"Гамма"
Искусство безопасности

Исследование различных характеристик шифра «Кузнечик» на российских процессорах и платформах IoT

Овчинников Андрей Игоревич
ФГУП «НПП «ГАММА»
ovchinnikov.ai@nppgamma.ru

Мелешин А. Е.
ФГУП «НПП «ГАММА»
Истомин А. А.
ФГУП «НПП «ГАММА»

"Гамма"

Искусство безопасности

ШИФРОВАНИЕ НА «IOT» ПРОЦЕССОРАХ

"Гамма"
Искусство безопасности

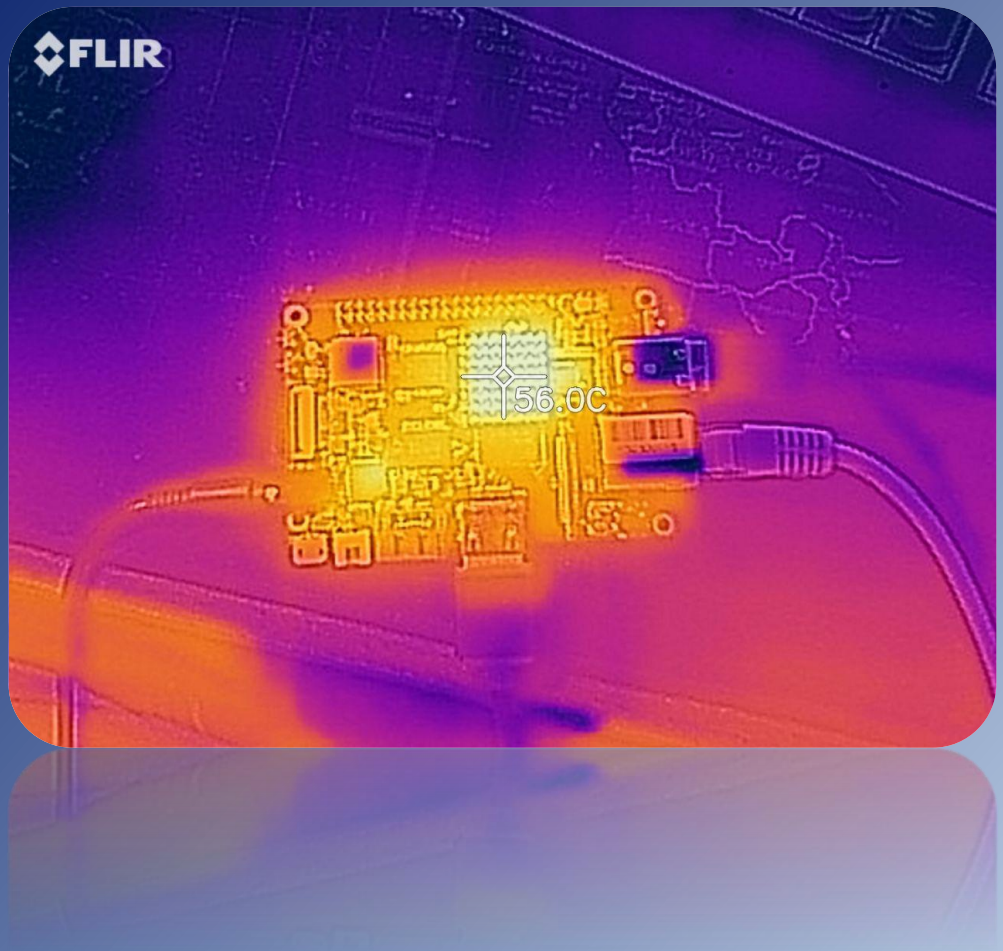
Фундамент работы

1. Процессоры и контроллеры на базе **ARM** (Allwinner, Rockchip, Broadcom и т.д.) в центре устройств **“IoT”** (интернета вещей) используются как сенсоры для управления умным домом в качестве сигнализации, а также в коммуникационных устройствах таких, как смартфоны, планшеты или **IP/Видео-IP-телефонии**.
2. В большинстве случаев существующие инфраструктуры или компонентные базы не подлежат изменению по «железу» без огромных затрат. Дорабатывать возможно только программное обеспечение.
3. Данное исследование рассматривает десятку самых распространенных чипов и платформ с точки зрения скорости шифрования **«Кузнечиком»,** а также потребления памяти и электроэнергии при шифровании.

"Гамма"
Искусство безопасности

Главные Игроки

- SAMSUNG
- Allwinner
- Rockchip
- Broadcom
- Mediatek
- NXP
- …



"Гамма"
Искусство безопасности

Реализация программы для измерений

- **Исходники:** nettle / GostCrypt / GOST
- «Чистый» C/C++ , без «ручной» оптимизации
- Compiler : -O3

"Гамма"
Искусство безопасности

Таблица измерений

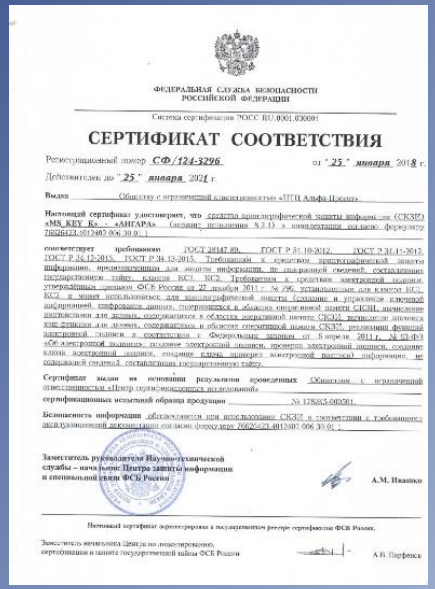
Производитель	Наименование	Архитестура	Потоки	макс. Частота	Мощность(Вт.)	Скорость (МБ/с)	Скорость/Поток	Скорость/Вт.
Broadcom	BCM2835	32bit	1	1000 MHz	0.4	**0.70**	0.70	1.75
Broadcom	BCM2709	32bit (64 теор.)	4	1400 MHz	3.5	**4.70**	1.18	1.34
Allwinner	R40	64bit	4	1200 MHz	5,0	**5.20**	1.30	1.04
Allwinner	H3	32bit	4	1200 MHz	3,0	**5.70**	1.43	1.90
Allwinner	H8 (8 потоков теор.)	32bit	4	2000 MHz	7.5	**7.10**	1.78	0.95
Allwinner	H5	64bit (HMP)	4	1400 MHz	5,0	**9.10**	2.28	1.82
Amlogic	905	64bit	4	1500 MHz	4,0	**13.00**	3.25	3.25
Samsung	S5P6818	32bit	8	1400MHz	7,0	**15.40**	1.93	2.20
Samsung	Exynos 5422	32bit (HMP)	8	2GHz / 1.3GHz	14,0	**31.40**	3.93	2.24
Intel	i7-6700	64bit	8	4000 MHz	91,0	**125.00**	15.63	1.37
Intel	i7-5820	64bit	12	3600 MHz	140,0	**160.00**	13.33	1.14
Intel	Xeon-E5-2697 v3	64bit	28	3600 MHz	290,0	**490.00**	17.50	1.69

"Гамма"
Искусство безопасности

СКЗИ "MS_KEY K" - "АНГАРА"

- **Особенности:**
- Используемый процессор: NXP P5

- **Скорость работы:**
- шифрование/расшифрование **в режимах (ECB, CBC, OFB, CFB): 3400 байт/сек**
- **вычисление имитовставки: 3900 байт/сек**
- **пиковое энергопотребление: 87,5 милливатт**



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации ФСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-3296 от "25" января 2018 г.

Действителен до "25" января 2021 г.

Выдан Обществу с ограниченной ответственностью «ПТЦ Альфа Проект»

Настоящий сертификат удостоверяет, что средства криптографической защиты информации (СКЗИ) «MS_KEY K» – «АНГАРА» Согласно исполнению 8.7.13 в комплектации согласно формуляру 76926423.6012407.006 30 01-1

соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015, Требованиям к средствам криптографической защиты шифрования, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, классов КС1, КС2. Требованиям к средствам электронной подписи, утвержденных приказом ФСБ России от 27 декабря 2011 г. № 796, устанавливающих для классов КС1, КС2, и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование данных, подготовленных в объектах иных видов защиты СКЗИ), вычисление имитовставки для данных, содержащихся в объектах операционной среды СКЗИ, вычисление значения хэш-функции для данных, содержащихся в объектах операционной среды СКЗИ, реализации функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

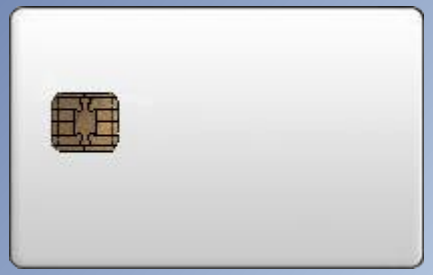
Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «Центр сертификационных исследований» сертификационных испытаний образца продукции № 175265-080301

Безопасность информации обеспечивается при использовании СКЗИ в соответствии с требованиями эксплуатационной документации согласно формуляру 76926423.6012407.006 30 01-1

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России А.М. Иванько

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.В. Парфенов



"Гамма"
Искусство безопасности

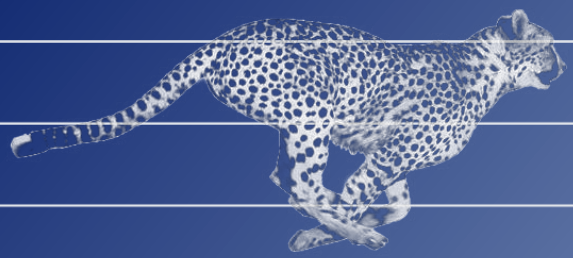
Требуемые скорости

• Телеметрия	**< 1 МБ/с**
• CAN/MODBUS	**< 1 МБ/с**
• 150 одновременных VoIP(HQ) звонков	**2 МБ/с**
• Репликация данных системы СКУД	**0,5-4 МБ/с**
• 8 потоков от видеокамер (1080p) сигнализации	**5,7 МБ/с**
• Удаленное администрирование	**0,2-10 МБ/с**
• 4К UHQ Видеоконференция (4 потоков)	**12-20 МБ/с**

"Гамма"
Искусство безопасности

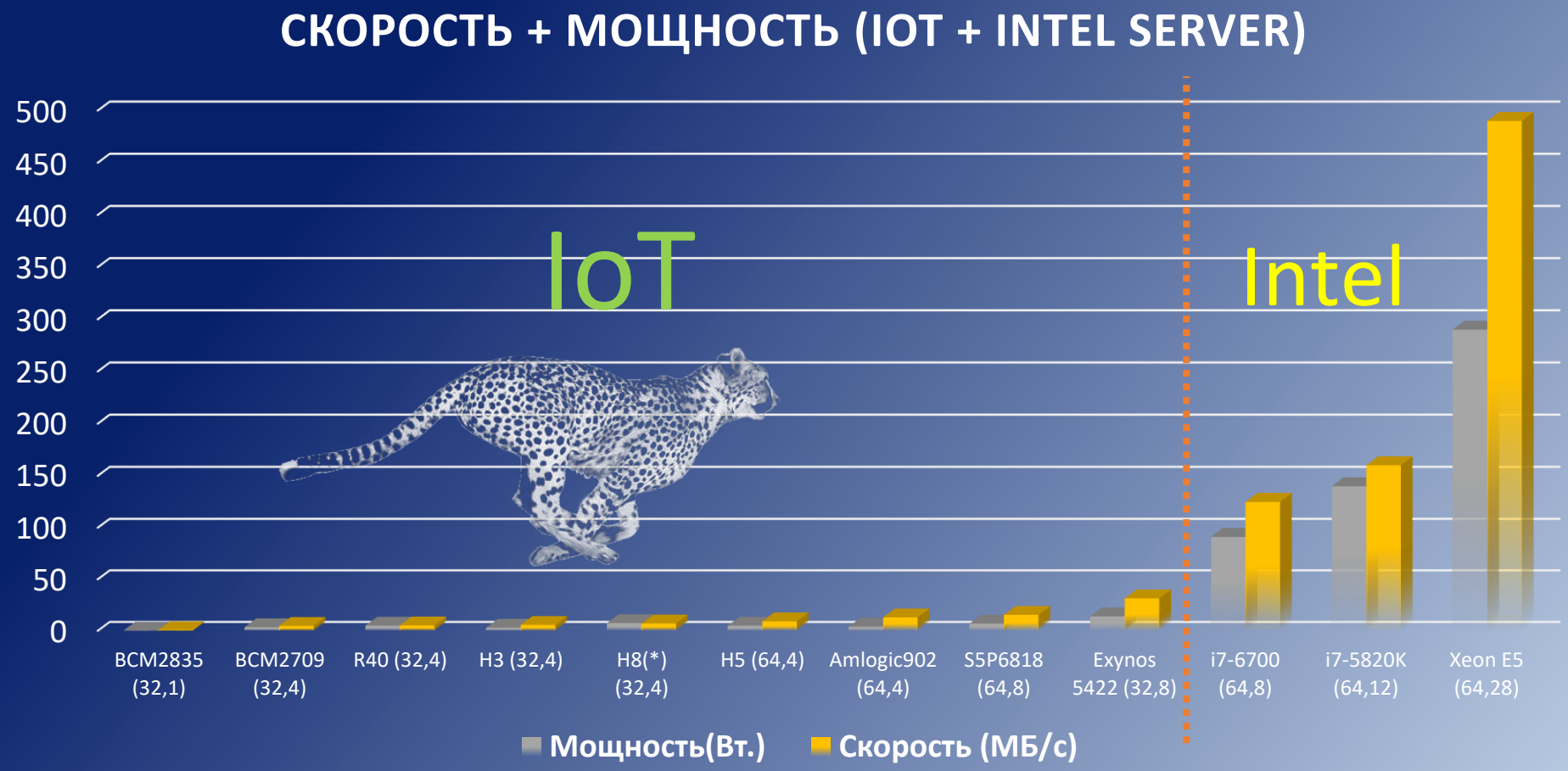
Графики – Скорость IoT

Скорость + Мощность (IoT) 0,7- 31,4 МБ/с



"Гамма"
Искусство безопасности

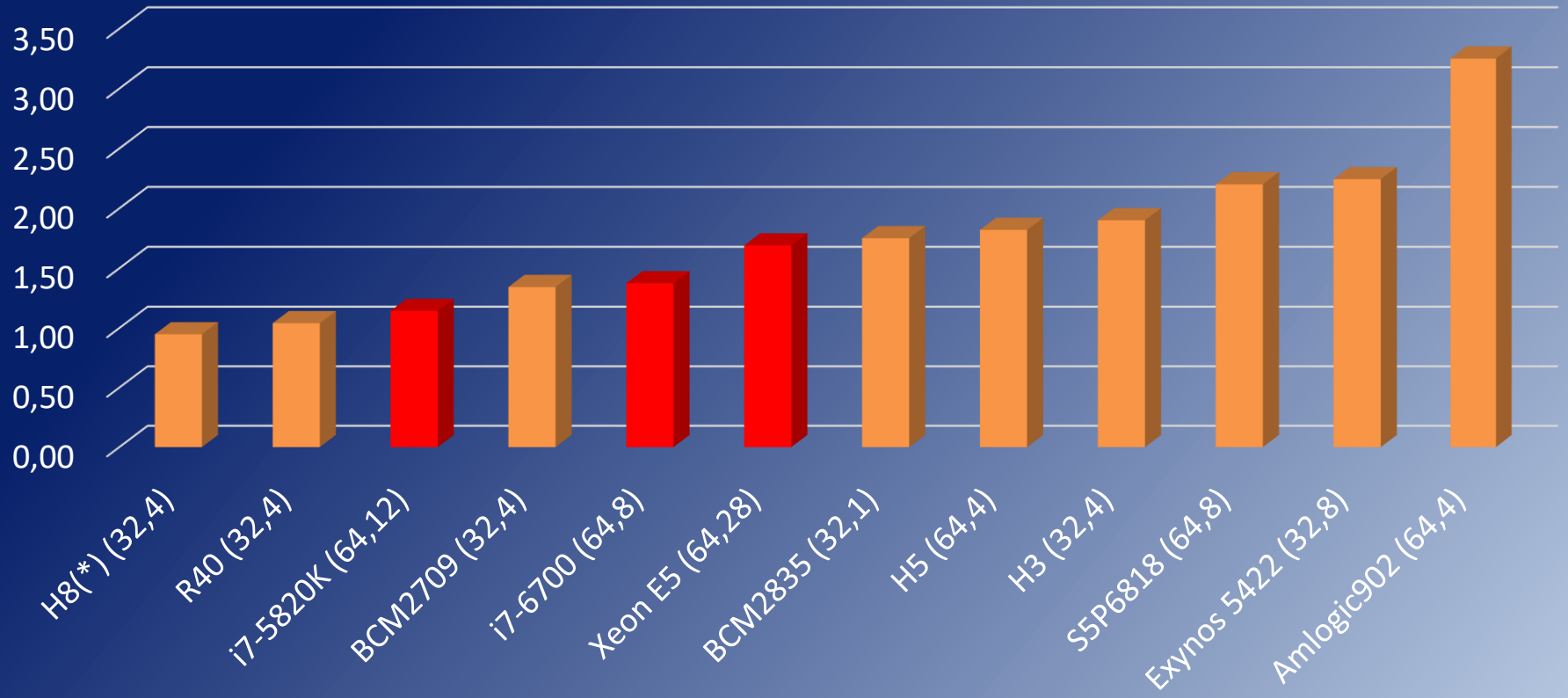
Графики – Скорость «Все»



"Гамма"
Искусство безопасности

Скорость / Мощность

Скорость / Вт. ≈ 1-3 MB/s/W



"Гамма"
Искусство безопасности

IoT - Процессоры

Все протестированные процессоры имели на кремне интегрированный графический процессор (**Mali™-450**).

Только у одного, у **Samsung Exynos Octa 5422,** графический чип был с модулем более высокого класса (**Mali™-T628**), который имел возможность программирования на языке **OpenCL**

Мы решили исследовать возможности использования встроенной GPU вместо или параллельно к CPU на компактных платформах

"Гамма"
Искусство безопасности

Результаты реализации шифра на OpenCL

- На **Samsung Exynos5422** (ARM® Cortex™-A15 Quad 2.0GHz / Cortex™ -A7 Quad 1.4GHz), используя исключительно интегрированную GPU (Mali™-T628), мы добились следующего результата:

- Только CPU работает : **31.5 MB/s**
- Только GPU работает : **0.68 MB/s** (**46,3*x*** медленнее)

(**для примера:** эта программа на AMD Radeon 6370M показывает следующую скорость:
- Шифрование, ECB: 11,65Мбайт/с
- Расшивафрование, ECB: 11,70Мбайт/с
)

ИТОГИ →

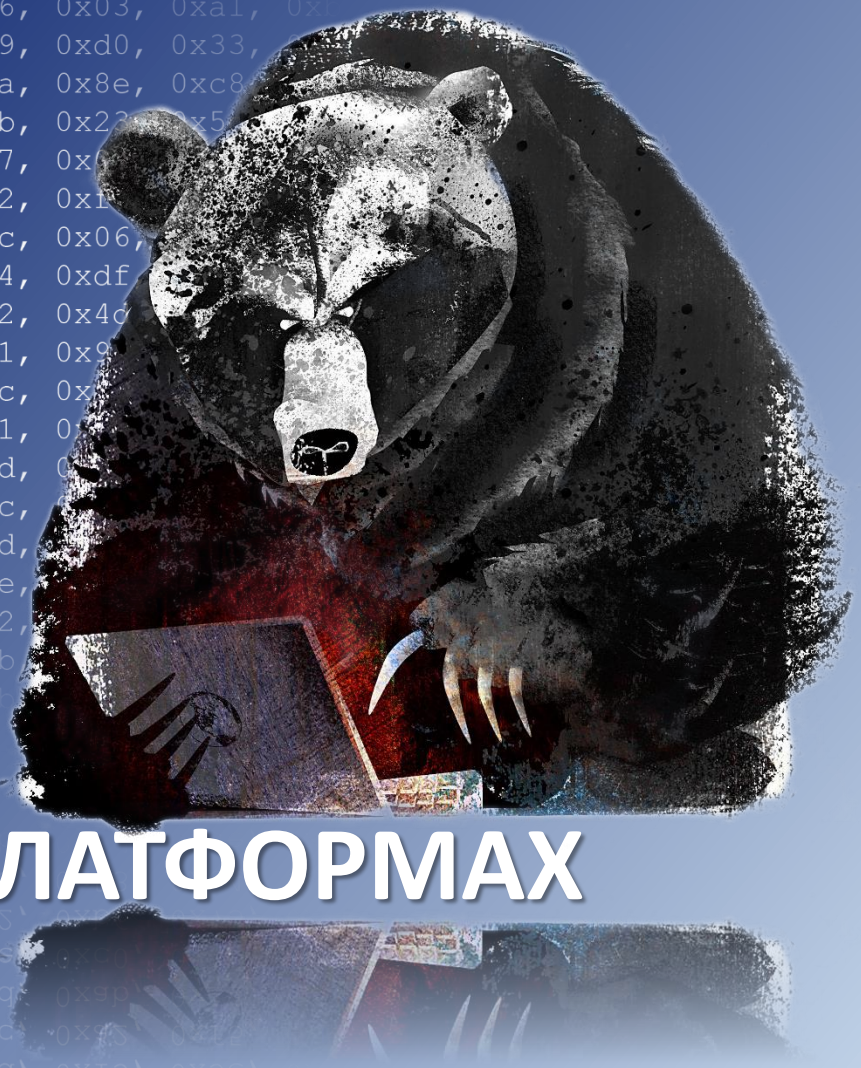
Пока не стоит на себя брать усилия использовать интегрированную GPU для дополнительных мощностей !

"Гамма"
Искусство безопасности

IoT - Итоги

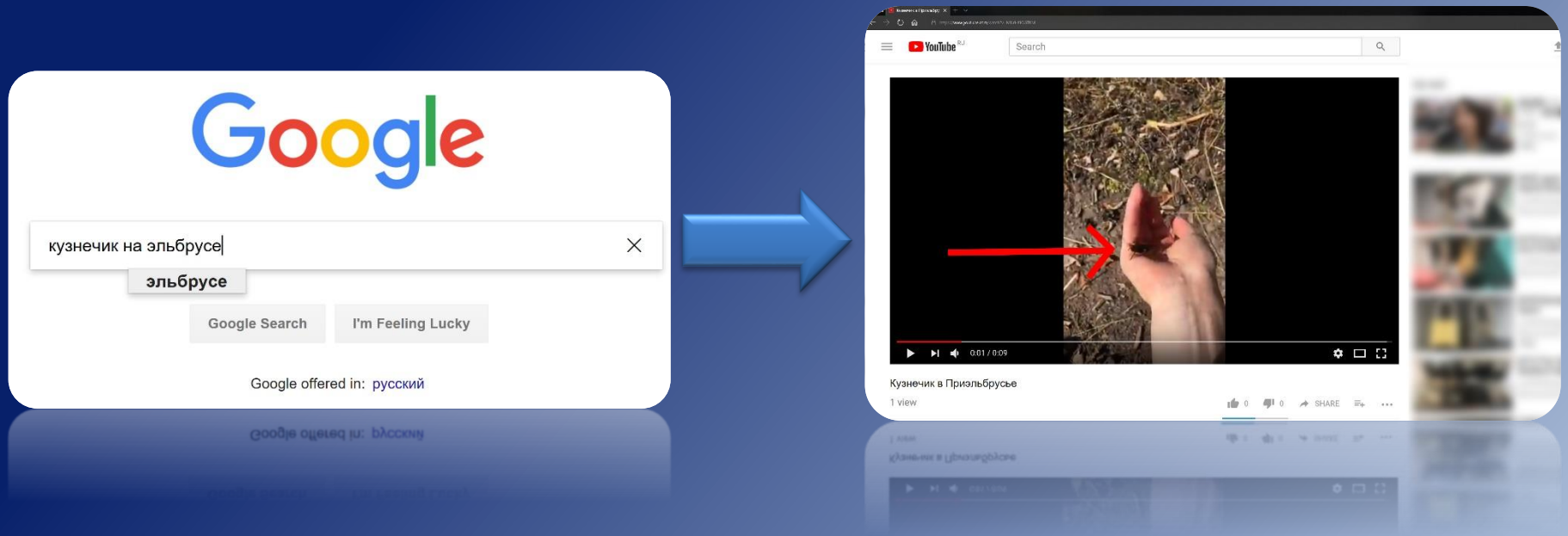
- Из этих данных можно вывести сценарии, где дополнительная нагрузка на систему в случае использования шифрования не мешает главной задаче процессора или ситуации, в которых алгоритм **ГОСТ Р 34.12–2015** слишком ***«тяжелый»*** для слабого процессора. Эти результаты помогут, например, реализации решения зашифрованной IP-телефонии или передаче зашифрованного видеопотока в системе СКУД без изменения компонентной базы или добавления дополнительных устройств.

- Энергетическая эффективность при вычислениях IoT-процессоров может превосходить многократно эффективность классических серверных процессоров



ШИФРОВАНИЕ НА ОТЕЧЕСТВЕННЫХ ПЛАТФОРМАХ

Одна из причин …



*а поиск **«Кузнечик на Байкале»** ведет к рыбалке …*

"Гамма"
Искусство безопасности

Эльбрус

- **Параметры стенда:**
  - 4 процессора e2k
    по 4 потока каждый
  - 64ГБ опер. памяти
  - ОС семейства Debian

```
processor: 0-15
vendor_id: EL2S4
cpu family: 4
model: 3
model name: E2S
revision: 1
cpu MHz: 750.18640
L1 cache size: 64 KB
L1 cache line: 32 bytes
L2 cache size: 2048 KB
L2 cache line: 64 bytes
bogomips: 1500.22
```

Результат измерения:

1,44МБ/с /на ядро : 23МБ/с на АРМ

"Гамма"
Искусство безопасности

Байкал – Т1

- **Параметры стенда:**
  - Процессор : Т1
  - оперативная память:2GB
  - ОС: Linux

```
system type: Baikal-T Generic SoC
machine: Baikal-T1 BFK2 ev. board
processor: 0-1
cpu model: MIPS P5600 V3.0
FPU V2.0
BogoMIPS : 1196.85
wait instruction: yes
microsecond timers: yes
tlb_entries: 576
extra interrupt vector: yes
hardware watchpoint: yes, count: 4
address/irw mask: [0x0ffc, 0x0ffc,
0x0ffb, 0x0ffb]
isa: mips1 mips2 mips32r1 mips32r2
```

Результат измерения:

1,11МБ/с /на ядро : 2,2МБ/с на плату

"Гамма"
Искусство безопасности

Комдив

- **Параметры стенда:**
  - Процессор: **K64M**
  - оперативная память:2GB
  - ОС: AstraLinux

```
system type: BAGET
machine: SRISA 1890VM8IA mITX v.2
processor: 0
cpu model: SRISA K64M V4.3
FPU V0.0
BogoMIPS: 531.66
wait instruction: yes
microsecond timers: yes
tlb_entries: 64
extra interrupt vector: yes
hardware watchpoint: yes, count: 2,
address/irw mask: [0x0fff, 0x0fff]
isa: mips1 mips2 mips3 mips4 mips5
mips32r1 mips64r1ASEs
implemented: cpv
shadow register sets: 1
```

Результат измерения:

2,7МБ/с /на ядро (1) = на АРМ

"Гамма"
Искусство безопасности

Русские Платформы - Итоги

- **Эльбрус**
  - плохая оптимизация компилятора
  - проблематичный теплоотвод
- **Байкал**
  - Сложность разработки / адаптации
  - Отзывчивая техподдержка
- **Комдив**
  - Лучшая техподдержка
  - Наличие репозитария
  - Лучшая скорость / ядро .

МУЛЬТИКЛЕТОЧНЫЕ ПРОЦЕССОРЫ (ПЕРСПЕКТИВНОЕ РАЗВИТИЕ)

"Гамма"
Искусство безопасности

Мультиклеточные процессоры

Мултиклет

До 4 Клеток

(**64 Клетки** в разработке)

Mellanox (Tilera)

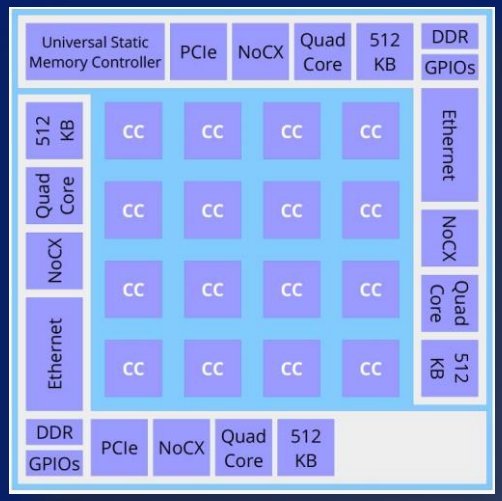
До 72 Клеток
(Первый на рынке)

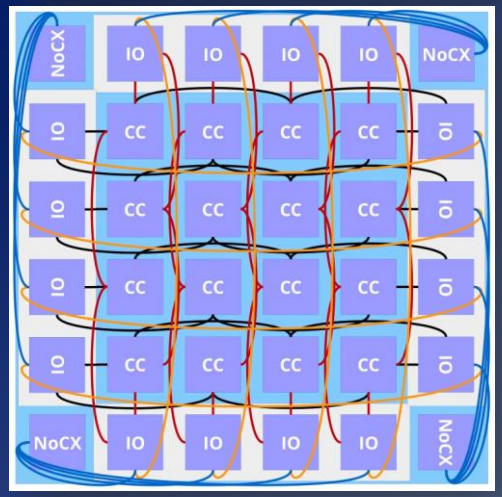
Kalray

До 288 Клеток (690 GFLOPS)

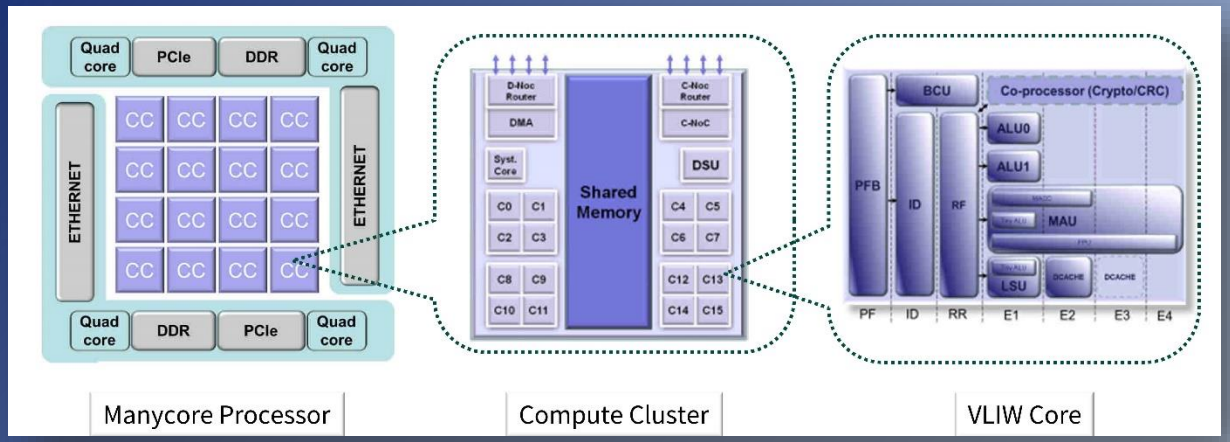
*(**1150 GFLOPS** в разработке)*

Мультиклеточные процессоры на примере **Kalray**





Архитектура Процессора «MPPA® Bostan»



634 GFLOPS за 25Вт. @600МГц

"Гамма"
Искусство безопасности

Измерение на Bostan 288

- Процессор **Bostan 288** - @600Ghz - 25W
- GP – General Purpose (общего назначения, без специальных ускорителей, например, для шифрования)
- Программа без оптимизации

Скорость : 671МБ/с

(после первого анализа коллеги пришли ко мнению, что можно удвоить скорость, не меняя платформу, а только переписав часть модулей (#HighlyLikely))

"Гамма"
Искусство безопасности

Измерение на Bostan 288

Для сравнения :

	Bostan	Core i7-5820K	2*XEON E5	Amlogic 902
	288 Cores	12 Threads	28 Cores	4 cores
Speed (MB/s)	671	160	480	13,1
TDP (W)	25	140	290	10
MB/s/W	**26,84**	1,14	1,66	3,25

"Гамма"
Искусство безопасности

Итоги

- **Мультиклеточные / матричные процессоры**, по нашим измерениям, показали себя как перспективная технология, одновременно в энергетической эффективности и скорости криптографических вычислений

"Гамма"
Искусство безопасности

Специальное спасибо

Поляков А. (НПП «Гамма»):
«armv7» Assembler Ref. Implementation

Фийоль Е. (ESIEA France):
Kalray BOSTAN 288 – Benchmark

Работа выполнена с использованием оборудования Лаборатории электроники **«Байкал»** на базе факультета **ВМК МГУ** имени **М.В. Ломоносова**

"Гамма"
Искусство безопасности

Вопросы?

Овчинников Андрей Игоревич
ФГУП «НПП «ГАММА»
ovchinnikov.ai@nppgamma.ru

Мелешин А. Е.
ФГУП «НПП «ГАММА»
Истомин А. А.
ФГУП «НПП «ГАММА»