Ежегодная международная научно-практическая конференция
«РусКрипто'2019»

Способ снижения накладных расходов в канале между скоростными шифраторами

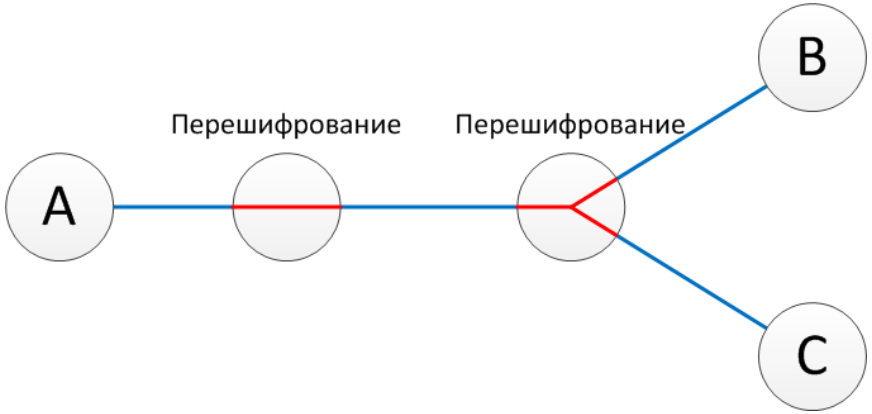
Бородин Михаил[1], Илья Калистру[2]
Исследователь[1], Архитектор аппаратных платформ[2], ОАО ИнфоТеКС[1,2]

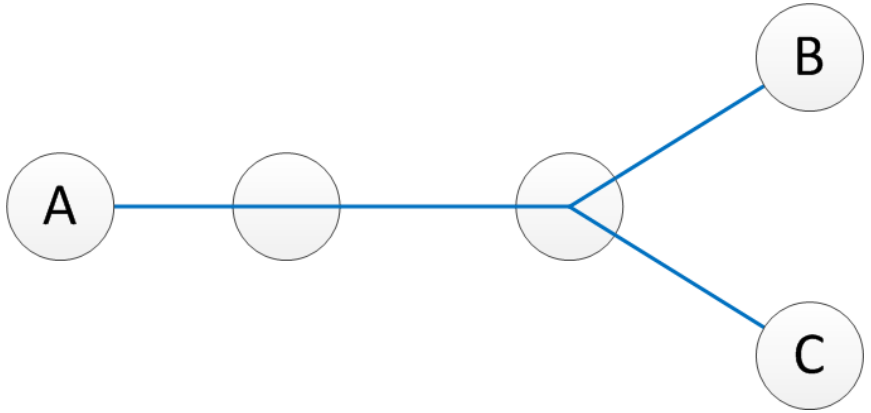
Структура доклада

- Мировой опыт построения высокоскоростных шифраторов. Основные характеристики
- Протокола передачи данных
- Вопросы эффективной реализации этого протокола
- Эксплуатационные достоинства AEAD режимов

Мировой опыт. Основные характеристики

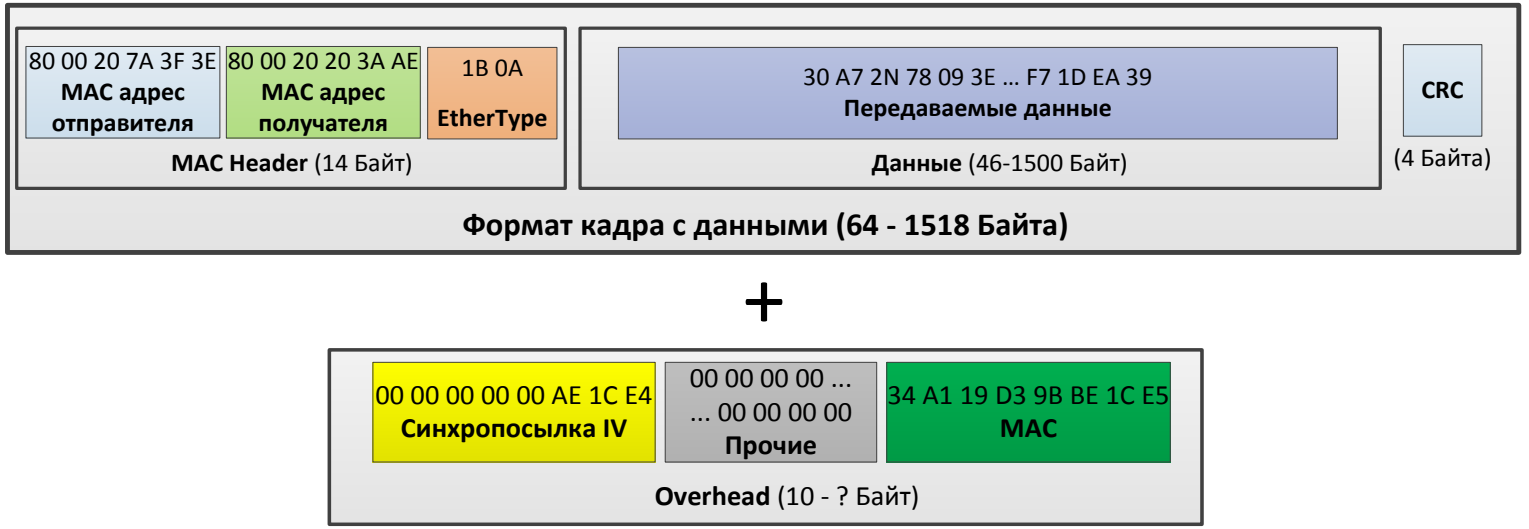
- Эксплуатационные характеристики:
  - Типы сети функционирования
    - LAN, MAN, WAN
    - Точка / мультиточка
    - Шифрование между конечными узлами / промежуточное перешифрование





Мировой опыт. Основные характеристики

- Эксплуатационные характеристики:
  - Скорость работы шифраторов (1G / 10G / 100G / …)
    - Пропускная способность самих устройств
    - Вносимые в канал накладные расходы (overhead)

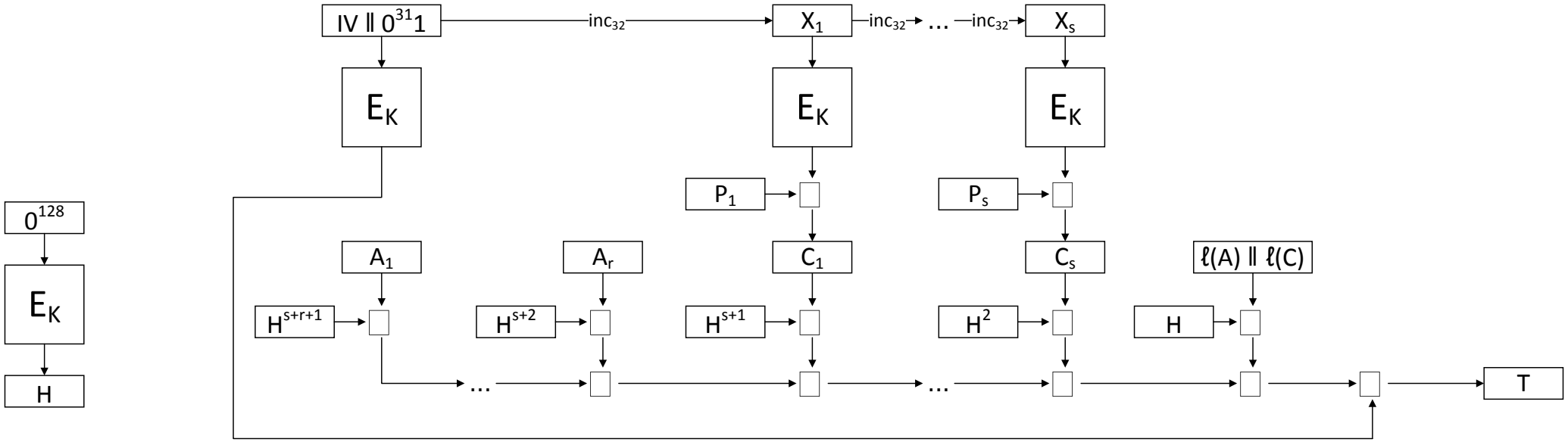


Мировой опыт. Основные характеристики

- Эксплуатационные характеристики:
  - Вносимые задержки (~100 мкс/ ~10 мкс / ~1 мкс)

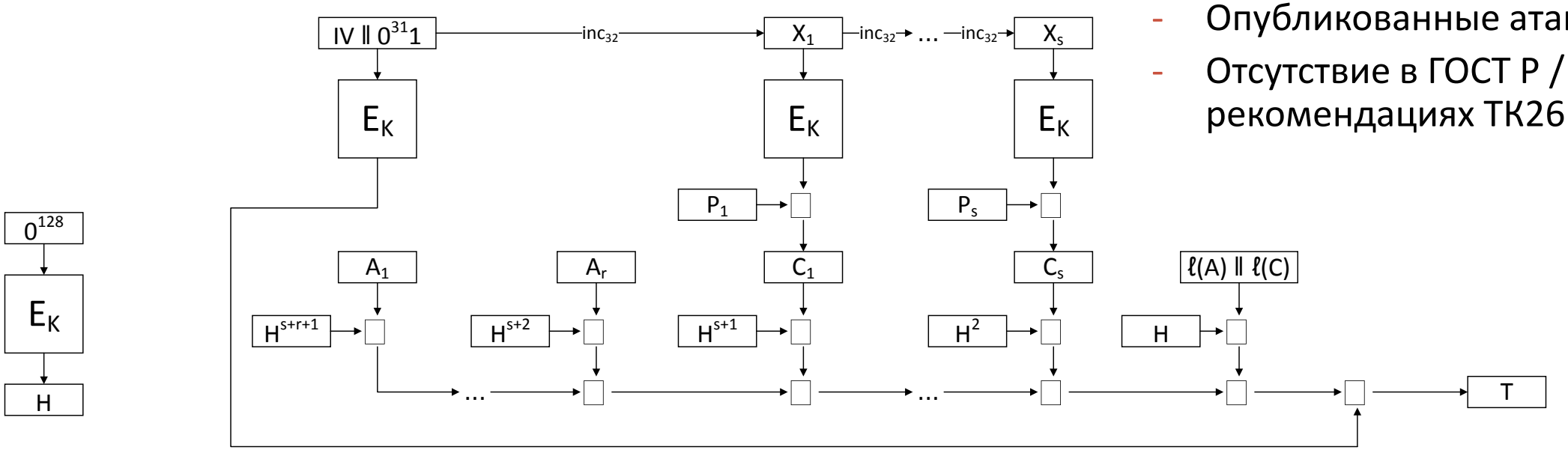
Мировой опыт. Основные характеристики

- Криптографические характеристики:
  - AEAD режим (AES - GCM)



Мировой опыт. Основные характеристики

- Криптографические характеристики:
  - AEAD режим (AES - GCM)



- ✓ ISO/IEC 19772:2009
- ✓ NIST Special Publication 800-38D
- ✓ Высокоскоростная реализация

- Опубликованные атаки
- Отсутствие в ГОСТ Р / рекомендациях ТК26

Мировой опыт. Основные характеристики

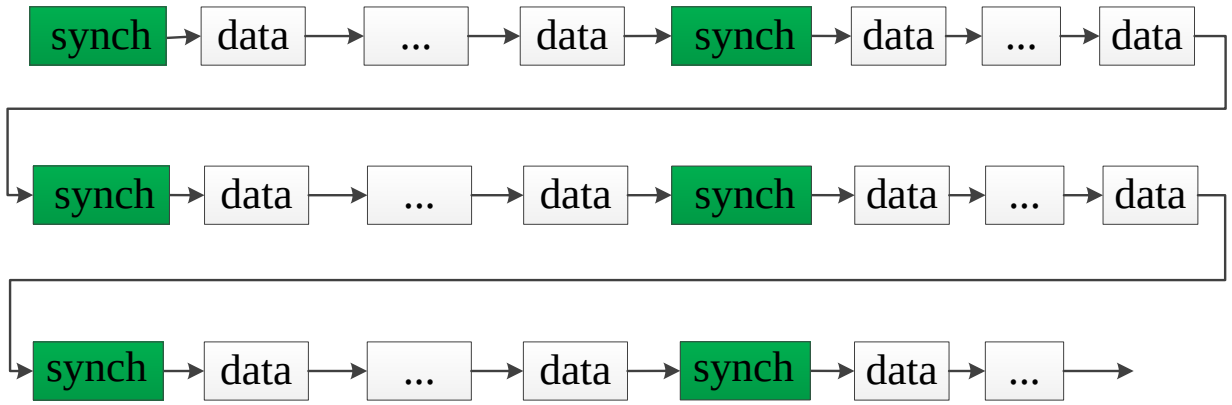
- Криптографические характеристики:
  - Протокол передачи данных (Проприетарный)

Подходящий протокол передачи данных

- Эксплуатационные характеристики:
  - Типы сети функционирования (**точка-точка, сети общего пользования**)
  - Скорость работы шифраторов (**10G / 100G / …**)
  - Вносимые задержки (**~7 мкс / ~ 0,7 мкс / …**)
- Криптографические характеристики:
  - Протокол передачи данных (**Проприетарный**)
  - AEAD режим (**Кузнечик - GCM**)

Протокол передачи данных

- Последовательность кадров:

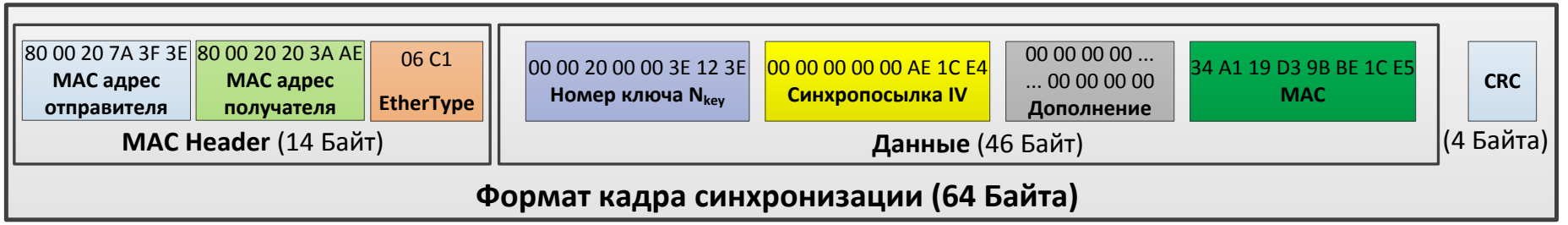


synch - Кадр синхронизации

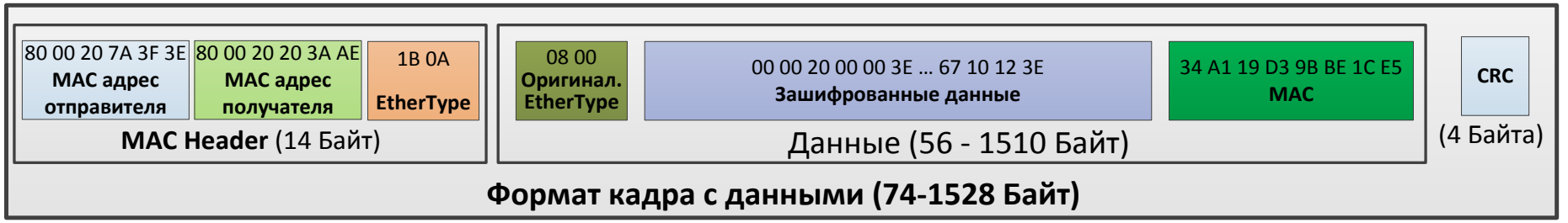
data - Кадр с данными

Протокол передачи данных

- Формат кадра синхронизации (64 Байта):

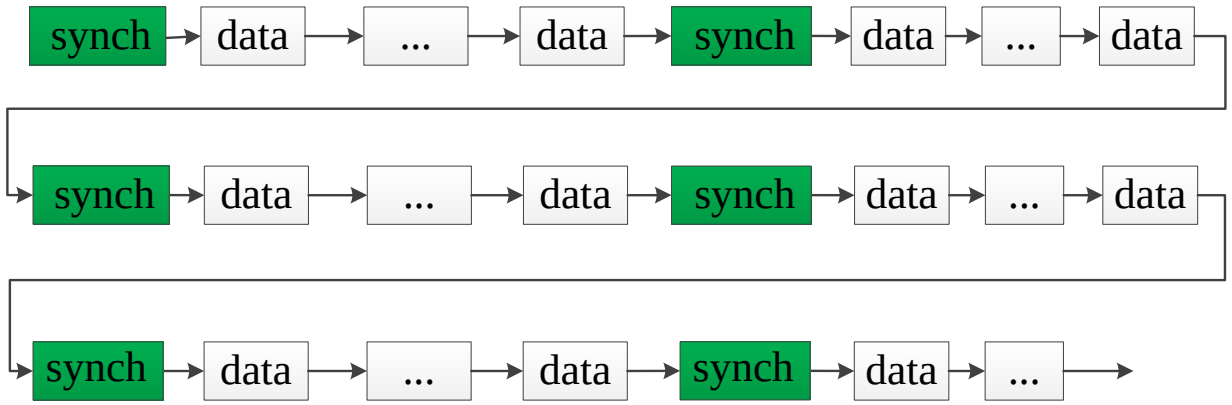


- Формат кадра с данными (74 – 1510 Байт):



Протокол передачи данных

- Последовательность кадров:



synch - Кадр синхронизации

data - Кадр с данными

Частота отправки кадров синхронизации определяется исходя из:

- ✓ Среднего размера кадров с данными;
- ✓ Вероятности потерь/ошибок в канале;
- ✓ Вероятности нарушения порядка следования кадров.

Вопросы эффективной реализации этого протокола

- Параллельная обработка на разных вычислительных узлах:

+:

- Простота реализации;
- Вариативность в криптографических алгоритмах.

-:

- Входные буферы;
- Большие задержки;
- Наличие балансировщика.

- Конвейерная обработка:

+ :

- Минимизация задержек

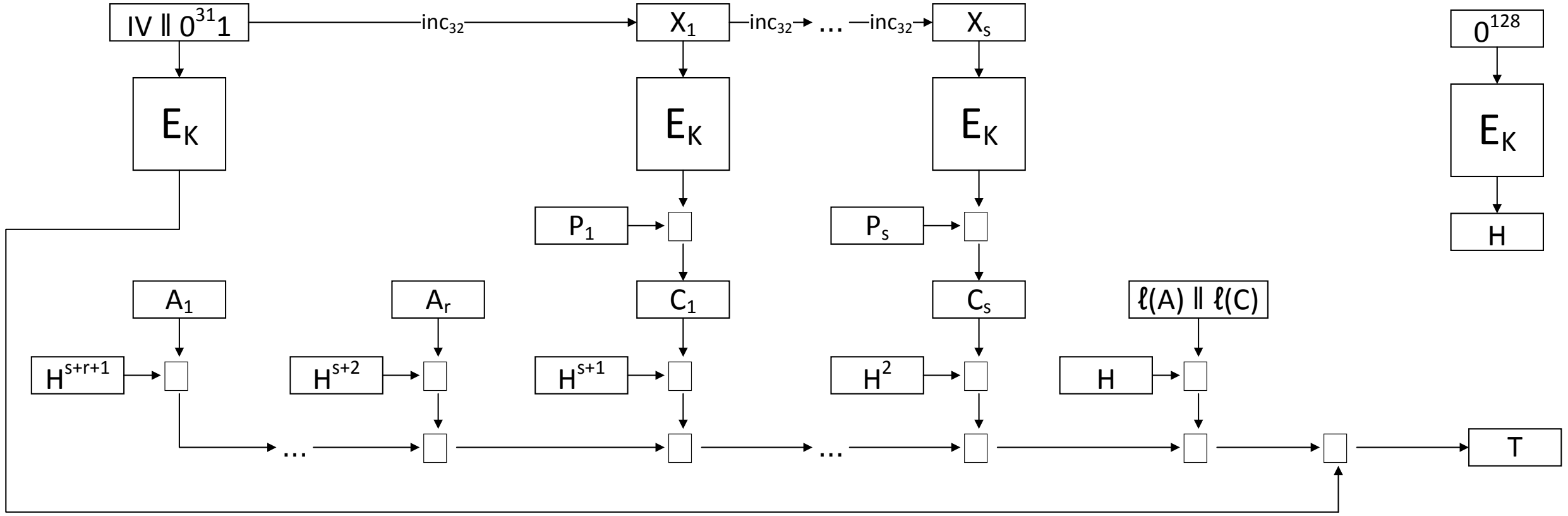
-:

- Большая глубина конвейера
- Задержка зависит от криптографических алгоритмов

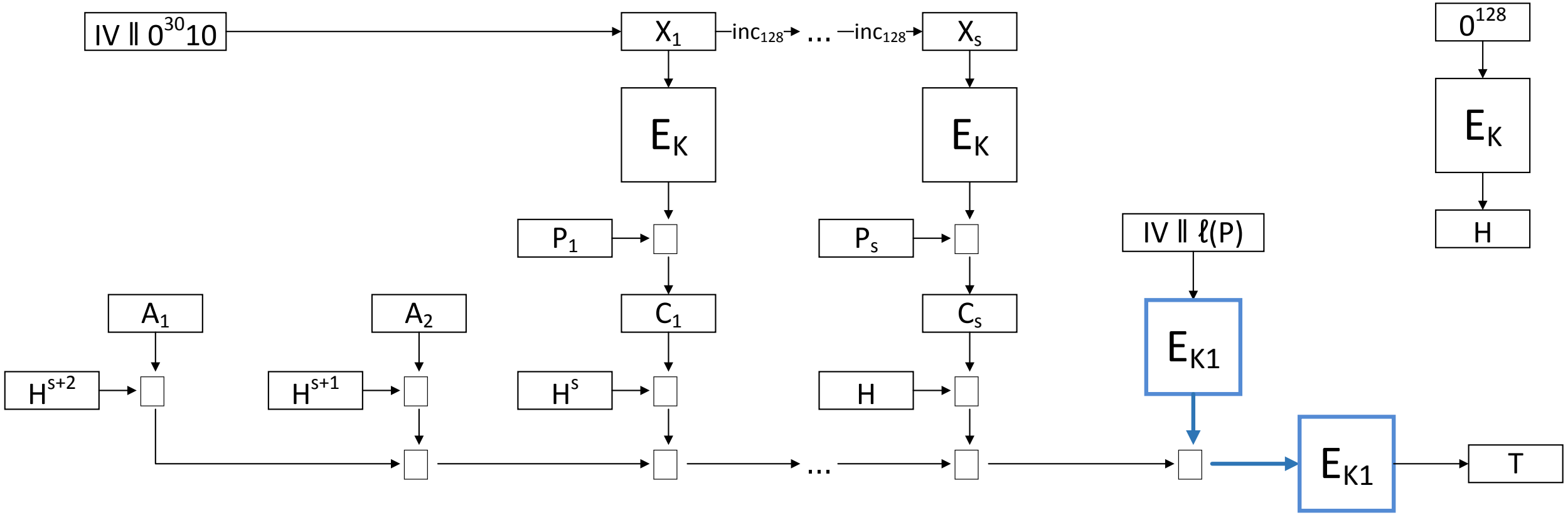
Вопросы эффективной реализации этого протокола

Вопросы эффективной реализации этого протокола

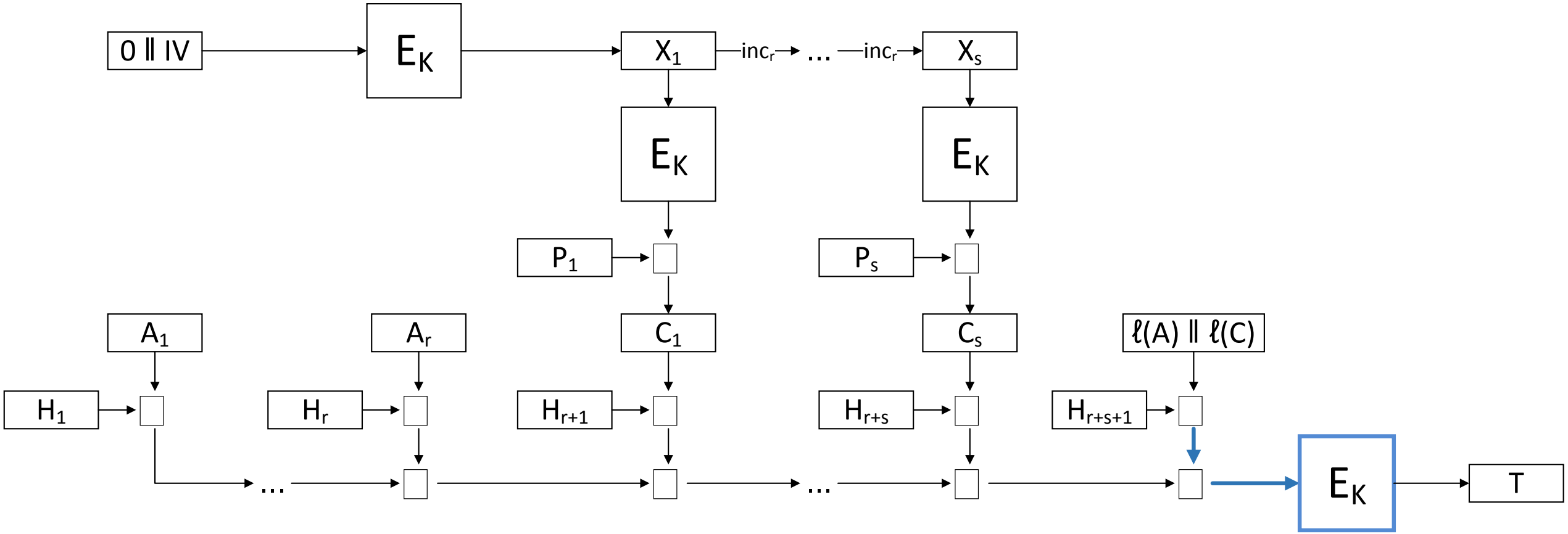
Эксплуатационные достоинства AEAD режимов (GCM)



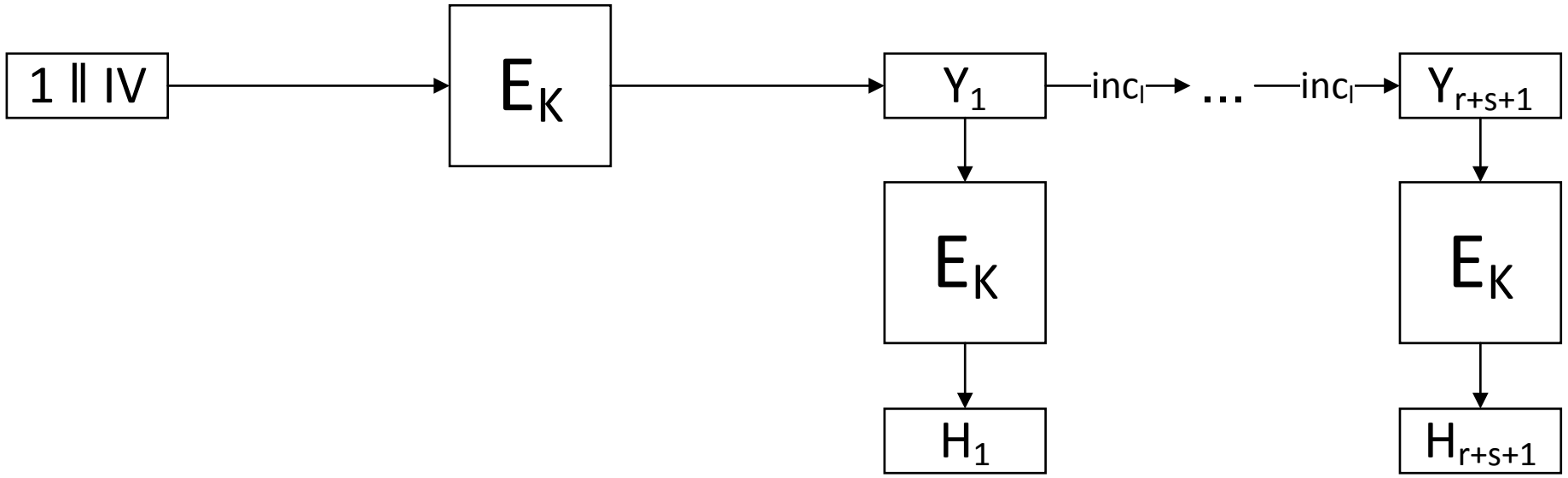
Эксплуатационные достоинства AEAD режимов (Нефрит)



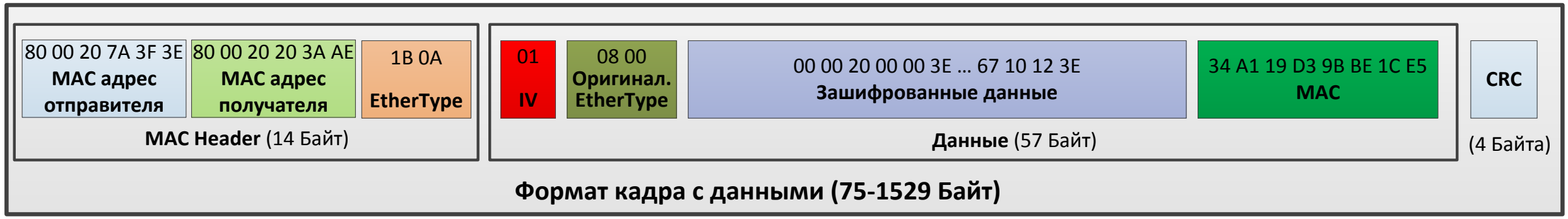
Эксплуатационные достоинства AEAD режимов (MGM)



Эксплуатационные достоинства AEAD режимов (MGM)



Эксплуатационные достоинства AEAD режимов



Теоретические оценки пропускной способности канала

Размер входящего кадра (Байт)	Максимальное количество кадров в защищенном канале	Скорость потока во входящем / исходящем канале (Гбит/с)	Скорость передачи полезной информации в сети (Гбит/с)
64	**132 978 270**	89,7	55,3
128	79 113 641	93,7	73,4
256	43 706 133	96,5	85,3
512	23 062 644	98,2	92,2
1024	11 859 538	99,1	96,0
1518	8 074 905	99,4	**97,3**

Спасибо за внимание!

Контактная информация

Электронная почта:

Бородин Михаил Mikhail.Borodin@infotecs.ru

Илья Калистру Ilia.Kalistru@infotecs.ru

Набор основных пиктограмм