Ежегодная международная научно-практическая конференция
«РусКрипто’2019»

Обзор результатов анализа шифра «Кузнечик»

Маршалко Г.Б., Бондаренко А.И., Агафонова А.В.
ТК 26

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 34.12—2015

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Блочные шифры

Издание официальное

Москва
Стандартинформ
2016

ЕВРАЗИЙСКИЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ (EACC)

EURO-ASIAN COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION (EASC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ 34.12–2018

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Блочные шифры

Минск
Евразийский совет по стандартизации, метрологии и сертификации
2018

ISO/IEC JTC1/SC27 N18980

Date: 2018-12-11

ISO/IEC FDIS 18033-3:2018(E)

ISO/IEC JTC1/SC27/WG2

Secretariat: DIN

IT Security techniques — Encryption algorithms — Part 3: Block ciphers

IT Techniques de sécurité — Algorithmes de chiffrement — Partie 3: Chiffrement par blocs

ISO/IEC FDIS 18033-3:2018(E)

Independent Submission
Request for Comments: 7801
Category: Informational
ISSN: 2070-1721

V. Dolmatov, Ed.
Research Computer Center MSU
March 2016

GOST R 34.12-2015: Block Cipher "Kuznyechik"

Abstract

This document is intended to be a source of information about the Russian Federal standard GOST R 34.12-2015 describing the block cipher with a block length of n=128 bits and a key length of k=256 bits, which is also referred to as "Kuznyechik". This algorithm is one of the set of Russian cryptographic standard algorithms (called GOST algorithms).

1. Scope

The Russian Federal standard [GOST3412-2015] specifies basic block ciphers used as cryptographic techniques for information processing and information protection including the provision of confidentiality, authenticity, and integrity of information during information transmission, processing, and storage in computer-aided systems.

The cryptographic algorithms specified in this standard are designed both for hardware and software implementation. They comply with modern cryptographic requirements and put no restrictions on the confidentiality level of the protected information.

The standard applies to development, operation, and modernization of the information systems of various purposes.

конференция РусКрипто

Принципы синтеза перспективного алгоритма блочного шифрования с длиной блока 128 бит

Василий Шишкин

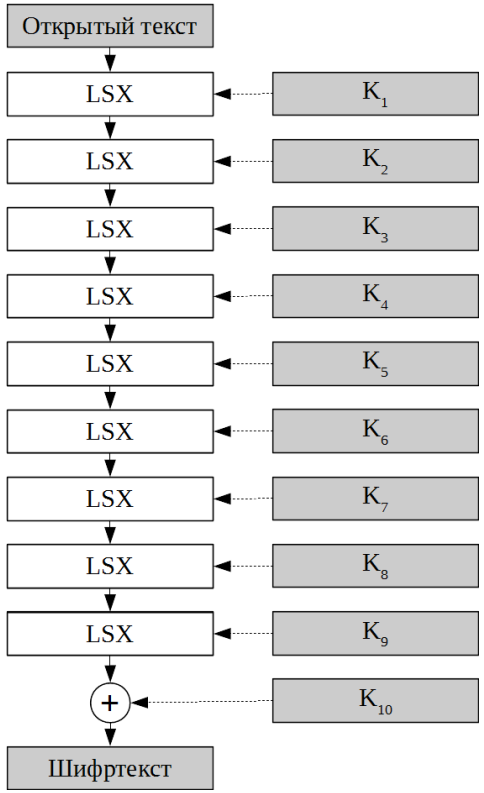
«РусКрипто'2013»

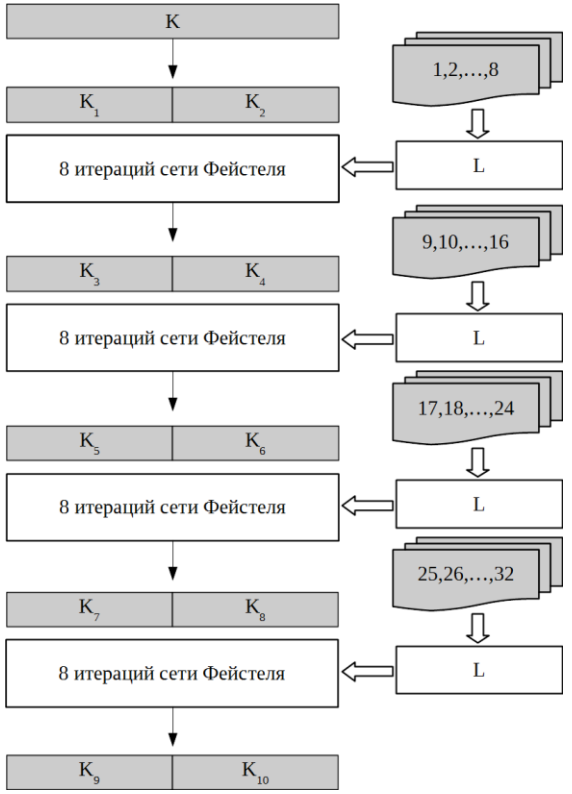
28 марта, 2013

2013 2015 2016 2018 2019

Блочный шифр «Кузнечик»

- длина блока – 128 бит
- длина ключа – 256 бит
- 9,5 итераций SP-сети
- ключевая развертка – сеть Фейстеля

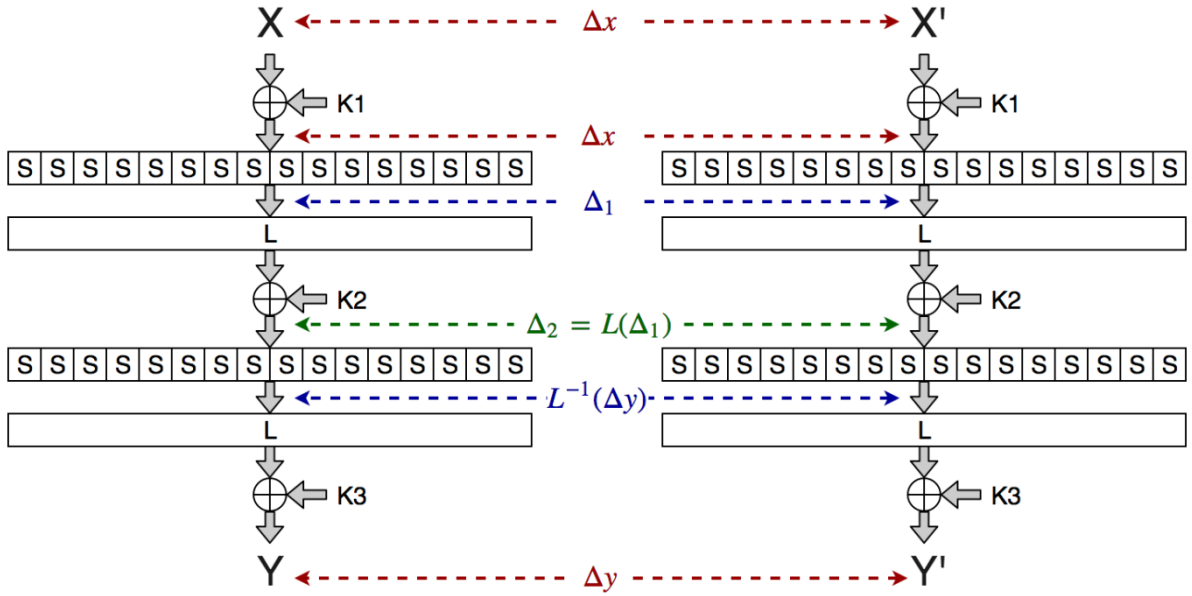




«Кузнечик» - 7 лет интенсивного криптоанализа

- статистические методы (линейный и дифференциальный)
- структурные методы (инвариантные подпространства, «встречи посередине», алгебраический с мультимножествами)
- со связанными ключами
- по побочным каналам и с внесением ошибок

Дифференциальный и линейный методы



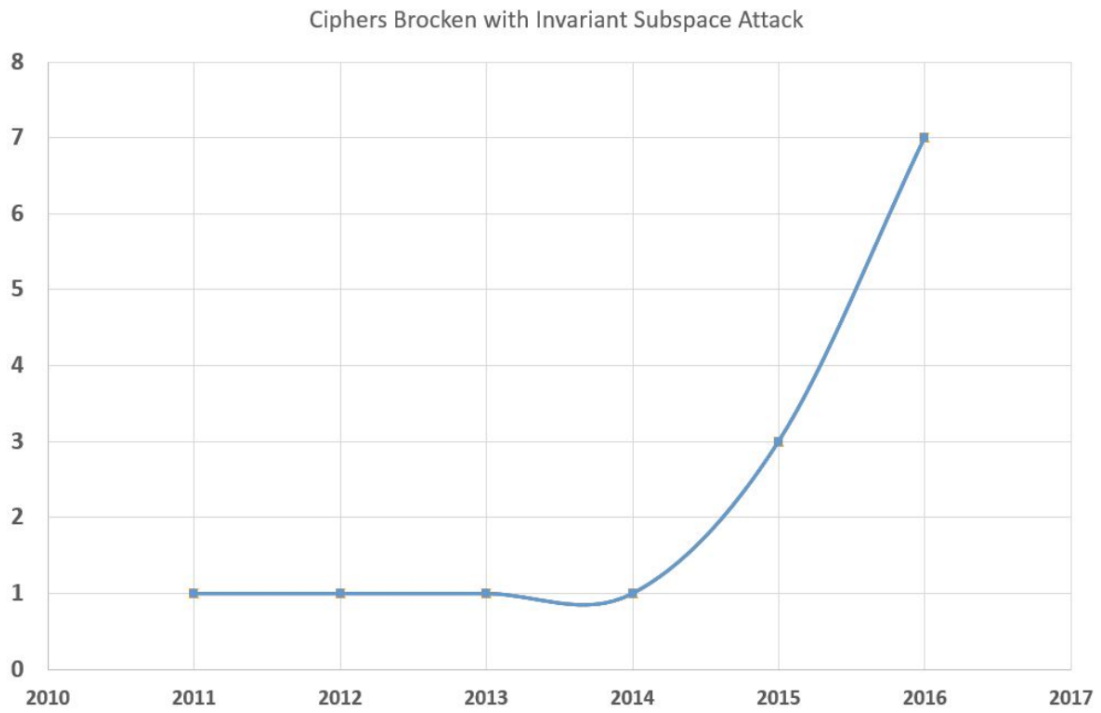
- Основные методы анализа блочных алгоритмов
- **Ф.М. Малышев**. Двойственность разностного и линейного методов в криптографии

Криптографический анализ шифра «Кузнечик» - дифференциальный и линейный методы

- **Vitaly Kiryukhin.** Exact maximum expected differential and linear probability for 2-round Kuznyechik

- Алгоритмы поиска линейных и разностных соотношений на 2 раунда
- MEDP = $2^{-86.66...}$
- MELP = $2^{-76.739...}$

Структурные методы анализа

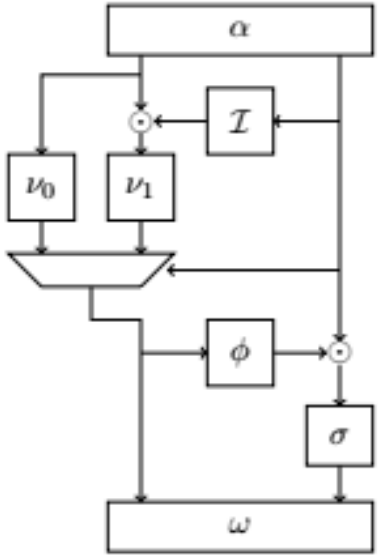


- Наиболее активно развивающееся направление
- Использование структур (например, подпространств), сохраняемых преобразованиями шифра
- **Gregor Leander**. Structural attacks on block ciphers

Хайли лайкли: «секретная» структура S-блока?

- **A. Biryukov**, **L. Perrin**, **A. Udovenko**. The Secret Structure of the S-Box of Streebog, Kuznechik and Stribob, 2015
- **A. Biryukov**, **L. Perrin**, **A. Udovenko**. Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1, 2016
- **L. Perrin**, **A. Udovenko**. Exponential S-Boxes: a Link Between the S-Boxes of BelT and Kuznyechik/Streebog, 2016
- **L. Perrin.** Partitions in the S-Box of Streebog and Kuznyechik, 2019

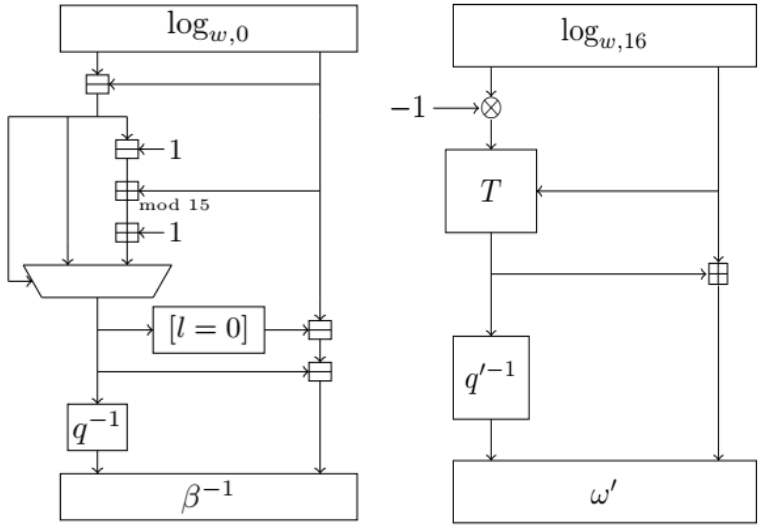
Авторы нашли «секретную» структуру



Хайли лайкли: «секретная» структура S-блока?

- **A. Biryukov**, **L. Perrin**, **A. Udovenko**. The Secret Structure of the S-Box of Streebog, Kuznechik and Stribob, 2015
- **A. Biryukov**, **L. Perrin**, **A. Udovenko**. Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1, 2016
- **L. Perrin**, **A. Udovenko**. Exponential S-Boxes: a Link Between the S-Boxes of BelT and Kuznyechik/Streebog, 2016
- **L. Perrin.** Partitions in the S-Box of Streebog and Kuznyechik, 2019

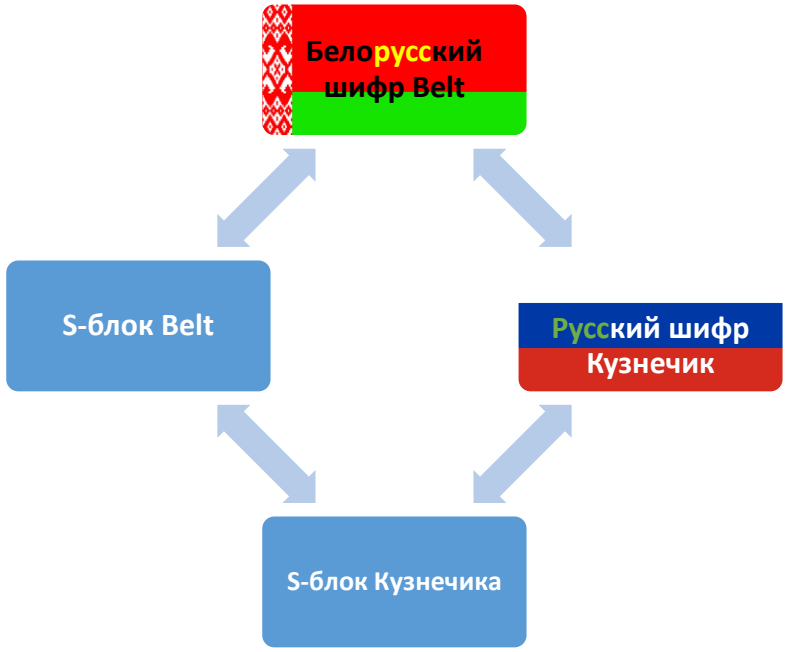
Авторы нашли еще две «секретные» структуры



Хайли лайкли: «секретная» структура S-блока?

- **A. Biryukov**, **L. Perrin**, **A. Udovenko**. The Secret Structure of the S-Box of Streebog, Kuznechik and Stribob, 2015
- **A. Biryukov**, **L. Perrin**, **A. Udovenko**. Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1, 2016
- **L. Perrin**, **A. Udovenko**. Exponential S-Boxes: a Link Between the S-Boxes of BelT and Kuznyechik/Streebog, 2016
- **L. Perrin.** Partitions in the S-Box of Streebog and Kuznyechik, 2019

А также следующую «таинственную» связь



Хайли лайкли: «секретная» структура S-блока?

- **A. Biryukov**, **L. Perrin**, **A. Udovenko**. The Secret Structure of the S-Box of Streebog, Kuznechik and Stribob, 2015
- **A. Biryukov**, **L. Perrin**, **A. Udovenko**. Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1, 2016
- **L. Perrin**, **A. Udovenko**. Exponential S-Boxes: a Link Between the S-Boxes of BelT and Kuznyechik/Streebog, 2016
- **L. Perrin.** Partitions in the S-Box of Streebog and Kuznyechik, 2019

Предложена еще одна, по словам авторов, самая правильная структура

Algorithm 1 A new decomposition of π.

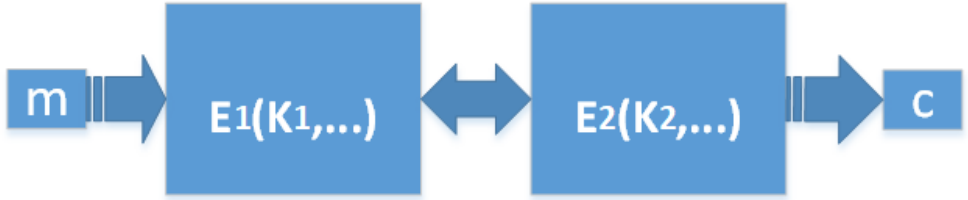
1: **function** $\pi(x \in \mathrm{GF}(2^8))$
2: **if** $x = 0$ **then**
3: **return** $\kappa(0)$
4: **else**
5: $k = \log_{\alpha}^{\mathrm{FLY}}(x)$
6: $i \leftarrow k \mod 17$; $j \leftarrow \lfloor k/17 \rfloor$
7: **if** $i = 0$ **then**
8: **return** $\kappa(16 - j)$
9: **else**
10: **return** $\kappa(16 - i) \oplus (\alpha^{17})^{s(j)}$
11: **end if**
12: **end if**
13: **end function**

Криптографический анализ шифра «Кузнечик» - метод «встречи посередине»

- **R. AlTawy**, **A. M. Youssef**. A Meet in the Middle Attack on Reduced Round Kuznyechik
- **M. Tolba**, **A. M. Youssef**. Improved Meet-in-the-Middle Attacks on Reduced Round Kuznyechik

- 6 раундов
- требуемая память – 2^{218} по 128 бит
- требуемый материал – 2^{113}
- вычислительная сложность – 2^{213}

$$E((K_1,K_2),m)=E_2(K_2,E_1(K_1,m))$$



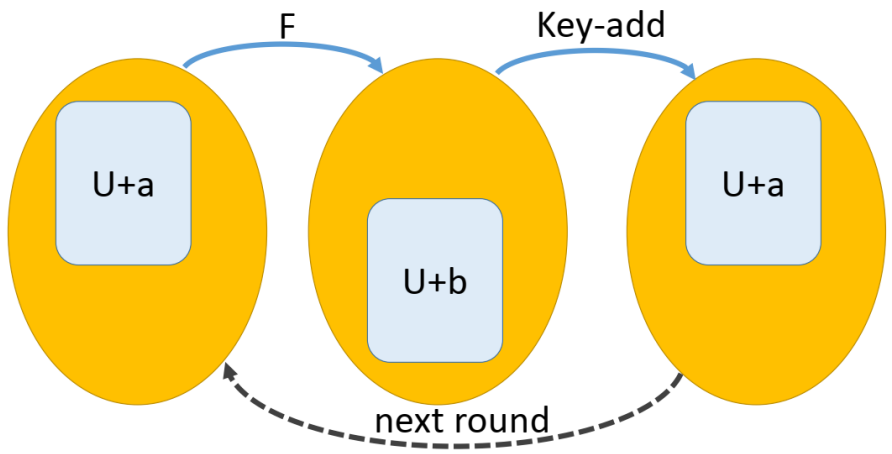
Криптографический анализ шифра «Кузнечик» – алгебраический анализ с мультимножествами

- **A. Biryukov**, **D. Khovratovich**, **L. Perrin**. Multiset-Algebraic Cryptanalysis of Reduced Kuznyechik, Khazad, and secret SPNs.
- используются алгебраические свойства преобразований на множествах специального вида

- 7 раундов
- требуемая память – 2^{140}
- требуемый материал – 2^{128}
- вычислительная сложность – 2^{155}

Криптографический анализ шифра «Кузнечик»

- **D. A. Burov**, **B.A. Pogorelov**. The influence of linear mapping reducibility on the choice of round constants



- Метод позволяет выделить классы слабых ключей, сохраняющих инварианты раунда
- Не применим к «Кузнечику», даже в случае замены констант

Криптографический анализ практических реализаций

- утечки по побочным каналам
- внесение/возникновение ошибок при выполнении алгоритма

Криптографический анализ шифра «Кузнечик» - побочные каналы

- **D. Fomin**. A timing attack on CUDA implementations of an AES-type block cipher

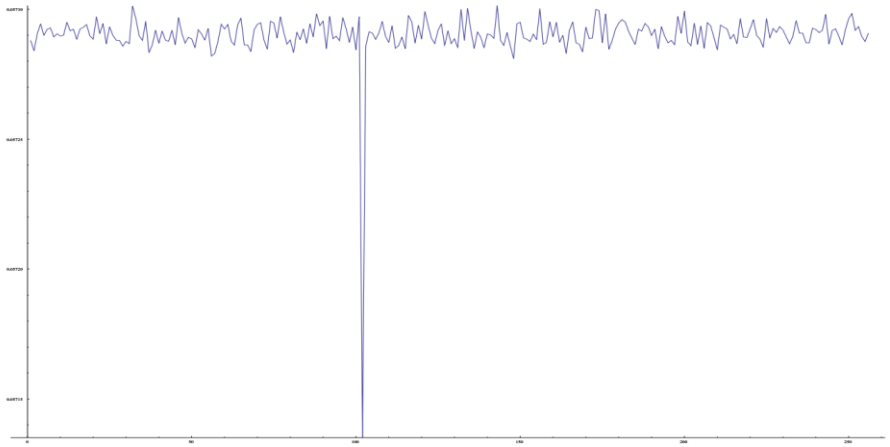
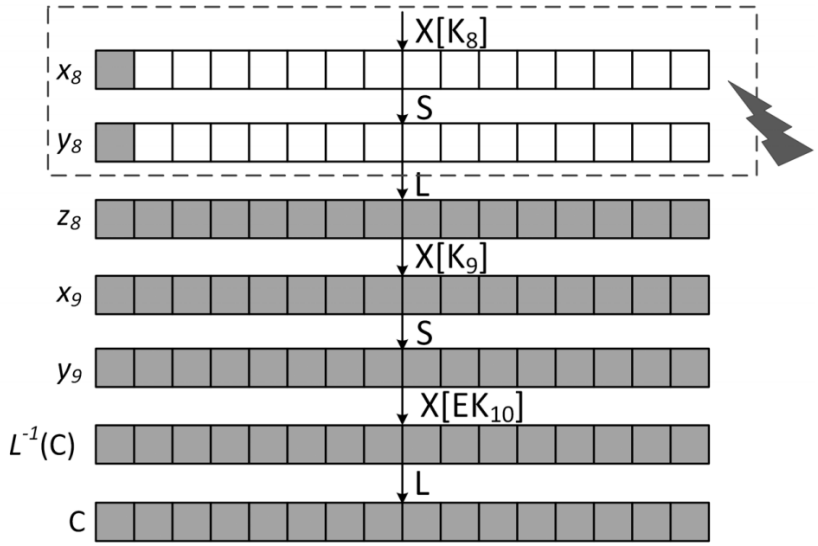


Fig. 1. Timing attack on GTX 285 (256MB array size)

- Показано, что в отличие от AES timing-атаки при реализации на GPU к «Кузнечику» не применимы

Криптографический анализ шифра «Кузнечик» - анализ с внесением ошибок

- **R. AlTawy**, **O. Duman**, **A. M. Youssef**. Fault Analysis of Kuznyechik



- Нарушитель может вносить случайные ошибки на 8 итерации
- Необходимо две пары шифртекстов (полученных при наличии двух ошибок)
- Последовательно определяются байты ключа K_{10}
- Затем определяется K_9

Атаки со связанными ключами

- используют пары открытый/шифрованный текст, полученные на различных ключах, связанных некоторым соотношением
- в общем случае неэффективны, поскольку требуется производить поиск ключей с заданным соотношением
- **V. Rudskoy.** On zero practical significance of «Key recovery attack on full GOST block cipher with zero time and memory»

Криптографический анализ шифра «Кузнечик» со связанными ключами

- **E. Alekseev**, **K. Goncharenko**, **G. Marshalko**. Provably secure counter mode with related key-based internal re-keying
- **Е.А. Ищукова**, **А.В. Красовский**, **И.Ю. Половко.** Анализ шифра «Кузнечик» методом связанных ключей

- Вследствие сложной ключевой развертки атака применима только к варианту шифра с уменьшенным числом раундов и упрощенной ключевой разверткой

Резюме

- за прошедшие 7 лет российскими и зарубежными специалистами проведены исследования стойкости блочного шифра «Кузнечик» к основным типам атак, рассматриваемых для блочных шифров
- каких-либо слабостей не обнаружено
- можно ожидать, что «Кузнечик» и дальше будет являться объектом пристального изучения со стороны криптографического сообщества

Спасибо за внимание

Вопросы