Огонь, вода и медные трубы: 10 лет стандартизации «Кузнечика»

Иванов А.В., Матюхин Д.В., Маршалко Г.Б., Шишкин В.А.

19 марта 2025 г.

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
2015

МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ (МГС)
INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION (ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ 34.12— 2018

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Блочные шифры

Издание официальное

Москва
Стандартинформ
2018

конференция
РусКрипто

Принципы синтеза перспективного алгоритма блочного шифрования с длиной блока 128 бит

Василий Шишкин

«РусКрипто'2013»

28 марта, 2013

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"

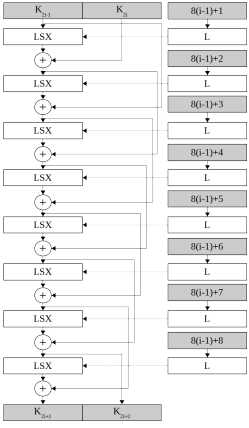
Abstract

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).

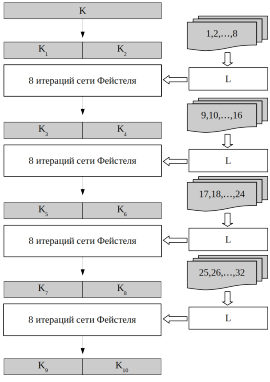
2013 2015 2016 2018

Блочный шифр «Кузнечик»

- Длина блока – 128 бит
- Длина ключа – 256 бит
- Большое линейное преобразование 128×128 бит
- 9,5 итераций SP-сети
- Ключевая развертка – сеть Фейстеля



Шифрование



Ключевая развертка

Стандартизированный алгоритм «Кузнечик»: в фокусе внимания

- Исследование стойкости к различным методам криптографического анализа
- Разработка эффективных реализаций на различных вычислительных платформах
- Использование алгоритма в других стандартизированных криптографических механизмах, средствах криптографической защиты информации, открытых библиотеках

ОГОНЬ: криптографический анализ

- Статистические методы (линейный и разностный)
- Структурные методы (инвариантных подпространств, согласования)
- Алгебраический с мультимножествами
- Со связанными ключами
- С использованием квантовых вычислителей
- С использованием информации из побочных каналов
- С внесением ошибок

Линейный и разностный методы

- X. Chen, G. Liu, B.Sun, C. Li, Impossible differentials for SPN-ciphers (2017)
  - Поиск разностного соотношения, имеющего нулевую вероятность
  - Невозможный дифференциал на 3 итерации
- Е. Толоманенко, Дифференциальный анализ трех раундов шифра «Кузнечик» (2018)
  - Вероятность появления разностного соотношения
  - Для трех итераций вероятность появления 2^{-108}
- V. Kiryukhin, Exact maximum expected differential and linear probability for 2-round Kuznyechik (2018)
  - Максимальные значения средних по ключам разностной и линейной характеристик
  - Для двух итераций $MEDP = 2^{-86.66\ldots}$, $MELP = 2^{-76.739\ldots}$
- V. Kiryukhin, An algorithm for bounding non-minimum weight differentials in 2-round LSX-ciphers (2020)
  - Максимальные значения средних по ключам разностной и линейной характеристик заданного веса
  - Для двух итераций $MEDP^{+}_{\mathcal{B}+3} = 2^{-88.42\ldots}$, $MELP^{+}_{\mathcal{B}+3} = 2^{-80.50\ldots}$

Обобщения: структурные методы анализа

- D. Burov, B. Pogorelov,The influence of linear mapping reducibility on the choice of round constants (2017)
  - Метод позволяет выделить классы слабых ключей, сохраняющих инварианты на итерациях шифра
  - Не применим к «Кузнечику», даже в случае замены констант
- D. Fomin, On the impossibility of invariant attack on Kuznyechik (2021)
  - Метод основан на построении инвариантных подпространств для преобразований шифра
  - Не применим к «Кузнечику»
- D. Fomin, О существовании нелинейных инвариантов специального вида для раундовых преобразований XSL-алгоритмов (2021)
  - Исследуются способы построения инвариантных подпространств одного типа
  - Исследуемых подпространств для алгоритма «Кузнечик» не существует
- M. ElSeikh, A.M. Youssef, On MILP-based automated search for bit-based division property for ciphers with (large) linear layers (2021)
  - Поиск интегрального соотношения
  - Для 4 итераций на материале 2^{120} пар открытого/шифрованного текстов
- С. Давыдов, Об инвариантных подпространствах матриц-циркулянтов и рекурсивных матриц (2023)
  - Исследуются способы построения инвариантных подпространств одного типа
  - Исследуемых подпространств для алгоритма «Кузнечик» не существует

Алгебраический анализ с мультимножествами

- A. Biryukov, D. Khovratovich, L. Perrin, Multiset-Algebraic Cryptanalysis of Reduced Kuznyechik, Khazad, and secret SPNs (2017)
  - Комбинация интегрального метода и метода частичных сумм
  - Для 7 итераций на материале 2^{128} с трудоемкостью $2^{154,5}$ операций зашифрования
- O. Dunkelman, S. Ghos, N. Keller, G. Leurent, A. Marmor, V. Mollimard, Partial sums meet FFT: Improved attack on 6-round AES (2023)
  - Комбинация интегрального метода, метода частичных сумм и применения быстрого преобразования Фурье
  - Для 7 итераций на материале 2^{128} с трудоемкостью 2^{148}

Криптографический анализ со связанными ключами

- E. Alekseev, K. Goncharenko, G. Marshalko, Provably secure counter mode with related key-based internal re-keying (2018)
  - Алгоритм определения ключа на материале, полученном на ключах, связанных определенным соотношением
  - Для 3 итераций алгоритма, алгоритм развертки ключа сокращен до 2 итераций
- V. Kiryukhin, Related-key attack on 5-round Kuznyechik (2019)
  - Алгоритм определения ключа на материале, полученном на ключах, связанных определенным соотношением
  - Для 5 итераций алгоритма, алгоритм развертки ключа сокращен до 2 итераций

Метод согласования

- R. AlTawy, A.M. Youssef, A Meet in the Middle Attack on Reduced Round Kuznyechik (2015)
  - Использует разделение неизвестных переменных и их перебор с использованием памяти
  - Для 5 итераций с памятью $2^{153,3}$ на материале – 2^{113} и трудоемкостью – $2^{140,3}$ операций зашифрования
- M. Tolba, A.M. Youssef, Improved Meet-in-the-Middle Attacks on Reduced Round Kuznyechik (2015)
  - Использует разделение неизвестных переменных и их перебор с использованием памяти
  - Для 6 итераций с памятью 2^{225} на материале – 2^{113} и трудоемкостью – 2^{231} операций зашифрования

Квантовый криптоанализ

- D. Denisenko, G. Marshalko, M. Nikitenkova, V. Rudskoi, V. Shishkin, Estimating the Complexity of Grover's Algorithm for Key Search of Block Ciphers Defined by GOST R 34.12-2015 (2019)
  - Оцениваются параметры алгоритма определения ключа на квантовом вычислителе:
    - Количество кубит – 1024
    - Количество вентилей CNOT – 1795232

Побочные каналы

- D. Fomin, A timing attack on CUDA implementations of an AES-type block cipher (2015)
  - Восстановление ключа на основе измерения времени выполнения зашифрования
  - Не применим к «Кузнечику»
- C. Delaunay, A. Istomin, E. Filiol, Kuznyechik, optimized implementations on FPGA and microcontrollers and their DPA analysis resistance (2019)
  - Восстановление ключа по измерению энергопотребления при зашифровании
  - Не применим к «Кузнечику»
- T. Lavrentieva, S. Matveev, Side-channel countermesure based on decomposed s-boxes of Kuznyechik (2020)
  - Метод защиты от атак по побочным каналам, основанный на маскировании преобразований S-блока

Анализ с внесением ошибок

- R. AlTawy, O. Duman, A.M. Youssef, Fault Analysis of Kuznyechik (2019)
  - Восстановление ключа на основе анализа результата зашифрования, при выполнении которого индуцируются ошибки
  - Нарушитель вносит случайные ошибки на 8-й и 7-й итерациях шифрования. Необходимы две пары шифртекстов (полученных при наличии двух ошибок и без)
  - Последовательно определяются байты ключей K_{10} и K_9 , откуда восстанавливается ключ

ВОДА: поиск «секретной» структуры

- 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)

Несколько вариантов эквивалентных представлений S-блока:

- не привели к построению новых методов криптографического анализа или совершенствованию известных
- привели к появлению новых эффективных реализаций алгоритма

Эффективная реализация S-блока

- N. Borisenko, D. Vasinev, D.T. Khoang, Method of forming S-blocks with minimum number of logic elements (2016)
  - Исследуется возможность представления подстановки в базисе операций AND, XOR, OR и NOT
  - 681 операция
- O. Avraamova, D. Fomin, V. Serov, A. Smirnov, V. Shokov, A compact bit-sliced representation of Kuznyechik S-box (2020)
  - 235 операций
- O.C. Puente, R.F. Leal, R.A. de la Cruz Jimenez, On the bit-slice representations of some nonlinear bijective transformations (2023)
  - 176 операция
- D. Fomin, D. Trifonov, Computational work for some TU-based permutations (2023)
  - 169 операций

Эффективная реализация линейного преобразования

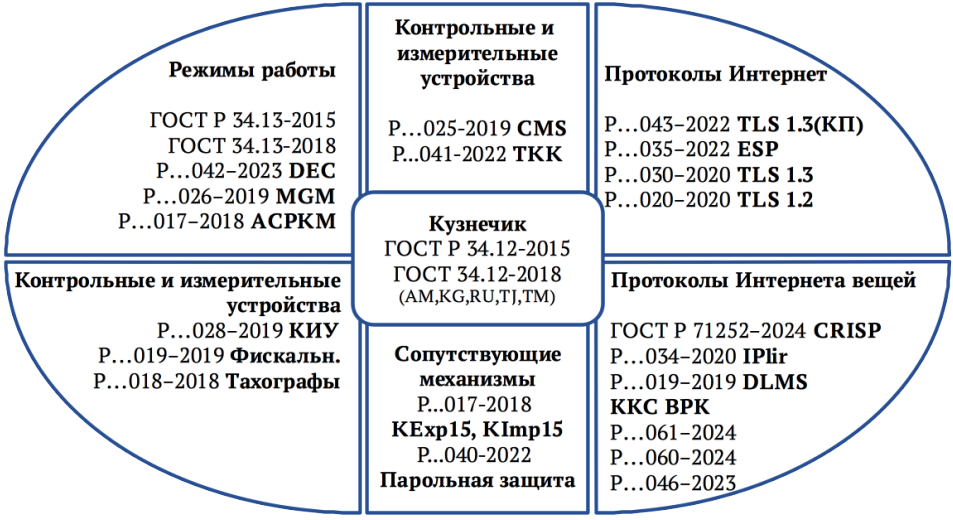
- С. Давыдов, В. Шишкин, Способы разложения рекурсивных матриц и их применение к реализации линейных преобразований (2023)
  - Предложены способы разложения рекурсивных матриц, которые позволяют строить реализацию алгоритма «Кузнечик», сравнимую по скорости с реализацией, использующей табличное задание преобразований, но использующую меньше памяти

МЕДНЫЕ ТРУБЫ: реализация на различных платформах[1]

- И. Калистру, М. Бородин, А. Рыбкин, Р. Гладько, Способы реализации алгоритма «Кузнечик» на программируемых логических интегральных схемах (2018)
  - ПЛИС Kintex-7
  - 51,2 Гбит/с
- А. Борисов, Е. Мясников, Реализация алгоритмов шифрования «Магма» и «Кузнечик» с помощью HIP (2020)
  - AMD Radeon Vega 56
  - 176 Гбит/с
- И. Гафуров, Высокоскоростная программная реализация алгоритмов шифрования из ГОСТ Р 34.12-2015 (2022)
  - Intel Core i3 9100f
  - 195 Мбайт/с
- Ю. Гольчевский, Д. Ушаков, Ускорение криптографических вычислений путем низкоуровневой оптимизации базовых блоков (2023)
  - разные процессоры
  - до 240 Мбайт/с

[1] Также Роспатентом зарегистрировано большое количество патентов на изобретения и свидетельств о регистрации программ для ЭВМ, реализующих «Кузнечик»

Использование в стандартизированных механизмах



Резюме

- За прошедшие 10 лет российскими и зарубежными специалистами проведены всесторонние исследования стойкости блочного шифра «Кузнечик» к различным типам атак
- Каких-либо криптографических слабостей не обнаружено
- Получил широкое внедрение
- «Кузнечик» продолжает оставаться объектом пристального изучения со стороны криптографического сообщества, результаты исследований подтверждают его соответствие современным требованиям к стойкости блочных шифров

Доклад про «КузНеч и К» посвящается...

80-летию со дня рождения АЛЕКСАНДРА АЛЕКСАНДРОВИЧА НЕЧАЕВА

- Автора более 100 научных работ, соавтора классического пособия «Алгебра»
- Воспитавшего 12 кандидатов, 3 из которых стали докторами наук
- Предложившего идею построения линейного преобразования «Кузнечика»

65-летию со дня рождения АЛЕКСЕЯ СЕРГЕЕВИЧА КУЗЬМИНА

- Автора более 50 научных работ, соавтора многократно переизданного пособия «Основы криптографии»
- Воспитавшего 15 кандидатов наук
- Председателя технического комитета ТК 26 и программного комитета CTCrypt, члена программного комитета РусКрипто