РАЗДЕЛ II. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Богатова О.А., Магомедов Ш.Г.

Оценка эффективности решений в области криптографической безопасности для устройств интернета вещей

Российский технологический университет
(Россия, Москва)

doi: 10.18411/lj-10-2019-20

idsp: ljjournal-10-2019-20

Аннотация

Актуальность темы обусловлена тем, что в связи с ростом технологий появляется большое количество мобильных и стационарных роботов, используемых в повседневной жизни, например квадрокоптеры, доставляющие посылки, или системы «умный дом», служащие для автоматизации управления различными гаджетами, используемыми в домашних нуждах. Малоресурсная криптография служит для обеспечения защиты таких систем, в статье приведен краткий обзор и сравнение различных методов шифрования криптографической безопасности интернета вещей.

Ключевые слова: криптография, стойкость шифров, криптоалгоритмы, малоресурсная криптография, интернет вещей, шифрование.

Abstract

The relevance of the topic is due to the fact that due to the growth of technology there is a large number of mobile and stationary robots used in everyday life, such as quadcopters delivering parcels, or "smart home" systems that serve to automate the management of various gadgets used in home needs. Low-resource cryptography serves to ensure the protection of such systems, the article provides a brief overview and comparison of various methods of cryptographic security encryption of the Internet of things.

Keywords: cryptography, cipher strength, crypto algorithms, low-resource cryptography, Internet of things, encryption.

Некоторые из алгоритмов ориентированы на аппаратную реализацию, другие, наоборот, показывают лучшие характеристики при программной реализации.

В 1976 году появилась революционная статья У. Диффи и М. Хеллмана, в которой предлагалось новое направление в криптографии и вводились основные понятия криптографии с открытым ключом, до этого в криптографии использовались только алгоритмы с секретным ключом.

У. Диффи и М. Хеллман предложили два фундаментальных изменения: персонализация ключей (каждый объект в системе имеет свой собственный ключ); разделение ключей (каждый ключ делится на открытый и закрытый, которые вместе образуют ключевую пару).

Данный вид шифрования основывается на идее односторонней функции с потайным входом. Функция называется односторонней, если ее легко вычислить, но невозможно инвертировать в доступных временных рамках, учитывая существующую вычислительную мощность, не зная секретного ключа.

Самой известной задачей, которая используется для этих целей является факторизация больших натуральных чисел, на которой и основан алгоритм шифрования системы RSA.

Стойкость шифрования напрямую привязана к размеру ключа, а увеличение размера ключа в два раза обеспечивает экспоненциальное увеличение криптостойкости,

хотя и снижает производительность. Ключи RSA обычно имеют длину 1024 или 2048 бит, однако существуют экспертные мнения, согласно которым, в ближайшее время появится возможность взламывать 1024-битные ключи, поэтому NIST требует перехода на минимальную длину ключа 2048 бит или 4096 бит [2]. Следует отметить, что в 2013 году группа криптографов, возглавляемая с А. Шамиром, успешно определила 4096-битный ключ RSA, применяя акустический криптоанализ, однако любой алгоритм шифрования уязвим для данного метода атаки [3].

Альтернативой RSA в реализации шифрования с открытым ключом является эллиптическая криптография ECC (Elliptic Curve Cryptography), которая позволяет обеспечивать более высокую безопасность с применением меньшей вычислительной мощности, что делает ее более подходящей для мобильных приложений.

Алгоритм основан на алгебраической структуре эллиптических кривых над конечными полями. ECC алгоритм является наиболее эффективным алгоритмом, поскольку позволяет обеспечить сопоставимый уровень безопасности при использовании ключа меньшего размера (с размером ключа в 224 бита обеспечивает одинаковый уровень безопасности с RSA с ключом в 2048 бит) [4]. Алгоритм в основном используется в средах с ограниченными ресурсами. Использование короткого ключа позволяет уменьшить энергопотребление (использование ресурсов оперативной памяти и процессора) и ускорить шифрование. В Европе многие IT решения, основанные на смарт-картах, используют ECC шифрование, например, национальное удостоверение личности стран Европейской экономической зоны, новая карта медицинского страхования в Германии и др.

Также в области классической криптографии наиболее распространенными являются, например, DSA (Американский стандарт шифрования) и ГОСТ 34.12-2015 (Российский стандарт шифрования, включающий алгоритмы шифрования Магма и Кузнечик) [3].

В сравнении с малоресурсной криптографией, такие стандарты шифрования, как ЕС и ГОСТ, обрабатывают информацию достаточно быстро. Например, Кузнечик (длина блока – 128 бит, длина ключа – 256 бит) в своей скоростной реализации 54 Мбайт/с, а DSA (длина блока – 128 бит, длина ключа – 128 бит) – 51 Мбайт/с [5,6]. Но подобные шифры занимают гораздо больше ROM и RAM памяти компьютера, примерно соразмерно со скоростью выполнения, что отвергает применение данных алгоритмов в режимах ограниченных возможностей, таких как конечный запас энергии и ограниченный объем памяти.

Также хотелось бы отметить использование протоколов в Интернете вещей. Для того чтобы любые компоненты Интернета вещей могли полноценно функционировать и взаимодействовать между собой, зачастую необходимо устанавливать защищенное соединение между всеми компонентами данной системы. Данный процесс подразумевает использование криптографических алгоритмов и ключей для шифрования трафика, с предварительным прохождением процесса аутентификации. Сам процесс аутентификации является ключевой процедурой, так как без него злоумышленник может вмешаться в сетевое взаимодействие, отправлять свои команды, чем полностью нарушает функционирование всей сети Интернета вещей. Для всех вышеперечисленных целей, как правило, используются протоколы.

Например, протокол IKE (Internet Key Exchange) используется в виртуальных частных сетях, устанавливает защищенный канал связи, осуществляет процесс аутентификации сторон взаимодействия, а также основан на протоколе разделения секрета Диффи - Хеллмана (DH) [1,5]. Собственно, протокол Диффи - Хеллмана позволяет нескольким взаимодействующим сторонам получить общий секретный ключ для использования его в симметричном шифровании, например, в любом алгоритме малоресурсной криптографии, что весьма удобно. Но, в процессе применения протокола IKE лежит использование криптографии с открытым ключом, что

автоматически неприемлемо в Интернете вещей. Криптография с открытым ключом довольно ресурсоемкая, не отвечает требованиям малоресурсности и не может поддерживаться устройствами Интернета вещей.

Аналогичным образом существуют стандарты ZigBee и Bluetooth LE, описывающие взаимодействие устройств Интернета вещей между собой. Главным недостатком этих протоколов является отсутствие защиты от атаки методом "Man in the middle" (MITM, «человек посередине»). Злоумышленник может вклиниться в обмен информацией, «подслушать» трафик и перехватить обмен ключами, а затем использовать link key – стандартный ключ связи, который используют производители. Это вмешательство MITM позволяет скомпрометировать сетевой ключ, сетевое взаимодействие, открыть устройства сети для атак.

Ниже представлены протоколы MQTT, XMPP, DDS и AQMP, которые обеспечивают коммуникацию устройств Интернета вещей.

MQTT [1]. Данный протокол собирает данные с различных устройств и оборудования и передает полученную информацию на сервер. При этом он обеспечивает надежную передачу данных, без потерь, и также может работать в условиях связи с перебоями.

XMPP [2]. Протокол, используемый для обмена мгновенными сообщениями между людьми, а также сообщениями о присутствии. Для Интернета вещей реализует простой способ адресации устройств.

DDS [5]. Протокол, который распределяет данные, полученные с одних устройств, для передачи другим устройствам. Основная задача протокола – соединение с целевыми устройствами.

AQMP [4]. Промежуточный протокол, который организует и обрабатывает очередь сообщений.

Таблица 1.
Сравнения программных реализаций малоресурсных алгоритмов шифрования

Алгоритм	RCA	DSA	ECC
Параметр оценки			
Реализация (программная/аппаратная)	программная	программная	программная
Длина ключа (бит)	128	80	80
Размер блока	128	64	поточный шифр
Скорость шифрования одного блока данных	5 Мбайт/с	1 Мбайт/с	0,6 Мбайт/с
Количество раундов шифрования	18	31	-
Количество памяти, занимаемое реализацией	4780 байт	1000 байт	-
Задействование оперативной памяти	180 байт	18 байт	-

Как можно увидеть, особенности протокола напрямую зависят от области его применения. Например, MQTT следует использовать при сборе показателей давления или температуры, а AQMP – при организации очереди сообщений при совершении банковских транзакций.

Так как малоресурсные криптографические алгоритмы зачастую используются в мобильной робототехнике и в Интернете вещей, то на них могут совершаться разнообразные атаки с целью кражи или фальсификации обрабатываемой, хранимой или передаваемой информации.

Например, в работе Бабенко Л.К. содержится описание алгебраической атаки на малоресурсный шифр Present. Как известно, Present является симметричным блочным алгоритмом шифрования с длиной блока 64 бита и длиной ключа 80 или 128 бит, при этом количество раундов шифра равно 32 м. Авторам работы удалось описать и провести алгебраический анализ пяти раундов шифра Present [1].

Исходя из полученных авторами данных и составленной таблицы (Таблица 1.) можно сделать вывод, что Алгебраический анализ пяти раундов и восстановление ключа 128 бит при заданных вычислительных мощностях (2 ГГц ЦПУ и 1 Гб оперативной памяти) выполняется успешно за очень короткое время. Также при комбинировании некоторых методов криптоанализа авторы смогли весьма успешно проанализировать до 26 раундов данного шифра. Поэтому для обеспечения безопасности компонентов Интернета вещей необходимо использовать максимальное количество раундов данного криптографического алгоритма.

В работе «Сетевые технологии Интернета вещей» аналогичным образом осуществлялся алгебраический анализ шифра Present, и методы авторов данной работы также оказались успешными на первых пяти раундах шифра. Начиная с шестого раунда шифр Present оказывается стойким против алгебраического криптоанализа [6].

Что касается криптоанализа малоресурсного шифра Clefta, разработанного Sony Corporation, то сама компания привела документ, содержащий различные подходы к криптоанализу данного шифра.

Авторы разбирают множество способов криптоанализа Clefta, приводят примеры и обосновывают, как тот или иной метод анализа может быть направлен на данный шифр. Например, авторы отмечают, что Clefta благодаря своим особенностям является стойкой к дифференциальному криптоанализу, более 10 раундов Clefta стойки к атакам прямоугольником, и обладает достаточной стойкостью против слайдовой атаки. Также авторы рассматривают не только программно-реализованный алгоритм, но и аппаратно-ориентированную версию.

И в конце следует отметить, что различные легковесные шифры используются для разных целей, в зависимости от поставленной задачи. В одном случае необходима быстрая скорость обработки данных, а в другом, например, нужно ограничить энергопотребление или же обрабатывать информацию в условиях ограниченных запасов памяти. У классических криптографических шифров отмечаются высокие скорости шифрования данных, но при этом они не могут быть использованы в системах с ограниченными ресурсами, где нашли применение легковесные шифры. Также среди малоресурсных шифров имеются аппаратно- и программно-ориентированные алгоритмы, использование которых также варьируется в зависимости от поставленной задачи перед системой.

Что касается протоколов взаимодействия устройств Интернета вещей, они имеют различные степени защищенности, или вообще отсутствуют. Использование асимметричной криптографии малоресурсными устройствами Интернета вещей нецелесообразно, в силу высокой ресурсоемкости данных алгоритмов, поэтому и не используются аналогичные протоколы, основанные на асимметричной криптографии.

В результате исследования атак на малоресурсные шифры следует отметить, что большинство из рассмотренных на данный момент не способны максимально успешно взломать шифры целиком за приемлемое время, но в связи с ростом вычислительных мощностей устройства Интернета вещей могут оказаться под угрозой.

1. Бабенко Л.К., Беспалов Д.А., Макаревич О.Б., Чесноков Р.Д., Трубников Я.А. Разработка и исследование программно-аппаратного комплекса шифрования по алгоритму present для решения задач малоресурсной криптографии // Известия ЮФУ. 2014. № 2. С. 174-180.
2. Жуков А.Е. Легковесная криптография. Часть 1 // Вопросы кибербезопасности. 2015. № 1. С. 26-43.
3. Жуков А.Е. Легковесная криптография. Часть 2 // Вопросы кибербезопасности. 2015. № 2. С. 2-10.
4. The 128-bit Blockcipher CLEFIA. Algorithm Specification. [Электронный ресурс]. URL: http://www.cryptrec.go.jp/english/cryptrec_13_spec_cypherlist_files/PDF/22_00espec.pdf
5. Бабенко Л.К., Голотин Д.В., Макаревич О.Б. Создание и исследование малоресурсной реализации поточного шифра Trivium // Известия ЮФУ 2016. № 12. С. 42-54.
6. Сетевые технологии Интернета вещей [Электронный ресурс]. URL: https://habrahabr.ru/company/ericsson_ru/blog/301494/