УДК 004.021

АНАЛИЗ АЛГОРИТМОВ ШИФРОВАНИЯ МАЛОРЕСУРСНОЙ КРИПТОГРАФИИ В КОНТЕКСТЕ ИНТЕРНЕТА ВЕЩЕЙ

[1,2]Ищукова Е.А., [1]Толоманенко Е.А.

[1]ФГАОУ ВО «Южный федеральный университет», Таганрог, e-mail: uaishukova@sfedu.ru, kat.tea@mail.ru;

[2]ИИПРУ КБ НЦ РАН, Нальчик

В нынешнее время Интернет вещей стремительно развивается и проникает во все сферы жизни общества. Благодаря Интернету вещей человек получает постоянную поддержку от предметов, которые его окружают, все процессы при этом осуществляются прозрачно, а также человек не должен продумывать, как надо это сделать, а знать, что должно в итоге получиться. Для того, чтобы обезопасить взаимодействие между человеком и устройствами, а также между самими устройствами, целесообразно использовать шифрование. Обычное классическое применение общеизвестных блочных и поточных алгоритмов шифрования, например, национальных стандартов, не всегда удобно и применимо в рамках данной задачи. На смену классическим алгоритмам шифрования приходят особые алгоритмы шифрования, так называемые малоресурсные. Легковесная, или малоресурсная, криптография рассматривает алгоритмы шифрования, которые используются в различных устройствах в условиях ограниченных ресурсов. Например, при ограниченном запасе электропитания, небольшом объеме памяти, маленьких размерах устройств. Зачастую такими устройствами являются роботизированные системы, например мобильные роботы или беспилотные летательные аппараты. Помимо легковесных алгоритмов шифрования, устройства Интернета вещей используют различные протоколы взаимодействия между собой в сети. Эти протоколы имеют различное назначение и характеристики, а также отличаются свойствами безопасности. Некоторые из общеизвестных протоколов имеют уязвимости и подвержены атакам. А в некоторых протоколах и вовсе отсутствуют механизмы безопасности.

Ключевые слова: малоресурсная криптография, легковесная криптография, алгоритмы шифрования, Clefia, Present, Trivium, Интернет вещей, протоколы IoT

ANALYSIS OF THE ALGORITHMS FOR ENCRYPTION OF LIGHTWEIGHT CRYPTOGRAPHY IN THE CONTEXT OF THE INTERNET OF THINGS

[1,2]Ishchukova E.A., [1]Tolomanenko E.A.

[1]Federal Autonomous Educational Institution of Higher Education Southern Federal University, Taganrog, e-mail: uaishukova@sfedu.ru, kat.tea@mail.ru;

[2]Institute of Informatics and Regional Management Problems of the KB SC RAS, Nalchik

At the present time, the Internet of things is rapidly developing and penetrating into all spheres of society. Thanks to the Internet of Things, a person receives constant support from the objects that surround him, all processes are carried out transparently, and a person should not think through how to do it, but know what should happen in the end. In order to secure the interaction between humans and devices, as well as between the devices themselves, it is advisable to use encryption. The usual classical application of well-known block and stream encryption algorithms, for example, national standards, is not always convenient and applicable within the framework of this task. The classical encryption algorithms are replaced by special encryption algorithms, the so-called short-resourced ones. Lightweight, or short-resource, cryptography examines encryption algorithms that are used in various devices with limited resources. For example, with a limited power supply, a small amount of memory, small size devices. Often, such devices are robotic systems, for example, mobile robots or unmanned aerial vehicles. In addition to lightweight encryption algorithms, IoT devices use different protocols for interacting with each other on the network. These protocols have different purposes and characteristics, as well as different security features. Some of the well-known protocols have vulnerabilities and are subject to attacks. And in some protocols, there are no security mechanisms at all.

Keywords: low resource cryptography, lightweight cryptography, encryption algorithms, Clefia, Present, Trivium, Internet of Things, IoT Protocols.definition

Цель исследования 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.

Хотелось бы отметить некоторые работы в области малоресурсной криптографии. Авторы статей предлагают различные подходы к реализации тех или иных легковесных алгоритмов шифрования. Некоторые из алгоритмов ориентированы на аппаратную реализацию, другие, наоборот,

показывают лучшие характеристики при программной реализации.

Малоресурсная криптография

Например, статья Л.К. Бабенко, Д.В. Голотина, О.Б. Макаревича [1] содержит описание поточного шифра Trivium [2] и его аппаратной реализации. В статье сказано, что шифр Trivium является алгоритмом, наиболее ориентированным на аппаратную реализацию, чем на программную. Авторы описали, что данный шифр реализован на ПЛИС, плате Марсоход2Bis. В реализации осуществлена связь с компьютером, при этом передача данных компьютеру осуществляется с фиксированной скоростью в 9600 бит/с, или 1200 байт/с и ограничивается характеристиками com-порта. Также авторы рассматривают разработанную уменьшенную модель в сравнении с моделью, реализованной создателями, которая может быть полезной при работе с небольшими мобильными роботами.

В статье Л.К. Бабенко, Д.В. Голотина [3] описана программная реализация шифра Trivium. Авторы рассказывают, что полученная программа выполняет шифрование 13,5 Мб за 168,7 с, что означает скорость примерно в 640 Кбит/с. Также авторы отмечают, что полученное решение в сравнении, например, с DES превышает скорость вдвое, при условии использования процессора с частотой 2,1 ГГц.

Шифр Present [4] описан в статье Л.К. Бабенко, Д.А. Беспалова, О.Б. Макаревича, Р.Д. Чеснокова, Я.А. Трубникова [5]. Авторы данной статьи разработали программную реализацию и синтезировали аппаратный блок для системы на кристалле в рамках требований к малоресурсной криптографии и получили достаточно эффективное решение для применения его в устройствах. Полученные авторами характеристики: частоты ПЛИС – 160 МГц максимально (работа схемы алгоритма), скорость 301.2 Мбит/с.

Статьи Жукова [6] и [7] содержат обзор исследований, содержащих описание шифров по малоресурсной криптографии, куда попали такие шифры, как Present, Trivium и Clefia. Автор отметил, что некоторые аппаратные шифры, такие как Present или KATAN, теряют свои полезные свойства при программной реализации и показывают худшие результаты. Проанализировав сводные таблицы автора статьи, отражающие скорость работы различных шифров, например, такого, как Clefia, можно сказать, что данный шифр является неплохим вариантом для использования его для шифрования в мобильной робототехнике.

Шифр Clefia [8] был разработан компанией Sony для использования в качестве безопасной альтернативы шифру AES. Размер блока алгоритма шифрования Clefia составляет 128 бит, а ключи могут быть длиной как 128 бит, так и 192 и 256 бит. В основе алгоритма лежит сеть Фейстеля, а именно две различные 32-битные функции – F0 и F1, поэтому количество раундов алгоритма зависит напрямую от длины ключа: при длине ключа 128 бит количество раундов будет составлять 18, при 192 битах – 22 раунда, при 256 битах – 36 раундов. Количество подключей также подчиняется данному принципу и составляет 36, 44 и 52 подключа соответственно. При этом в алгоритме применяются отбеливающие ключи, замедляющие процесс криптоанализа данного шифра. Также для защиты от методов дифференциального и линейного криптоанализа разработчики Sony применили Diffusion Switching Mechanism. Также было объявлено, что данный шифр защищен и от алгебраических атак, и от другого вида атак ввиду использования двух типов таблиц подстановки. Также хотелось бы отметить ключевые функции алгоритма, такие как Double Swap (двойная замена), функции получения S-блоков замены. Шифр Clefia реализован компанией Sony на языке программирования C и упора на скорость не осуществлялось. Следует отметить, что функцию двойной замены можно удачно реализовать с упором на скорость с помощью операций битовых сдвигов, используемых в C++.

В статьях Жукова [6] и [7] помимо обзора легковесных шифров содержится информация о скоростных и других показателях данного вида шифров. На основе проанализированных статей [8] и [9] и полученных данных мы можем предположить скорость работы программных реализаций малоресурсных алгоритмов шифрования, таких как Clefia, Present и Trivium. Например, при предполагаемой частоте работы процессора примерно в 2 ГГц вышерассмотренные алгоритмы будут иметь характеристики, отображенные в таблице.

По имеющимся данным из статей [7] и [10] можно сказать, что шифр Clefia имеет хорошую скорость работы и обработки блоков данных. Аппаратно-ориентированный шифр Present имеет более низкую скорость обработки при программной реализации. Шифр Trivium также более ориентирован на аппаратную реализацию.

Сравнение алгоритмов шифрования

В общем смысле в области классической криптографии наиболее распростра-

ненными являются, например, AES [10] – Американский стандарт шифрования и ГОСТ 34.12–2015 [11] – Российский стандарт шифрования, включающий алгоритмы шифрования Магма и Кузнечик.

В сравнении с малоресурсной криптографией, такие стандарты шифрования, как AES и ГОСТ, обрабатывают информацию достаточно быстро. Например, Кузнечик (длина блока – 128 бит, длина ключа – 256 бит) в своей скоростной реализации 54 Мбайт/с [12], а AES (длина блока – 128 бит, длина ключа – 128 бит) – 51 Мбайт/с [13]. 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.

Протоколы

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 нарушит функционирование всей сети Интернета вещей. Для всех вышеперечисленных целей, как правило, используются протоколы.

Например, протокол IKE (Internet Key Exchange) [14] используется в виртуальных частных сетях, устанавливает защищенный канал связи, осуществляет процесс аутентификации сторон взаимодействия, а также основан на протоколе разделения секрета Диффи – Хеллмана [15]. 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 [16, 17] и Bluetooth LE [18], описывающие взаимодействие устройств Интернета вещей между собой. Главным недостатком этих протоколов является отсутствие защиты от атаки методом «человек посередине». Злоумышленник может вклинится в обмен информацией, «подслушать» трафик и перехватить обмен ключами, а затем использовать link key – стандартный ключ связи, которые используют производители. Это вмешательство «человека посередине» позволяет скомпрометировать сетевой ключ, сетевое взаимодействие, открыть устройства сети для атак.

Существуют следующие протоколы для обеспечения коммуникации устройств Интернета вещей:

– MQTT [19]. 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 [20]. Протокол, используемый для обмена мгновенными сообщениями между людьми, а также сообщениями о присутствии. Для Интернета вещей реализует простой способ адресации устройств;

Сравнения программных реализаций малоресурсных алгоритмов шифрования

Алгоритм / Параметр оценки	Clefia	Present	Trivium
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	–

– DDS [21]. Протокол, который распределяет данные, полученные с одних устройств, для передачи другим устройствам. Основная задача протокола – соединение с целевыми устройствами.

– AQMP [22]. Промежуточный протокол, который организует и обрабатывает очередь сообщений.

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.

Атаки на алгоритмы малоресурсной криптографии

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 [23] 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 [23] удалось описать и провести алгебраический анализ пяти раундов шифра Present. Исходя из полученных авторами данных и составленной таблицы 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 [24] 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.

Что касается криптоанализа малоресурсного шифра Clefia, разработанного Sony Corporation, то сама компания привела документ, содержащий различные подходы к криптоанализу данного шифра [25]. Авторы разбирают множество способов криптоанализа Clefia, приводят примеры и обосновывают, как тот или иной метод анализа может быть направлен на данный шифр. Например, авторы отмечают, что Clefia благодаря своим особенностям является стойкой к дифференциальному криптоанализу, более 10 раундов Clefia стойки к атакам прямоугольником, и обладает достаточной стойкостью против слайдовой атаки. Также авторы рассматривают не только программно-реализованный алгоритм, но и аппаратно-ориентированную версию.

Заключение

В заключение хотелось бы 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 их отсутствие. 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.

Работа выполнена при поддержке гранта РФФИ № 17-07-00654-а.

Список литературы

1. Бабенко Л.К., Голотин Д.В., Макаревич О.Б. Создание и исследование малоресурсной реализации поточного шифра Trivium // Известия ЮФУ. 2016. № 12. С. 42–54.

2. Yun Tian, Gongliang Chen, Jianhua Li. On the Design of Trivium. School of Information Security Engineering, Shanghai

Jiaotong University, China [Электронный ресурс]. URL: https://eprint.iacr.org/2009/431.pdf (дата обращения: 25.01.2019).

3. Бабенко Л.К., Голотин Д.В. Об основных особенностях функционирования и реализации поточного шифра Trivium // Известия ЮФУ. 2015. № 5. С. 103–111.

4. A. Bogdanov, L.R. Knudsen, G. Leander. PRESENT: An Ultra-Lightweight Block Cipher [Электронный ресурс]. URL: https://web.archive.org/web/20101217063636/http://www.ist-ubisecsens.org/publications/present_ches2007.pdf (дата обращения: 25.01.2019).

5. 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.

6. Жуков А.Е. Легковесная криптография. Часть 1 // Вопросы кибербезопасности. 2015. № 1. С. 26–43.

7. Жуков А.Е. Легковесная криптография. Часть 2 // Вопросы кибербезопасности. 2015. № 2. С. 2–10.

8. 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 (дата обращения: 25.01.2019).

9. Cazorla M., Marquet K., Minier M. Survey and Benchmark of Lightweight Block Ciphers for Wireless Sensor Networks. [Электронный ресурс]. URL: https://eprint.iacr.org/2013/295.pdf (дата обращения: 25.01.2019).

10. Advanced encryption standard (AES) [Электронный ресурс]. URL: https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf (дата обращения: 25.01.2019).

11. ГОСТ 34.12–2015 [Электронный ресурс]. URL: https://web.archive.org/web/20150924113434/http://www.tc26.ru/standard/gost/GOST_R_3412-2015.pdf (дата обращения: 25.01.2019).

12. Ищукова Е.А., Кошуцкий Р.А., Бабенко Л.К. Разработка и реализация высокоскоростного шифрования данных с использованием алгоритма Кузнечик [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/razrabotka-i-realizatsiya-vysokoskorostnogo-shifrovaniya-dannyh-s-ispolzovaniem-algoritma-kuznechik (дата обращения: 25.01.2019).

13. Intel Core i5 (Clarkdale): анализ аппаратного ускорения шифрования AES. [Электронный ресурс]. URL: http://www.thg.ru/cpu/aes_clarkdale/print.html (дата обращения: 25.01.2019).

14. The Internet Key Exchange (IKE) [Электронный ресурс]. URL: https://tools.ietf.org/html/rfc2409 (дата обращения: 25.01.2019).

15. Whitfield Diffie, Martin E. Hellman. New Directions in Cryptography [Электронный ресурс]. URL: https://ee.stanford.edu/~hellman/publications/24.pdf (дата обращения: 25.01.2019).

16. ZigBee [Электронный ресурс]. URL: https://web.archive.org/web/20100526153954/http://www.daintree.net/downloads/whitepapers/zigbee_primer.pdf (дата обращения: 25.01.2019).

17. ZigBee Specification [Электронный ресурс]. URL: http://www.zigbee.org/wp-content/uploads/2014/11/docs-05-3474-20-0csg-zigbee-specification.pdf (дата обращения: 25.01.2019).

18. Bluetooth с низким энергопотреблением [Электронный ресурс]. URL: https://www.bluetooth.com/specifications (дата обращения: 25.01.2019).

19. MQTT [Электронный ресурс]. URL: http://mqtt.org(дата обращения: 25.01.2019).

20. XMPP [Электронный ресурс]. URL: https://xmpp.org (дата обращения: 25.01.2019).

21. DDS [Электронный ресурс]. URL: https://www.omg.org/spec/#DDS (дата обращения: 25.01.2019).

22. AQMP [Электронный ресурс]. URL: https://www.amqp.org (дата обращения: 25.01.2019).

23. Jorge Nakahara Jr, Pouyan Sepehrdad, Bingsheng Zhang, Meiqin Wang. Linear (Hull) and Algebraic Cryptanalysis of the Block Cipher PRESENT // Proceedings of 8th International Conference «Cryptology and Network Security», Japan, December 12–14, 2009. DOI: 10.1007/978-3-642-10433-6_5.

24. Lucia Lacko-Barto˘sov´a. Algebraic cryptanalysis of present based on the method of syllogisms // Tatra Mt. Math. Publ. 53 (2012), 201–212. DOI: 10.2478/v10127-012-0047-3.

25.The 128-bit Blockcipher CLEFIA. Security and Performance Evaluations. Revision 1.0, June 1, 2007. Sony Corporation [Электронный ресурс]. URL: https://www.sony.net/Products/cryptography/clefia/download/data/clefia-eval-1.0.pdf (дата обращения: 25.01.2019).