Alternative security models for pseudorandom functions

Kirill Tsaregorodtsev
Researcher at Cryptography laboratory,
JSRPC ``Kryptonite”, Moscow, Russia

CTCrypt’2023

Outline

Table of Contents

The origin of the problem

- Analysis of 5G-AKA protocol.

The origin of the problem

- Analysis of 5G-AKA protocol.
- We want: **session key secrecy, explicit authentication, user privacy**.

The origin of the problem

- Analysis of 5G-AKA protocol.
- We want: **session key secrecy, explicit authentication, user privacy**.
- These properties give rise to the different security models for the underlying pseudorandom functions (PRF).

5G-AKA in a nutshell

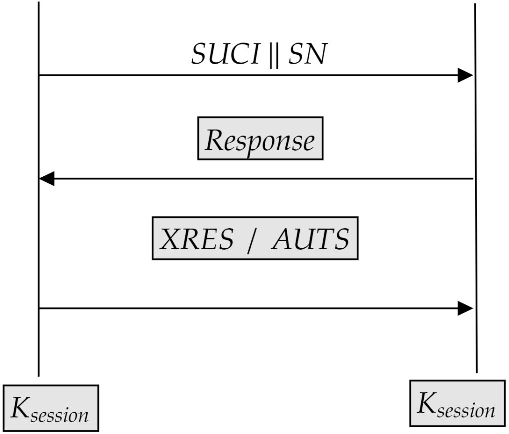
- Key agreement protocol based on a pre-shared secret keys.

5G-AKA in a nutshell

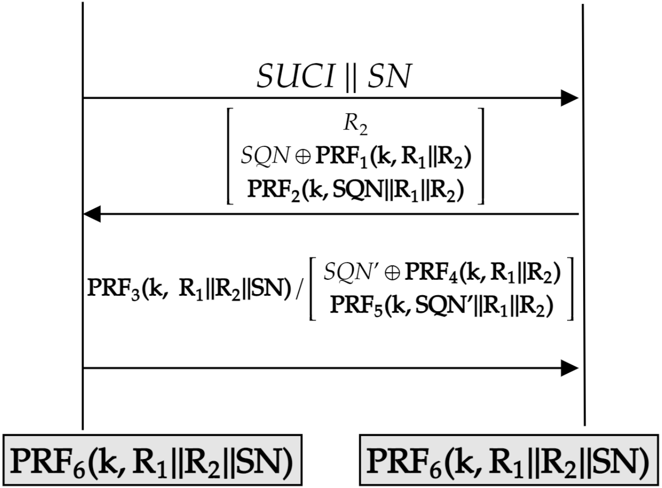
- Key agreement protocol based on a pre-shared secret keys.
- Main part of the protocol: three messages.

5G-AKA in a nutshell

- Key agreement protocol based on a pre-shared secret keys.
- Main part of the protocol: three messages.



5G-AKA: focusing on PRFs



Our goals

- identify “correct” security properties needed for the reduction of 5G-AKA protocol;

Our goals

- identify “correct” security properties needed for the reduction of 5G-AKA protocol;
- propose security models for PRF that formalizes these properties;

Our goals

- identify “correct” security properties needed for the reduction of 5G-AKA protocol;
- propose security models for PRF that formalizes these properties;
- analyze obtained models; show that they can be reduced to the standard security model for PRF.

Object of study: function family $\mathcal{F}$

$$\mathcal{F} = \{\mathcal{F}_k \in Funs(Dom, Range) \mid k \in Keys\}$$

Object of study: function family $\mathcal{F}$

$$\mathcal{F} = \{\mathcal{F}_k \in Funs(Dom, Range) \mid k \in Keys\}$$

Examples: block cipher “Magma”

$$\mathcal{F}_k(m) = E(k, m),\ Keys = \{0,1\}^{256},\ Dom = Range = \{0,1\}^{64},$$

Object of study: function family $\mathcal{F}$

$$\mathcal{F} = \{\mathcal{F}_k \in Funs(Dom, Range) \mid k \in Keys\}$$

Examples: block cipher “Magma”

$$\mathcal{F}_k(m) = E(k, m),\ Keys = \{0,1\}^{256},\ Dom = Range = \{0,1\}^{64},$$

MAC function $\mathrm{MAC}(k, \cdot)$ (in that case $Dom = \{0,1\}^*$).

PRF model

The advantage of the adversary $\mathcal{A}$ in the PRF model for the function family $\mathcal{F}$ is the following quantity:

$$\mathrm{Adv}_{\mathcal{F}}^{\mathrm{PRF}}(\mathcal{A}) = \mathbb{P}\left[\mathrm{Exp}_{\mathcal{F}}^{\mathrm{PRF\text{-}1}}(\mathcal{A}) \to 1\right] - \mathbb{P}\left[\mathrm{Exp}_{\mathcal{F}}^{\mathrm{PRF\text{-}0}}(\mathcal{A}) \to 1\right].$$

The advantage of the adversary $\mathcal{A}$ in the PRF model for the function family $\mathcal{F}$ is the following quantity:

$$\mathrm{Adv}_{\mathcal{F}}^{\mathrm{PRF}}(\mathcal{A}) = \mathbb{P}\left[\mathrm{Exp}_{\mathcal{F}}^{\mathrm{PRF\text{-}1}}(\mathcal{A}) \to 1\right] - \mathbb{P}\left[\mathrm{Exp}_{\mathcal{F}}^{\mathrm{PRF\text{-}0}}(\mathcal{A}) \to 1\right].$$

$\underline{\mathrm{Exp}_{\mathcal{F}}^{\mathrm{PRF\text{-}1}}(\mathcal{A})}$

$k \leftarrow^{\$} \mathit{Keys}$

$b' \leftarrow^{\$} \mathcal{A}^{\mathcal{O}_{\mathrm{prf}}}$

$\textbf{return } b'$

$\underline{\mathcal{O}_{\mathrm{prf}}(m)}$

$\textbf{return } \mathcal{F}_k(m)$

PRF model

The advantage of the adversary $\mathcal{A}$ in the PRF model for the function family $\mathcal{F}$ is the following quantity:

$$\mathrm{Adv}_{\mathcal{F}}^{\mathrm{PRF}}(\mathcal{A}) = \mathbb{P}\left[\mathrm{Exp}_{\mathcal{F}}^{\mathrm{PRF\text{-}1}}(\mathcal{A}) \to 1\right] - \mathbb{P}\left[\mathrm{Exp}_{\mathcal{F}}^{\mathrm{PRF\text{-}0}}(\mathcal{A}) \to 1\right].$$

$\underline{\mathrm{Exp}_{\mathcal{F}}^{\mathrm{PRF\text{-}1}}(\mathcal{A})}$	$\underline{\mathrm{Exp}_{\mathcal{F}}^{\mathrm{PRF\text{-}0}}(\mathcal{A})}$	$\underline{\mathcal{O}_{\mathrm{prf}}(m)}$
$k \xleftarrow{\$} \mathit{Keys}$	$\mathit{Asked} \leftarrow [\,]$	**if** $\mathit{Asked}[m] = \perp$
$b' \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_{\mathrm{prf}}}$	$b' \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_{\mathrm{prf}}}$	$\quad \mathit{Asked}[m] \xleftarrow{\$} \mathit{Range}$
return b'	**return** b'	**fi**
$\underline{\mathcal{O}_{\mathrm{prf}}(m)}$		**return** $\mathit{Asked}[m]$
return $\mathcal{F}_k(m)$		

PRF model: success measure

$$\mathrm{Adv}_{\mathcal{F}}^{\mathrm{PRF}}(t, q, \ell, \mu)$$

maximal advantage $\mathrm{Adv}_{\mathcal{F}}^{\mathrm{PRF}}(\mathcal{A})$, where the maximum is taken over the adversaries $\mathcal{A}$ with

PRF model: success measure

$$\mathrm{Adv}_{\mathcal{F}}^{\mathrm{PRF}}(t, q, \ell, \mu)$$

maximal advantage $\mathrm{Adv}_{\mathcal{F}}^{\mathrm{PRF}}(\mathcal{A})$, where the maximum is taken over the adversaries $\mathcal{A}$ with

- time complexity is at most t,
- the number of queries to $\mathcal{O}_{\mathrm{prf}}$ does not exceed q,
- total length of the queries $\sum |m|$ does not exceed ℓ,
- maximal query length $\max |m|$ does not exceed μ.

PRF in 5G-AKA

$$\mathcal{F}_k(x) = \text{Hash}\,(k \| \text{Hash}\,(k \| x))$$

Table 1: Calculation of values depending on the pre-shared secret k

Value	$S3G$ function	Computation rule	Indices
σ_1	f_1	$\mathcal{F}_k(SQN \,\|\, RAND \,\|\, Const_1)$	$[1:\ tlen]$
σ_2	f_1^*	$\mathcal{F}_k(SQN_{UE} \,\|\, RAND \,\|\, Const_1)$	$[257:\ 256 + tlen]$
RES	f_2	$\mathcal{F}_k(RAND \,\|\, Const_2)$	$[1:\ reslen]$
AK	f_5		$[257:\ 256 + 48]$
AK^*	f_5^*		$[305:\ 304 + 48]$
CK	f_3	$\mathcal{F}_k(RAND \,\|\, Const_3)$	$[1:\ klen]$
IK	f_4		$[257:\ 256 + klen]$

Fields dependent on the shared secret key k

- σ_1, σ_2 (part of the $AUTN$, $AUTS$ resp.): integrity of the transmitted messages within the session; explicit authentication Home Network and User resp.

Fields dependent on the shared secret key k

- σ_1, σ_2 (part of the $AUTN$, $AUTS$ resp.): integrity of the transmitted messages within the session; explicit authentication Home Network and User resp.
- RES: explicit User authentication, confirmation of successful completion on the User's side.

Fields dependent on the shared secret key k

- σ_1, σ_2 (part of the $AUTN$, $AUTS$ resp.): integrity of the transmitted messages within the session; explicit authentication Home Network and User resp.
- RES: explicit User authentication, confirmation of successful completion on the User's side.
- AK, AK^* (used in $AUTN$, $AUTS$ resp.): pseudorandom sequence masking the connection counters SQN.

Fields dependent on the shared secret key k

- σ_1, σ_2 (part of the $AUTN$, $AUTS$ resp.): integrity of the transmitted messages within the session; explicit authentication Home Network and User resp.
- RES: explicit User authentication, confirmation of successful completion on the User's side.
- AK, AK^* (used in $AUTN$, $AUTS$ resp.): pseudorandom sequence masking the connection counters SQN.
- CK, IK: session key derivation $k_{session}$.

5G-AKA: focusing on PRFs

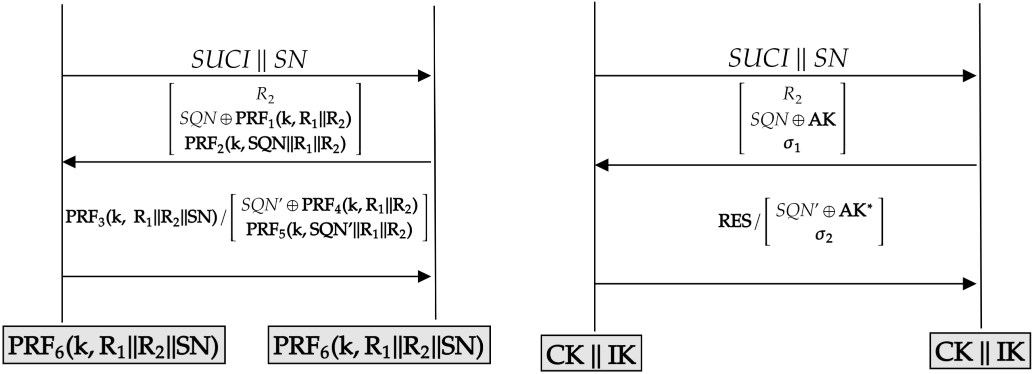


Table of Contents

Session key secrecy

- **High-level goal:** obtaining information about the session key.
- **Goal (in model):** distinguish between a **segment** of a pseudorandom function output and a random string (in the presence of additional information).

Session key secrecy

- **High-level goal:** obtaining information about the session key.
- **Goal (in model):** distinguish between a **segment** of a pseudorandom function output and a random string (in the presence of additional information).
- **High-level capabilities:** compromise session keys in sessions other than the one being attacked, as well as receiving the values of σ_1, σ_2, RES (transmitted in plaintext) or partial information about the values of AK, AK^*.
- **Capabilities (in model):** learning output segments of a pseudorandom function.

PRF$^+$ model: pseudocode

$\mathrm{Exp}_{\mathcal{F}}^{\mathrm{PRF}^+\text{-}b}(\mathcal{A})$

$k \xleftarrow{\$} \mathit{Keys}$

$\mathit{Asked} \leftarrow [\,]$

$b' \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_{\mathrm{prf}}, \mathcal{O}^b_{\mathrm{test}}}$

return b'

$\mathcal{O}_{\mathrm{prf}}(m, idx_1, idx_2)$

if $(\mathit{Asked}[m] \cap [idx_1 : idx_2] \neq \varnothing)$

  return $\perp$

fi

$\mathit{Asked}[m] \leftarrow \mathit{Asked}[m] \cup [idx_1 : idx_2]$

return $\mathcal{F}_k(m)[idx_1 : idx_2]$

$\mathcal{O}^b_{\mathrm{test}}(m, idx_1, idx_2)$

if $(\mathit{Asked}[m] \cap [idx_1 : idx_2] \neq \varnothing)$

  return $\perp$

fi

if $(b = 0)$

  $val \xleftarrow{\$} \{0,1\}^{idx_2 - idx_1 + 1}$

else

  $val \leftarrow \mathcal{F}_k(m)[idx_1 : idx_2]$

fi

$\mathit{Asked}[m] \leftarrow \mathit{Asked}[m] \cup [idx_1 : idx_2]$

return val

PRF^+ model: success measure

$$\mathrm{Adv}_{\mathcal{F}}^{\mathrm{PRF}^+}(t, q_{prf}, q_{test})$$

maximal value among $\mathrm{Adv}_{\mathcal{F}}^{\mathrm{PRF}^+}(\mathcal{A})$, where:

PRF^{+} model: success measure

$$\mathrm{Adv}_{\mathcal{F}}^{\mathrm{PRF}^{+}}(t, q_{prf}, q_{test})$$

maximal value among $\mathrm{Adv}_{\mathcal{F}}^{\mathrm{PRF}^{+}}(\mathcal{A})$, where:

- $\mathcal{A}$'s time complexity does not exceed t,
- $\mathcal{A}$ makes no more than q_{prf} queries to the $\mathcal{O}_{\mathrm{prf}}$,
- q_{test} queries to $\mathcal{O}_{\mathrm{test}}^{b}$ oracles.

PRF^+ model: reduction

The following inequality holds:

$$\mathrm{Adv}_{\mathcal{F}}^{\mathrm{PRF}^+}(t, q_{prf}, q_{test}) \leq 2 \cdot \mathrm{Adv}_{\mathcal{F}}^{\mathrm{PRF}}(t + q_{prf} + q_{test}, q_{prf} + q_{test}).$$

PRF^{+} model: idea

- “true” segments does not help much...

PRF^+ model: idea

- “true” segments does not help much…
- because they are indistinguishable from random ones,

PRF^{+} model: idea

- “true” segments does not help much...
- because they are indistinguishable from random ones,
- hence, $\mathcal{O}_{\mathrm{prf}}$ can be excluded (i.e., modelled with a random string generator).

PRF^{+} model: idea

- "true" segments does not help much...
- because they are indistinguishable from random ones,
- hence, $\mathcal{O}_{\mathrm{prf}}$ can be excluded (i.e., modelled with a random string generator).
- PRF^{+} model can be naturally generalized to the case of $D \in \mathbb{N}$ parties; by hybrid argument this case can be reduced to the case $D = 1$.

Table of Contents

Explicit authentication

- **High-level goal:** explicit participant authentication.
- **Goal (in model):** forge the segment of a pseudorandom function output (in the presence of additional information).

Explicit authentication

- **High-level goal:** explicit participant authentication.
- **Goal (in model):** forge the segment of a pseudorandom function output (in the presence of additional information).
- **High-level capabilities:** compromise session keys in sessions other than the one being attacked, as well as receiving the values of σ_1, σ_2, RES (transmitted in plaintext) or partial information about the values of AK, AK^*.
- **Capabilities (in model):** learning output segments of a pseudorandom function.

UF-PRF model: pseudocode

$\mathrm{Exp}_{\mathcal{F}}^{\text{UF-PRF}}(\mathcal{A})$

$k \leftarrow^{\$} \mathit{Keys}$

$\mathit{Asked} \leftarrow [\,]$

$\mathit{win} \leftarrow \mathit{false}$

$\mathcal{A}^{\mathcal{O}_{\mathrm{prf}}, \mathcal{O}_{\mathrm{vfy}}}$

return win

$\mathcal{O}_{\mathrm{prf}}(m, \mathit{idx}_1, \mathit{idx}_2)$

$\mathit{Asked}[m] \leftarrow \mathit{Asked}[m] \cup [\mathit{idx}_1 : \mathit{idx}_2]$

return $\mathcal{F}_k(m)[\mathit{idx}_1 : \mathit{idx}_2]$

$\mathcal{O}_{\mathrm{vfy}}(m, \tau, i)$

$\mathit{val} \leftarrow \mathcal{F}_k(m)[i : i + \mathit{tlen} - 1]$

$\mathit{res} \leftarrow (\tau = \mathit{val})$

if $(\mathit{Asked}[m] \cap [i : i + \mathit{tlen} - 1] = \emptyset)$

  $\mathit{win} \leftarrow \mathit{win} \vee \mathit{res}$

fi

return res

UF-PRF model: success measure

$$\mathrm{Adv}_{\mathcal{F}}^{\text{UF-PRF}}(t, q_{prf}, q_{vfy}, tlen)$$

maximal value among $\mathrm{Adv}_{\mathcal{F}}^{\text{UF-PRF}}(\mathcal{A})$, where

UF-PRF model: success measure

$$\mathrm{Adv}_{\mathcal{F}}^{\text{UF-PRF}}(t, q_{prf}, q_{vfy}, tlen)$$

maximal value among $\mathrm{Adv}_{\mathcal{F}}^{\text{UF-PRF}}(\mathcal{A})$, where

- $\mathcal{A}$'s time complexity does not exceed t,
- the length of the segment to be predicted is $tlen$,
- $\mathcal{A}$ makes no more than q_{prf} queries to the $\mathcal{O}_{\text{prf}}$,
- q_{vfy} queries to $\mathcal{O}_{\text{vfy}}$ oracles.

UF-PRF model: reduction

The following inequality holds:

$$\mathrm{Adv}_{\mathcal{F}}^{\mathrm{UF\text{-}PRF}}(t, q_{prf}, q_{vfy}, tlen) \leq \mathrm{Adv}_{\mathcal{F}}^{\mathrm{PRF}^+}(t + q_{prf} + q_{vfy}, q_{prf}, q_{vfy}) + \frac{q_{vfy}}{2^{tlen}}.$$

UF-PRF model: idea

- It is hard to distinguish segments from random ones...

[1] Bellare, Goldreich, and Mityagin, *The Power of Verification Queries in Message Authentication and Authenticated Encryption*.

UF-PRF model: idea

- It is hard to distinguish segments from random ones…
- hence, it is even harder to predict it completely[1]…

[1] Bellare, Goldreich, and Mityagin, *The Power of Verification Queries in Message Authentication and Authenticated Encryption*.

UF-PRF model: idea

- It is hard to distinguish segments from random ones…
- hence, it is even harder to predict it completely[1]…
- BUT: there is a chance to guess correctly ($\frac{q_{vfy}}{2^{tlen}}$ term).

[1] Bellare, Goldreich, and Mityagin, *The Power of Verification Queries in Message Authentication and Authenticated Encryption*.

UF-PRF model: idea

- It is hard to distinguish segments from random ones...
- hence, it is even harder to predict it completely[1]...
- BUT: there is a chance to guess correctly ($\frac{q_{vfy}}{2^{tlen}}$ term).
- UF-PRF model can be naturally generalized to the case of $D \in \mathbb{N}$ parties; by hybrid argument this model can be reduced to the case $D = 1$.

[1] Bellare, Goldreich, and Mityagin, *The Power of Verification Queries in Message Authentication and Authenticated Encryption*.

Table of Contents

User privacy

- **High-level goal:** indistinguishable behaviour of users (cannot deduce which user is answering to the queries).
- **Goal (in model):** determine whether the adversary interacts with the “left” or “right” oracle (see also[2], LOR-DCPA model).

[2] Bellare, Kohno, and Namprempre, “Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the Encode-then-Encrypt-and-MAC paradigm.”

- **High-level goal:** indistinguishable behaviour of users (cannot deduce which user is answering to the queries).
- **Goal (in model):** determine whether the adversary interacts with the “left” or “right” oracle (see also[2], LOR-DCPA model).
- **High-level capabilities:** compromise session keys in sessions other than the one being attacked, as well as receiving the values of σ_1, σ_2, RES (transmitted in plaintext) or partial information about the values of AK, AK^*.
- **Capabilities (in model):** learning output segments of a pseudorandom function.

[2] Bellare, Kohno, and Namprempre, “Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the Encode-then-Encrypt-and-MAC paradigm.”

- The adversary has to determine on which of the keys (“left” k_{i_0} or “right” k_{i_1}) and which message (“left” m_0 or “right” m_1) is processed by the oracle $\mathcal{O}^b_{\mathrm{lor}}$.

LOR-PRF model: preliminary remark

- The adversary has to determine on which of the keys (“left” k_{i_0} or “right” k_{i_1}) and which message (“left” m_0 or “right” m_1) is processed by the oracle $\mathcal{O}^b_{\mathrm{lor}}$.
- To exclude the possibility of trivial attacks the adversary **is not allowed to repeat** messages for each fixed key k_i.

LOR-PRF model: preliminary remark

- The adversary has to determine on which of the keys ("left" k_{i_0} or "right" k_{i_1}) and which message ("left" m_0 or "right" m_1) is processed by the oracle $\mathcal{O}^b_{\mathrm{lor}}$.
- To exclude the possibility of trivial attacks the adversary **is not allowed to repeat** messages for each fixed key k_i.
- In 5G-AKA message uniqueness is implemented by adding a counter SQN (number of connections) to the messages, as well as the randomness $RAND$.

LOR-PRF model: pseudocode

$\mathrm{Exp}_{\mathcal{F}}^{\text{LOR-PRF-}b}(\mathcal{A})$	$\mathcal{O}_{\mathrm{lor}}^{b}(m_0, i_0, m_1, i_1)$
for $i \in \{1, \ldots, d\}$	**if** $(m_0 \in Msg[i_0]) \vee (m_1 \in Msg[i_1])$
$\quad k_i \leftarrow^{\$} Keys$	$\quad$ **return** $\perp$
endfor	**fi**
$Msg \leftarrow [\,]$	$Msg[i_0] \leftarrow Msg[i_0] \cup \{m_0\}$
$b' \leftarrow^{\$} \mathcal{A}^{\mathcal{O}_{\mathrm{lor}}^{b}}$	$Msg[i_1] \leftarrow Msg[i_1] \cup \{m_1\}$
return b'	**return** $\mathcal{F}_{k_{i_b}}(m_b)$

$$\mathrm{Adv}_{\mathcal{F}}^{\text{LOR-PRF}}(t, Q; d)$$

maximal value among $\mathrm{Adv}_{\mathcal{F}}^{\text{LOR-PRF}}(\mathcal{A})$ in LOR-PRF Experiment with d users, where

LOR-PRF model: success measure

$$\mathrm{Adv}_{\mathcal{F}}^{\mathrm{LOR\text{-}PRF}}(t, Q; d)$$

maximal value among $\mathrm{Adv}_{\mathcal{F}}^{\mathrm{LOR\text{-}PRF}}(\mathcal{A})$ in LOR-PRF Experiment with d users, where

- $\mathcal{A}$'s time complexity does not exceed t,
- number of queries to $\mathcal{O}_{\mathrm{lor}}^{b}$ oracle on the key k_i (either as "left", or as "right", i.e., queries of the form $(\cdot, i, \cdot, \cdot)$ or $(\cdot, \cdot, \cdot, i)$) does not exceed $Q[i]$.

$\mathrm{LOR\text{-}PRF}$ model: reduction

$$\mathrm{Adv}_{\mathcal{F}}^{\mathrm{LOR\text{-}PRF}}(t, Q; d) \leq 2d \cdot \mathrm{Adv}_{\mathcal{F}}^{\mathrm{PRF}}(t + d + \sum_i Q[i], \max_i Q[i]).$$

LOR-PRF model: idea

- A series of hybrids $\mathcal{B}_{b_0}^{b_1,\ldots,b_d}(\mathcal{A})$,

LOR-PRF model: idea

- A series of hybrids $\mathcal{B}_{b_0}^{b_1,\dots,b_d}(\mathcal{A})$,
- bit b_0 — whether "left" or "right" messages are processed

LOR-PRF model: idea

- A series of hybrids $\mathcal{B}_{b_0}^{b_1,\dots,b_d}(\mathcal{A})$,
- bit b_0 — whether "left" or "right" messages are processed
- bit b_i, $i \in \{1, \dots, d\}$ — what will be used as the i-th function: a truly random or pseudorandom function;

LOR-PRF model: idea

- A series of hybrids $\mathcal{B}_{b_0}^{b_1,\dots,b_d}(\mathcal{A})$,
- bit b_0 — whether “left” or “right” messages are processed
- bit b_i, $i \in \{1,\dots,d\}$ — what will be used as the i-th function: a truly random or pseudorandom function;
- process the inputs (m_0, i_0, m_1, i_1) as follows:
  - if $b_0 = 0$, $b_{i_0} = 0$: return a random string of appropriate length;
  - if $b_0 = 0$, $b_{i_0} = 1$: return $\mathcal{F}_{k_{i_0}}(m_0)$;
  - if $b_0 = 1$, $b_{i_1} = 0$: return a random string of appropriate length;
  - if $b_0 = 1$, $b_{i_0} = 1$: return $\mathcal{F}_{k_{i_1}}(m_1)$;

Table of Contents

Concluding remarks

- Three models were analyzed:

Concluding remarks

- Three models were analyzed:
- PRF^{+}: hard to distinguish segments of PRF from a truly random strings in the presence of additional information;

Concluding remarks

- Three models were analyzed:
- PRF^{+}: hard to distinguish segments of PRF from a truly random strings in the presence of additional information;
- $\mathrm{UF\text{-}PRF}$: hard to forge segments of PRF;

Concluding remarks

- Three models were analyzed:
- PRF^{+}: hard to distinguish segments of PRF from a truly random strings in the presence of additional information;
- $\mathrm{UF\text{-}PRF}$: hard to forge segments of PRF;
- $\mathrm{LOR\text{-}PRF}$: hard to guess which message was processed;

Concluding remarks

- Three models were analyzed:
- PRF^{+}: hard to distinguish segments of PRF from a truly random strings in the presence of additional information;
- $\mathrm{UF\text{-}PRF}$: hard to forge segments of PRF;
- $\mathrm{LOR\text{-}PRF}$: hard to guess which message was processed;
- Models can be used in the analysis of 5G-AKA protocol security.

- Bellare, Mihir, Oded Goldreich, and Anton Mityagin. *The Power of Verification Queries in Message Authentication and Authenticated Encryption*. Cryptology ePrint Archive, Paper 2004/309. **https://eprint.iacr.org/2004/309**. 2004. URL: **https://eprint.iacr.org/2004/309**.
- Bellare, Mihir, Tadayoshi Kohno, and Chanathip Namprempre. "Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the Encode-then-Encrypt-and-MAC paradigm." In: *ACM Transactions on Information and System Security (TISSEC)* 7.2 (2004), pp. 206–241.

Thank you for your attention!

Author(s):

Tsaregorodtsev Kirill

Researcher at Cryptography laboratory,
JSRPC “Kryptonite”, Moscow, Russia
k.tsaregorodtsev@kryptonite.ru