УДК 519.719.2 + 004.056 Вестник УрФО № 4(30) / 2018, с. 27–30

Бондакова О. С., Зязин В. П.

DOI: 10.14529/secur180404

О ПЕРВИЧНОЙ ОЦЕНКЕ ВЕРОЯТНОСТИ ВОЗНИКНОВЕНИЯ КОЛЛИЗИИ ДЛЯ УМЕНЬШЕННОГО ВАРИАНТА ХЭШ-ФУНКЦИИ «СТРИБОГ»

В статье обоснована актуальность исследований в направлении синтеза lightweight криптосхем, с целью их использования в технологиях IIoT и IoT. И необходимость проведения криптографического анализа таких «облегченных» криптопримитивов.

Ключевые слова: *уменьшенная хэш-функция «Стрибог», разностный криптоанализ хэш-функций, криптография в IIoT.*

Bondakova O. S., Ziazin V. P.

ABOUT THE PRIMARY ESTIMATION OF THE PROBABILITY OF THE COLLISION FOR A REDUCED VARIANT OF THE "STRIBOG" HASH-FUNCTION

The article proves the relevance of research in the direction of synthesis of lightweight cryptocircuits, with the aim of using them in IIoT and IoT technologies. And the need for cryptographic analysis of such "lightweight" cryptoprimitives.

Keywords: *reduced hash function "Stribog", difference cryptanalysis of hash functions, cryptography in IIoT.*

На XXIII международной научно-практической конференции «Комплексная защита информации» была представлена хэш-функция с размером хэш-кода 64 бит [1], в качестве возможного механизма защиты информации, в краткосрочном периоде времени. Малый размер блока позволяет сделать реализацию хэш-функции быстрой и не требующей больших ресурсов, что является её преимуществом для применения в устройствах IIoT. Однако определение оптимального количества раундов в ней является важной

задачей как со стороны криптографических качеств функции, так и её быстродействия. Эта задача требует проведение исследования стойкости хэш-функции к различным атакам

Одной из важных характеристик криптографической хэш-функции, является низкая вероятность возникновения коллизии. С учетом, предполагаемой области применения исследуемой хэш-функции, наибольший интерес вызывают коллизии возникающий для сообщений отличающихся в определенных позициях. На основании этого было принято решение о получении первичной оценки стойкости хэш-функции [1] по средствам применения к ней разностного метода криптографического анализа.

Кратко опишем основные особенности анализируемого примитива. Хэш-функция, описанная в [1], основана на модифицированной МД-конструкции [1], общий вид которой можно представить в виде рисунка 1.

Где h_1 – значение, получаемое применением одношаговой функции сжатия h к блоку сообщения m_1, N_1 – количество захэшированных до этого бит, Σ – результат сложения всех захэшированных блоков сообщения в кольце $Z_{2^{64}}$. Одношаговая функция сжатия h построена по схеме Миягучи-Пренеля:

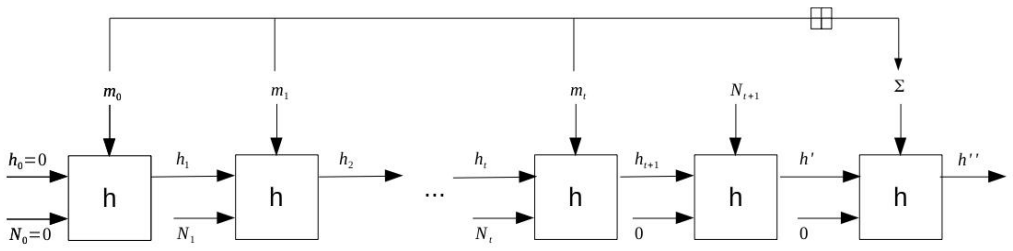

Рис. 1. Общая структура исследуемой хэш-функции

$$h(m_i) = E(m_i, h_i \oplus N_i) \oplus m_i \oplus h_i.$$

Где $E(m_i, h_i \oplus N_i)$ - алгоритм блочного шифрования (внутренний блочный шифр). В качестве внутреннего блочного шифра используется XSPL-шифр.

Известно, что стойкость к коллизиям МД-конструкции и её модификаций, зависит от стойкости к коллизиям, используемой в них одношаговой функции сжатия. Поэтому представляется возможность, сведения анализа свойств функции к исследованию свойств внутреннего блочного шифра.

Разностный метод криптографического анализа является одним из классических методов криптоанализа блочных шифров [2]. Основные подходы и принципы, которого, были также описаны в работе [3]. Для нахождения коллизии для функции сжатия, необходимо построить дифференциальный путь, у которого разность открытых текстов равна разности, соответсвующих им, шифртекстов. Пример такого дифференциального пути для открытых текстов, различающихся только в первом полубайте, приведен на рис.2.

Посредством вычислительного эксперимента, были построены все возможные виды дифференциальных путей для размера блока равного 64 битам. Здесь и далее под видом дифференциального пути подразумевается расположение активных полубайт в разностях, входящих в него.

Для этого использовались характеристики параметров хэш-функции, приведенные в [1]. Из [1] известно, что при умножении вектора из 4-х полубайт на матрицу в линейном преобразовании, суммарный вес (количество активных полубайт) входного и результирующего векторов не должен быть меньше 5. Поэтому при построении всех видов дифференциальных путей после применения преобразования L рассматривались вектора всех весов, в которые могли перейти исходные вектора. Из полученных векторов составлялись все возможные комбинации, которые и образовывают блоки на выходе линейного преобразования L. Пример дифференциального пути на 4 раунда представлен на рисунке 2.

Для оценки вероятности каждого вида дифференциального пути, было вычислено $P=(\rho_\pi)^k$, где - количество активных S-боксов, входящих в путь. Также известно [1], что $\rho_\pi = \frac{1}{4}$ есть максимально возможная вероятность перехода одного полубайта разности в некоторый другой для выбранной подстановки. Пара сообщений, удовлетворяющая дифференциальному пути может быть найден, если вероятность пути $P < \frac{1}{2^n}$, в случае исследуемой функции n=64.

Поскольку для любого дифференциального пути можно вычислить его вероятность, будем считать эту вероятность вероятностью возникновения коллизия для сообщений, отличающихся в соответствующих позициях.

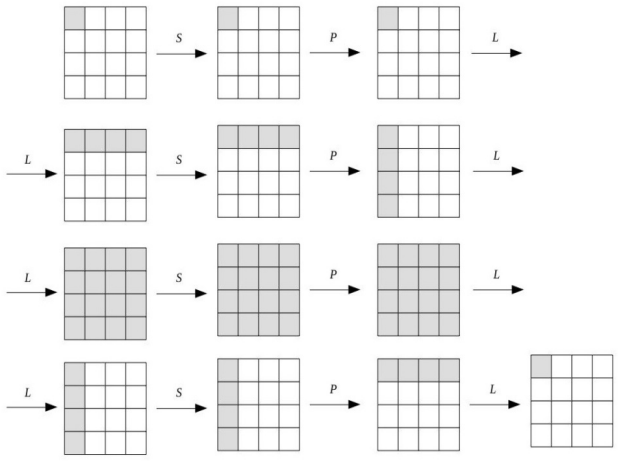

Рис. 2. Пример дифференциального пути на 4 раунда

Полученные в результате вычислительного эксперимента данные представлены в таблице 1. Каждый вид дифференциального пути охарактеризуем тремя параметрами:

1) количество активных полубайт в разности открытых текстов.

2) количество раундов, на которые «протянут» путь.

3) вероятность пути.

В соответствии со значениями этих параметров все виды дифференциальных путей разбиты на группы. Первый столбец таблицы содержит все возможные значения первого параметра от 1 до 16. В каждой строке содержится информация по всем видам путей имеющих соответственное значение первого параметра. Каждый из остальных столбцов отвечает возможным значениям второго параметра. В ячейках записаны значения вероятностей для наиболее крупных групп путей с соответствующими первым и вторым параметрами. В скобках указаны их примерные доли среди видов путей с таким же значением первого параметра.

Жирным шрифтом выделены значения вероятностей для групп путей, имеющих самую большую долю среди других групп с таким же значением первого параметра.

На основании данных таблицы можно сделать вывод, что подход синтеза хэш-функции в [1], позволяет с большой долей вероятности достичь хороших криптографических качеств примитива, имеющего размер хэш-кода 64 бит. Поскольку основная большая часть дифференциальных путей имеют оценку сверху вероятности , или достаточно близкую к ней.

Невозможно построить дифференциальные пути более на 4 раунда, в не зависимости от конкретных значений параметров преобразований, если выполнены требования к параметрам преобразований [1].

В дальнейшем планируется продолжить вычислительные эксперименты и убедится, что при фиксации параметров преобразовании хэш-функции, коллизий не возникает, либо они имеют вероятность близкую к $\frac{1}{2^{64}}$.

Количество активных полубайт в разности открытых текстов	**1 раунд**	**2 раунд**	**3 раунд**	**4 раунд**
1	–	–	–	**2^{-50} (100%)**
2	–	–	–	**2^{-62} (77%)**
3	–	–	2^{-46}	**2^{-62} (83%)**
4	–	2^{-40}	2^{-52}	**2^{-62} (76%)**
5	–	–	2^{-52}	**2^{-62} (62%)**
6	–	2^{-42}	**2^{-60} (36%)**	2^{-62}
7	2^{-16}	2^{-42}	**2^{-60} (38%)**	2^{-62}
8	2^{-18}	2^{-44}	**2^{-60} (39%)**	2^{-62}
9	2^{-20}	2^{-44}	**2^{-62} (66%)**	2^{-62}
10	2^{-22}	2^{-44}	**2^{-62} (89%)**	2^{-62}
11	2^{-24}	2^{-46}	**2^{-62} (96%)**	2^{-62}
12	2^{-24}	2^{-46}	**2^{-60} (34%)**	2^{-62}
13	2^{-26}	2^{-46}	**2^{-62} (39%)**	2^{-62}
14	2^{-28}	2^{-48}	**2^{-62} (49%)**	2^{-62}
15	2^{-30}	2^{-48}	**2^{-62} (65%)**	2^{-62}
16	2^{-32}	2^{-50}	**2^{-62} (88%)**	2^{-60}

Литература

1. Бондакова О. С. «Уменьшенный вариант хэш-функции «Стрибог» и его свойства» - XXIII научно-практическая конференция «Комплексная защита информации» // https://kzi.su/

2. BihamE., ShamirA. Differential Cryptanalysis of DES-ike Cryptosystems (Extended Abstract). Lect. Note. Comp. Sci,. 1991.

3. Kiryukhin V., "Exact Maximum Expected Differential and Linear Probability for 2-round Kuznyechik", 7th Workshop on Current Trends in Cryptology (CTCrypt 2018) ,May 28-30, 2018.

References

1. Bondakova O. S. «Umen'shennyj variant hehsh-funkcii «Stribog» i ego svojstva» - XXIII nauchno-prakticheskaya konferenciya «Kompleksnaya zashchita informacii» // https://kzi.su/

2. BihamE., ShamirA. Differential Cryptanalysis of DES-ike Cryptosystems (Extended Abstract). Lect. Note. Comp. Sci,. 1991.

3. Kiryukhin V., "Exact Maximum Expected Differential and Linear Probability for 2-round Kuznyechik", 7th Workshop on Current Trends in Cryptology (CTCrypt 2018) ,May 28-30, 2018.

БОНДАКОВА Ольга Сергеевна, студент кафедры Информационной безопасности Института кибернетики ФГБОУ ВО «МИРЭА – Российский технологический университет». Россия, 119454 г. Москва, проспект Вернадского, дом 78. E-mail: o.bondakova@mail.ru

ЗЯЗИН Валентин Петрович, профессор кафедры информационной безопасности, Института Кибернетики ФГБОУ ВО «МИРЭА – Российский технологический университет». 119454, г. Москва, проспект Вернадского, 78. E-mail: zval47@yandex.ru

BONDAKOVA Olga, student of the Information Security Department of the Institute of Cybernetics, FSBEI of HE "MIREA - Russian Technological University". Russia, 119454, Moscow, Vernadskogo Avenue, Building 78. E-mail: o.bondakova@mail.ru

ZIAZIN Valentin, professor at Information Security department of Cybernetics Institute Federal State Budgetary Educational Institution of Higher Education "MIREA - Russian Technological University". 119454, Moscow, Vernadskogo Avenue, Building 78. E-mail: zval47@yandex.ru