Об участии российских специалистов в развитии криптографических протоколов сетей связи 5G в 3GPP

Давыдов Степан

Лаборатория криптографии

«НПК «Криптонит»

РусКрипто’2022

КРИПТОНИТ

Криптографические протоколы в сетях связи 5G

КРИПТОНИТ

Национальная программа «Цифровая экономика РФ» по переводу важных информационных систем на отечественные криптографические алгоритмы с целью обеспечения их технологической независимости.

В ноябре 2020 года в рамках заседания Президиума Правительственной комиссии по цифровому развитию утверждена **дорожная карта развития мобильных сетей 5G** для развертывания телекоммуникационной сети на базе отечественного оборудования и алгоритмов.

«НПК «Криптонит»

Криптографические протоколы в сетях связи 5G

КРИПТОНИТ

Состав работ «НПК «Криптонит»

ЦЕЛЬ

Реализация системного проекта по разработке линейки российского оборудования необходимого для строительства мобильных сетей связи стандарта 5G/IMT-2020, с дальнейшим сопровождением разработки и ввода в эксплуатацию российского оборудования

ЗАДАЧИ	Технологические	Бизнес	НПА	Стандартизация	Лаборатория
	• Разработка технологической карты оборудования; • Разработка тех требований и ТЗ на ОКР по каждому типу оборудования; • Мониторинг процесса разработки; • Проведение предварительного радиопланирования; • Расчет пилотной зоны;	• Анализ и оценка приоритетных рынков сбыта; • Разработка бизнес плана и стратегии развития комплексного российского решения; • Разработка финансовой модели и политики ценообразования; • Разработка продуктовой документации и «виртуальной витрины»;	• Разработка нормативно-правовых актов для внедрения и эксплуатации разрабатываемого оборудования и мобильных сетей связи стандарта 5G/IMT-2020;	• Разработка предложений, их внесение и лоббирование в части стандартизации отечественных криптографических алгоритмов для мобильных сетей связи 5G/IMT-2020;	• Создание современной телекоммуникационной лаборатории для тестирования и сертификации российского оборудования для мобильных сетей связи 5G/IMT-2020 и проверки оборудования на совместимость (IT тестирование);
РЕЗУЛЬТАТЫ	• Технологическая карта оборудования и описание к ней; • Технические задания на ОКР по разработке оборудования; • Предварительное радиопланирование;	• Описание рынка с учетом расчета емкости; • Бизнес модель и план развития, включая ценовую политику; • Каталог разрабатываемого оборудования;	• Проекты НПА и сопровождение процесса их утверждения;	• Внесение предложений по стандартизации отечественных криптографических алгоритмов и сопровождение процесса их утверждения;	• Описание лаборатории и сопровождение процесса ее строительства;

Криптографические протоколы в сетях связи 5G

КРИПТОНИТ

Разработка и стандартизация протоколов безопасности в 5G на базе российских криптографических алгоритмов в рамках двух направлений

Криптографические протоколы в сетях связи 5G

КРИПТОНИТ

Вводная часть
«**Стандартизация российских криптографических механизмов в сетях связи 5G/IMT-2020: задачи, перспективы**» (Екатерина Грибоедова и др., РусКрипто 2021)

https://www.ruscrypto.ru/resource/archive/rc2021/files/10_griboedova_drynkin.pdf

Криптографические протоколы в сетях связи 5G

КРИПТОНИТ

Росстандарт

Проблемы

- Зашитые зарубежные алгоритмы
- Устаревшие принципы построения криптографических протоколов, наличие большого числа уязвимостей
- Отсутствие налаженных контактов с остальными участниками 3GPP

Стратегия на 2021-2022 год

- Устранение существующих уязвимостей
- Приобретение экспертного веса в 3GPP

Криптографические протоколы в сетях связи 5G

КРИПТОНИТ

Основные этапы (подпротоколы) обеспечения криптографической безопасности в сетях связи 5G

ECIES: Передача идентификатора абонента SUPI в защищенном виде

AKA-протокол: Аутентификация сторон и выработка общего мастер-ключа

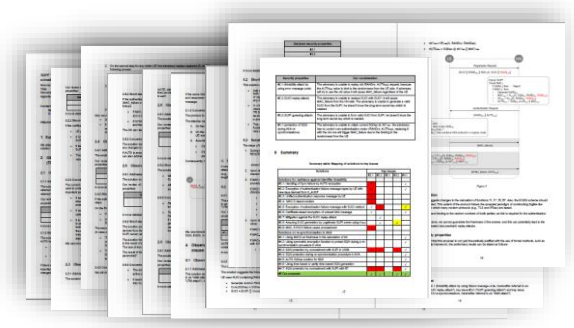
3GPP TR 33.846

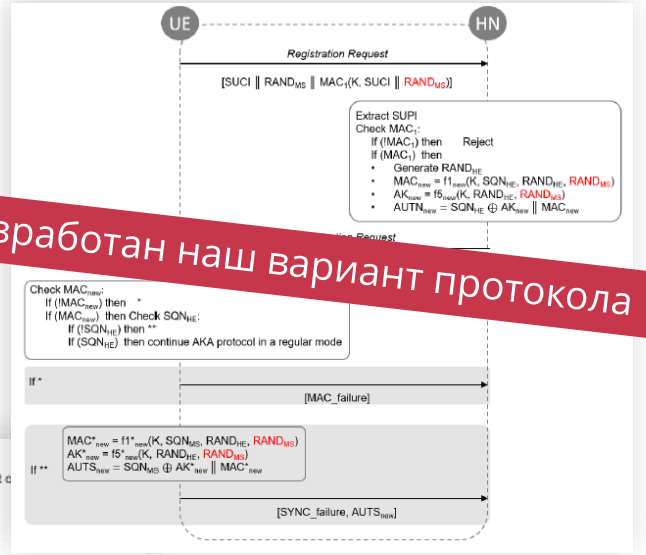
Выработка ключевого материала для каждого типа трафика

Защита трафика

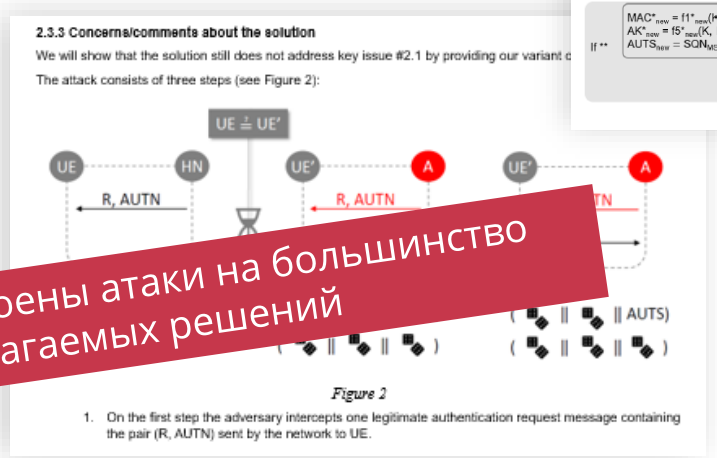
Криптографические протоколы в сетях связи 5G

КРИПТОНИТ





Разработан наш вариант протокола



Построены атаки на большинство предлагаемых решений

Криптографические протоколы в сетях связи 5G

КРИПТОНИТ

Meeting 104-e (август 2021)

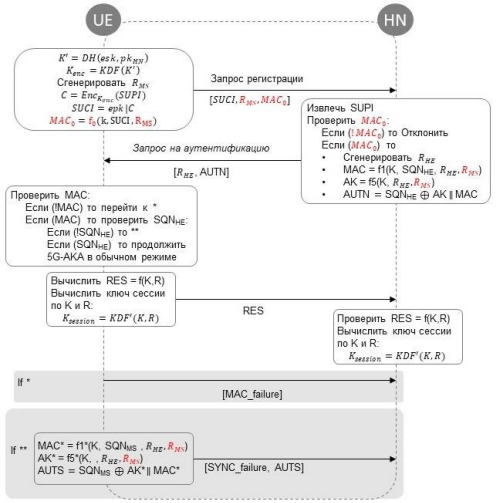
1) Observations on TR 33.846 – документ с анализом всех предлагаемых в TR 33.846 решений

Таблица 1: Сравнение решений, представленных в 3GPP TR 33.846

Название решения	Уязвимости			
	#2.1	#2.2	#3.2	#4.1
#2.1: Handling of Sync failure by AUTS encryption	x			✓
#2.2: Encryption of authentication failure message types by UE with new keys derived from K_AUSF	x			✓
#2.3: Unified authentication response message by UE	x			
#2.4: MAC-S based solution	x			
#2.5: Encryption of authentication failure message with SUCI method	✓	x		✓
#2.6: Certificate based encryption of unicast NAS message	✓			✓
#2.7: Mitigation against the SUCI replay attack		✓		
#2.8: Assuring SUCI generation by Legitimate SUPI owner using K_{SUCI}		✓	✓	
#2.9: MAC, SYNCH failure cause concealment	x			
#2.10: Solution to Key Issue #2.2: SUCI replay		✓!		
#2.11: Mitigate the SUCI replay based on UE's public key		✓!		
#3.1: Mitigation of SUPI guessing and SUCI replay attack using long term key		x	✓	✓
#3.2: Adding Check Value behind SUPI to mitigate the SUPI guessing attacks			✓	
#3.3: Mitigation of SUPI guessing attack			✓	
#4.1: Using MACS as freshness in the calculation of AK				✓
#4.2: Using symmetric encryption function to protect SQN during a re-synchronisation procedure in AKA				✓
#4.3: SQN protection by concealment with SUPI in USIM	x	x	x	✓
#4.4: SQN protection during re-synchronisation procedure in AKA				✓
#4.5: AUTS SQN_{MS} solution for 5GS				✓
#4.6: Using time-based or partly time-based SQN generation				✓
#4.7: SQN protection by concealment with SUPI with f5*	x	x	x	✓

принят к сведению без каких-либо существенных замечаний

2) AKA-протокол «НПК «Криптонит» - предлагается добавить в AKA протокол случайности с двух сторон и вычисление имитовставок



одобрен и включен в документ TR 33.846 как решение, защищающее от 4 уязвимостей

Криптографические протоколы в сетях связи 5G

КРИПТОНИТ

Meeting 105-e (ноябрь 2021)

Представлены 9 документов формата Change Request, содержащие предложения по внесению изменений в документ 3GPP TR 33.846 в соответствии с принятым ранее документом «Observations on TR 33.846».

- ✓ **7 документов были приняты без комментариев** со стороны участников встречи, предлагаемые изменения были добавлены в новую версию документа TR 33.846.
- ✓ **1 документ был принят после согласования вносимых правок** с компанией Huawei, изменения были добавлены в новую версию документа TR 33.846.
- ✓ По **1 документу** вносимые правки не были согласованы с компанией Thales, документ был принят к сведению (noted), обсуждение внесения правок было перенесено на 2022 год.

S3-213851	Update to solution #2.1	JSRPC Kryptonite	Approved.
S3-213852	Update to solution #2.2	JSRPC Kryptonite	Approved.
S3-213853	Update to solution #2.3	JSRPC Kryptonite	r3 is approved.
S3-213854	Update to solution #2.4	JSRPC Kryptonite	Noted.
S3-213855	Update to solution #2.5	JSRPC Kryptonite	Approved.
S3-213859	Update to solution #2.12	JSRPC Kryptonite	Approved.
S3-213892	Editor note removal for solution#2.8	Nokia, Nokia Shanghai Bell	Approved.
S3-213856	Update to solution #3.1	JSRPC Kryptonite	Approved.
S3-213857	Update to solution #4.3	JSRPC Kryptonite	Approved.
S3-213858	Update to solution #4.7	JSRPC Kryptonite	Approved.

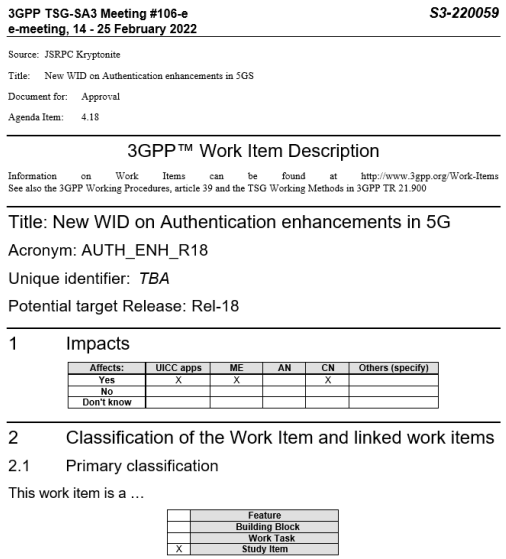
Криптографические протоколы в сетях связи 5G

КРИПТОНИТ

Meeting 106-e (февраль 2022)

Представлен документ:

«New WID on Authentication enhancements in 5GS», в котором предлагается продолжить работу по анализу и модернизации протокола аутентификации



3GPP TSG-SA3 Meeting #106-e
e-meeting, 14 - 25 February 2022

S3-220059

Source: JSRPC Kryptonite

Title: New WID on Authentication enhancements in 5GS

Document for: Approval

Agenda Item: 4.18

3GPP™ Work Item Description

Information on Work Items can be found at http://www.3gpp.org/Work-Items
See also the 3GPP Working Procedures, article 39 and the TSG Working Methods in 3GPP TR 21.900

Title: New WID on Authentication enhancements in 5G

Acronym: AUTH_ENH_R18

Unique identifier: *TBA*

Potential target Release: Rel-18

1 Impacts

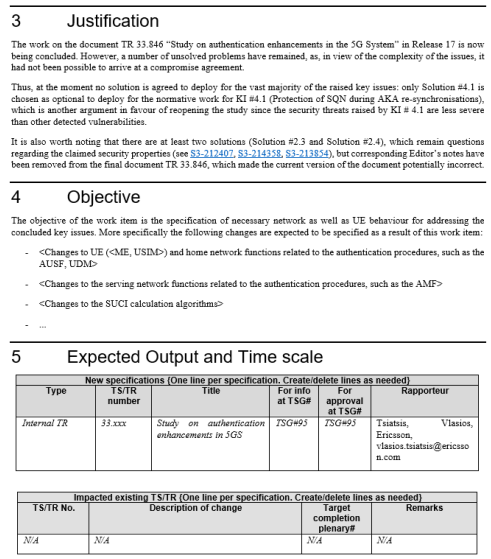
Affects:	UICC apps	ME	AN	CN	Others (specify)
Yes	X	X		X	
No					
Don't know					

2 Classification of the Work Item and linked work items

2.1 Primary classification

This work item is a …

	Feature
	Building Block
	Work Task
X	Study Item



3 Justification

The work on the document TR 33.846 "Study on authentication enhancements in the 5G System" in Release 17 is now being concluded. However, a number of unsolved problems have remained, as, in view of the complexity of the issues, it had not been possible to arrive at a compromise agreement.

Thus, at the moment no solution is agreed to deploy for the vast majority of the raised key issues: only Solution #4.1 is chosen as optional to deploy for the normative work for KI #4.1 (Protection of SQN during AKA re-synchronisation), which is another argument in favour of reopening the study since the security threats raised by KI # 4.1 are less severe than other detected vulnerabilities.

It is also worth noting that there are at least two solutions (Solution #2.3 and Solution #2.4), which remain questions regarding the claimed security properties (see S3-212407, S3-214358, S3-213854), but corresponding Editor's notes have been removed from the final document TR 33.846, which made the current version of the document potentially incorrect.

4 Objective

The objective of the work item is the specification of necessary network as well as UE behaviour for addressing the concluded key issues. More specifically the following changes are expected to be specified as a result of this work item:

- <Changes to UE (<ME, USIM>) and home network functions related to the authentication procedures, such as the AUSF, UDM>
- <Changes to the serving network functions related to the authentication procedures, such as the AMF>
- <Changes to the SUCI calculation algorithms>
- …

5 Expected Output and Time scale

New specifications {One line per specification. Create/delete lines as needed}					
Type	TS/TR number	Title	For info at TSG#	For approval at TSG#	Rapporteur
Internal TR	*33.xxx*	*Study on authentication enhancements in 5GS*	*TSG#93*	*TSG#93*	Tsiatsis, Vlasios, Ericsson, vlasios.tsiatsis@ericsson.com

Impacted existing TS/TR {One line per specification. Create/delete lines as needed}			
TS/TR No.	Description of change	Target completion plenary#	Remarks
N/A	*N/A*	*N/A*	*N/A*

Итог: были собраны замечания, было решено продолжить работу на следующем заседании, документ получил статус “noted”

Tdoc#	Title	Source	Disposition
S3-220059	New WID on Authentication enhancements in 5GS	JSRPC Kryptonite	Noted

Криптографические протоколы в сетях связи 5G

КРИПТОНИТ

Meeting 107-e (май 2022)

«Криптонит» **будет добиваться включения в план работ Release 18 разработки безопасного AKA-протокола с доказательством его стойкости** в моделях, исследующих аутентификацию, приватность и выработку общего ключа

Более подробно в докладе
«Еще раз о важности построения модели противника на примере протокола аутентификации 5G-AKA» (Царегородцев Кирилл и др., секция «Криптография и криптоанализ»)

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.”

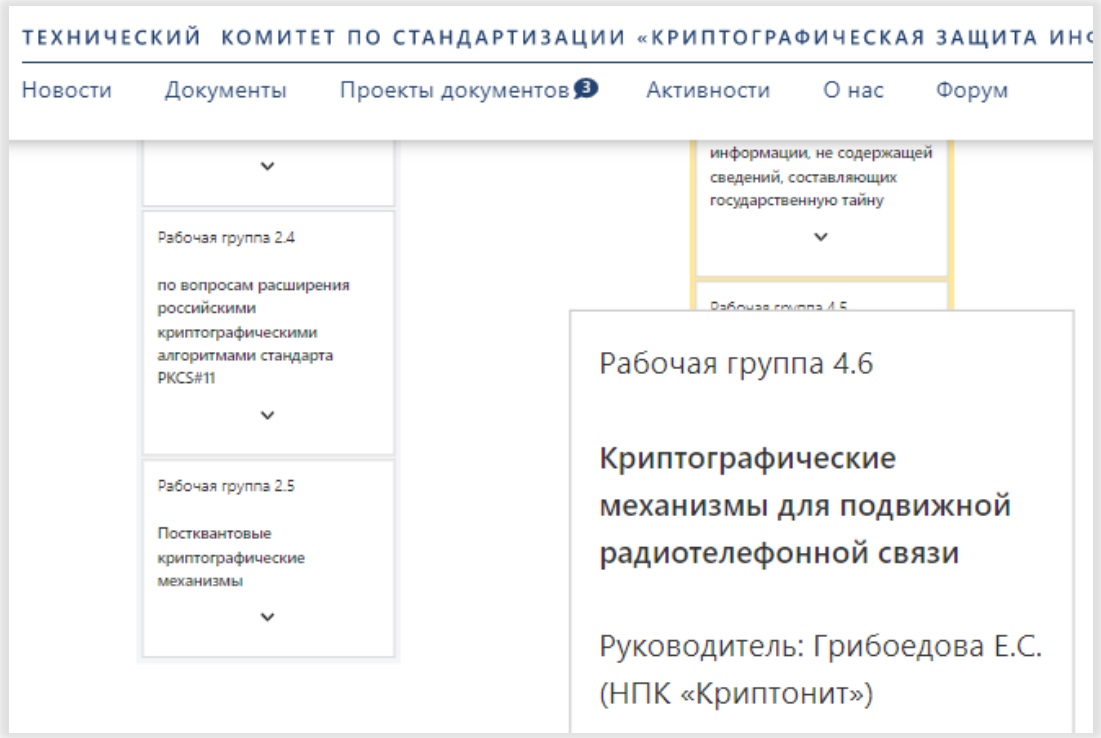
SA3 106e meeting communication

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

Криптографические протоколы в сетях связи 5G

5G 3GPP

5G Росстандарт



- ✓ Создана новая рабочая группа РГ ТК26 **КМ ПРТС**
- ✓ Подготовка проектов рекомендаций по стандартизации с предложениями по внедрению “криптонаборов” на базе российских стандартов

Спасибо за внимание!

Авторы доклада:

Давыдов Степан

Специалист-исследователь,
Лаборатория криптографии «НПК «Криптонит»
s.davydov@kryptonite.ru

Грибоедова Екатерина

Руководитель направления стандартизации,
Лаборатория криптографии «НПК «Криптонит»
e.griboedova@kryptonite.ru