КРИПТОНИТ

Концепции построения малоресурсных блочных шифрсистем:

так ли нужны максимально рассеивающие линейные преобразования?

С.А. Давыдов, АО «НПК «Криптонит»

Малоресурсные алгоритмы

КРИПТОНИТ

Свойства:

- минимизация мощности
- минимизация энергии
- пропускная способность (задержка)
- площадь микросхемы

Универсальная оценка*

$$\frac{\text{пропускная способность}}{\text{площадь}}$$

*Banik, Subhadeep, Sumit Kumar Pandey, Thomas Peyrin, Yu Sasaki, Siang Meng Sim and Yosuke Todo. “GIFT: A Small Present - Towards Reaching the Limit of Lightweight Encryption.” Workshop on Cryptographic Hardware and Embedded Systems (2017)

Особенности реализации на ASIC

КРИПТОНИТ

1 GE (Gate Equivalence) – площадь NAND

Библиотека		NAND NOR	NOT	XOR XNOR	AND OR	ANDN ORN	NAND3 NOR3	XOR3 XNOR3	MAOI1	MOAI1
UMC	180nm	1.00	0.67	3.00	1.33	1.67	1.33	4.67	2.67	2.00
NanGate	45nm	1.00	0.67	2.00	1.33	-	1.33	-	-	-

Operation	Function	Operation	Function
NAND	$(a, b) \rightarrow \neg(a \wedge b)$	XOR	$(a, b) \rightarrow a \oplus b$
NOR	$(a, b) \rightarrow \neg(a \vee b)$	XNOR	$(a, b) \rightarrow \neg(a \oplus b)$
AND	$(a, b) \rightarrow a \wedge b$	NAND3	$(a, b, c) \rightarrow \neg(a \wedge b \wedge c)$
OR	$(a, b) \rightarrow a \vee b$	NOR3	$(a, b, c) \rightarrow \neg(a \vee b \vee c)$
NOT	$a \rightarrow \neg a$	ANDN	$(a, b) \rightarrow \neg a \wedge b$
MAOI1	$(a, b, c, d) \rightarrow \neg((a \wedge b) \vee (\neg(c \vee d))$	ORN	$(a, b) \rightarrow \neg a \vee b$
MOAI1	$(a, b, c, d) \rightarrow \neg((a \vee b) \wedge (\neg(c \wedge d))$		

Thomas Peyrin, Lightweight Symmetric-Key Cryptography, CTCRYPT 2018
Jean, Jérémy, Thomas Peyrin, Siang Meng Sim and Jade Tourteaux. “Optimizing Implementations of Lightweight Building Blocks.” IACR Trans. Symmetric Cryptol. 2017 (2017): 130-168.

Типы реализаций

Раундовая

Один раунд за такт

- Меньше площадь и затрачиваемая энергия
- Снижается пропускная способность

Параллельная

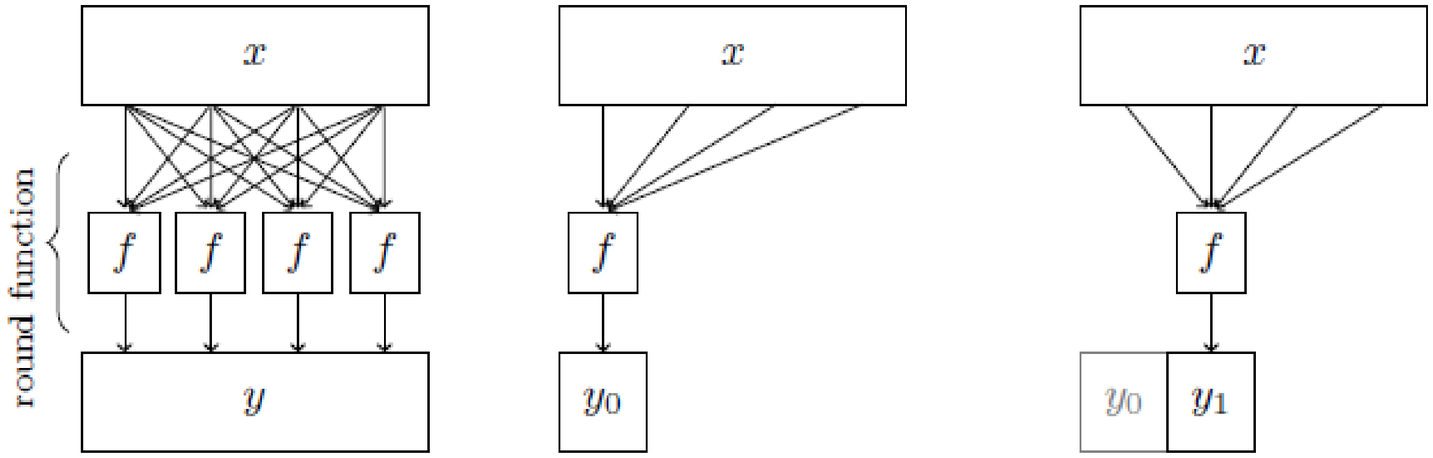
Несколько раундов за такт

- Высокая пропускная способность
- Больше площадь и затрачиваемая энергия

Сериализованная

Часть раунда за такт (например один S-блок)

- Можно значительно сократить площадь и энергопотребление
- Не всегда возможно оптимизировать реализацию из-за накладных расходов на дополнительную логику управления

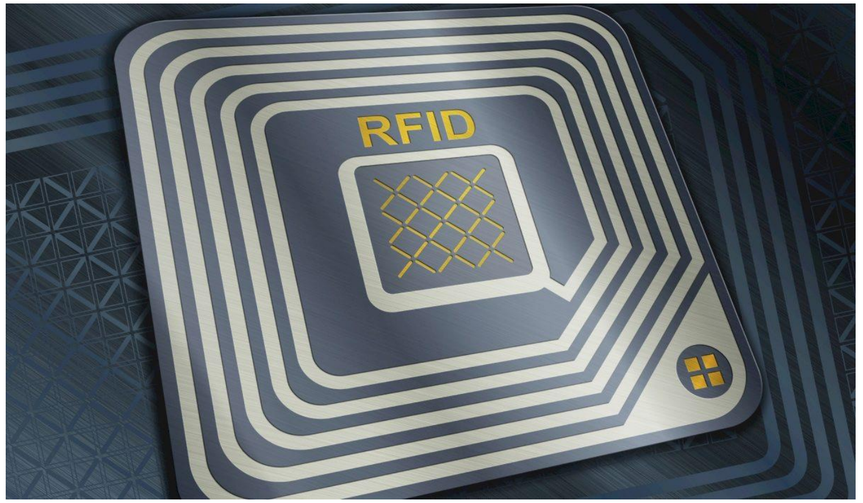


(a) Round-based ($t = 1$). (b) Serial ($t = 1$). (c) Serial ($t = 2$).

Алгоритм Магма:

- 800-1000 GE*
- ключ – 256 бит
  1 бит ≈ 6 GE
  256 бит ≈ 1500 GE

200-2000 GE**



*scan flip-flops*** (6.25 GE) или D-триггер и мультиплексор (4.5 + 2 GE)*

* Poschmann, Axel & Ling, San & Wang, Huaxiong. (2010). 256 Bit Standardized Crypto for 650 GE – GOST Revisited. 6225. 219-233.

** Weis, Stephen & Sarma, Sanjay & Rivest, Ronald & Engels, Daniel. (2003). Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. Lect. Note. Comput. Sci.. 2802.

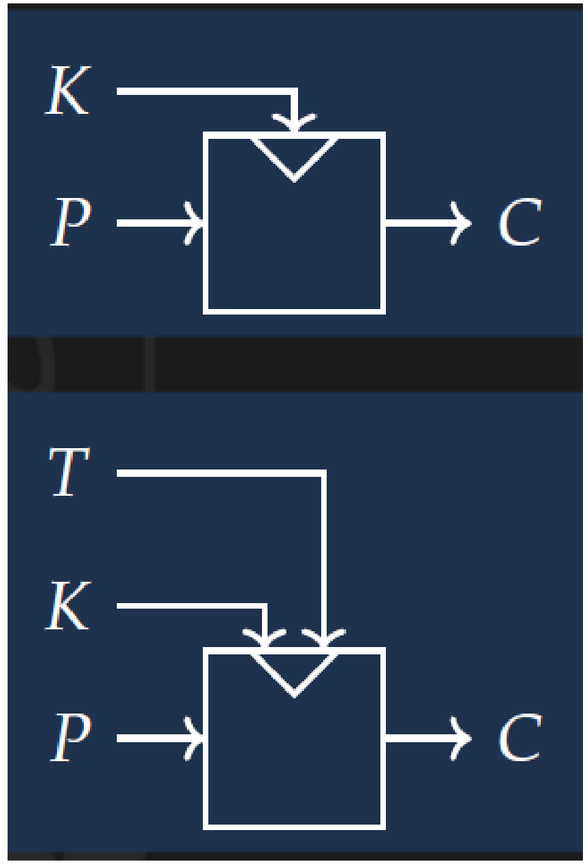
*** Virtual Silicon Inc.: 0.18 µm VIP Standard Cell Library Tape Out Ready, Part Number: UMCL18G212T3, Process: UMC Logic 0.18 µm Generic II Technology: 0.18µm (July 2004).

Блочные шифры с параметром (tweak)

КРИПТОНИТ

$$\{0,1\}^K \times \{0,1\}^P \to \{0,1\}^C$$

$$\{0,1\}^T \times \{0,1\}^K \times \{0,1\}^P \to \{0,1\}^C$$



Liskov, Moses D., Ronald L. Rivest and David A. Wagner. “Tweakable Block Ciphers.” *Journal of Cryptology* 24 (2002): 588-613.

Блочные шифры с параметром (tweak)

КРИПТОНИТ

Плюсы:

- режим шифрования в рамках примитива;
- больший объём материала на ключ;
- защита от атак по побочным каналам.

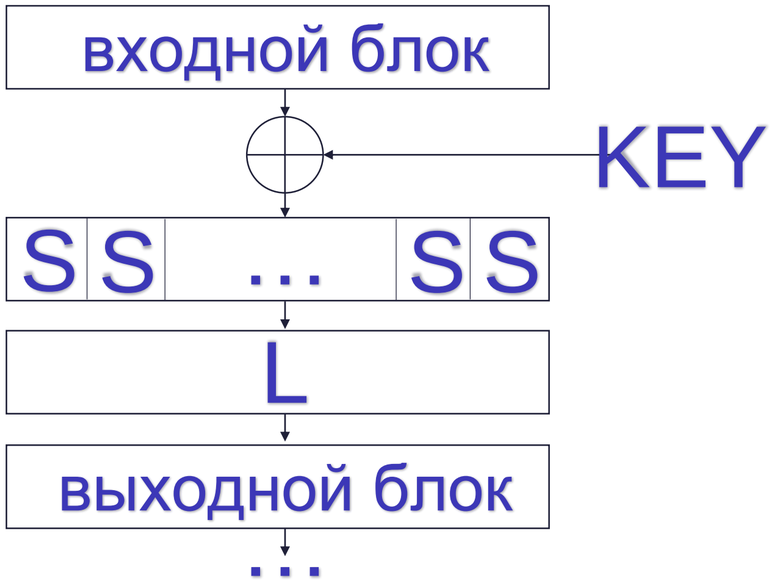
Минусы:

- возрастание трудоёмкости алгоритма.

Liskov, Moses D., Ronald L. Rivest and David A. Wagner. “Tweakable Block Ciphers.” *Journal of Cryptology* 24 (2002): 588-613.

XSL-схемы

1 раунд XSL-схемы



Синонимы: SP-сеть, XSPL-схема, LSX-схема

4-битовые подстановки

КРИПТОНИТ

- 4-битовые подстановки разбиваются на 302 класса аффинной эквивалентности

- Оптимальные характеристики 4-битовых подстановок:

Линейная характеристика	Разностная характеристика	Степень нелинейности
$\mathrm{l}_s = \max\limits_{\substack{\alpha,\beta\neq 0^n,\\ \alpha,\beta\in V_n}} \lvert 2\cdot P\{(S(x),\beta)=(x,\alpha)\}-1\rvert$	$\Delta_s = \max\limits_{\substack{\alpha,\beta\neq 0^n,\\ \alpha,\beta\in V_n}} P\{S(x)\oplus S(x\oplus\alpha)=\beta\}$	$\lambda_s = \min\limits_{\substack{\beta\neq 0^n,\\ \beta\in V_n}} \deg(S(x),\beta)$
$l_s = \frac{1}{2}$	$\Delta_s = \frac{4}{16} = \frac{1}{4}$	$\lambda_s = 3$

- 16 оптимальных классов

Подходы к выбору S-блоков

КРИПТОНИТ

Present / LED

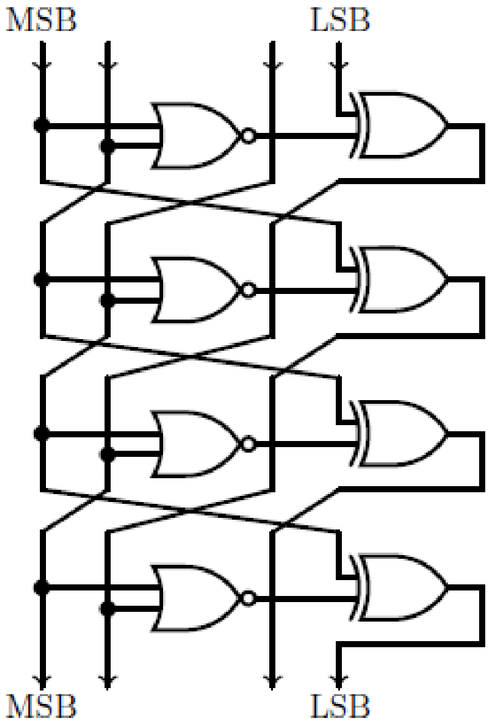
- Выбирали S-блок с оптимальными криптографическими характеристиками и компактной аппаратной реализацией
- Накладывали дополнительные условия для улучшения «лавинного» эффекта:

$$\mathrm{P}\{S(x) \oplus S(x \oplus \alpha) = \beta\} = 0, \quad \mathrm{wt}(\alpha) = wt(\beta) = 1$$

$$|2 \cdot \mathrm{P}\{(S(x), \beta) = (x, \alpha)\} - 1| = \frac{1}{4}, \mathrm{wt}(\alpha) = wt(\beta) = 1$$

Skinny, Midori

- Перебор комбинаций NAND/NOR/XOR/XNOR с ограничением на число операций и требованием оптимальных значений криптографических характеристик.



Подходы к выбору S-блоков

Gift

NOT, NAND, NOR – N-инструкции («размер» 1)

XOR, XNOR – X-инструкции («размер» 2)

Использовали только обратимые инструкции: a $\leftarrow NOT(a)$, a $\leftarrow a$ X b, a $\leftarrow a$ X (b N c), a $\leftarrow a$ X ((b N c) N d)

Критерии S-блока:

- «Размер» реализации не превышает 17.
- Хорошие криптографические характеристики (не обязательно оптимальные).
- Существует одинаковая BOGI(Bad Output must go to Good Input) перестановка для разностной и линейной характеристик.

Для поиска строили PE*(permutation-xor equivalence) S-блоки из нужных классов и смотрели их характеристики.

Δx \ Δy	1000	0100	0010	0001
1000	0	2	2	0
0100	0	0	0	0
0010	0	0	0	0
0001	0	2	2	0

**permutation-xor equivalence:* $S'(x) = P_0 S\big(P_i(x \oplus c_i)\big) \oplus c_0$, *где* P_0, P_i *матрицы перестановки*

Выбор L-преобразований

КРИПТОНИТ

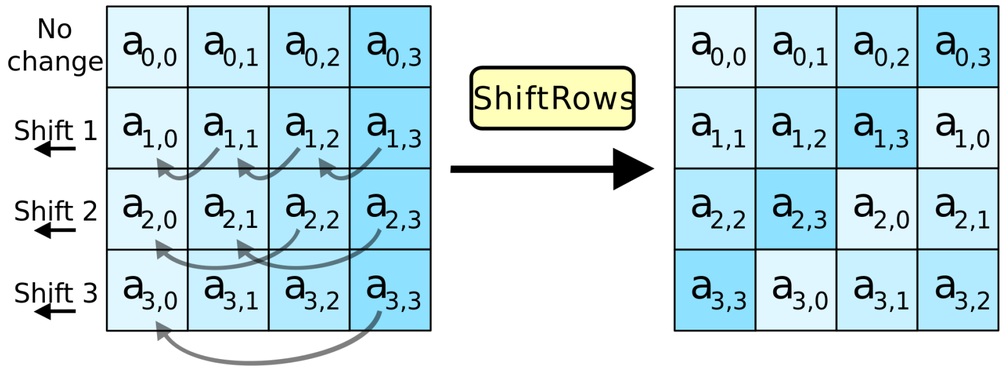
Определение

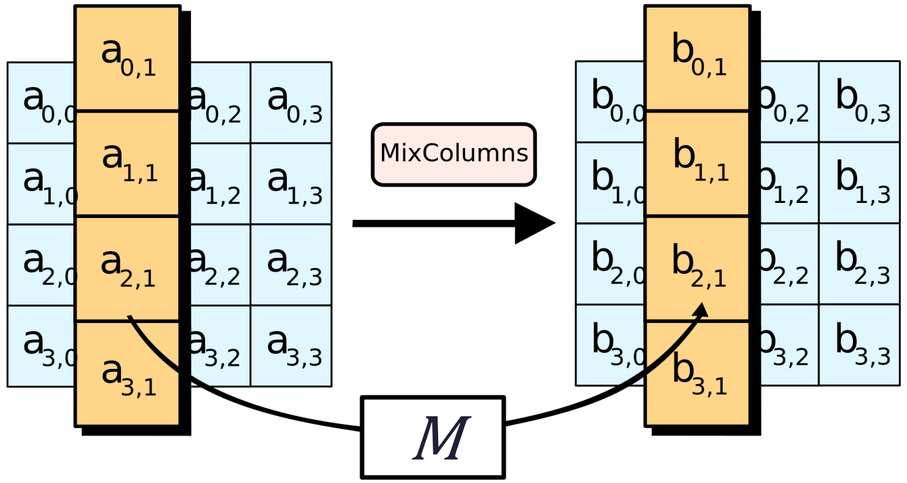
Показатель рассеивания линейного преобразования L

$$\tau(L) = \min_{a \neq 0} wt(a) + wt(aL)$$

AES-структура

L = ShiftRows · MixColumns





Выбор L-преобразований

КРИПТОНИТ

$A_S(r)$ — минимальное число активных S-блоков за r раундов

Теорема*

- Пусть в AES-структуре $\tau(M) = \rho$.
- Тогда $A_S(4) = \rho^2$.

Для любых $\alpha \neq 0, \beta$

$$P_{(\alpha,\beta)}(r) \leq (\Delta_s)^{A_S(r)},$$

$P_{(\alpha,\beta)}(r)$ - вероятность одной цепочки, переводящей разность α в β за r раундов

Насколько точная оценка?? **

* Ф. М. Малышев, Д. И. Трифонов, “Рассеивающие свойства XSLP-шифров”, *Матем. вопр. криптогр.*, **7**:3 (2016), 47–60

** Nyberg, K., Knudsen, L.R.: Provable security against a differential attack. J. Cryptol. **8**(1), 27–37 (1995).

Выбор L-преобразований

Авторы PRESENT, Gift, Skinny, Midori используют указанную оценку $P_{(\alpha,\beta)}(r)$.

В * показан пример «игрушечной» шифрсистемы с оценкой $P_{(\alpha,\beta)}(4) \leq 2^{-216}$, при этом вероятность перехода разности α в β за 4 раунда ≈ 2^{-118}.

В ** предлагается автоматизированное средство оценки вероятностей перехода разности α в β за r раундов.

* Dunkelman, O., Kumar, A., Lambooij, E., Sanadhya, S.K. (2020). Counting Active S-Boxes is not Enough. In: Bhargavan, K., Oswald, E., Prabhakaran, M. (eds) Progress in Cryptology – INDOCRYPT 2020. INDOCRYPT 2020. Lecture Notes in Computer Science(), vol 12578. Springer, Cham.

** Cui T., Mao Y., Yang Y., Zhang Yi, Zhang J., Jin C. Congruent Differential Cluster for Binary SPN Ciphers // IEEE Transactions on Information Forensics and Security. 2024. Vol. 19. pp. 2385-2397.

Выбор L-преобразований

КРИПТОНИТ

		показатель рассеивания	реализация
LED	$\begin{pmatrix} 4 & 2 & 1 & 1 \\ 8 & 6 & 5 & 6 \\ B & E & A & 9 \\ 2 & 2 & F & B \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 4 & 2 & 1 & 1 \end{pmatrix}^4$	$\tau(M) = 5$	$serial$
Midori	$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$	$\tau(M) = 4$	$6\ XOR$
Skinny	$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$	$\tau(M) = 2$	$3\ XOR$
Present/Gift	перестановка бит	$\tau(M) = 2$	0

Сравнение шифрсистем

КРИПТОНИТ

Блок 64 бита, S-блок 4 бита

Шифрсистема	Показатель рассеивания, максимум 5	Мин. число активных S-блоков за r раундов	Площадь S-блока, STM 90 nm	Площадь S-блока, NanGate 45nm
LED	5	100/16	22,5 GE	24,33 GE
Midori	4	84/16		13,3 GE
Skinny	2	75/16	12 GE	
GIFT	2 (перестановка бит)	36/18	16,5 GE	
PRESENT	2 (перестановка бит)	30/15	22,5 GE	24,33 GE

Сравнение шифрсистем

КРИПТОНИТ

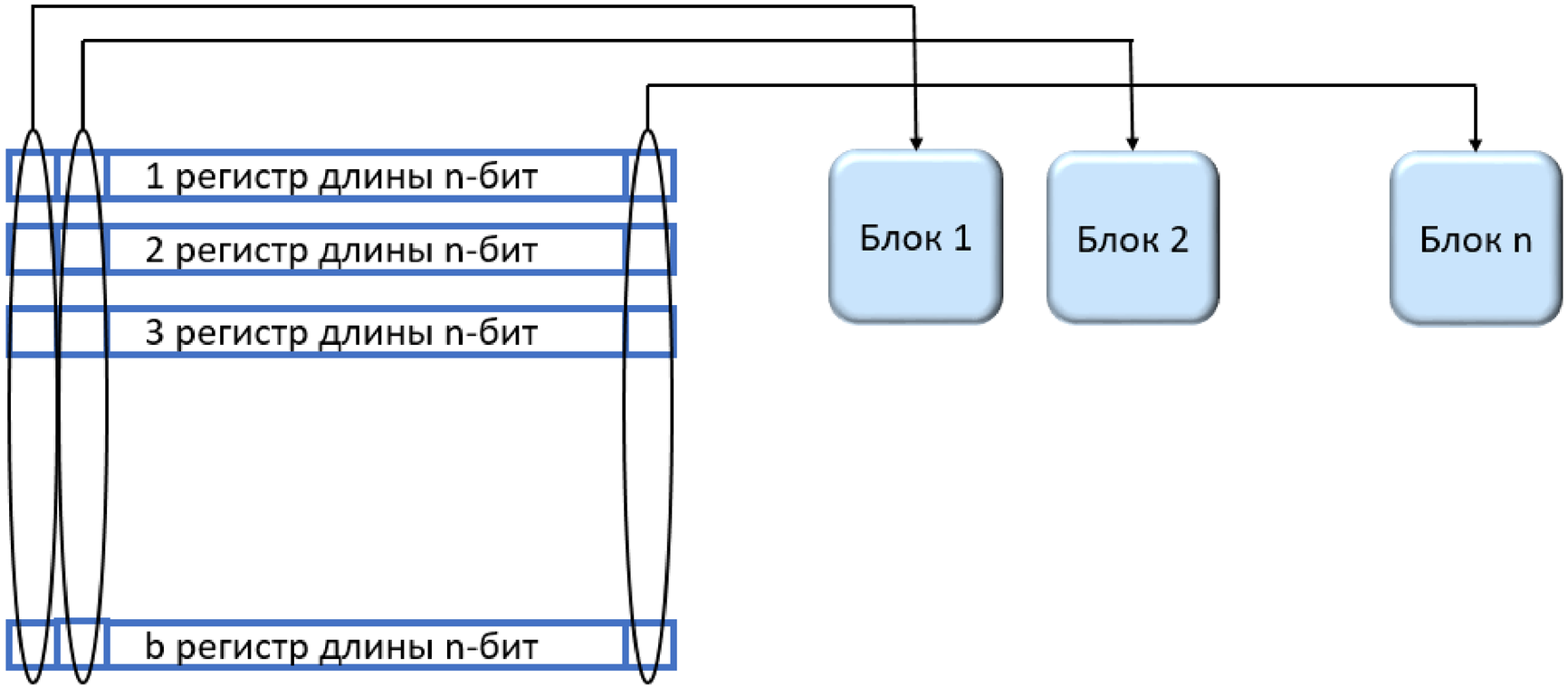
Блок 64 бита, ключ 128 бит

Раундовая реализация

Шифрсистема	Площадь (GE)	Задержка (нс)	Мощность (мкВТ), 10 МГц	Энергия (пДж)
LED	1831	5.25	131.3	656.5
Midori	1542	2.06	60.6	103.0
Skinny	1477	1.84	80.3	297.0
GIFT	1345	1.83	74.8	216.9
PRESENT	1560	1.63	71.1	234.6

Особенности программной реализации

Bit-slice реализация



n: размер регистра = число блоков
b: размер блока = число регистров

Особенности аппаратной реализации

- Эффективность реализации отличается для разных наборов логических элементов:
  - *S-блок Gift может быть реализован за 6 XOR + 3 AND + 1 OR + 1 NOT.*
  - *Наличие элементов XNOR и NAND позволяет реализовать за 6 XNOR + 3 NAND + 1 OR.*

  - *Использование 4-входных AND-NOR и OR-NAND вместо 2-входных XOR и XNOR может[*] уменьшить площадь схемы.*

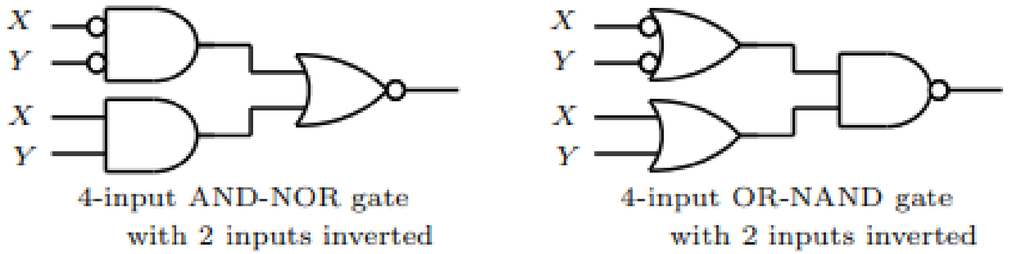
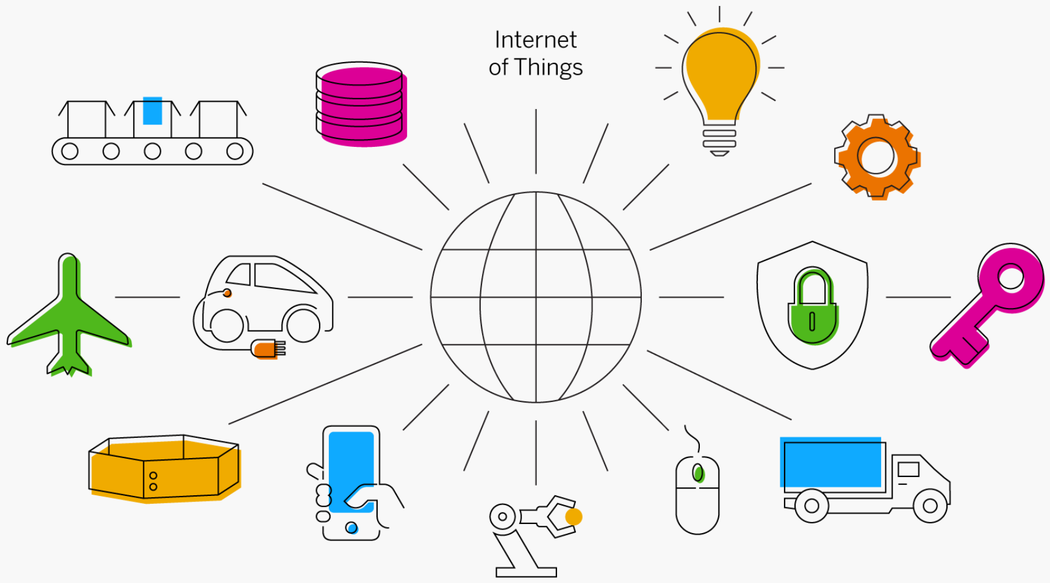


Fig. 6. 4-input AND-NOR and 4-input OR-NAND gates with 2 inputs inverted, which correspond to XOR and XNOR gate

[*] Beierle, Christof, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich and Siang Meng Sim. “The SKINNY Family of Block Ciphers and its Low-Latency Variant MANTIS.” IACR Cryptol. ePrint Arch. 2016 (2016): 660

Выводы

1. Использование параметров tweak.
2. S и L преобразования выбираются в связке.
3. Достаточное число активных S-блоков при легковесном L.
4. S и L обладают эффективными реализациями для различных архитектур.
5. Возможность программной bit-slice реализации.



КРИПТОНИТ

Спасибо за внимание!

Степан Давыдов s.davydov@kryptonite.ru

Анастасия Чичаева a.chichaeva@kryptonite.ru

Юрий Шкуратов y.shkuratov@kryptonite.ru