

«ПРАПОР-К»

**перспективное отечественное
семейство низкоресурсных
криптографических алгоритмов**

Андрей Дмух, Дмитрий Трифонов

«ПРАПОР»

(Перспективные Российские Алгоритмы для Платформ с Ограниченными Ресурсами)
Выбор принципиальной схемы

Что учитывалось при разработке:

- ✓ Унификация
- ✓ Имеющаяся элементная база
- ✓ Криптография
- ✓ Эффективность реализации на ПЛИС (СБИС)
- ✓ Санкционные ограничения

Выбор принципиальной схемы:

- ✓ SP-сеть
- ✓ XSL*- (XSLP-) сеть
- ✓ Сеть Фейстеля

«ПРАПОР-К»

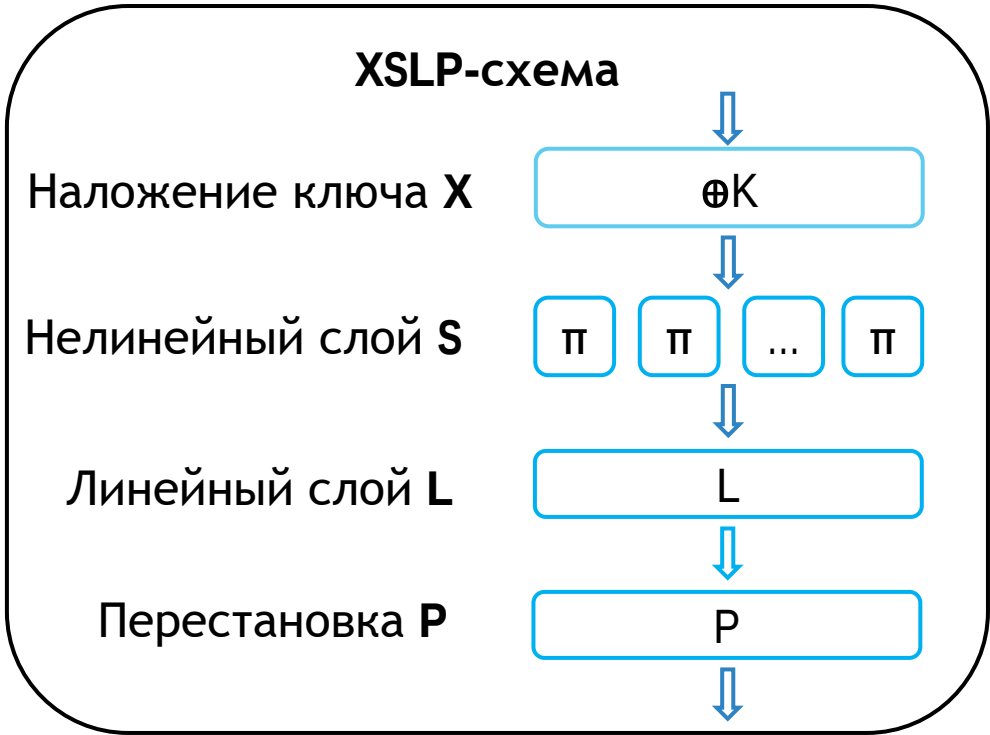
Семейство из 20 алгоритмов

Длина блока $n \in \{64, 80, 96, 112, 128\}$

Длина ключа $k \in \{192, 256, 320, 384\}$

* идеи: Малышев Ф.М., Посельников В.М., Зубков А.М., Нечаев А.А.

«ПРАПОР-К». Общие сведения

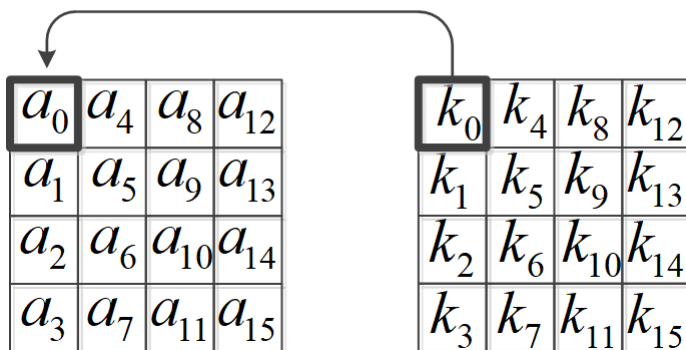


Число раундов в зависимости от длины блока n (битов) и длины ключа k (битов)

$n \backslash k$	192	256	320	384
64	15	16	17	18
80	15	16	16	17
96	14	15	16	16
112	14	15	15	16
128	14	14	15	15

«ПРАПОР-К»(64, k), раундовое преобразование

Наложение ключа X



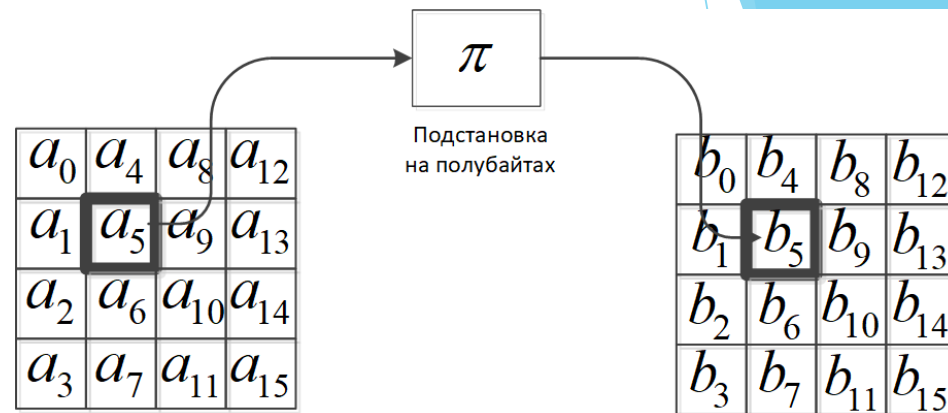
Антипкин В.Г., Пасько Д.О.,
Рудской В.И., Трифонов Д.И. (2023)

Линейный слой L



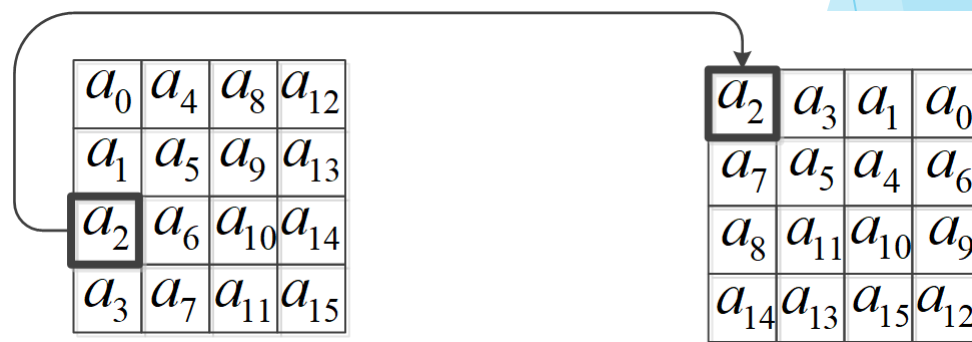
Малышев Ф.М. (1993)
Нечаев А.А. (1999)

Нелинейный слой S



Менячихин А.В., Буров Д.А. (2019)

Перестановка полубайтов P



Малышев Ф.М. (1984)

«ПРАПОР-К»

Функция зашифрования

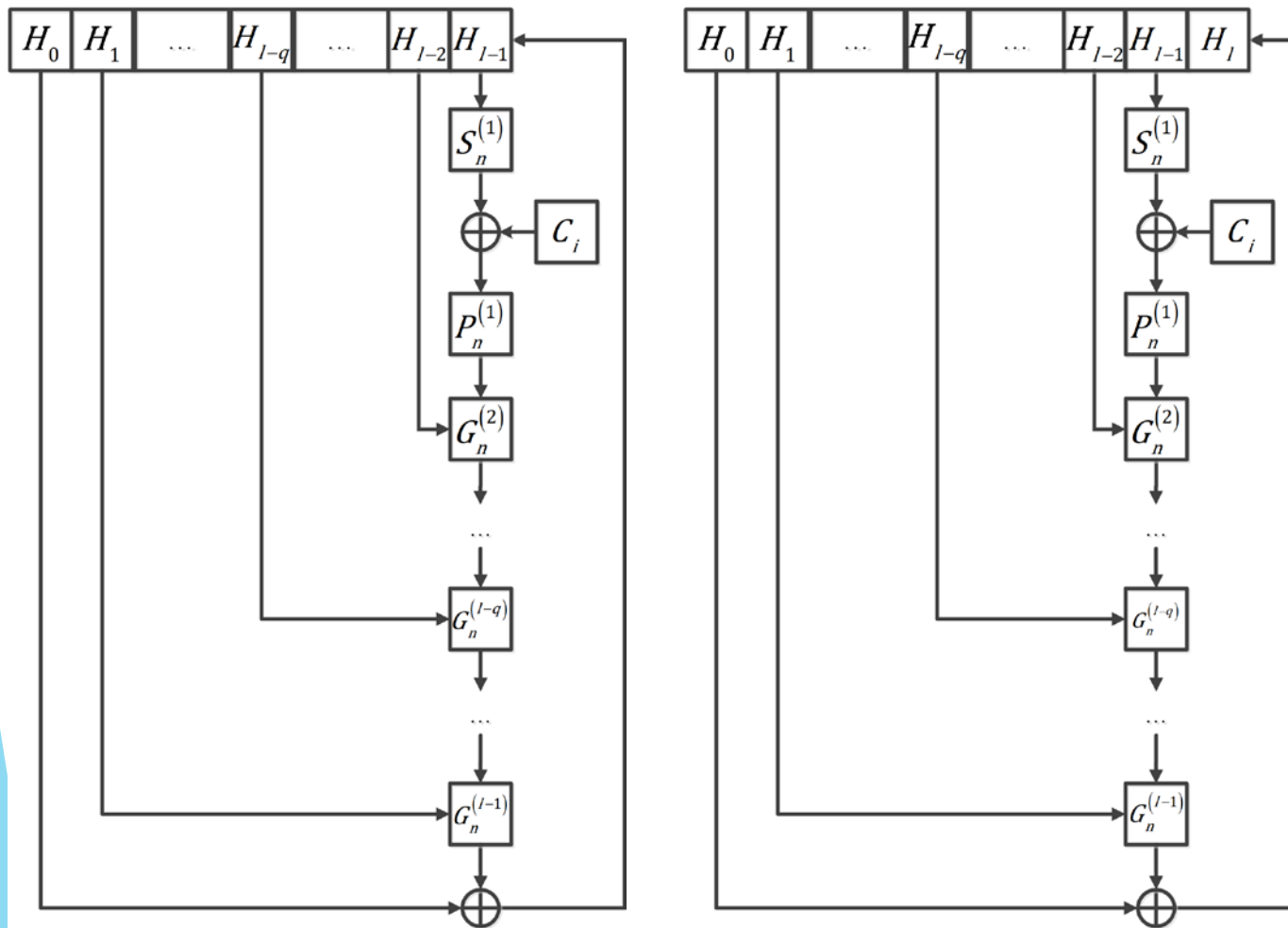
При $n \in \{64, 80\}$:

$$F_n(a, K) = X_n[M_{N+1}]P_n L_n S_n X_n[M_N] \dots P_n L_n S_n X_n[M_1](a);$$

При $n \in \{96, 112, 128\}$:

$$F_n(a, K) = X_n[M_{N+1}]P_n L_n P_n L_n S_n X_n[M_N] \dots P_n L_n P_n L_n S_n X_n[M_1](a).$$

«ПРАПОР-К»(n, k), алгоритм развёртывания ключа, $k \geq 3n$



$$l = \lceil k/n \rceil$$

$H_0, \dots, H_{l-1}$ – ячейки размера n битов

H_l – ячейка размера $k - n \cdot l$ битов

Начальное заполнение – рабочий ключ

$$K = (K_0, \dots, K_l),$$

$$K_0, \dots, K_{l-1} \in V_n, K_l \in V_{k-n \cdot l}$$

$\hat{S}_{n,k}^{(j)}$ – нелинейное преобразование, аналогичное S

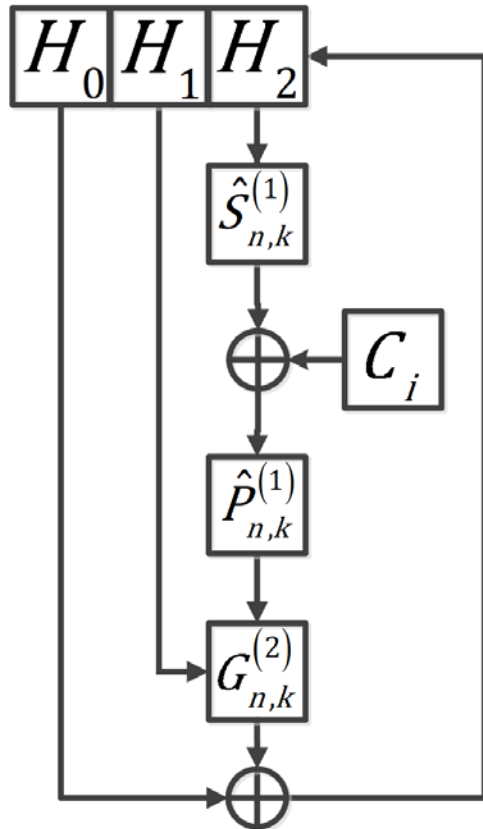
$\hat{P}_{n,k}^{(j)}$ – перестановка битов

C_i – константы, зависящие от номера такта i

Такт работы заключается в сдвиге заполнения регистра на n битов влево и записи на освободившееся место n битов, полученных с функции усложнения

Первые $l \cdot n$ битов начального заполнения образуют первые l раундовых ключей. Далее первые $l \cdot n$ битов заполнения через каждые $t(n, k)$ тактов образуют очередные l раундовых ключей

«ПРАПОР-К»(n, k), алгоритм развёртывания ключа, $k < 3n$

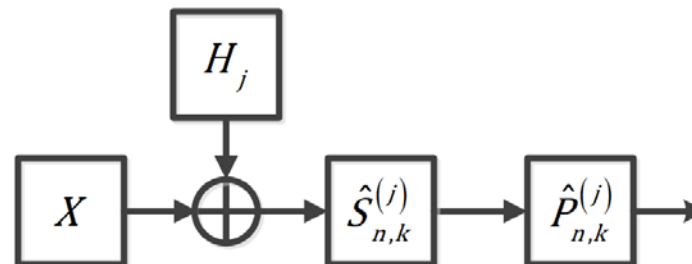


H_0, H_1, H_2 – ячейки размера n битов

Начальное заполнение – рабочий ключ K , дополненный до длины $3n$ битов нулями

Такт работы и функция усложнения аналогичны случаю $k \geq 3n$

$G_{n,k}^{(j)}(H_j, X):$



Режимы работы

По ГОСТ Р 34.13-2015, ГОСТ 34.13-2018:

- Режим простой замены (Electronic Codebook, ECB)
- Режим гаммирования (Counter, CTR)
- Режим гаммирования с обратной связью по выходу (Output Feedback, OFB)
- Режим простой замены с зацеплением (Cipher Block Chaining, CBC)
- Режим гаммирования с обратной связью по шифртексту (Cipher Feedback, CFB)
- Режим выработки имитовставки (Message Authentication Code algorithm, CMAC)

По Изменению № 1 ГОСТ 34.13-2018:

- Режим аутентифицированного шифрования с ассоциированными данными (Authenticated Encryption with Associated Data, AEAD) – алгоритмы с длиной блока 64 или 128 битов и длиной ключа 256 битов
- Режим гаммирования с преобразованием ключа (Counter Advanced Cryptographic Prolongation of Key Material, CTR-ACPKM) – алгоритмы с длиной ключа 192 или 256 битов, с обоснованием возможности обработки заданного объёма материала на одном начальном ключе

Некоторые результаты криптографического анализа

Теорема 1. Для показателя рассеивания $\theta = \theta(r)$ линейной среды XSLP-шифра «ПРАПОР-К» на $r \in \mathbb{N}$ итераций (относительно линейного метода) имеем:

1. при $k' = 4$

$$\theta(r) = (m' + 1)^2 \left\lfloor \frac{r-1}{4} \right\rfloor + \theta \left(r - 4 \left\lfloor \frac{r-1}{4} \right\rfloor \right), \quad r \geq 5,$$

$$\theta(1) = 1, \quad \theta(2) = m' + 1, \quad \theta(3) = 2m' + 1, \quad \theta(4) = (m')^2 + 2m' + 1;$$

2. при $k' = 5$

$$\theta(r) \geq (m' + 1)^2 \left\lfloor \frac{r-1}{4} \right\rfloor + \theta \left(r - 4 \left\lfloor \frac{r-1}{4} \right\rfloor \right), \quad r \geq 5,$$

$$\theta(1) = 1, \quad \theta(2) = m' + 1, \quad \theta(3) = 2m' + 1, \quad \theta(4) = (m')^2 + 2m' + 1.$$

Некоторые результаты криптографического анализа

Решатели смешанного линейно-целочисленного программирования
(Mixed Integer Linear Programming – MILP)

XS y_1 **LPLP** z_1 **XS** y_2 **LPLP** z_2 **XS** y_3 **LPLP** z_3 **XS** y_4 **LPLP** z_4

	MILP (без матриц)	MILP (с матрицами)
$\sum r(y_i)$	22	≥ 24

Некоторые результаты криптографического анализа АРК

Утверждение 1. *Если найдутся две пары наборов входных переменных $\bar{x}$ и $\bar{x}'$ соседних по x_j таких, что для одной пары значения координатных функций f_i совпадают, а для другой пары значения различны, то f_i зависит от x_j существенно и нелинейно.*

1. Для всех $n = 64, 80, 96, 112, 128$; $k = 192, 256, 320, 384$ выполнить шаги 2-5 алгоритма.
2. Для всех $i = 1, \dots, \mathfrak{L}$ выполнить шаги 3-5 алгоритма.
3. Случайно вырабатываем N пар заполнения регистра H , соседних по i -й переменной.
4. Для всех N пар вырабатываем заполнение $H(t)$ регистра H в такт с номером t .
5. Проверяем получившиеся наборы пар заполнения регистра H на существенную и нелинейную зависимость по i -й переменной согласно утверждению 1.

«ПРАПОР-К» – эффективность программной реализации. Техника `vperm` [1,2]

Основная идея: в один 128- или 256-битный регистр записывать несколько блоков открытого текста и проводить манипуляции с регистром таким образом, чтобы обрабатывать эти блоки параллельно.

Эксперименты: Intel Core i9-10980XE с базовой частотой 3000 МГц.

	AES-192	LED-128	ПРАПОР-К (64,192)
Производительность, тактов на байт	6.7 – 9.3	27	8.3

[1] Mike Hamburg. Accelerating AES with Vector Permute Instructions. In Christophe Clavier and Kris Gaj, editors. Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop, Lausanne, Switzerland, September 6-9, 2009, Proceedings, volume 5747 of LNCS. Springer, 2009, pages 18–32.

[2] Ryad Benadjila, Jian Guo, Victor Lomne, and Thomas Peyrin. Implementing Lightweight Block Ciphers on x86 Architectures. Cryptology ePrint Archive, Report 2013/445, 2013.

Эффективность программной реализации подстановки из раундовой функции

Идея Фомина, Соловьёва:
34 операции, базис AND, XOR

Общие части

$t_0 = x_0 \text{ AND } x_1$

$t_1 = x_2 \text{ AND } x_3$

$t_2 = x_1 \text{ AND } x_2$

$t_3 = x_1 \text{ AND } x_3$

$t_4 = x_0 \text{ AND } x_2$

$t_5 = t_2 \text{ AND } x_3 \text{ // } x_1 * x_2 * x_3$

$t_6 = t_0 \text{ AND } x_3 \text{ // } x_0 * x_1 * x_3$

$t_7 = t_4 \text{ AND } x_3 \text{ // } x_0 * x_2 * x_3$

$t_8 = t_0 \text{ AND } x_2 \text{ // } x_0 * x_1 * x_2$

$y_0 = x_0 \text{ XOR } t_0 \text{ XOR } x_2 \text{ XOR } x_3 \text{ XOR } t_1 \text{ XOR } t_5$

$y_1 = 1 \text{ XOR } x_0 \text{ XOR } t_0 \text{ XOR } t_2 \text{ XOR } t_3 \text{ XOR } t_6 \text{ XOR } t_7 \text{ XOR } t_5$

$y_2 = x_0 \text{ XOR } t_4 \text{ XOR } t_3 \text{ XOR } t_6 \text{ XOR } t_1$

$y_3 = x_0 \text{ XOR } x_1 \text{ XOR } x_2 \text{ XOR } t_4 \text{ XOR } t_2 \text{ XOR } t_8 \text{ XOR } t_3 \text{ XOR } t_1 \text{ XOR } t_7 \text{ XOR } t_5$

SAT-решатели:

22 операции, базис AND, OR, XOR, NAND, NOR, XNOR, ANDN, ORN

$y_0 = x_2 \text{ XOR } (x_3 \text{ XOR } \text{NOT}(x_1 \text{ OR } (x_0 \text{ XOR } \text{NOT}(x_2 \text{ AND } x_3))))$

$y_1 = \text{NOT}(x_0 \text{ XOR } \text{NOT}((x_1 \text{ XOR } \text{NOT}(x_0 \text{ AND } x_2)) \text{ OR } \text{NOT}(x_3 \text{ OR } (x_0 \text{ XOR } x_2))))$

$y_2 = \text{NOT}(x_0 \text{ XOR } \text{NOT}((x_0 \text{ XOR } x_3) \text{ AND } (x_2 \text{ XOR } (x_1 \text{ AND } \text{NOT } x_0))))$

$y_3 = x_0 \text{ XOR } ((x_1 \text{ OR } (x_2 \text{ AND } \text{NOT } x_0)) \text{ AND } ((x_0 \text{ AND } x_2) \text{ OR } \text{NOT } x_3))$

«ПРАПОР-К» – эффективность реализации

ПЛИС Kintex UltraScale xsku040-ffva1156-2-е на частоте 312.5 МГц, базовый блочный шифр, среда разработки Vivado 24.04

Без ключевой развёртки

	LUT, $V_6 \rightarrow V_1$	D-triggers	CARRY8
«Магма» (две копии)	4096 (1.69%)	4352 (0.90%)	256 (0.84%)
«Кузнечик»	15181 (6.26%)	19840 (4.09%)	0
«ПРАПОР-К»(128, 256)	5538 (2.28%)	3712 (0.77%)	0

С ключевой развёрткой

	LUT, $V_6 \rightarrow V_1$	D-triggers	CARRY8
«Магма» (две копии)	4096 (1.69%)	4352 (0.90%)	256 (0.84%)
«Кузнечик»	89378 (36.87%)	98432 (20.30%)	0
«ПРАПОР-К»(128, 256)	23654 (9.76%)	27792 (5.73%)	0

Вместе с Заключением

- В работе предлагается к апробации семейство низкоресурсных криптографических алгоритмов «ПРАПОР-К», предназначенных для реализации на платформах с ограниченными ресурсами. Приведены некоторые результаты криптографических исследований алгоритмов семейства, а также результаты по эффективности их реализации на различных платформах.
- Наилучшими методами анализа алгоритмов семейства «ПРАПОР-К» являются универсальные методы, при условии использования в указанных выше стандартизированных режимах работы рекомендаций на объём материала, обрабатываемого на одном ключе (порядка $2^{n/2} \sqrt{\pi_0}$, где π_0 - максимальная допустимая вероятность эффективного применения методов криптографического анализа, n - размер блока в битах
- Полная спецификация и контрольные примеры: см. [Матюхин Д.В. Если не ГОСТ, но очень хочется: «ПРАПОР-К» и «Рамен-К» — новые семейства \(низкоресурсных\) блочных шифров. Рускрипто 2026.](#)