

Real World Deniability in Messaging

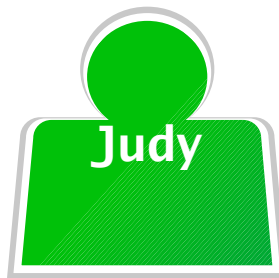
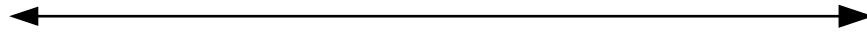
Daniel Collins, Simone Colombo, Loïs Huguenin–Dumittan
EPFL, Lausanne, Switzerland
ia.cr/2023/403

Deniability?

Moxie Marlinspike: “If someone receives an OTR [Off–The–Record] message from you, they can be absolutely sure you sent it (rather than having been forged by some third party), but can’t prove to anyone else that it was a message you wrote.”

Reference: <https://signal.org/blog/simplifying-otr-deniability/>

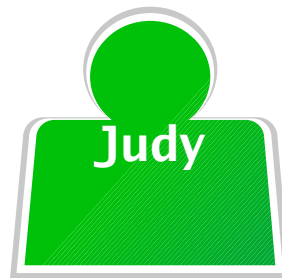
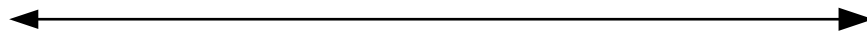
Deniability?



Deniability?



"Let's go to the protest!" -A
"I don't want to" -B

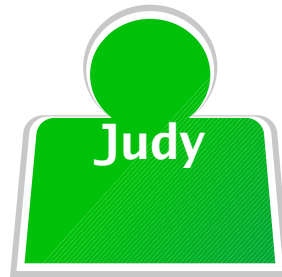


Deniability?

Judge, here's the conversation!
Alice sent me this!



"Let's go to the protest!" -A
"I don't want to" -B



Deniability?

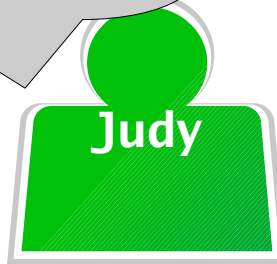
Judge, here's the conversation!
Alice sent me this!



"Let's go to the protest!" -A
"I don't want to" -B



But one can easily fabricate
this transcript...
This is inadmissible.



Deniability?

- **Claimed by different primitives and protocols.**

Deniability?

- **Claimed by different primitives and protocols.**
- **Many flavours (online/offline, honest/malicious, ...)**

Deniability?

- **Claimed by different primitives and protocols.**
- **Many flavours (online/offline, honest/malicious, ...)**
- **Ongoing (long-term) debate in the community on its relevance.**

Overview

- **The pitfalls of deniability from a**
 - **Technical perspective; and a**
 - **Legal and social perspective.**

Overview

- **The pitfalls of deniability from a**
 - **Technical perspective; and a**
 - **Legal and social perspective.**
- **Can we fix this? A potential solution.**

Case Study: Signal

- **Uses X3DH and the Double Ratchet.**

Case Study: Signal

- **Uses X3DH and the Double Ratchet.**
- **Claims that X3DH provides deniability.**

Case Study: Signal

- **Uses X3DH and the Double Ratchet.**
- **Claims that X3DH provides deniability.**
- **Many recent works consider X3DH's deniability [UG15, UG18], [VGIK20], [HKKP21, HKKP22], [BFGJS22].**

Case Study: Signal

- **Vatandas et al. [VGIK20] show that:**
 - **X3DH is “deniable”.**
 - **X3DH “deniable” \Rightarrow Double Ratchet “deniable”.**

Case Study: Signal

- **Vatandas et al. [VGIK20] show that:**
 - **X3DH is “deniable”.**
 - **X3DH “deniable” => Double Ratchet “deniable”.**
- **Great!**

Case Study: Signal

- **What's on top of X3DH/the Double Ratchet?**

Case Study: Signal

- **What's on top of X3DH/the Double Ratchet?**
- **Signal has two authentication modes: "regular" and "sealed sender".**

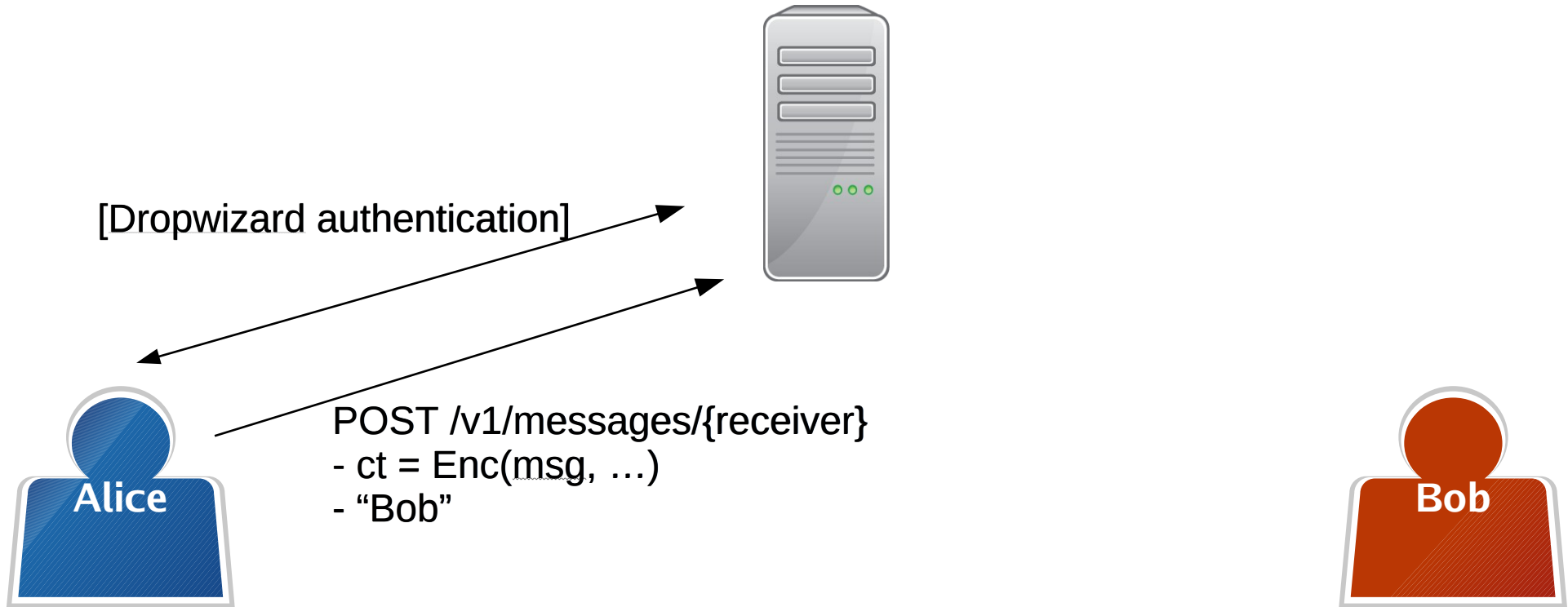
Case Study: Signal

- What's on top of X3DH/the Double Ratchet?
- Signal has two authentication modes: "regular" and "sealed sender".
- These render Signal fairly *undeniable* in practice.

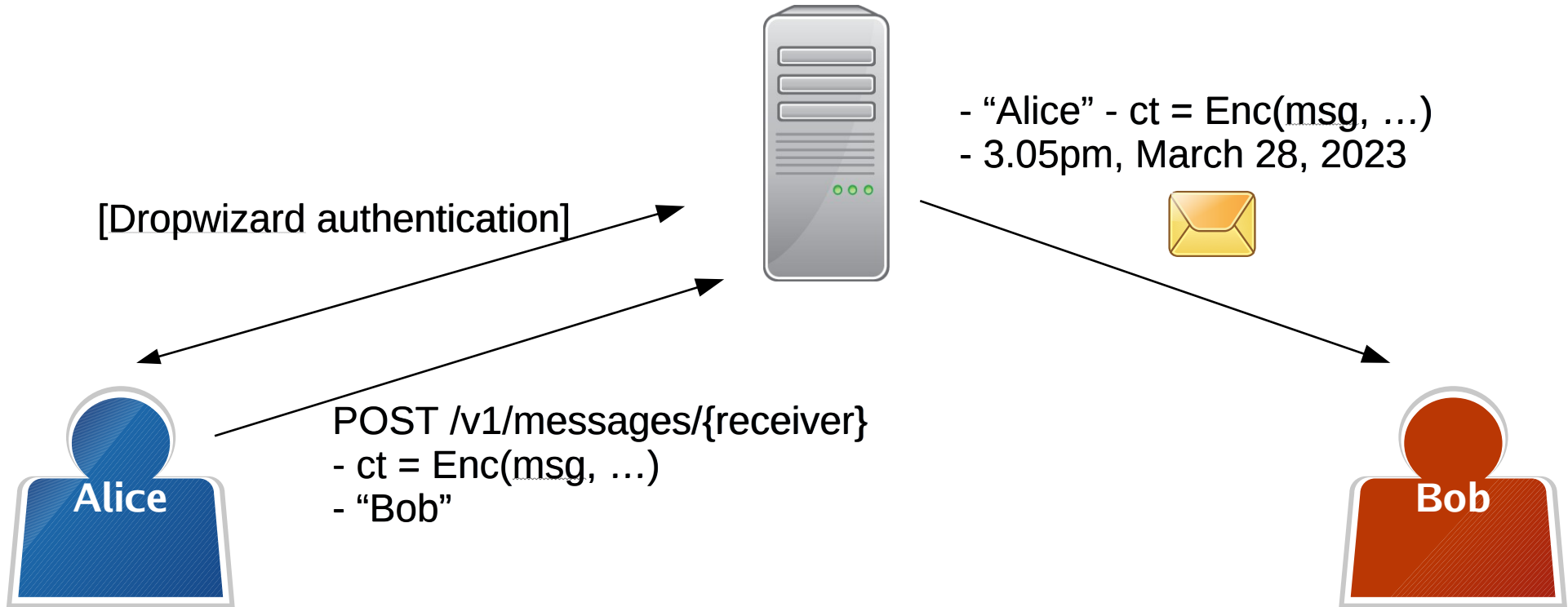
Signal with “regular” authentication



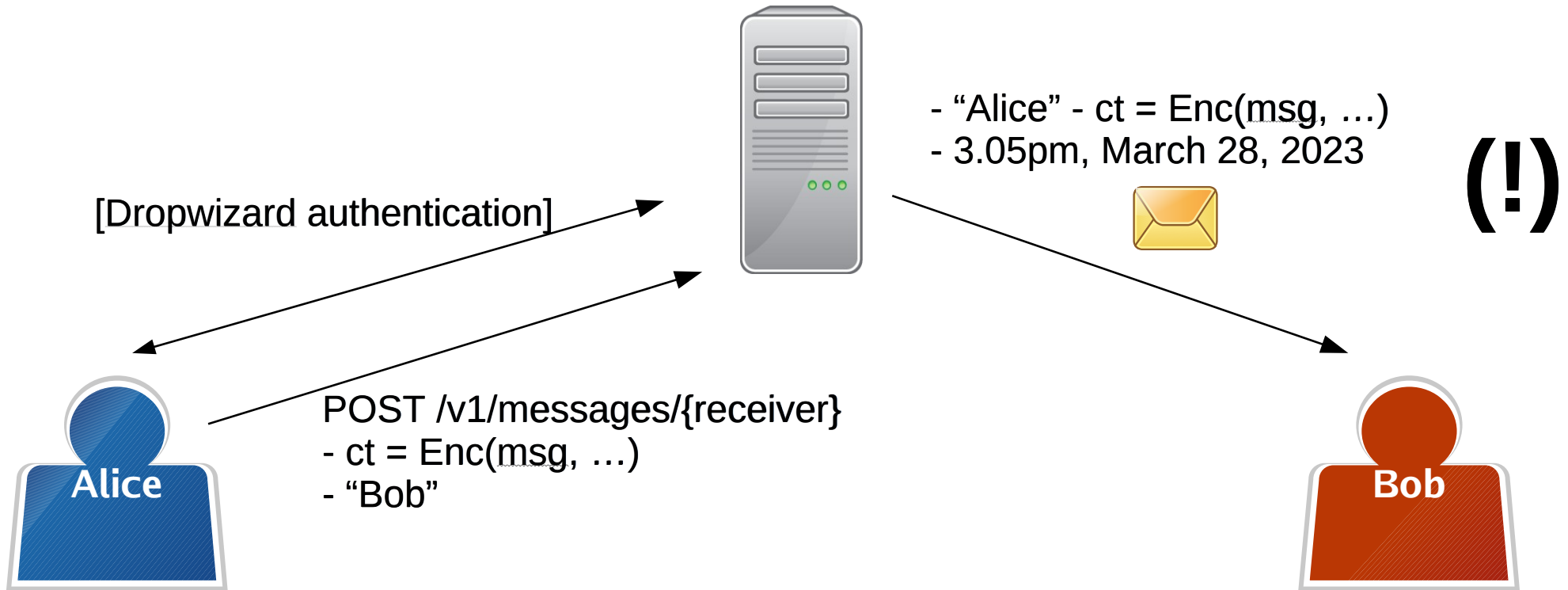
Signal with “regular” authentication



Signal with “regular” authentication



Signal with “regular” authentication



Signal with “regular” authentication: deniability

- **If a judge takes Bob’s phone, either the message came from Alice or Bob modified his messages.**

Signal with “regular” authentication: deniability

- If a judge takes Bob’s phone, either the message came from Alice or Bob modified his messages.
- Deniability depends on Bob’s *technical expertise*.

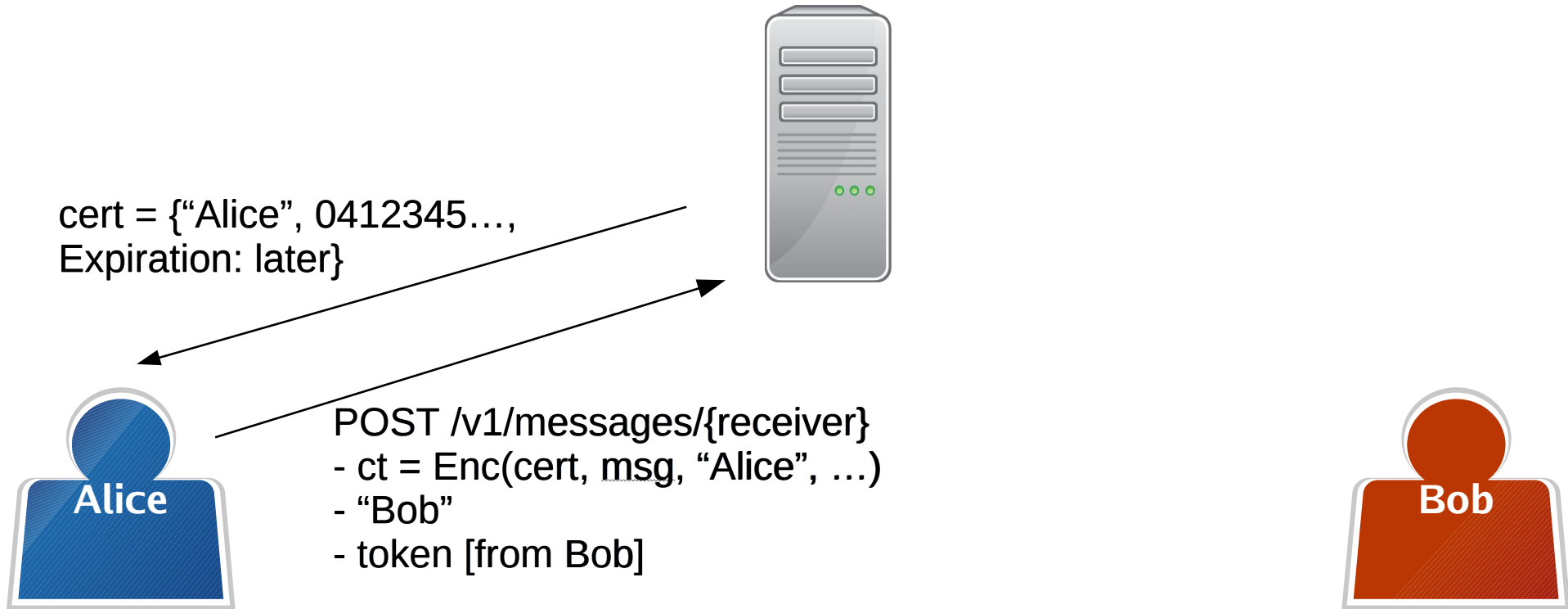
Signal with “regular” authentication: deniability

- If a judge takes Bob’s phone, either the message came from Alice or Bob modified his messages.
- Deniability depends on Bob’s *technical expertise*.
- (Even worse if the server stores logs).

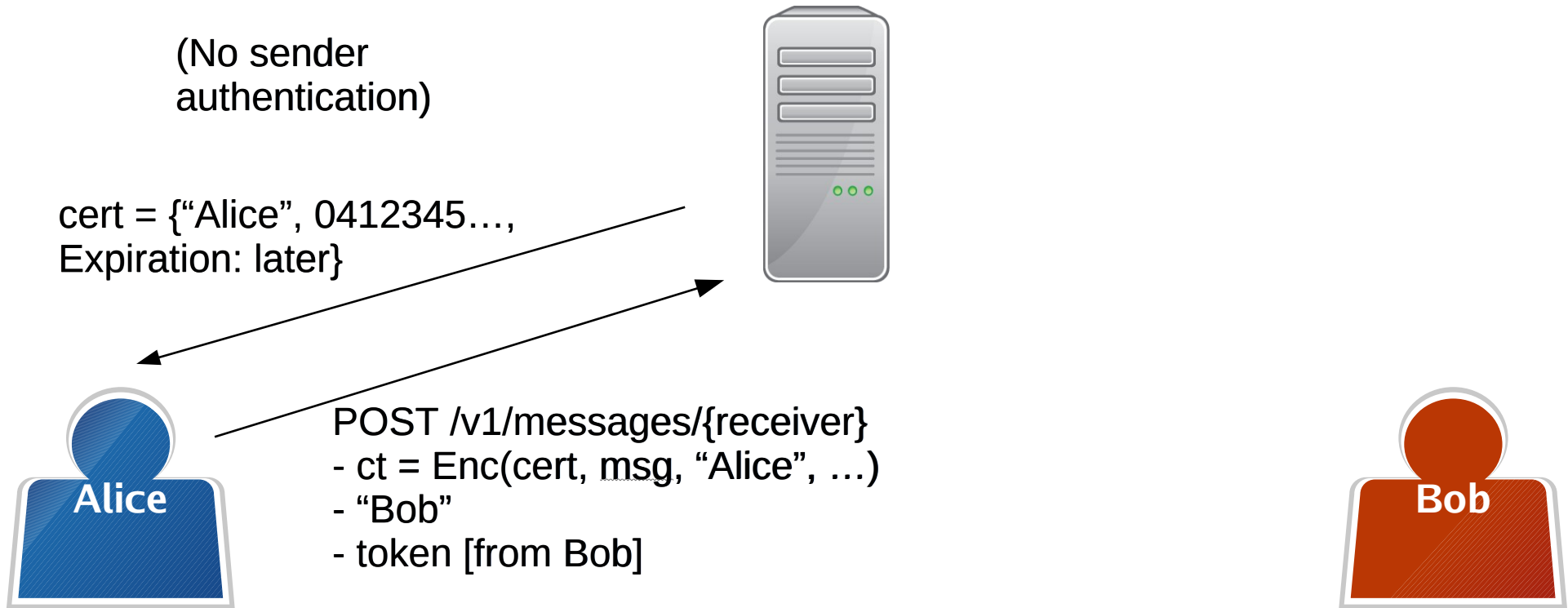
Signal with “sealed sender” authentication



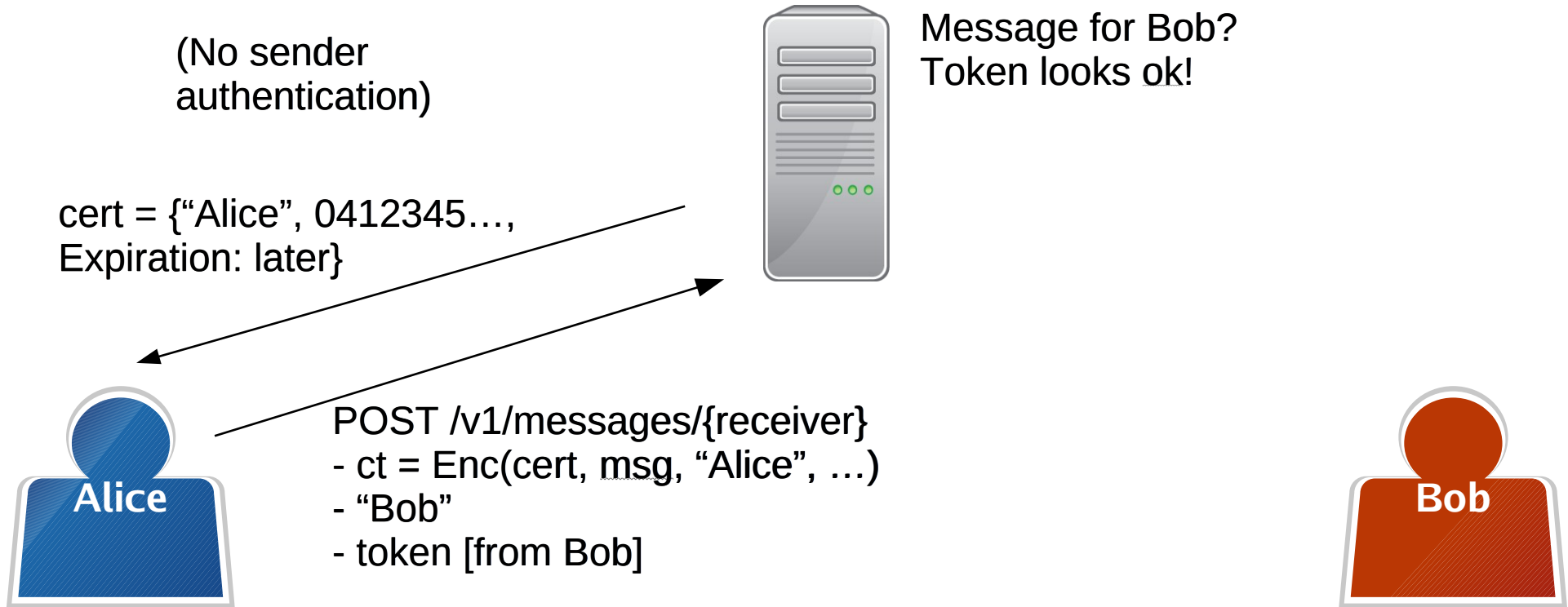
Signal with “sealed sender” authentication



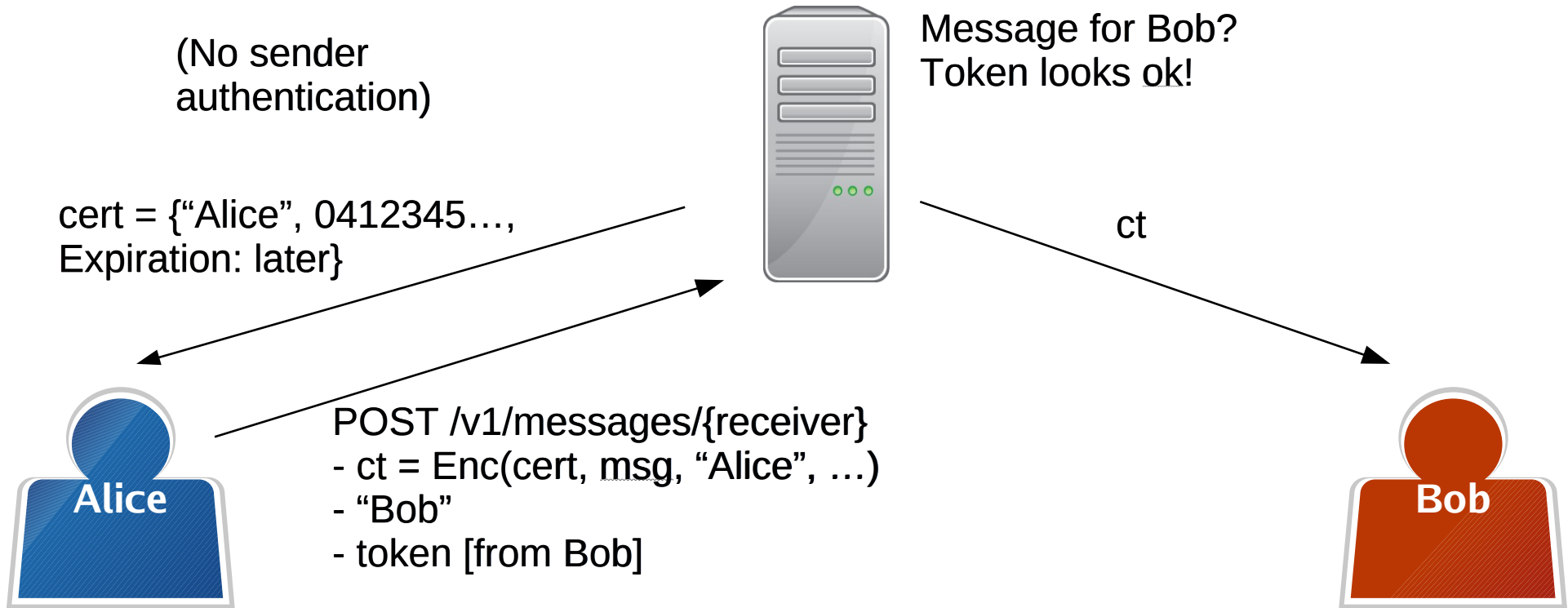
Signal with “sealed sender” authentication



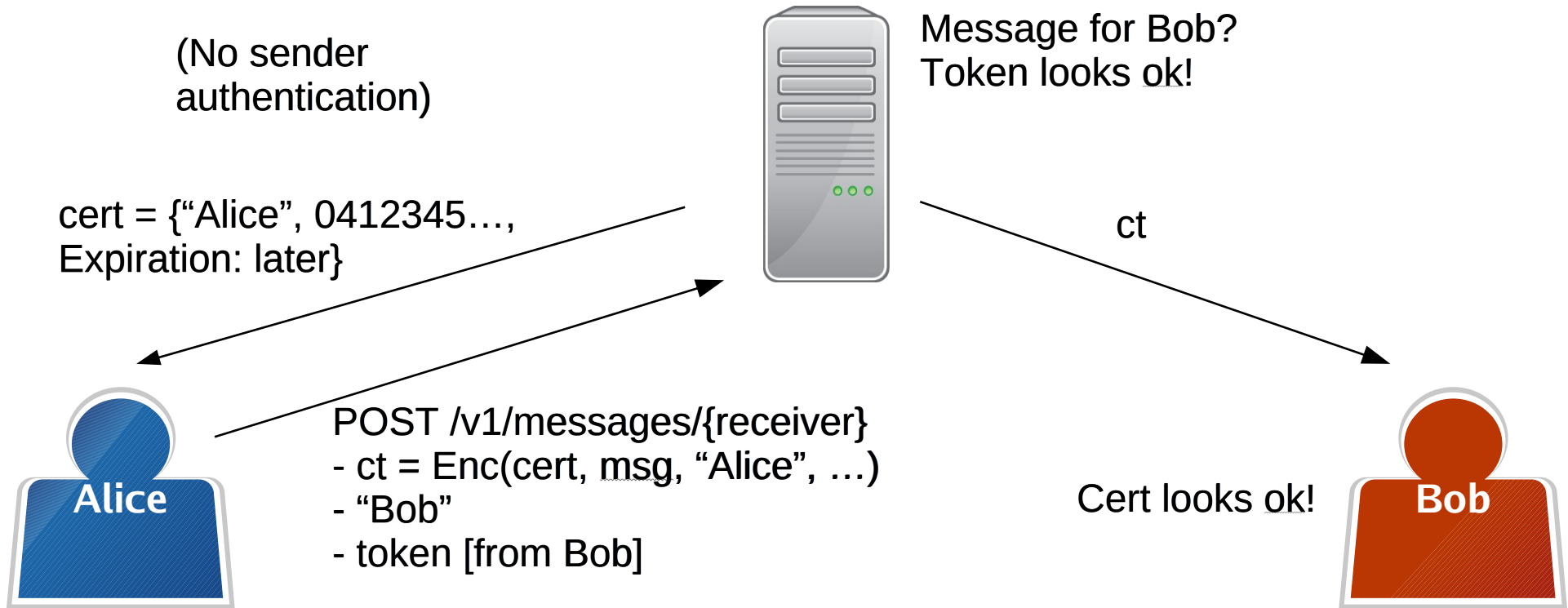
Signal with “sealed sender” authentication



Signal with “sealed sender” authentication



Signal with “sealed sender” authentication



Signal with “sealed sender” authentication

- **Enabled by default only between mutual contacts.**

Signal with “sealed sender” authentication

- **Enabled by default only between mutual contacts.**
- **(Network adversary can break anonymity).**

Signal with “sealed sender” authentication

- **Enabled by default only between mutual contacts.**
- **(Network adversary can break anonymity).**
- **Alice’s certificate must have been recently sent to Bob or someone Bob knows! Unlikely.**

Is deniability used?

Court cases in French-speaking Switzerland

- Openly accessible case data.

ine.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

JURISPRUDENCE DU TRIBUNAL CANTONAL

[Derniers arrêts publiés](#) | [Nouvelle recherche](#)

Décision

N° dossier: Type Année

Revue juridique:

Article de loi:

Titre/résumé:

Document: whatsapp

Date décision: au:

Date actualisation: au:

Rechercher Nb trouvés / page: 5 [aide complète en format pdf](#)

Critères de recherche:
Autorité: CCI or CC2 or ARAN or ARMC or ARMP or ASLP or ASA or NOTA or ASSLP or ATS or CHAC or CHAR or CCIV or CC or CACIV or CA or CCC or CCP or CDP or CMP
Document: whatsapp

résultats: 1 - 5 de 36 fiche(s) trouvée(s)

Is deniability used?

Court cases in French-speaking Switzerland

- Openly accessible case data.
- No mention of Signal.

ine.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

JURISPRUDENCE DU TRIBUNAL CANTONAL

[Derniers arrêts publiés](#) | [Nouvelle recherche](#)

Décision

N° dossier: Type Année

Revue juridique:

Article de loi:

Titre/résumé:

Document: whatsapp

Date décision: au:

Date actualisation: au:

Rechercher Nb trouvés / page: 5 [aide complète en format pdf](#)

Critères de recherche:
Autorité: 'CCI' or 'CC2' or 'ARAN' or 'ARMC' or 'ARMP' or 'ASLP' or 'ASA' or 'NOTA' or 'ASSLP' or 'ATS' or 'CHAC' or 'CHAR' or 'CCIV' or 'CC' or 'CACIV' or 'CA' or 'CCC' or 'CCP' or 'CDP' or 'CMP'

Document: whatsapp

résultats: 1 - 5 de 36 fiche(s) trouvée(s)

Is deniability used?

Court cases in French-speaking Switzerland

- Openly accessible case data.
- No mention of Signal.
- Lots of mentions of WhatsApp.

ine.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

JURISPRUDENCE DU TRIBUNAL CANTONAL

[Derniers arrêts publiés](#) | [Nouvelle recherche](#)

Décision

N° dossier: Type Année

Revue juridique:

Article de loi:

Titre/résumé:

Document: whatsapp

Date décision: au:

Date actualisation: au:

Nb trouvés / page: 5 [aide complète en format pdf](#)

Critères de recherche:
Autorité: 'CCI' or 'CC2' or 'ARAN' or 'ARMC' or 'ARMP' or 'ASLP' or 'ASA' or 'NOTA' or 'ASSLP' or 'ATS' or 'CHAC' or 'CHAR' or 'CCIV' or 'CC' or 'CACIV' or 'CA' or 'CCC' or 'CCP' or 'CDP' or 'CMP'

Document: whatsapp

résultats: 1 - 5 de 36 fiche(s) trouvée(s)

Is deniability used?

Court cases in French-speaking Switzerland

- Openly accessible case data.
- No mention of Signal.
- Lots of mentions of WhatsApp.
- One failed challenge to a transcript's validity.

ine.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

JURISPRUDENCE DU TRIBUNAL CANTONAL

[Derniers arrêts publiés](#) | [Nouvelle recherche](#)

Décision

N° dossier: Type Année ?

Revue juridique: ?

Article de loi: ?

Titre/résumé: ?

Document: whatsapp ?

Date décision: au: ?

Date actualisation: au: ?

Rechercher Nb trouvés / page: 5 [aide complète en format pdf](#)

Critères de recherche:
Autorité: CCI or CC2 or ARAN or ARMC or ARMP or ASLP or ASA or NOTA or ASSLP or ATS or CHAC or CHAR or CCIV or CC or CACIV or CA or CCC or CCP or CDP or CMP
Document: whatsapp

résultats: 1 - 5 de 36 fiche(s) trouvée(s)

Is deniability used? Court cases in the US

- Signal in high-profile cases (United States v. Rhodes et al., United States v. Jarret Crisler...)

no signal

SupersaiyanStatik SupersaiyanStatik (owner)

It's on the news. 2 of them I only shot twice meaning I ain't miss a shot

10/26/2020 8:02:59 PM(UTC-4)

Source Extraction:

Legacy

Source Info:

00008030-00114C920E9A802E_files_partial-afu.zip/private/var/mobile/Containers/Shared/AppGroup/92097A4F-38D4-42F7-AB93-83DD8744714E/grdb/signal.sqlite/signal.sqlite.decrypted : 0x14D12D0 (Table: model_TSInteraction, model_OWSUserProfile, Size: 22642688 bytes)

SupersaiyanStatik SupersaiyanStatik (owner)

Greatest shot in the world U tryna challenge me? Lol

10/26/2020 8:03:13 PM(UTC-4)

Is deniability used? Court cases in the US

- Signal in high-profile cases (United States v. Rhodes et al., United States v. Jarret Crisler...)
- Seemingly uncontested.

noisy

SupersaiyanStatik SupersaiyanStatik (owner)

It's on the news. 2 of them I only shot twice meaning I ain't miss a shot

10/26/2020 8:02:59 PM(UTC-4)

Source Extraction:
Legacy

Source Info:
00008030-00114C920E9A802E_files_partial-afu.zip/private/var/mobile/Containers/Shared/AppGroup/92097A4F-38D4-42F7-AB93-83DD8744714E/grdb/signal.sqlite/signal.sqlite.decrypted : 0x14D12D0 (Table: model_TSIinteraction, model_OWSUserProfile, Size: 22642688 bytes)

SupersaiyanStatik SupersaiyanStatik (owner)

Greatest shot in the world U tryna challenge me? Lol

10/26/2020 8:03:13 PM(UTC-4)

Why has deniability not caught on?

- **Lack of awareness/technical knowledge.**

Why has deniability not caught on?

- **Lack of awareness/technical knowledge.**
- **Evidence contains a lot more than phone transcripts.**

Why has deniability not caught on?

- **Lack of awareness/technical knowledge.**
- **Evidence contains a lot more than phone transcripts.**
- **Forgeries/false testimony disincentivised due to being illegal.**

Can we make deniability catch on?

- **Phones reveal a lot to a judge.**

Can we make deniability catch on?

- **Phones reveal a lot to a judge.**
- **Parties can claim tampering, but depends on technical ability and not easy to explain.**

A possible solution

- **Sent/received messages can be *edited* in a messaging app's GUI.**

A possible solution

- **Sent/received messages can be *edited* in a messaging app's GUI.**
- **[RMAMM23] suggests it could improve deniability!**

Do we even want deniability?

- **Pros: Could protect people.**
- **Cons: Could protect people.**

Do we even want deniability?

- **Pros: Could protect people.**
- **Cons: Could protect people.**
- **Practical deniability amplifies *both* of these aspects.**

Take-home: making a deniable system

- **Who are you defending against?**

Take-home: making a deniable system

- **Who are you defending against?**
- **Signal/WhatsApp/...: phone numbers aren't too deniable.**

Take-home: making a deniable system

- **Who are you defending against?**
- **Signal/WhatsApp/...: phone numbers aren't too deniable.**
- **Practical/explainable deniability is better.**

Take-home: making a deniable system

- **Who are you defending against?**
- **Signal/WhatsApp/...: phone numbers aren't too deniable.**
- **Practical/explainable deniability is better.**
- **Minimise metadata/auxiliary information (Signal is the best here).**

Take-home: making a deniable system

- **Who are you defending against?**
- **Signal/WhatsApp/...: phone numbers aren't too deniable.**
- **Practical/explainable deniability is better.**
- **Minimise metadata/auxiliary information (Signal is the best here).**
- **Anonymity may be better for some applications.**

Let's continue the debate!
ia.cr/2023/403
Twitter: @dcol97

References

- [UG15] Unger, Goldberg: Deniable Key Exchanges for Secure Messaging, CCS'15
- [UG18] Unger, Goldberg: Improved Strongly Deniable Authenticated Key Exchanges for Secure Messaging, PoPETs 2018.1
- [VGIK20]: Vatandas, Gennaro, Ithurnburn, Krawczyk: On the Cryptographic Deniability of the Signal Protocol, ACNS 2020
- [HKKP21/22]: Hashimoto, Katsumata, Kwiatkowski, Prest: An Efficient and Generic Construction for Signal's Handshake (X3DH): Post-Quantum, State Leakage Secure, and Deniable, PKC 2021/JoC 2022
- [BFGJS22]: Brendel, Fiedler, Günther, Janson, Stebila: Post-quantum Asynchronous Deniable Key Exchange and the Signal Handshake, PKC 2022
- [RMAMM23]: Reitinger, Malkin, Akgul, Mazurek, Miers: Is Cryptographic Deniability Sufficient? Non-Expert Perceptions of Deniability in Secure Messaging, S&P 2023