Real World Deniability in Messaging

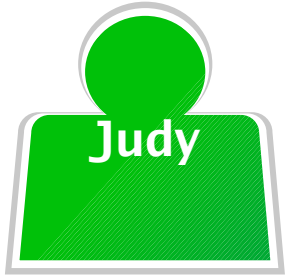
Daniel Collins, Simone Colombo, Loïs Huguenin–Dumittan
EPFL, Lausanne, Switzerland
ia.cr/2023/403

Deniability?

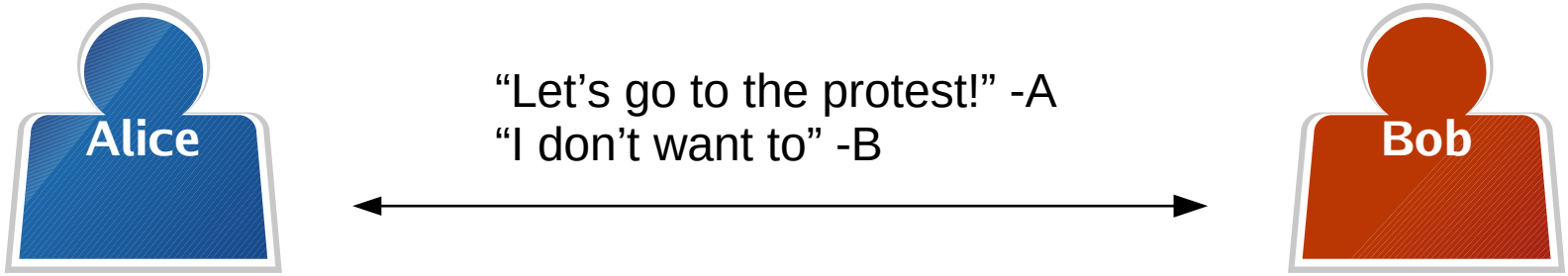
Moxie Marlinspike: "If someone receives an OTR [Off–The–Record] message from you, they can be absolutely sure you sent it (rather than having been forged by some third party), but *can't prove to anyone else that it was a message you wrote*."

Reference: https://signal.org/blog/simplifying–otr–deniability/

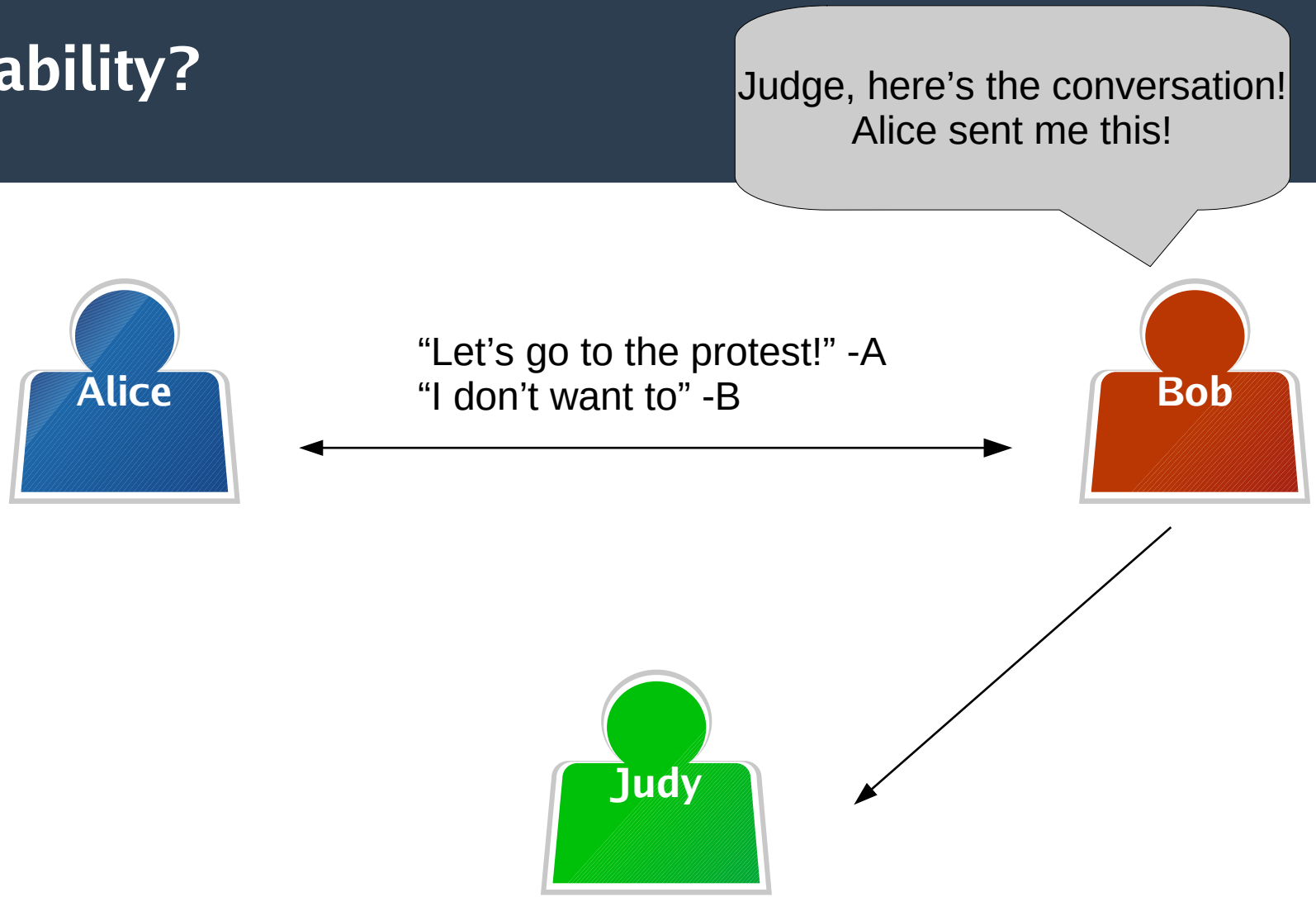
Deniability?



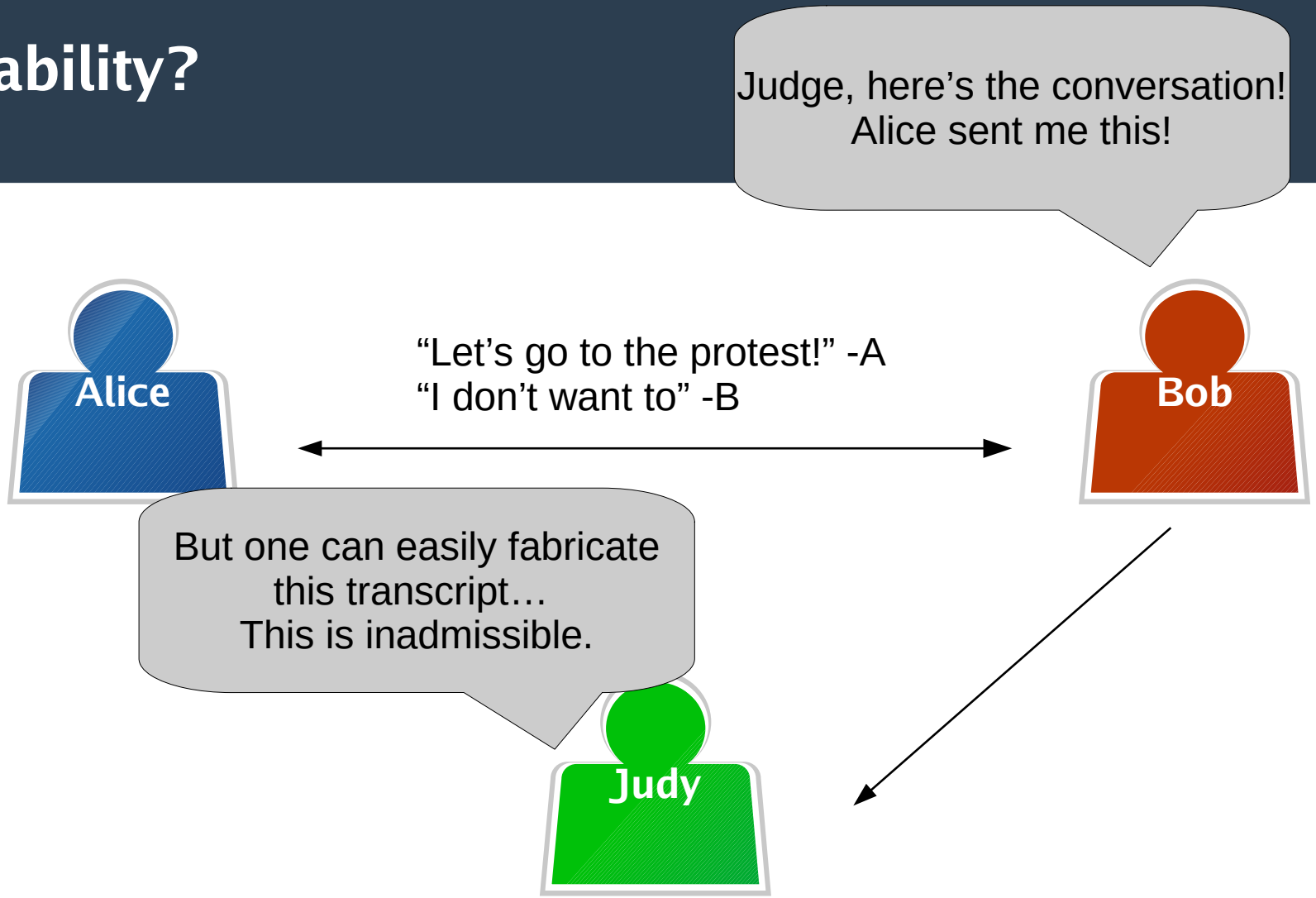
Deniability?



Deniability?



Deniability?



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” => 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

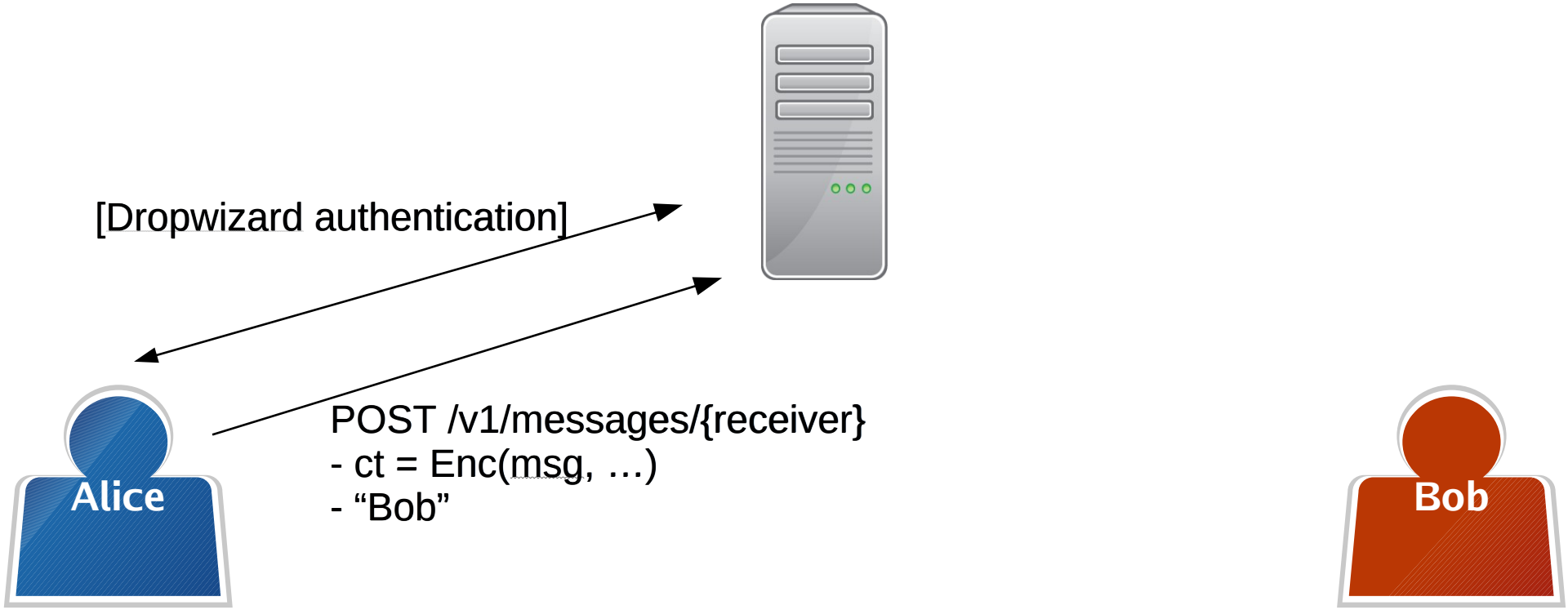
- What's on top of X3DH/the Double Ratchet?
- Signal has two authentication modes: ”regular” and “sealed sender”.

Case Study: Signal

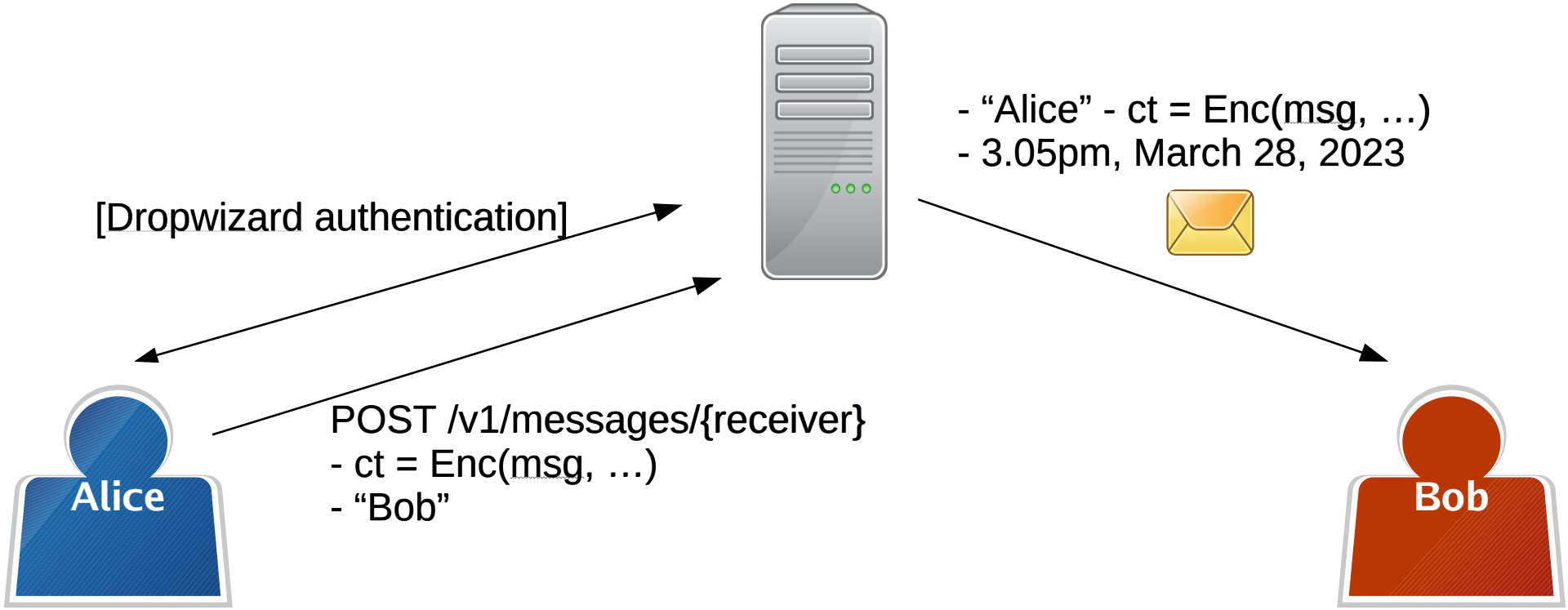
- What's on top of X3DH/the Double Ratchet?
- Signal has two authentication modes: ”regular” and “sealed sender”.
- These render Signal fairly *undeniable* in practice.

Signal with “regular” authentication

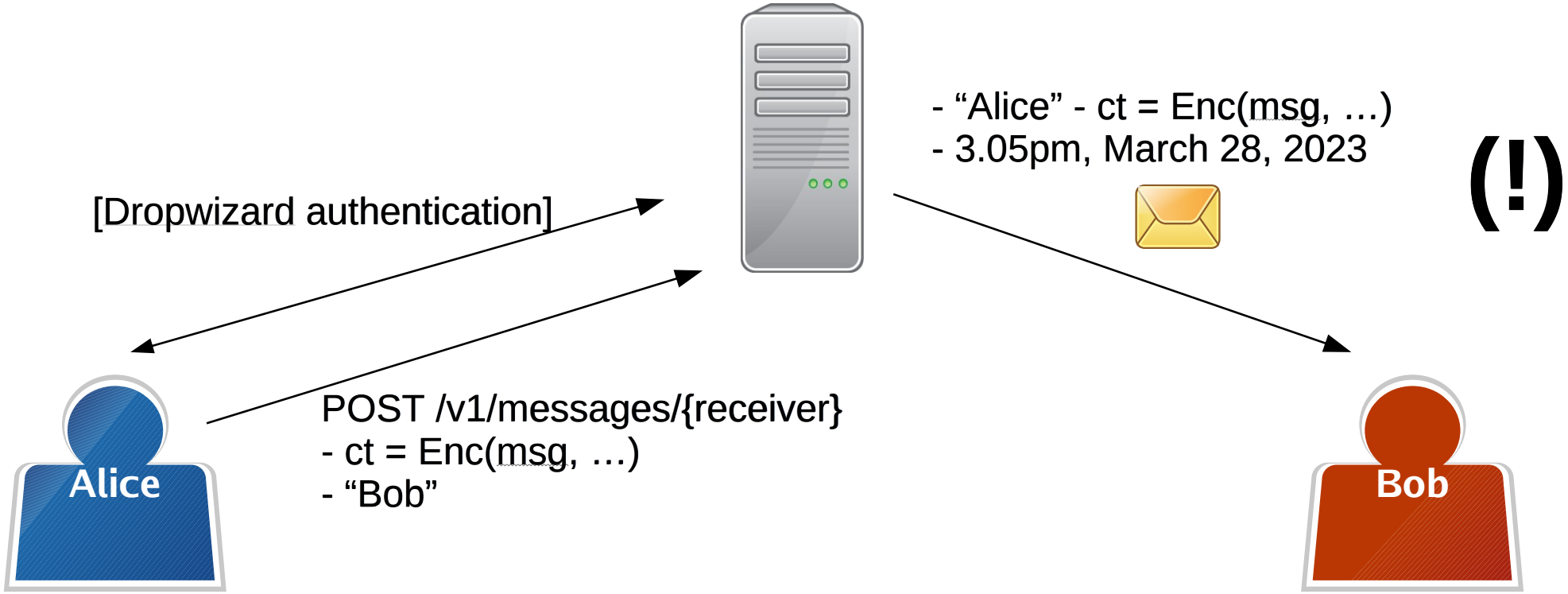
Signal with “regular” authentication



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

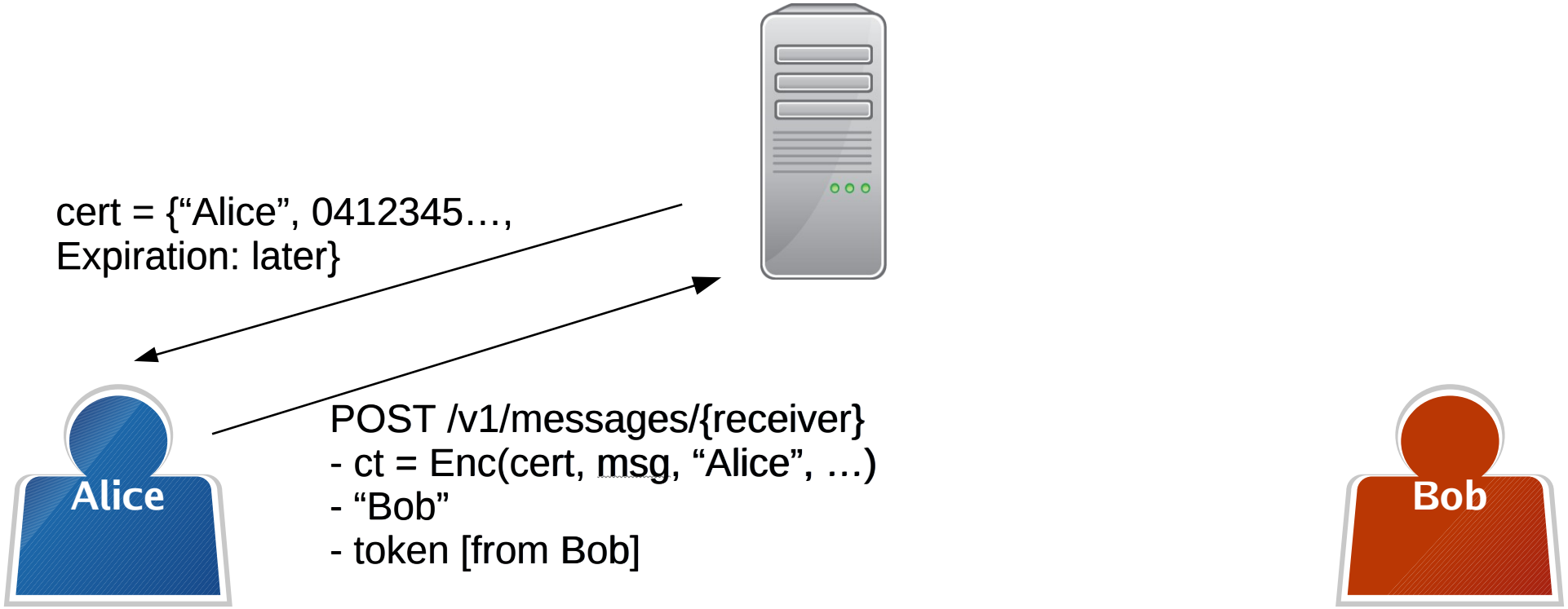
- If a judge takes Bob’s phone, either the message came from Alice or Bob modified his messages.
- Deniability depends on Bob’s *technical expertise*.

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

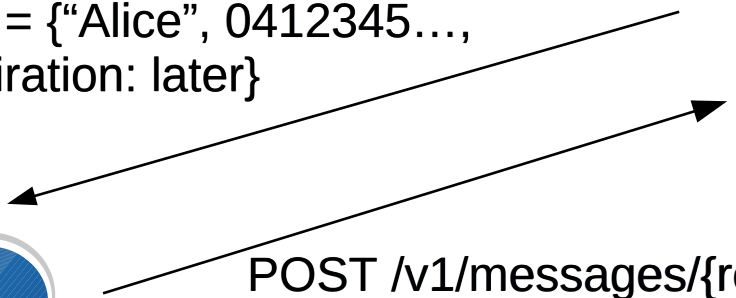
Signal with “sealed sender” authentication



Signal with “sealed sender” authentication

(No sender authentication)

cert = {“Alice”, 0412345…, Expiration: later}



POST /v1/messages/{receiver}
- ct = Enc(cert, msg, “Alice”, …)
- “Bob”
- token [from Bob]

Signal with “sealed sender” authentication

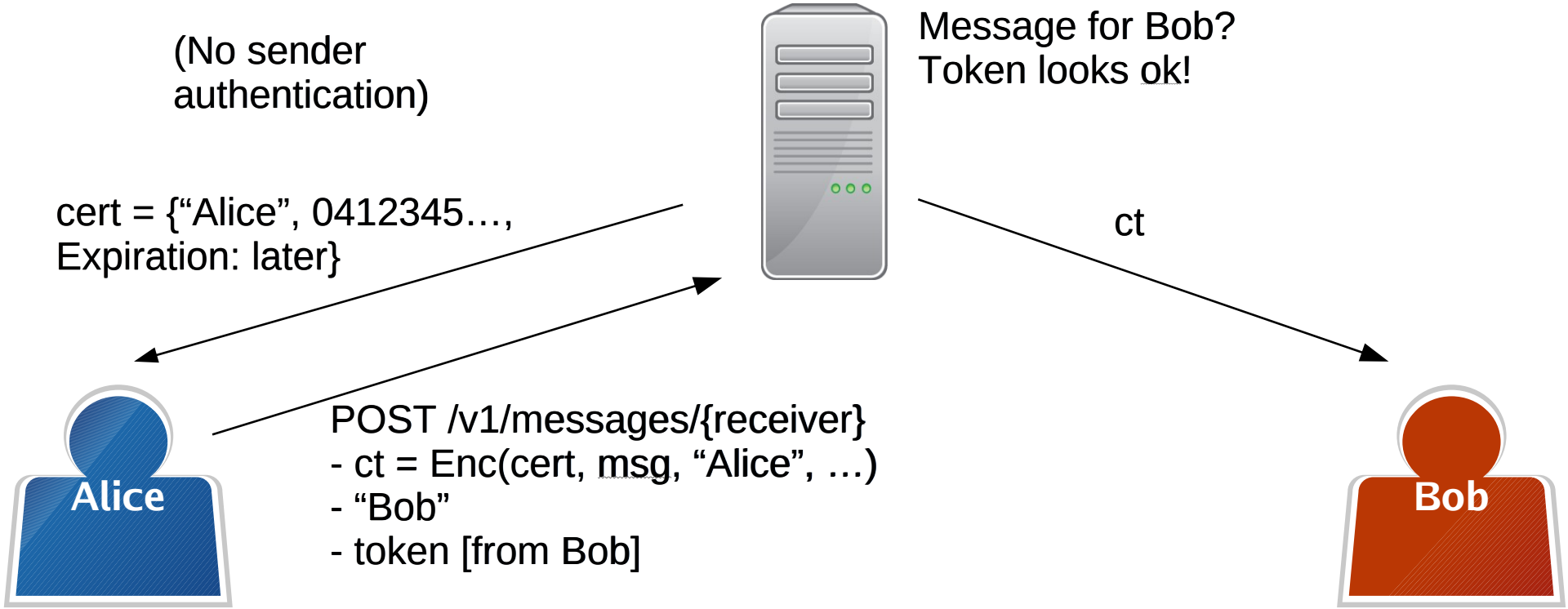
(No sender authentication)

Message for Bob?
Token looks ok!

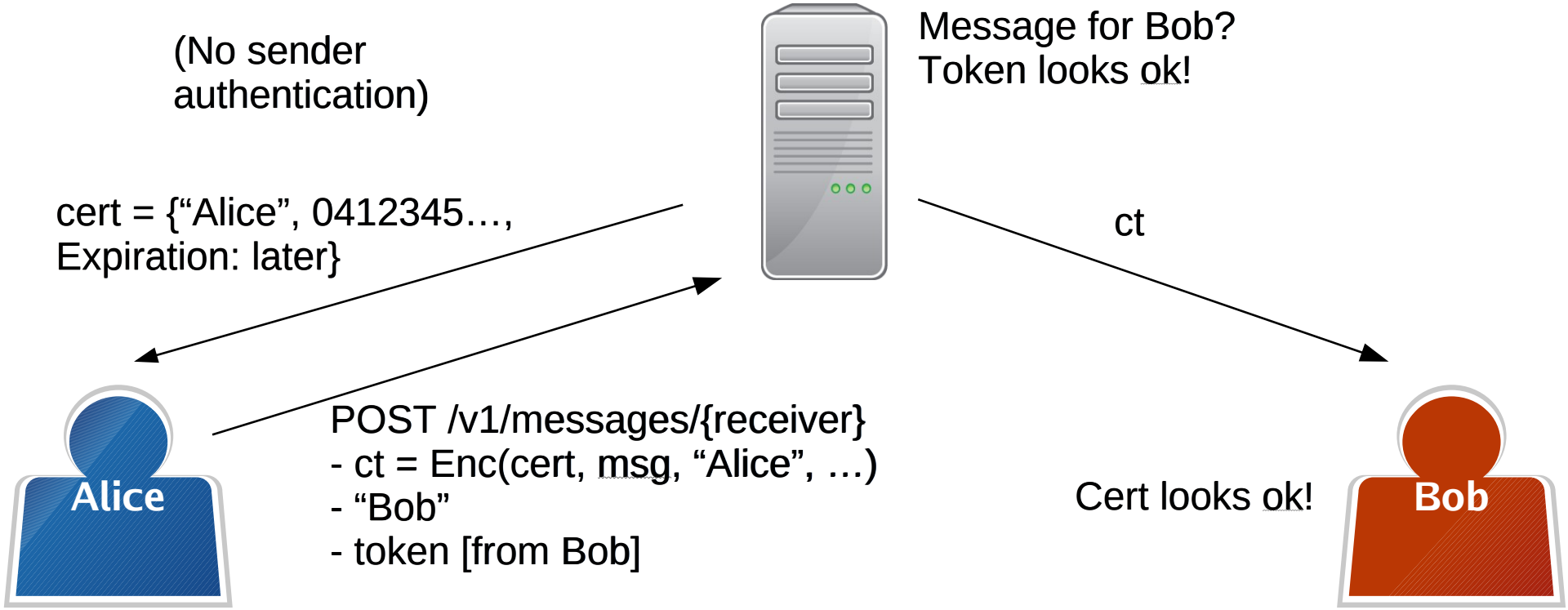
cert = {“Alice”, 0412345…,
Expiration: later}

POST /v1/messages/{receiver}
- ct = Enc(cert, msg, “Alice”, …)
- “Bob”
- token [from Bob]

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

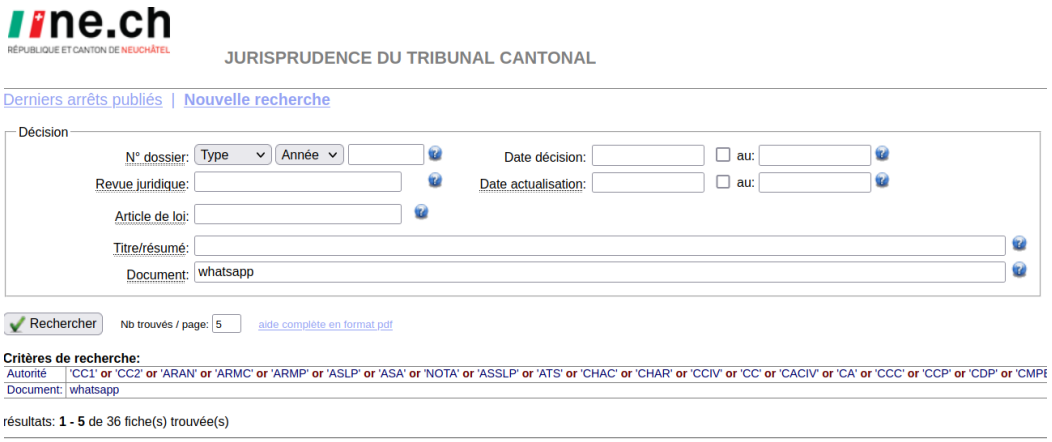
- Enabled by default only between mutual contacts.
- (Network adversary can break anonymity).

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.

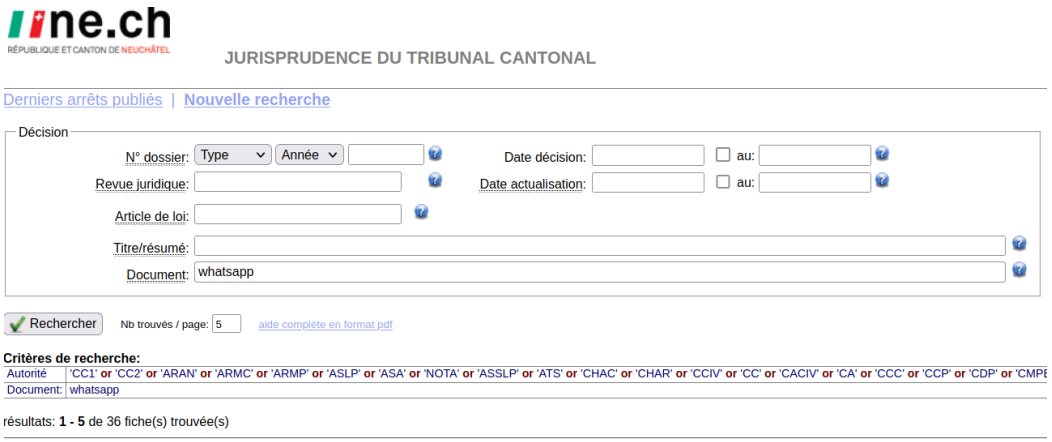
Is deniability used?
Court cases in French-speaking Switzerland

- Openly accessible case data.



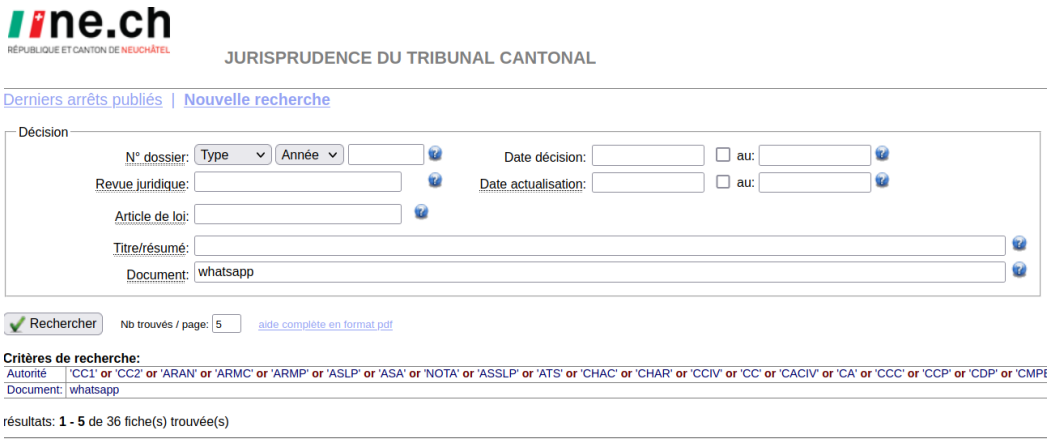
Is deniability used?
Court cases in French–speaking Switzerland

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



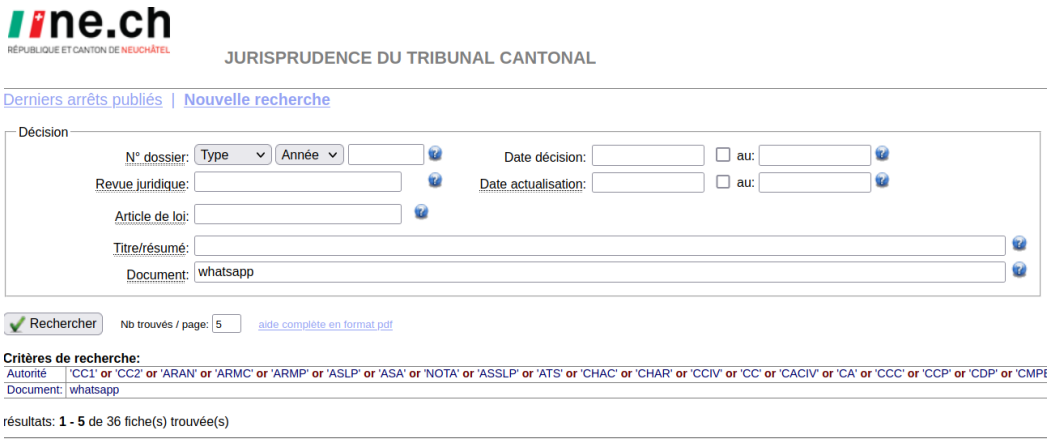
Is deniability used?
Court cases in French–speaking Switzerland

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



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.

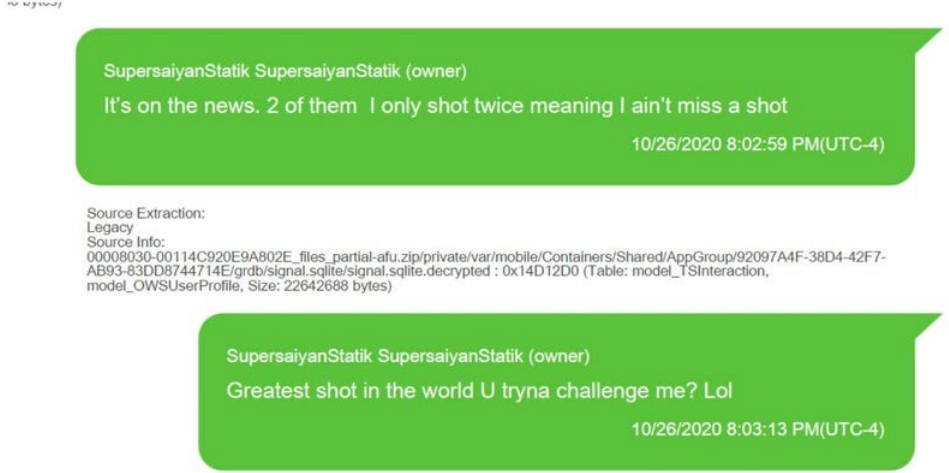


Is deniability used? Court cases in the US

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

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.



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, Ithurburn, 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