ФГУП «НПП «ГАММА»

ENSTA BRETAGNE

ensilos

ПРОЕКТ «АЛЬГИЗ»

О реализации высокоскоростного аппаратного шифратора в HSM (Hardware Security Module) на базе ПЛИС

FILIOL Pierre,
ENSTA Bretagne, France

DELAUNAY Cédric,
ENSTA Bretagne, France

ISTOMIN Alexander Alexandrovich,
"NPP "GAMMA", MSTU Bauman, Russia

FILIOL Eric,
ENSIBS Cybersecurity Department, France, HSE (Russia)

ФИЙОЛЬ Пьер,
ENSTA Bretagne , Франция

ДЕЛОНЕ Седрик,
ENSTA Bretagne , Франция

ИСТОМИН Александр Александрович,
ФГУП «НПП «ГАММА», МГТУ им. Н.Э. Баумана, Россия

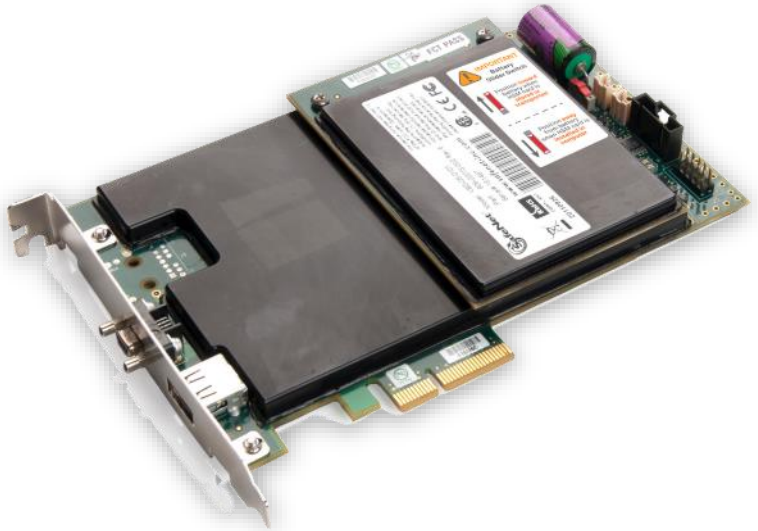
ФИЙОЛЬ Эрик,
ENSIBS Департамент Кибербезопасности, Франция, ВШЭ (Россия)

XXII - RUSCRYPTO 2020
18.03.2020

Объект исследования

- **Аппаратные шифраторы,** в большинстве случаев спроектированы как чистые монолитные системы, где всё, от фактического шифрования/дешифрования до основной обработки, а иногда также и ввод/вывод данных, реализовано в одной конструкции.

Что такое «HSM» ?



- HSM : Hardware Security Module
  Аппаратные модули безопасности

- - это защищенные от взлома аппаратные устройства, которые усиливают методы шифрования, генерируя ключи, шифруя и расшифровывая данные, а также создавая и проверяя цифровые подписи.

PicoEVB и NiteFury

- Проекты на CrowdSupply (Crowdfunding - Платформа)
- PicoEVB и NiteFury - открытые платформы на базе ПЛИС

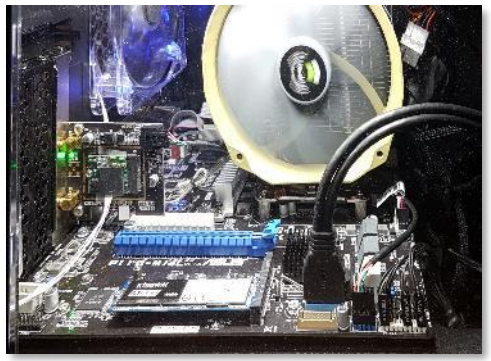
Цель проекта

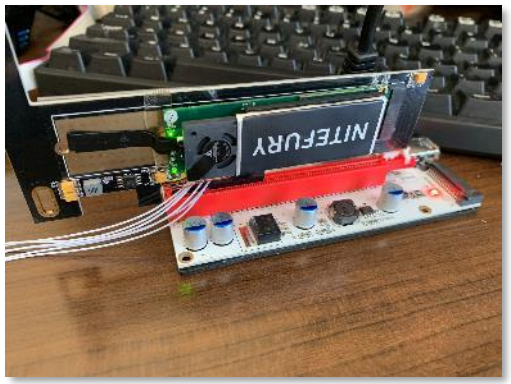
- Проект «АЛЬГИЗ» - не просто очередная реализация ГОСТ Р 34.12-2015 - «Кузнечика» на Платформе ПЛИС -

это исследование возможностей и реализация с наименьшими затратами первоначального прототипа HSM - Аппаратного Модуля Безопасности, оснащенного национальными алгоритмами,

представляет собой решение, которое позволяет использовать существующую аппаратную платформу (Ноутбук, АПМ, Маршрутизатор, ИП-Телефон, …), обеспечивая ей преимущество аппаратного шифрования без вмешательства в перепроектирование самого программно-аппаратного решения.

Примеры



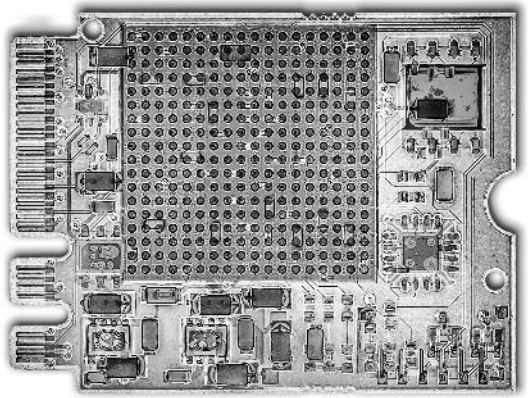


HSM Модуль в маршрутизаторе

HSM Модуль в АПМ / Ноутбуке

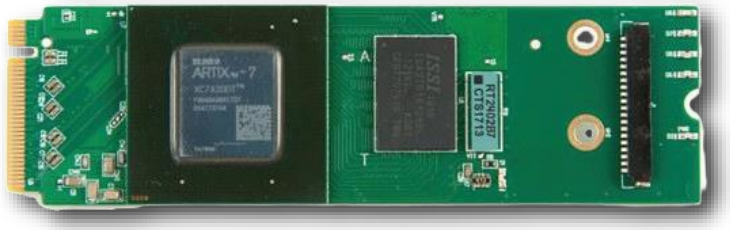
PicoEVB

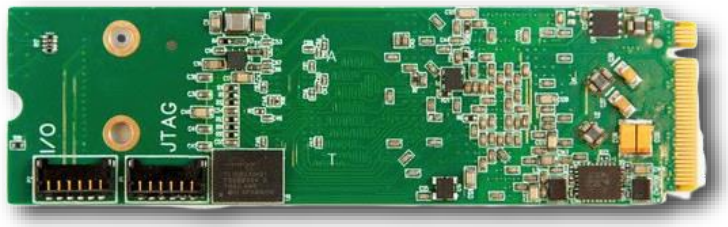
- В продаже с мая 2018
- M.2 2230 A. / E. Key
- **ПЛИС:** Xilinx Artix **XC7A50T** - 2CSG325C
- JTAG (Через FDTI), GPIOs, LEDs
- **PCIe Gen.2 x1 = 4 Gigabit/s max**
- Open – Source Hardware **= Конструкторские источники для этой платы в открытом доступе**
- ≈250$



NiteFury

- В продаже с октября 2019
- M.2 2280 M.Key
- **ПЛИС:** Xilinx Artix **XC7A200T** - 2FBG484E Speed Grade -3
- JTAG, GPIOs, LEDs
- **PCIe Gen.2 x4 = 16 Gigabit/s max**
- 4 GB DDR3
- Open – Source Hardware = **Конструкторские источники для этой платы в открытом доступе**
- ≈360$

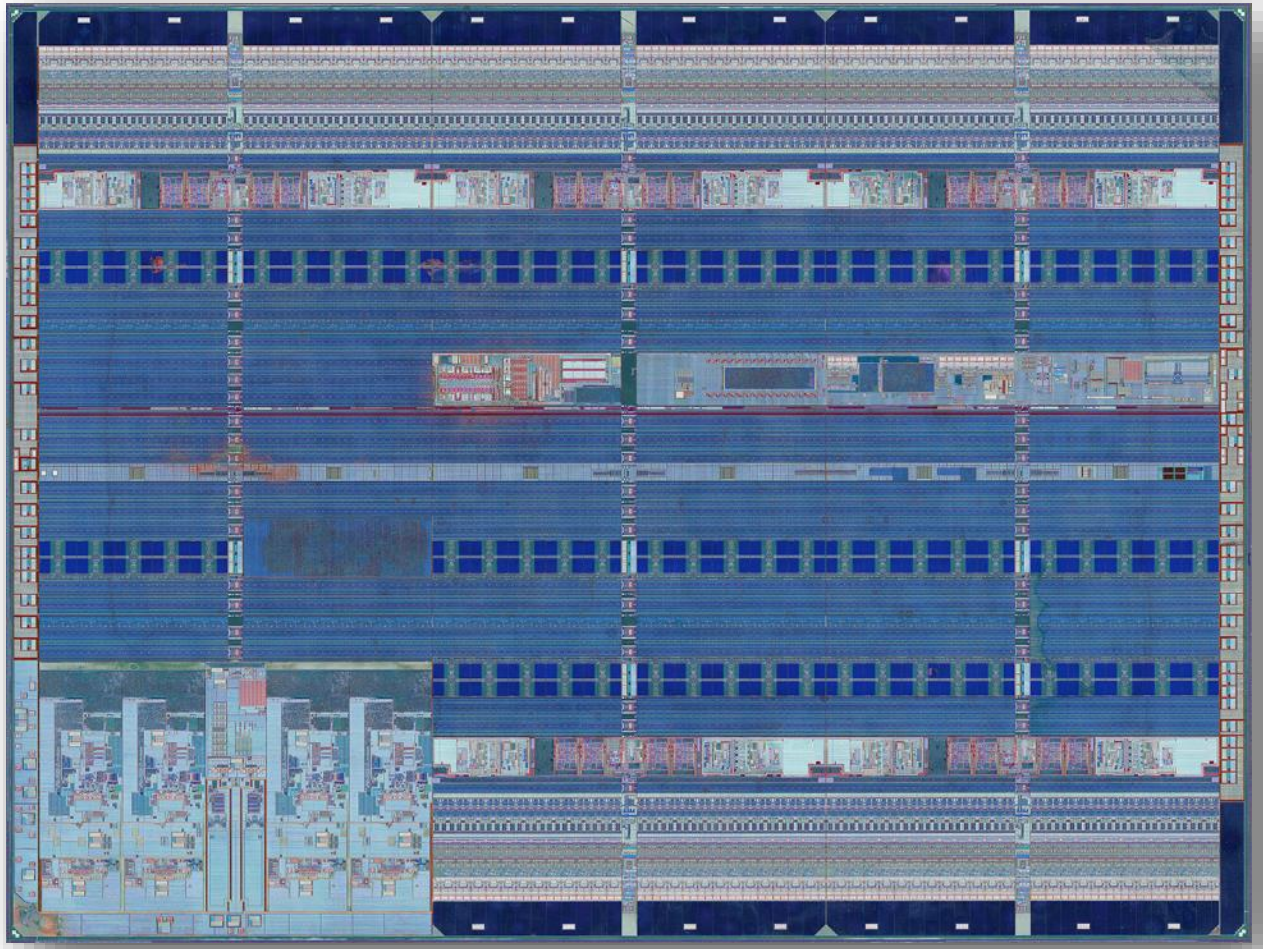




ПЛИС : XILINX Artix 7

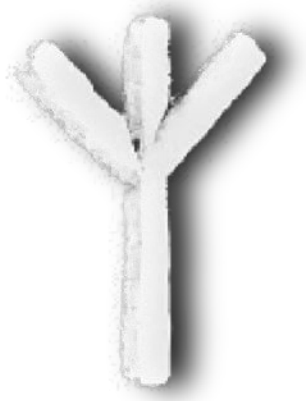
- **Artix 7 50T:**
  52K Logic Cells
  2.7Kb BRAM
  PCIe Gen2

- **Artix 7 200T:**
  215K Logic Cells
  13.1Kb BRAM
  PCIe Gen2



Почему «Альгиз» ?

- Альгиз – это одна из рун **Алфавита Викингов**



- **Она обозначает**

ЗАЩИТУ и БЕЗОПАСНОСТЬ

Краткая история проекта

- **Первая часть** (Седрик Д., Эрик Ф., Александр И.):
  - Модули PicoEVB
  - РусКрипто 2019
  - Дипломная Работа Седрика Д.
  - … «Геополитика»

- **Вторая часть** (Пьер Ф., Александр И., Эрик Ф.):
  - Модули NiteFury
  - Пьер пишет свою версию
  - Битва с **«ННД»**
  - РусКрипто 2020 ←
  - …

Н.Н.Д.

- **Нет Никакой Документации !**

- Описание модулей на сайте разработчика представлено с ошибками

- NiteFury вообще не задокументирован. Много ложных или противоречивых данных в GitHub
- Нет примеров из Интернет сети (тем более, что найдено несколько примеров для более старых версий, которые изменились).
- Нелегко получить помощь в Интернете (ни у кого нет информации, никто не отвечает на запросы).
- Отсутствие вариантов аппаратной реализации коммуникаций с HSM-модулем, доступных в интернете, где возможна реализация отдельного сопроцессора.

Архитектура Шифратора «АЛЬГИЗ»

ПРОЕКТ «АЛЬГИЗ» - О реализации высокоскоростного аппаратного шифратора в HSM на базе ПЛИС

18.03.2020

Модули

- **Модуль Шифрования**

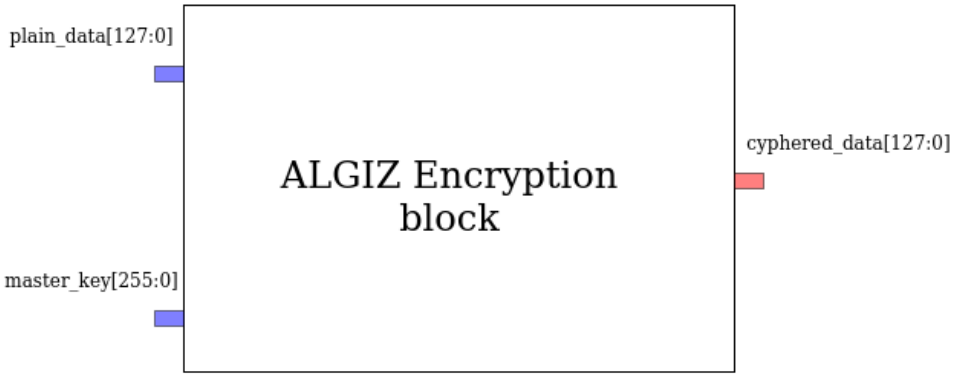
  - **ГОСТ Р 34.12-2015 -** «Кузнечик»
  - Режим простой замены с зацеплением – **«Cipher Block Chaining - CBC»**

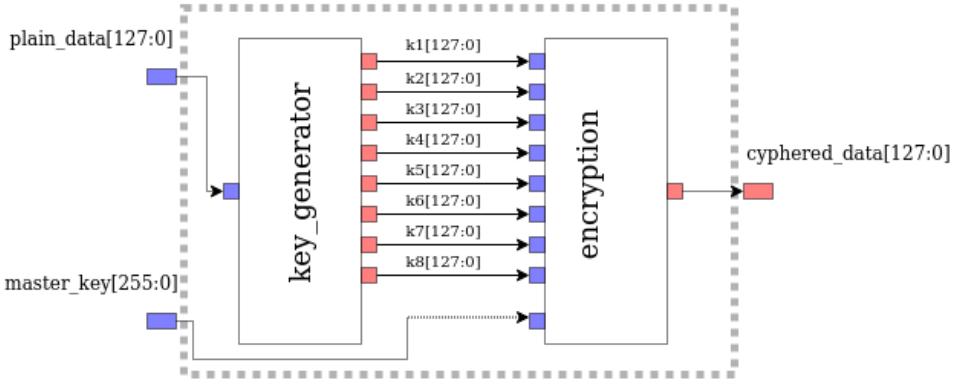
- **Модуль Коммуникации**

  - Вариант 1: **«Memory-Mapping»**
  - Вариант 2: **«Streaming»**

Модуль Шифрования 1/6

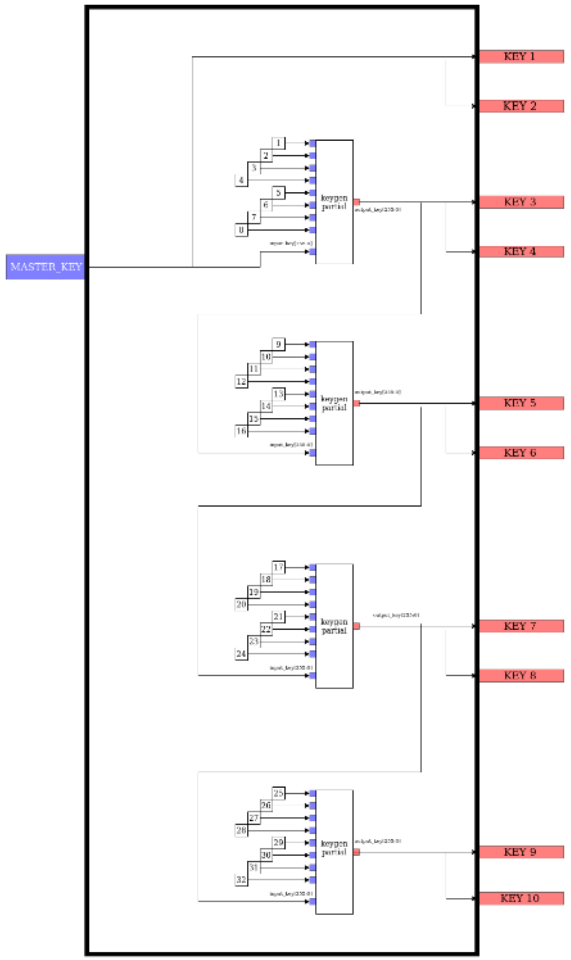
Верхний уровень

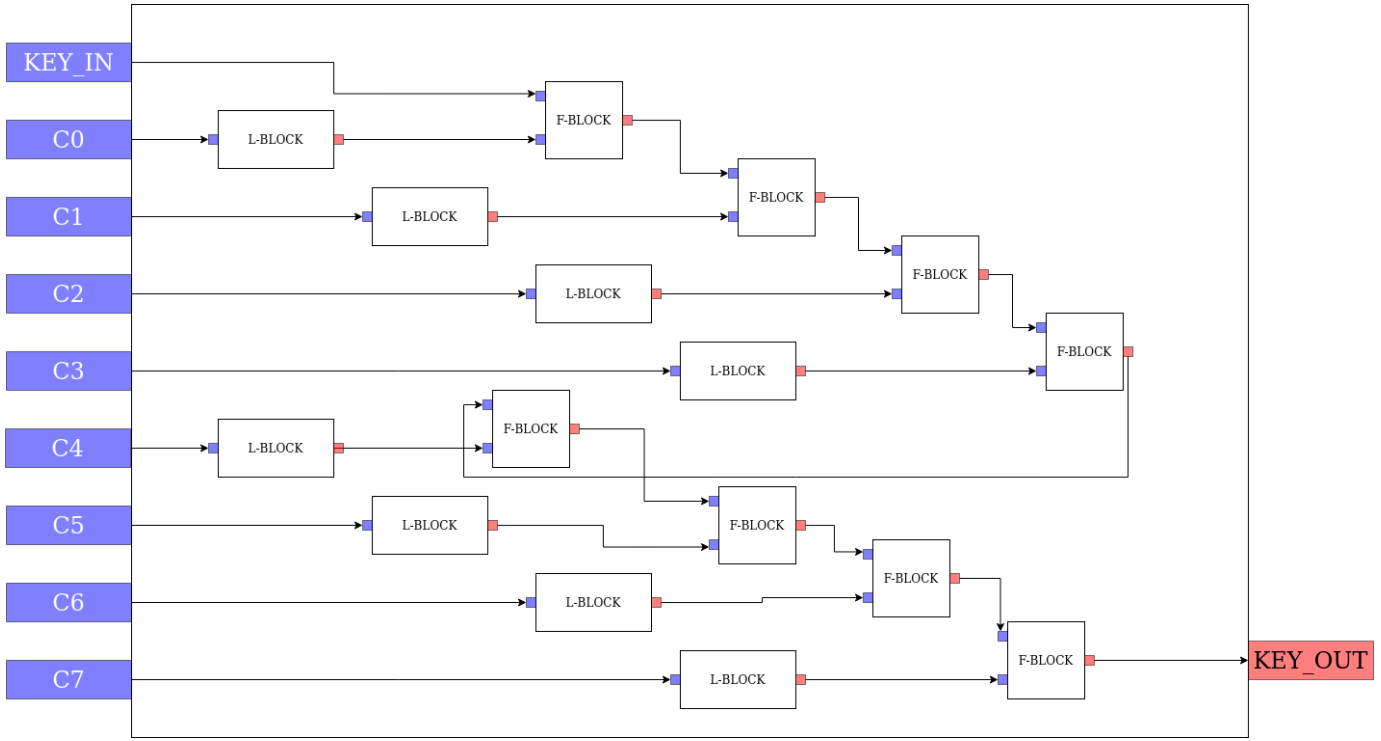




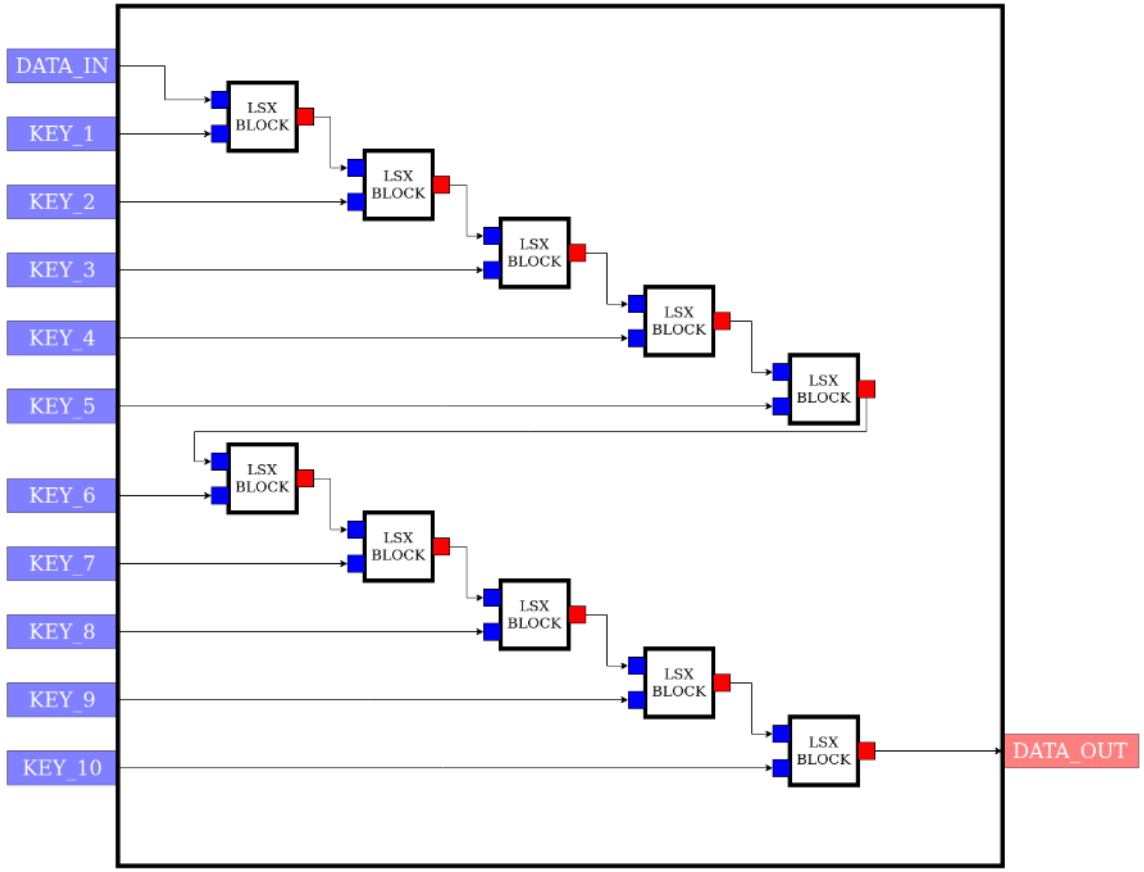
Модуль Шифрования 2/6

Блоки развёртывания ключа



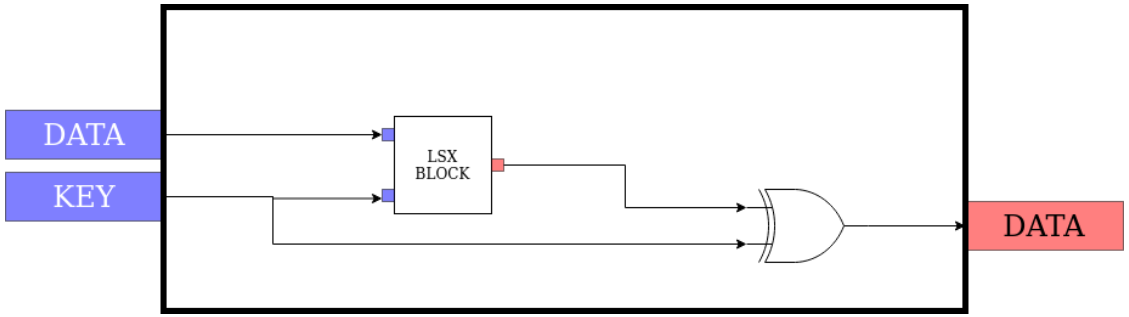


Модуль Шифрования 3/6

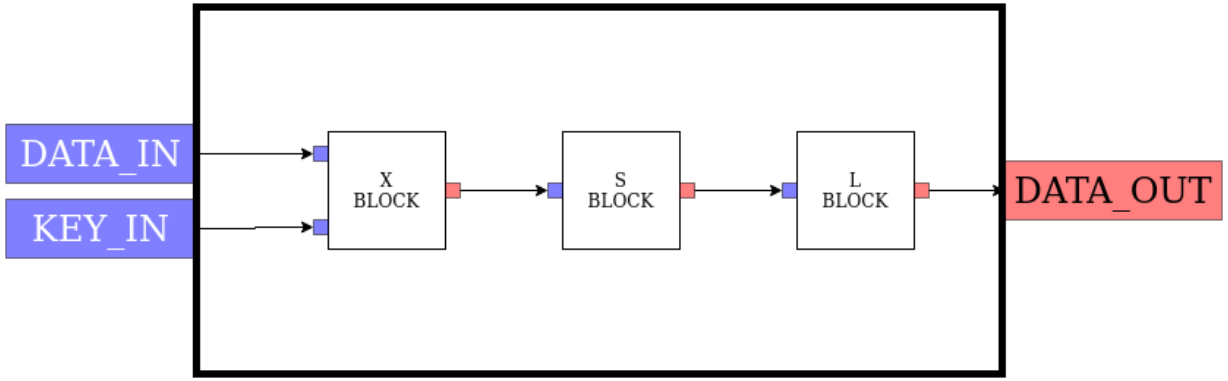


“Шифровальный”-Блок

Модуль Шифрования 4/6

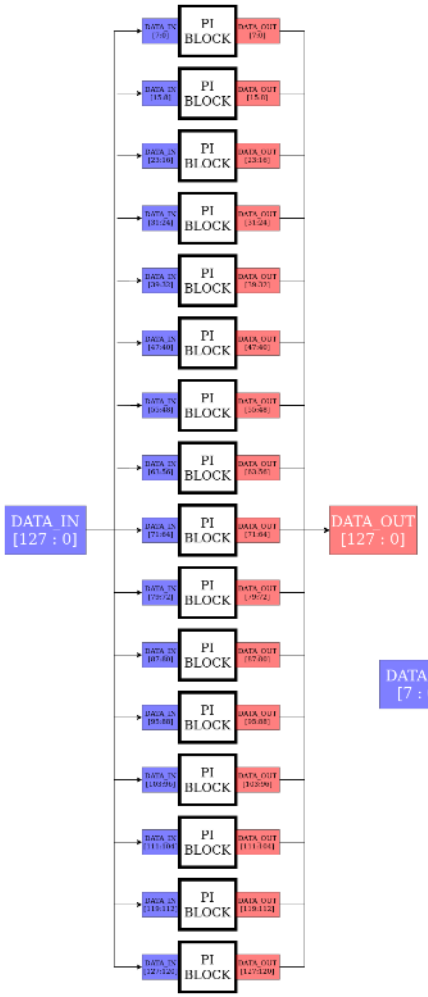


“F”-Блок

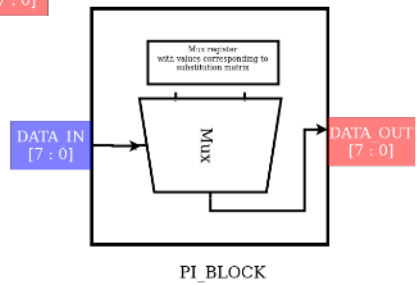


“LSX”-Блок

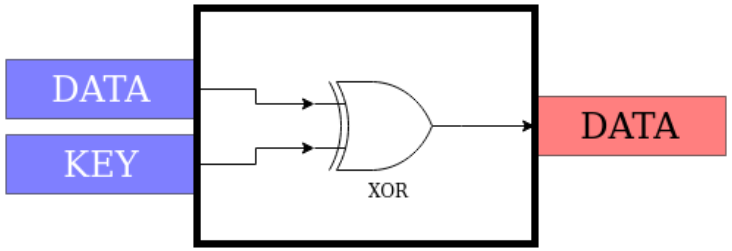
Модуль Шифрования 5/6



“S”-Блок

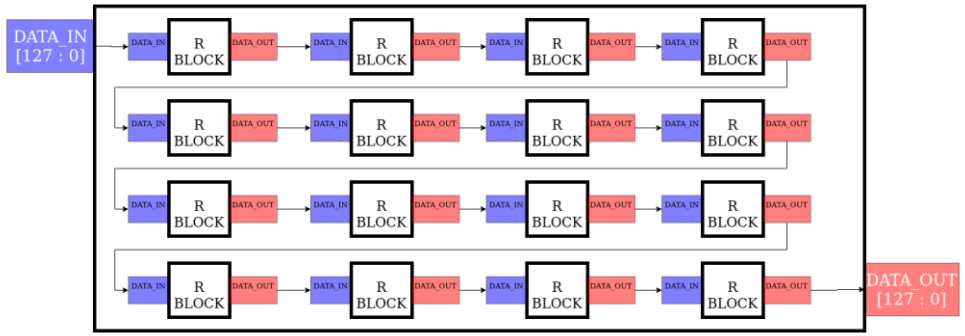


“PI”-Блок

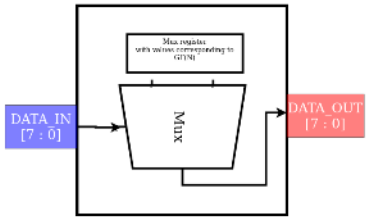


“X”-Блок

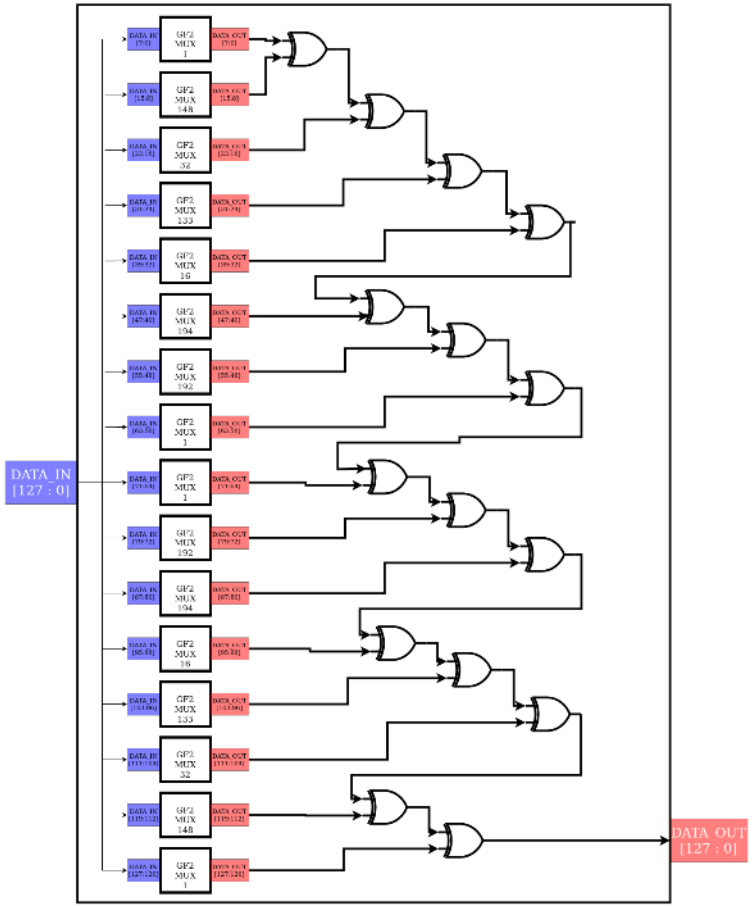
Модуль Шифрования 6/6



“L”-Блок

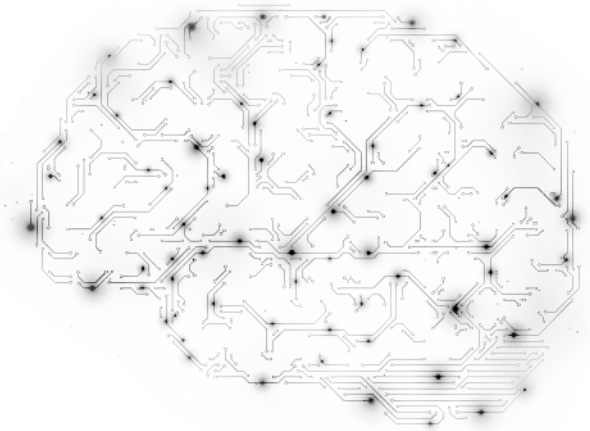


GF2_MUX_N



“R”-Блок

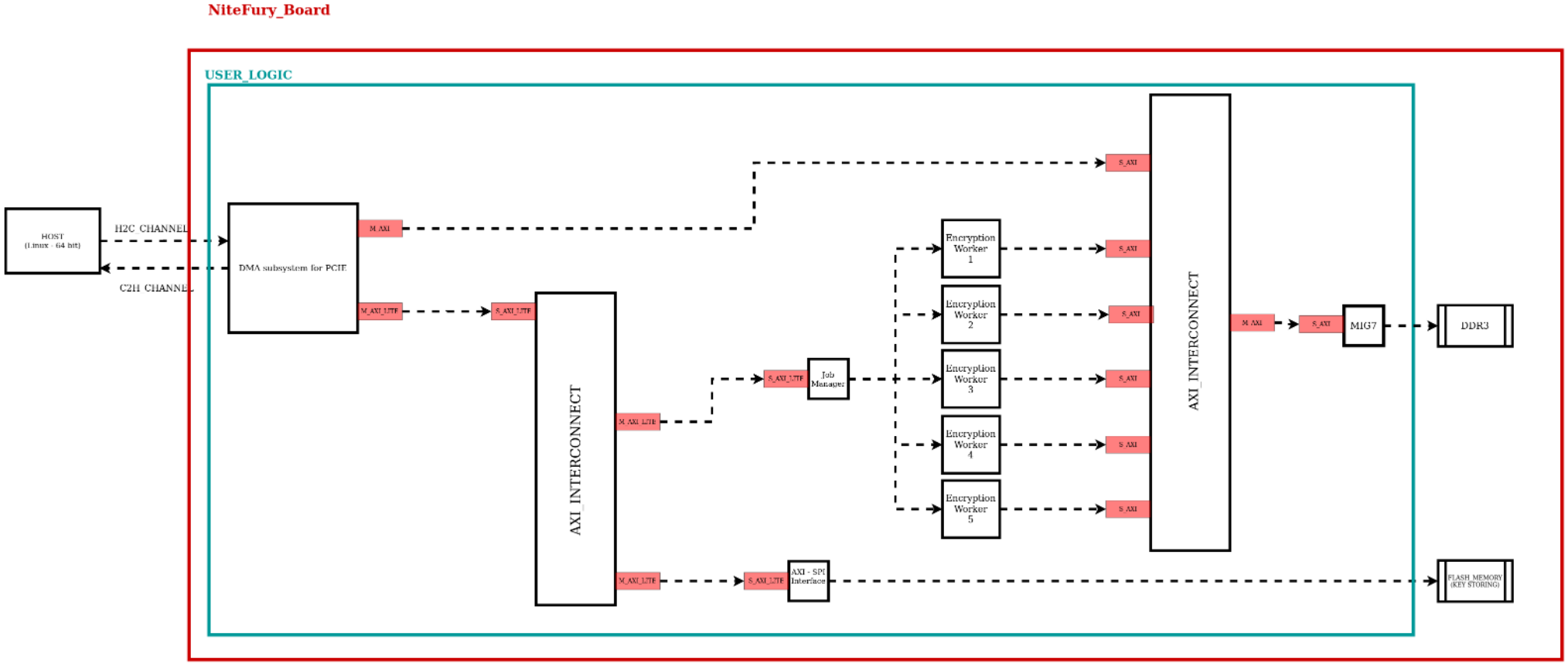
Решения коммуникации с модулем



- Метод 1
  - **“Memory - Mapping”**
- Метод 2
  - **“Streaming”**

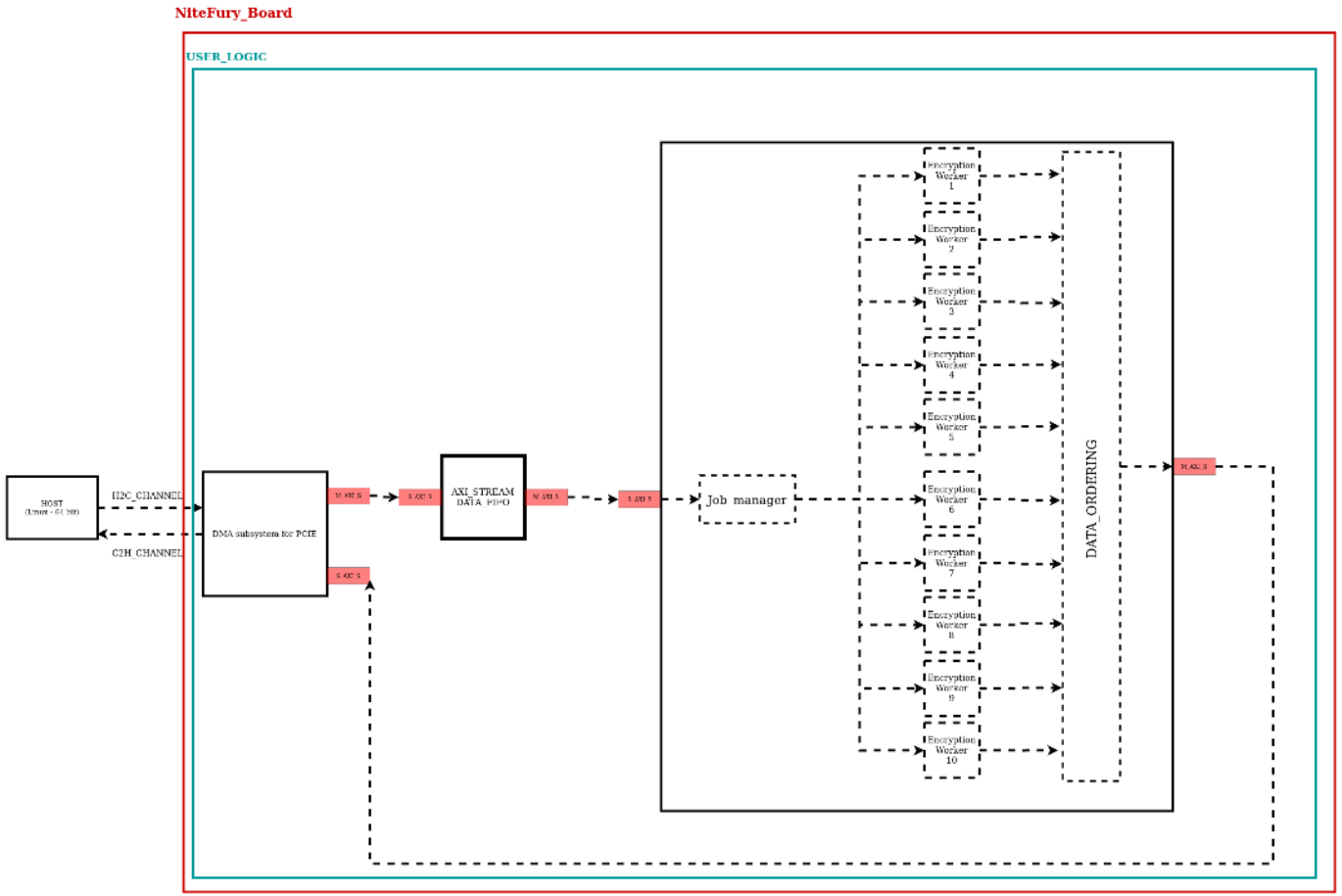
Метод 1: “Memory - Mapping”

- “Memory - Mapping” : Отображение Памяти DDR3 в пространстве адресов AXI



Метод 2: “Streaming”

- “Streaming” : Отправка данных потоком на модуль шифрования и обратно к ОС в обход памяти DDR3 (Метод «PicoEVB»)



Производительность

и сравнение с другими реализациями на ПЛИС ГОСТ 34.12-2015

Использованные Ресурсы

- 1. Метод отображения памяти

Site Type	Used	Fixed	Available	Util%
Slice LUTs	23361	0	133800	17.46
LUT as Logic	20601	0	133800	15.40
LUT as Memory	2760	0	46200	5.97
LUT as Distributed RAM	2589	0		
LUT as Shift Register	171	0		
Slice Registers	24564	0	267600	9.18
Register as Flip Flop	24564	0	267600	9.18
Register as Latch	0	0	267600	0.00
F7 Muxes	193	0	66900	0.29
F8 Muxes	11	0	33450	0.03

- 2. Метод потока

Site Type	Used	Fixed	Available	Util%
Slice LUTs	14274	0	133800	10.67
LUT as Logic	12807	0	133800	9.57
LUT as Memory	1467	0	46200	3.18
LUT as Distributed RAM	1435	0		
LUT as Shift Register	32	0		
Slice Registers	15673	0	267600	5.86
Register as Flip Flop	15673	0	267600	5.86
Register as Latch	0	0	267600	0.00
F7 Muxes	154	0	66900	0.23
F8 Muxes	13	0	33450	0.04

Использованные Ресурсы

- Шифрование

Site Type	Used	Fixed	Available	Util%
Slice LUTs	15461	0	133800	11.56
LUT as Logic	15461	0	133800	11.56
LUT as Memory	0	0	46200	0.00
Slice Registers	64	0	267600	0.02
Register as Flip Flop	64	0	267600	0.02
Register as Latch	0	0	267600	0.00
F7 Muxes	0	0	66900	0.00
F8 Muxes	0	0	33450	0.00

Скорость на NiteFury

«Кузнечик» - Режим простой замены с зацеплением (CBC)
Без оптимизации

Такт Шифратора	5 МГц
Количество необходимых циклов	1
Время шифрования 128 бит	200 ns
Скорость шифрования одного «процесса»	**608 Mbit/s = 76MB/s**
Максимальное число шифровальных единиц	6 (Memory Management) 7 (Stream)
Максимальная общая скорость шифрования	3.6GBit/s = 456MB/s (MM) **4.3GBit/s = 532MB/s (Stream)**

Скорость на NiteFury

- **Оптимизации по скорости будут предприниматься только тогда, когда:**
  - Будет решена проблема с коммуникацией модуля HSM с ОС, и будет выбран оптимальный метод для HSM -Аппаратного Модуля Безопасности
  - Будет фиксирован Режим Шифрования

- → <u>Выбор оптимизации зависит от доступного места на ПЛИСе</u>

Другие имплементации на ПЛИС

И. И. Калистру, М. А. Бородин, А. С. Рыбкин, Р. А. Гладько
Способы реализации алгоритма «Кузнечик» на программируемых логических интегральных схемах (2018)

- Режим гаммирования с конвейеризации (36 x)
  – 400МГц на XILINX Kintex (Прототип на Virtex Ultrascale +)
- **51.2GBit/s (6.4 GB /s)**

Овчинников@RusCrypto 2017

- **ALTERA Cyclone IV серии EP4CE6E22C8**
- Режим гаммирования
- **560MBit/s – 3.5GBit/s (70MB/s - 432MB/s)**

Другие имплементации на ПЛИС

Корешкова Александра Алексеевна

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ БЫСТРОДЕЙСТВУЮЩЕГО КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ (2016)

Режим гаммирования

- XILINX Artix 100T
- 168.3MBit/s – 1.4GBit/s (21.0MB/s – 181.4MB/s)

Выводы и следующие Шаги

Выводы и следующие Шаги

- Для полного аппаратного модуля безопасности HSM нужно реализовать:
  - Систему обмена ключей
  - Систему безопасного хранения ключей
  - Генератор случайных чисел
  - Защиту ПЭМИН, НСД,…

- Перепроектирование модулей PicoEVB + NiteFury
  - Память убрать ?
  - Сильнее ПЛИС на PicoEVB
  - …

Вопросы ?

Спасибо за внимание

- **ФИЙОЛЬ Пьер,**
  ENSTA Bretagne , Франция
  pierre.filiol@ensta-bretagne.org
- **ДЕЛОНЕ Седрик,**
  ENSTA Bretagne , Франция
  cedric.delaunay@ensta-bretagne.org
- **ИСТОМИН Александр Александрович (* Главный контакт)**
  ФГУП «НПП «ГАММА», МГТУ им. Н.Э. Баумана, Россия
  istomin.a@nppgamma.ru
- **ФИЙОЛЬ Эрик,**
  ENSIBS Департамент Кибербезопасности, Франция, ВШЭ (Россия)
  eric.filiol@univ-ubs.fr