, это "что-то более сильное".

Сущность подхода к построению хэш-функции

Как известно, единственным способом уменьшить вероятность коллизии для хэш-функции при криптоанализе, основанном на парадоксе "дней рождения", является увеличение длины дайджеста документа.

Суть предлагаемого подхода состоит в совместном использовании принципов *диверсности* и *композитности* при хэшировании сообщения, целостность которого необходимо обеспечить.

В соответствии с первым из них пользователи заранее определяют множество стандартных бесключевых КХФ $MH(\cdot) = = \{H_1(\cdot),\ldots,H_p(\cdot)\}$, которые используются для генерации хэш-значения в данном сеансе связи.

При этом выбор конкретных элементов множества $MH(\cdot)$ осуществляется на основе использования секрета (ключа, парольной фразы) по некоторому несекретному правилу, заранее определяемому взаимодействующим пользователями.

Надо заметить, что элементы диверсного подхода при выполнении хэширующих преобразований присутствуют в некоторых широкоприменяемых приложениях по защите данных. Например, в протоколе SSL (Secure Socket Layer – протокол защищённых сокетов) в том случае, когда используется цифровая подпись на основе криптоалгоритма RSA, хэш-значение сообщения представляет собой конкатенацию хэш-значений, полученных в результате хэширования данного сообщения посредством хэш-функций MD-5 и SHA-1.

Подобным образом совместное применение хэш-функций MD-5 и SHA-1 имеет место в более новой версии SSL – протоколе TLS (Transport Layer Security – протокол защиты транспортного уровня) при формировании сообщения о завершении протокола квитирования между сервером и клиентом, а также при реализации псевдослучайной функции, применяемой для генерирования секретных значений, используемых в последствии при формировании ключей или проверке их подлинности [3].

Согласно принципу композитности, основанному на описанном в подходе [2], результирующее хэш-значение m сообщения M представляет собой конкатенацию хэш-значения m*, полученного путём преобразовани H(M), и хэш-значения m**, являющегося результатом преобразования посредством той же хэш-функции хэш-значения m*, соединённого с документом M, т.е.

$$m = m^* || m^{**} =$$

$$H(M) || H(m^* || M) = H(M) || H(H(M) || M),$$

где $||$ – оператор конкатенации.

Очевидно, что данный подход может быть расширен в том смысле, что хэширование документа с присоединённым к нему ранее полученным хэш-значением может быть многократным. Типовое хэш-преобразование в таком случае определяется как раунд, и в общем случае пользователи могут выполнять n раундов хэш-преобразований.

Формально результат хэш-преобразования на i-м раунде можно представить следующим образом:

$$\forall j = 1,\ldots,p: m_i = H_j(m_0 || \ldots || m_{i-1} || M), \; i = 1,\ldots,n;$$

где $m_0 = H(M)$ – дайджест исходного сообщения M.

Как видно из приведенного соотношения, значение i-го дайджеста зависит от значений дайджестов, сформированных на предыдущих раундах, а результирующий дайджест m есть конкатенация дайджестов, полученных на всех раундах хэширования, т.е.

$$m = m_0 || m_1 || \ \dots || m_n.$$

Очевидно, что в таком случае его длина равна n·length(m_0), т.е. увеличенной в n раз длине дайджеста стандартной хэш-функции, что с учётом сказанного выше означает, что для формирования результирующего дайджеста требуется сохранять в процессе вычислений дайджесты, рассчитанные на всех раундах.

В соответствии с принятыми обозначениями структура i-того раунда хэш-преобразования показана на рис. 1.

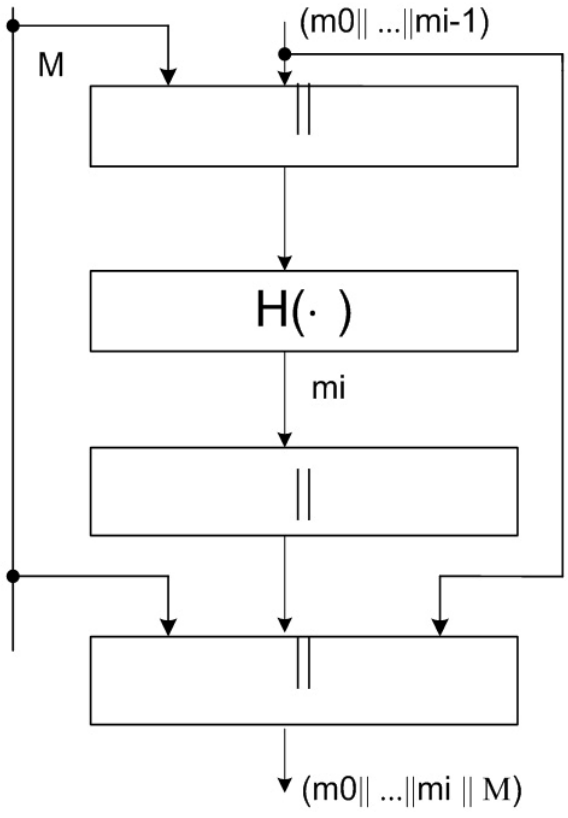

Рис. 1. Структура i-го раунда хэш-преобразования

Заключение

Таким образом, пользователи, не делая секретным множества MH(·), но, варьируя $H_j(\cdot)$ и числом раундов n преобразований, создают неопределённость для криптоаналитика относительно того, какие хэш-функции из множества MH(·) и сколько раундов хэш-преобразований использовались в данном сеансе.

Предполагается, что как за счёт упомянутого обстоятельства, так и за счёт увеличения длины дайджеста, данный подход позволит увеличить криптостойкость механизма хэширования данных. Очевидно, при этом, что достижение предполагаемого эффекта будет связано с увеличением времени вычисления хэш-значения документа. Поэтому представляет интерес то, в какой степени это время увеличится для различных значений параметра n по сравнению со стандартным (“однораундовым”) подходом.

Литература

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: ТРИУМФ, 2003. – 816 с.

2. Menezes A., Van Oozcchot P. Handbook of applied cryptography. – CRC Press, 1996. – 780 p.

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

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

5. Горбенко І.Д., Гриненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації. – Х.: ХНУРЕ, 2004. – 368 с.

Поступила в редакцию 25.12.2007

Рецензент: д-р техн. наук, проф., И.Д. Горбенко, Харьковский национальный университет радиоэлектроники, Харьков.