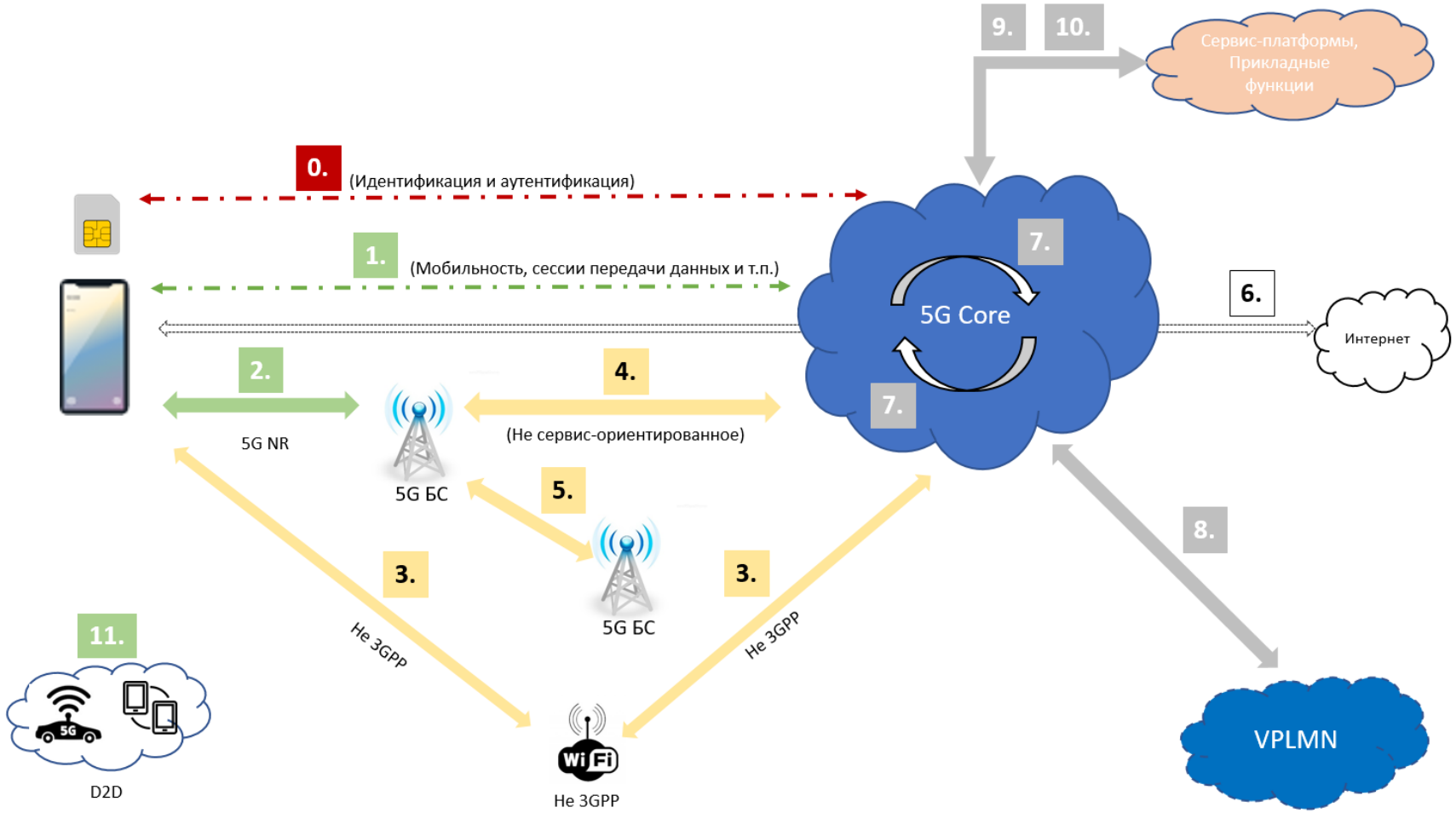
Сегменты криптографической защиты в сетях ПРТС 5-го поколения

А.А. Чичаева, Р.И. Самохвалов

КРИПТОНИТ

Сегменты криптографической защиты в сетях 5G

0	Идентификация и аутентификация абонента	ECIES + 5G-AKA
1	Управления мобильностью, сессиями передачи данных, SMS, местоположением (NAS-сообщений)	NEA, NIA
2	Доступ к ресурсам сети через радиоподсистему 3GPP	NEA, NIA
3	Доступ к ресурсам сети через не-3GPP сети	IPSec
4	Не сервис-ориентированного взаимодействия элементов опорной сети	IPSec
5	Взаимодействия между базовыми станциями (интерфейсы Xn, F1, E1)	IPSec
6	Обмен данными абонентского устройства с внешними сетями (в т.ч. Интернет и IMS)	не актуально
7	Сервис-ориентированного взаимодействия элементов опорной сети	TLS
8	Межоператорское взаимодействие	TLS
9	Обмена данными с прикладными функциями оператора связи или внешними прикладными функциями	TLS
10	Предоставление бизнес-услуг	TLS
11	Взаимодействия между устройствами (V2X, ProSe)	возможно использовать NEA, NIA, необходимо распределить ключи



Сегменты защиты и используемые алгоритмы

- **Зелёный цвет** — ведётся разработка соответствующих механизмов.

- **Синий цвет** — необходимо запланировать разработку в первую очередь.

- **Красный цвет** — разработка не актуальна.

- **Жёлтый цвет** — разработка не актуальна на текущий момент, но может быть проведена во вторую очередь.

0	Идентификация и аутентификация абонента	ECIES + 5G-AKA
1	Управления мобильностью, сессиями передачи данных, SMS, местоположением (NAS-сообщений)	NEA, NIA
2	Доступ к ресурсам сети через радиоподсистему 3GPP	NEA, NIA
3	Доступ к ресурсам сети через не-3GPP сети	IPSec
4	Не сервис-ориентированного взаимодействия элементов опорной сети	IPSec
5	Взаимодействия между базовыми станциями (интерфейсы Xn, F1, E1)	IPSec
6	Обмен данными абонентского устройства с внешними сетями (в т.ч. Интернет и IMS)	не актуально
7	Сервис-ориентированного взаимодействия элементов опорной сети	TLS
8	Межоператорское взаимодействие	TLS
9	Обмена данными с прикладными функциями оператора связи или внешними прикладными функциями	TLS
10	Предоставление бизнес-услуг	TLS
11	Взаимодействия между устройствами (V2X, ProSe)	возможно использовать NEA, NIA, необходимо распределить ключи

IPSec в сетях 5G

КРИПТОНИТ

1. Взаимодействия между базовыми станциями (интерфейсы Xn, F1, E1).
2. Не сервис-ориентированное взаимодействие элементов опорной сети.
3. Передача данных при подключении через не-3GPP сети доступа.

Протокол IKEv2

Профиль определен в 3GPP TS 33.310.

Основывается на RFC 7296 и RFC 8247.

Должны поддерживаться следующие алгоритмы:

- Конфиденциальность: AES-GCM на базе AES-128
- PRF_HMAC_SHA2_256
- Целостность: AUTH_HMAC_SHA256_128
- Diffie-Hellman Group 19 (256-bit random)

Могут поддерживаться следующие алгоритмы:

- Конфиденциальность: AES-GCM на базе AES-256
- PRF_HMAC_SHA2_384
- Diffie-Hellman group 20 (384-bit random)
- Diffie-Hellman group 31 (Curve25519)

Протокол ESP

Профиль определен в 3GPP TS 33.210.

- Соответствует RFC 4303
- Туннельный режим – обязательный, Транспортный режим – опциональный
- Криптографические механизмы из RFC 8221
- Должен поддерживаться AES-GMAC на базе AES-128

Протокол IKEv2

Р 1323565.1.048–2023 «Информационная технология. Криптографическая защита информации. Использование российский криптографических алгоритмов в протоколе обмена ключами в сети Интернет версии 2 (IKEv2)»

Трансформы:

PRF_HMAC_STREEBOG_512

GOST3410_2012_256

GOST3410_2012_512

Протокол ESP

Р 1323565.1.035–2021 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе защиты информации ESP»

Трансформы:

ENCR_KUZNYECHIK_MGM_KTREE

ENCR_MAGMA_MGM_KTREE

DTLS в 3GPP

В дополнение к IPsec может поддерживаться **DTLS** для интерфейсов взаимодействия базовых станций: E1, Xn-C, F1-C.

- Профиль определен в 3GPP TS 33.210
- Профиль сертификата определен в 3GPP TS 33.310
- DTLS должен соответствовать RFC 6083 и RFC 6347

DTLS в России

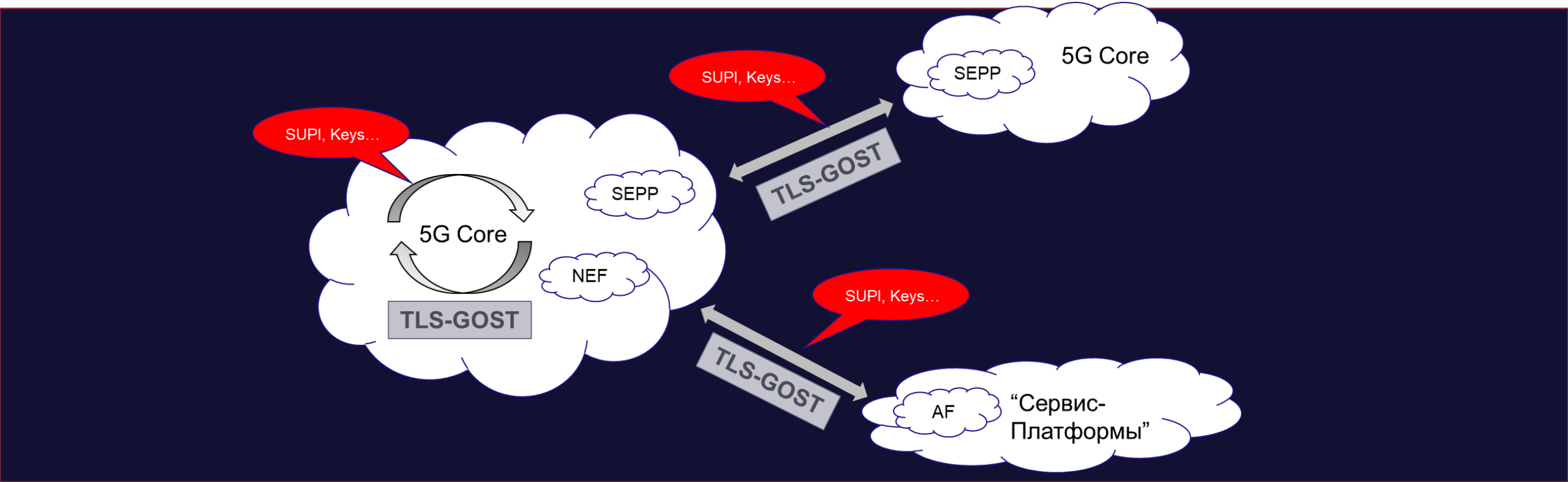
Ведется разработка методических рекомендаций:

«Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в датаграммном протоколе безопасности транспортного уровня (DTLS 1.2) С описанием профилей для индустриальных систем»

TLS в сетях 5G

КРИПТОНИТ

1. Взаимодействие элементов опорной сети по сервис-ориентированным интерфейсам (SBI)
2. Межоператорское взаимодействие
3. Обмен данными с прикладными функциями



TLS в 3GPP

Профиль определен в 3GPP TS 33.210.

- TLS 1.2 должен быть определен как в RFC 5246
- TLS 1.3 должен быть определен как в RFC 8446

TLS в России

Р 1323565.1.020-2020 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)»

Р 1323565.1.030-2020 «Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3)»

Алгоритмы NEA/NIA

КРИПТОНИТ

Алгоритмы из **семейства NEA/NIA** (new encryption algorithm, new integrity algorithm) используются в сетях пятого поколения (5G).

Алгоритмы NEA/NIA обеспечивают свойства:

- Конфиденциальность
- Целостность

Участники информационного обмена

КРИПТОНИТ

1 **NAS, Non Access Startum**

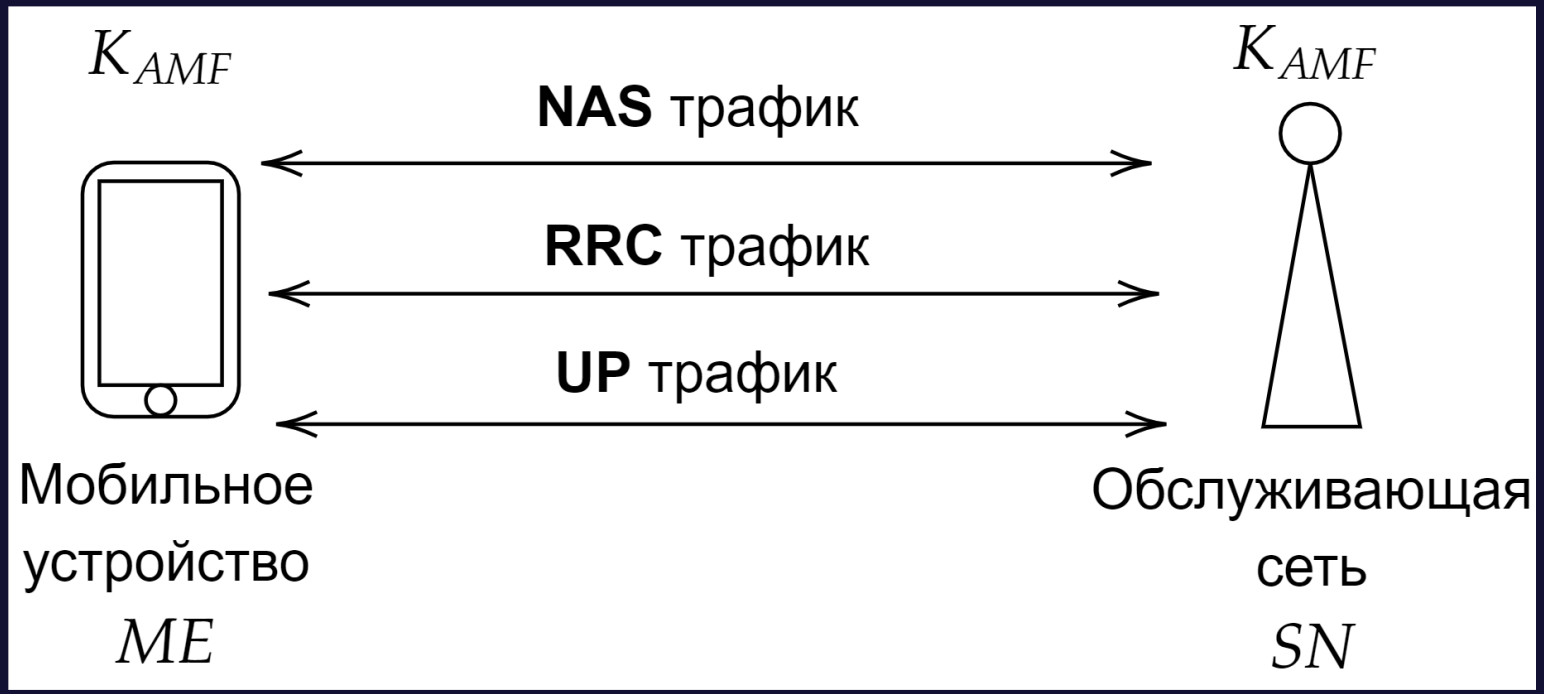
- протоколы для сигнального трафика между оборудованием абонента и ядром 5G

2 **RRC, Radio Resource Control**

- протокол управления радиоресурсами

3 **UP, User Plane**

- пользовательский трафик



Стандарты для сотовой связи

КРИПТОНИТ

3GPP TS 33.501 – архитектура безопасностей сетей 5G

NEA1/NIA1	SNOW 3G
NEA2/NIA2	AES
NEA3/NIA3	ZUC
NEA7/NIA7	Кузнечик

[1] 3GPP TS 33.501 (2022). Security architecture and procedures for 5G system. V18.0.0.

Алгоритмы NEA/NIA

КРИПТОНИТ

$$NEA(P) \parallel NIA(P) = ENC(K_e, IV, P) \parallel MAC(K_i, IV \parallel P)$$

≈

Encrypt and MAC

Нестойкий ???

Алгоритмы NEA/NIA

КРИПТОНИТ

$$NEA(P) \parallel NIA(P) = ENC(K_e, IV, P) \parallel MAC(K_i, IV \parallel P)$$

$$IV = COUNT \parallel BEARER \parallel DIR \parallel 0^{26}$$

- $COUNT$ – 32-битовый счетчик соединений
- $BEARER$ – 5-битовый идентификатор виртуального соединения
- DIR – 1 бит, указывающий направление передачи данных (к абоненту / от абонента)

Алгоритмы NEA/NIA на основе российских алгоритмов

КРИПТОНИТ

$$NEA(P) \parallel NIA(P) = ENC(K_e, IV, P) \parallel MAC(K_i, IV \parallel P)$$

- Enc – блочный шифр Кузнечик в режиме гаммирования CTR [2]
- MAC – блочный шифр Кузнечик в режиме выработки имитовставки $OMAC1$ [2]
- $HMAC$ – конструкция $HMAC_{256}$ [3] на основе хэш-функции Стрибог

[2] ГОСТ 34.13 – 2018 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров.
[3] Р 50.1.113 – 2016 Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования

Описание алгоритмов NEA/NIA

КРИПТОНИТ

Схема шифрования $\mathcal{SE}$ – тройка (**Kgen, Enc, Dec**):

- **Kgen –** вероятностный алгоритм, возвращающий случайно выбранный ключ K
- Алгоритм **Enc** принимает на вход ключ K, вектор инициализации IV, сообщение m и возвращает шифртекст $ct \leftarrow Enc_K^{IV}(m)$
- Алгоритм **Dec** принимает на вход ключ K, вектор инициализации IV, шифртекст ct и возвращает отрытый текст $\mathrm{m} \leftarrow Dec_K^{IV}(ct)$

Свойство корректности: для любых K, IV, m выполнено $Dec_K^{IV}\left(Enc_K^{IV}(m)\right) = m$

Схема выработки имитовставки $\mathcal{MA}$ – тройка (**Kgen, Tag, Vfy**):

- **Kgen –** вероятностный алгоритм, возвращающий случайно выбранный ключ K
- Алгоритм **Tag** принимает на вход ключ K, сообщение m и возвращает имитовставку $\tau \leftarrow Tag_K(m)$
- Алгоритм **Vfy** принимает на вход ключ K, сообщение m , а также имитовстаку τ и возвращает результат проверки имитовставки $b \leftarrow Vfy_K(m, \tau) \in \{0,1\}$

Свойство корректности: для любых K, m выполнено $Vfy_K(m, Tag_K(m)) = 1$

Описание алгоритмов NEA/NIA

Алгоритмы NIA/NEA $\mathcal{AE}$ следующая тройка:

- **Алгоритм генерации ключа** $\mathcal{AE}.KGen$ выбирает пару независимых ключей $K_e \leftarrow \mathcal{SE}.KGen$ и $K_i \leftarrow \mathcal{MA}.KGen$ и возвращает $\mathrm{K} \leftarrow (K_e, K_i)$
- **Алгоритм зашифрования** $\mathcal{AE}.Enc_K^{IV}$
- **Алгоритм расшифрования** $\mathcal{AE}.Dec_K^{IV}$

$\mathcal{AE}.\mathbf{Enc}_K^{IV}(m)$

$K_e, K_i \leftarrow K$

$ctxt \leftarrow \mathcal{SE}.\mathbf{Enc}_{K_e}^{IV}(m)$

$\sigma \leftarrow \mathcal{MA}.\mathbf{Tag}_{K_i}(IV \,\|\, m)$

$ct \leftarrow ctxt \,\|\, \sigma$

return ct

$\mathcal{AE}.\mathbf{Dec}_K^{IV}(ct)$

$K_e, K_i \leftarrow K$

$ctxt, \tau \leftarrow ct$

$m \leftarrow \mathcal{SE}.\mathbf{Dec}_{K_e}^{IV}(ctxt)$

$\sigma \leftarrow \mathcal{MA}.\mathbf{Tag}_{K_i}(IV \,\|\, m)$

if $\sigma \neq \tau$

  return $\perp_{MAC}$

fi

return m

Модель противника

КРИПТОНИТ

Угрозы, формализуемые моделью:

- Нарушение конфиденциальности
- Нарушение целостности
- Криптографическая привязка параметров, от которых зависит IV к шифртексту

Угрозы, не рассматриваемые моделью:

- Нарушение порядка сообщений
- Устойчивость к повторам IV
- Целостность при возможности частичного расшифрования шифртекста
- Атаки с использованием побочных каналов

Модель IND-CCA3

$\mathbf{Exp}^{\text{IND-CCA3-}b}_{\mathcal{AE}}(\mathcal{A})$

$K \leftarrow\$ \mathcal{AE}.\mathbf{KGen}()$
$params \leftarrow \emptyset$
$sent \leftarrow \emptyset$
$b' \leftarrow\$ \mathcal{A}^{O^b_{\text{enc}}, O^b_{\text{dec}}}$
return b'

$O^b_{\text{dec}}(IV, ct)$

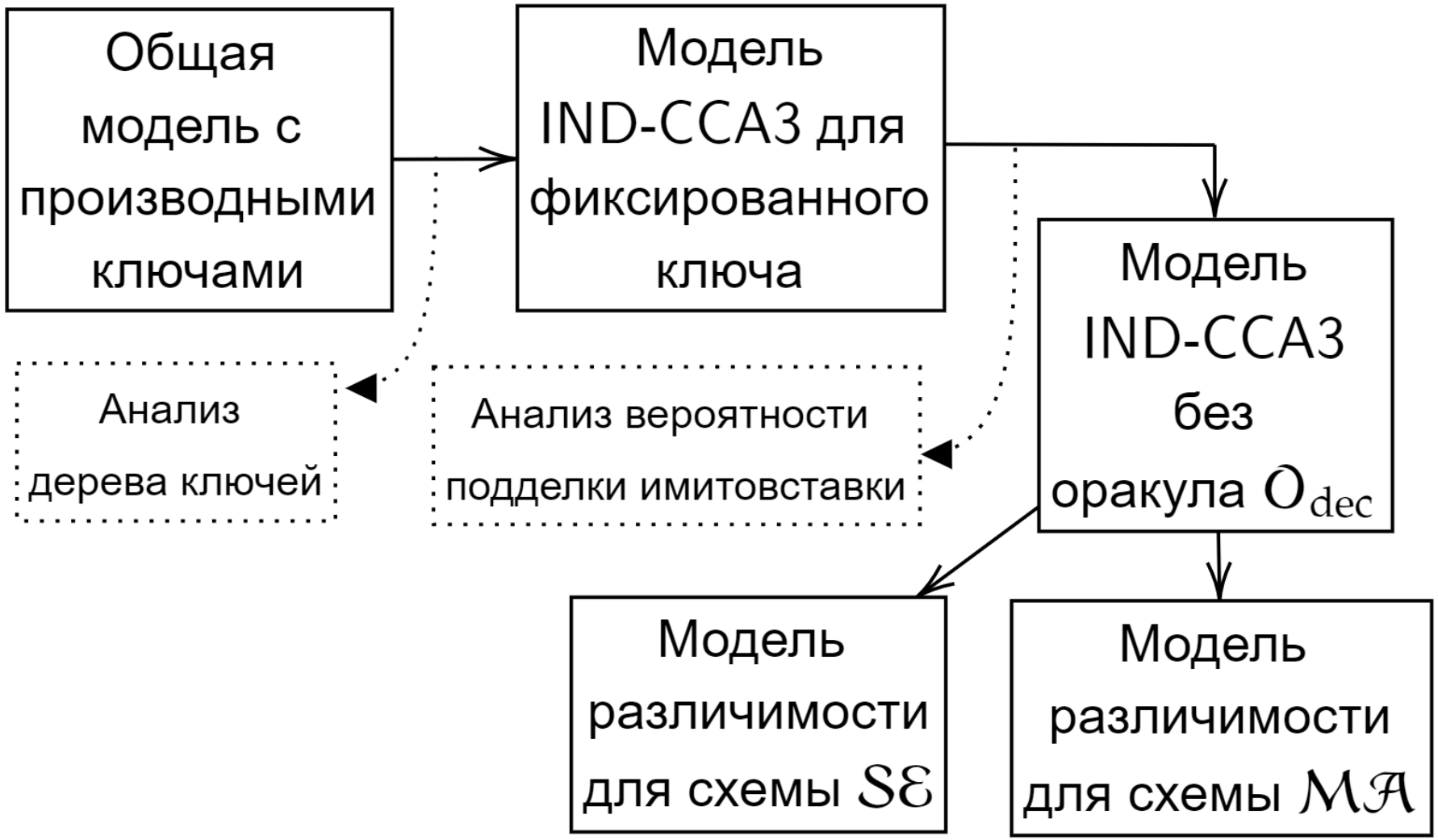
$m \leftarrow \mathcal{AE}.\mathbf{Dec}^{IV}_K(ct)$
$par \leftarrow \mathbf{Parse}(IV)$
if $((par, ct) \in sent)\,\text{OR}(b = 0)$
  $m \leftarrow \perp$
fi
return m

$O^b_{\text{enc}}(IV, m_0, m_1)$

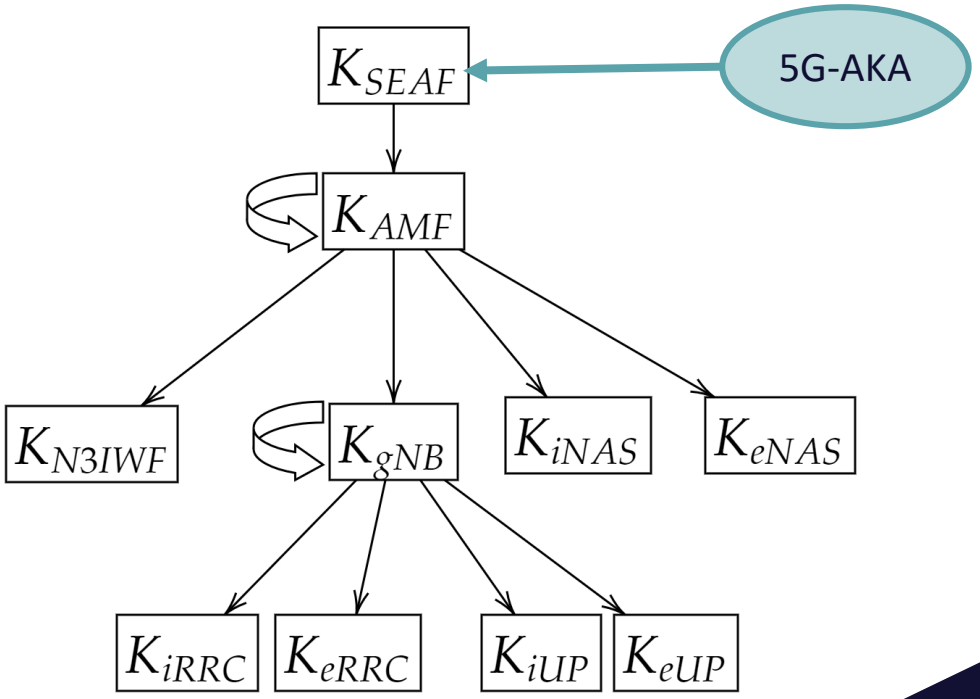
$par \leftarrow \mathbf{Parse}(IV)$
if $par \in params$
  return $\perp$
fi
$ct \leftarrow \mathcal{AE}.\mathbf{Enc}^{IV}_K(m_b)$
$sent \leftarrow sent \cup \{(par, ct)\}$
$params \leftarrow params \cup \{par\}$
return ct

Анализ алгоритмов NEA/NIA

КРИПТОНИТ



Ключевое дерево



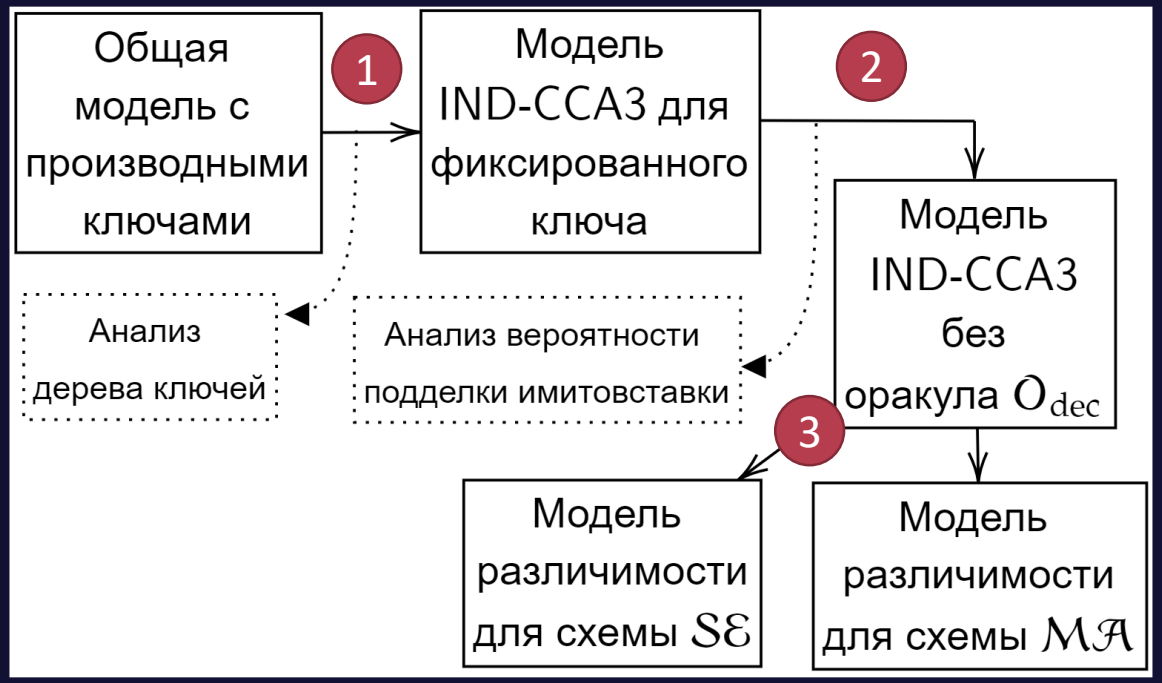
Производные ключи вырабатываются на основе псевдослучайной функции $\mathcal{F}$:

$$K_Y \leftarrow \mathcal{F}(K_X, S_X)$$

где S_X - константа, зависящая от характеристик соединения и типа трафика

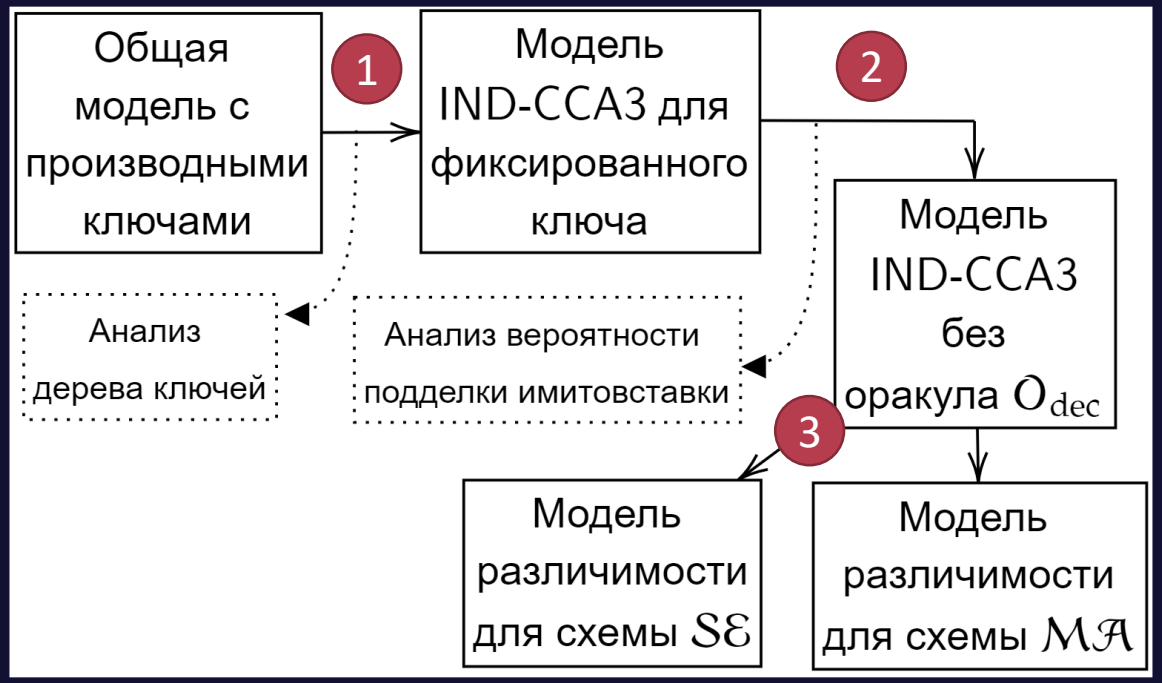
Анализ алгоритмов NEA/NIA

1. С помощью техники «гибридного аргумента» перейти к модели с фиксированным ключом



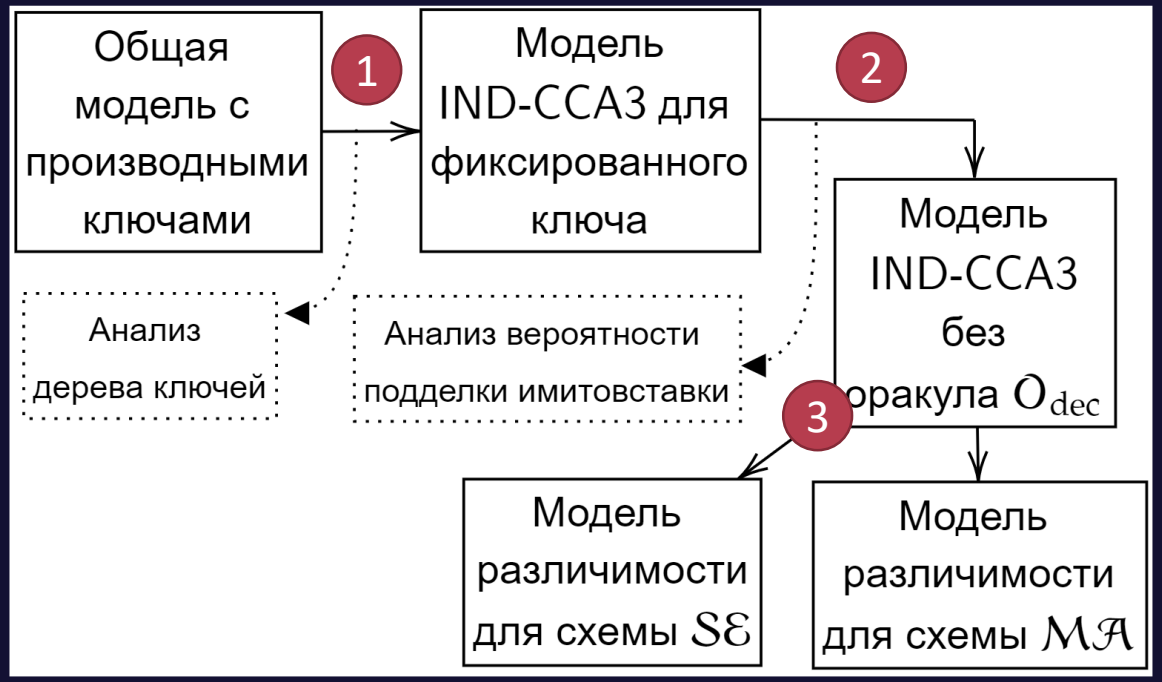
Анализ алгоритмов NEA/NIA

1. С помощью техники «гибридного аргумента» перейти к модели с фиксированным ключом
2. Исключить оракул O_{dec} в модели IND-CCA3 из рассмотрения



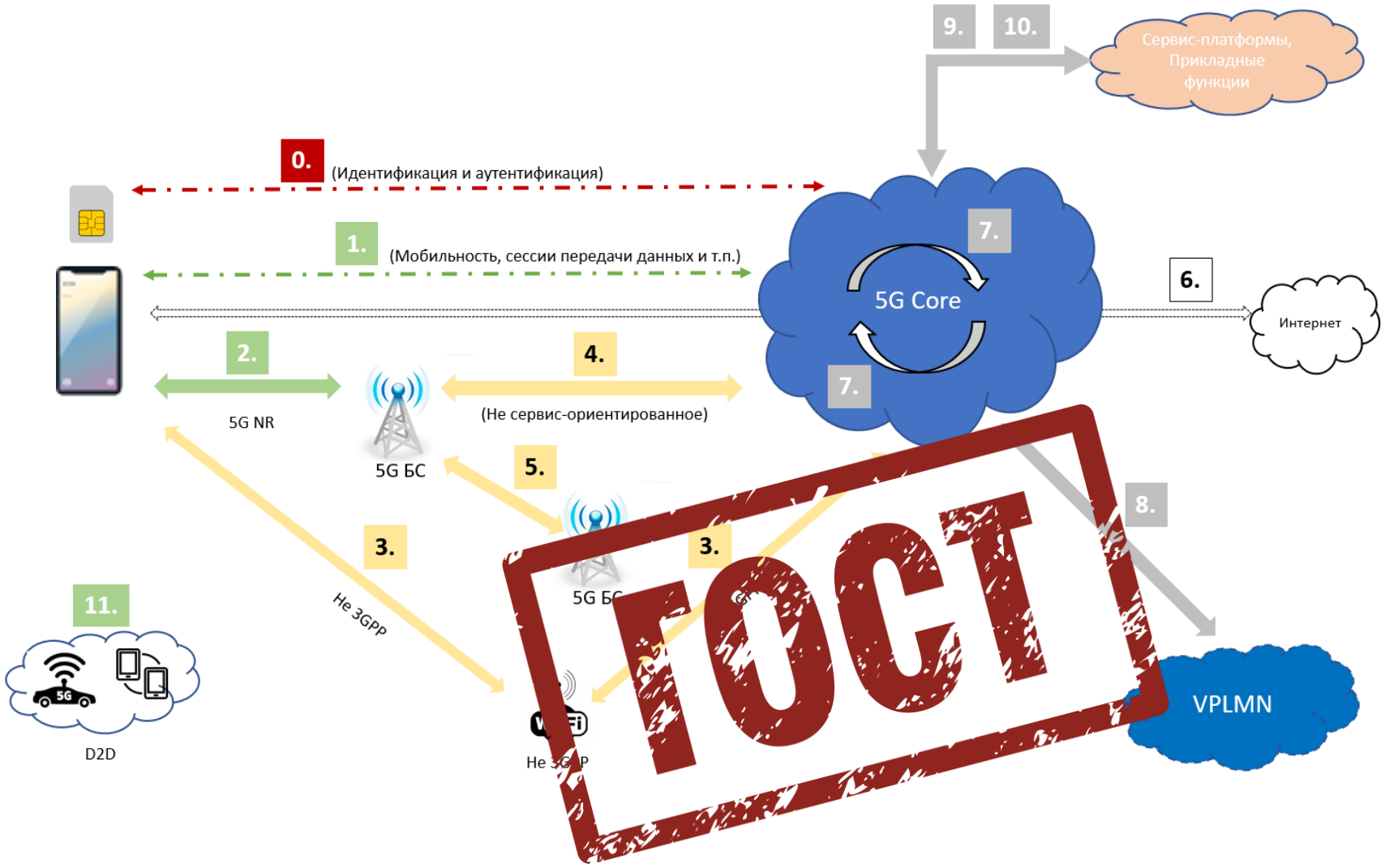
Анализ алгоритмов NEA/NIA

1. С помощью техники «гибридного аргумента» перейти к модели с фиксированным ключом
2. Исключить оракул O_{dec} в модели IND-CCA3 из рассмотрения
3. С помощью техники «гибридного аргумента» разбить модель на две подмодели: LOR-CPNA и PRF



Сегменты криптографической защиты в сетях 5G

КРИПТОНИТ



Спасибо за внимание!

Авторы доклада:

Чичаева Анастасия

Специалист-исследователь,
Лаборатория криптографии
a.chichaeva@kryptonite.ru

Самохвалов Роман

Специалист-исследователь в области телекоммуникаций,
Лаборатория телекоммуникаций и спецтехники
r.samokhvalov@kryptonite.ru