Александр А. Козлов1, Михаил А. Иванов2

*1ООО НТЦ «Вулкан»,*

*ул. Ибрагимова, 31, Москва, 105318, Россия*

*2Национальный исследовательский ядерный университет «МИФИ»,*

*Каширское ш., 31, Москва, 115409, Россия*

*1e-mail: a.kozlov@ntc-vulkan.ru, https://orcid.org/0000-0002-4310-2360*

*2e-mail: maivanov@mephi.ru, https://orcid.org/0000-0002-3204-8055*

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ЛИНЕЙНОГО АНАЛИЗА
К ARX АЛГОРИТМАМ СТОХАСТИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ДАННЫХ
В ЗАВИСИМОСТИ ОТ ФУНКЦИИ СМЕШЕНИЯ С РАУНДОВЫМ КЛЮЧОМ

*DOI: http://dx.doi.org/10.26583/bit.2021.2.06*

*Аннотация.* ARX алгоритмы стохастического преобразования являются перспективным решением в области разработки непредсказуемых генераторов псевдослучайных чисел для низкоресурсных систем. Простота реализации ARX операций, а также их высокая энергоэффективность делают привлекательным выбор алгоритмов стохастического преобразования данных, основанных на этих операциях, для обеспечения конфиденциальности информации. Существующие исследования по возможности применения линейного анализа к ARX алгоритмам стохастического преобразования используют неточные линейные аппроксимации раундовых преобразований. Ключевой идеей линейного анализа является использование линейных статистических аналогов нелинейных функций. Линейные аппроксимации используются для выражения зависимости входа алгоритма стохастического преобразования от его выхода в виде линейной функции. Полученная линейная функция выполняется с некоторой вероятностью, зависящей от вероятности выполнения использованных линейных аппроксимаций. Единственной нелинейной операцией в ARX алгоритмах, является сложение по модулю 2*n*. В данной работе проводится исследование ограничений применимости линейного подхода для анализа ARX алгоритмов стохастического преобразования. Исследование проводится для различных случаев реализации функции смешения с раундовым ключом (key mix function): использование операции сложения по модулю 2*n*, операции сложения по модулю 2 и операции циклического сдвига. Для каждого из вариантов проведено исследование возможности применения линейной аппроксимации соответствующей операции ARX алгоритма для проведения его линейного анализа. Для ARX алгоритмов стохастического преобразования, использующих в качестве функции смешения с раундовым ключом сложение по модулю 2*n* или сложение по модулю 2, получены оценки на число операций сложения по модулю 2*n* в них, необходимое для обеспечения их устойчивости к линейному анализу.

*Ключевые слова: сложение по модулю 2n, ARX, линейный анализ, генераторы псевдослучайных чисел.*

*Для цитирования:* *КОЗЛОВ, Александр А.; ИВАНОВ, Михаил А. ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ЛИНЕЙНОГО АНАЛИЗА К ARX АЛГОРИТМАМ СТОХАСТИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ДАННЫХ В ЗАВИСИМОСТИ ОТ ФУНКЦИИ СМЕШЕНИЯ С РАУНДОВЫМ КЛЮЧОМ. Безопасность информационных технологий, [S.l.], v. 28, n. 2, p. 62–69, 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1341>. Дата доступа: 14 apr. 2021.*

*DOI: http://dx.doi.org/10.26583/bit.2021.2.06.*

Alexander A. Kozlov1, Mikhail A. Ivanov2 *1LLС Scientific and Technical Center «Vulkan»,*

*Ibragimova str., 31, Moscow, 105318, Russia*

*2National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),*

*Kashirskoe shosse, 31, Moscow, 115409, Russia*

*1e-mail: a.kozlov@ntc-vulkan.ru, https://orcid.org/0000-0002-4310-2360 2e-mail: MAIvanov@mephi.ru, https://orcid.org/0000-0002-3204-8055*

**The possibility of applying linear analysis to the ARX stochastic algorithms depending on round key functions**

*DOI: http://dx.doi.org/10.26583/bit.2021.2.06*

*Abstract.* ARX stochastic algorithms are a promising solution in the development of unpredictable pseudo- random number generators for low-resource systems. The ease of implementation of their round operations, as well as their high energy efficiency, make the choice of such algorithms attractive for ensuring the confidentiality of information. Existing studies on the possibility of applying linear analysis to ARX stochastic algorithms use imprecise linear approximations of round functions. The key idea of linear analysis is the use of linear statistical analogs of non-linear functions. Linear approximations are used to express the inputs of the stochastic transformation algorithm by its outputs as a linear function. The resulting linear function is true with a certain probability, which depends on the probability of fulfilling the used linear approximations. The only non-linear operation in ARX algorithms is addition modulo 2*n*. In this paper we study the limitations of the applicability of the linear analysis to ARX stochastic transformation algorithms. The study is carried out for various cases of the implementation of round key addition: the use of the addition modulo 2*n,* the addition modulo 2, and the cyclic shift. For ARX stochastic transformation algorithms, using addition modulo 2*n*or addition modulo 2 as a round key mix operation, estimates are obtained for the number of addition operations modulo 2*n*needed to ensure their stability to linear analysis.

*Keywords: addition modulo 2n, ARX, linear analysis, pseudorandom number generator.*

*For citation: KOZLOV, Alexander A.; IVANOV, Mikhail A. The possibility of applying linear analysis to the ARX stochastic algorithms depending on round key functions. IT Security (Russia), [S.l.], v. 28, n. 2, p. 62–69, 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1341>. Date accessed: 14 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.06.*

**Введение**

Алгоритмы стохастического преобразования данных, использующие только операции сложения по модулю , циклического сдвига и сложения по модулю 2 (XOR) называются ARX (Addition-Rotate-XOR) алгоритмами, а соответствующие математические операции – ARX операциями. ARX алгоритмы относятся к типу низкоресурсных алгоритмов стохастического преобразования [1–2]. Можно выделить следующие требования к таким алгоритмам:

1. Реализация алгоритма должна иметь пониженное энергопотребление;
2. Реализация алгоритма должна использовать небольшой объем оперативной памяти.

Кроме того их производительность не должна уступать производительности не низкоресурсных алгоритмов стохастического преобразования.

ARX операции являются наиболее перспективными для построения низкоресурсных алгоритмов стохастического преобразования. Преимуществом использования этих операций является то, что они обеспечивают высокое быстродействие, как при программной, так и при аппаратной реализации. В то же время при их правильной композиции, они обладают хорошими математическими свойствами: высокой степенью нелинейности и рассеивания. Примерами алгоритмов стохастического преобразования, построенных на основе ARX операций, являются алгоритмы Salsa20 [3], PRESENT [4], SIMECK [5], SPECK [6], FEAL [7]. RC5-12 [8], Chaskey [9], SPARX [10], LEA [11], HIGHT [12].

Построенные на основе ARX операций блочные алгоритмы стохастического преобразования могут использоваться в качестве элемента непредсказуемых генераторов псевдослучайных чисел (ГПСЧ), которые могут найти широкое применение в технических областях, связанных с ограничениями в доступных вычислительных мощностях, например в сенсорных сетях [13]. Для этого эти алгоритмы должны быть стойкими по отношению к известным методам анализа, в частности к линейному анализу [14].

Ключевой идеей линейного анализа является использование линейных статистических аналогов (линейных аппроксимаций) нелинейных функций. Линейные аппроксимации используются для выражения зависимости входа алгоритма стохастического преобразования от его выхода в виде линейной функции. Полученная линейная функция выполняется с некоторой вероятностью, зависящей от вероятности выполнения использованных линейных аппроксимаций.

Единственной нелинейной операцией в ARX алгоритмах, является сложение по модулю 2*n*. В [15] представлен анализ линейных свойств операции сложения по модулю 2*n*, полученные линейные аппроксимации операции сложения по модулю 2*n* могут быть использованы для проведения линейного анализа ARX алгоритмов стохастического преобразования. В данной работе проводится исследование ограничений применимости линейного анализа ARX алгоритмов стохастического преобразования на основе полученных в [15] линейных аппроксимаций. Исследование проводится для различных случаев реализации функции смешения с раундовым ключом (key mix function): использование операции сложения по модулю 2*n*, операции сложения по модулю 2 и операции циклического сдвига.

* + - 1. **ARX алгоритмы с реализацией функции смешения с раундовым ключом
			на основе операции сложения по модулю 2*n***

Если операция сложения по модулю 2*n* используется для реализации функции смешения с раундовым ключом, то одно из входных чисел является константой (раундовым ключом). Условие фиксированного раундового ключа – это условие задачи проведения анализа конкретного экземпляра некоторого ARX преобразования. Обозначим ARX алгоритмы стохастического преобразования с реализацией функции смешения с раундовым ключом на основе операции сложения по модулю 2*n* через . Чтобы исследовать возможность применения линейного анализа для алгоритмов  рассмотрим сложение двух *n*-разрядных чисел  и 

 , (1)

где  – фиксированный раундовый ключ, , ,
 значение переноса в *i*-й разряд, .

Для (1) в [15] были доказаны три утверждения, представленные далее.

**Утверждение 1**. В выражении (1) для любого  и любого фиксированного раундового ключа  вероятность совпадения бита переноса *pi* со значением бита входного слова *xi-*1

 . (2)

**Утверждение 2.** В выражении (1) для любого  и любого фиксированного раундового ключа  вероятность совпадения бита переноса *pi* со значением бита раундового ключа *ki-*1

 . (3)

**Утверждение 3.** Для любого фиксированного раундового ключа, если значение вероятности (2) ниже, чем 0.75, то значение вероятности (3) обязательно выше, чем 0.75, и наоборот.

Рассмотрим некоторый ARX алгоритм . Обозначим через *L* множество ARX алгоритмов стохастического преобразования, не устойчивых к линейному анализу. Используя (1) – (3) докажем следующее утверждение.

**Утверждение 4.** Еслито число операций сложения по модулю 2*n* в  не превышает , .

***Доказательство*.**

Рассмотрим линейные аппроксимации каждой из операций алгоритма .

Операция XOR линейна, аппроксимация не требуется.

Операция циклического сдвига на фиксированную величину линейна, аппроксимация не требуется.

Рассмотрим аппроксимацию выражения (1). Значение выходов соотношения (1) может быть выражено так:

  (4)

  (5)

В классическом методе линейного анализа используется одна единственная линейная аппроксимация алгоритма. В рассматриваемой ситуации это невозможно – так как достоверно неизвестны вероятности выполнения аппроксимации для (1). Однако можно составить несколько различных линейных аппроксимаций алгоритма *arx* и провести линейный анализ для каждой из них по отдельности. Из утверждения 3 следует, что либо (4), либо (5) выполняется с вероятностью выше, чем 0.75, но неизвестно какое именно. Поэтому вместо того, чтобы выразить алгоритм  через одну линейную функцию, выполняющуюся с заданной вероятностью, выразим алгоритм *arx* через множество линейных функций, которое обозначим .

Для этого, каждую из операций сложения по модулю 2*n* будем аппроксимировать, используя по отдельности выражения (4) и (5). Каждая такая аппроксимация должна рассматриваться отдельно, поэтому число линейных аппроксимаций всего алгоритма  будет увеличиваться в два раза при каждой линейной аппроксимации операции сложения по модулю 2*n*.

Если всего в алгоритме  было  операций сложения по модулю 2*n*, то получим 2*t* линейных аппроксимаций. В силу того, что  содержит все возможные случаи линейной аппроксимации операции сложения по модулю 2*n*, то согласно утверждению 3 в содержится функция , все линейные аппроксимации операции сложения по модулю 2*n* входящие в которую выполняются с вероятностью не меньше, чем 0.75.

Всего в входит  линейных аппроксимаций. Каждая входит с преобладанием не меньше, чем 0.25. Отсюда, согласно лемме о накапливании [14], общее преобладание для функции будет не меньше, чем . Известно, что для проведения линейного анализа для некоторой аппроксимации, выполняемой с преобладанием , требуется открытых текстов. Тогда, для проведения линейного анализа на основе аппроксимации с преобладанием  требуется 22*t+*2 открытых текстов.

Чтобы точно установить функцию , нужно провести статистический подсчет согласно методу линейного анализа для всех 2*t* линейных аппроксимаций. Тогда общая вычислительная сложность составит . Всего для алгоритма  существует  открытых текстов. Отсюда получаем, что .

* + - 1. **ARX алгоритмы с реализацией функции смешения с раундовым ключом
			на основе операции сложения по модулю 2**

Обозначим ARX **алгоритмы с реализацией функции смешения с раундовым ключом на основе операции** XOR через . Чтобы исследовать возможность применения линейного анализа для алгоритмов  рассмотрим сложение двух произвольных *n*-разрядных чисел  и $Y=(y\_{n-1}, y\_{n-2}, ..., y\_{0})$

 , (6)

где , ,  $-$ значение переноса в *i*-й разряд, .

Если операция сложения по модулю 2*n* не используется для реализации функции смешения с раундовым ключом, то оба входных операнда этой операции не являются константой. Для (6) в [15] были доказаны два утверждения, представленные далее.

**Утверждение 5.** В выражении (6) для любого  и любого 

 . (7)

**Утверждение 6.** В выражении (6) для любого  и любого 

 . (8)

Рассмотрим некоторый ARX алгоритм . Используя (7) – (8) докажем следующее утверждение.

**Утверждение 7.** Если  и  то число операций сложения по модулю 2*n* в  не превышает .

***Доказательство.***

Рассмотрим линейные аппроксимации каждой из операций алгоритма .

Операция XOR линейна, аппроксимация не требуется.

Операция циклического сдвига на фиксированную величину линейна, аппроксимация не требуется.

Рассмотрим аппроксимацию выражения (6).

Соотношения выполняются с вероятностью 0.75. В [15] было доказано, что эти линейные аппроксимации являются наилучшими для операции сложения по модулю 2*n*.

Если всего в алгоритме  было  операций сложения по модулю 2*n*, то для составления линейной аппроксимации алгоритма  в лучшем случае будет использовано *t* линейных аппроксимаций операции сложения по модулю 2*n*. Каждая из аппроксимаций выполняется с вероятностью 0.75. Согласно лемме о накапливании [14], общее преобладание для функции линейной аппроксимации алгоритма  будет не меньше, чем . Тогда, для проведения линейного анализа на основе аппроксимации с преобладанием  требуется 22*t+*2 открытых текстов. Всего для алгоритма  существует  открытых текстов. Отсюда получаем, что .

1. **ARX алгоритмы с реализацией функции смешения с раундовым ключом**

**на основе операции циклического сдвига**

Обозначим через  операцию циклического сдвига *n*-разрядного числа на  бит вправо

  (9)

где .

Операция циклического сдвига *n*-разрядного числа на *r* бит влево может быть выражена как . Поэтому здесь и далее без ограничения общности будем рассматривать только операцию циклического сдвига вправо.

Если значение сдвига *r* фиксировано, то выход операции  однозначно выражается через вход исходя из определения самой операции (9).

Рассмотрим случай, когда значение сдвига зависит от значения раундового ключа

 , (10)

где  – некоторая функция зависимости от раундового ключа . 

В этом случае величина сдвига неизвестна, и возможны все линейные аппроксимации для некоторого выхода *yi* операции циклического сдвига, *i* = 0, 1, ..., *n* – 1:

  (11)

Величина раундового ключа является неизвестной, но фиксированной. Это означает, что среди всех возможных аппроксимаций выхода *yi* в соотношении (11) верна только одна. Установить какая именно, не имея информации о значении раундового ключа, невозможно. Поэтому применение классического линейного анализа ARX алгоритмов стохастического преобразования для рассматриваемого случая невозможно.

**Заключение**

Получена оценка на число операций сложения по модулю 2*n* в ARX алгоритмах стохастического преобразования, устойчивых к линейному анализу. Если в ARX алгоритме с длиной входного слова *m* для реализации функции смешения с раундовым ключом используется операция сложения по модулю 2*n*, , то он устойчив к линейному анализу, если число операций сложения по модулю 2*n* в нем не меньше чем . Если для реализации функции смешения с раундовым ключом используется операция XOR, то ARX алгоритм устойчив к линейному анализу, если число операций сложения по модулю 2*n* в нем не меньше чем .

СПИСОК ЛИТЕРАТУРЫ:

1. Жуков А.Е. Легковесная криптография. Часть 1. Вопросы кибербезопасности. 2015. №1(9). С. 23–46. URL: https://cyberrus.com/wp-content/uploads/2015/05/vkb\_09\_04.pdf (дата обращения: 20.01.2021).
2. Жуков А.Е. Легковесная криптография. Часть 2. Вопросы кибербезопасности. 2015. №2(10). C. 2–10. URL: https://cyberrus.com/wp-content/uploads/2015/05/vkb\_10\_01.pdf (дата обращения: 20.01.2021).
3. Bernstein D.J. (2008) The Salsa20 Family of Stream Ciphers. In: Robshaw M., Billet O. (eds) New Stream Cipher Designs. Lecture Notes in Computer Science, vol. 4986. Springer, Berlin, Heidelberg.
DOI: https://doi.org/10.1007/978-3-540-68351-3\_8.
4. Bogdanov A. et al. (2007) PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier P., Verbauwhede I. (eds) Cryptographic Hardware and Embedded Systems - CHES 2007. CHES 2007. Lecture Notes in Computer Science, vol. 4727. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-74735-2\_31.
5. Yang G., Zhu B., Suder V., Aagaard M.D., Gong G. (2015) The Simeck Family of Lightweight Block Ciphers. In: Güneysu T., Handschuh H. (eds) Cryptographic Hardware and Embedded Systems -- CHES 2015. CHES 2015. Lecture Notes in Computer Science, vol. 9293. Springer, Berlin, Heidelberg.
DOI: https://doi.org/10.1007/978-3-662-48324-4\_16.
6. Beaulieu R., Shors D., Smith J., Treatman-Clark S., Weeks B., Wingers L. (2015) The Simon and Speck Block Ciphers on AVR 8-Bit Microcontrollers. In: Eisenbarth T., Öztürk E. (eds) Lightweight Cryptography for Security and Privacy. LightSec 2014. Lecture Notes in Computer Science, vol. 8898. Springer, Cham.
DOI: https://doi.org/10.1007/978-3-319-16363-5\_1.
7. Shimizu A., Miyaguchi S. (1988) Fast Data Encipherment Algorithm FEAL. In: Chaum D., Price W.L. (eds) Advances in Cryptology – EUROCRYPT’ 87. EUROCRYPT 1987. Lecture Notes in Computer Science,
vol. 304. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-39118-5\_24.
8. Rivest R.L. (1995) The RC5 encryption algorithm. In: Preneel B. (eds) Fast Software Encryption. FSE 1994. Lecture Notes in Computer Science, vol. 1008. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-60590-8\_7.
9. Mouha N., Mennink B., Van Herrewege A., Watanabe D., Preneel B., Verbauwhede I. (2014) Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers. In: Joux A., Youssef A. (eds) Selected Areas in Cryptography - SAC 2014. SAC 2014. Lecture Notes in Computer Science, vol. 8781. Springer, Cham.
DOI: https://doi.org/10.1007/978-3-319-13051-4\_19.
10. Dinu D., Perrin L., Udovenko A., Velichkov V., Großschädl J., Biryukov A. (2016) Design Strategies for ARX with Provable Bounds: Sparx and LAX. In: Cheon J., Takagi T. (eds) Advances in Cryptology – ASIACRYPT 2016. ASIACRYPT 2016. Lecture Notes in Computer Science, vol. 10031. Springer, Berlin, Heidelberg.
DOI: https://doi.org/10.1007/978-3-662-53887-6\_18.
11. Hong D., Lee JK., Kim DC., Kwon D., Ryu K.H., Lee DG. (2014) LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors. In: Kim Y., Lee H., Perrig A. (eds) Information Security Applications. WISA 2013. Lecture Notes in Computer Science, vol 8267. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-05149-9\_1.
12. Hong D. et al. (2006) HIGHT: A New Block Cipher Suitable for Low-Resource Device. In: Goubin L., Matsui M. (eds) Cryptographic Hardware and Embedded Systems - CHES 2006. CHES 2006. Lecture Notes in Computer Science, vol. 4249. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/11894063\_4.
13. Варгаузин В.А. Радиосети для сбора данных от сенсоров, мониторинга и управления на основе стандарта IEEE 802.15.4 // ТелеМультиМедия. 2005. № 6. С. 23–27.
URL: http://book.itep.ru/depository/zigbee/802.15.4.pdf (дата обращения: 20.01.2021).
14. Matsui M. (1994) Linear Cryptanalysis Method for DES Cipher. In: Helleseth T. (eds) Advances in Cryptology – EUROCRYPT ’93. EUROCRYPT 1993. Lecture Notes in Computer Science, vol 765. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-48285-7\_33.
15. Козлов А.А., Карондеев А.М., Силков А.А. Сложение по модулю 2n в блочном шифровании. Вопросы кибербезопасности. 2015. №3(11). C. 34–42. URL: https://cyberrus.com/wp-content/uploads/2015/09/vkb\_11\_4.pdf (дата обращения: 20.01.2021).

REFERENCES:

1. Zhukov А.Е. Lightweight Cryptography, Cybersecurity Issues. 2015, no. 1(9). Part 1. P. 23–46.
URL: https://cyberrus.com/wp-content/uploads/2015/05/vkb\_09\_04.pdf (accessed: 20.01.2021) (in Russian).
2. Zhukov А.Е. Lightweight Cryptography, Cybersecurity Issues. 2015, no. 2(10). P. 2–10.
URL: https://cyberrus.com/wp-content/uploads/2015/05/vkb\_10\_01.pdf (accessed: 20.01.2021) (in Russian).
3. Bernstein D.J. (2008) The Salsa20 Family of Stream Ciphers. In: Robshaw M., Billet O. (eds) New Stream Cipher Designs. Lecture Notes in Computer Science, vol. 4986. Springer, Berlin, Heidelberg.
DOI: https://doi.org/10.1007/978-3-540-68351-3\_8.
4. Bogdanov A. et al. (2007) PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier P., Verbauwhede I. (eds) Cryptographic Hardware and Embedded Systems -- CHES 2007. CHES 2007. Lecture Notes in Computer Science, vol. 4727. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-74735-2\_31.
5. Yang G., Zhu B., Suder V., Aagaard M.D., Gong G. (2015) The Simeck Family of Lightweight Block Ciphers. In: Güneysu T., Handschuh H. (eds) Cryptographic Hardware and Embedded Systems -- CHES 2015.
CHES 2015. Lecture Notes in Computer Science, vol. 9293. Springer, Berlin, Heidelberg.
DOI: https://doi.org/10.1007/978-3-662-48324-4\_16.
6. Beaulieu R., Shors D., Smith J., Treatman-Clark S., Weeks B., Wingers L. (2015) The Simon and Speck Block Ciphers on AVR 8-Bit Microcontrollers. In: Eisenbarth T., Öztürk E. (eds) Lightweight Cryptography for Security and Privacy. LightSec 2014. Lecture Notes in Computer Science, vol. 8898. Springer, Cham.
DOI: https://doi.org/10.1007/978-3-319-16363-5\_1.
7. Shimizu A., Miyaguchi S. (1988) Fast Data Encipherment Algorithm FEAL. In: Chaum D., Price W.L. (eds) Advances in Cryptology – EUROCRYPT’ 87. EUROCRYPT 1987. Lecture Notes in Computer Science,
vol. 304. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-39118-5\_24.
8. Rivest R.L. (1995) The RC5 encryption algorithm. In: Preneel B. (eds) Fast Software Encryption. FSE 1994. Lecture Notes in Computer Science, vol 1008. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-60590-8\_7.
9. Mouha N., Mennink B., Van Herrewege A., Watanabe D., Preneel B., Verbauwhede I. (2014) Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers. In: Joux A., Youssef A. (eds) Selected Areas in Cryptography -- SAC 2014. SAC 2014. Lecture Notes in Computer Science, vol. 8781. Springer, Cham.
DOI: https://doi.org/10.1007/978-3-319-13051-4\_19.
10. Dinu D., Perrin L., Udovenko A., Velichkov V., Großschädl J., Biryukov A. (2016) Design Strategies for ARX with Provable Bounds: Sparx and LAX. In: Cheon J., Takagi T. (eds) Advances in Cryptology – ASIACRYPT 2016. ASIACRYPT 2016. Lecture Notes in Computer Science, vol. 10031. Springer, Berlin, Heidelberg.
DOI: https://doi.org/10.1007/978-3-662-53887-6\_18.
11. Hong D., Lee JK., Kim DC., Kwon D., Ryu K.H., Lee DG. (2014) LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors. In: Kim Y., Lee H., Perrig A. (eds) Information Security Applications. WISA 2013. Lecture Notes in Computer Science, vol. 8267. Springer, Cham.
DOI: https://doi.org/10.1007/978-3-319-05149-9\_1.
12. Hong D. et al. (2006) HIGHT: A New Block Cipher Suitable for Low-Resource Device. In: Goubin L., Matsui M. (eds) Cryptographic Hardware and Embedded Systems - CHES 2006. CHES 2006. Lecture Notes in Computer Science, vol. 4249. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/11894063\_4.
13. Vargauzin V.A. Radioseti dlja sbora dannyh ot sensorov, monitoringa i upravlenija na osnove standarta IEEE 802.15.4, TeleMultiMedija, 2005, no. 6. P. 23–27. URL: http://book.itep.ru/depository/zigbee/802.15.4.pdf (accessed: 20.01.2021) (in Russian).
14. Matsui M. (1994) Linear Cryptanalysis Method for DES Cipher. In: Helleseth T. (eds) Advances
in Cryptology – EUROCRYPT ’93. EUROCRYPT 1993. Lecture Notes in Computer Science, vol. 765. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-48285-7\_33.
15. Kozlov A.A., Karondeev A.M., Silkov A.A. Addition modulo 2n in block ciphers. Cybersecurity Issues. 2015, no. 3(11). P. 34–42. URL: https://cyberrus.com/wp-content/uploads/2015/09/vkb\_11\_4.pdf
(accessed: 20.01.2021) (in Russian).

*Поступила в редакцию – 25 января 2021 г. Окончательный вариант – 08 апреля 2021 г.*

*Received – January 25, 2021. The final version – April 08, 2021.*