О некоторых результатах в области информационной безопасности перспективных сетей подвижной радиосвязи в Российской Федерации

Антон Науменко

ООО «СФБ Лаб», АО «ИнфоТеКС»

РусКрипто’2024
20-21 марта 2024

Anton.Naumenko@infotecs.ru

СФБ ЛАБ

Алгоритмы S3G-128 и S3G-256

Алгоритмы S3G-128 и S3G-256 основаны на хэш-функции Стрибог-512

$$\mathsf{S3G}(K, T) = \mathsf{H}(K|T)$$

Р 1323565.1.003-2017

Криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов, предназначенные для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи

Алгоритмы S3G-128 и S3G-256

S3G-128:

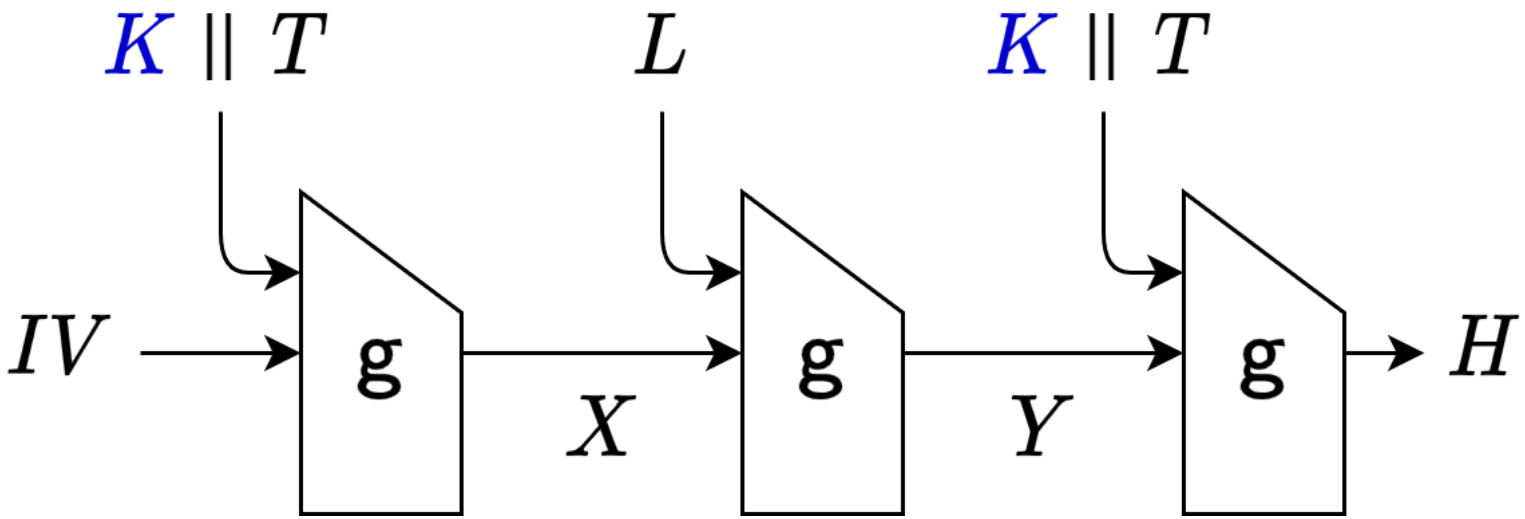
- ключ – 128 бит
- текст от 159 до 383 бит
- ключ и текст всегда помещаются **в один** 512-битный блок

S3G-256:

- ключ – 128 или 256 бит
- текст от 344 до 680 бит
- ключ и текст всегда помещаются **в два** 512-битных блока

Возможности ускорения алгоритма S3G

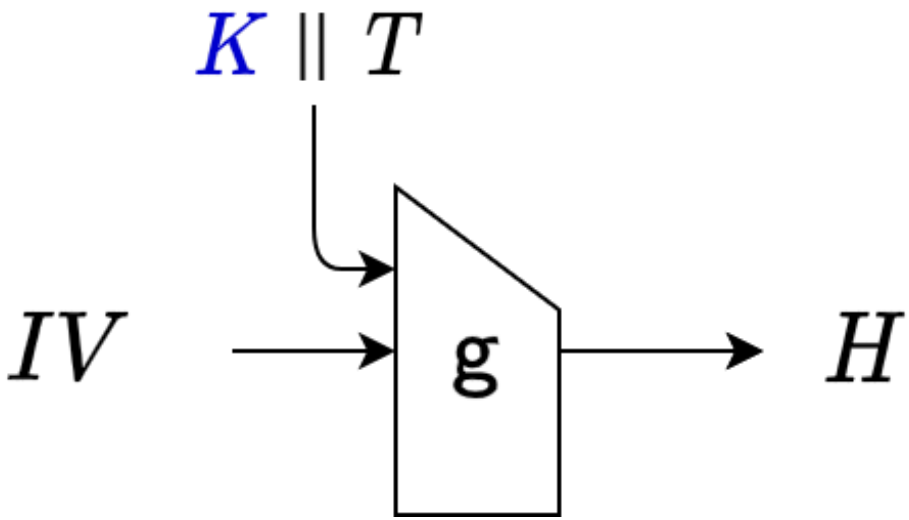
Алгоритм S3G-128



3 вызова функции сжатия:
– ключ и текст с учётом дополнения 10..0
– битовая длина
– контрольная сумма = единственному блоку

Усеченная версия

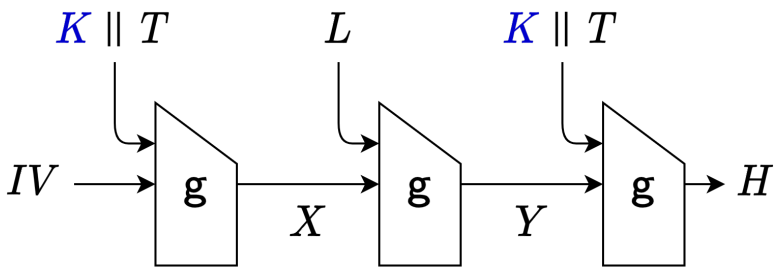
Идея: усечение S3G-128 с трёх до одного вызова функции сжатия g

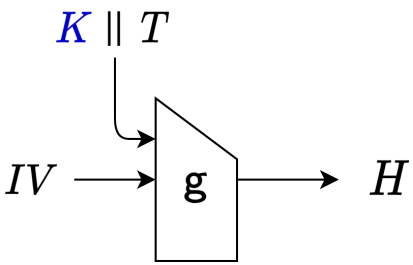


Кирюхин В.А.

О свойствах алгоритма S3G-128 при использовании усеченной хэш-функции «Стрибог» – Рускрипто 2022

Ускорение S3G-128





- ускорение в 3 раза
- стойкость остается на таком же уровне
- схожим образом можно ускорить S3G-256
- доложено на заседании РГ ТК 26 (апрель, 2022 год)

Необходимость исправления порядка байт в S3G

Пример для S3G-256

Рассмотрим вычисление H_0:

$$H_0 = \mathsf{S3G}(K, T) = \mathsf{H}(\underbrace{KV}_{K} | \underbrace{TOP|instance|inf_1|algoname256}_{T})$$

ключ $K \in V_{256}$
данные $T \in V_{344}$

Обработка блоков согласно ГОСТ 34.11-2018

Обработка начинается с **младших** байт текста, которые находятся в записи **справа**.

1. Дополнение до 1024 бит

$$\underbrace{0..01}_{424}|K|T$$

2. Разбиение на блоки

$$\underbrace{0...01|K_1}_{512} \mid \underbrace{K_2|T}_{512}$$

$K = K_1|K_2,$
$K_1 \in V_{88},$
$K_2 \in V_{168}$

Сначала обрабатывается блок $(K_2|T)$, затем $(0...01|K_1)$

Выводы

Ключ в S3G-256:

1. не находится в начале (относительно фактического порядка обработки)
2. разбивается на подблоки, каждый из которых обрабатывается на разных итерациях функции сжатия

S3G-128

СФБ ЛАБ

У S3G-128 ключ и данные всегда находятся в **единственном** блоке, но **позиции** байт ключа в этом блоке также **меняются** в зависимости от длины сообщения

Следствия

СФБ ЛАБ

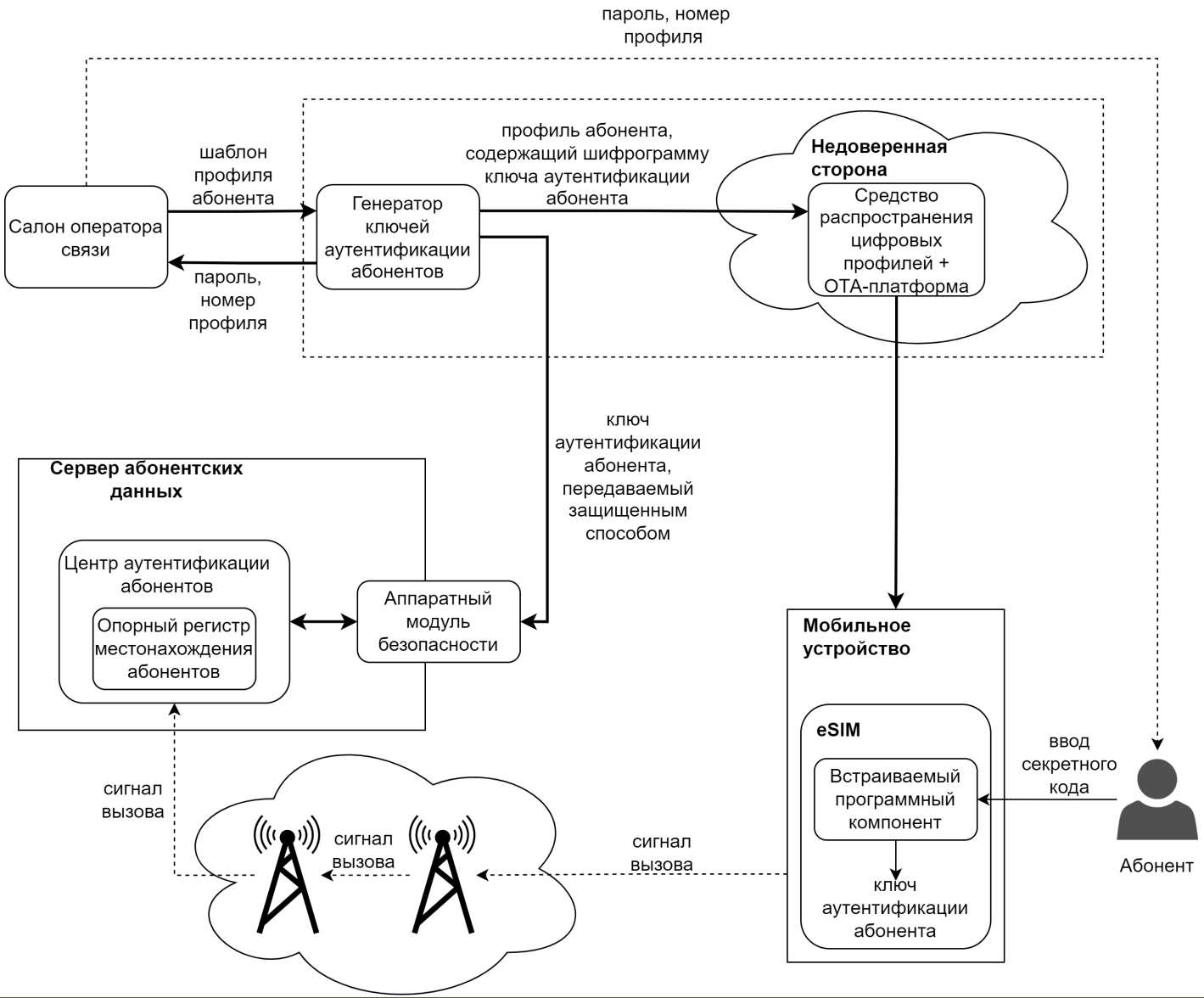
- Затрудняется обоснование как для конструктивного криптоанализа, так и с точки зрения «доказуемой стойкости»
- К хэш-функции неявно выдвигается требование «быть случайным оракулом»
- В общем случае (ключ длиннее 256 бит) появляются атаки на вскрытие ключа, более эффективные, чем универсальные

Что было сделано?

- о проблеме доложено на заседании РГ ТК 26 (апрель, 2023)
- проведено криптографическое исследование двух вариантов (ключ в начале, ключ в конце)
  $\Rightarrow$ обе версии допустимы, но первая предпочтительнее
- результаты исследований доложены на заседании РГ ТК 26 (октябрь, 2023)
- подготовлен обновленный проект Рекомендаций, обоснование стойкости, эталонная реализация

Особенности моделей угроз для участников перспективной системы ПРС

Система доверенной аутентификации абонентов



Заключение

1. Разработан механизм ускорения реализации S3G

Заключение

1. Разработан механизм ускорения реализации S3G
2. КС3 для Sim/eSim может быть уточнена для сценариев атак с привлечением владельца/легального пользователя мобильного устройства

Заключение

СФБ ЛАБ

1. Разработан механизм ускорения реализации S3G
2. КС3 для Sim/eSim может быть уточнена для сценариев атак с привлечением владельца/легального пользователя мобильного устройства
3. Актуальной с точки зрения развития систем ПРС кажется идея выпустить отдельные требования именно для случая использования мобильных устройств (предложения Регулятора, Рускрипто‘21)

Благодарю за внимание!

Антон Науменко

ООО «СФБ Лаб», АО «ИнфоТеКС»
РусКрипто’2024
20-21 марта 2024
Anton.Naumenko@infotecs.ru