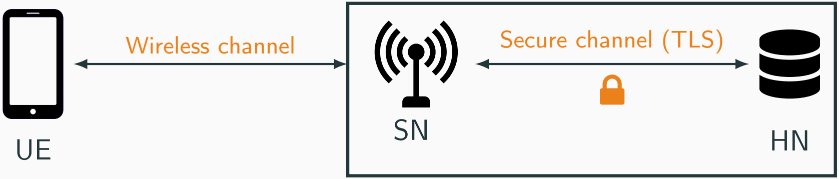
The 5G-AKA Authentication Protocol Privacy

Adrien Koutsos
Max Planck Institute for Security and Privacy
work done while at the LSV, ENS Paris-Saclay

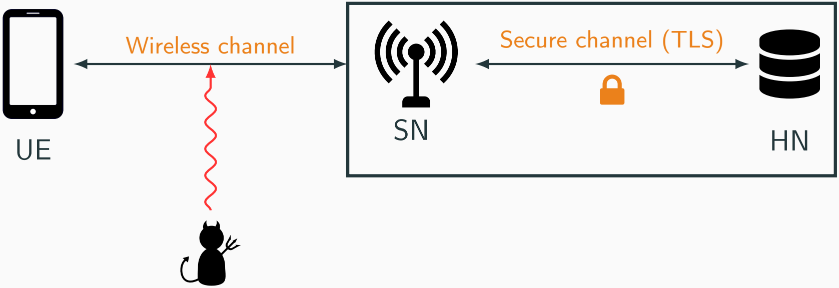
November 28, 2019

The 4G-AKA and 5G-AKA Protocols

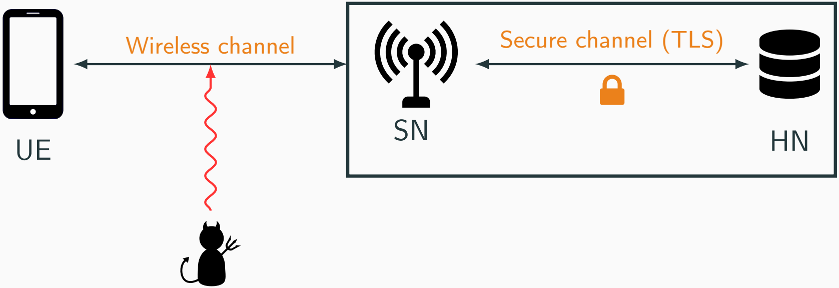
Authentication and Key Agreement Protocol



Authentication and Key Agreement Protocol



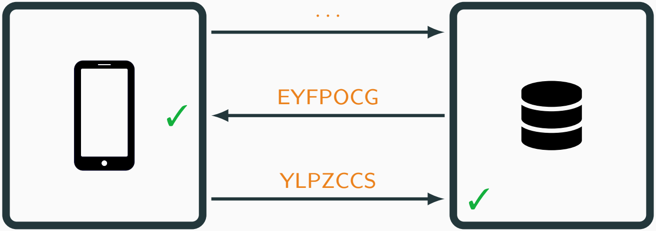
Authentication and Key Agreement Protocol



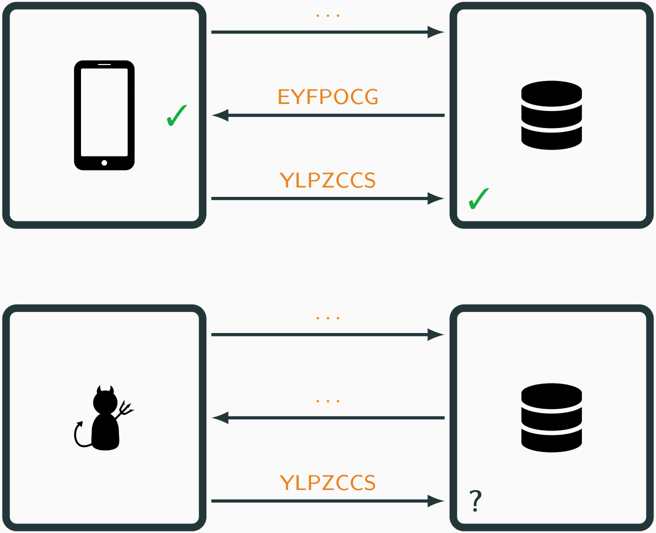
Security Properties

- **Mutual authentication** between the user and the service provider.
- **Privacy** of the user against an outside observer.

Authentication Protocol



Authentication Protocol



. . .

EYFPOCG

✓

YLPZCCS

✓

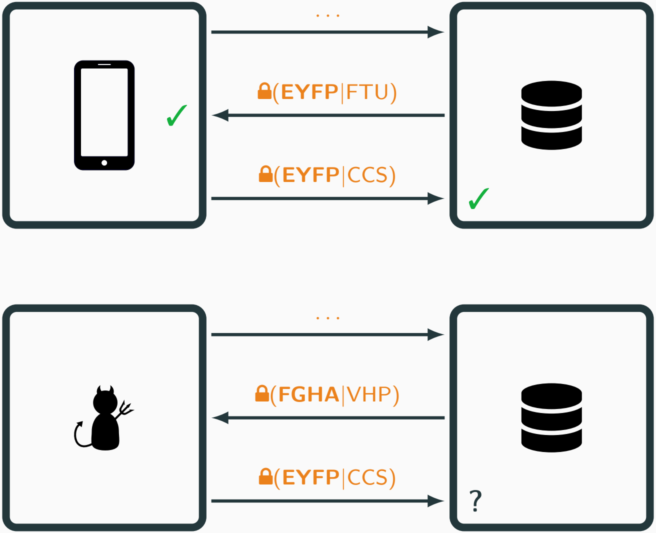
. . .

. . .

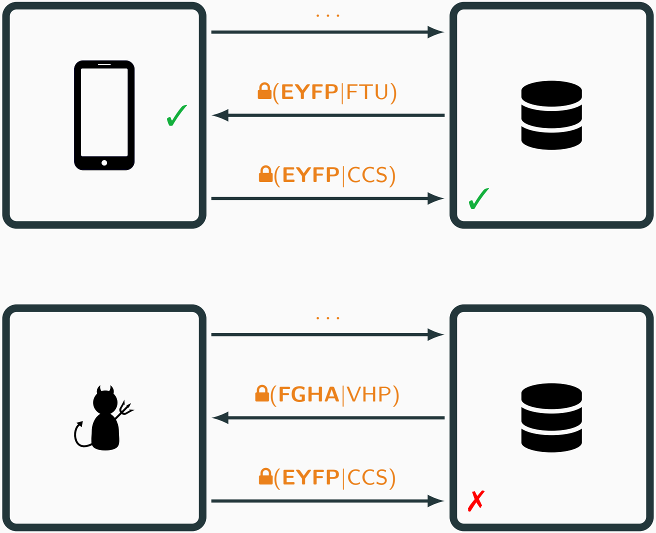
YLPZCCS

?

Authentication Protocol



Authentication Protocol



. . .

🔒(**EYFP**|FTU)

✓

🔒(**EYFP**|CCS)

✓

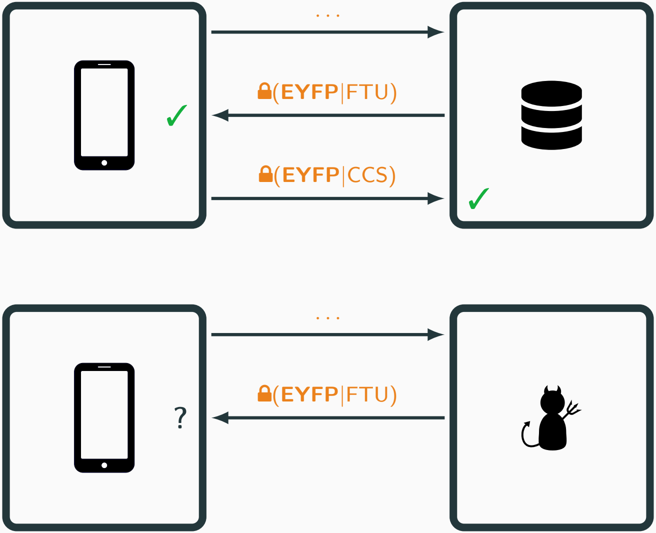
. . .

🔒(**FGHA**|VHP)

🔒(**EYFP**|CCS)

✗

Authentication Protocol



. . .

🔒(**EYFP**|FTU)

✓

🔒(**EYFP**|CCS)

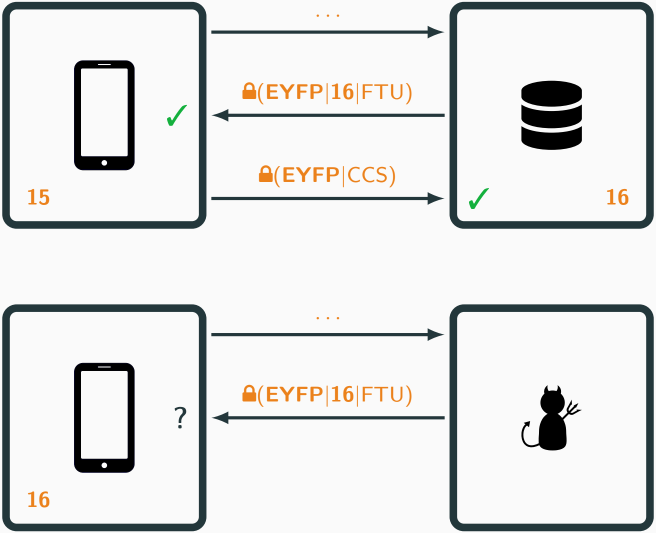
✓

. . .

🔒(**EYFP**|FTU)

?

Authentication Protocol



. . .

🔒(**EYFP**|**16**|FTU)

✓

🔒(**EYFP**|CCS)

15

✓

16

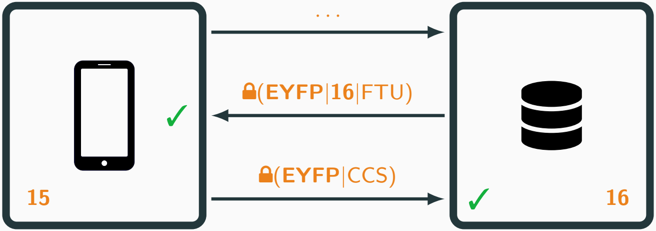
. . .

🔒(**EYFP**|**16**|FTU)

?

16

Authentication Protocol



. . .

🔒(**EYFP**|**16**|FTU)

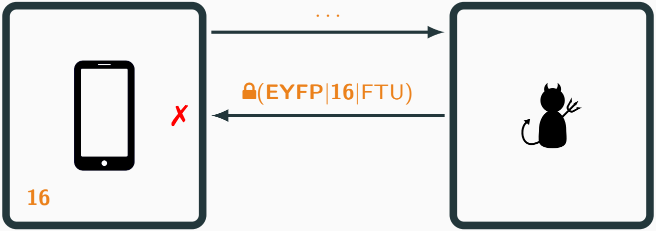
🔒(**EYFP**|CCS)

✓

✓

15

16



. . .

🔒(**EYFP**|**16**|FTU)

✗

16

Security of the Protocol

Is this secure?

Security of the Protocol

Is this secure?

For authentication, yes.

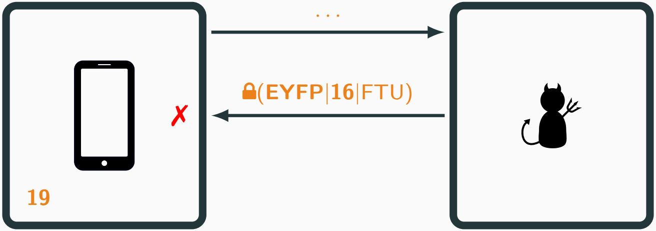
Security of the Protocol

Is this secure?

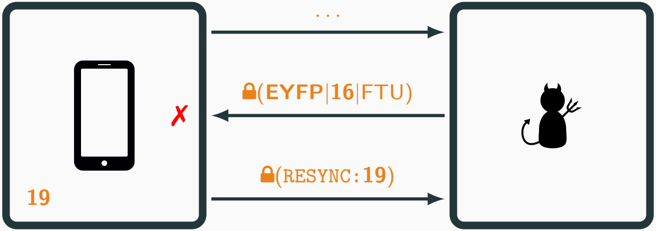
For authentication, yes.

For privacy, no.

Privacy Attack



Privacy Attack



. . .

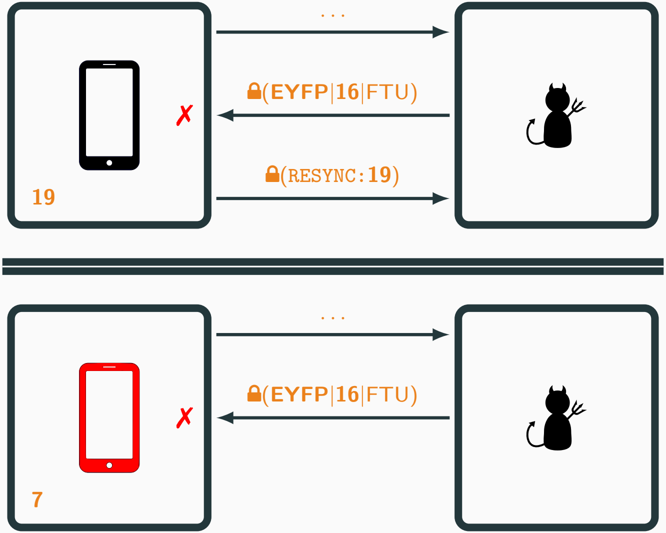
🔒(**EYFP**|**16**|FTU)

✗

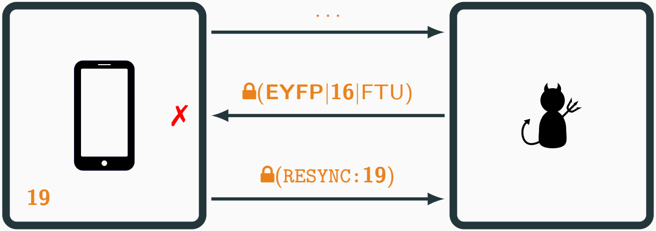
🔒(RESYNC:**19**)

19

Privacy Attack



Privacy Attack



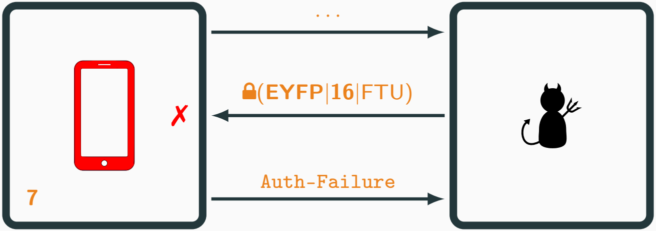
. . .

✗

🔒(EYFP|16|FTU)

🔒(RESYNC:19)

19



. . .

✗

🔒(EYFP|16|FTU)

Auth-Failure

7

Unlinkability

Privacy Attack

The adversary breaks the user privacy by finding **links between the user sessions** of the protocol.

Unlinkability

Privacy Attack

The adversary breaks the user privacy by finding **links between the user sessions** of the protocol.

Unlinkability

The adversary **cannot track** a user through its protocol sessions.

Goal

Goal

Design a modified version of AKA, called AKA^{+}, such that:

- Provides some form of **unlinkability**.

Goal

Goal

Design a modified version of AKA, called AKA$^+$, such that:

- Provides some form of **unlinkability**.
- Satisfies the design and efficiency **constraints** of 5G-AKA.

Goal

Goal

Design a modified version of AKA, called AKA$^+$, such that:

- Provides some form of **unlinkability**.
- Satisfies the design and efficiency **constraints** of 5G-AKA.
- Is **proved secure**.

Theorem

Theorem

The AKA$^+$ protocol is σ-unlinkable for **an arbitrary number of agents and sessions** when:

- The asymmetric encryption $\{\_\}_{\_}^{\_}$ is $\textsc{ind-cca}_1$.
- H and H$^{\mathsf{r}}$ (resp. Mac^1–Mac^5) are jointly $\textsc{prf}$.

Conclusion

Conclusion

Contributions

- Presented the basics of the 5G-AKA protocol.
- Showed a known privacy attacks against 5G-AKA.
- Proposed a fixed version, and proved it secure in the computational model.

Thanks for your attention

References i

[Arapinis et al., 2012] Arapinis, M., Mancini, L. I., Ritter, E., Ryan, M., Golde, N., Redon, K., and Borgaonkar, R. (2012).
New privacy issues in mobile telephony: fix and verification.
In *the ACM Conference on Computer and Communications Security, CCS'12*, pages 205–216. ACM.