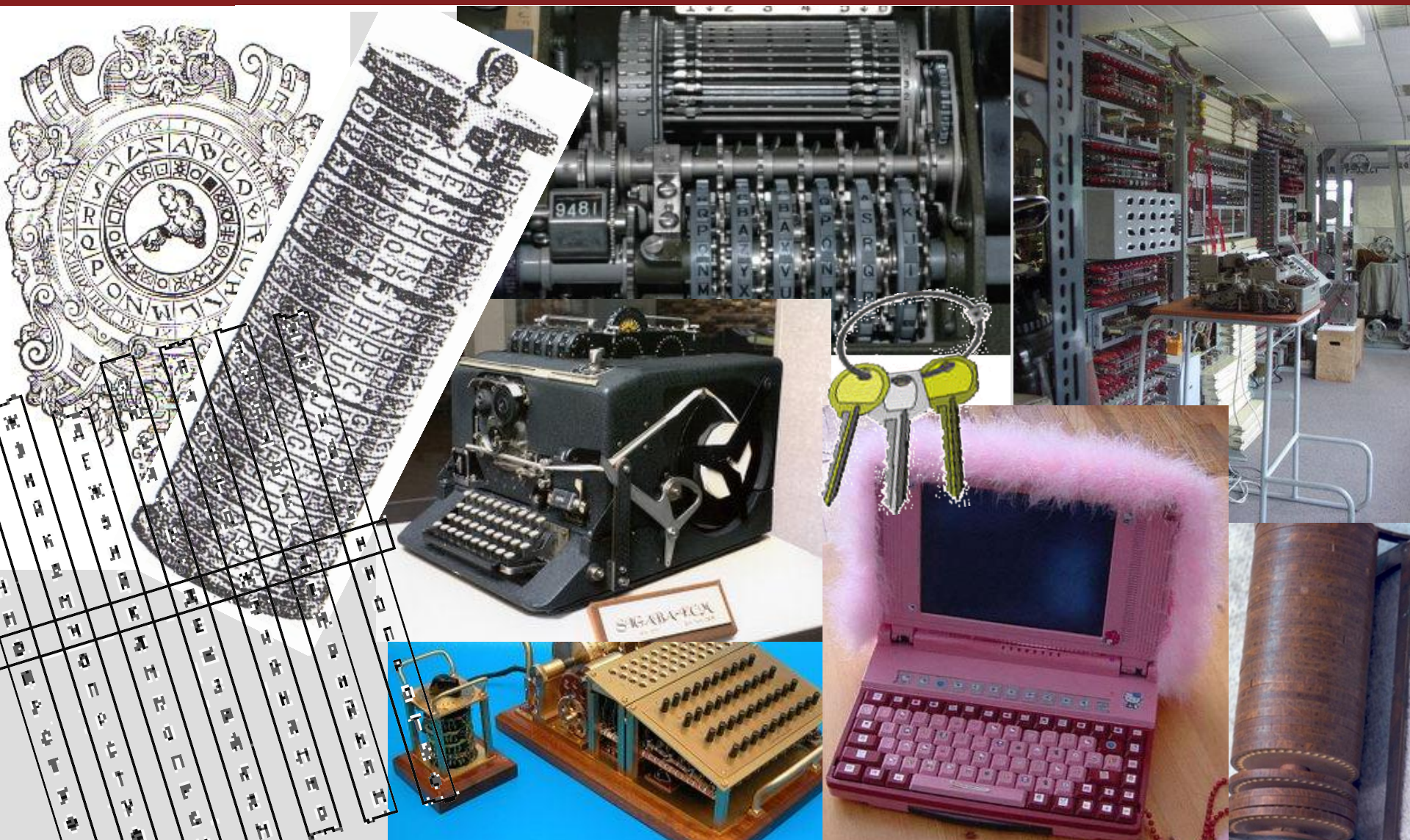
Ассоциация
РусКрипто

Малоресурсная криптография

Ассоциация РусКрипто

Развитие средств коммуникации



Ассоциация РусКрипто

Internet of Things — An action plan for Europe

Communication from the Commission to the European Parliament, the Council, the European economic and Social Committee and the Committee of the Regions

Ассоциация
РусКрипто

От Интернента РС к Интернету вещей (IoT)

Christof Paar, Axel Poschmann:

«The upcoming era of pervasive computing will be characterized by many smart devices that — because of the tight cost constraints inherent in mass deployments — have very limited resources in terms of memory, computing power, and battery supply.»

Ассоциация РусКрипто

Интернет вещей

Уже сейчас 98.8% всех изготовленных процессоров используется во встроенных приложениях и лишь 1.2% – в традиционных компьютерах.

Ассоциация РусКрипто

Интернет вещей

Интернет вещей (Internet of Things – IoT) представляет собой беспроводную самоконфигурирующуюся сеть между объектами типа бытовых приборов, транспортных средств, датчиков, а так же меток радиочастотной идентификации (Radio Frequency IDentification, RFID).

Ассоциация РусКрипто

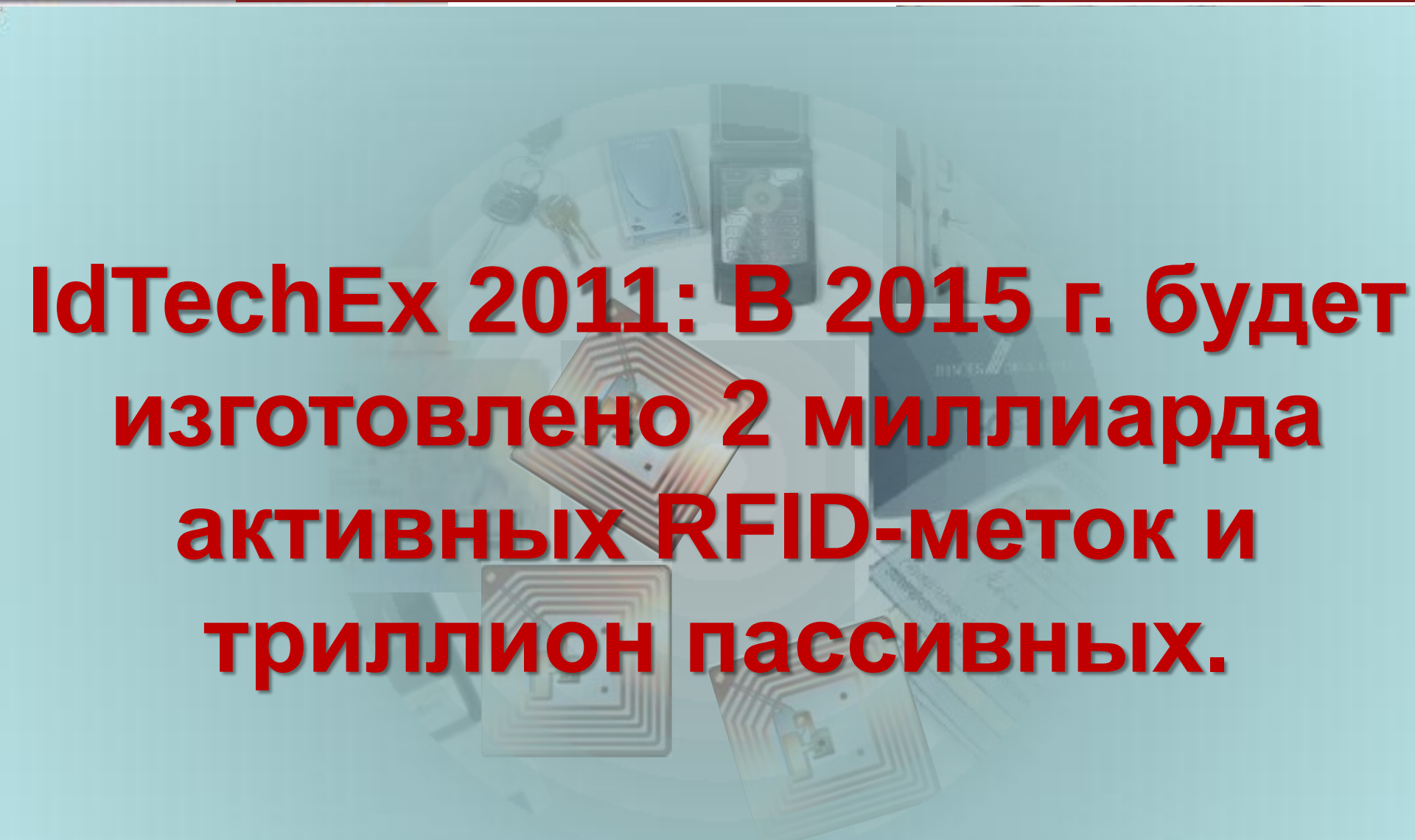
Интернет вещей

Ассоциация РусКрипто

Интернет вещей

Ассоциация РусКрипто

Интернет вещей



IdTechEx 2011: В 2015 г. будет изготовлено 2 миллиарда активных RFID-меток и триллион пассивных.

Ассоциация РусКрипто

Интернет вещей

Крупнейшим потребителем RFID-меток является сеть супермаркетов Walmart. На втором месте идет министерство обороны США.

Ассоциация РусКрипто

"SAP IoT Definition". SAP Research. Retrieved 2011-03-18.

- **A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in information processes. Services are available to interact with these 'smart objects' over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues.**

"SAP IoT Definition".
SAP Research. Retrieved 2011-03-18.

Ассоциация РусКрипто

"SAP IoT Definition". SAP Research. Retrieved 2011-03-18.

- **A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in information processes. Services are available to interact with these 'smart objects' over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues**

"SAP IoT Definition". SAP Research. Retrieved 2011-03-18.

Ассоциация РусКрипто

директор ЦРУ Дэвид Петрэус:

- Данные с подключенных к Интернету бытовых приборов можно использовать для составления максимально подробного досье на любого человека.

National Security Agency

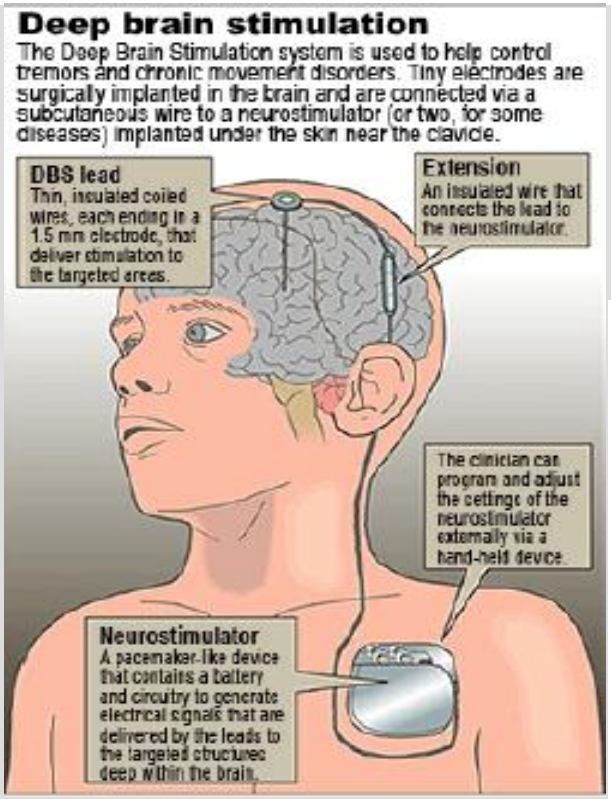
NSA Trusted Systems Research Group.

A presentation given to the MIT Media Lab, 30 Jan 2013.

“RFID technology adoption is accelerating rapidly. Merged into real-time location systems (RTLS) and converged with worldwide communications systems, by 2013 RFIDs will be a pervasive way to identify, locate, and track people and objects.”

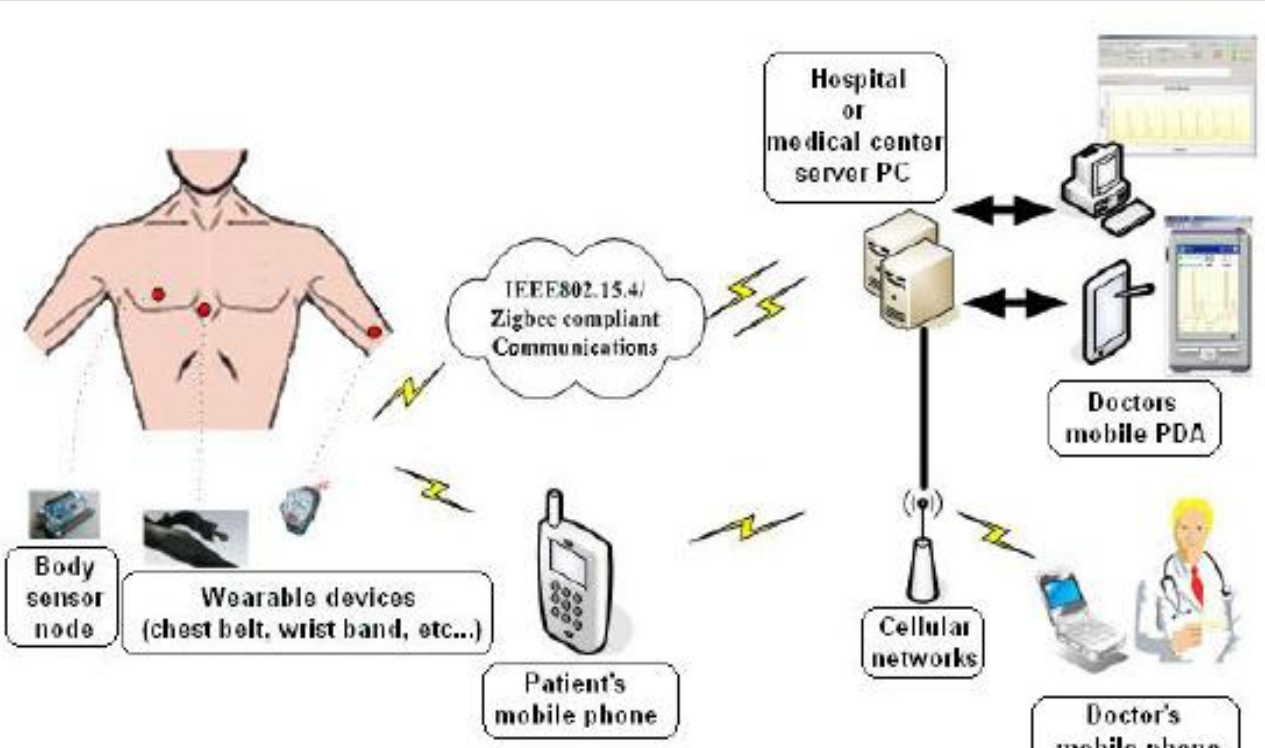
Ассоциация РусКрипто

Имплантированные медицинские сенсоры



электронный стимулятор мозга

электронный стимулятор сердца



инъекции инсулина

Малоресурсная криптография

Lightweight Cryptography for the Internet of Things

Легковесная криптография

Ассоциация РусКрипто

Малоресурсная криптография

Легковесная криптография

(низкоресурсная криптография)

Ассоциация РусКрипто

Малоресурсная криптография

Ассоциация РусКрипто

Малоресурсная криптография

Типичные ограничения:

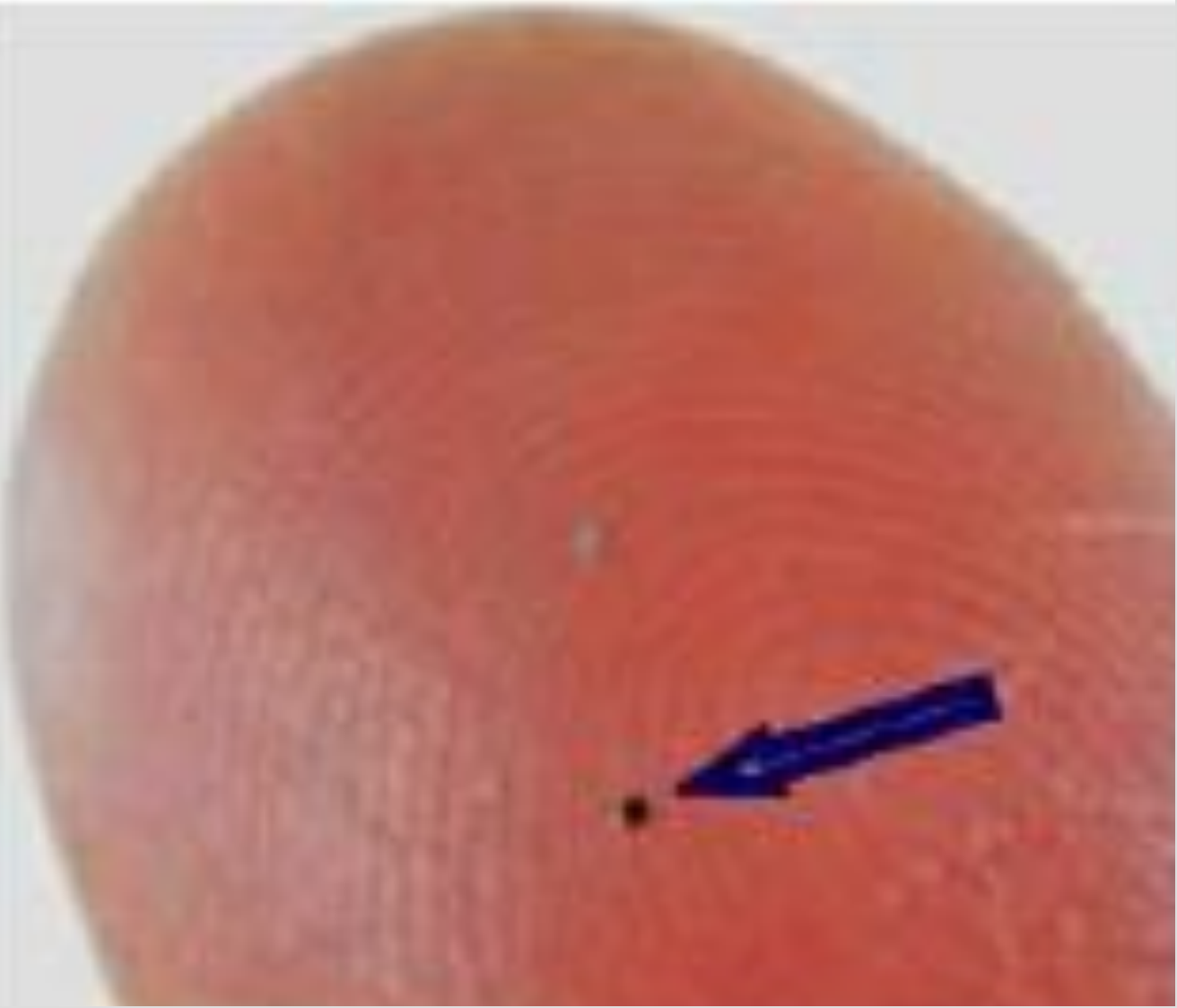
- **размер микросхемы**
- **потребляемая энергия**
- **размер программного кода**
- **размер оперативной памяти**
- **ширина полосы рабочих частот канала связи**
- **время, затраченное на исполнение программы.**

Ассоциация РусКрипто

Малоресурсная криптография

Типичные

- **размер м**
- **потребля**
- **размер п**
- **размер о**
- **ширина канала с**
- **время, за программ**



Ассоциация РусКрипто

Международные стандарты

- **ISO/IEC FDIS 29192-1 -- 29192-4.**
  - **-- Information technology**
  - **-- Security techniques**
  - **-- Lightweight cryptography**
  - **Part 1: General.**
  - **Part 2: Block ciphers.**
  - **Part 3: Stream ciphers.**
  - **Part 4: Mechanisms using asymmetric techniques.**

Ассоциация РусКрипто

Международные стандарты

- Key size - [bits]
- Block size - [bits]
- Area - [GE]
- Cycles - [CLK]
- Bits per cycles - [bits/CLK]
- Power - [GE]
- Energy - [GE*CLK]
- Energy per bit - [GE*CLK/bits]
- Technology - [μm]

Малоресурсная криптография

Table 2.1: Area requirements and corresponding gate count of selected standard cells of the UMCL18G212T3 library.

Standard cell	Process	Library	Cell name	Area in μm^2	GE
NOT	0.18μm	UMCL18G212T3	HDINVBD1	6.451	0.67
NAND	0.18μm	UMCL18G212T3	HDNAN2D1	9.677	1
NOR	0.18μm	UMCL18G212T3	HDNOR2D1	9.677	1
AND	0.18μm	UMCL18G212T3	HDAND2D1	12.902	1.33
OR	0.18μm	UMCL18G212T3	HDOR2D1	12.902	1.33
MUX	0.18μm	UMCL18G212T3	HDMUX2D1	22.579	2.33
XOR (2)	0.18μm	UMCL18G212T3	HDEXOR2D1	25.805	2.67
XOR (3)	0.18μm	UMCL18G212T3	HDEXOR3D1	45.158	4.67
D Flip flop	0.18μm	UMCL18G212T3	HDDFFPB1	51.61	5.33
Scan D flip-flop /w enable	0.18μm	UMCL18G212T3	HDSDFPQ1	58.061	6
Scan flip-flop	0.18μm	UMCL18G212T3	HDSDEPQ1	83.866	8.67
complex Scan flip-flop	0.18μm	UMCL18G212T3	HDSDERSPB1	119.347	12.33

Ассоциация РусКрипто

Малоресурсная криптография

Table 4.1: Area requirements of selected standard cells in our UMC 0.13 μm library (FSC0L_D).

Standard cell	Number of inputs	Area [μm^2]	Area [GE]
NOT	1	3 – 28	0.75 – 7
NAND	2	4 – 23	1 – 5.75
	3	6 – 14	1.5 – 3.5
	4	12 – 18	3 – 4.5
NOR	2	4 – 40	1 – 10
	3	6 – 13	1.5 – 3.25
	4	11 – 19	2.75 – 4.75
AND	2	5 – 19	1.25 – 4.75
	3	7 – 16	1.75 – 4
	4	10 – 33	2.5 – 8.25
OR	2	5 – 25	1.25 – 6.25
	3	7 – 26	1.75 – 6.5
XOR	2	11 – 16	2.75 – 4
	3	22 – 26	5.5 – 6.5
	4	30 – 31	7.5 – 7.75
MUX	2	9 – 28	2.25 – 7
	3	16 – 27	4 – 6.75
	4	25 – 35	6.25 – 8.75
D Flip Flop	1	20 – 40	5 – 10
Scan Flip Flop	1	25 – 47	6.25 – 11.75

Ассоциация РусКрипто

Блочные шифры

ISO/IEC FDIS 29192-2:

- PRESENT
- CLEFIA

Ассоциация РусКрипто

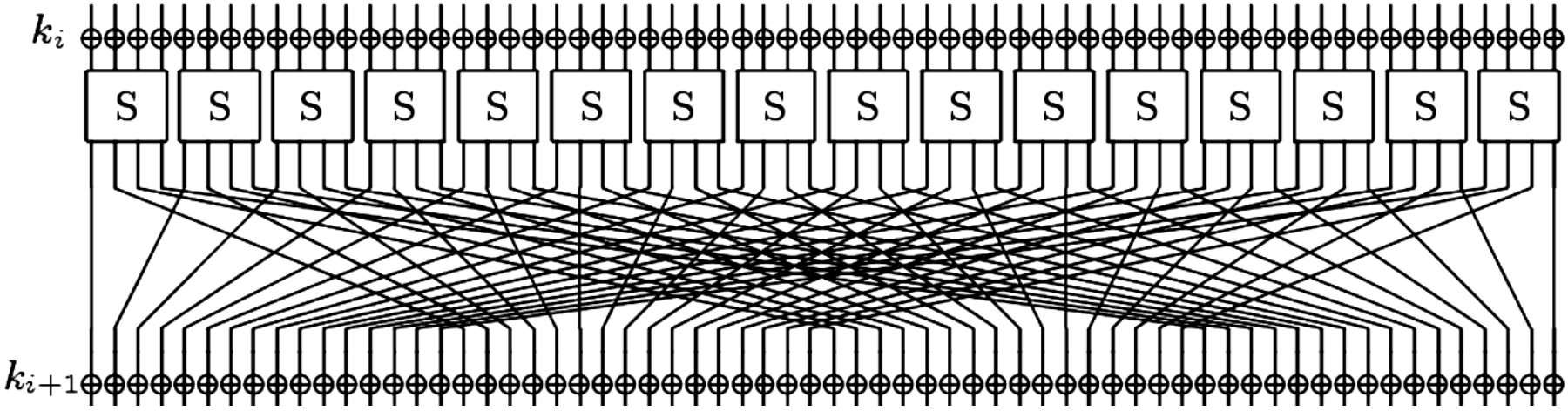
PRESENT

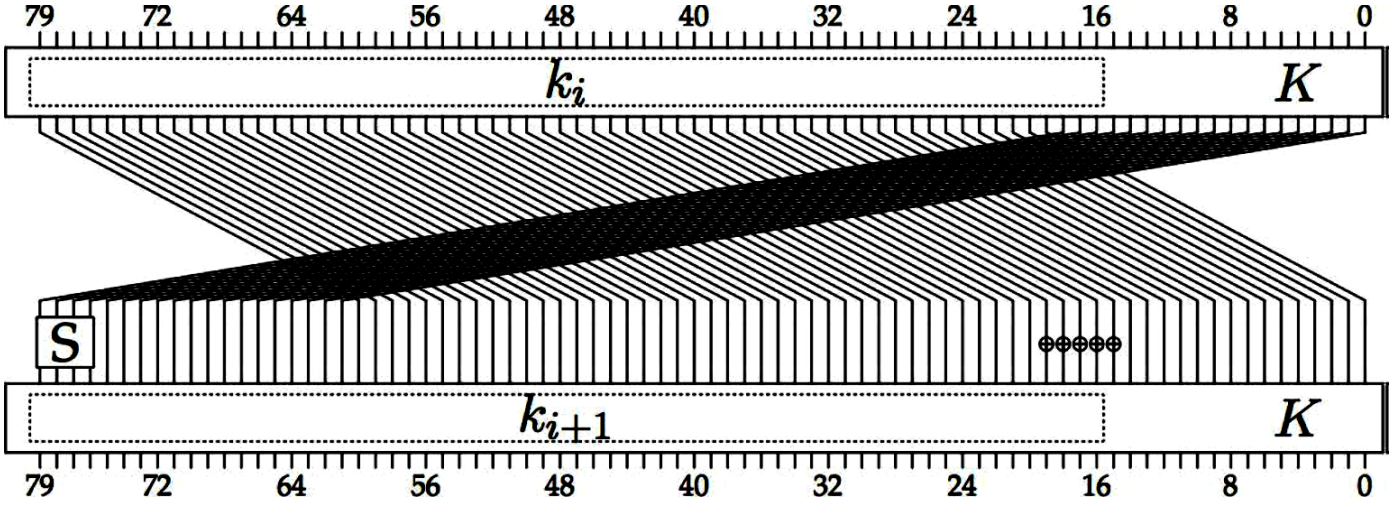
Блочный шифр PRESENT разработан группой исследователей из Германии, Дании и Франции: A.Bogdanov, L.R.Knudsen, G.Leander, C.Paar, A.Poschmann, M.J.B.Robshaw, Y.Seurin, C.Vikkelsoe. Впервые представлен на конференции CHES 2007.

PRESENT является классической SP-сетью (Substitution Permutation Network) с 64-битным информационным блоком, 80-битным или 128-битным ключом и состоит 31+1 цикла (round) шифрпреобразований.

Ассоциация РусКрипто

PRESENT





Ассоциация РусКрипто

PRESENT

Аппаратная реализация

Ключ	Тактов на блок	Произв. [Kbps]	Площ. [GE]	Эфф. [bps/GE]	Ток [μA]
80	547	11.70	1,075	10.89	1.4
80	32	200.00	1,570	127.40	2.78
80	32	200.00	1,623	127.40	1.83
128	559	11.45	1,391	8.23	N/A
128	32	200.00	1,884	106.20	3.67

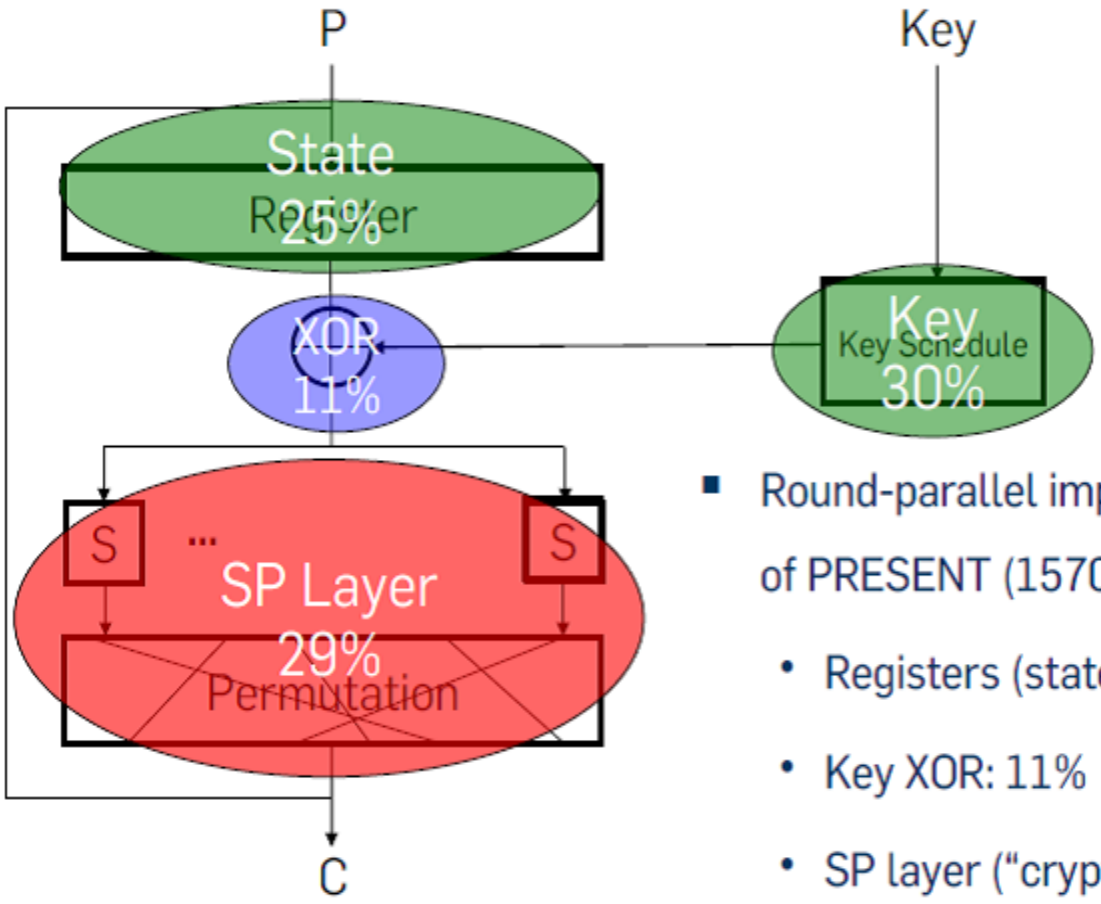
Enc.

Ассоциация РусКрипто

PRESENT
Аппаратная реализация

Lightweight Block Ciphers

PRESENT – Resource Utilization



- Round-parallel implementation of PRESENT (1570 GE)
  - Registers (state+key): 55%
  - Key XOR: 11%
  - SP layer (“crypto” part): 29%

PRESENT
Криптостойкость

Число раунд.	Тип атаки	Сложность		
		Материал	Время	Память
16 (32)	Alg.-Diff.	2^{62} CP	2^{46} clk.	2^{30} Bytes
16 (32)	Differential	2^{64} KP	2^{65} MA	$2^{31.6}$ Bytes
16 (32)	Stat. Satur.	$c \cdot 2^{36}$ CP	2^{28} MA	2^{16} Count.
16 (32)	Stat. Satur.	$c \cdot 2^{33}$ CP	2^{57} MA	2^{32} Count.
24 (32)	Lin. w. keys	$2^{63.5}$ KP	не опр.	не опр.
25 (32)	M.dim. Lin.	$2^{62.4}$ KP	2^{65} Enc.	2^{34} Bytes
26 (32)	M.dim. Lin.	2^{64} KP	2^{72} Enc.	2^{34} Bytes

$k = 80$

PRESENT
Криптостойкость

Число раунд.	Тип атаки	Сложность		
		Материал	Время	Память
7 (32)	Bit-Patt. Int.	$2^{24.3}$ CP	2^{100} MA	2^{77} Bytes
17 (32)	Rel. K. Rect.	2^{63} CP	2^{104} MA	2^{53} Bytes
17 (32)	Alg.-Diff.	2^{62} CP	2^{98} clk.	2^{30} Bytes
18 (32)	Alg.-Diff.	2^{62} CP	2^{103} clk.	2^{30} Bytes
19 (32)	Alg.-Diff.	2^{62} CP	2^{113} clk.	2^{30} Bytes
25 (32)	Linear Hull	2^{64} KP	$2^{98.6}$ Enc.	2^{40} blocks

$k = 128$

Ассоциация РусКрипто

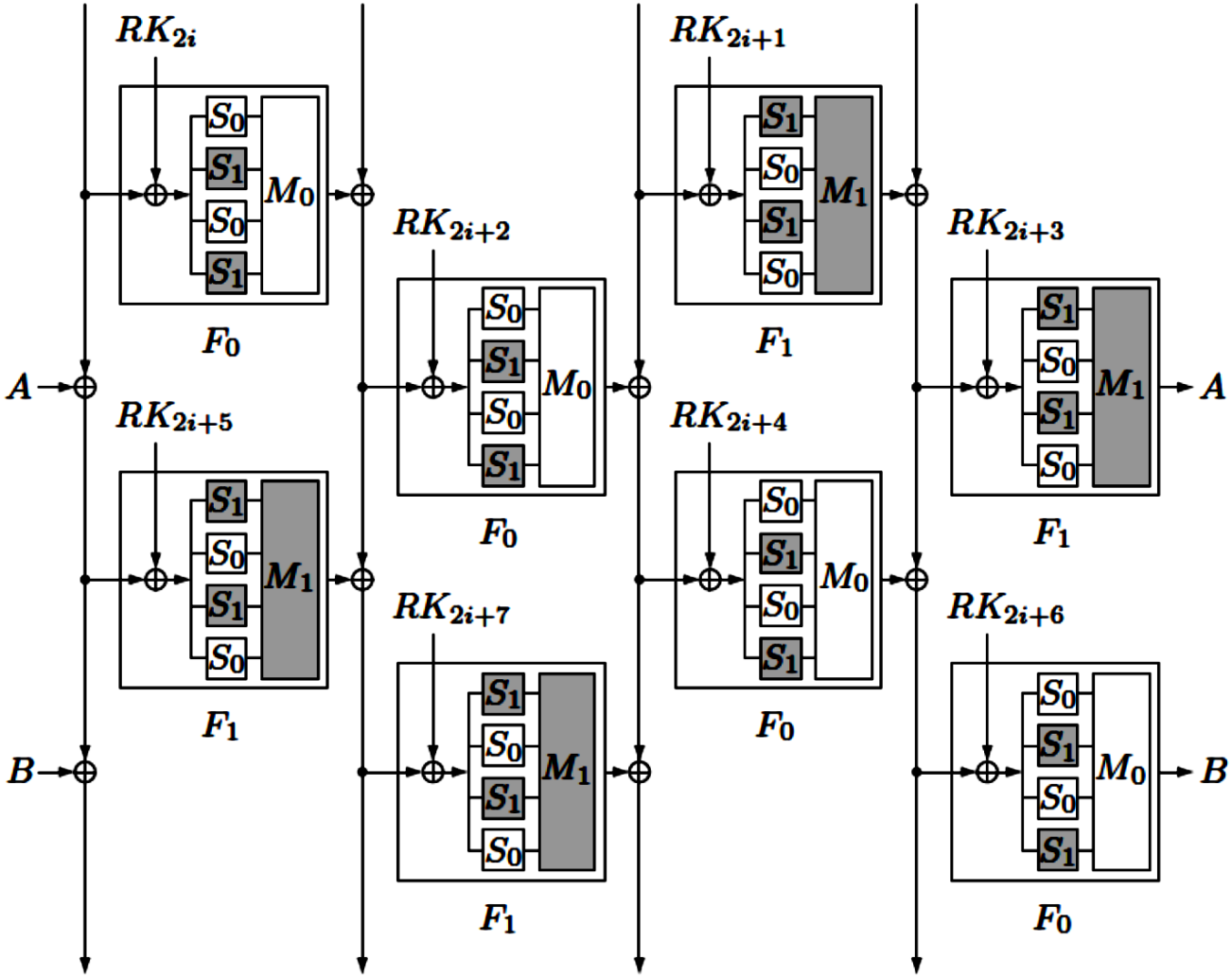
CLEFIA

Блочный шифр CLEFIA является совместной разработкой корпорации Sony и группы исследователей из Университета г. Нагоя (Япония). Впервые представлен на конференции FSE 2007.

Шифр представляет собой обобщенную схему Фейстеля, в которой 128-битный информационный блок разбивается на 4 подблока. Ключ – 128, 192 или 256 бит. В зависимости от длины ключа алгоритм имеет соответственно 18, 22, или 26 циклов шифрования.

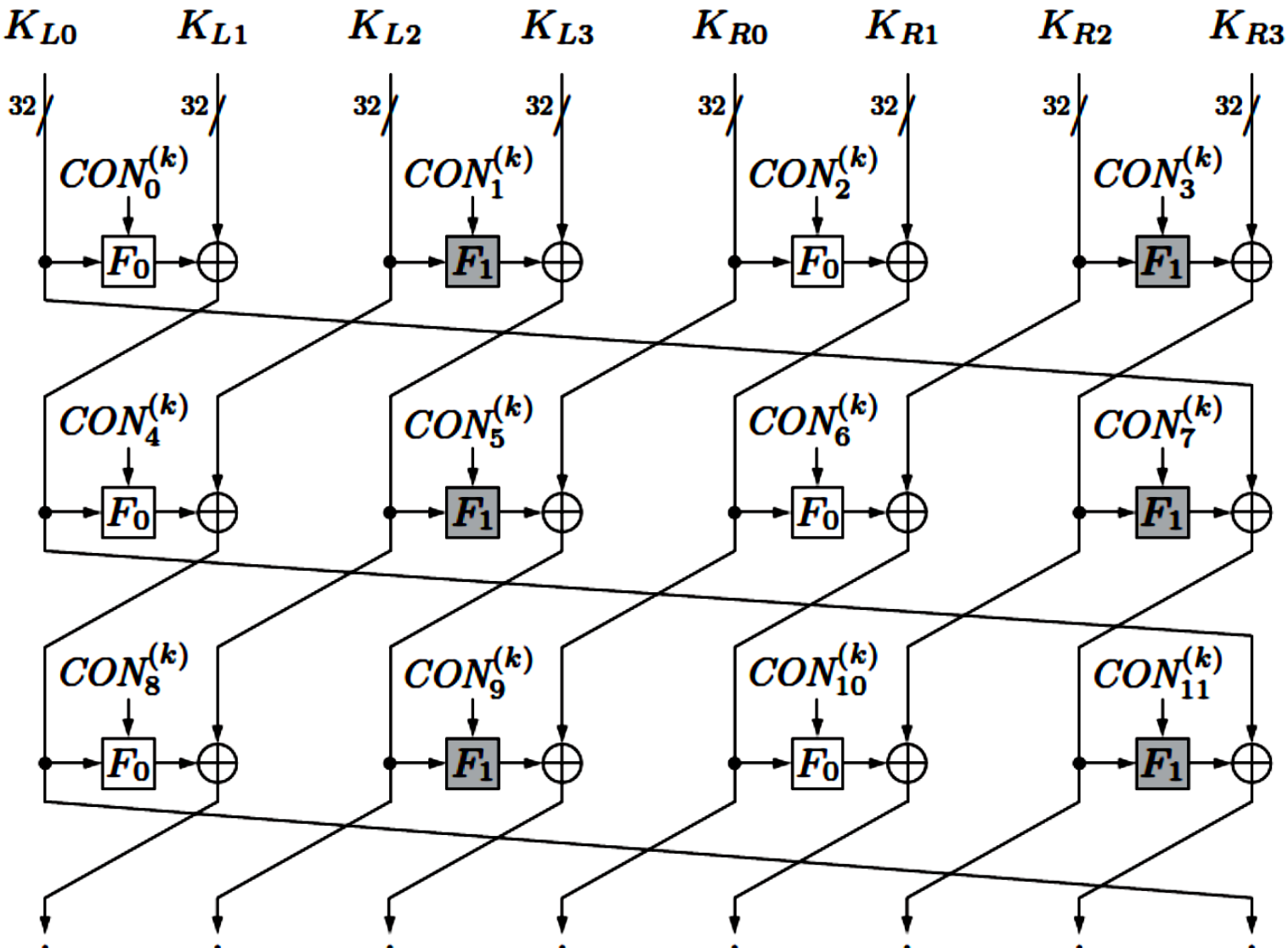
Ассоциация РусКрипто

CLEFIA



Ассоциация РусКрипто

CLEFIA



Ассоциация РусКрипто

CLEFIA
Аппаратная реализация

Ключ	Тактов на блок	Произв. [Kbps]	Площ. [GE]	Эфф. [bps/GE]	Ток [μA]
128	36	355.6	4,950	71.83	N/A
128	18	711.11	5,979	118.93	N/A
192	22	581.8	8,536	68.16	N/A
256	26	492.3	8,482	58.04	N/A

Enc. + Dec.

Ассоциация РусКрипто

CLEFIA
Криптостойкость

Число раунд.	Тип атаки	Сложность		
		Материал	Время	Память
10 (18)	Imp. Diff.	$2^{101.7}$ CP	2^{102} Enc.	2^{32} blocks
11 (22)	Imp. Diff.	$2^{103.5}$ CP	2^{188} Enc.	2^{121} blocks
12 (26)	Imp. Diff.	$2^{103.8}$ CP	2^{252} Enc.	2^{153} blocks
12 (18)	Imp. Diff.	$2^{118.9}$ CP	2^{119} Enc.	2^{73} blocks
12 (18)	Imp. Diff.	2^{111} CP	2^{111} Enc.	2^{81} blocks
13 (22)	Imp. Diff.	$2^{119.8}$ CP	2^{146} Enc.	2^{120} blocks
13 (22)	Imp. Diff.	$2^{111.8}$ CP	2^{155} Enc.	2^{112} blocks
14 (26)	Imp. Diff.	$2^{120.3}$ CP	2^{212} Enc.	2^{121} blocks
14 (26)	Imp. Diff.	$2^{112.3}$ CP	2^{220} Enc.	2^{113} blocks

Ассоциация РусКрипто

Аппаратная реализация блочных шифров

Алгоритм	Тактов на блок	Произв. [Kbps] 100 kHz	Площ. [GE]	Технол. [μm]
DES *n* = 64 *k* = 56	144	44.40	2,309	0.18
DESXL *n* = 64 *k* = 184	144	44.40	2,168	0.18
AES-128 *n* = 128 *k* = 128	1,032	12.40	3,400	0.35
PRESENT-80 *n* = 64 *k* = 80	32	200.00	1,570	0.18
Clefia *n* = 128 *k* = 128	36	355.56	4,993	0.09
Hight *n* = 64 *k* = 128	34	188.20	3,048	0.25
mCrypton *n* = 64 *k* = 96	13	492.30	2,681	0.13

Ассоциация РусКрипто

Программная реализация блочных шифров

Алгоритм	Шифр. такт/бл.	Произв. Kbps 4 MHz	Расш. такт/бл.	Произв. (% AES)	Размер кода [bytes]	SRAM [bytes]	Размер кода (% AES)
DES *n* = 64 *k* = 56	8,633	29.6	8,154	38.4	4,314	0	152.4
DESXL *n* = 64 *k* = 184	8,531	30.4	7,961	39.4	3,192	0	112.8
AES *n* = 128 *k* = 128	6,637	77.1	7,429	100.0	2,606	224	100.0
PRESENT *n* = 64 *k* = 80	10,723	23.7	11,239	30.7	936	0	33.1

Ассоциация РусКрипто

Программная реализация блочных шифров

Алгоритм	Шифр. такт/бл.	Произв. Kbps 4 MHz	Расш. такт/бл.	Произв. (% AES)	Размер кода [bytes]	Размер кода (% AES)
PRESENT *n* = 64 *k* = 80	10,723	23.7	11,239	30.7	936	33.1
Hight *n* = 64 *k* = 128	2,964	80.3	2,964	104.2	5,672	200.4
IDEA *n* = 64 *k* = 128	2,700	94.8	15,393	123.0	596	21.1
TEA *n* = 64 *k* = 128	6,271	40.8	6,299	53.0	1,140	40.3
SEA *n* = 96 *k* = 96	9,654	39.7	9,654	51.5	2,132	75.3

Ассоциация РусКрипто

Реализация блочных шифров на ПЛИС

Алгоритм	Макс. частота [MHz]	# Slice	Произв. [MB/s]	Пр/Slice [kb/s/slice]	ПЛИС
AES $n = 128$ $k = 128$	60	522	166	0.32	XC2S30-6
	196.1	17,425	25,107	1.44	XC3S2000-5
	67	264	2.2	0.01	XC2S15-6
	123	1,214	358	0.29	XC2V40-6
	150	1,800	1700	0.9	Spartan-3
Present $n = 64$ $k = 80$	258	176	516	2.93	XC3S400-5
$k = 128$	254	202	508	2.51	XC3S400-5

Ассоциация РусКрипто

Реализация блочных шифров на ПЛИС

Алгоритм	Макс. частота [MHz]	# Slice	Произв. [MB/s]	Пр/Slice [kb/s/slice]	ПЛИС
Present $n = 64$ $k = 80$	258	176	516	2.93	XC3S400-5
Present $n = 64$ $k = 128$	254	202	508	2.51	XC3S400-5
Hummingbird $n = 16$ $k = 256$	40.1	273	160.4	0.59	XC3S200-5
XTEA $n = 64$ $k = 128$	62.6	254	36	0.14	XC3S50-5
XTEA $n = 64$ $k = 128$	332.2	9,647	20,645	2.14	XC5VLX85-3
ICEBERG $n = 64$ $k = 128$	–	631	1,016	1.61	Virtex-2
SEA $n = 96$ $k = 96$	145	424	156	0.368	XC2V4000

Ассоциация РусКрипто

Реализация на VIRTEX-II XILINX

слайс (slice) – 2 LUT (4 входа) + 2 Flip-Flops + мультиплексоры + логика переноса + арифметические операции

		S-блоки	# Flip-Flop	# LUT	# Slice	Макс. частота [MHz]	такт /бл	Произв. [MB/s]	Пр/Slice kb/s/slice	Пр. [MB/s] 13.56MHz	Тр/Slice kb/s/slice 13.56MHz
AES $n = 128$ $k = 128$	Iter	[26]	271	1862	976	60.94	26	300.01	307.39	66.76	68.40
		LUT	271	3296	1672	74.42	26	366.38	219.12	66.76	39.93
	Ser	[26]	286	358	267	43.79	160	35.03	131.21	10.85	40.63
		LUT	286	495	333	56.00	160	44.80	134.53	10.85	32.58
Clefia $n = 128$ $k = 128$	Iter	[11]	409	1228	693	46.13	46	128.36	185.23	37.73	54.45
		LUT	409	1944	1040	50.42	46	140.30	134.90	37.73	36.28
	Ser	[11]	329	602	347	49.05	272	23.08	66.52	6.38	18.39
		LUT	329	787	439	57.75	272	27.18	61.91	6.38	14.54
Clefia $n = 128$ $k = 128$	Iter	[11]	409	1228	693	46.13	34	173.67	250.60	51.05	73.66
		LUT	409	1944	1040	50.42	34	189.82	182.52	51.05	49.09
	Ser	[11]	329	602	347	49.05	160	39.24	113.08	10.85	31.26
		LUT	329	787	439	57.75	160	46.20	105.24	10.85	24.71
Present $n = 64$ $k = 80$	Iter	LUT	200	303	155	155.76	47	212.10	1368.38	18.46	119.13
	Ser	LUT	203	258	131	114.17	295	24.77	189.08	2.94	22.46

Ассоциация РусКрипто

Реализация на VIRTEX-II XILINX

слайс (slice) – 2 LUT (4 входа) + 2 Flip-Flops + мультиплексоры + логика переноса + арифметические операции

		S-блоки	# Flip-Flop	# LUT	# Slice	Макс. частота [MHz]	такт /бл	Произв. [MB/s]	Пр/Slice kb/s/slice	Пр. [MB/s] 13.56MHz	Тр/Slice kb/s/slice
AES $n = 128$ $k = 128$	Iter	[26]	271	1862	976	60.94	26	300.01	307.39	66.76	68.40
		LUT	271	3296	1672	74.42	26	366.38	219.12	66.76	39.93
	Ser	[26]	286	358	267	43.79	160	35.03	131.21	10.85	40.63
		LUT	286	495	333	56.00	160	44.80	134.53	10.85	32.58
Clefia $n = 128$ $k = 128$	Iter	[11]	409	1228	693	46.13	46	128.36	185.23	37.73	54.45
		LUT	409	1944	1040	50.42	46	140.30	134.90	37.73	36.28
	Ser	[11]	329	602	347	49.05	272	23.08	66.52	6.38	18.39
		LUT	329	787	439	57.75	272	27.18	61.91	6.38	14.54
Clefia $n = 128$ $k = 128$	Iter	[11]	409	1228	693	46.13	34	173.67	250.60	51.05	73.66
		LUT	409	1944	1040	50.42	34	189.82	182.52	51.05	49.09
	Ser	[11]	329	602	347	49.05	160	39.24	113.08	10.85	31.26
		LUT	329	787	439	57.75	160	46.20	105.24	10.85	24.71
Present $n = 64$ $k = 80$	Iter	LUT	200	303	155	155.76	47	212.10	1368.38	18.46	119.13
	Ser	LUT	203	258	131	114.17	295	24.77	189.08	2.94	22.46

Ассоциация РусКрипто

Реализация на VIRTEX-5 XILINX

слайс (slice) – 4 LUT (6 входов) + 4 Flip-Flops + мультиплексоры + логика переноса + арифметические операции

		S-блоки	# Flip-Flop	# LUT	# Slice	Макс. частота [MHz]	такт /бл	Произв. [MB/s]	Пр/Slice kb/s/slice	Пр. [MB/s] 13.56MHz	Пр/Slice kb/s/slice
AES $n = 128$ $k = 128$	Iter	[26]	271	1391	456	96.04	26	472.81	1036.87	66.76	146.40
		LUT	271	1266	359	136.84	26	673.67	1876.53	66.76	185.95
	Ser	[26]	286	274	137	77.29	160	61.83	451.33	10.85	79.18
		LUT	286	258	113	113.25	160	90.60	801.77	10.85	96.00
Clefia $n = 128$ $k = 128$	Iter	[11]	409	816	243	108.66	46	302.36	1244.27	37.73	155.28
		LUT	409	809	267	267.00	46	742.96	2782.61	37.73	141.32
	Ser	[11]	329	469	156	110.69	272	52.09	333.91	6.38	40.90
		LUT	329	467	155	93.96	272	44.22	285.27	6.38	41.17
Clefia $n = 128$ $k = 128$	Iter	[11]	409	816	243	108.66	34	409.07	1683.43	51.05	210.08
		LUT	409	809	267	267.00	34	1005.18	3764.71	51.05	191.20
	Ser	[11]	329	469	156	110.69	160	88.55	567.64	10.85	69.54
		LUT	329	467	155	93.96	160	75.17	484.95	10.85	69.99
Present $n = 64$ $k = 80$	Iter	LUT	200	285	87	250.89	47	341.64	3926.87	18.46	212.24
	Ser	LUT	203	237	70	245.76	295	53.32	761.68	2.94	42.03

Ассоциация РусКрипто

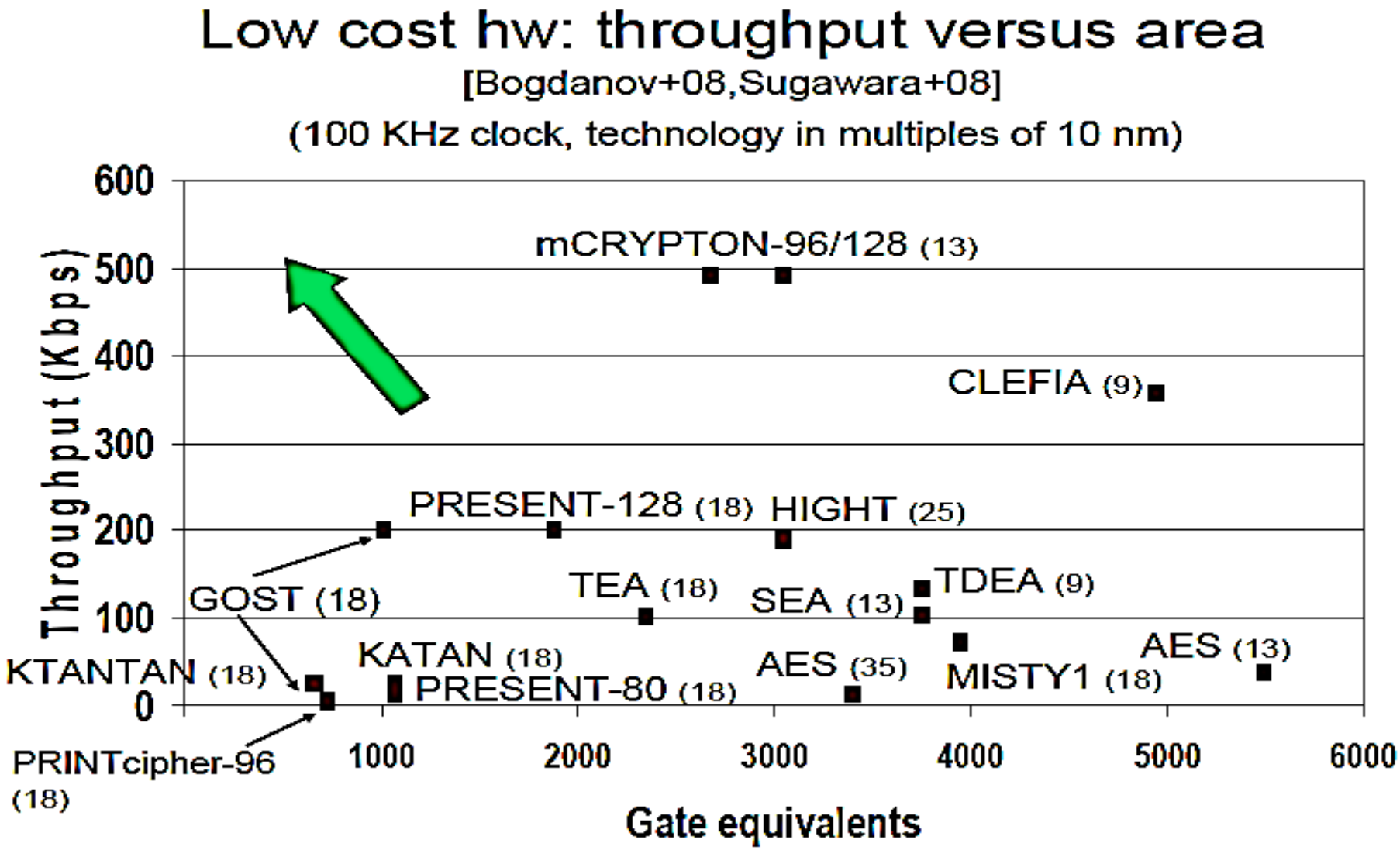
Реализация на VIRTEX-5 XILINX

слайс (slice) – 4 LUT (6 входов) + 4 Flip-Flops + мультиплексоры + логика переноса + арифметические операции

		S-блоки	# Flip-Flop	# LUT	# Slice	Макс. частота [MHz]	такт /бл	Произв. [MB/s]	Пр/Slice kb/s/slice	Пр. [MB/s]	Пр/Slice kb/s/slice
										13.56MHz	
AES $n = 128$ $k = 128$	Iter	[26]	271	1391	456	96.04	26	472.81	1036.87	66.76	146.40
		LUT	271	1266	359	136.84	26	673.67	1876.53	66.76	185.95
	Ser	[26]	286	274	137	77.29	160	61.83	451.33	10.85	79.18
		LUT	286	258	113	113.25	160	90.60	801.77	10.85	96.00
Clefia $n = 128$ $k = 128$	Iter	[11]	409	816	243	108.66	46	302.36	1244.27	37.73	155.28
		LUT	409	809	267	267.00	46	742.96	2782.61	37.73	141.32
	Ser	[11]	329	469	156	110.69	272	52.09	333.91	6.38	40.90
		LUT	329	467	155	93.96	272	44.22	285.27	6.38	41.17
Clefia $n = 128$ $k = 128$	Iter	[11]	409	816	243	108.66	34	409.07	1683.43	51.05	210.08
		LUT	409	809	267	267.00	34	1005.18	3764.71	51.05	191.20
	Ser	[11]	329	469	156	110.69	160	88.55	567.64	10.85	69.54
		LUT	329	467	155	93.96	160	75.17	484.95	10.85	69.99
Present $n = 64$ $k = 80$	Iter	LUT	200	285	87	250.89	47	341.64	3926.87	18.46	212.24
	Ser	LUT	203	237	70	245.76	295	53.32	761.68	2.94	42.03

Ассоциация РусКрипто

Блочные шифры



Ассоциация РусКрипто

Поточные шифры

ISO/IEC FDIS 29192-3:

- Enocoro
- Trivium

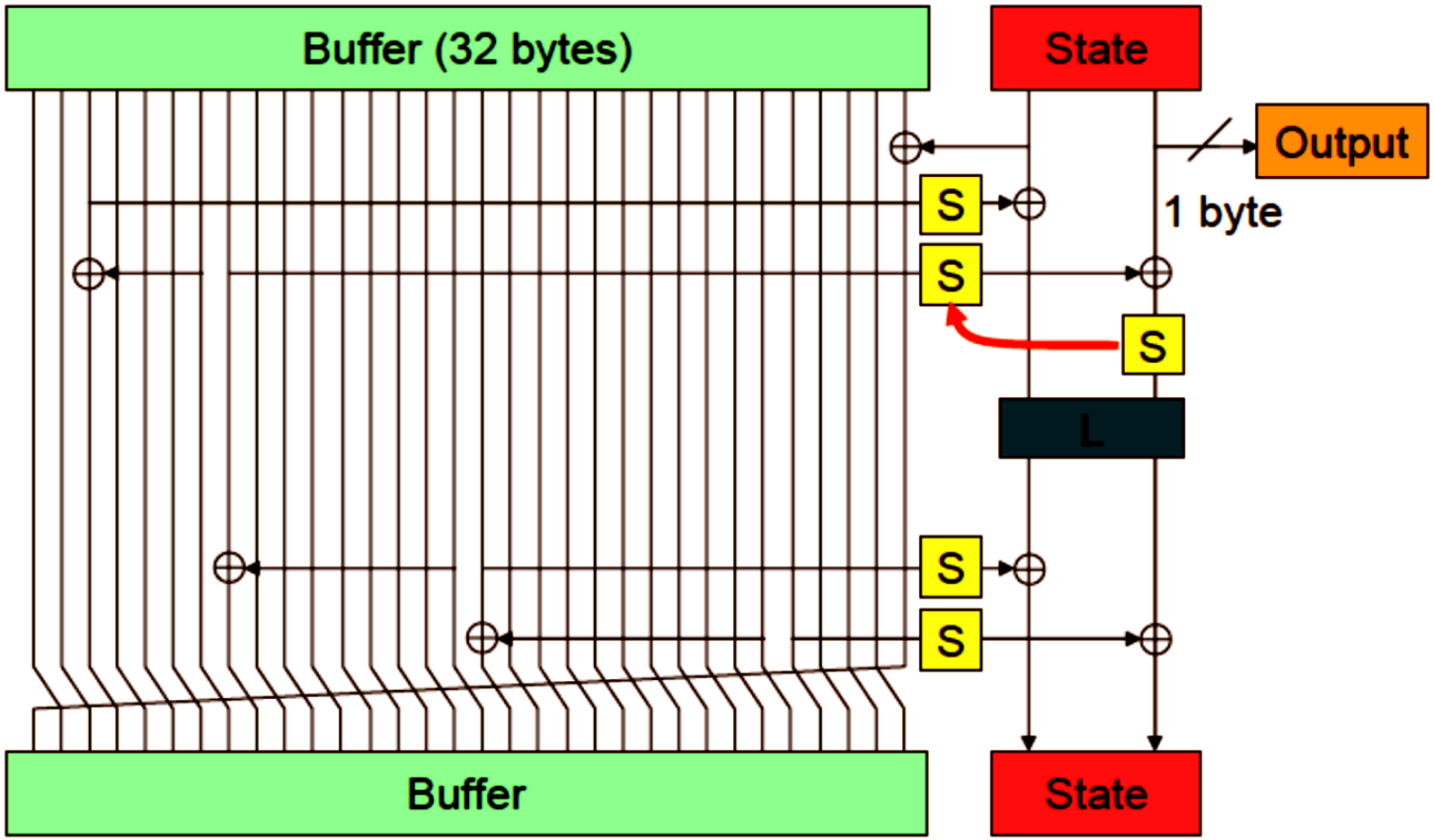
Enocoro

Поточный шифр Enocoro разработан фирмой Hitachi по поручению Национального института информационных и коммуникационных технологий Японии (NICT) в 2007.

В стандарт ISO/IEC 29192-3 входят шифры Enocoro-80 и Enocoro-128v2. Это байтно-ориентированные поточные шифры с ключом, равным, соответственно 80 и 128 бит.

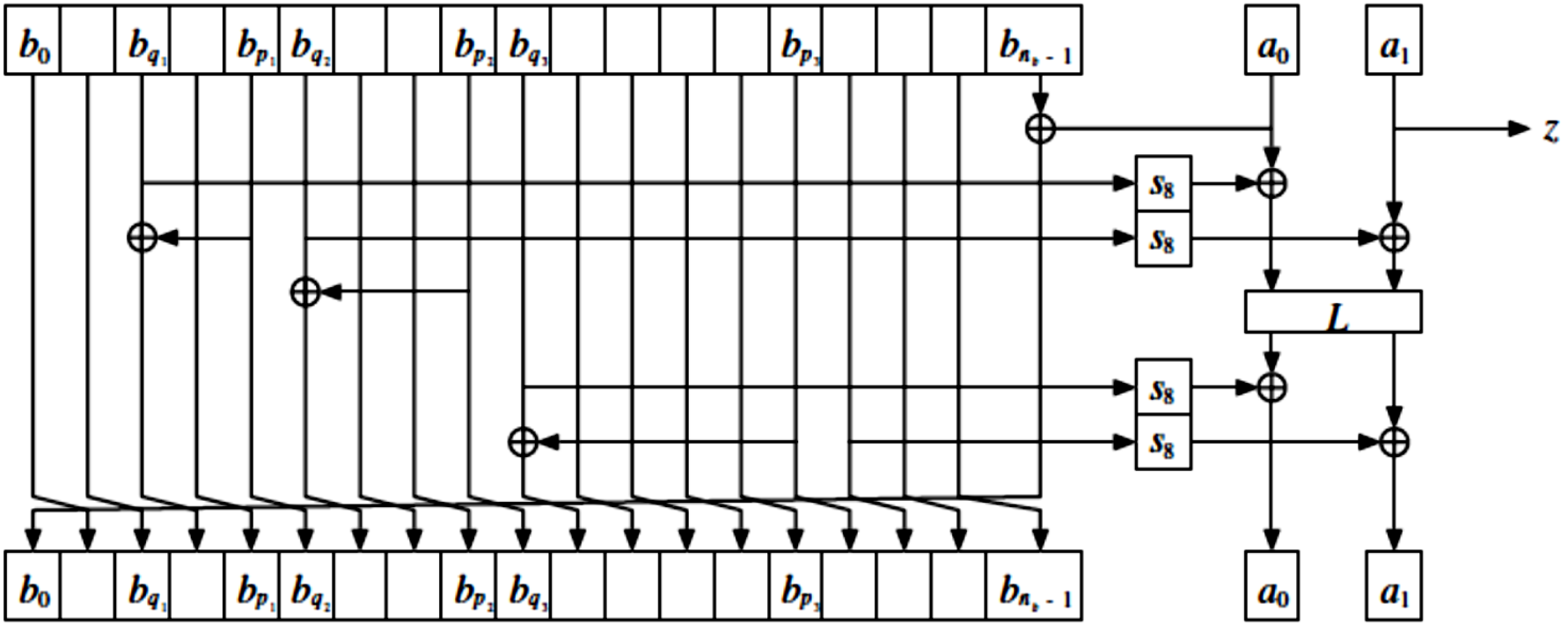
Ассоциация РусКрипто

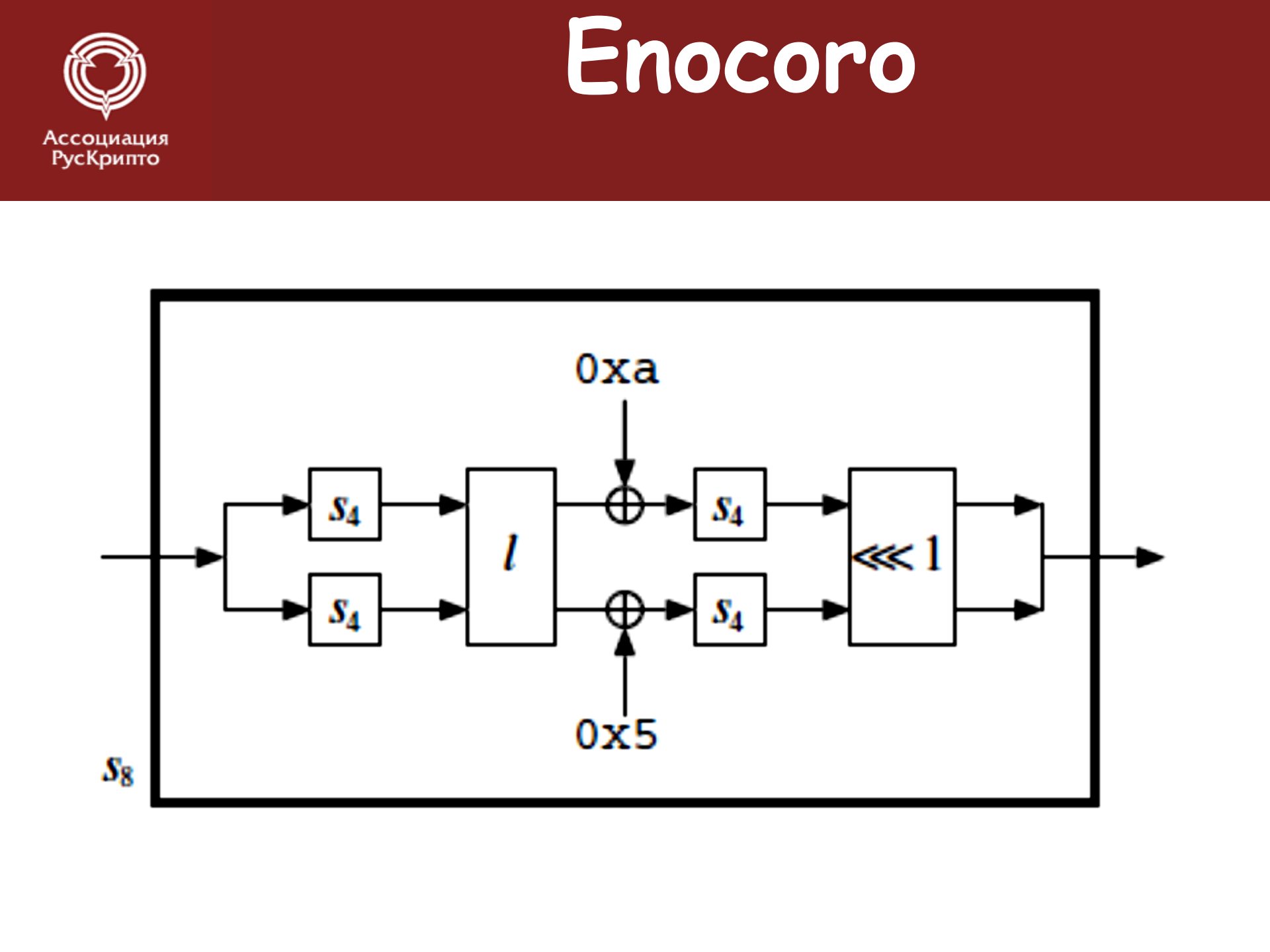
Enocoro



Ассоциация РусКрипто

Enocoro




Ассоциация
РусКрипто
Enocoro
0xa
s_4
s_4
l
s_4
s_4
$\lll 1$
0x5
s_8

Ассоциация РусКрипто

Enocoro
Аппаратная реализация

Алгоритм	Тактов на иниц. [clk]	Выход [b/clk]	Площ. [GE]	Технол. [μm]
Enocoro-80 $n = 8$ $k = 80$	40	8	2,700	0.18
Enocoro-128 $n = 8$ $k = 80$	96	8	4,100	0.18

Trivium

Поточный шифр Trivium разработан бельгийскими учеными Christophe de Canniere и Bart Preneel.

Впервые представлен в 2005 г. в качестве участника европейского проекта eSTREAM по Профилю 2 (поточные шифры, ориентированные на аппаратную реализацию). В 2008 г., как один из победителей конкурса, вошел портфолио европейского проекта eSTREAM.

Ассоциация РусКрипто

Trivium

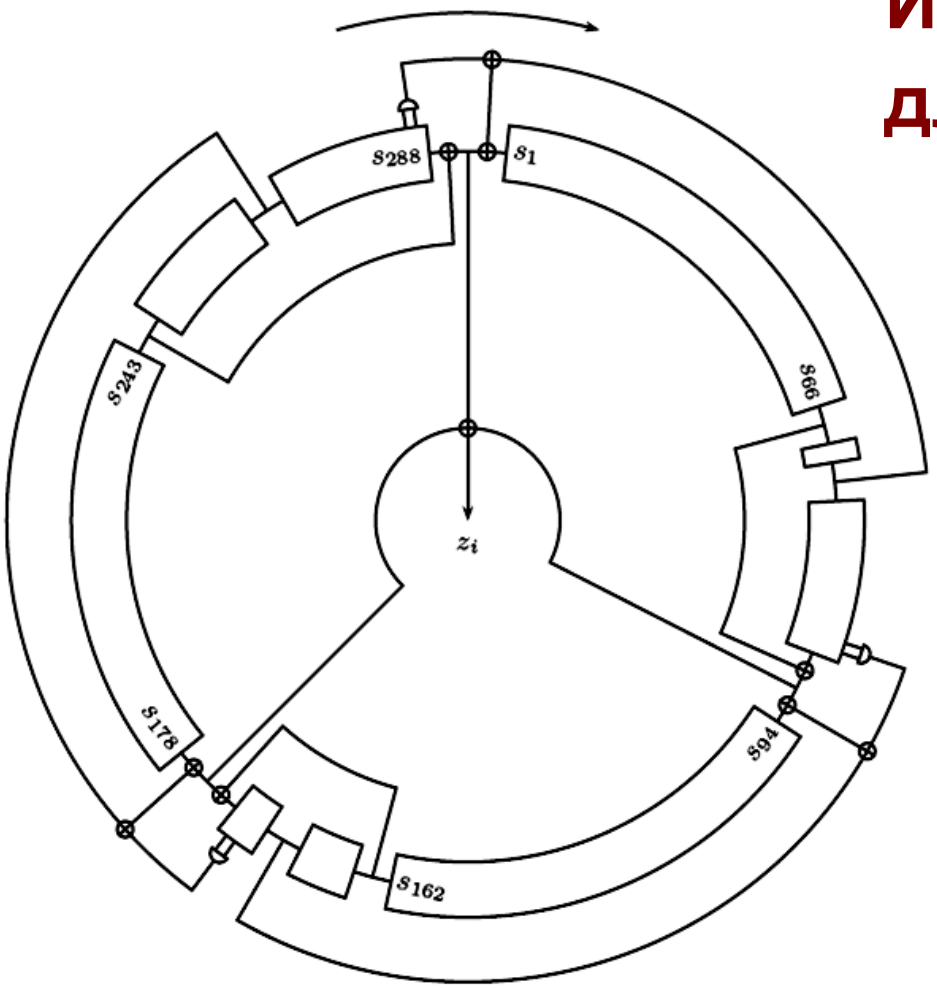
Работа алгоритма определяется 80-битным секретным ключом и 80-битным IV.

Внутреннее состояние соответствующего автомата определяется 288 битами, объединенными в три нелинейных регистра сдвига по 93, 84 и 111 бит соответственно.

Выходом является битовая последовательность, определяемая как сумма съемов с каждого из регистров. Максимальная длина выходной последовательности, полученной на одном ключе — 2^{64} бита.

Ассоциация РусКрипто

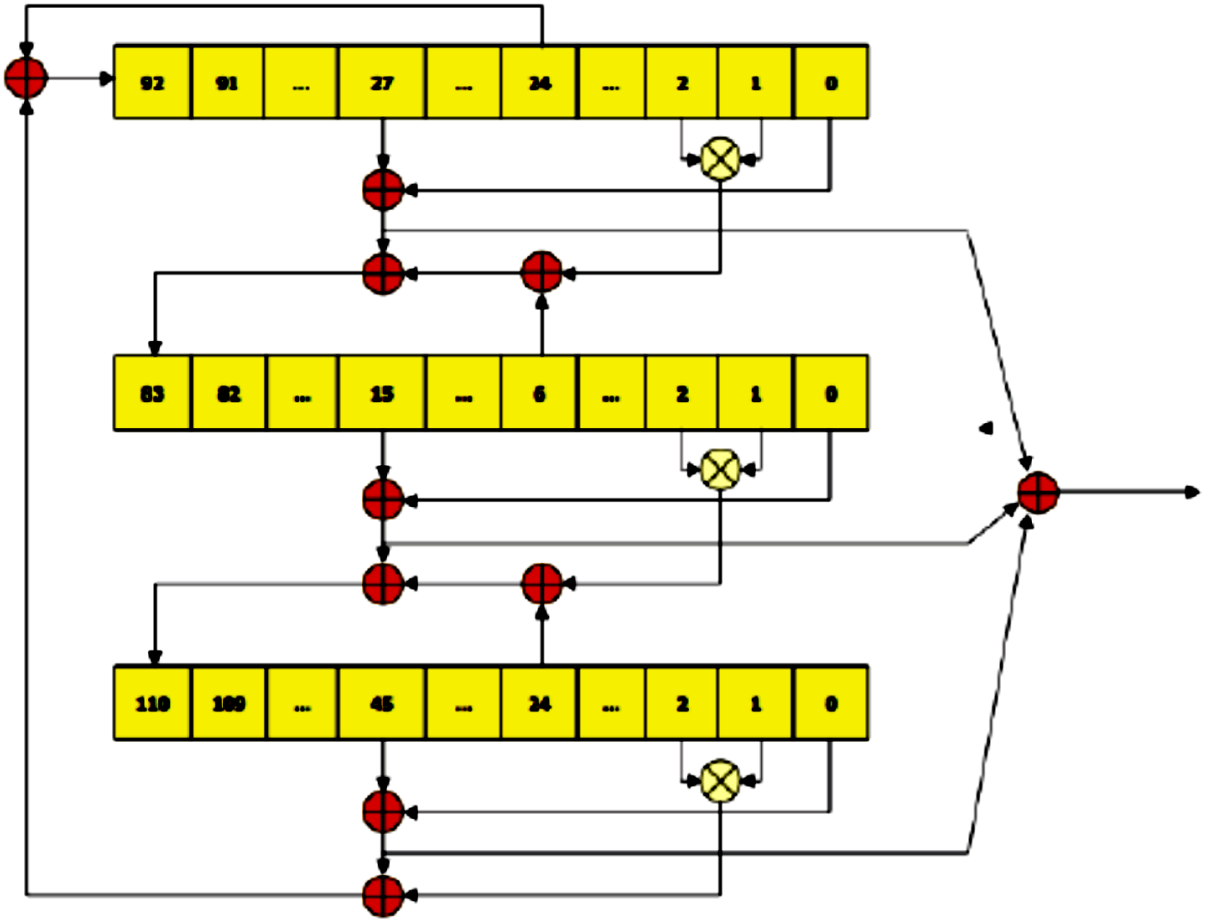
Trivium



Имеется возможность для распараллеливания – до 66 параллельных итераций (как правило, выбирают 8, 16, 32 или 64).

Ассоциация РусКрипто

Trivium



Ассоциация РусКрипто

Trivium
Аппаратная реализация

Алгоритм	Тактов на иниц. [clk]	Выход [b/clk]	Площ. [GE]	Технол. [μm]
Trivium $n = 1$ $k = 80$	1152	1	2,599	0.13

Ассоциация РусКрипто

Реализация поточных шифров

Алгоритм	Тактов на блок	Произв. [Kbps] 100 kHz	Площ. [GE]	Технол. [μm]
AES-128 *n* = 128 *k* = 128	1,032	12.40	3,400	0.35
PRESENT-80 *n* = 64 *k* = 80	32	200.00	1,570	0.18
Trivium *n* = 1 *k* = 80	1	100.00	2,599	0.13
Grain *n* = 1 *k* = 80	1	100.00	1,294	0.13

Ассоциация РусКрипто

Реализация поточных шифров на ПЛИС

Алгоритм	Время [ns]	Такт/ блок	# Slice	Произв. [MB/s]	Пр/Slice [kb/s/slice]	ПЛИС
Present $n = 64$ $k = 128$	8.78	256	117	28.46	0.24	xc3s50-5
Trivium $n = 1$ $k = 80$	4.17	1	50	240	4.80	xc3s50-5
Trivium(x64) $n = 64$ $k = 80$	4.74	1	344	13,504	39.26	xc3s400-5
Grain v1 $n = 1$ $k = 80$	5.10	1	44	196	4.45	xc3s50-5
Grain 128 $n = 1$ $k = 128$	5.10	1	50	196	3.92	xc3s50-5
MICKEY v2 $n = 1$ $k = 80$	4.29	1	115	233	2.03	xc3s50-5
MICKEY128 $n = 1$ $k = 128$	4.48	1	176	223	1.27	xc3s50-5

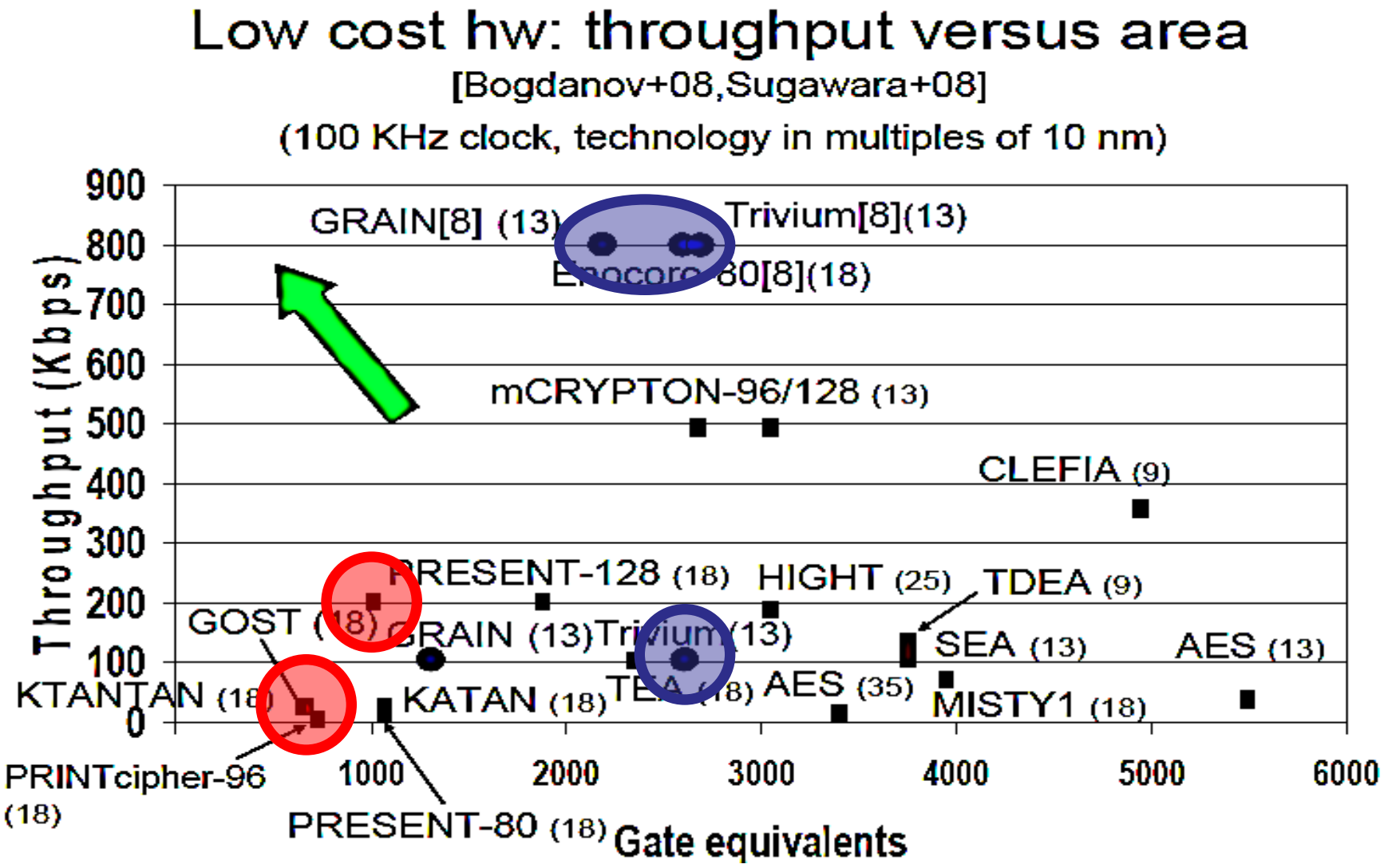
Ассоциация РусКрипто

Реализация поточных шифров на Xilinx Virtex-II XC2V6000-4ff1152

Алгоритм	Частота [MHz]	# Slice	Произв. [Mb/s]	Пр/Slice [Mb/s/slice]
Trivium	207	41	207	5.05
Grain-128	181	48	181	3.77
MICKEY-128 2.0	200	190	200	1.05
Phelix	62.5	1,213	1000	0.82

Ассоциация РусКрипто

Поточные шифры



Ассоциация РусКрипто

Открытый ключ

ISO/IEC FDIS 29192-4:

- cryptoGPS – односторонний механизм аутентификации, основанный на дискретном логарифме над эллиптической кривой.
(Girault, Poupard, Stern)

Ассоциация РусКрипто

Открытый ключ

Алгоритм	Крипт. ст. [bit]	Время работы [clk]	Площ. [GE]	Технол. [μm]
cryptoGPS	80	724	2876	0.13

Ассоциация РусКрипто

Открытый ключ

ISO/IEC FDIS 29192-4:

- ALIKE (Authenticated Lightweight Key Exchange) — односторонний механизм ключевого обмена, базирующийся на шифровании.

Ассоциация РусКрипто

Открытый ключ

Алгоритм	Размер кода 8051 core [kbytes]	Время работы [ms]	Частота 8051 core [MHz]
ALIKE	1.6	80	31

Ассоциация РусКрипто

Открытый ключ

ISO/IEC FDIS 29192-4:

- Механизм выработки цифровой подписи.

Ассоциация РусКрипто

Открытый ключ

Алгоритм	Размер кода [Byte]	RAM [Byte]	Время работы [ms]	Энергия [µJ]
IBS Выработка подписи	54,308	858	896	12,370
IBS Проверка подписи	55,374	922	5,610	77,400

Криптография с открытым ключом

Вычисления в конечном поле

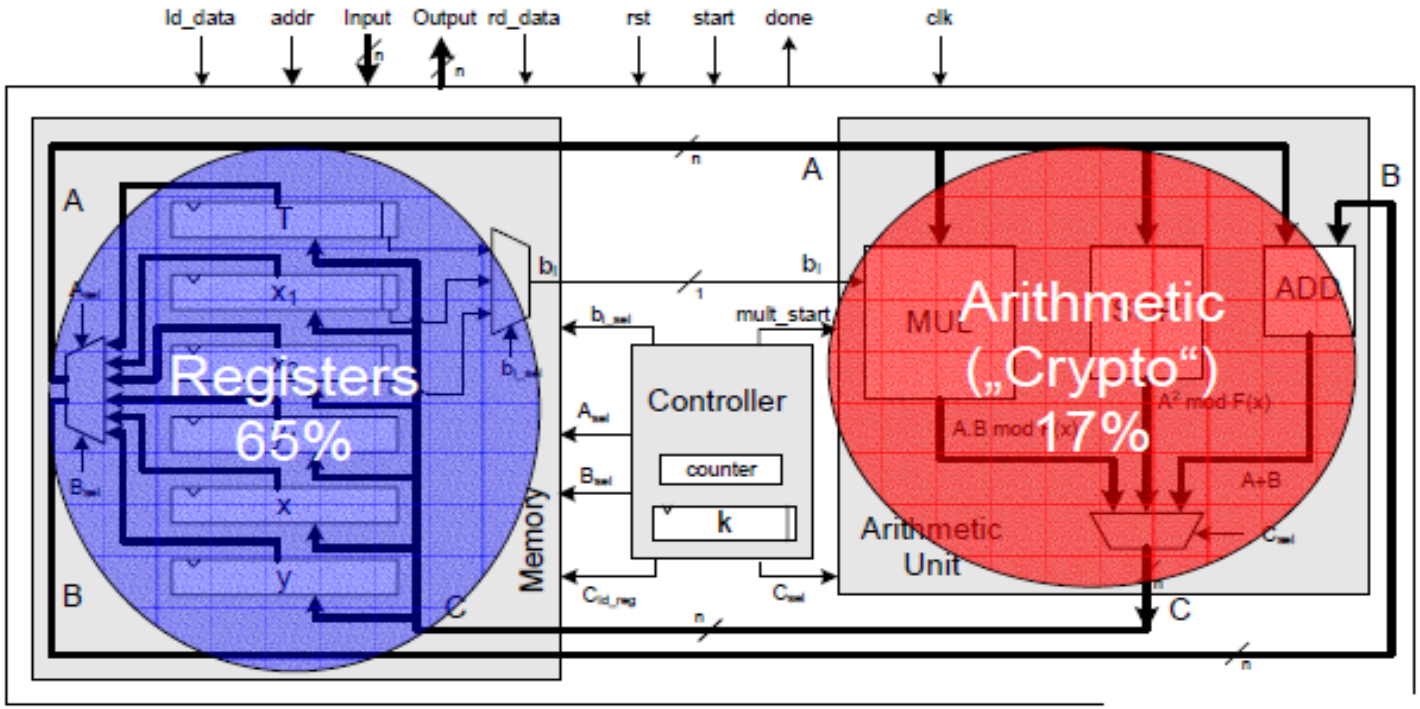
Размер поля	Arithmetic (gates)	Memory (gates)	Total (gates)	Time (ms)
113	1,625	6,686	10,112	47
131	2,071	7,747	11,969	61
163	2,572	9,632	15,094	108
193	2,776	11,400	17,723	139

Ассоциация РусКрипто

Криптография с открытым ключом

The Tiny ECC Processor Design

- ECC processor implementation for $2^{113}, 2^{131}, 2^{163}, 2^{193}$



Ассоциация РусКрипто

Отечественная легковесная криптография