В свою очередь, известно, что с ростом длины параметры КВ-кодов становятся только лучше или, как минимум, не ухудшаются, что сделало множество КВ-кодов популярным объектом для исследований. Однако процесс исследования этих объектов весьма затруднителен, КВ-коды плохо поддаются декодированию.

В данной работе строится способ декодирования квадратично-вычетных кодов при помощи теории норм синдромов, основанной на инвариантности норменных и полиномиальных орбит ошибок. Были изучены квадратично-вычетные коды длины 31 и 73. Для них были построены норменные, полиномиальные орбиты, построен алгоритм декодирования данных кодов в системе компьютерной алгебры Wolfram Mathematica. Данный алгоритм отличается своей простотой, скоростью и эффективностью.

ОСОБЕННОСТИ ПРИМЕНЕНИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ ДЛЯ АУТЕНТИФИКАЦИИ В СИСТЕМАХ IoT

Н.С. Руденко, Г.А. Власова

Тенденция массового перехода от интернета персональных компьютеров к интернету вещей (Internet of Things, IoT) ставит новые задачи по обеспечению надежности и безопасности работы сетей. Одним из основных средств защиты информации для IoT является использование криптографических алгоритмов. В связи с тем, что многие приспособления в сети мобильны и зачастую имеют небольшие размеры, существуют общие ограничения на ресурсы времени и памяти. Эти ограничения распространяются и на криптографические схемы, открывая новое направление – разработки и исследования алгоритмов малоресурсной криптографии (Lightweight Cryptography, LWC).

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 энергопотребления в пределах 10–40 μW и размеров микросхемы 10,000–20,000 GE (условных логических элементов, Gate Equivalent). Известные реализации алгоритма RSA значительно превышают 15,000 GE. 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 15,000 GE. Что касается программной реализации, то тщательная оптимизация алгоритмов позволяет микроконтроллерам выполнять операции ассиметричной криптографии менее чем за 1 секунду, что вполне достаточно для большинства приложений. При этом программно-аппаратная реализация, создает наилучший баланс между размером и скоростью для многих распространенных вычислительных приложений.

Одним из наиболее надежных симметричных алгоритмов является ГОСТ 28147-89. Результаты сравнений популярных симметричных шифров показывают, что ГОСТ 28147-89 при аналогичной криптостойкости обладает достаточным для IoT быстродействием. Также хорошие результаты показывают отечественные алгоритмы, собранные в библиотеке bee2.

В результате можно сделать вывод о том, что использование малоресурсных криптографических алгоритмов для аутентификации в сетях IoT вполне возможно и не практически не влияет на удобство их эксплуатации пользователем.

ЛЕГКОВЕСНАЯ КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ

Т.Х. Рустамов

Легковесная криптография – раздел криптографии, имеющий своей целью разработку алгоритмов для применения в устройствах, которые не способны обеспечить большинство существующих шифров достаточными ресурсами (память, электропитание, размеры) для функционирования. Области блочного шифрования наиболее популярными легковесными алгоритмами считаются CLEFIA и PRESENT. Оба алгоритма известны еще с 2007 г. В 2012 г. организации ISO и IEC включили алгоритмы PRESENT и CLEFIA в международный стандарт

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