ПЕРСПЕКТИВНЫЙ БЛОЧНЫЙ СИММЕТРИЧНЫЙ ШИФР, ОПТИМИЗИРОВАННЫЙ ДЛЯ АППАРАТНОЙ РЕАЛИЗАЦИИ

Олейников Р. В.[1], Киянчук Р. И.[2]
[1]ЗАО «Институт информационных технологий»
61166, г. Харьков, ул. Бакулина 12, E-mail: roliynykov@gmail.com
[2]Харьковский национальный университет радиоэлектроники
61166, г. Харьков, пр. Ленина 14,
каф. Безопасности информационных технологий, тел. (057) 702-14-25
E-mail: ruslan.kiyanchuk@gmail.com

Confidentiality of data transfer in modern information and telecommunication systems is usually provided by application of symmetric block ciphers. At the same time widely used block ciphers are generally designed for software implementation (AES) or special-purpose hardware modules (DES, TripleDES). Their system-on-a-chip implementations with strict constraints to the number of logic gates and energy consumption are quite ineffective. Consequently, such systems require a new generation cryptographic algorithms. Our paper examines requirements for symmetric block ciphers designed for lightweight hardware implementations, describes the perspective cipher specifications, its properties and comparison with already existing ciphers.

Массовая компьютеризация, активное использование электронных устройств в повседневной жизни и повсеместный доступ к Интернет открывают множество новых возможностей, но являются причиной возникновения значительных рисков, связанных с обработкой конфиденциальной информации. Финансовые приложения, беспроводные сенсорные сети, использование RFID-меток для учёта и в системах автоматического сбора пошлины требуют безопасной обработки и обмена данными с обеспечением целостности и конфиденциальности [3].

Большинство современных блочных симметричных шифров (БСШ) ориентированы на программную реализацию, а при аппаратной реализации требуют значительных ресурсов (количества вентилей, площади на кристалле, частоты процессора и энергопотребления) для получения приемлемого уровня производительности. Ограниченные ресурсы встраиваемых устройств не позволяют эффективно применять существующие надёжные шифры. По этой причине возникла потребность в разработке перспективных БСШ, ориентированных на эффективную аппаратную реализацию и гарантирующих приемлемый уровень безопасности данных [2]. Одной из последних разработок в данной области является шифр PRESENT, рассчитанный на аппаратную реализацию в устройствах с жёстко ограниченными ресурсами.

1 Описание шифра PRESENT

Основными требованиями к шифру PRESENT являются удовлетворительная безопасность, эффективность реализации и простота. Его возможно применять в условиях очень ограниченного аппаратного обеспечения, где использование существующих блочных симметричных шифров, таких как AES, невозможно.

1.1 Требования к перспективным блочным шифрам для аппаратной реализации

Разработчики PRESENT поставили перед шифром следующие требования [1]:

1. Шифр рассчитан на аппаратную реализацию.
2. Приложения требуют лишь удовлетворительный уровень безопасности.
3. Приложениям с малой степени вероятности понадобится шифрование больших объёмов данных. Реализация шифра может быть оптимизирована на компактность кода или производительность без ущерба стойкости и применимости.
4. В некоторых устройствах ключ шифрования фиксирован и встроен на этапе разработки. В таких устройствах нету необходимости в процедуре разворачивания ключа, следовательно, исключается множество атак на функцию выработки раундовых ключей.

5. Следом за безопасностью, основным ограничением служит размер аппаратной реализации шифра. Третьей важной метрикой является максимальное и среднее потребление энергии, а также требования к производительности.

6. В приложениях, требующих эффективного использования пространства на кристалле, блочный шифр часто необходим только в режиме шифрования, что сокращает накладные расходы на реализацию.

Криптоалгоритм PRESENT – блочный симметричный шифр с размером блока равным 64-м битам и размером ключа в 80 бит. Спецификация также описывает вариант с размером ключа в 128 бит. Аппаратная реализация PRESENT в режиме шифрования и расшифрования остаётся более компактной, чем AES только в режиме ифрования. Подключи могут вычисляться параллельно во время самой процедуры шифрования. PRESENT представляет собой SPN-структуру и состоит из 31 цикла. Последний, 32-й раундовый ключ используется для отбеливания после основной процедуры шифрования. Основной цикл состоит из линейного битового перемешивания и нелинейного слоя замены. Нелинейный слой использует 4-битовую подстановку, которая применяется 16 раз для всего блока в каждом цикле. Данные складываются с ключем по модулю 2.

1.2 Слой замен

В качестве нелинейного слоя используется одна 4-х битная подстановка $F_2^4 \to F_2^4$. Это прямое последствие жёстких требований к эффективности и компактности реализации. Симметричная 8-битная подстановка требует около 1000 вентильных эквивалентов (GE), столько же требует полная реализация шифра PRESENT [5]. Подстановка $F_2^6 \to F_2^4$ требует 128 GE, а подстановка $F_2^4 \to F_2^4$ – 21 - 39 GE. Для того, чтобы достигнуть лавинный эффект, на подстановку накладываются дополнительные ограничения. Обозначим коэффициент Фурье, как

$$S_b^W(a) = \sum_{x \in F_2^4} (-1)^{<b,S(x)>+<a,x>}. \quad (1)$$

Тогда подстановка PRESENT (табл. 1) удовлетворяет следующим условиям:

1. для любой фиксированной ненулевой входной разницы $\Delta_I \in F_2^4$ и любой фиксированной ненулевой выходной разницы $\Delta_O \in F_2^4$ требуется

$$\#\left\{x \in F_2^4 | S(x) + S(x + \Delta_I) = \Delta_O\right\} \le 4; \quad (2)$$

2. для любой фиксированной ненулевой входной разницы $\Delta_I \in F_2^4$ и любой фиксированной выходной разности $\Delta_O \in F_2^4$ таких, что $wt(\Delta_I) = wt(\Delta_O) = 1$, имеем

$$x \in F_2^4 | S(x) + S(x + \Delta_I) = \Delta_O = 0; \quad (3)$$

3. для всех ненулевых $a \in F_2^4$ и всех ненулевых $b \in F_2^4$ выполняется $\left|S_b^W(a)\right| \le 8$;

4. для всех $a \in F_2^4$ и всех ненулевых $b \in F_2^4$ при $wt(a) = wt(b) = 1$ имеем $\left|S_b^W(a)\right| \le 4$.

Таблица 1: Подстановка PRESENT

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Из всего множества подстановок, удовлетворяющих условия, выбрана была та, аппаратная реализация которой требует наименьшее количество вентилей [1].

Максимальная вероятность выполнения дифференциальной характеристики для подстановки PRESENT равна 2^{-2}, следовательно для 25 циклов шифра данная вероятность будет составлять 2^{-100}. Максимальное отклонение линейной характеристики составляет $1/4$. Следовательно, вероятность выполнения линейного уравнения также равна $1/2 - 1/4 = 1/4$. При линейном криптоанализе для аппроксимирования 28 циклов

шифра, необходимо обладать 2^{84} парами сообщение/шифротекст, что превышает множество возможных входных блоков PRESENT.

1.3 Слой перемешивания

Главным аспектом при разработке слоя перемешивания было количество необходимых для реализации вентилей. Линейное битовое перемешивание не требует транзисторов в аппаратной реализации и хранения констант, поэтому может быть реализовано лишь разводкой контактов. К примеру, МДР-преобразование использующееся в AES-подобных шифрах при эффективной реализации требует хранение предварительно вычисленной таблицы степеней и таблицы логарифмов, а вычисление каждого элемента состоит из сложения и двух подстановок. Перемешивание PRESENT функционально можно описать с помощью формулы (4).

$$P(i) = \begin{cases} i \cdot 16 \bmod 63, & i \in 0, \ldots, 62 \\ 63, & i = 63. \end{cases} \quad (4)$$

1.4 Разворачивание ключей

Мастер-ключ хранится в регистре K и представлен последовательностью бит $k_{79}k_{78}\ldots k_0$. На каждом раунде подключём являются 64 старших (левых) бита регистра ключа. После выделения подключа, регистр обновляется по следующему закону:

1. $[k_{79}k_{78}k_1k_0] = [k_{18}k_{17}k_{20}k_{19}]$
2. $[K_{79}k_{78}k_{77}k_{76}] = S[k_{79}k_{78}k_{77}k_{76}]$
3. $[k_{19}k_{18}k_{17}k_{16}k_{15}] = [k_{19}k_{18}k_{17}k_{16}k_{15} \oplus round\_counter]$

Стойкость шифра зависит от надёжности схемы разворачивания ключа. В алгоритме PRESENT счётчик циклов складывается по модулю 2 с битами регистра ключа для уменьшения зависимостей между раундовыми ключами. Для внесения нелинейности в формирование подключей при изменении состояния регистра ключа часть битов проходят замену по подстановке (табл. 1). К 21-му циклу все биты ключевого регистра являются нелинейной функцией от мастер-ключа, а после 21-го цикла каждый бит подключа зависит минимум от 4-х бит мастер-ключа.

1.5 Расшифрование

Для расшифрования криптограмм используются аналогичные преобразования, обратные оригинальным. Раундовые ключи подаются в шифр в том же порядке, что и при шифровании.

2 Характеристики аппаратной реализации шифра PRESENT

Авторы шифра рассматривали несколько целевых платформ для реализации: от интегральных схем ASIC и более гибких FPGA до чисто программных реализаций для 4-, 8-, 16- и 32-битных процессоров. Так как наиболее высокопроизводительной и миниатюрной является реализация ASIC, рассмотрим её подробнее. Результаты измерений статистики ASIC реализации шифра PRESENT по 180-нанометровому технологическому процессу с обработкой 4 бит за такт, представлена ниже.

Площадь: 1075 GE – требования к занимаемой площади измеряются в $нм^2$ и сильно зависят от технологического процесса и библиотеки стандартных ячеек. Для независимого сравнения требований принято указывать площадь в вентильных эквивалентах [GE]. Один вентильный эквивалент равен площади, занимаемой одним И-НЕ элементом с наименьшим номинальным током. Площадь в вентильных эквивалентах рассчитывается делением общей площади реализации на площадь И-НЕ элемента.

Производительность: 11.7 Kbps – скорость формирования нового результата относительно времени. Количество сформированных битов делится на затраченное время и представляется в битах за секунду [bps]. Эффективность: 10.89 $\frac{bps}{GE}$ – отношение площади реализации к производительности. Используется для измерения эффективности

аппаратного обеспечения. Измеряется в вентильных эквивалентах на бит в секунду $\left[\frac{GE}{bps}\right]$.

3 Сравнение PRESENT, ГОСТ 28147-89 и AES

Учитывая многолетний анализ и распространённость шифров AES и ГОСТ, актуально сравнение с ними нового шифра PRESENT. Сравнение шифров приведено в таблице 2. Следует отметить, что рассмотренная реализация PRESENT рассчитана на 4-битный процессор (обрабатывает 4 бита за такт), тогда как AES и ГОСТ не способны работать на 4-разрядных процессорах.

Таблица 2: Сравнение производительности PRESENT, AES и ГОСТ 28147-89

Шифр	Ключ, бит	Блок, бит	Производ., Кб/с	Площадь, GE	Эффектив., $\frac{bps}{GE}$
ГОСТ	256	64	14	800	17.5
AES	128	128	80	3100	25.81
PRESENT	64	80	11.7	1075	10.89

4 Выводы

Шифр PRESENT разрабатывался специально для аппаратной реализации и работы на устройствах с очень ограниченными ресурсами, таких как RFID-метки, где достаточно обеспечить удовлетворительный уровень безопасности для малых объёмов данных. Поэтому он неприменим для шифрования больших объёмов данных, требующих высокий уровень безопасности. Отсутствие сложных операций (умножение, модульное сложение) и таблиц предвычислений обеспечивают компактность аппаратной реализации, требование меньшей площади на кристалле, а следовательно – дешёвую себестоимость. Однако сравнение шифров PRESENT, AES и ГОСТ 28147-89 показало, что последний также хорошо показывает себя в сфере облегчённой криптографии и превосходит PRESENT по компактности реализации [4]. При модификации алгоритма ГОСТ, а именно замены восьми разных подстановок одной, аппаратная реализация будет занимать лишь 651 вентильных эквивалентов. К тому же в отличие от PRESENT, шифр ГОСТ 28147-89 испытан временем и хорошо проанализирован, существует множество его реализаций.

Учитывая подачу шифра ГОСТ на международный стандарт шифрования, актуальны дальнейшие исследования возможности применения шифра на устройствах с ограниченными ресурсами (энергопотребление, устойчивость к атакам по сторонним каналам). В свою очередь PRESENT может функционировать на 4-битных процессорах и является более гибким в реализации, что позволяет эффективно применять его на устройствах разной архитектуры.

Литература:

1. A. Bogdanov and C. Paar and A. Poschmann and others. PRESENT: An Ultra-Lightweight Block Cipher. *Proceedings of CHES 2007*. Springer-Verlag, 2007.

2. *A Survey of Lightweight-Cryptography Implementations*, 2007. Copublished by the IEEE CS and the IEEE CASS.

3. Axel Poschmann. Lightweight Cryptography From an Engineers Perspective. Technical report, Horst-Görtz Institut für IT Sicherheit, 2007.

4. Poschmann, Axel and Ling, San and Wang, Huaxiong. 256 bit standardized crypto for 650 GE: GOST revisited. *Proceedings of the 12th international conference on Cryptographic hardware and embedded systems* in CHES'10, pages 219--233, Berlin, Heidelberg, 2010. Springer-Verlag.

5. C. Rolfes and A. Poschmann and C. Paar. Security for 1000 Gate Equivalents. *ecrypt workshop SECSI - Secure Component and System Identification*. -, 2008.