Аппаратная реализация ГОСТ 28147-89 для прозрачного шифрования потоков данных

конференция
РусКрипто'2013

•http://www.ruscrypto.ru/conference/

Шарамок Александр Владимирович
начальник отдела разработки средств связи

ООО Фирма «АНКАД»

Содержание доклада

1 Основные методы оптимизации (повышения) быстродействия алгоритма;

2 Возможные преимущества аппаратной реализации;

3 Эволюция реализации алгоритма в аппаратуре ООО Фирма «АНКАД»;

4 Достигнутые характеристики по быстродействию.

Основные методы оптимизации

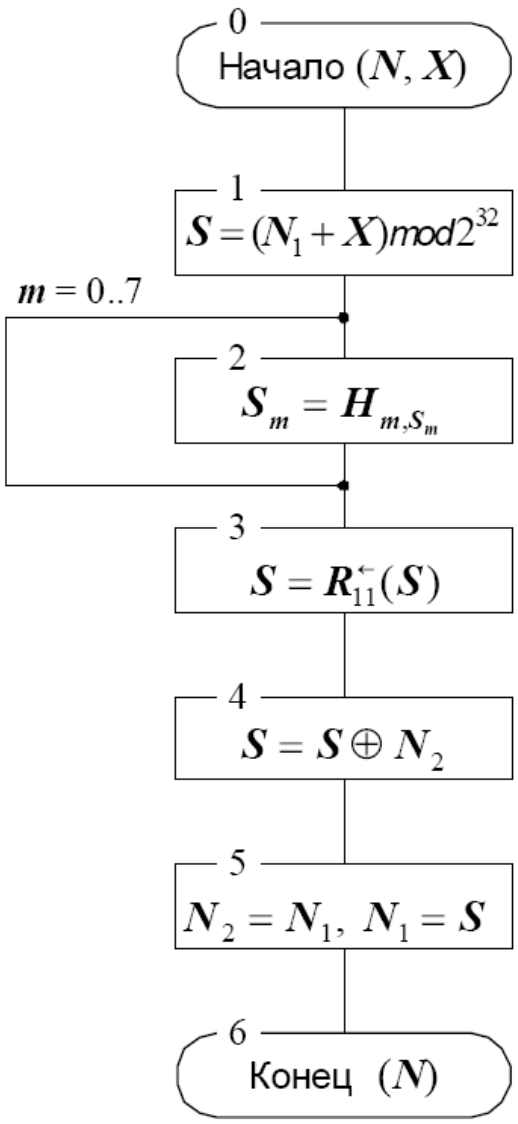
Основные методы оптимизации изложены в статье Винокурова А. ГОСТ, не прост, а очень прост. Журнал «Монитор», № 1, 5, 1995 г. (расширенный вариант статьи «Алгоритм шифрования ГОСТ 28147-89, его использование и реализация для компьютеров платформы Intel x86» на сайте Винокурова А.).

Основные методы оптимизации быстродействия:

- ГОСТ 28147-89 по своей сути вычислимая функция, её или её отдельные элементы можно представить таблично;

- преобразование циклических структур в линейные повышает быстродействие.

Оптимизация простой замены



1. Избавление от циклов:

а) в табличном преобразовании 4-х битовых блоков;

б) в общей 32-х раундовой структуре алгоритма;

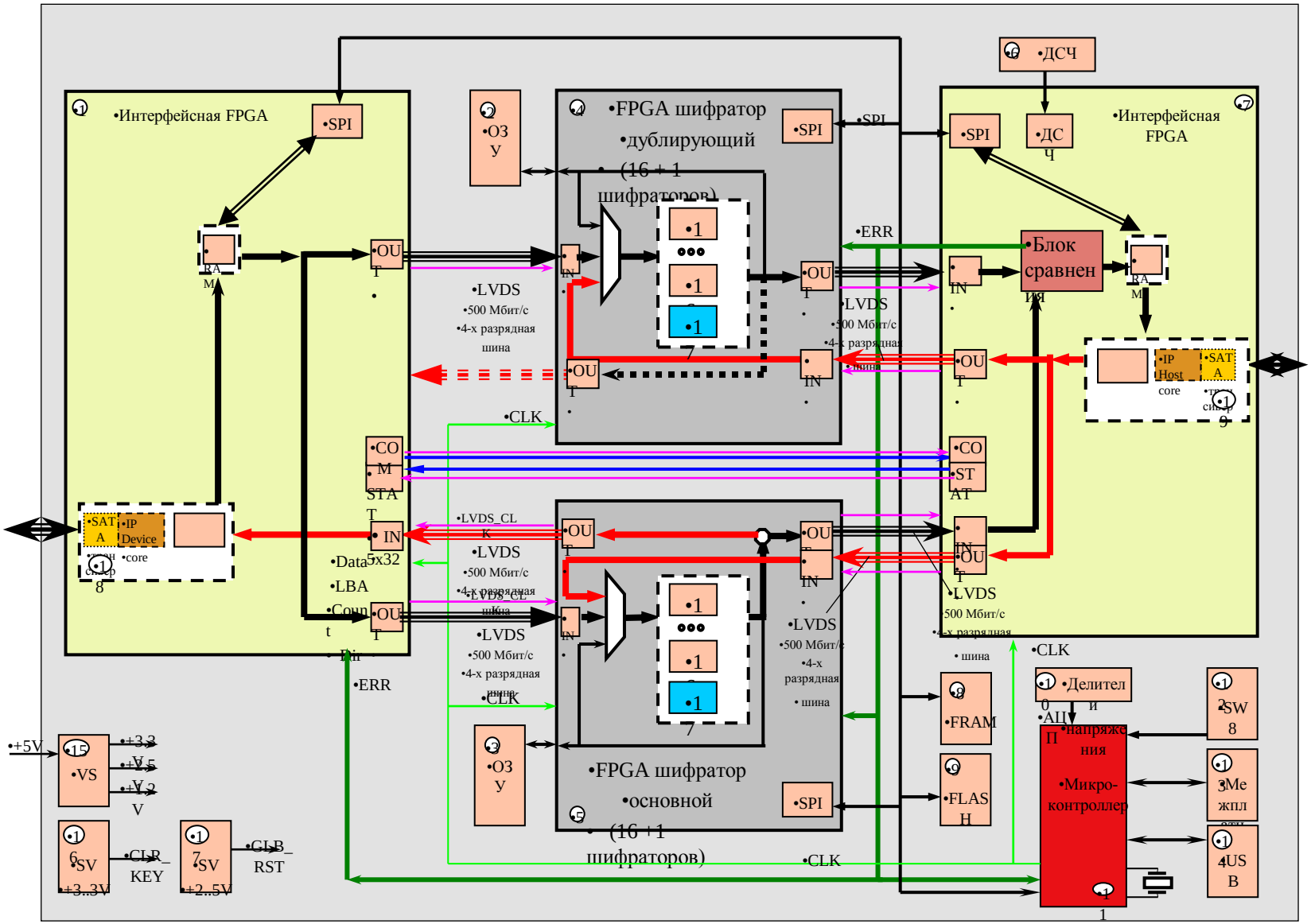
2. Реализация табличных преобразований:

а) в табличном преобразовании 4-х битовых блоков;

б) объединение в единое табличное преобразование преобразования 4-х битовых блоков и операции циклического сдвига.

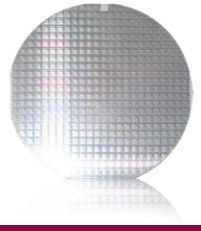
Оптимизация быстродействия – баланс между быстродействием и объемом (кода или аппаратных структур).

Пример структуры проходного шифратора



Характеристики шифропроцессоров серии «Блюминг»

Параметры	«Блюминг-1»	«Блюминг-2»	«Блюминг-1К»
Год разработки	1990	1992/1997	1995
Реализуемый алгоритм	ГОСТ	ГОСТ + дополнительные + модернизированные	ГОСТ + дополнительные
Число выполняемых режимов	21	83	50
Число хранимых ключей	3	4	3
Вид технологии	n-МОП	КМОП(2М)	КМОП(1М)
Размер кристалла, мм	4 x 4	8.2 x 5.6	5.8 x 5.8
Количество транзисторов	19000	47273	25728
Количество кристаллов на пластине	350	116	185
Количество тактов на обработку блока	175	114	116
Тактовая чистота, МГц	7.0	20.0	15.0
Быстродействие, Мбайт/с	0.32	1.404	1.03



Алгоритм скрытного суммирования

Если при сложении двух операндов и *X*, один из которых является маскированным гаммой *Г*, перенос в старшие разряды формировать по правилу:

$$\eta_r = \left\lfloor \frac{\left|\tilde{k}_r - \gamma_r\right|_q + x_r + \eta_{r-1}}{q} \right\rfloor,$$

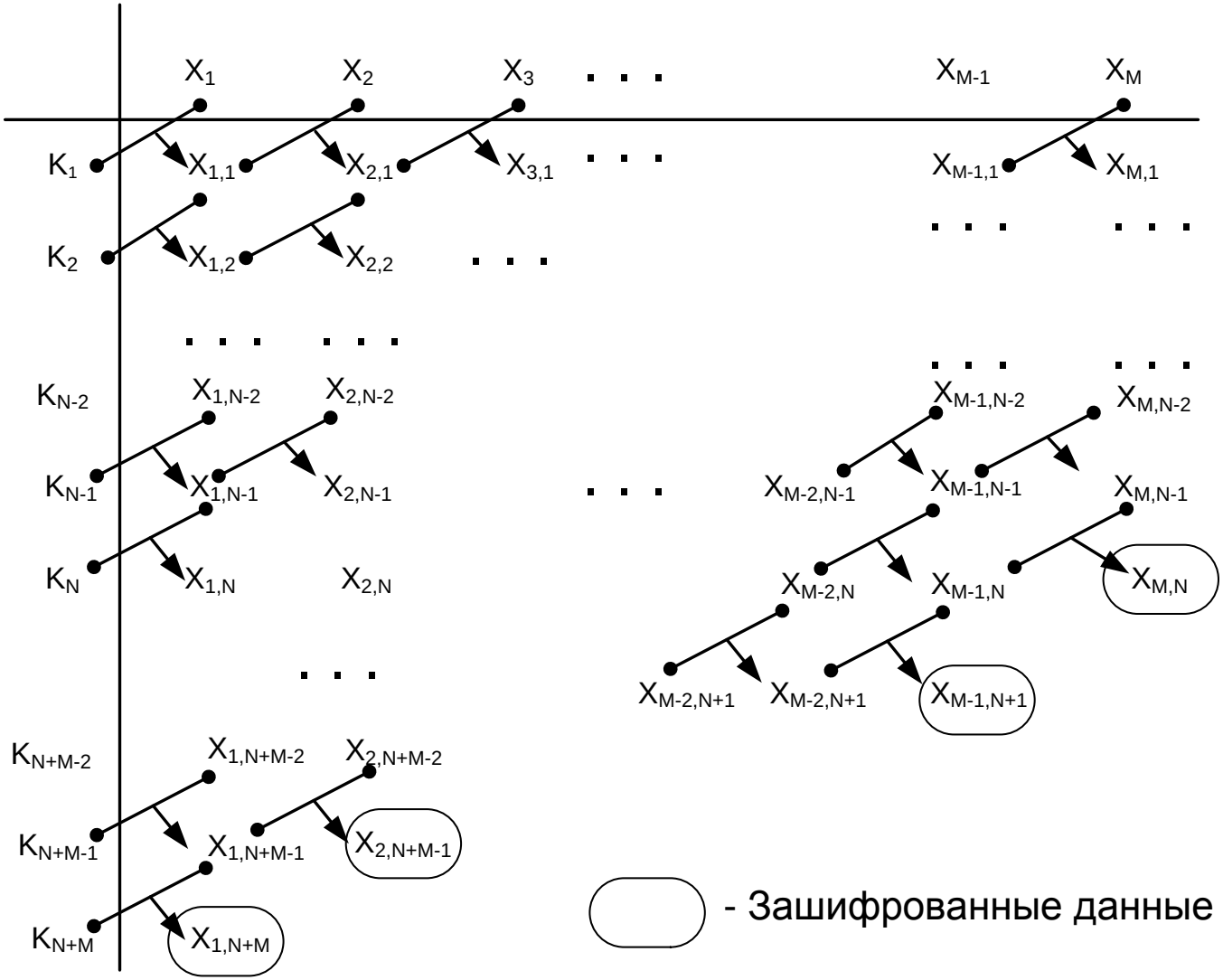
то при поразрядном вычитании по модулю основания *q* использованной ранее маски *Г* из результата *S'*, будет получена сумма *S* по модулю q^n двух не маскированных операндов *K* и *X*.

Для двоичной системы счисления

$$s'_r = \left|\tilde{k}_r + x_r + \eta_{r-1}\right|_2, \qquad \eta_r = \left\lfloor \frac{\left|\tilde{k}_r + \gamma_r\right|_2 + x_r + \eta_{r-1}}{2} \right\rfloor;$$

$$s'_r = \left|s'_r + \gamma_r\right|_2.$$

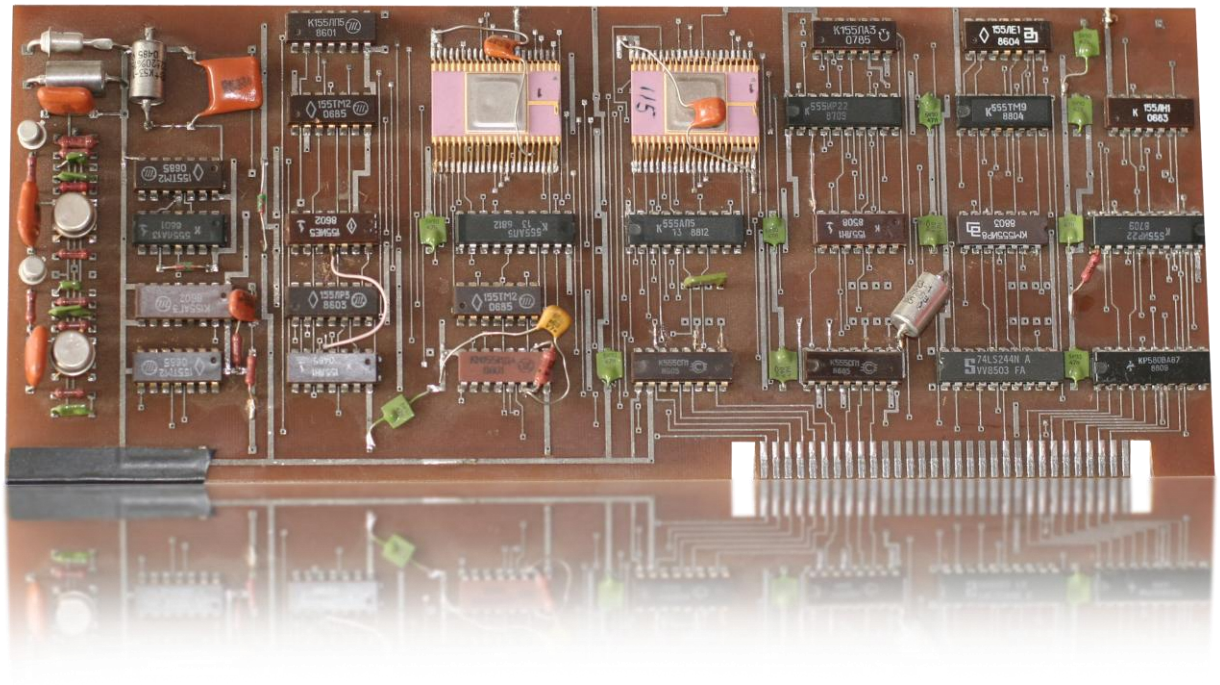
Реализация принципиально новых алгоритмов преобразований



В аппаратуре возможно реализовать алгоритмы принципиально неэффективно реализуемые программно.

Например, алгоритмы с сетевой структурой.

Эволюция реализации алгоритма ГОСТ 28147-89



1991

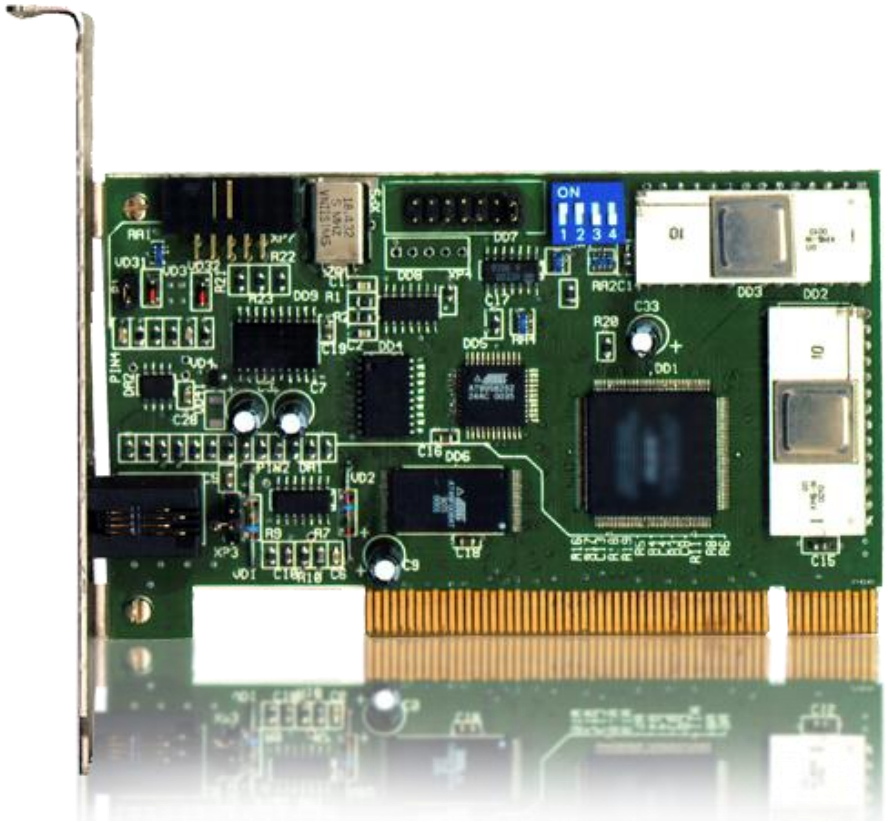
Эволюция реализации алгоритма ГОСТ 28147-89

1993

Эволюция реализации алгоритма ГОСТ 28147-89

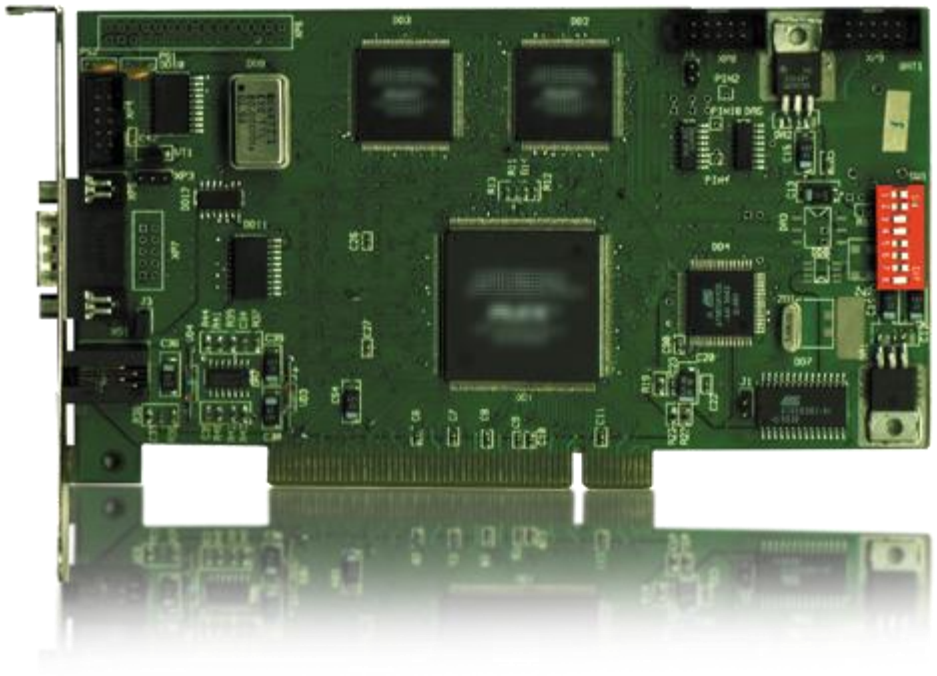
1997

Эволюция реализации алгоритма ГОСТ 28147-89



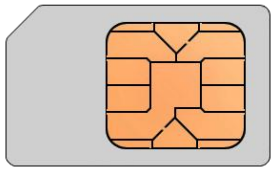
1999

Эволюция реализации алгоритма ГОСТ 28147-89



2000

Эволюция реализации алгоритма ГОСТ 28147-89



ancud.OS

Смарт-карта — генерация и хранение ключей, аутентификация, ЭЦП

Устройство АНКАДЕР

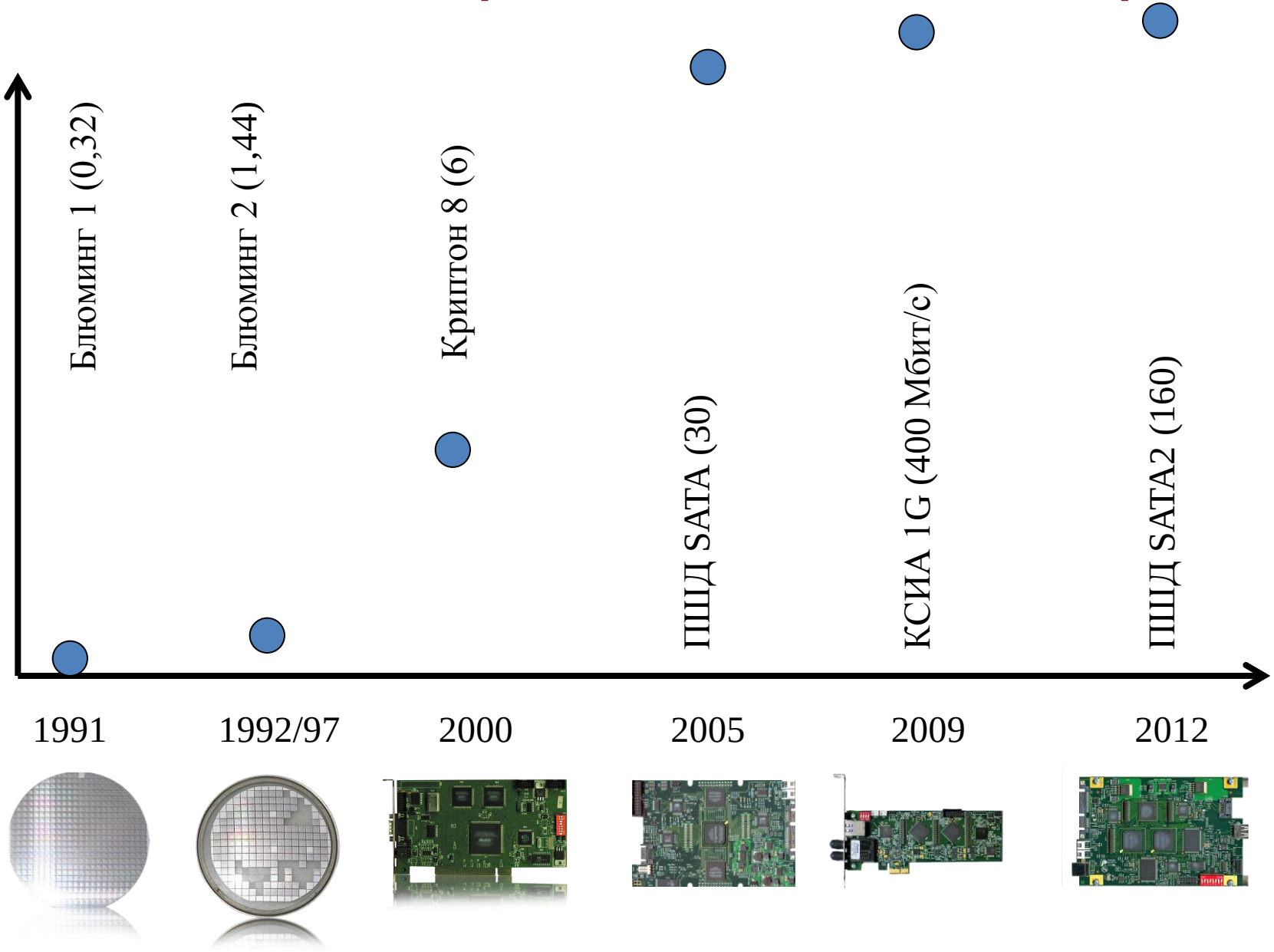
MicroSD-карта — хранение доверенной среды и конфиденциальной информации (КИ)

USB-ридер — обеспечение взаимодействия microSD-карты и смарт-карты с компьютером

Доверенная среда (ДоС) — замкнутая программная среда (ОС + модули безопасности + прикладное ПО) для защищённой обработки КИ

2010

Повышение производительности в 500 раз



Спасибо за внимание!

ООО Фирма «АНКАД»

Москва, Зеленоград, проезд 4806, д. 5, стр. 20

тел. (499) 731-0000, (499) 731-2050

факс (499) 731-2060

Шарамок Александр Владимирович

Начальник отдела разработки средств связи

тел. (499) 731-0000, (499) 731-2050, доб. 106

сот. (926) 131-6286 e-mail: sharamok@mail.ru