облегченного шифрования ISO/IEC 29192-2:2012. В феврале 2014г. стало известно о разработке нового легковесного блочного шифра Halka. Его основное отличие − использование восьмибитных *S*-боксов, в то время как большинство других блочных алгоритмов с легковесными свойствами используют четырехбитные *S*-боксы. Использование же восьмибитных *S*-боксов гарантирует более высокую криптостойкость. В рамках проекта eSTREAM, существовавшего с 2004г. по 2008г. в качестве конкурса на разработку поточных шифров, в числе «победителей» оказались такие легковесные поточные шифры, как Grain (версия 1), MICKEY (версия 2) и Trivium.

На сегодняшний день известны такие механизмы легковесной хэш-функции, как S-Quark и D-Quark, PHOTON и SPONGENT. Все эти алгоритмы, как и победитель конкурса SHA-3 Keccak, основываются на принципе криптографической губки, что позволяет оперировать с данными произвольной длины, как на входе, так и на выходе алгоритма. В конце декабря прошлого года криптографическому сообществу стало известно еще об одной разработке легковесной хэш-функции под названием LHash. Авторы заявляют, что созданный ими механизм, расширяющий описанный ранее принцип криптографической губки, позволил разработать компромиссный по безопасности, скорости, энергозатратам и стоимости реализации алгоритм.

В области криптографии с открытым ключом вопрос поиска оптимального легковесного алгоритма, сравнимого по надежности с RSA или с алгоритмами, основанными на эллиптических кривых, остается открытым, поскольку асимметричные системы более требовательны к временным ресурсам, чем симметричные. Однако некоторые достижения в этом направлении все же имеются, например, в работе для пассивных RFID-систем.

В настоящее время наиболее «легковесными» являются алгоритмы асимметричной криптографии, работающие с эллиптическими кривыми (ECC – Elliptic Curves Cryptography). Типичными значениями параметров различных процессоров, предназначенных для вычислений с эллиптическими кривыми, являются величины в пределах 10–40 μW и 10000–20000 GE. Близкими к ним являются и значения параметров у процессоров, предназначенных для вычислений с гиперэллиптическими кривыми (HECC – HyperElliptic Curves Cryptography).

Таким образом, по сравнению с симметричной криптографией, асимметричная криптография с безопасной длиной ключа, реализованная на аппаратном уровне, по-прежнему требует значительно больших ресурсов (по крайней мере, 10000 дополнительных логических элементов), при этом реализуется вполне приемлемая скорость работы. Для криптографии с открытым ключом верхняя граница на размер микросхемы устанавливается в 15000 GE.

Что касается программной реализации, то тщательная оптимизация алгоритмов позволяет микроконтроллерам выполнять операции ассиметричной криптографии менее чем за 1 с, что вполне достаточно для большинства приложений. При этом программно-аппаратная реализация, по-видимому, создает наилучший баланс между размером и скоростью для многих распространенных вычислительных приложений.

Литература

1. Жуков А.Е. Легковесная криптография: нетребовательная к ресурсам и стойкая к атакам // Материалы форума PositiveHackDays 2012.

2. PRESENT: An Ultra-Lightweight Block Cipher. CHES / A. Bogdanov [et al.]. 2007. № 4727. P. 450−466.

НОВЫЕ СРЕДСТВА БЕЗОПАСНОСТИ WINDOWS SERVER 2012/16. ДИНАМИЧЕСКИЙ КОНТРОЛЬ ДОСТУПА

В.Т. Садовский, В.Д. Мильто, Е.А. Зайченко

Изучение свойств, функций операционных систем семейства Windows Server является актуальной задачей для дисциплин «Администрирование и программирование распределенных приложений», «Системное программное обеспечение» по специальности «Автоматизированные системы обработки информации». В практике применения Windows Server 2012/16 [1, 2] динамический контроль доступа представляет собой наиболее фундаментальное изменение по безопасности доступа к ресурсам сети. В более ранних версиях

доступ к ресурсам файлового сервера, к принтерам и другим устройствам в доменной сети с контроллером домена и службой каталогов Active Directory осуществлялся при помощи списков доступа Access Control List (ACL), а для более защищенных ресурсов с применением шифрования – службы управления правами (Rights Management Services). С помощью этих средств администратор мог назначить права доступа к папкам, файлам для определенного пользователя, используя только его членство в определенной группе безопасности домена. При большом количестве общих папок и других ресурсов приходилось создавать большое количество групп в домене.

Динамический контроль доступа Dynamic Access Control Windows Server (DAC) создает дополнительный уровень безопасности, применение этой технологии позволяет сконфигурировать права доступа к папкам и файлам, учитывая не только членство в группах безопасности, но и другие параметры пользователей и устройств, зафиксированные в Active Directory сервера, например: Department (Отдел), Country (Страна) и т. п. Технология базируется на трех основных понятиях: классификация документов (на основе свойств файлов, например, местоположение файла); утверждение (сформулированное условие, которое соответствует значениям атрибута пользователя или компьютера); аудит (политика аудита позволяет получить информацию о попытках доступа к конфиденциальной информации).

Литература

1. Microsoft Windows Server 2012. Полное руководство / Р. Моримото [и др.]. М.: ООО «И.Д. Вильямс», 2013. 1456 с.

2. Windows Server 2012 R2. Полное руководство / М. Минаси [и др.]. М.: ООО «И.Д. Вильямс», 2015. 960 с.

ОДНОСТОРОННЯЯ ФУНКЦИЯ НА ОСНОВЕ ТЕОРИИ СЛУЧАЙНЫХ РЕШЕТОК

С.Б. Саломатин

Основные задачи, связанные с построением односторонних функций на основе теории решеток связаны с решением двух задач. Первая – задача декодирования на абсолютном расстоянии d. Если d больше определенной величины, то решение гарантированно существует. Вторая задача связана с декодированием на граничном расстоянии: если решение существует, то оно единственно. Решение этих двух задач на случайных решетках может быть сформулировано в рамках задачи инвертирования функции $f(\mathbf{x}) = \mathbf{A}\mathbf{x} \bmod p$.

Определим решетку L как подгруппу векторов по модулю p целых чисел. Дуальную (ортогональную) к ней решетку обозначим как D. Конечное множество точек Q решеток образуют множество с координатами в $\{0, 1, \ldots, p-1\}$.

Дуальные решетки могут быть использованы для получения различных (эквивалентных) конструкций односторонних функций. Образуем решетку $L(\mathbf{A})$ из случайной матрицы $\mathbf{A}$ массива целых чисел с модулярной операцией. Тогда решение двух основных задач криптографических решеток в рамках выбора случайной точки $\mathbf{v}$ и вектора ошибки $\mathbf{x}$ и получения целевого показателя $\mathbf{t} = \mathbf{v}+\mathbf{x}$. Решетки периодичны по модулю p, все векторы редуцированы по модулю p и точка решетки может быть выбрана из массива конечного множества $L \bmod p$ с равномерным распределением. Случайная точка представляется как $v = \mathbf{A}\mathbf{s} \bmod p$. Односторонняя функция имеет вид A’$\mathbf{s} + \mathbf{x} \bmod p$, где вектор $\mathbf{s}$ принадлежит векторному массиву целых чисел. Односторонняя функция имеет два входа: вектор $\mathbf{s}$ из массива случайных чисел с равномерным распределением и вектор ошибки $\mathbf{x}$, соответствующий заданной функции f. Функция становится свободной от коллизий при достаточно большом размере вектора $\mathbf{x}$.

Односторонняя функция на основе случайных решеток может быть использована в схемах сетевого кодирования и системах связи.