"Гамма"
Искусство безопасности

МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ И ТОРГОВЛИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ «НАУЧНО-ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ

«Гамма»

"Гамма"
Искусство безопасности

О подходах к испытаниям высокоскоростных СКЗИ (Оптимизация исследований)

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

Цели и задачи исследования

- Цель:
  - Создание стенда для функциональных испытаний высокоскоростных СКЗИ
- Задачи:
  - Создать макет стенда для функциональных испытаний высокоскоростных СКЗИ
  - Реализовать алгоритмы шифрования ГОСТ Р 34.12–2015
  - Оценить скоростные характеристики

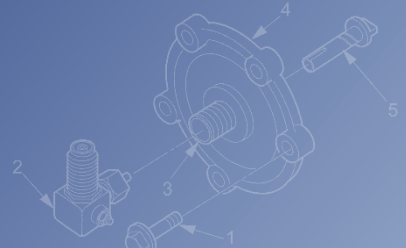
"Гамма"
Искусство безопасности

Аппаратные СКЗИ

- USB <->USB
- PCIe <-> Ethernet, USB, SATA
- и другие различные комбинации интерфейсов

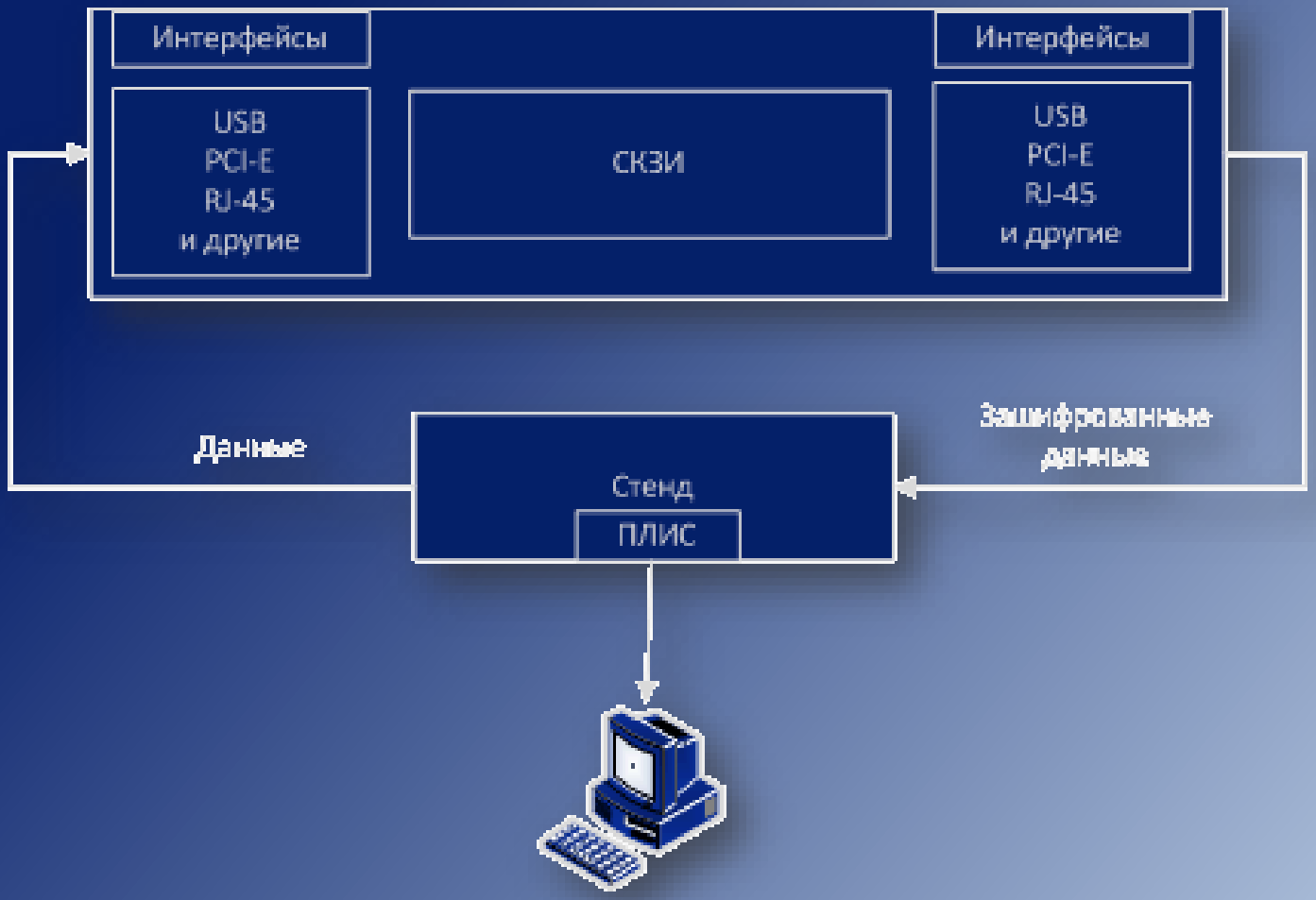
Пути исследования

- Программные средства
  - Недостатки:
    - Небольшая скорость
    - Большая стоимость стенда
- Аппаратные средства
  - Достоинства:
    - Большее доверие к стенду



"Гамма"
Искусство безопасности

Схема стенда для проведения испытаний



Исследования скоростных характеристик

- **Д.Б. Фомин**, «Реализация блочного шифра типа XSL с MDS-матрицей линейного преобразования на **NVIDIA CUDA**», Математические вопросы криптографии, 2015

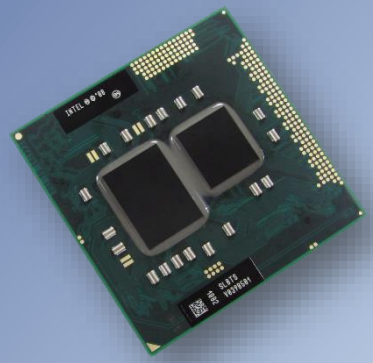
- **Е. А. Ищукова , Р. А. Кошуцкий , Л. К. Бабенко,** «Разработка и реализация высокоскоростного шифрования данных с использованием алгоритма кузнечик», 2015

"Гамма"
Искусство безопасности

Результаты предыдущих исследований

- GTX Titan - **5 518 МБ/с**

- GT 640 – **887 МБ/с**
- GT 610 – **202 МБ/с**



- Intel® Core™ i5 CPU M 480 2.67GHz - 54 МБ/с
- Intel® Xeon E5-1620 v4 – **498 МБ/с**

"Гамма"
Искусство безопасности

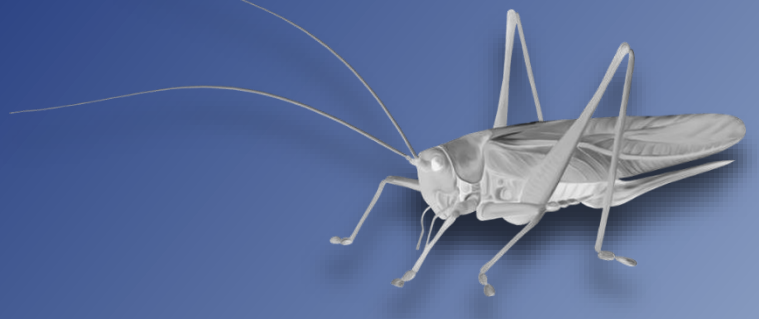
Результаты скоростных характеристик алгоритмов шифрования на ПЛИС

Характеристики Алгоритма	*Алгоритмы*			
	AES (подстановочно-перестановочная сеть)	**DES** (сеть Фейстеля)	**ГОСТ 28147-89** (сеть Фейстеля)	**IDEA** (модификация сети Фейстеля)
Тип шифрования	**Симметричный, блочный**			
Длина блока, (бит)	128	64	64	64
Число раундов	10	16	32	8
Размер ключа, (бит)	256	56	256	128
Кристалл ПЛИС	Xilinx Virtex 5	Xilinx Virtex – E	Altera Arria II GX EP2AGX125	Xilinx XC4000
Частота	347,6 МГц	19,4 МГц	125 МГц	33 МГц
Скорость	**44,5 Гб/с**	**4,25 Гб/с**	**748 Мб/с**	**528 Мб/с**

ПЛИС, использованный для отладки

FPGA ALTERA Cyclone IV серии EP4CE6E22C8

Простая реализация ГОСТ Р 34.12-2015

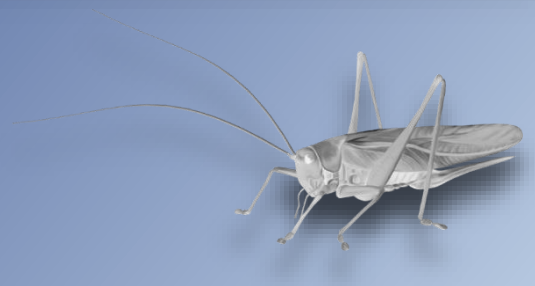


- Особенности:
  - Низкая скорость (порядка 70МБ/с)
  - Среднее количество занимаемой памяти (55%)
  - Небольшие трудозатраты на разработку

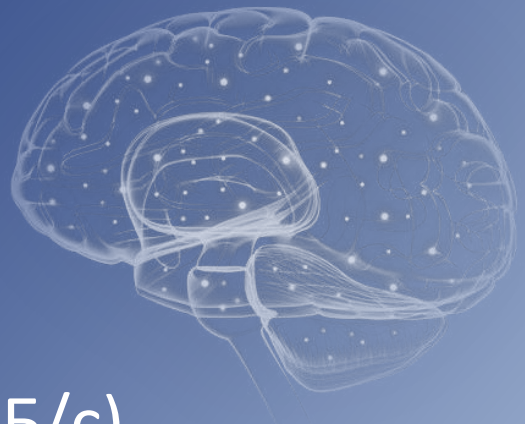
"Гамма"
Искусство безопасности

Занимаемая память

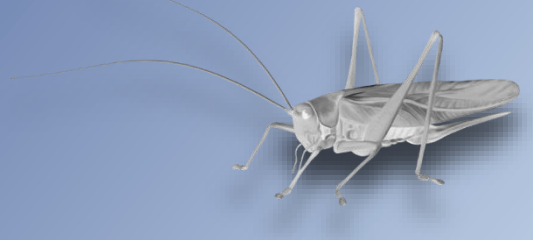
	Compilation Hierarchy Node	LC Combinationals	LC Registers	Memory Bits
1	|serialGPIO	3432 (131)	3679 (43)	61440
1	▷ |async_receiver:RX|	39 (18)	34 (13)	0
2	▷ |async_transmitter:TX|	44 (23)	33 (12)	0
3	◢ |block:b|	3218 (1226)	3569 (1688)	61440
1	|X:r10|	128 (128)	128 (128)	0
2	▷ |expand_key:k_next|	1527 (352)	1369 (553)	28672
3	◢ |round:r2|	337 (0)	384 (0)	32768
1	▷ |L:l1|	209 (123)	256 (256)	0
2	▷ |S:s|	0 (0)	0 (0)	32768
3	|X:x|	128 (128)	128 (128)	0



Оптимизация по памяти

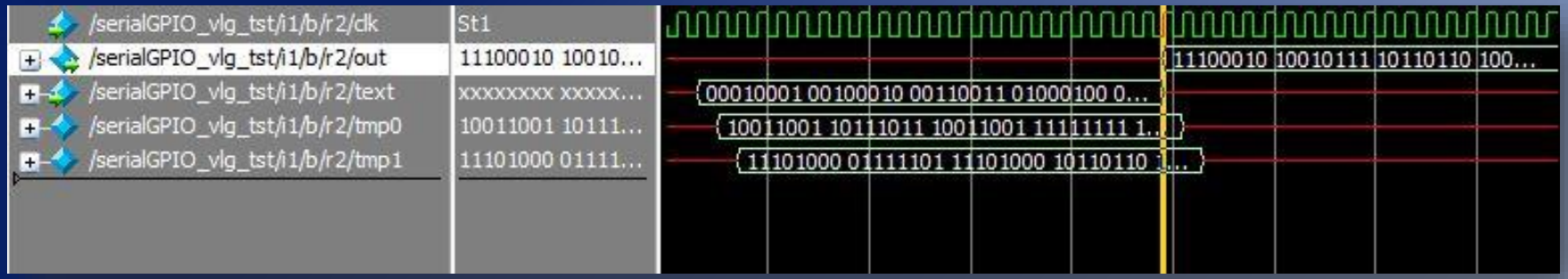


- Особенности
  - Низкая скорость (порядка 70МБ/с)
  - Минимальное количество занимаемой памяти (порядка 1500 логических элементов) (=24%)

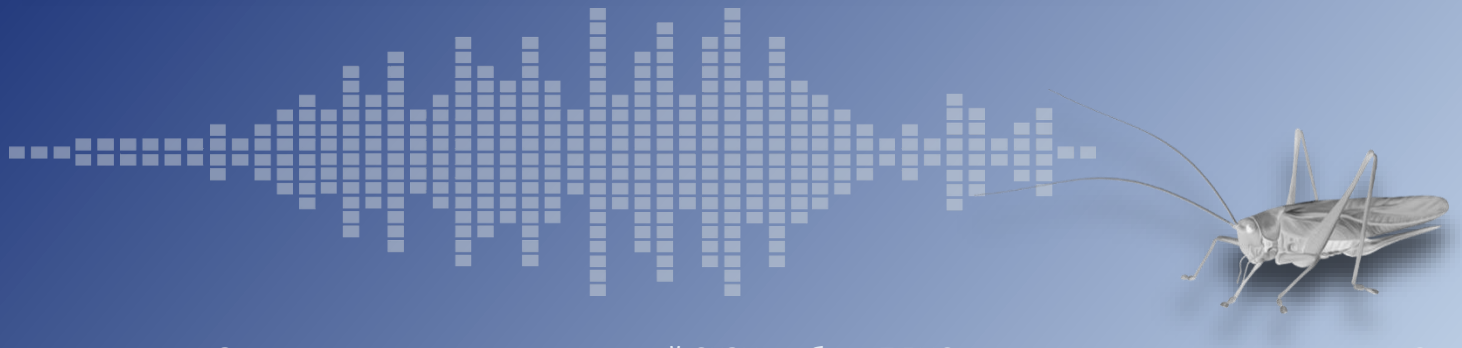


"Гамма"
Искусство безопасности

Частотные характеристики



	Fmax	Restricted Fmax	Clock Name	Note
1	131.6 MHz	131.6 MHz	clk	
2	248.69 MHz	248.69 MHz	block:b|clk_vn	



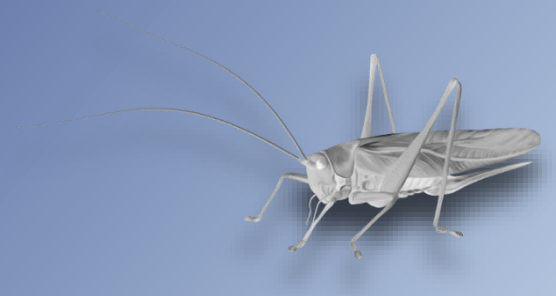
Оптимизация по скорости

- Особенности
  - Высокая скорость
  - Максимальное количество занимаемой памяти – 64Кбайта
  - Хранение MDS-матрицы

"Гамма"
Искусство безопасности

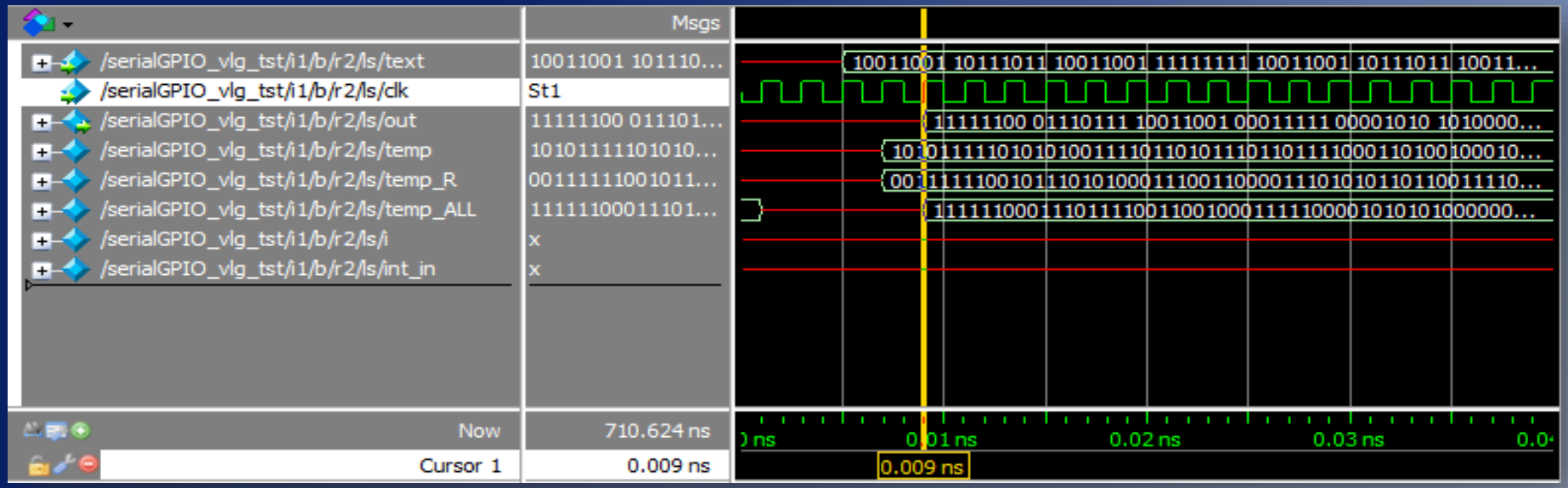
Занимаемая память

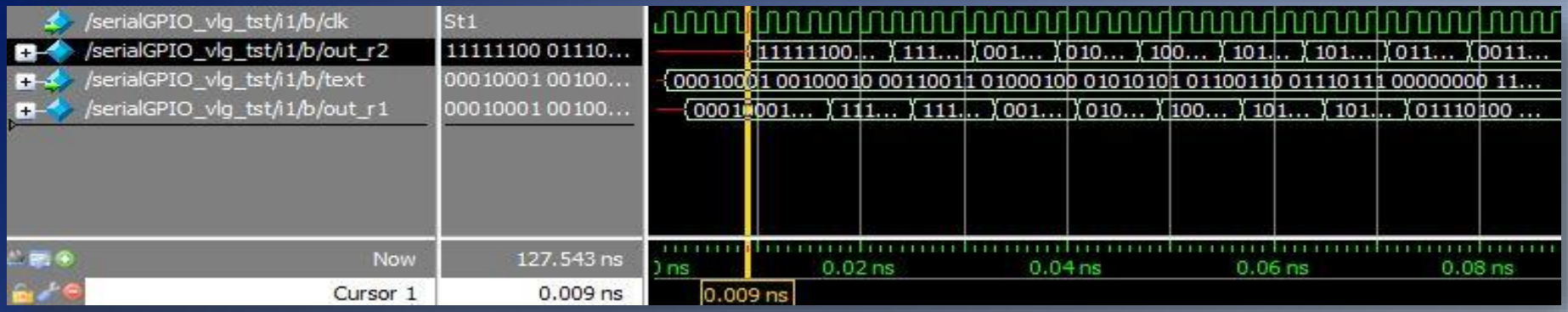
Total logic elements	1,615
Total combinational functions	1,423
Dedicated logic registers	860
Total registers	860
Total pins	20
Total virtual pins	0
Total memory bits	524,288
Embedded Multiplier 9-bit elements	0



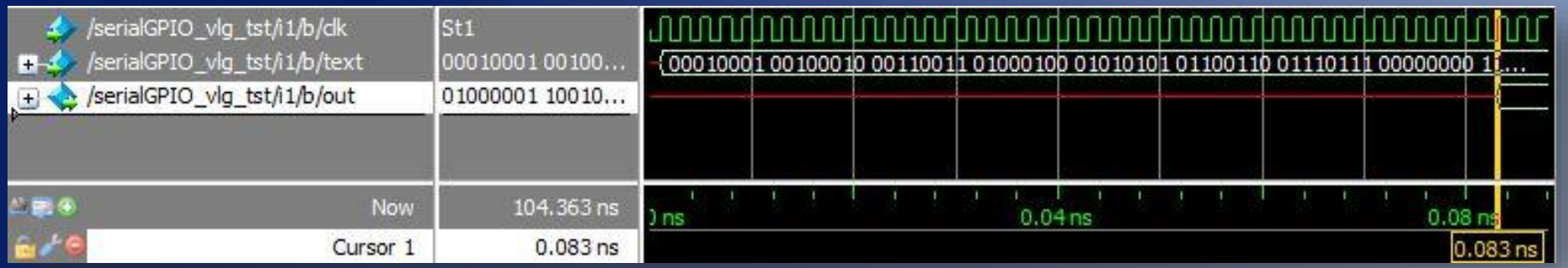
"Гамма"
Искусство безопасности

Частотные характеристики





Частотные характеристики



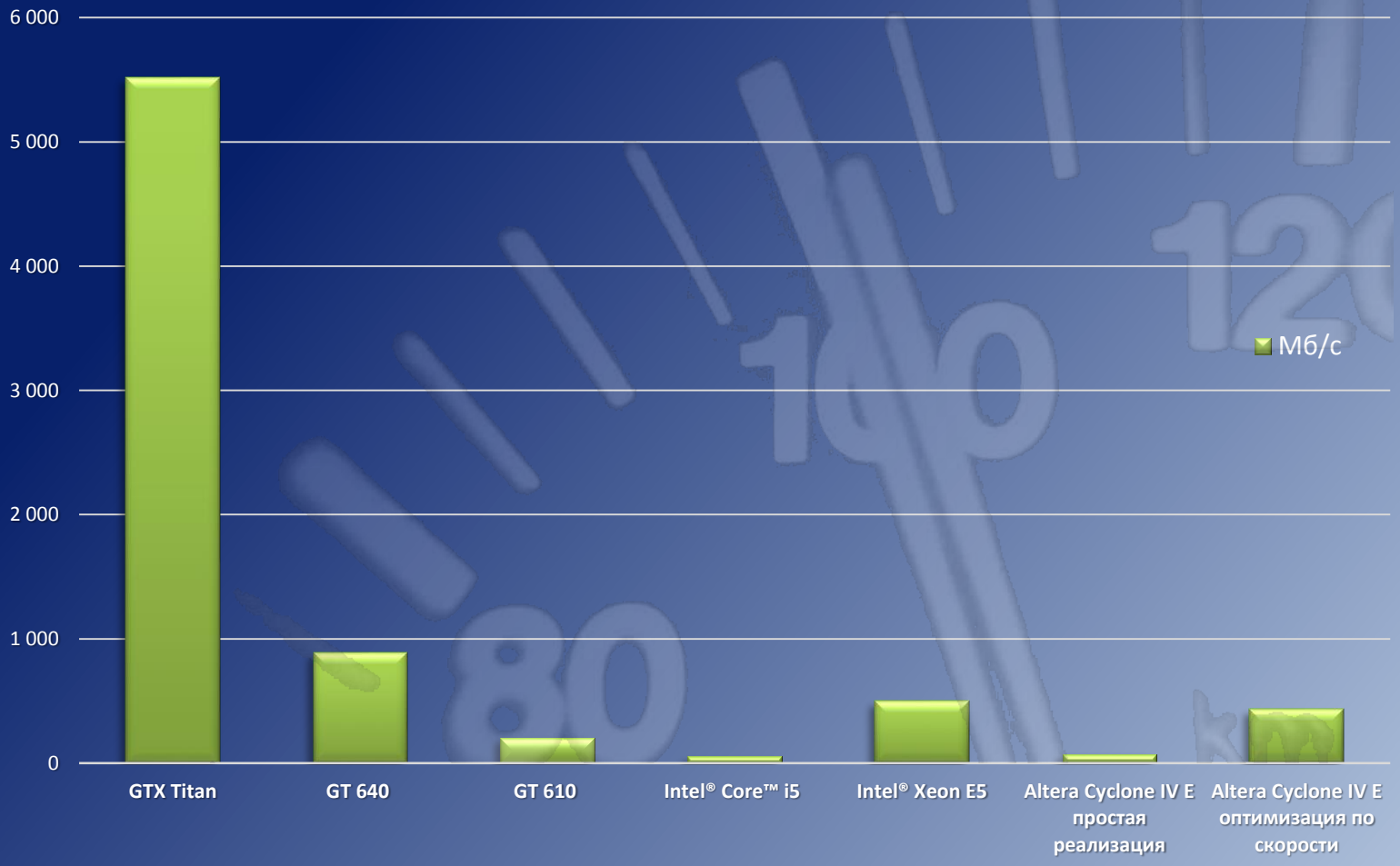
	Fmax	Restricted Fmax	Clock Name	Note
1	156.74 MHz	156.74 MHz	clk	
2	292.91 MHz	292.91 MHz	block:b|clk_vn	

Результаты исследования скоростных характеристик

- Максимальная полученная скорость шифрования - **432Мб/с**

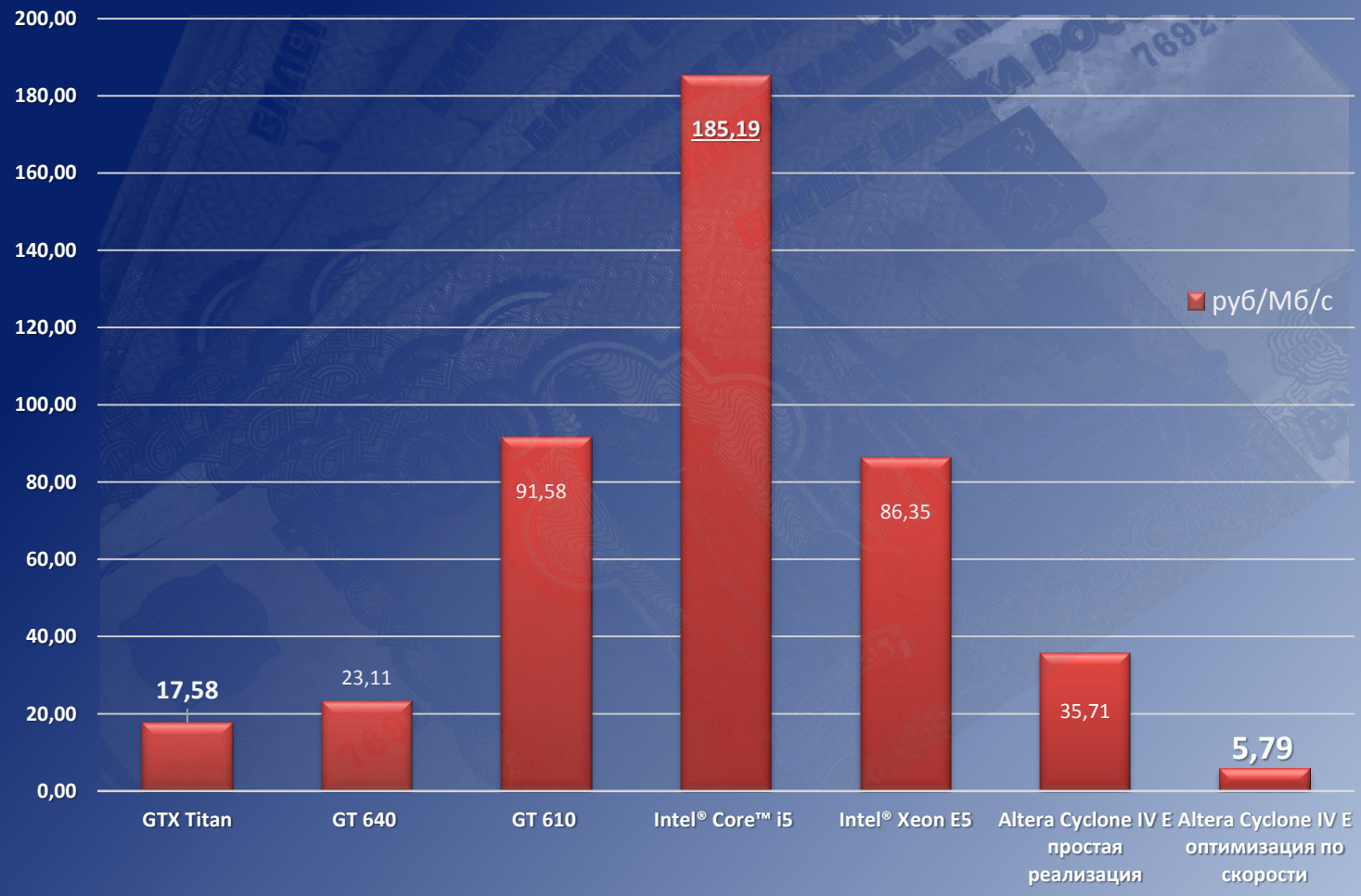
"Гамма"
Искусство безопасности

Скоростные характеристики



"Гамма"
Искусство безопасности

Денежные затраты



"Гамма"
Искусство безопасности

Результаты

- Создан стенд для функциональных испытаний высокоскоростных **СКЗИ**
- Увеличена достоверность результатов исследования
- Проведен сравнительный анализ различных вариантов реализации алгоритма шифрования **«Кузнечик»**
- Получен опыт разработки и собраны рекомендации шифраторов на **ПЛИС**
- Уменьшены трудозатраты на испытания СКЗИ до 20%

"Гамма"
Искусство безопасности

Спасибо за внимание!

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