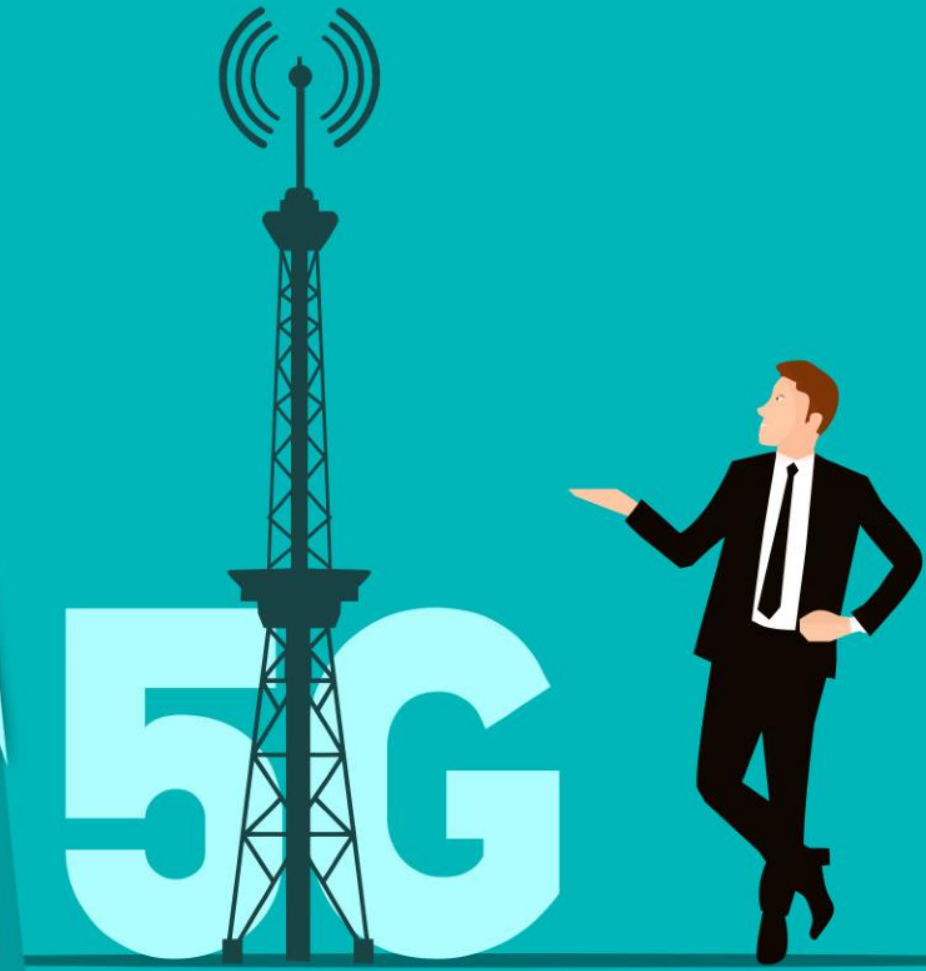
Разработка протокола аутентифицированной выработки ключей 5G-AKA-GOST

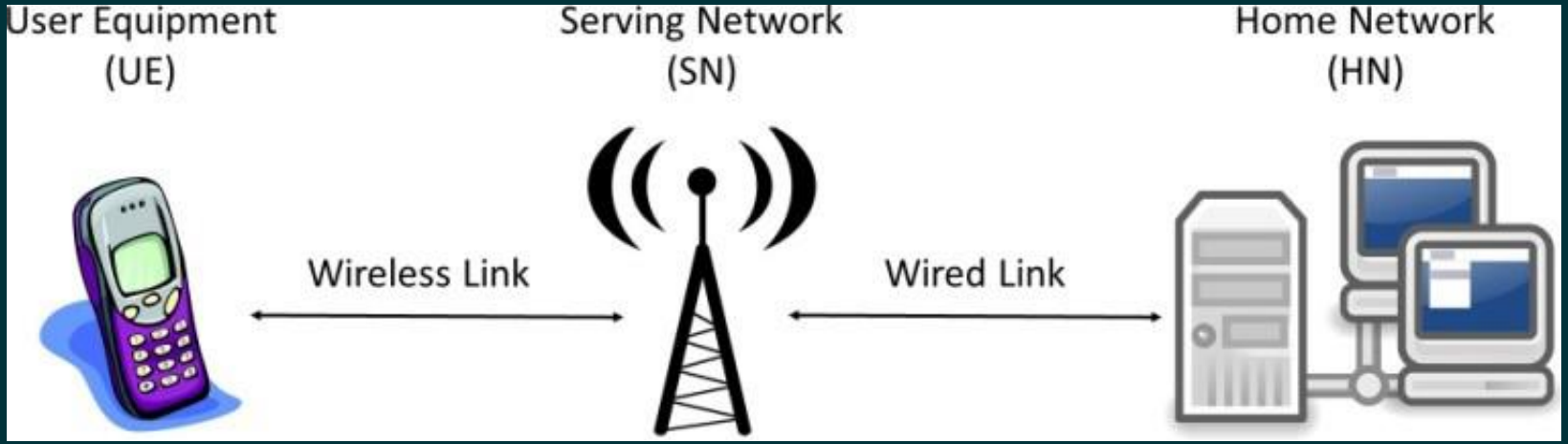


Степан Давыдов

АО «НПК «Криптонит»

В рамках НИР «Мобильность» АНО «НТЦ ЦК»

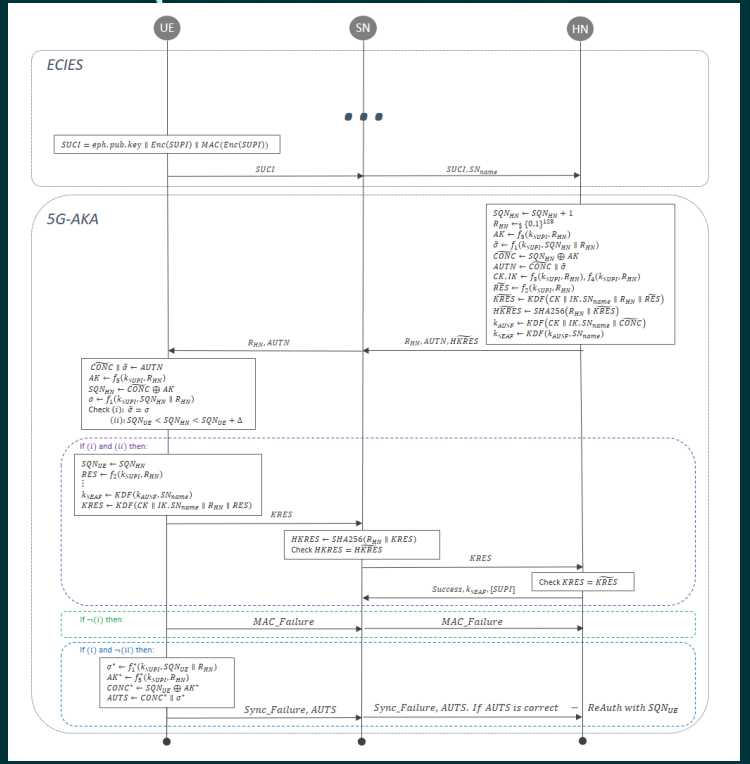
Аутентификация абонентов в сетях 5G



В рамках обоснования стойкости промежуточный участник SN может быть объединён с HN

Механизм аутентификации 5G

- Схема ECIES (стандарт ISO, ANSI, SEC1v2, 3GPP)
- Протокол 5G-AKA (стандарт 3GPP)
  - Включает в себя механизм S3G
  - Подвержен значительному числу replay атак с нарушением приватности абонента



3GPP TS 33.102

Следующие свойства безопасности должны быть обеспечены:

- Конфиденциальность постоянного идентификатора пользователя
- Конфиденциальность местоположения пользователя
- Неотслеживаемость

5 Security features

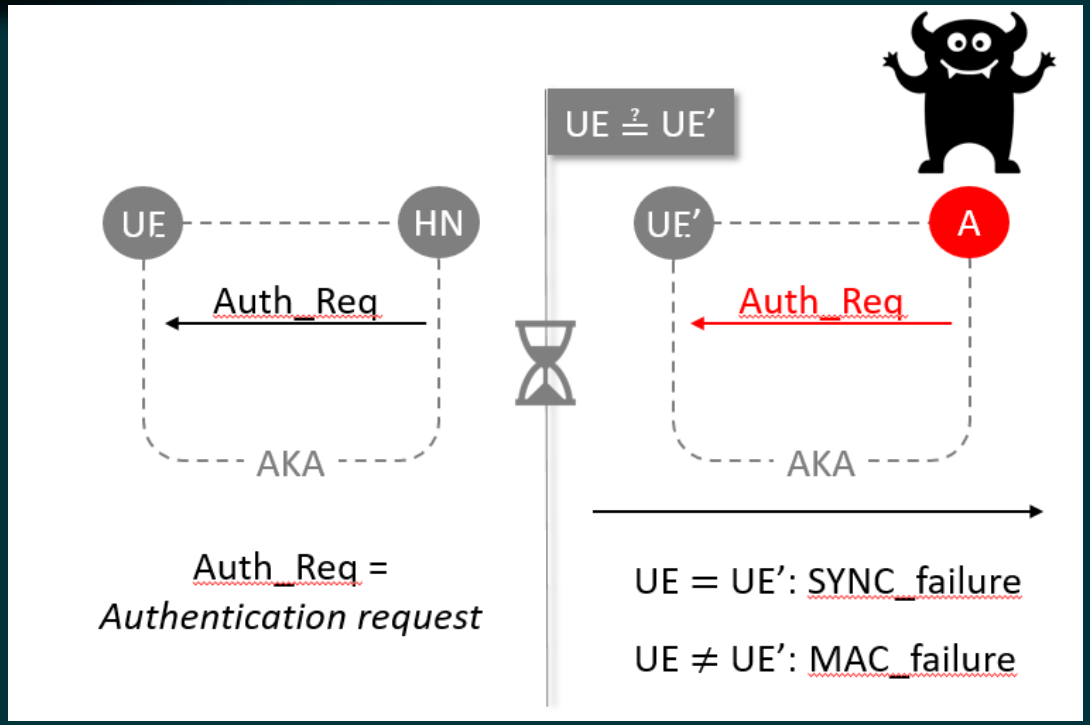
5.1 Network access security

5.1.1 User identity confidentiality

The following security features related to user identity confidentiality are provided:

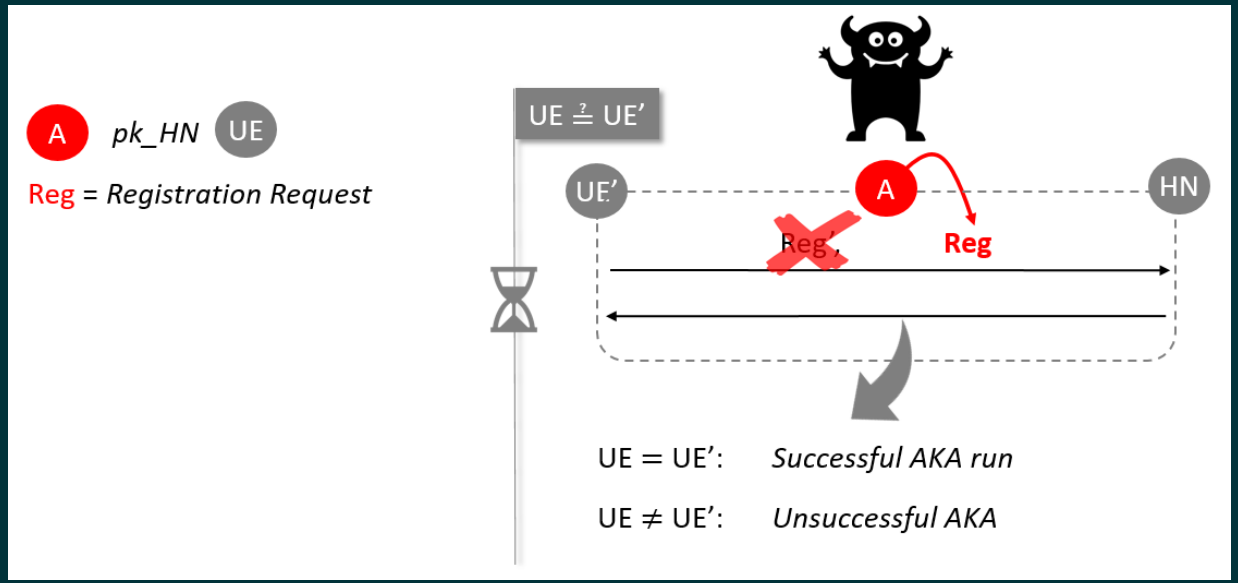
- **user identity confidentiality:** the property that the permanent user identity (IMSI) of a user to whom a services is delivered cannot be eavesdropped on the radio access link;
- **user location confidentiality:** the property that the presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link;
- **user untraceability:** the property that an intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link.

LFM-атака (пример)



Результат: противник установил соответствие между абонентами UE и UE'

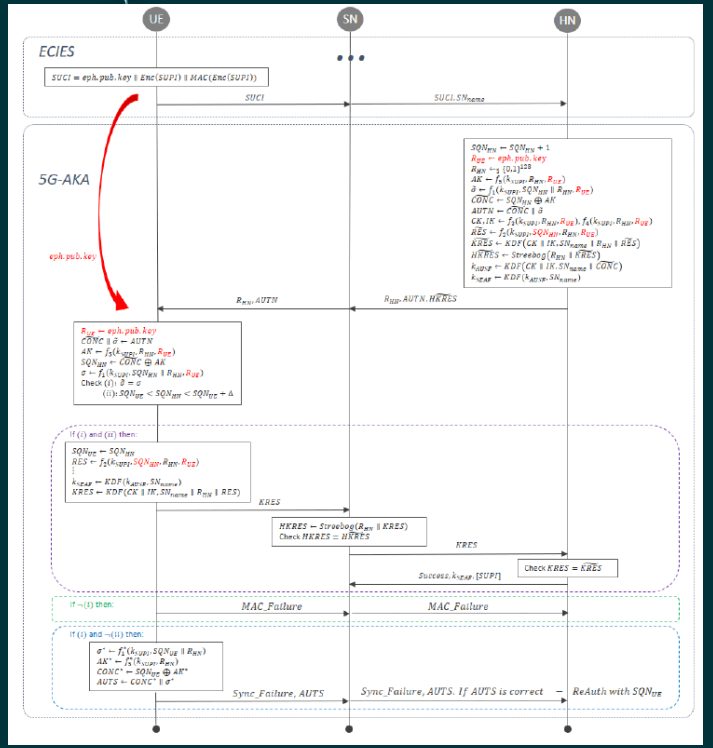
SUPI check атака



Результат: противник проверил, является ли подключающийся абонент абонентом UE

Протокол 5G-AKA-GOST

- Добавлена случайность со стороны абонента UE, обеспечена защита от replay атак
- В контрольное значение RES механизма S3G добавлен параметр SQN для отслеживания рассинхронизации

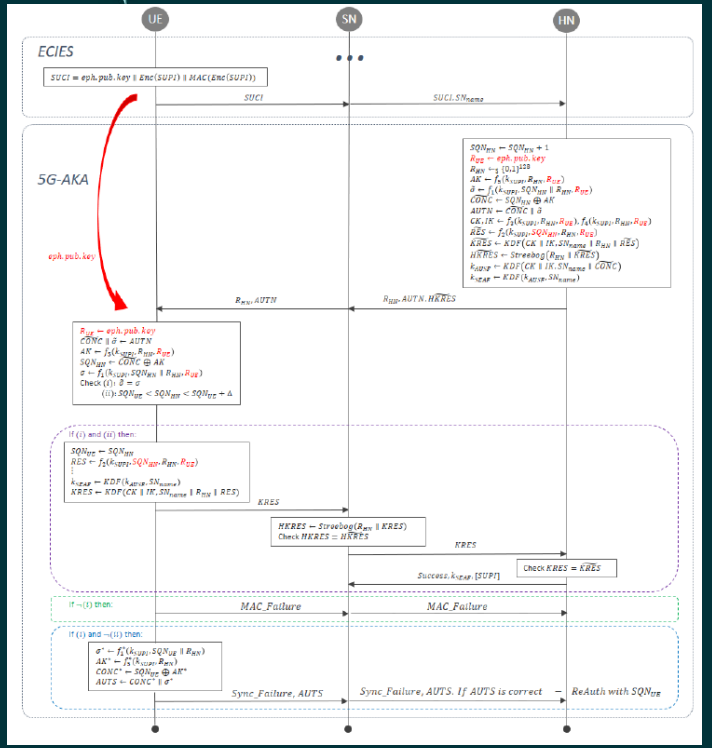


Протокол 5G-AKA-GOST

Алгоритмы

- шифрования
- хэширования
- выработки ключей
- вычисления имитовставки

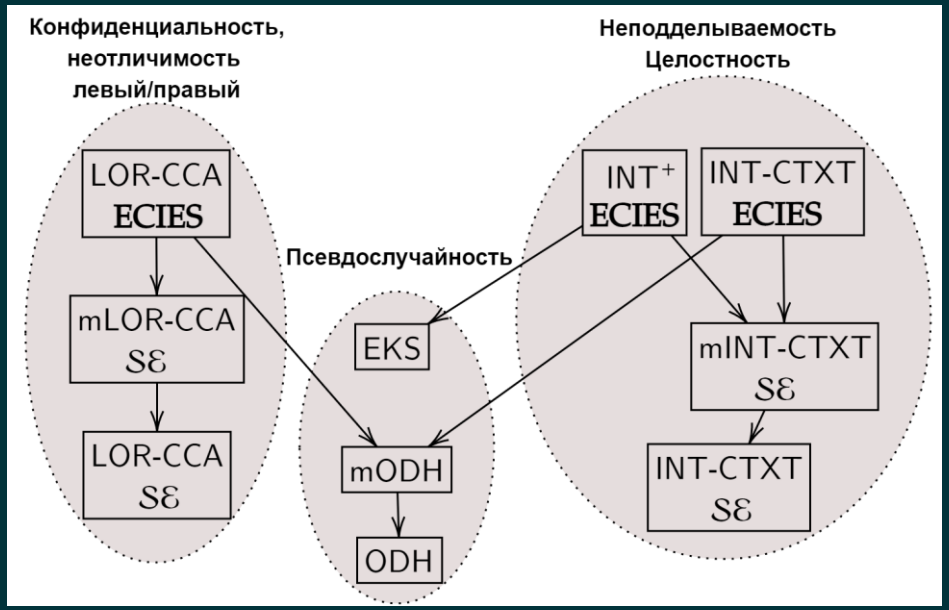
заменены отечественными аналогами

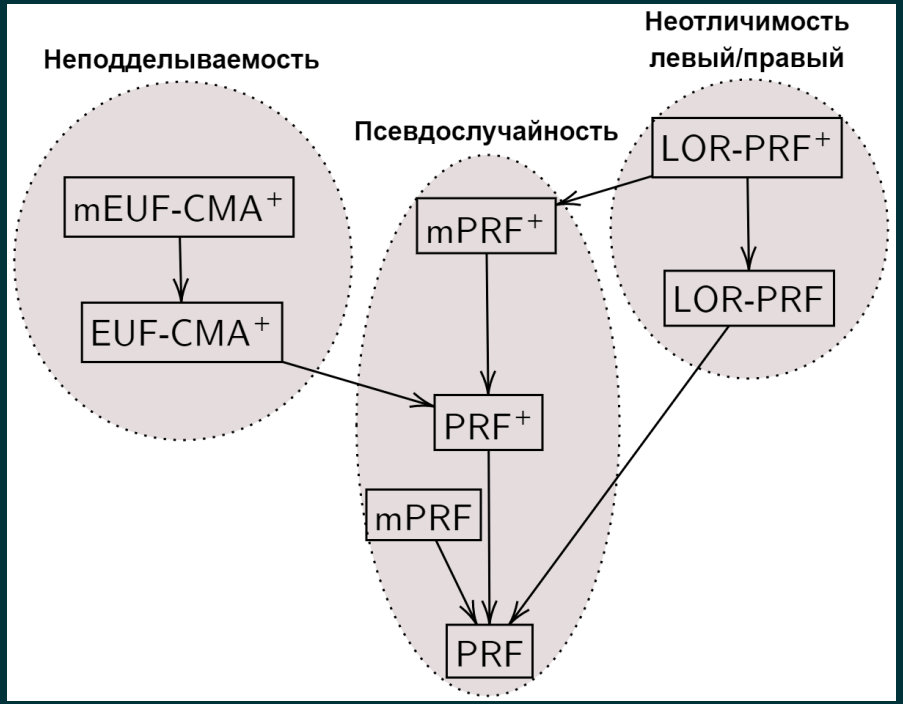


Модель противника

- **Базис**: стандартные модели для AKE-протоколов
- **Добавление**: модель для анонимности в терминах неразличимости участников
- **Итог**: комбинированная модель противника, учитывающая все неформальные требования к протоколу

Модель противника

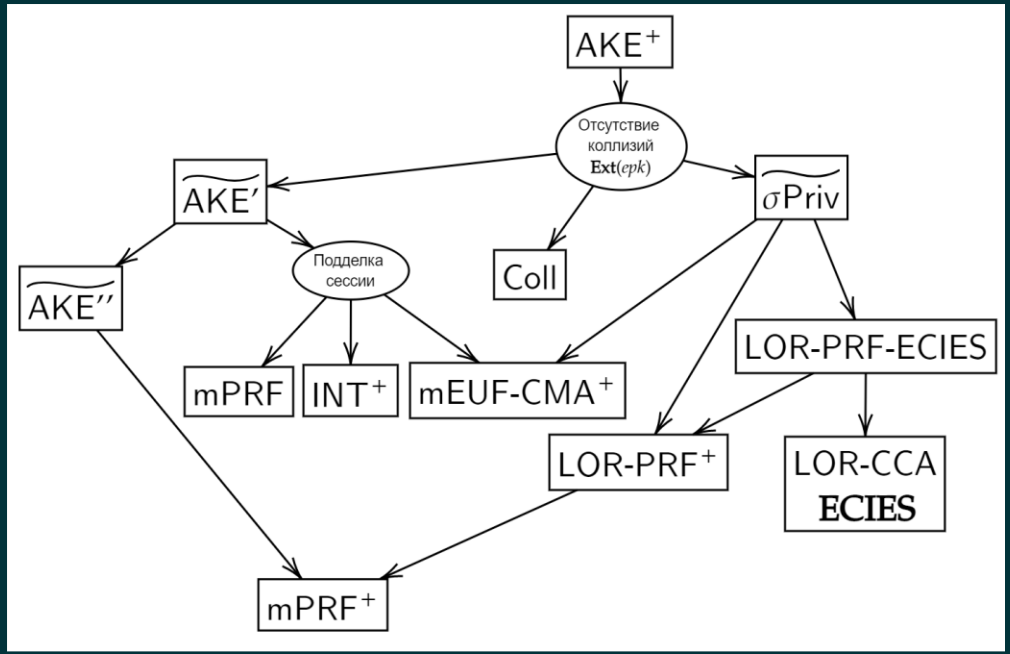




Анализ протокола

Стойкость протокола сводится к стойкости базовых задач в более простых моделях:

- задача Диффи-Хеллмана на ЭК (с доп. информацией)
- отличение блочного шифра от случайной подстановки
- отличение ключевой хэш-функции от случайной функции



Внедрение протокола 5G-AKA-GOST в РФ

- Добавление случайности пользователя: изменения в USIM и HSM отечественного производства (технологически осуществимо)

Внедрение протокола 5G-AKA-GOST в РФ

- Добавление функции хэширования Стрибог: изменения в мобильных терминалах, базовых станциях, производимых за рубежом (требуются технологические разработки)

Гармонизация протокола 5G-AKA-GOST с 3GPP

- Добавление случайности пользователя: по стандартам 3GPP соответствующие функции (механизм S3G) задаются операторами связи (сложно)

- Добавление функции хэширования Стрибог: предусмотрена только функция SHA-256, протокол не содержит полей для выбора хэш-функции (очень сложно)

Протокол 5G-AKA-GOST

- Схема ECIES остаётся без изменений, необходимо выполнять схему в сим-карте

- Открытый ключ UE (ТЭК из схемы ECIES) подаётся на вход механизма S3G, выполняемого в сим-карте

Протокол 5G-AKA-GOST

Необходима разработка алгоритма S3G-5G:

- добавление случайности UE
- изменение функции RES

- ускорение алгоритма?

V. A. Kiryukhin, “Keyed Streebog is a secure PRF and MAC”, *Матем. вопр. криптогр.*, **14**:2 (2023), 77–96

Протокол 5G-AKA-GOST

СПАСИБО ЗА ВНИМАНИЕ!

Степан Давыдов, АО «НПК «Криптонит» **s.davydov@kryptonite.ru**

Кирилл Царегородцев, АО «НПК «Криптонит» **k.tsaregorodtsev@kryptonite.ru**

Юрий Шкуратов, АО «НПК «Криптонит» **y.shkuratov@kryptonite.ru**