Ежегодная международная научно-практическая конференция
«РусКрипто’2020»

Аспекты криптографической защиты протокола NB-Fi

Алексеев Евгений Константинович, к.ф.-м.н.,
Начальник отдела криптографических исследований, КриптоПро
Старший научный сотрудник лаборатории стандартизации, Академия криптографии РФ

Криптографический анализ протокола NB-Fi

- Исследование проведено в рамках НИР «Циферблат», поставленного Академией криптографии РФ, под руководством Бондаренко А.И.

- Работы были проведены следующими специалистами:
  - Алексеев Е.К.
  - Ахметзянова Л.Р.
  - Николаев В.Д.
  - Смышляев С.В.

- Работа проводилась в тесном сотрудничестве с представителями компании Waviot (Бакуменко А.В., Батура Д., Молин А.С., Орлов А.О.) и Станиславом Елизаровым (Сколково).

Протокол беспроводной передачи данных на основе узкополосной модуляции радиосигнала (NB-Fi)

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ

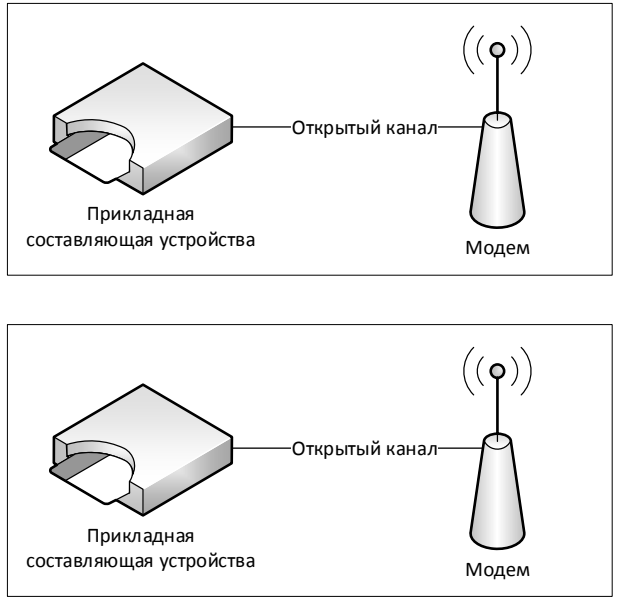
Информационные технологии

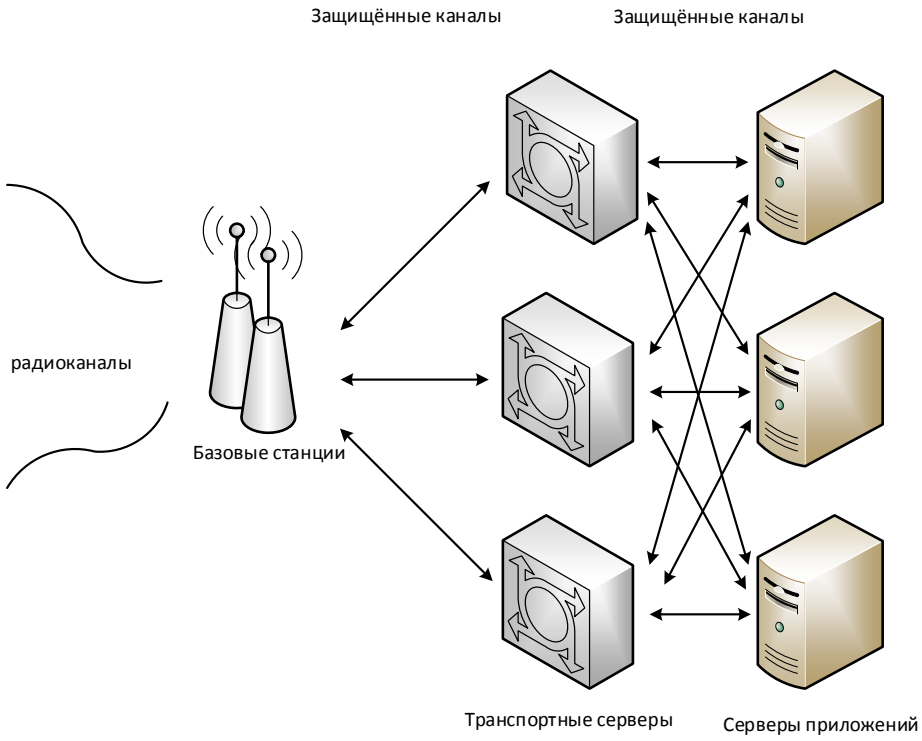
ИНТЕРНЕТ ВЕЩЕЙ

Протокол беспроводной передачи данных на основе узкополосной модуляции радиосигнала (NB-Fi)

Компоненты взаимодействия

- Прикладная составляющая конечного устройства
- Модем конечного устройства
- Базовая станция
- Транспортный сервер
- Сервер приложений





Участники взаимодействия

- Конечное устройство (прикладная составляющая и модем);
- Оператор сети (базовая станция и транспортный сервер);
- Прикладной оператор (сервер приложений)

Конечное устройство

Оператор сети

Прикладной оператор

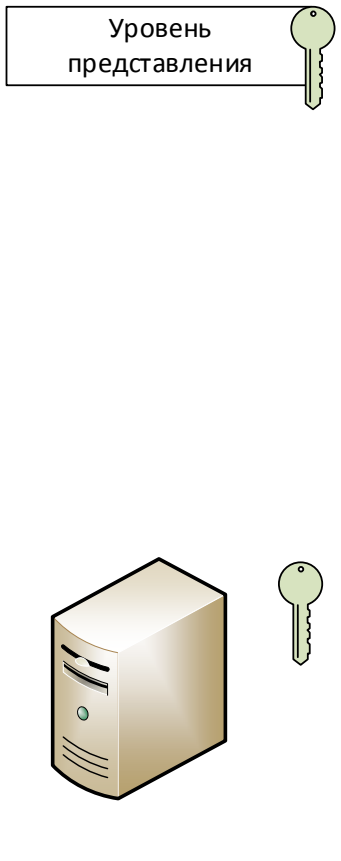
Стек протоколов NB-Fi

- **физический уровень**: прием/передача произвольной информации по среде распространения;
- **MAC-уровень**: передача информационного пакета на выбранном физическом уровне, исправление ошибок;
- **транспортный уровень**: защищенная передача полезной нагрузки и управляющих команд между оператором сети и устройствами;
- **уровень представления**: защищенная передача данных уровня приложения между прикладными операторами и их устройствами.

Стек протоколов NB-Fi

Конечное устройство

Оператор сети



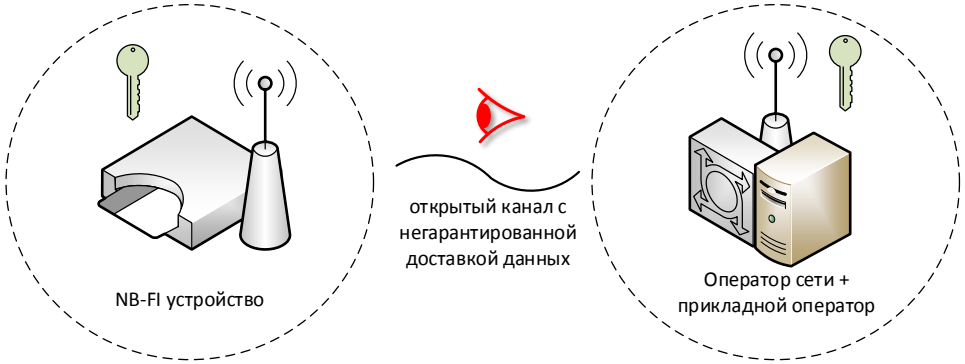
Прикладной оператор

Модель противника

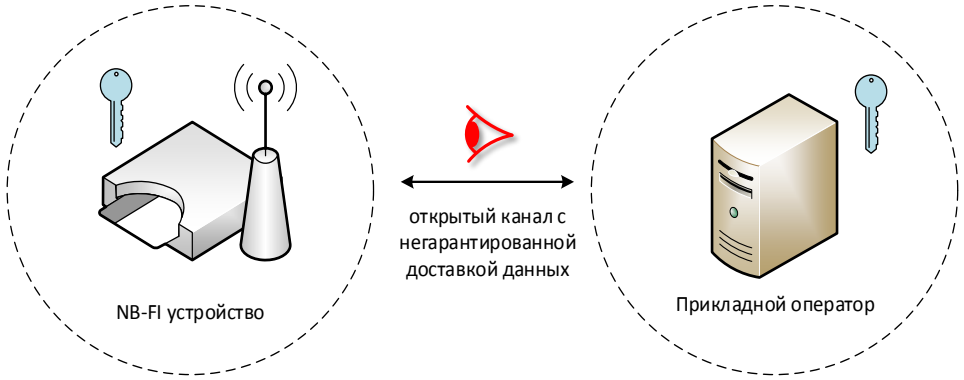
- Модель угрозы
  - Нарушение конфиденциальности потока данных
  - Нарушение целостности потока данных (по модулю утерянных пакетов)
- Тип атаки
  - Возможность навязывать любые открытые данные для передачи их по защищенному каналу в любом направлении
  - Возможность модифицировать, удалять данные, передаваемые в любом направлении
- Ресурсы
  - Возможность накапливать достаточно большой объем информации (порядка 40 МБ)
  - Неограниченное количество попыток подделки данных

Сценарии функционирования системы

- Оператор сети не является противником

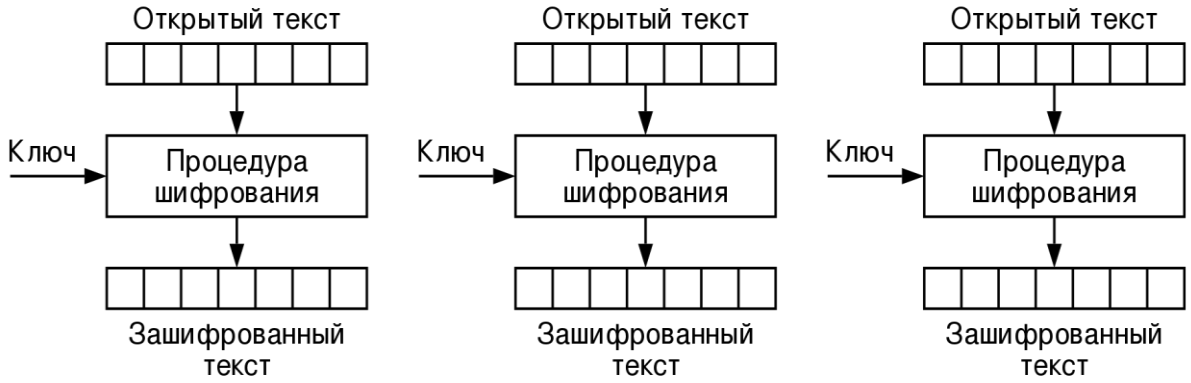


- Оператор сети является противником



Используемые алгоритмы

- Базовое семейство перестановок: ГОСТ Р 34.12-2015 «Магма»
- Шифрование: режим простой замены (ECB):



- Алгоритм CRC16:
  - CRC(x) = Data(x) * x^16 mod G(x)
  - Data(x) – соответствующий данным многочлен над GF(2) степени <битовая_длина_данных - 1>, а G(x) – фиксированный многочлен степени 16

Формат пакета транспортного уровня

- Признак системности пакета: SYS
- Номер пакета ITER размера 5 бит
- Поле Payload длины от 8 до MAXLEN (не более 128) байт содержит непосредственно данные в зашифрованном виде
- Шифрование может быть отключено с помощью системного пакета CONF
- Поле Payload CRC длины 2 байта содержит значение контрольной суммы незашифрованного поля Payload и поля Header

Header				Payload	Payload CRC
SYS	ACK	MULTI	ITER		
1 бит	1 бит	1 бит	5 битов	8 - 128 байт	2 байта

Смена ключа шифрования

- Выделение нового ключа шифрования выполняет конечное устройство по собственной инициативе, либо по запросу от сервера при помощи системного пакета с типом GETNEWKEY
- Устройство:
  - вырабатывает 32-байтовое ключевое значение
  - отправляет данный ключ на сервер в виде пяти системных пакетов типов KEY0–KEY4
- Сервер:
  - выполняет отправку системного пакета типа CONF, содержащего в поле Payload контрольную сумму ключа размером 4 байта (CRC-32)
- Устройство:
  - получив этот пакет, сверяет контрольную сумму и в случае совпадения применяет новый ключ

Оценка стойкости: конфиденциальность

- Уязвимости режима ECB:
  - противник имеет возможность вскрывать малоэнтропийные данные по шифртексту

- Уязвимости из-за использования CRC-16:
  - Поле Payload CRC передается в канал в открытом виде и линейно зависит от открытых данных

Оценка стойкости: целостность

- **На уровне отдельных сообщений**:
  - Алгоритм CRC-16 (CRC-32) не является криптографическим механизмом, следовательно противник имеет возможность недетектируемо модифицировать открытый заголовок или известную ему часть открытых данных
- **На уровне потока**:
  - Из-за частого повторения номеров сообщений (ITER, 5 бит) противник может дублировать пакеты. От этого не спасло бы даже использование стойкой схемы вычисления имитовставки вместо CRC-16
- **На уровне потоков**:
  - Для шифрования пакетов используется один и тот же ключ как в одну сторону, так и в другую. Такая особенность протокола позволит проводить так называемые «атаки отражения»

Оценка стойкости: последствия

- **Отключение шифрования на устройстве**
  - Противник может сформировать корректный системный пакет, содержащий команду CONF с флагом FLG_NO_ENC, отключающим шифрование

- **Установка ключа на сервера противником**
  - Противник может сформировать корректные системные пакеты KEY0–KEY4, содержащие известный противнику ключ шифрования

- **Компрометация битов ключа**
  - Противник может получить 80 битов информации о следующем секретном ключе сторон. Это не позволяет рассчитывать на стойкость применяемого для шифрования данных блочного шифра Магма

Новая версия защиты данных в NB-Fi

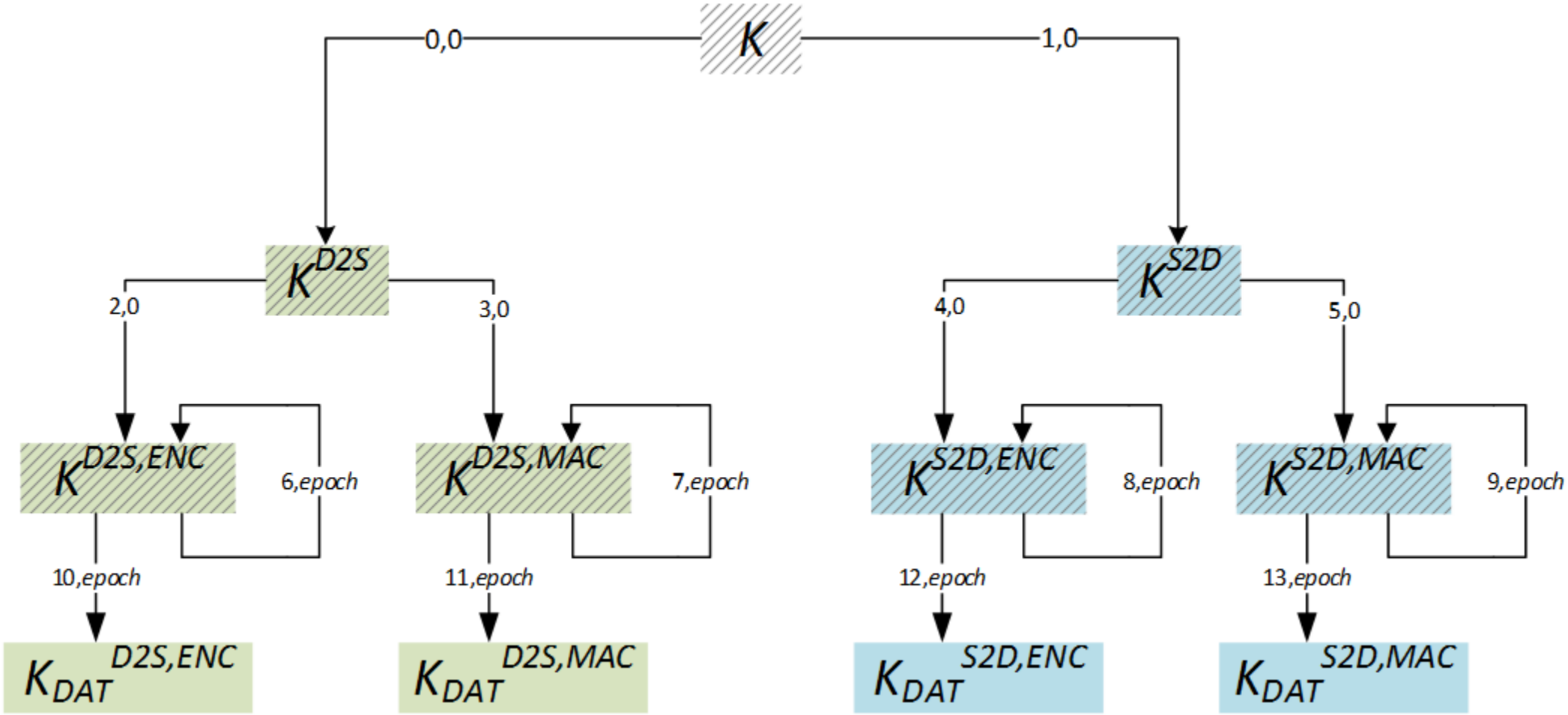
- Иерархия ключей:
  - Общий секретный ключ K устройства и базовой станции
  - Мастер-ключи каждого направления (D2S, S2D)
  - Мастер-ключи шифрования и имитозащиты
  - Ключи обработки данных

- Последовательная смена ключей (serial re-keying, RFC 8645)

- Использование легковесной функции диверсификации ключей:

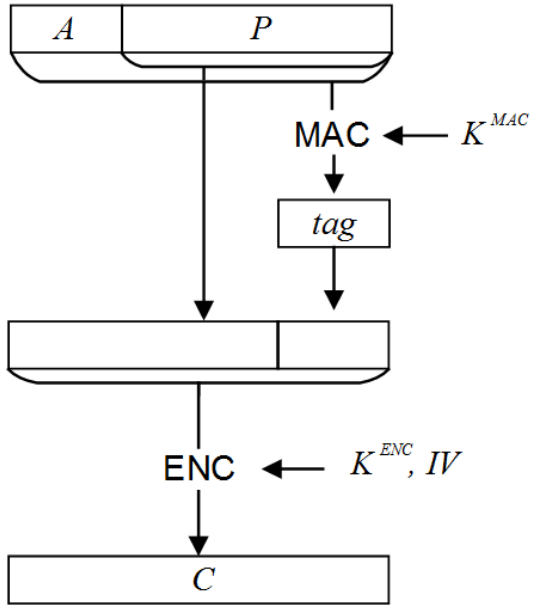
$$Divers(K_{old}, seed) = CTR_{Magma}(K_{old}, seed, 0^k)$$

Новая версия защиты данных в NB-Fi



Новая версия защиты данных в NB-Fi

- Формат пакета:
  - Номер сообщения – 8 бит
  - Имитовставка – 24 бита

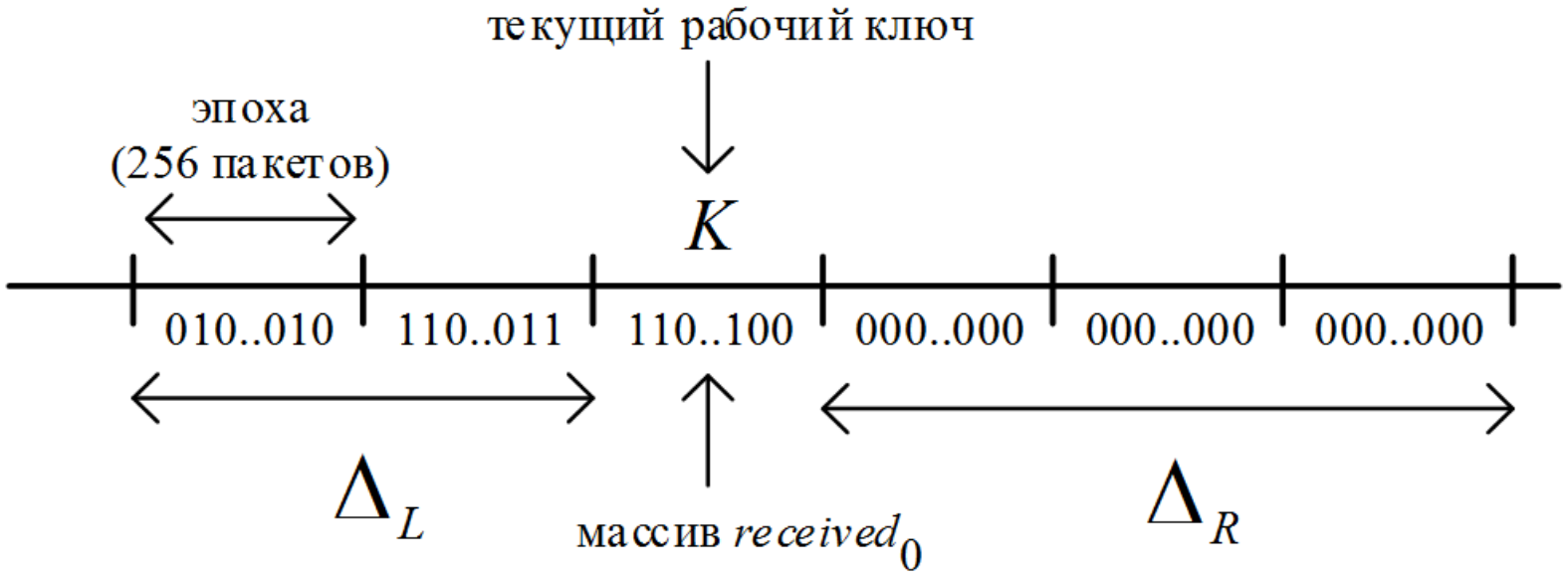


- Схема защиты данных:
  - MAC-then-Encrypt (аналогично TLS 1.2)

- Используемые примитивы и схемы:
  - Семейство перестановок: «Магма» (ГОСТ Р 34.12-2015)
  - Алгоритм шифрования: CTR (ГОСТ Р 34.13-2015)
  - Алгоритм выработки имитовставки: OMAC (ГОСТ Р 34.13-2015)

Новая версия защиты данных в NB-Fi

- Порядок синхронизации ключей:
  - Текущий рабочий ключ
  - Хранится несколько «предыдущих ключей»
  - Сначала осуществляется поиск «назад», потом «вперед» с обновлением текущего рабочего ключа в случае, если поиск завершился успешно



Контактная информация

Электронная почта:

alekseev@cryptopro.ru

Телефон:

+7-903-159-33-62

Сайт:

cryptopro.ru