УДК 621.3.06

ДИФФЕРЕНЦИАЛЬНЫЙ КРИПТОАНАЛИЗ БЛОЧНОГО ARX-ШИФРА «КИПАРИС-256»

Р. Ю. ЕЛИСЕЕВ, М. Ю. РОДИНКО, Р. В. ОЛЕЙНИКОВ

В статье представлены результаты дифференциального криптоанализа симметричного блочного шифра «Кипарис-256», выполненного с применением ряда методов, в частности, с помощью алгоритма Мацуи и использованием частичных таблиц распределения разностей. В ходе исследований был найден ряд дифференциальных характеристик вплоть до пяти циклов шифрования. Кроме того, был обнаружен ряд характеристик с вероятностями от 2^{-2} до 2^{-5}, входы и выходы которых имеют малый вес Хэмминга.

Ключевые слова: малоресурсная криптография, блочный симметричный шифр, дифференциальный криптоанализ, дифференциальная характеристика.

ВВЕДЕНИЕ

Метод построения симметричных криптографических преобразований на основе ARX (Addition-Rotation-XOR) конструкций [1] привлекает все большее внимание разработчиков. С одной стороны, метод дает возможность создавать очень простые в описании и реализации преобразования. С другой стороны, возникают проблемы при попытках криптоанализа ARX-преобразования классическими методами.

На сегодняшний день ARX-шифры активно исследуются как с точки зрения поиска универсальных алгоритмов и подходов к криптоанализу [2], так и построения примитивов с заданными криптографическими свойствами [1]. Тем не менее, даже при исследовании произвольного алгоритма на основе ARX преобразований все еще сложно однозначно говорить о доказуемой криптостойкости: почти под каждый алгоритм необходимо разрабатывать свою доказательную базу.

Последнее связано с тем, что большая часть существующей доказательной базы для блочных шифров создана для алгоритмов, чья цикловая функция основана на чередовании линейных и нелинейных преобразований с известными математическими свойствами [3]. Такие шифры хорошо зарекомендовали себя с точки зрения криптостойкости и эффективности реализации на широком спектре платформ и элементных баз. Известными примерами подобных шифров являются DES [4], [5], ГОСТ 28147-89 [6], Camellia [7], AES [8], Калина [9]. Все они имеют доказательную стойкость, однако достаточно сложны в оптимизированной программной реализации и сильно зависят от качества (и главное наличия) кэширования данных на уровне процессора для хранения предварительно рассчитанных Т-таблиц [10].

В связи с вышесказанным, малоресурсные алгоритмы, в частности, основанные на ARX, привлекают все больше внимания разработчиков. В Украине разработан малоресурсный блочный шифр «Кипарис», обеспечивающий компактную реализацию и высокую скорость преобразований на различных платформах [11].

Целью статьи является поиск дифференциальных характеристик в перспективном блочном ARX-шифре «Кипарис-256» [11] и изучение принципов распространения дифференциальных разностей через циклы шифрования. Несмотря на малоресурсный дизайн (с точки зрения программной реализации на широком спектре платформ общего назначения), алгоритм использует нелинейные преобразования с достаточно большими размерами входов-выходов (сложение по модулю 2^{32} в 256-битной версии), что заметно осложняет его исследование классическими методами и алгоритмами дифференциального криптоанализа, ориентированными на SPN-архитектуру цикловой функции с небольшими табличными нелинейными преобразованиями.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Дифференциальный криптоанализ

Дифференциальный криптоанализ [4] – статистическая атака на симметричные криптопреобразования, изучающая изменения разности между двумя парами тестов по мере их прохождения через компоненты преобразования.

При анализе шифра рассматриваются, в первую очередь, дифференциальные пути (характеристики), т.к. на сегодняшний день только характеристики могут быть эффективно вычислены для современных шифров.

Под дифференциальной характеристикой понимают набор разностей между двумя текстами в определенные моменты вычислений (на входе, выходе и между циклами, например), в то время как дифференциал состоит лишь из пары входной разности и выходной. В общем случае один дифференциал состоит из множества дифференциальных характеристик, сумма вероятностей которых и составляет его вероятность.

1.2. Описание блочного шифра «Кипарис»

Алгоритм шифрования «Кипарис» [11] выполняет преобразования блоков данных размером 256 и 512 бит с использованием ключа шифрования такой же

длины. Длина ключа совпадает с размером блока. Таким образом, алгоритм поддерживает два варианта шифрования: «Кипарис-256» и «Кипарис-512».

К входным данным алгоритма принадлежат открытый текст и ключ шифрования, представленные в виде строк длиной $8 \times l$ бит. С исходными данными алгоритма принадлежит шифртекст, представленный в виде строки длиной $8 \times l$ бит.

Для шифра «Кипарис-256» $l = 32$, количество циклов шифрования $N_r = 10$ для шифра «Кипарис-512» $l = 64$, количество циклов шифрования $N_r = 14$.

«Кипарис-256» ориентирован на использование на 32-битных платформах, «Кипарис-512» – на применение на 64-битных платформах.

На вход процедуры шифрование подается блок открытого текста в виде одномерного массива из восьми l-битных слов (word) и цикловые ключи. После окончания процедуры шифрование полученный шифртекст представляется в виде последовательности l-битных слов.

В основе шифра «Кипарис» лежит сеть Фейстеля, один цикл которой изображен на рис. 1.

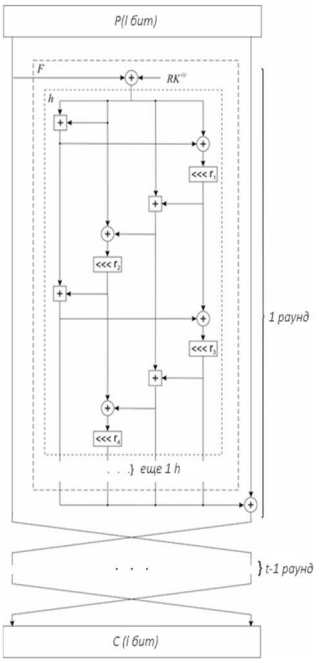

Рис. 1. Графическое представление шифра «Кипарис»

Блок открытого текста делится на два подблока длиной $4 \times l$ бит. Левый подблок поступает на вход циклового преобразования F.

Сначала подблок составляется по модулю 2 с цикловым ключом, а затем дважды обрабатывается функцией HalfRound (обозначена h на рис. 1).

На вход функции HalfRound подается четыре l-битных слова (l_0, l_1, l_2, l_3). Значения циклических сдвигов (rot0, rot1, rot2, rot3) зависят от длины блока и практически равны:

1) для шифра «Кипарис-256» $(\text{rot}_0, \text{rot}_1, \text{rot}_2, \text{rot}_3) = (16,12,8,7)$.

2) для шифра «Кипарис-512» $(\text{rot}_0, \text{rot}_1, \text{rot}_2, \text{rot}_3) = (32,24,16,15)$.

Для простоты последующего анализа в одном применении функции HalfRound можно выделить 4 применения более простой «элементарной» функции (рис. 2):

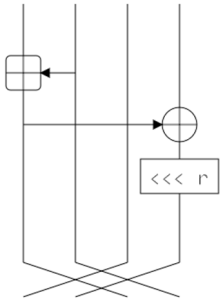

Рис. 2. Элементарный цикл «Кипарис-256»

Такое изображение позволяет упростить анализ цикловой функции благодаря тому, что каждый из таких повторяющихся циклов содержит в себе лишь одну нелинейную операцию.

1.3. Анализ модульного сложения

Вероятность преобразования разности по модулю 2 (xor difference probability) представляет собой вероятность того, что при входных разностях α, β на выходе сумматора окажется разность γ. Реализация на практике может быть построена на основе битовых преобразований, что позволяет существенно ускорить и упростить процесс расчетов [12].

$$XDP^{+}(\alpha,\beta\to\gamma)=\begin{cases}0 & if \quad eq(\alpha<<1,\beta<<1,\gamma<<1)\wedge \\ & \quad \wedge(\alpha\oplus\beta\oplus\gamma\oplus(\alpha<<1))\neq 0\\ 2^{-w_h\left(\neg eq(\alpha,\beta,\gamma)\wedge mask(n-1)\right)} & else,\end{cases}$$

где $eq(\alpha, \beta, \gamma)$ – функция побитового сравнения, возвращающая «1» в случае, если все 3 бита на соответствующих позициях равны и «0» в противном случае; w_h – вес Хемминга или количество ненулевых бит в слове, $mask(n)$ – функция, возвращающая слово из n единиц в младших позициях, остальные заполняются нулями.

1.4. Частичная таблица распределения разностей

Большинство современных стандартизированных и используемых на практике блочных шифров основаны на биективных блоках подстановки 8×8 бит или 4×4 бит. Такие размеры удобны не только в различных видах реализации, но и для дифференциального криптоанализа, так как позволяют построить полную таблицу распределения разностей – отображение пары входная-выходная разность в вероятность такого перехода по всем возможным наборам данных.

Общий размер полной таблицы составляет 2^{m+n} элементов, где m – количество входов S-блока, а n – количество выходов.

В случае же ARX преобразований, где обычно используются сумматоры достаточно большой разрядности (в случае «Кипарис-256» – 32-битовые), размеры полных таблиц становятся слишком большими для современных компьютеров, а время их построения – не практичным.

В связи с этим был предложен подход [13] на основе т.н. неполных таблиц распределения разностей (англ. partial difference distribution table, pDDT), которые включают в себя не все множество возможных входов-выходов, а только ту его часть, вероятность элементов которой превышает определенный заданный предел. Такие таблицы содержат гораздо меньшее количество элементов и как следствие легко могут быть использованы для «крупных» операций. Более того, в случае сложения (и некоторых других операций), по мере увеличения разрядности общая вероятность монотонно убывает, что приводит к возможности достаточно эффективно отсекать бесперспективные (с точки зрения вероятности преобразования) наборы разностей на ранних этапах.

1.5. Частичная таблица распределения разностей для сложения

Алгоритм построения неполной таблицы распределения разностей для сложения представлен на рис. 3. Основная идея состоит в рекурсивном поиске в глубину всех возможных комбинаций входных-выходных значений, которые собираются, бит за битом. На каждом шаге осуществляется проверка текущей вероятности и если она ниже заданного граничного значения – поиск в поддереве не производится, так как вероятность не может увеличиться.

1.6. Алгоритм Мацуи

В 1994 был предложен алгоритм [14], часто называемый в литературе алгоритмом Мацуи (англ. Matsui), предназначенный для эффективного поиска лучших дифференциальных путей или линейных аппроксимаций для DES (применим в неизменном виде к любой сети Фейстеля с двумя ветвями). Тем не менее, в общем случае алгоритм не гарантирует, что найденная характеристика или аппроксимация будет иметь наибольшую возможную вероятность.

```
Procedure compute_pddt (n, p_theshold, k, α_k, β_k, γ_k) :
  If n == k:
      Add (α_k, β_k, γ_k) to D
      Return
  For x,y,z ∈ {0, 1}:
      α_{k+1} ← x|α_k
      β_{k+1} ← y|β_k
      γ_{k+1} ← z|γ_k
      p_{k+1} = xdp+(α, β, γ)
      If p_{k+1} ≥ p_threshold :
          compute_pddt(n, p_theshold, k + 1, α_{k+1}, β_{k+1}, γ_{k+1})
```

Рис. 3. Алгоритм построения pDDT для сложения

Идея заключается в рекурсивном поиске на заданном количестве циклов n. Входными данными являются известные лучшие вероятности первых $n-1$ циклов, обозначаемые как $B_1, B_2, \ldots, B_{n-1}$, а также предположительная вероятность цикла n, обозначаемая как $\underline{B_n}$. В результате своей работы алгоритм возвращает B_n. Важным условием является выполнение $\underline{B_n} \le B_n$, так же $\underline{B_n}$ должен быть как можно ближе к B_n, чтобы ускорить выполнение алгоритма.

Псевдокоды этапов рекурсивного поиска отображены в алгоритмах 1–4. При окончании каждого из них управление передается предыдущему. После окончания всех итераций первого шага переменная $\underline{B_n}$ содержит лучшую найденную вероятность дифференциального пути или линейной аппроксимации (нотация ориентирована на поиск дифференциальных характеристик).

Алгоритм 1. Первый этап поиска.

- Выполнить для всех ΔX_1:
  - $p_1 = \max\limits_{\Delta Y}(\Delta X_1, \Delta Y)$;
  - если $[p_1, B_{n-1}] \ge \underline{B_n}$:
    - переход на второй этап.

Алгоритм 2. Второй этап поиска.

- Для всех возможных ΔX_2 и ΔY_2:
  - $p_2 = (\Delta X_2, \Delta Y_2)$;
  - если $[p_1, p_2, B_{n-2}] \ge \underline{B_n}$:
    - переход на третий этап.

Алгоритм 3. i-й этап поиска, где $3 \le i \le n-1$

- Для всех ΔY_i:
  - $\Delta X_i = \Delta X_{i-2} \oplus \Delta Y_{i-1}$;
  - $p_i = (\Delta X_i, \Delta Y_i)$;
  - если $[p_1, p_2, \ldots, p_i, B_{n-i}] \ge \underline{B_n}$:
    - переход на $i+1$ этап.

Алгоритм 4. Последний этап поиска

- $\Delta X_n = \Delta X_{n-2} \oplus \Delta Y_{n-1}$;
- $p_n = (\Delta X_n, \Delta Y)$;
- если $[p_1, p_2, \ldots, p_n] \ge \underline{B_n}$:
  - $\underline{B_n} = [p_1, p_2, \ldots, p_n]$.

Повышение быстродействия в алгоритме достигается благодаря отсечению на каждом из шагов разностей, на основе которых невозможно построить дифференциальный путь не хуже текущего лучшего известного. Именно с этим связаны необходимость выбирать начальную оценку максимально близкой к лучшей возможной вероятности, но не большей ее ($\underline{B_n} \le B_n$). Стоит также заметить, что оценка вероятности конечной характеристики на каждом из этапов обладает погрешностью, поэтому в общем случае

невозможно доказать, что результаты будут действительно оптимальными.

2. МЕТОДЫ ИССЛЕДОВАНИЙ

2.1. Основной анализ на основе алгоритма Мацуи и pDDT

Дифференциальный криптоанализ блочного ARX-шифра «Кипарис-256» состоит из следующих шагов:

1) построение pDDT для операции сложения;
2) построение pDDT для «элементарного» цикла;
3) построение pDDT для цикловой функции;
4) использование pDDT цикловой функции в алгоритме Мацуи для поиска оптимальных дифференциальных характеристик через несколько циклов.

2.2. Дополнительный анализ на основе SMT-решателя

Также, независимо проводились исследования с использованием SMT-решателя Z3 [15]. С его помощью производился:

1) поиск дополнительных маршрутов прохождения дифференциальных путей через цикловую функцию в алгоритме Мацуи. Маршруты рассчитывались таким образом, чтобы «выводить» алгоритм на входы предварительно подготовленной pDDT цикловой функции;

2) поиск одноцикловых характеристик с фиксированной вероятностью.

2.3. Частичная таблица распределения разностей сложения

Частичная таблица распределения разностей сложения строилась по приведенному выше алгоритму и для ускорения процесса не включает записи с вероятностями ниже 2^{-3}. Такое граничное значение позволяет, с одной стороны, очень эффективно рассчитывать и хранить в оперативной памяти таблицу, с другой же стороны дает очень высокие погрешности при поиске дифференциальных характеристик, т.к. большая часть возможных дифференциальных переходов не принимается во внимание.

pDDT для «элементарного» цикла (рис.2) легко выводится из таблицы сложения, поэтому в ходе расчетов не хранилась и рассчитывалась «на лету».

2.4. Частичная таблица распределения разностей цикловой функции

В первую очередь были исследованы 2^{16} разностей, в старших разрядах входных слов цикловой функции, которые последовательно проходили через всю цикловую функцию.

После чего все те же входные разности были использованы как промежуточный результат выполнения цикловой функции, полученный между двумя применениями HalfRound преобразований «Кипарис-256». Более подробно процесс такого поиска на исходных данных, построенных с учетом весов Хэмминга, описан в [16].

Так же был использован адаптивный выбор входных разностей с минимизацией битовых весов, были исследованы все комбинации из 1, 2 и 3 активных бит. Однако поиск велся не из «середины» цикловой функции, а со всех точек между «элементарными» циклами.

Во всех трех случаях вероятности дифференциальных характеристик не ограничивались какими-либо граничными значениями (в силу небольших объемов входных данных). Вероятность полноциклового пути оценивалась как произведение вероятностей переходов на отдельных нелинейных преобразованиях.

2.5. Поиск дифференциальных характеристик

После получения частичной таблицы распределения разностей для одного применения цикловой функции она может быть использована в алгоритме Мацуи. Поскольку предварительные результаты по шифру «Кипарис-256» отсутствовали, в качестве начальных вероятностей были взяты 0, что лишь немного замедляет алгоритм (по сути, первая найденная характеристика считается лучшей известной на момент начала анализа).

В качестве рабочих одноцикловых вероятностей в основном использовалась pDDT цикловой функции, отсортированная по убыванию вероятности, что позволяет сразу же получить достаточно хорошее приближение к наилучшему дифференциальному пути (в ходе расчетов первый найденный путь всегда был лучшим). Начальный набор вероятностей был расширен за счет расчета «на лету» характеристик для входов, не известных pDDT, что позволяет продолжать поиск в ситуациях, когда разность выхода предыдущего цикла имеет большое количество активных бит. Ограничений на вероятности таких путей не налагалось.

Для повышения быстродействия, эти промежуточные характеристики хранились в кэше небольшого размера (1000 элементов) до его переполнения. При переполнении кэш полностью очищался.

3. РЕЗУЛЬТАТЫ ИССЕДОВАНИЙ

В результате работы была найдена характеристика с вероятностью 2^{-2} через один цикл, что подтверждает предыдущие результаты, дополнительно был найден ряд характеристик с вероятностями 2^{-6}, 2^{-9}, 2^{-10} и ниже. Все эти дифференциальные пути использовались при поиске многоцикловых характеристик.

Лучшие результаты и их вероятности:

- 3 цикла: 80000000 00000000 80000000 80008000 -> 88000000 40404404 00808088 00800088 с вероятностью 2^-12;
- 4 цикла: 80000000 00000000 80000000 80008000 -> 68208626 75211214 CA4A2004 6AC4EA4C с вероятностью 2^-106;

– 5 циклов: 80000000 00000000 80000000 80008000 -> AF6A6C6F 1C9496F1 2F6EE961 5ACFAE08 с вероятностью 2^-253.

Приведенные выше данные говорят о том, что, несмотря на достаточно простое цикловое преобразование, сложность атаки быстро растет по мере увеличения количества циклов. Это связано с хорошим лавинным эффектом, благодаря которому очень сложно получить дифференциальный путь через один цикл, который, имея большую вероятность сам по себе, на выходе имел разность, позволяющую в следующем цикле также получить переход с большой вероятностью.

С другой же стороны, алгоритм имеет одноцикловые характеристики с высокой вероятностью и низким весом Хэмминга, как входа, так и выхода. Примеры таких характеристик:

– 00000000 80000000 00800000 80008080 -> 80000000 00004000 00000080 00000080 с вероятностью 2^{-2};
– 00000000 80000000 00800000 80008080 -> 80000000 0000C000 00000180 00000080 с вероятностью 2^{-3};
– 00000000 80000000 01800000 80008080 -> 80000000 0000C000 00000180 00000080 с вероятностью 2^{-4};
– 81181000 80081000 00000000 01008000 -> 00000000 00000040 80000000 00000000 с вероятностью 2^{-5}.

Эти переходы не использовались в расчетах и не присутствовали в pDDT цикловой функции.

Использование же SMT-решателя для поиска дополнительных путей в алгоритме Мацуи эффекта не дало по той причине, что найденные «короткие пути» имели низкую вероятность, хотя были построены на основе pDDT с высокими вероятностями.

ВЫВОДЫ

На основе полученных данных можно утверждать, что шифр «Кипарис-256» является устойчивым к дифференциальному криптоанализу после 6 циклов, однако уже после 4 циклов анализ имеет большую сложность данных и не может быть осуществлен на практике.

Таким образом, запас стойкости алгоритма «Кипарис-256» по отношению к рассмотренной атаке составляет 4 цикла из 10.

Литература

[1] *Dinu, D., Perrin, L., Udovenko, A., Velichkov, V., Großschädl, J., & Biryukov, A.* (2016). Design Strategies for ARX with Provable Bounds: SPARX and LAX (Full Version). IACR Cryptology ePrint Archive.

[2] *Mouha, N., Velichkov, V., Canniere, C. De., Preneel B.* Toolkit for the Differential Cryptanalysis of ARX-based Cryptographic Constructions, Workshop on Tools for Cryptanalysis, 2010.

[3] *Heys, M.* The Design of Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis. Journal of Cryptology - JOC. 9. 148–155. 10.1007/BF02254789.

[4] *Biham, E. and A. Shamir.* "Differential cryptanalysis of DES-like cryptosystems." In Menezes and Vanstone 90, 2–21.

[5] National Institute of Standards and Technology, "FIPS-46-3: Data Encryption Standard." Oct. 1999.

[6] ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Изд-во стандартов, 1989. – 20 с.

[7] *Aoki, K., Ichikawa, T., and Kanda. M. Camellia*: A 128-Bit Block Cipher Suitable for Multiple Platforms-Design and Analysis-. 2000, http://www.cryptonessie.org.

[8] International Organization for Standardization. ISO/IEC 18033-3:2010. Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers, 2010.

[9] ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення [Текст]. – Введ. 01–07–2015. – К.: Мінекономрозвитку України, 2015. – 119 с.

[10] *Daemen, J.* (1999). AES Proposal: Rijndael.

[11] Родінко, М. Ю. Постквантовий малоресурсний симетричний блоковий шифр «Кипарис» / М. Ю. Родінко, Р. В. Олійников // Радиотехника. – 2017. – Вып. 189. – С. 100–107.

[12] *Wallén, J.* (2003). On the Differential and Linear Properties of Addition.

[13] *Biryukov, A., and Velichkov, V.* "Automatic search for differential trails in arx ciphers," in Topics in Cryptology (CT-RSA'14), pp. 227–250, Springer, 2014.

[14] *Matsui, M.* On correlation between the order of S-boxes and the strength of DES. In: De Santis A. (eds) Advances in Cryptology — EUROCRYPT'94. EUROCRYPT 1994. Lecture Notes in Computer Science, vol 950. Springer, Berlin, Heidelberg.

[15] *Leonardo Mendonça de Moura and Nikolaj Bjørner.* Z3: An Efficient SMT Solver. In Proceedings of the 14th International Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS 2008), Budapest, Hungary. 337– 340.

[16] *Rodinko, M., Oliynykov, R., and Eliseev, R.* "Search for one-round differential characteristics of lighweight block cipher Cypress-256", 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kiev, 2018, pp. 312–315.

Поступила в редколлегию 03.12.2018

Елисеев Роман Юрьевич, студент, ХНУРЭ. Область научных интересов – анализ и синтез симметричных криптографических преобразований.

Родинко Мария Юрьевна, аспирантка кафедры безопасности информационных систем и технологий ХНУ им. В.Н. Каразина. Область научных интересов – анализ и синтез блочных симметричных шифров.

Олейников Роман Васильевич, доктор технических наук, профессор кафедры безопасности информационных систем и технологий ХНУ им. В.Н. Каразина. Область научных интересов – анализ и синтез симметричных криптографических преобразований, безопасность программного обеспечения, сетевая безопасность, блокчейн.

УДК 621.3.06

Єлисєєв Р. Ю. **Диференційний криптоаналіз блокового ARX-шифру «Кипарис-256»** / Р. Ю. Єлисєєв, М. Ю. Родінко, Р. В. Олійников // Прикладна радіоелектроніка: наук. – техн. журнал. – 2018. – Том 17, № 3, 4. – С. 121–126.

У статті наведено результати диференційного криптоаналізу симетричного блокового шифру «Кипарис-256», виконаного із застосуванням ряду методів, зокрема, за допомогою алгоритму Мацуї і використанням часткових таблиць розподілу різниць. В ході досліджень було знайдено ряд диференційних характеристик включно до п’яти циклів шифрування. Крім того, був виявлений ряд характеристик з ймовірністю від 2^{-2} до 2^{-5}, входи і виходи яких мають малу вагу Хемінга.

Ключові слова: малоресурсна криптографія, блоковий симетричний шифр, диференційний криптоаналіз, диференційна характеристика.

Іл.: 3. Бібліогр.: 16 назв.

UDC 621.3.06

Eliseev R. Yu. **Differential cryptanalysis of ARX block cipher Cypress-256** / R. Yu. Eliseev, M. Yu. Rodinko, R. V. Oliynykov // Applied Radio Electronics: Sci. Journ. – 2018. – Vol. 17, № 3, 4. – P. 121–126.

This paper presents the results of differential cryptanalysis of the block cipher Cypress-256 performed by several methods, in particular, with the help of Matsui algorithm and application of partial difference distribution tables. As a result a number of differential characteristics up to five rounds of ciphering were found. In addition, a number of differential characteristics with low probabilities (2^{-2}, 2^{-3}, 2^{-4} and 2^{-5}) whose inputs and outputs have small Hamming weight were found.

Keywords: lightweight cryptography, block symmetric cipher, differential cryptanalysis, differential characteristic.

Fig.3. Ref.: 16 items.