Deniability in Automated Contact Tracing

Christoph Günther

Krzysztof Pietrzak

PETS 2024

ISTA Institute of Science and Technology Austria

FWF Austrian Science Fund

SPyCoDe

This research was funded in whole or in part by the Austrian Science Fund (FWF) 10.55776/F85.

Automated contact tracing (ACT)

- **Contact tracing:** Notify users about contacts with infected users

Automated contact tracing (ACT)

- **Contact tracing:** Notify users about contacts with infected users
- **Automated:** Without human labor

Automated contact tracing (ACT)

- **Contact tracing:** Notify users about contacts with infected users
- **Automated:** Without human labor

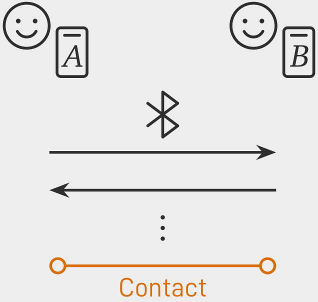
- A lot of research & development due to Covid-19

Automated contact tracing (ACT)

- **Contact tracing:** Notify users about contacts with infected users
- **Automated:** Without human labor

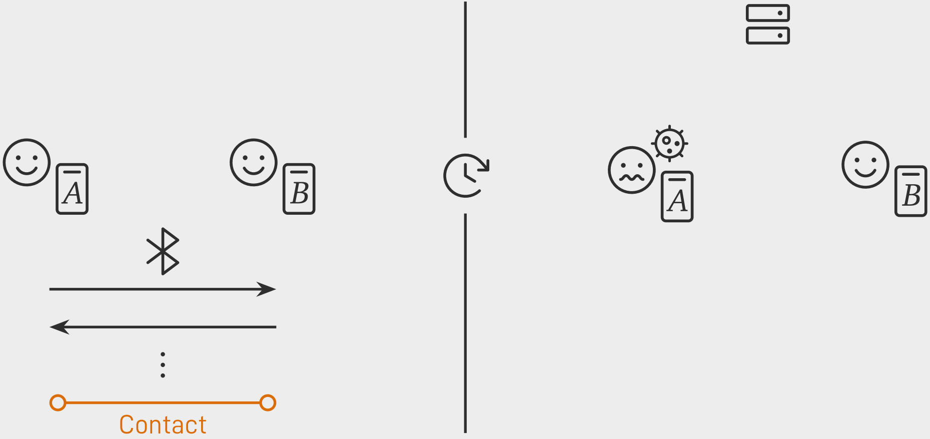
- A lot of research & development due to Covid-19
- Google and Apple jointly deployed protocol based on DP3T (Troncoso et al.)

ACT using Bluetooth Low Energy



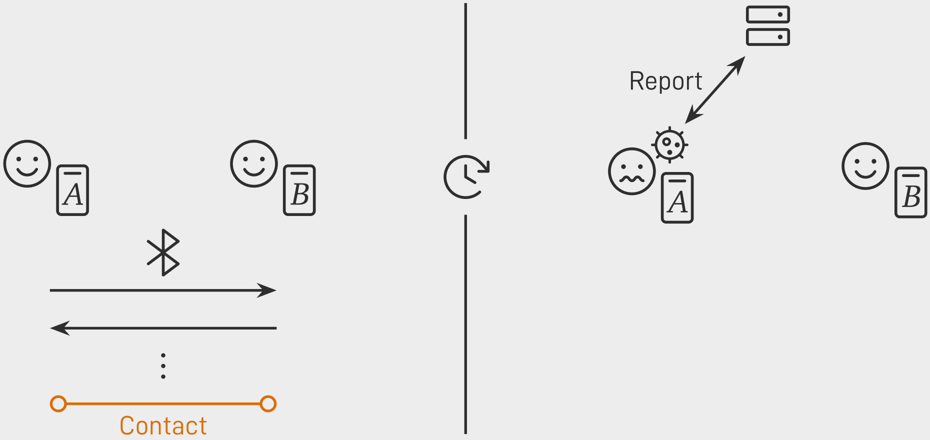
Icons by Phosphor licensed under MIT

ACT using Bluetooth Low Energy



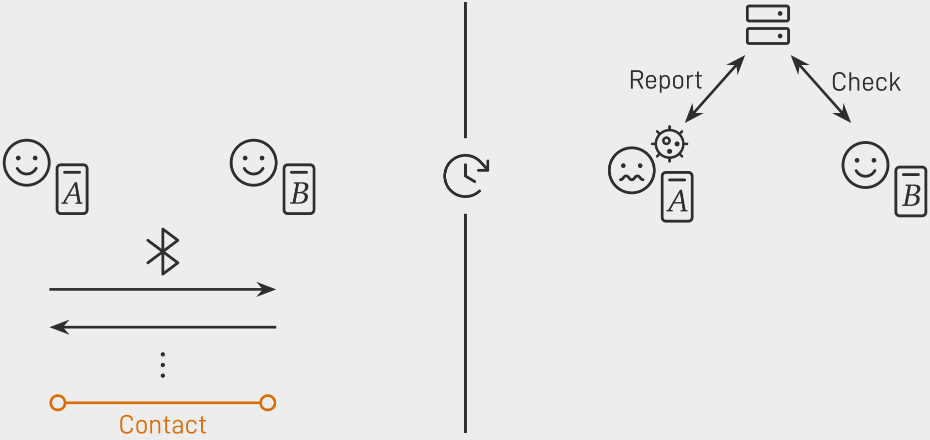
Icons by Phosphor licensed under MIT

ACT using Bluetooth Low Energy



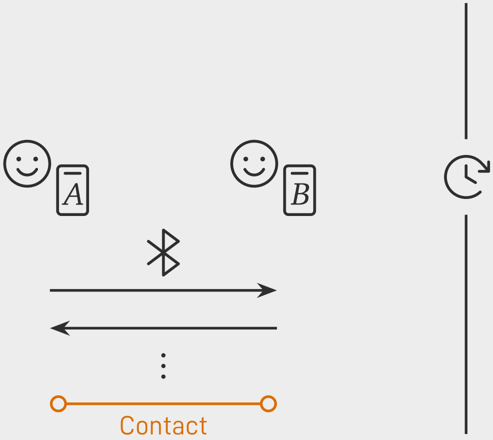
Icons by Phosphor licensed under MIT

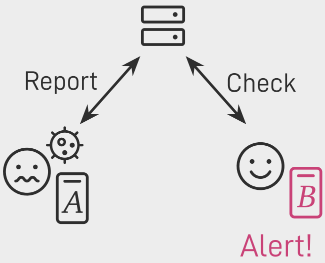
ACT using Bluetooth Low Energy



Icons by Phosphor licensed under MIT

ACT using Bluetooth Low Energy





Contact and A reported sick

$\Rightarrow$

B's check causes an alert

Icons by Phosphor licensed under MIT

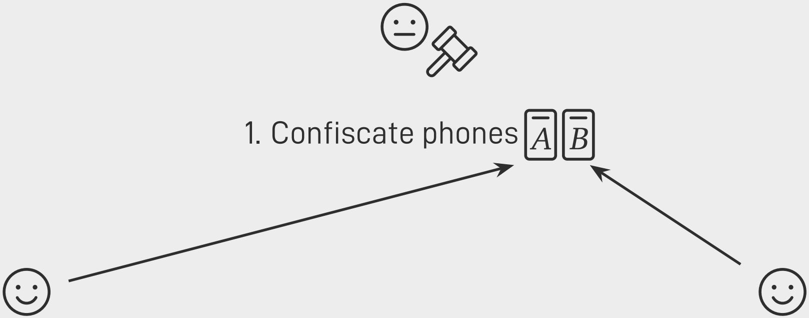
Privacy?

Digital evidence

Did A and B meet?

Digital evidence

Did A and B meet?



1. Confiscate phones

Digital evidence

Did A and B meet?

1. Confiscate phones A B
2. Report A

Digital evidence

Did A and B meet?

1. Confiscate phones A B
2. Report A
3. Check B

Digital evidence

Did A and B meet?

1. Confiscate phones A B
2. Report A
3. Check B

B got an alert $\Leftrightarrow$ A and B have met

Deniability

- User cannot deny having met by definition of ACT

Deniability

- User cannot deny having met by definition of ACT
- Misuse of the protocol!

Deniability

- User cannot deny having met by definition of ACT
- Misuse of the protocol!

Contact-time deniability

Did A and B meet at time t?

Deniability

- User cannot deny having met by definition of ACT
- Misuse of the protocol!

Contact-time deniability

Did A and B meet at time t?

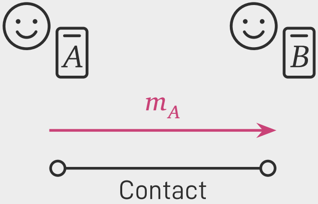
Impossibility result

Dilemma between contact-time deniability and security for a large class of protocols capturing many practically relevant ones

Impossibility result

Practical protocols are often…

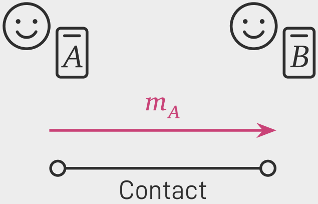
Unidirectional



Contact

Practical protocols are often…

Unidirectional



A

B

m_A

Contact

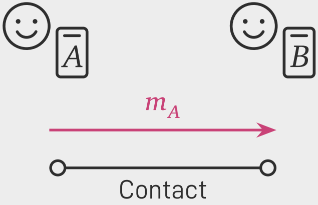
B received m_A and A reported sick

$\Rightarrow$

B's check causes an alert

Practical protocols are often…

Unidirectional

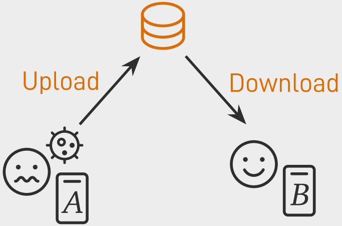


B received m_A and A reported sick

$\Rightarrow$

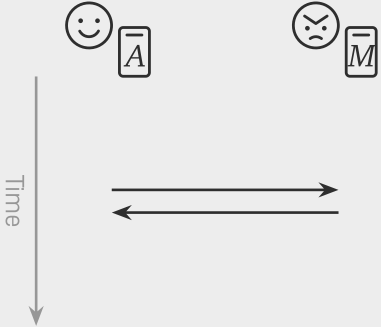
B's check causes an alert

Decentralized

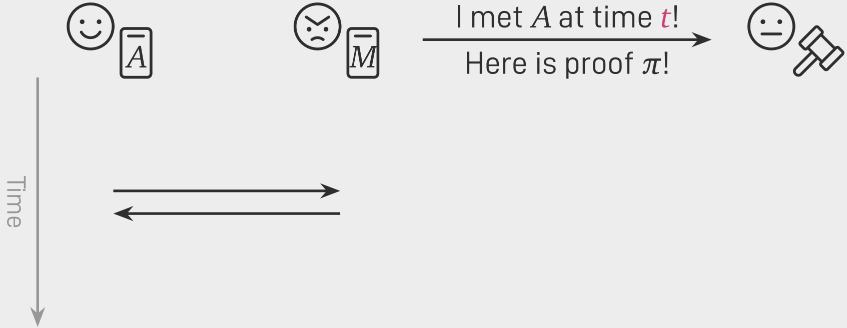


Server is a database

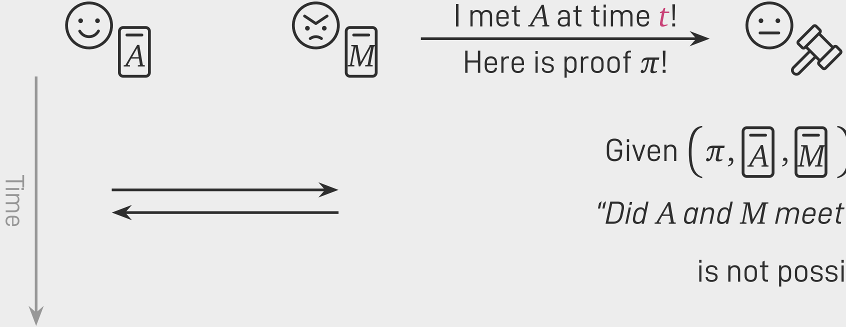
Contact-time deniability



Contact-time deniability



Contact-time deniability



I met A at time t!

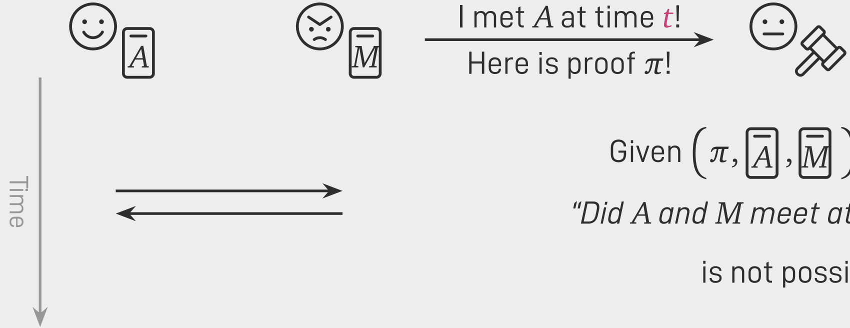
Here is proof π!

Given $\left(\pi, \boxed{A}, \boxed{M}\right)$, deciding

"Did A and M meet at time t?"

is not possible

Δ-contact-time deniability



I met A at time t!

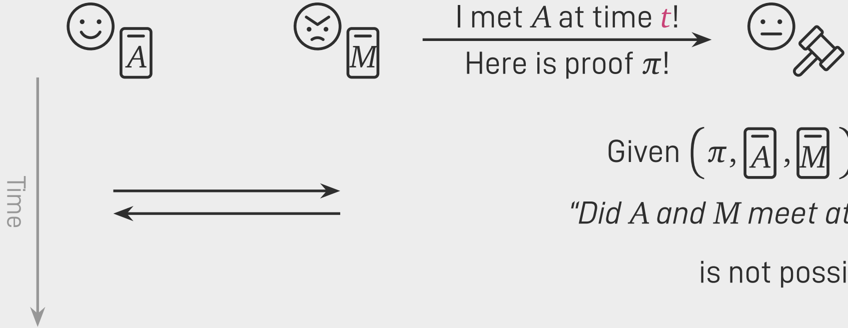
Here is proof π!

Given $\left(\pi, \boxed{A}, \boxed{M}\right)$, deciding

“Did A and M meet at time $t \pm \Delta$*?”*

is not possible

Δ-contact-time deniability



I met A at time t!

Here is proof π!

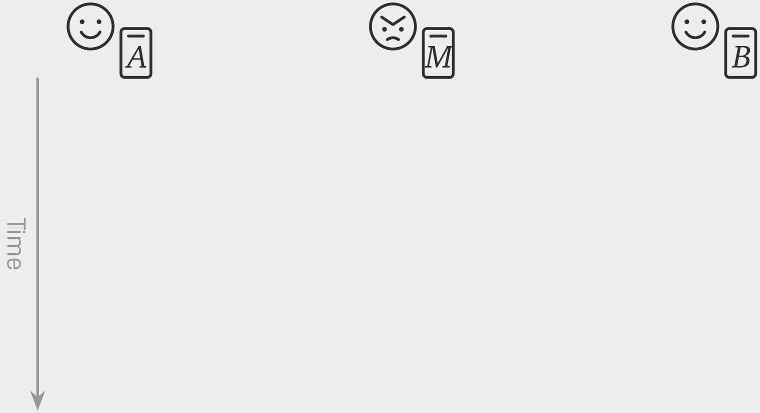
Given $\left(\pi, \boxed{A}, \boxed{M}\right)$, deciding

"Did A and M meet at time $t \pm \Delta$?"

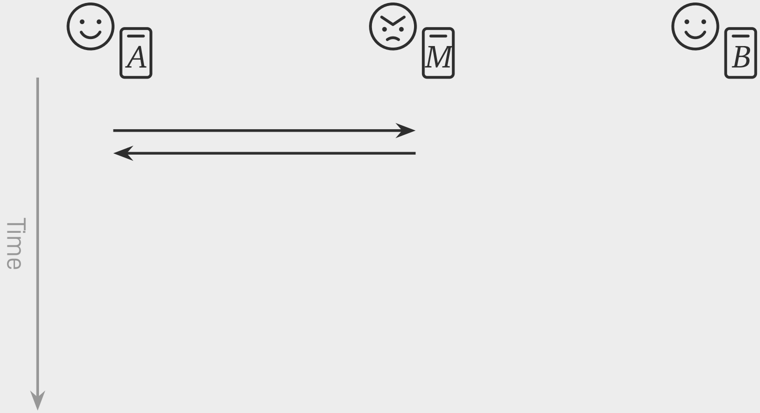
is not possible

Meaningful if large (e.g., a week)

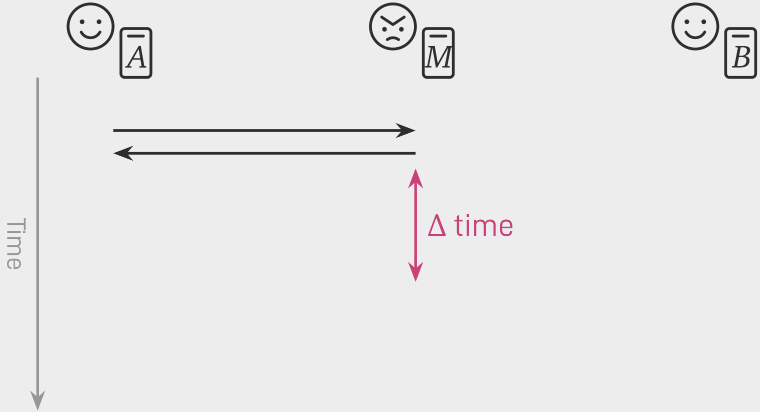
Δ-replay security



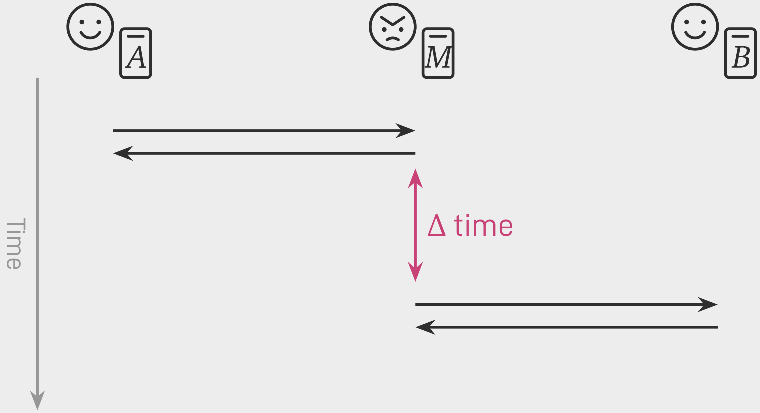
Δ-replay security



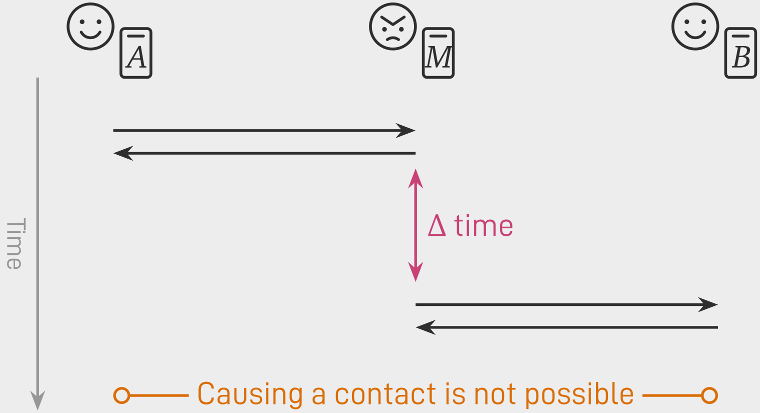
Δ-replay security



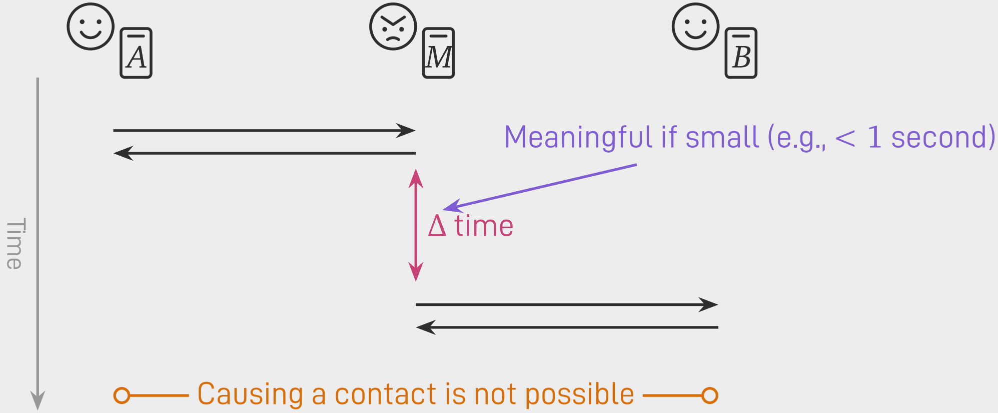
Δ-replay security



Δ-replay security



Δ-replay security



Meaningful if small (e.g., < 1 second)

Causing a contact is not possible

Main theorem

If a unidirectional, decentralized protocol is Δ-replay secure, then it can at most be Δ'-contact-time deniable with $\Delta > \Delta'$.

Main theorem

If a unidirectional, decentralized protocol is Δ-replay secure, then it can at most be Δ'-contact-time deniable with $\Delta > \Delta'$.

Problematic since

- Δ only meaningful if small
- Δ' only meaningful if large

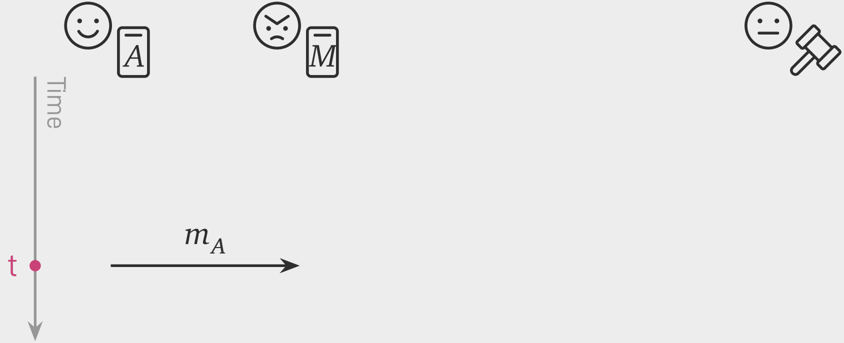
Proof

Want to show: Δ-replay secure ⇒ **not** Δ-contact-time deniable

$\bar{A}$
$\bar{M}$
Time

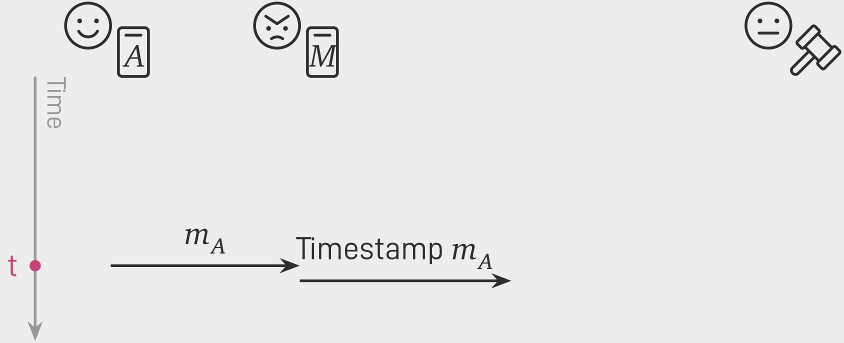
Proof

Want to show: Δ-replay secure ⇒ **not** Δ-contact-time deniable



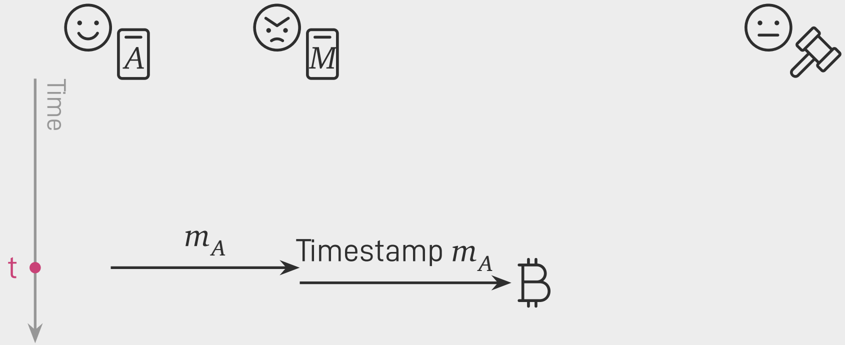
Proof

Want to show: Δ-replay secure ⇒ **not** Δ-contact-time deniable



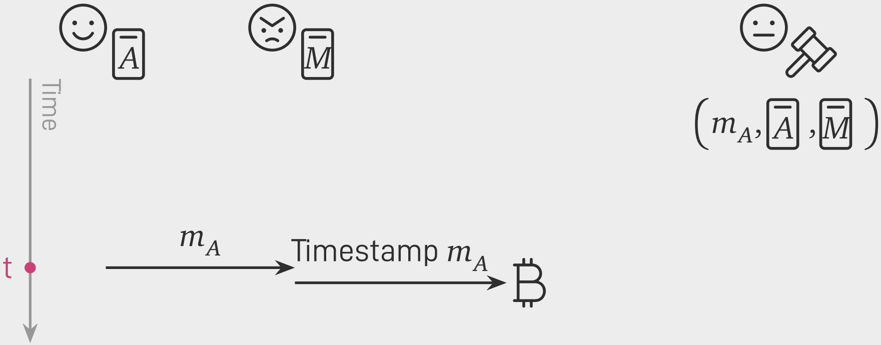
Proof

Want to show: Δ-replay secure ⇒ **not** Δ-contact-time deniable



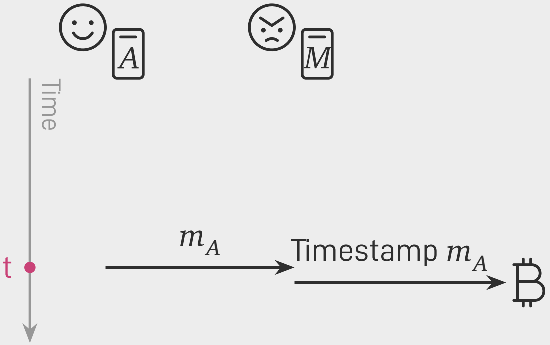
Proof

Want to show: Δ-replay secure ⇒ **not** Δ-contact-time deniable



Proof

Want to show: Δ-replay secure ⇒ **not** Δ-contact-time deniable

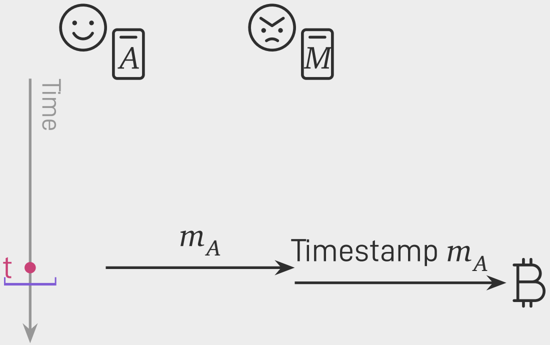


$(m_A, \boxed{A}, \boxed{M})$

1. Would receiving m_A at time t lead to contact with $\boxed{A}$?

Proof

Want to show: Δ-replay secure ⇒ **not** Δ-contact-time deniable



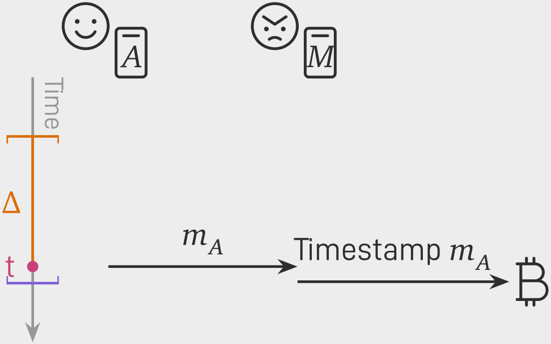
$(m_A, \boxed{A}, \boxed{M})$

1. Would receiving m_A at time t lead to contact with $\boxed{A}$?

2. $m_A \in$ ₿ at time t?

Proof

Want to show: Δ-replay secure ⇒ **not** Δ-contact-time deniable



$(m_A, \boxed{A}, \boxed{M})$

1. Would receiving m_A at time t lead to contact with $\boxed{A}$?

2. $m_A \in$ ₿ at time t?

3. Δ-replay attack not possible!

Various combinations exist

Protocol	Unidirectional	Replay-secure	Deniable
DP3T	✓	∼	∼
Challenge-Resp.	×	✓	✓
Delayed Auth.	✓	✓	×
CleverParrot	✓	✓	×
NTK	✓	∼	∼
DH-based	×	✓	✓

Table: Properties of existing decentralized protocols (cf. paper for details).

Conclusion

- Deniability not achievable for large part of the design space
- Extends to all decentralized ACT assuming stronger judge (cf. paper)
- How does this help in practice? (cf. paper)
  - Identify interesting points in the design space
  - Find creative ways to break out the theoretical model

Deniability in Automated Contact Tracing

C. U. Günther and K. Pietrzak

https://doi.org/10.56553/popets-2024-0134