# Еще раз о важности построения модели противника на примере протокола аутентификации 5G-AKA

Царегородцев Кирилл

Специалист-исследователь,
Лаборатория криптографии

Рускрипто’2022

КРИПТОНИТ

# Основные моменты

1. Приватность в 5G (объект изучения)

2. Доказуемая стойкость

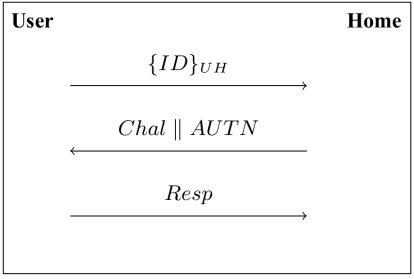
3. Модели в общем и криптографические

# Приватность в 5G (объект изучения)

# Очень кратко о 5G-AKA

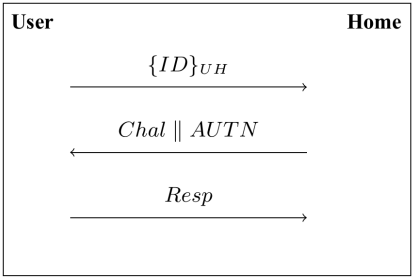
- Протокол аутентификации + аутентифицированной выработки общего ключа (AKE-протокол).
- Основное «тело» — три шага: идентификация (передача $ID$), запрос, ответ.
- Идейное продолжение протокола 4G (обратная совместимость).

# Высокоуровневое описание 5G-AKA




Поля $Chal$ и $AUTN$ не зависят от случайности со стороны пользователя $User$.

# Проблема: возможность replay-атак

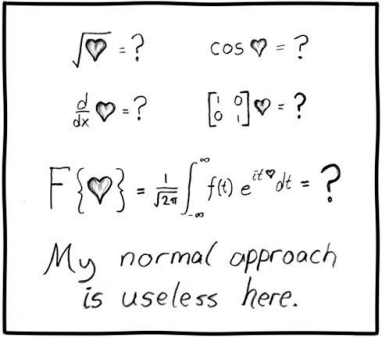



- Можно посылать «старые» $Chal$ и $AUTN$ и по коду ошибок различать пользователей.
- Практическое развитие идеи: атака LFM.
- Следствие: «приватность» под угрозой.

# Что думает 3GPP о приватности?

**[TS 133.102, Sec. 5.1.1]** (3G) 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.




[1] A Formal Analysis of 5G Authentication, D. Basin et. al.

# Неотслеживаемость (untraceability)

**TS 133.102**

*an intruder cannot deduce whether different services are delivered to the same user by eavesdropping*

1. То есть противник только пассивный? почему?
2. Что значит “не может определить”? устраивает ли нас ситуация, в которой определяет половину “цифр” в номере телефона?
3. Если “не получает никакой информации”, то что конкретно это значит?
   - Все сообщения в протоколе неотличимы от случайных бит (IND).
   - Все сообщения в протоколе можно промоделировать, не зная долговременных секретов (ZK).
   - Противник не может определить, с каким из двух участников он общается в данный момент времени (LOR).

# Пример: 5G-AKA

Подход 3GPP: у нас есть конкретная атака? Мы будем ставить конкретную заплатку в протоколе, защищающую от конкретной атаки.

**3GPP TR 33.846**

In case the linkability attack occurs, it represents a breach of the user's untraceability, the attacker can establish the traceability of a subscriber based on the study of the failure messages and can detect subscriber's presence in a specific area by replaying one old legitimate authentication vector.

**3GPP TR 33.846**

The 5G system shall support mechanisms to mitigate the linkability attacks.

# Пример: 5G-AKA

Подход 3GPP: у нас есть конкретная атака? Мы будем ставить конкретную заплатку в протоколе, защищающую от конкретной атаки.

**3GPP TR 33.846**

The 5G system should support mechanisms to mitigate SUCI based attacks.

**3GPP TR 33.846**

The 5G system should provide the mechanism to mitigate SUPI guessing attacks.

**3GPP TR 33.846**

The protection of SQN during AKA re-synchronisations should prevent the information leakage of SQN values.

**Kryptonite, SA3 106e meeting communication**

We believe that the main goal of this work is to develop a secure authentication protocol that allows you to deal with both currently known vulnerabilities and potentially possible but not yet found attacks. And the only sufficient guarantee is the security proof in some relevant adversary model (for authentication, privacy, key exchange, e.g.).

**SA3 106e meeting communication**

This “potentially possible but not yet found attacks.” sounds like a trip into a rabbit hole. When will you know that all or majority of “potentially possible but not yet found attacks” are covered in the study? In fact, what you are proposing is not dissimilar to studying “undetected breakins.”

**SA3 106e meeting communication**

Objectives shall also specify measurable goals allowing, e.g., the determination that the goals are met.

# Цикл разработки протокола

Немного обобщая, можно утверждать, что негласно принят следующий цикл разработки протокола:

1. Неформальные требования;
2. протокол с неформальным доказательством;
3. конкретные атаки (уязвимости);
4. новые ad-hoc требования по результатам анализа уязвимостей;
5. “латание дыр”: новые протоколы с неформальным доказательством;
6. ???
7. PROFIT!

# Чем такой подход плох?

- Неявные (не артикулированные) цели, ресурсы, предположения;
- Нет переиспользования опыта;

# Цели, ресурсы, предположения

Неявные (не артикулированные) цели, ресурсы, предположения;

- Одни эксперты будут склонны считать, что свойство «бессмысленно», и его необходимо исключить из рассмотрения…
- … в то время как другие будут предлагать решения, исходя из их понимания угрозы.

# Цели, ресурсы, предположения

*«… The attacker could generate valid SUCI* ***only if he knows the home network public key*** *associated to the subscription…»*


***«… The cell area is very big so it is difficult to trace the UE…»***

*«…encrypt the AUTS/random number and failure code, and the AUSF uses the $K_{AUSF}$ stored during previously successful authentication to decrypt the AUTS/random number and failure code. … If no stored $K_{AUSF}$,* ***the KEY is a 256-bit binary string of all 0s»***

[1] Вопросы разработки и стандартизации отечественных криптографических алгоритмов и протоколов в сетях связи 5G, Е. Грибоедова, CTCrypt2021

# Цели, ресурсы, предположения


| Key Issues | Security threats | Comments |
|---|---|---|
| Key Issue #2.1: Linkability by distinguishing MAC failure and synchronization failure | Traceability of the user/victim by IMSI-probing when an attacker tries to find out whether the subscriber with this identity is present in a given area. | Overall impact of the attack is low as it is only one of multiple IMSI probing type attacks that can be launched and so preventing this particular attack would not resolve the overall issue. |
| Key Issue #2.2: Linkability by SUCI replay | Traceability of the user/victim by IMSI-probing when an attacker tries to find out whether the subscriber with this identity is present in a given area. | Overall impact of the attack is low as it is only one of multiple IMSI probing type attacks that can be launched and so preventing this particular attack would not resolve the overall issue. |
| Key Issue #2.2: Linkability by generation of different SUCIs | Traceability of the user/victim by IMSI-probing when an attacker tries to find out whether the subscriber with this identity is present in a given area. | Overall impact of the attack is low as it is only one of multiple IMSI probing type attacks that can be launched and so preventing this particular attack would not resolve the overall issue. |
| Key Issue #2.2: DoS attack | DoS attack on UDM | Overall impact of this attack is low. |

Модель нарушителя до сих пор не согласована до конца: выдвигается предложения вычеркнуть основные угрозы 2.1, 2.2 и 3.2, поскольку есть более простые способы их реализовать (imsi paging).

[1]Вопросы разработки и стандартизации отечественных криптографических алгоритмов и протоколов в сетях связи 5G, Е. Грибоедова, CTCrypt2021

# Опыт, сын ошибок трудных

Нет переиспользования опыта.

- Многие трудности (на практике) неявно «закодированы» в общепризнанных моделях.
- Изучение безопасности для конкретного протокола без рассмотрения его в более общем контексте можно избыточно сузить рассматриваемые угрозы.

  *When will you know that all or majority of “potentially possible but not yet found attacks” are covered in the study?*

Именно тогда, когда получено доказательство в какой-либо общепризнанной модели для AKE-протоколов, для приватности и т.д.

# Доказуемая стойкость

# Что под этим понимает докладчик

- Формальная модель противника: тип атаки (возможности по взаимодействию с системой) + модель угрозы (какую задачу противник решает) + вычислительные ресурсы.
- Сведение анализа безопасности общей (интегрированной) системы (здания) к анализу безопасности “примитивов” (кирпичей).
- Использование “точных оценок”, а не асимптотик.

[1] Об одном подходе к формализации задач криптографического анализа, Алексеев Е.К. и др., Матем. вопр. криптогр. (в печати)

# Не единственный возможный подход к формализации

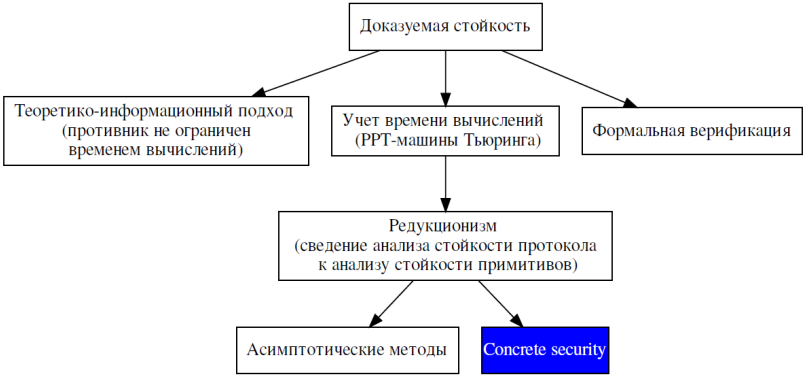


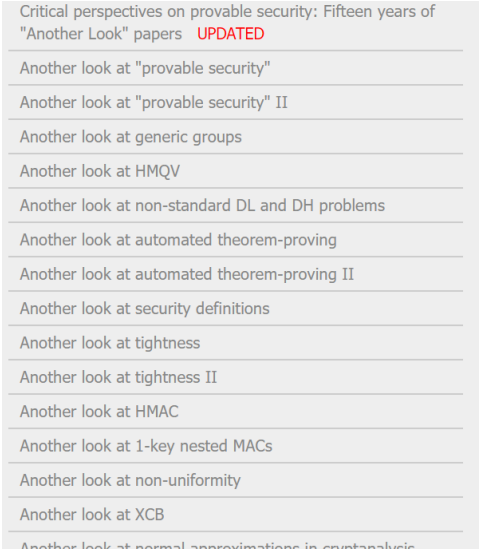

**Рис. 1:** Подходы к формализации

# Не панацея

1. Интерпретация в духе абсолютной стойкости даёт избыточно оптимистичные результаты (“нами был взломан доказуемо стойкий протокол”).
2. Ограничения в используемой «технике», сложности доказательства — дают избыточно пессимистичные результаты (forking lemma как пример).
3. Очень чувствительны к изначальным предположениям, вплоть до “незначительных” изменений.
4. Чувствительны к «композициям»: «стойкий» $P_1$ + «стойкий» $P_2$ может привести к «нестойкому» $P_3$.
5. Не всегда легко интерпретировать результаты.
6. Малопонятные модели, сложные доказательства.

# «И вообще в корне неверный»

- Различные идеализации (random oracle, ideal cipher, generic group, ...).
- Очень странные предположения о сложности задач.




[1]Another Look at Provable Security, Neal Koblitz and Alfred Menezes, https://www.math.uwaterloo.ca/ ajmeneze/anotherlook/index.shtml

# Кратко о предположениях



[1] Final Report on Main Computational Assumptions in Cryptography, K.U.Leuven

# Модели в общем и криптографические

# А что про другие модели?

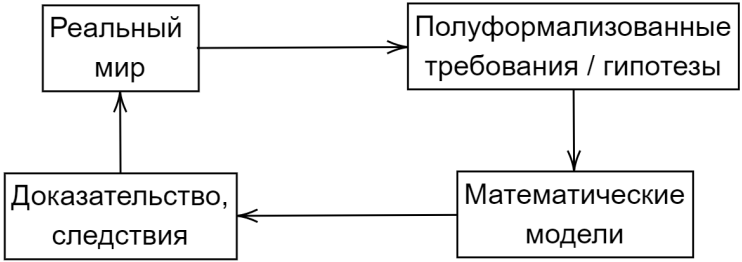



**Рис. 2:** Все стрелки в диаграмме, кроме одной, являются «неоднозначными»

# “В предыдущих сериях”


**Рис. 3:** И тут все стрелки «неоднозначны»

[1] Что плохого можно сделать, неправильно используя криптоалгоритмы, Алексеев Е.К., СТСrypt2019

# А есть ли “правильные” модели?

**George Box**

All models are wrong, but some are useful

- Вопрос, является ли модель правильной, бессмысленный — все модели игнорируют какие-либо аспекты «реальности».
- Таким образом, по определению любая модель неверна.
- Тем не менее, некоторые из них полезны (для некоторых частных ситуаций).

# А есть ли “правильные” модели?

**Richard McElreath, Statistical rethinking**

All statistical modeling has these same two frames: the small world of the model itself and the large world we hope to deploy the model in. Navigating between these two worlds remains a central challenge of statistical modeling. <...>

**Richard McElreath, Statistical rethinking**

The small world is the self-contained logical world of the model. Within the small world, all possibilities are nominated. There are no pure surprises, like the existence of a huge continent between Europe and Asia. Within the small world of the model, it is important to be able to verify the model’s logic, making sure that it performs as expected under favorable assumptions.

# Ещё немного о большом и малом мирах

**Richard McElreath, Statistical rethinking**

The large world is the broader context in which one deploys a model. In the large world, there may be events that were not imagined in the small world. Moreover, the model is always an incomplete representation of the large world, and so will make mistakes, even if all kinds of events have been properly nominated.

**Richard McElreath, Statistical rethinking**

The logical consistency of a model in the small world is no guarantee that it will be optimal in the large world.

# В переложении на криптографию

- **Small world** = формальная модель противника.
- **Large world** = реальная система, в которую встраивается протокол.
- **Ложноположительность:** не все атаки, описываемые в рамках формальной модели, переводятся в реальные атаки на криптосистему.
- **Ложноотрицательность:** если протокол является стойким в некоторой модели, то это не означает стойкости в некотором «абсолютном» смысле, только в рамках той модели, в которой получено доказательство.
- Интерпретация: «Недостаточно свидетельств для того, чтобы опровергнуть гипотезу о том, что протокол безопасен».

# Ложноположительное? Пример 1

- Конфиденциальность режима шифрования.
- IND: зашифрованный текст неотличим от случайных бит.
- LOR: зашифрование двух текстов дает неразличимые результаты.
- Есть примеры режимов шифрования, стойких в LOR-, но не в IND-смысле.
- Переводится ли угроза в модели IND в какую-либо реальную атаку на конфиденциальность режима шифрования?

# Ложноположительное? Пример 2

**On Privacy for RFID, S. Vaudenay**

Hence, our proof that IND-CCA security is not sufficient shows that the PKC protocol can be wide-strong private in the HPVP11 sense but not in the OV12 sense. <...> However, looking closer at what it means in practice, we can wonder to what extend the proof that IND-CCA security is not enough for OV12 privacy implies any privacy threat. Indeed, the inability to simulate the Result oracle in our counterexample does not seem to imply any leakage in identifying information. So, HPVP11 privacy may be enough in practice.

Бывают и еще более запутанные ситуации, где совсем ничего не понятно.

# Ложноотрицательное?

- Посмотрите серию статей “another look at ...”
- Посмотрите доклад CTCrypt 2019 года “Что плохого можно сделать, неправильно используя криптоалгоритмы?”
- Практически любая статья с названием, содержащем “cryptoanalysis of ... protocol”...
- ... потому что правилом хорошего тона в 21 веке является представлять протокол сразу вместе с доказательством стойкости в некоторой модели противника.

# Позиции доказуемой стойкости на данный момент

- Хотим мы этого или нет, но “provable security” на настоящий момент является lingua franca в криптографии и господствующей парадигмой/научно-исследовательской программой.
- Отклонения также возможны: см. пример Signal (сначала протокол, потом модель и доказательство)...
- ... или 5G.

# Цикл разработки протокола 2.0

Предлагается совершенно новый цикл разработки протокола:

1. Формальная модель;
2. протокол с формальным доказательством;
3. конкретные атаки (уязвимости), не учтенные в модели;
4. новые модели по по результатам анализа уязвимостей;
5. “латание дыр”: новые “доказуемо стойкие” протоколы;
6. ???
7. PROFIT!

# А зачем тогда вообще нужны модели?

1. Как инструмент коммуникации: в сжатом виде содержат то, что другие «умные люди» посчитали важным учитывать.
2. Совместно с доказательством: для более глубокого понимания задачи.
3. Для получения более точных выводов (с явным постулированием исходных предположений).
4. Явное отклонение от модели дает больше информации, чем полное соответствие ей: есть какие-то существенные аспекты реальности, неучтенные в модели.
5. Возможно: модели/совокупности моделей развиваются кумулятивно и неявно вбирают в себя всё лучшее, что было придумано ранее (см. п. 1).

# И еще один камень в сторону моделей

**Против метода, П. Фейерабенд**

... не существует правила — сколь бы правдоподобным и эпистемологически обоснованным оно ни казалось, — которое в то или иное время не было бы нарушено.

**Против метода, П. Фейерабенд**

... идея жёсткого метода или жёсткой теории рациональности покоится на слишком наивном представлении о человеке и его социальном окружении. <...> существует лишь один принцип, который можно защищать при всех обстоятельствах и на всех этапах человеческого развития, — все дозволено.

# Резюме

- Серебряной пули нет.
- Доказуемая стойкость — лишь один из возможных подходов к формальному анализу протоколов, который позволяет в численном виде выразить нашу уверенность в безопасности протокола в заданных предположениях.
- Модели безопасности ничем принципиально не отличаются от моделей в науке вообще.
- Подход не дает противоречивых результатов — точно в том же смысле, в каком классическая механика не противоречит релятивистской (при условии отсутствия ошибок в доказательствах).

# Спасибо за внимание!


**Рис. 4:** «Вероломство образов», Рене Магритт

# В работе над докладом принимали участие


## Грибоедова Екатерина

Руководитель направления стандартизации,
Лаборатория криптографии
e.griboedova@kryptonite.ru

## Кирилл Царегородцев

Специалист-исследователь,
Лаборатория телекоммуникаций
k.tsaregorodtsev@kryptonite.ru