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