https://doi.org/10.53656/math2023-5-8-sel

*Overview*
*Обзор*

# ИЗБОР И ОБОСНОВКА НА ПОКАЗАТЕЛИ ЗА СРАВНИТЕЛЕН АНАЛИЗ НА НИСКОРЕСУРСНИ ШИФРИ

**Диляна Димитрова**
*ВВМУ „Н. Й. Вапцаров“ – Варна*

**Резюме.** Основната цел на статията е подбор на показатели за оценка и анализ на нискоресурсни шифри с различна структура и принцип на работа, които да послужат при последващ сравнителен анализ на избрани шифри, финалисти в конкурса на NIST за нов нискоресурсен криптографски алгоритъм. Използвани методи: сравнителен анализ и обобщение. Въз основа на направеното проучване са подбрани два типа показатели – за оценка на възможностите на шифрите и за оценка на софтуерната им ефективност. Първият тип показатели е приложен върху представители на две семейства нискоресурсни шифри, като се установява кои имат по-добри характеристики.

*Ключови думи:* нискоресурсни алгоритми; показатели; сравнителен анализ

## 1. Въведение

Малките устройства от Интернет на нещата (Internet of Things, IoT) навлизат все повече във всекидневния ни живот. С това се появява и проблемът със защитата на предаваната от тях информация. Засиленото им използване води до повишена опасност от кибератаки. Техните слабости крият голям риск за потребителите и опазването на личната им информация. За да бъдат IoT устройствата по-защитени, трябва да се използват подходящи криптографски алгоритми, които да не натоварват устройството допълнително, тъй като то е ограничено откъм ресурси, но в същото време да са достатъчно надеждни.

За решаването на изброените проблеми се налага разработването на нови криптографски алгоритми, които да покриват изискванията на тези устройства. За тази цел NIST (National Institute of Standards and Technology) организира конкурс за нов криптографски алгоритъм. В периода 2019 – 2021 г. се провеждат два кръга. В първия[1] участват 57 кандидати, до втория са допуснати 32. Вторият кръг приключва през март 2021 г., когато са обявени финалистите в конкурса. През месец февруари 2023 г. е избрано семейство от нови криптографски алгоритми[1] ASCON, което предстои да бъде

стандартизирано от NIST. Въпреки това проучването и анализът им са от съществено значение за бъдещи изследвания. Затова трябва да бъдат подбрани подходящи показатели за сравнение.

Настоящото изследване може да бъде полезно на изследователи в областта на криптографията и криптоанализа, на киберспециалисти, може да послужи като референтен източник и информационен ресурс на специалисти в изброените области, както и на хора, занимаващи се със сигурност на IoT.

## 2. Актуалност на проблема

За настоящото изследване са проучени спецификации на нови нискоресурсни криптографски алгоритми, публикувани на официалния сайт на NIST. Изследвани са научни статии и доклади, публикувани в периода 2018 – 2023 г. Използвани са ключови думи: lightweight algorithms, NIST, comparative analysis, finalists, criteria, IoT.

Терминът, който се използва за новите криптографски алгоритми, приложими в устройствата с ограничени ресурси, на английски език е “lightweight”. В българския език няма наложено понятие, което да съответства на него, затова в настоящата публикация ще бъдат използвани думата „нискоресурсен“ и нейните производни. Тя най-точно описва целите на тези шифри.

Основната цел на проучването е да се подберат показатели за оценка и анализ на нискоресурсни шифри с различна структура и принцип на работа, които да послужат при последващ сравнителен анализ на избрани шифри, финалисти в конкурса на NIST.

В съществуващите литературни източници по темата са правени сравнителни анализи между различни нискоресурсни криптографски алгоритми. В проучването (Sehrawat et al. 2019) са описани показатели за сравнение на такива алгоритми в зависимост от софтуерната и хардуерната им имплементация. В него не са разгледани представители от финалистите в конкурса на NIST. В (Rushad et al. 2022) е представен анализ на някои от по-новите криптографски примитиви. Той се базира на дизайна, сигурността и производителността им. В отчет на NIST (Turan et al. 2023) са представени резултатите от конкурса за нов нискоресурсен криптографски алгоритъм. В (Madushan et al. 2022) са разгледани финалистите, представени са техни спецификации и различни атаки срещу тях. Въпреки направените изследвания могат да бъдат използвани и допълнителни показатели, с които да се направят по-подробен анализ и оценка на възможностите на нискоресурсните шифри.

От направения литературен обзор може да се заключи, че в зависимост от целта на изследването са използвани различни показатели за сравнение. Въпреки това не се наблюдават много проучвания върху финалистите от конкурса за нов нискоресурсен криптографски алгоритъм на NIST. Липсва цялостен сравнителен анализ на възможностите на тези шифри. В настоящото проучване е предложен набор от показатели, който може да се приложи за сравнителен анализ на шифри с различна структура и принцип на работа.

В изследвания период не са открити публикации на български език по темата.

## 3. Необходимост от използване на нискоресурсни шифри

При използването на IoT устройства конвенционалните криптографски методи, като световния стандарт AES, хеш-функции, като SHA-256, MD5, както и други методи за криптографска сигурност, като RSA, не работят оптимално върху системи с ограничени възможности на изчисленията и капацитет на паметта. Използването на познатите криптографски алгоритми върху IoT или вградени (embedded) устройства не е оптимален вариант, тъй като изискват повече изчислителна мощ. Те заемат твърде много физическо място и консумират прекалено много захранване.

Поради малките си размери и специфичното си приложение повечето IoT устройства не разполагат с изчислителните възможности на сървър или персонален компютър, затова за нискоресурсната криптография се въвеждат специални изисквания и ограничения, свързани с размера, консумацията и скоростта на обработка на данни. Задължителните изисквания, които трябва да се вземат под внимание при проектирането на нискоресурсен криптографски алгоритъм са размер, включващ обем на интегралната схема и количество използвана ROM и RAM памет, мощност, консумация на енергия, скорост на обработка на данни[2].

*Автентикационно шифриране със свързани данни (AEAD).* Много криптографски приложения изискват както конфиденциалност, така и автентикация на своите съобщения. Постигането на тази проверка се извършва с добавяне на допълнителни контролни тагове (MAC – Message Authentication Codes), които показват дали данните са били променяни[2]. Много съвременни приложения използват тези два метода – шифриране и MAC код, за да постигнат конфиденциалност и цялостност на данните. За съвременните шифри се наложи идеята за тяхното комбиниране в един общ модел, който да предоставя необходимата криптографска сигурност. Той цели да се улесни и стандартизира процесът на създаване на нови криптографски алгоритми. Използваният механизъм е известен като

Authenticated Encryption with Associated Data (AEAD)[2]. Той разполага с всички необходими елементи за справяне с проблема, свързан със сигурността и запазване целостта на данните. На български език няма наложен превод на AEAD. В настоящата публикация ще бъде използвано автентикационно шифриране със свързани данни.

Криптографските алгоритми, следващи AEAD схемата за реализация, изпълняват две основни процедури – автентикационно шифриране и автентикационно дешифриране. Процесът по шифриране генерира шифротекст на база подадените му от потребителя секретен ключ – K, уникално число (nonce) – N, открит текст – P, и свързани данни – A (Bozhko 2023). При извършване на обратния процес – дешифриране на шифротекста, въз основа на получените стойности след процедурата по дешифриране AEAD алгоритъмът може да генерира два изходни резултата. Единият е успешно дешифриран текст P, а другият може да бъде специален символ, показващ наличие на грешка, когато са открити компрометирани данни след дешифрирането.

## 4. Показатели за сравнителен анализ на нискоресурсни шифри

Показателите, които могат да се използват за сравнителен анализ и оценка на един криптографски алгоритъм, могат да обхващат различни аспекти, като софтуерна и хардуерна производителност, устойчивост срещу различни атаки и други. В настоящото проучване са подбрани показатели, целящи оценка на възможностите на новите криптографски алгоритми и софтуерната им ефективност. Те могат да се използват за сравнение на нискоресурсни шифри с различна структура и принцип на работа. По този начин могат да се направят по-обхватно проучване и сравнителен анализ на характеристиките им и да се оцени тяхната приложимост в Интернет на нещата.

***Показатели, оценяващи възможностите на криптографските алгоритми***

За анализ на възможностите на нискоресурсни криптографски алгоритми се предлагат следните показатели:

– AEAD – дали криптографският алгоритъм поддържа автентикационно шифриране със свързани данни;

– ниво на сигурност – силата на алгоритъма за криптиране се измерва в битове на базата на анализи, предоставени в спецификациите на всеки криптографски алгоритъм, който е тестван срещу различни видове атаки;

– размер на ключа – размер на криптографския ключ, използван от шифъра;

– уникално число (nonce) – стойност, която се използва само веднъж при криптиране или подписване на данни; нейната цел е да осигури уникалност и непредсказуемост, което помага за предотвратяване на атаки върху криптографските схеми;

– таг – малък блок от данни, който се извлича от откритият текст или шифротекста по време на процедурите шифриране и дешифриране, като се използва за целите на удостоверяването и проверката на целостта на данните;

– изграждащ блок – примитив, който формира основата на криптографския алгоритъм;

– режим на работа – определя как шифърът обработва данните, и задава правила за криптиране и декриптиране.

***Показатели за софтуерна ефективност***

Метриките, които могат да се използват за оценка на софтуерната производителност (Renner et al. 2023), са:

– време за изпълнение – средното време за генериране на тестов вектор; измерва се в микросекунди;

– размер на кода – размер на компилирания код в байтове;

– използвана RAM памет – измервана в байтове.

## 5. Приложение на показателите, оценяващи възможностите на криптографските алгоритми

За сравнение в настоящото проучване са избрани ASCON и Elephant, финалисти в конкурса на NIST.

ASCON е семейство от нискоресурсни автентикационни алгоритми за криптиране и хеширане. Избран е за победител в конкурса на NIST през февруари 2023 г. и очаква стандартизация. Разработен е през 2014 г. и е финалист в състезанието CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness)[4] през 2019 г. Дизайнът му е базиран на т. нар. „sponge“ конструкция – режим на работа, който се основава на пермутация с фиксирана дължина и на правило, което изгражда функция, преобразуваща вход с променлива дължина в изход с променлива дължина. Семейството ASCON включва 7 криптографски алгоритъма. Някои от тях са шифрите Ascon-128 и Ascon-128a и хеш-функцията Ascon-Hash (Dobraunig et al. 2021). Екипът на ASCON предлага още една разновидност на шифъра – ASCON-80pq, която цели по-голяма устойчивост срещу атаките за квантово възстановяване на ключа. Разгледаните представители от семейство ASCON използват „Duplex“ конструкцията (Bertoni et al. 2019). Чрез използването ѝ автентикационното шифриране изисква само едно извикване на основната пермутация на блок от съобщението. Входните блокове на

конструкцията се използват за въвеждане на ключа и блоковете на съобщението, междинните изходни блокове – като ключов поток, а последният – като MAC.

Elephant е автентикационна схема за криптиране, която използва конструкцията „encrypt-then-MAC“. При нея откритият текст първо се шифрира, след което се създава MAC на базата на получения шифротекст. Тя има три разновидности – Dumbo, Jumbo и Delirium. Размерът на блока на всяка от тях е съответно 160 бита, 176 бита и 200 бита. Първите две се основават на примитива Sponget hashing (Bogdanov et al. 2013). Третата се базира на примитива Keccak (Bertoni et al. 2019). Той предлага паралелен режим на работа, позволяващ ефективна обработка на множество блокове едновременно (Beyne et al. 2021).

**Таблица 1.** Сравнение между ASCON и Elephant

| **Финалист Показатели** | **ASCON** | | | **Elephant** | | |
|---|---|---|---|---|---|---|
| **AEAD** | Да | | | Да | | |
| **Разновидности** | ASCON-128 | ASCON-128a | ASCON-80pq | Dumbo | Jumbo | Delirium |
| **Ниво на сигурност [битове]** | 128 | 128 | 128 | 112 | 127 | 127 |
| **Размер на ключа [битове]** | 128 | 128 | 160 | 128 | 128 | 128 |
| **Уникално число (Nonce) [битове]** | 128 | 128 | 128 | 96 | 96 | 96 |
| **Таг [битове]** | 128 | 128 | 128 | 64 | 64 | 128 |
| **Изграждащ блок** | ASCON Permutation | | | Spongent-π[160] | Spongent-π[176] | KECCAK - f [200] |
| **Режим на работа** | Duplex | | | Encrypt-then-MAC | | |

В таблица 1 е показано сравнение между шифрите от семействата ASCON и Elephant, финалисти в конкурса за нов нискоресурсен криптографски алгоритъм на NIST. От него се вижда, че всеки един от тях поддържа AEAD схемата на реализация. Нивото на сигурност е в диапазона от 112 до 128 бита. Счита се, че стойност 128 бита осигурява необходимото ниво на сигурност

срещу класически атаки. От това може да се заключи, че представителите на ASCON предлагат по-добра защита в сравнение с тези на Elephant и са по-устойчиви срещу тях. От таблицата може да се получи информация за основните параметри на разгледаните шифри – размер на ключа, уникално число и таг. В нискоресурсната криптография те са от ключово значение за постигане на необходимото ниво на сигурност при ограничени ресурси и обмен на данни. Размерът на ключа на всички представители е 128 бита, което покрива минималната препоръчителна дължина на ключа в съвременните шифри. Изключение прави шифърът ASCON-80pq, който използва ключ с дължина 160 бита.

Разглежданите криптографски алгоритми използват различни режими на работа и изграждащи блокове. Режимите включват Duplex и Encrypt-then-MAC и определят как се извършват процедурите за шифриране и дешифриране на всеки шифър. Изграждащите блокове са ASCON Permutation, Spongent-π и KECCAK-f. Те са основни компоненти в дизайна на шифрите и играят важна роля за гарантиране на тяхната сигурност. Може да се заключи, че въпреки различните изграждащи блокове и режими на работа целта им остава една и съща – адаптиране към различни изисквания и цели на използване, докато се оптимизира производителността и се гарантира ефективно и сигурно криптиране на данните в различни среди с ограничени ресурси.

**6. Изводи**

1. Подбрани са основни показатели, чрез които може да се получи по-подробна представа за възможностите на новите нискоресурсни шифри с различна структура и принцип на работа.

2. Първата група показатели са приложени в сравнителен анализ на шифри от две семейства криптографски алгоритми – ASCON и Elephant. Резултатите от него показват, че представителите на ASCON представят по-добри резултати.

3. AEAD схемите за автентикация предлагат нов модел за проектиране и изграждане на криптографските алгоритми. Възможността за комбиниране на конфиденциалност и автентикация на данните в един криптографски механизъм позволява да се осигурят сигурност, надеждност и бързина при обработката на информация от съвременните криптографски алгоритми.

**Благодарности и финансиране**

Това изследване е подкрепено от Министерството на образованието и науката по Националната програма „Млади учени и постдокторанти 2“.

**Acknowledgments & Funding**

This research is supported by the Bulgarian Ministry of Education and Science under the National Program "Young Scientists and Postdoctoral Students 2|.

**БЕЛЕЖКИ**

1. NIST, 2023. Lightweight Cryptography | CSRC. [online]. July 2023. [Accessed 14 July 2023]. Available from: https://web.archive.org/web/20230713221829/https://csrc.nist.gov/Projects/lightweight-cryptography
2. NIST, 2018. Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process. [online], [Accessed 12 January 2023]. Available from: https://csrc.nist.gov/Projects/Lightweight-Cryptography
3. FORTINET, 2023. What Is a Message Authentication Code (MAC)? . [online]. 27 March 2023. [Accessed 3 April 2023]. Available from: https://web.archive.org/web/20230327125230/https://www.fortinet.com/resources/cyberglossary/message-authentication-code
4. CAESAR, 2023. Crypto competitions: CAESAR submissions. [online]. 26 May 2023. [Accessed 1 June 2023]. Available from: https://web.archive.org/web/20230526184909/https://competitions.cr.yp.to/caesar-submissions.html

**ЛИТЕРАТУРА**

BERTONI, G. et al., 2019. *Keccak Team.* [online]. 2019. [Accessed 5 February 2023]. Available from: https://keccak.team/sponge_duplex.html

BEYNE, T. et al., 2021. *Elephant v2 Specification.* NIST [online], [Accessed 13 April 2023]. Available from: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/elephant-spec-final.pdf

BOGDANOV, A. et al., 2013. SPONGENT: The design space of lightweight cryptographic hashing. *IEEE Transactions on Computers,* vol. 62, no. 10, pp. 2041 – 2053. DOI 10.1109/TC.2012.196.

BOZHKO, A.A., Ed., 2023. *Properties of AEAD algorithms.* [online]. 10 March 2023. [Accessed 16 June 2023]. Available from: https://www.ietf.org/id/draft-irtf-cfrg-aead-properties-01.html#name-aead-algorithms

DOBRAUNIG, Ch. et al., 2021. *Ascon v1.2.* Submission to NIST. [online], [Accessed 10 May 2023]. Available from: https://ascon.iaik.tugraz.at

MADUSHAN, H. et al., 2022. A Review of the NIST Lightweight Cryptography Finalists and Their Fault Analyses. *Electronics*, Vol. 11, Page 4199 [online], vol. 11, no. 24, pp. 4199. [Accessed 10 April 2023]. DOI 10.3390/ELECTRONICS11244199.

RENNER, S. et al., 2023. *NIST LWC Software Performance Benchmarks on Microcontrollers*. [online]. 4 June 2023. [Accessed 5 June 2023]. Available from: https://web.archive.org/web/20230604174109/https://lwc.las3.de/

RUSHAD, M. et al., 2022. Resource-Aware Cryptography: An Analysis of Lightweight Cryptographic Primitives. *SN Computer Science* [online], vol. 3, no. 1. [Accessed 6 June 2023]. DOI 10.1007/S42979-021-00984-Z.

SEHRAWAT, D. et al., 2019. Comparative Analysis of Lightweight Block Ciphers in IoT-Enabled Smart Environment. *6th International Conference on Signal Processing and Integrated Networks*, SPIN 2019, pp. 915 – 920. DOI 10.1109/SPIN.2019.8711697.

TURAN, M.S. et al., 2023. *NIST Internal Report NIST IR 8454 Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process*. [online], [Accessed 3 July 2023]. DOI 10.6028/NIST.IR.8454.

## SELECTION AND JUSTIFICATION OF CRITERIA FOR COMPARATIVE ANALYSIS OF LIGHTWEIGHT CIPHERS

**Abstract.** The main aim of the paper is selection of criteria for evaluation and analysis of lightweight ciphers with different structure and modes of operation to serve in the subsequent comparative analysis of selected ciphers, finalists in the NIST's competition for new lightweight cryptographic algorithm. Methods used: comparative analysis and summary. Based on the study, two types of criteria were selected - to assess the capabilities of ciphers and to assess their software performence. The first type of metrics has been applied on representatives of two families of lightweight ciphers, finding which have better characteristics.

*Keywords*: lightweight algorithms; criteria; comparative analysis

✉ **Dilyana Dimitrova, PhD student**
ORCID iD: 0000-0001-9950-5620
Web of Science Researcher ID: AES-8463-2022
Nikola Vaptsarov Naval Academy
73, Vasil Drumev St.
Varna, Bulgaria
E-mail: di.dimitrova@naval-acad.bg