УДК 004.056.55

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЛЕГКОВЕСНЫХ БЛОЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ NASH И SPECK, ИСПОЛЬЗУЕМЫХ В УСТРОЙСТВАХ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ (МИКРОКОНТРОЛЛЕРАХ)

Разумов П. В., Смирнов И. А., Черкесова Л. В.
Донской государственный технический университет, Ростов-на-Дону, Российская Федерация

therazumov@gmail.com
terran.doatk@mail.ru
chia2002@inbox.ru

Проведен сравнительный анализ легковесного алгоритма блочного шифрования Nash и алгоритма, представленного Агентством национальной безопасности США в 2013 году — Speck. Приведено их подробное описание. Исследование легковесных алгоритмов шифрования и их применение для задач кибербезопасности необходимо для создания новейших криптографических систем, ориентированных на предотвращение различного рода атак. Задача исследования заключается в изучении и анализе криптографических алгоритмов шифрования, используемых в устройствах с ограниченными возможностями по типу микроконтроллеров. В ходе исследования было установлено, что блочный алгоритм шифрования Nash показал более высокие результаты, так как число раундов выполнения шифра меньше, чем у алгоритма Speck, что обеспечивает большую стойкость данного алгоритма при наименьшем числе исполняемых раундов.

Ключевые слова: блочный алгоритм шифрования, легковесный алгоритм, криптографическая система, микроконтроллер, устройство с ограниченными возможностями, раундовая функция, блок данных, криптостойкость.

UDC 004.056.55

COMPARATIVE ANALYSIS OF LIGHTWEIGHT BLOCK ENCRYPTION ALGORITHMS NASH AND SPECK, WHICH ARE USED IN MICROCONTROLLERS

Razumov P.V., Smirnov I. A., Cherkesova L. V.
Don State Technical University, Rostov-on-Don, Russian Federation

therazumov@gmail.com
chia2002@inbox.ru
terran.doatk@mail.ru

The article is devoted to the comparative analysis of the lightweight Nash block encryption algorithm and the algorithm presented by the us national security Agency in 2013 - Speck. Their detailed description is given, the analysis is made. The task of the study is to investigate and analyze cryptographic encryption algorithms used in devices with limited capabilities such as microcontrollers. The study of lightweight encryption algorithms and their application for cybersecurity tasks is necessary to create the latest cryptographic systems aimed at preventing various types of attacks. The study revealed that the Nash block encryption algorithm showed a more optimized performance, since the number of rounds of cipher execution is less than that of the Speck algorithm, which provides greater stability of the algorithm with the least number of executable rounds.

Keywords: block encryption algorithm, lightweight algorithm, cryptographic system, microcontroller, device with limited capabilities, round function, data block, cryptographic strength.

Введение. Современный мир переполнен различного рода бытовыми устройствами, в том числе датчиками и механизмами распознавания, другими интеллектуальными системами, активно участвующими в жизни общества.

Каждую минуту люди взаимодействуют друг с другом посредством автоматизированных систем, управляют своей жизнью при помощи устройств, работающих на основе микроконтроллеров. А их низкая стоимость и легкодоступность способствуют широкому распространению микроконтроллеров в промышленных системах, системах управления, а также в бытовых приборах массового сегмента рынка.

В связи с распространением таких технологий в обществе их программная и техническая сложность увеличивается, что также касается и реализации сложных криптографических преобразований, а это в условиях современного мира, мира глобальных кибернетических войн, вирусов и охоты за информацией является проблемой весьма актуальной. Так, бывший директор ЦРУ Дэвид Петреус заявлял, что максимально подробное досье на любого человека можно составить, получив данные с бытовых приборов, подключенных к Интернету.

Необходимость защиты информации предполагает существование возможности реализации стандартных методов шифрования на микроконтроллерах, но данный метод не позволяет обеспечить необходимую скорость шифрования. Имеют место так называемые «легковесные» алгоритмы шифрования, в которых термин «легковесная» не означает «простая», а скорее — «низкоресурсная», что более точно отражает суть данной технологии.

Актуальность данной методики обусловлена условиями функционирования устройств, жесткими финансовыми рамками, а также значительными ограничениями на используемые ресурсы памяти, вычислительную мощность, источники питания и многое другое. Таким образом, накладываются ограничения на энергозатратность реализации криптографических алгоритмов, что обеспечивается размерами программного кода, оперативной памяти и временем, затраченным на исполнение программного средства.

Одними из наиболее эффективных криптографических систем такого рода следует признать алгоритмы SPECK и SIMON, которые были разработаны АНБ и опубликованы в июне 2013 года, незадолго до обнародования разоблачений Сноудена, которые серьёзно подорвал репутацию АНБ в части разработки криптографии, продемонстрировав тот факт, что эксперты АНБ сознательно ослабляли криптографические алгоритмы. Более того, на заседаниях ISO представители службы безопасности США отказались мотивировать выбранные константы для матриц перестановок алгоритмов. Все это в конце концов привело к тому, что приведенные алгоритмы перестали официально применяться в криптосистемах.

В этих алгоритмах отражена идея алгоритма шифрования, когда выполняется большое количество простых преобразований. Эта идея была высказана еще в 1950-х годах лауреатом Нобелевской премии по экономике Джоном Нэшэм [1].

Целью данного исследования является сравнительный анализ легковесного алгоритма блочного шифрования Nash, названного в честь Джона Нэша, и алгоритма, представленного Агентством национальной безопасности США в 2013 году — Speck [2–10].

Схема алгоритма Nash. Представим данный алгоритм шифрования следующим образом. В первую очередь, необходимо разбить текст на полублоки по 2^n бит. В свою очередь, каждый блок шифруется один за другим r раундов на последовательности раундовых ключей $k(i)$, которые рассчитываются из главного ключа по алгоритму «расширения ключа». Таким образом образуется блок данных, впоследствии разбивающийся на два полублока — левый $L(i)$ и правый $R(i)$ по 2^n бит каж-

дый. В дальнейшем на $(i+1)$ раунде производятся преобразования, обусловленные схемой раунда шифрования, приведённой на рис. 1.

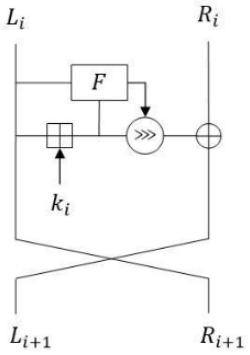

Рис. 1. Схема раунда шифрования

Для $(i+1)$ раунда уравнения шифрования блок данных выглядит следующим образом:

$R(i+1)=L(i)$

$L(i+1)=((L(i)\ xor\ k(i))>>>F(L(i),L(i)\ xor\ k(i)))\ xor\ R(i)$.

Что касается последнего раунда шифровния блока, то в нем полублоки $L(i)$ и $R(i+1)$ не меняются местами.

Рассмотрим более детально особенности преобразования раундов. Размер полублока составляет 2^n, где $n=5$ или 6. Размер блока равен 32 или 64 бит соответственно. Более того, также предлагается использовать размер блока, равный 64 или 128 бит.

Заметим, что в данном алгоритме присутствует функция смешивания с раундовым ключом $k(i)$: $\oplus$ — функция сложения двух целых чисел по модулю 2^n.

Следующий этап — функции управления сдвигами. Необходимо интерпретировать полублок $L(i)$ в качестве значений булевой функции n переменных. На выходе из алгоритма первый выходной бит F приобретает значение данной функции на наборе битов из $L(i),...,гдеi=1,....,n$. Или, используя эквивалентное обозначение, как значение ...., где применяется нумерация битов полублока от 0 до 2^{n-1}.

$L(i)\ xor\ k(i)$ следует интерпретировать как вектор значений булевой функции n переменных. В данном случае второй выходной бит приобретает значение данной функции на наборе битов из $L(i)$ вида $2^{i-1},....,гдеi=1,...,n$.

Рассмотрим также функцию выработки раундовых ключей, схема которой представлена на рис. 2.

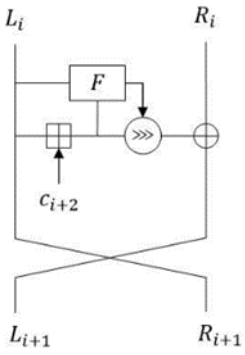

Рис. 2. Схема раунда формирования ключей

Заметим, что $L(0)-c(0), R(0)=c(1)$, где значение константы $c(i)$ определяется следующим образом. Сначала ключ разбивается на L блоков длины 2^n, а остальные $8-L$ блоков определяются как значения квадратного корня из простых чисел (таких, как корень 2, …). Данные блоки соответствуют $c(0),...,c(7)$. Далее, при расчете $c(i)$ необходимо взять данную константу с индексом $(i \bmod 6)+2$ и суммировать его по модулю 2 с номером раунда $c(i)=i \oplus c((i \bmod 6)+2)$. В итоге в качестве раундового ключа необходимо рассмотреть $k(i)=L(i+1)$.

Легковесный блочный шифр Speck. Спустя несколько лет после публикации блочных шифров Simon и Speck практических атак ни на один из них не появилось. Их наиболее яркими преимуществами являются простота и гибкость.

В отличие от своего родственного алгоритма Simon, оптимизированного под аппаратные средства, алгоритм Speck используется в рамках программной имплементации, в особенности в таких устройствах с ограниченными возможностями, как микроконтроллеры.

Блочный алгоритм шифрования Speck представляет собой ARX шифр — использует исключающее ИЛИ, сложение по модулю и методы циклического сдвига. Также предусматривает возможность выбора длины блока и ключа, исходя из значений, представленных в табл. 1, в зависимости от исполняемой задачи.

В данном алгоритме блок разбит на два слова, где длина ключа кратна длине слова.

Раундовая функция, изображенная на рис. 3, используется для вычисления раундовых ключей — номер раунда выдается в качестве ключа.

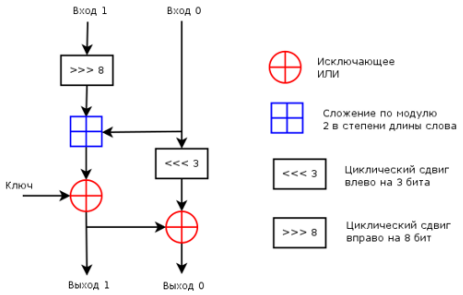

Рис. 3. Раундовая функция Speck

В случае, изображенном на рис. 4, если длина ключа равна длине блока, представляется возможным использовать код раундовой функции, что обеспечивает дополнительную гибкость.

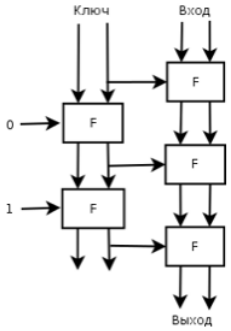

Рис. 4. Длина ключа Speck равна длине блока

Рассматривая вариант, в котором ключ длиннее блока, нетрудно заметить, что слова ключа используются циклически. Третий случай отображен на рис. 5.

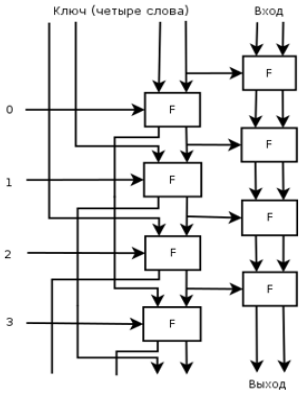

Рис. 5. Длина ключа Speck больше длины блока

Стоит добавить, что наиболее сильными сторонами данного алгоритма являются простота имплементации и незначительное требование используемой памяти. В нем отсутствуют какие-либо константы и перестановки, не используется технология отбеливания ключа.

Сравнительный анализ легковесных алгоритмов. В ходе исследования было произведено значительное количество практических испытаний, результаты проведенных экспериментов приведены в табл. 1 и 2 для блочных шифров Nash и Speck соответственно, в которых отображаются название конкретного алгоритма, размеры блока, длина ключа и количество раундов.

Таблица 1

Результаты испытаний блочного шифра Speck

Название	Размер блока, бит	Длина ключа, бит	Количество раундов
Speck 32/64	32	16*4=64	22
Speck 48/72	48	24*3=72	22
Speck 48/96	48	24*4=96	23
Speck 64/96	64	32*3=96	26
Speck 64/128	64	32*4=128	27
Speck 96/96	96	48*2=96	28
Speck 96/144	96	48*3=144	29
Speck 128/128	128	64*2=128	32
Speck 128/192	128	64*3=192	33
Speck 128/256	128	64*4=256	34

Таблица 2

Результаты испытаний блочного шифра Nash

Название	Размер блока, бит	Длина ключа, бит	Количество раундов
Nash 32/64	32	16*4=64	22
Nash 48/72	48	24*3=72	22
Nash 48/96	48	24*4=96	23
Nash 64/96	64	32*3=96	24
Nash 64/128	64	32*4=128	26
Nash 96/96	96	48*2=96	28
Nash 96/144	96	48*3=144	28
Nash 128/128	128	64*2=128	32
Nash 128/192	128	64*3=192	32
Nash 128/256	128	64*4=256	33

Количество выполняемых раундов в данных методах шифрования является наиболее важным фактором, обуславливающим быстроту, надежность, а также стойкость алгоритма. При проведении испытаний блочный алгоритм шифрования Nash показал себя более оптимизированным, так как число раундов выполнения шифра у него меньше, чем у алгоритма Speck. Для того чтобы повысить скорость выполнения и данного алгоритма, стоит воспользоваться особенностью алгоритма Speck, которая обеспечивает дополнительную гибкость выполнения. Чтобы оптимизировать скорость выполнения, необходимо заранее подсчитывать раундовые ключи, что позволит в некоторой мере увеличить скорость выполнения алгоритма и, в свою очередь, уменьшит исполняемое количество раундов.

Заключение. Увеличение программной и технической сложности коммуницирующих средств ограниченных возможностей, используемых в современном обществе, способствует развитию все более изощренных методов добывания конфиденциальной информации, включая бытовые приборы и технические устройства повседневного пользования. С другой стороны, этот процесс является двигателем для развития и реализации сложных и стойких криптографических алгоритмов.

Одними из наиболее ярких примеров такого рода алгоритмов могут служить такие легковесные алгоритмы, в которых выполняется большое количество простых преобразований, как блочные шифры Nash и Speck. Данные алгоритмы обладают высокой криптостойкостью, необходимой для обеспечения защиты информации.

Проведенный анализ данных алгоритмов показал, что блочный алгоритм шифрования Nash наиболее оптимизирован к работе, так как число раундов выполнения шифра меньше, чем у алгоритма Speck, что обеспечивает большую стойкость данного алгоритма при наименьшем числе исполняемых раундов.

Библиографический список

1. J. Nash, Letter to NSA, 1955, URL: www.nsa.gov/public_info/press_room/2012/nash_exhibit_shtm.

2. Microcontrollers-and-Processors. 2016 URL: www.nxp.com / products /microcntrollers-and-processors.

3. Interenet of Things. 2016 URL: http:// www.gemalto.com / iot.

4. McKay K., Bassham L., Turan M., Mouha N., DRAFT NISTIR 8114 Report on Lightweight Cryptography Computer Security Division Information Technology Laboratory NIST, 2016 URL: www.nist.gov.

5. D. Dinu, Y. Le Corre, D. Khovratovich, L. Perrin, J. Großschädl, A. Biryukov, Triathlon of Lightweight Block Ciphers for the Internet of Things, Report on Lightweight Cryptography Lightweight Cryptography Workshop 2015, Computer Security Division Information Technology Laboratory NIST, 2015 URL: www.nist.gov.

6. N. Mouha, B. Mennink, A. Van Herrewege, D. Watanabe, B. Preneel, I. Verbauwhede, Chaskey: a Lightweight MAC Algorithm for Microcontrollers, Lightweight Cryptography Workshop 2015, Cryptography Computer Security Division Information Technology Laboratory NIST, 2015 URL: www.nist.gov.

7. H. Tschofenig, M. Pegourie-Gonnard, Performance of State-of-the-Art Cryptography on ARM-based Microprocessors, NIST Lightweight Cryptography Workshop 2015.

8. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, L. Wingers, Simon and Speck: Block Ciphers for the Internet of Things, National Security, Agency 9800 Savage Road, Fort Meade, MD, 20755, USA, Memo 9 July 2015.

9. C. Shannon, Communication theory of secret systems, Bell Systems Techn. J. (1949) 656-715.

10. Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, Louis Wingers The Simon and Speck Families of Lightweight Block Ciphers.