Twice the Fun: Adapting Unicast Privacy Notions for Group Communication

Christoph Coijanovic [1] Christiane Kuhn [1] Thorsten Strufe [1]

[1]Karlsruhe Institute of Technology
firstname.lastname@kit.edu

Motivation

Picture credit: The New York Times

Political activists (e.g., in Myanmar) require private and secure means of communication.

Activist receiving critical messages faces persecution
Groups with critical messages are blocked by the regime
Popularity of group leaks strength of activists

Dissent [1]
Talek [2]
Blinder [3]
Riposte [4]

Metadata — protected by → ACNs

target

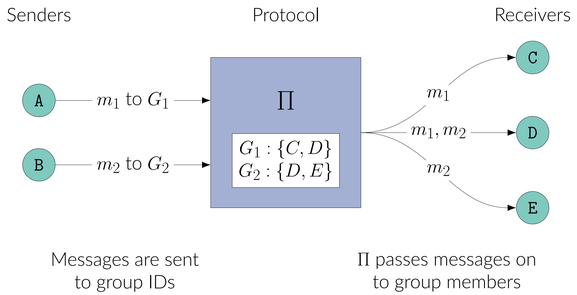
Privacy Goals – formalized by ► Privacy *Notions*

Often informal
Specific to one protocol

Enable rigorous *worst-case* analysis
Hierarchical structure enables comparison

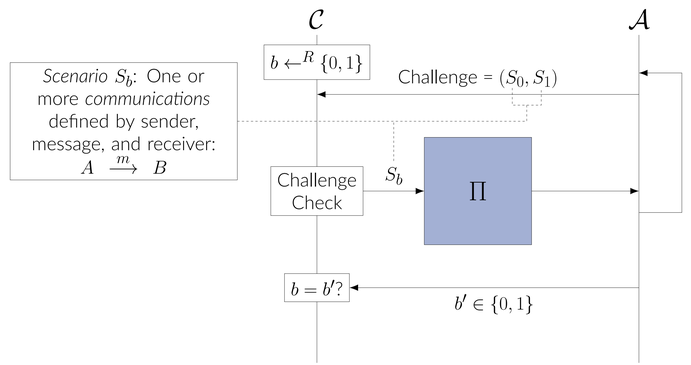
Challenge: Existing formalization approaches do not cover group setting!

Setting

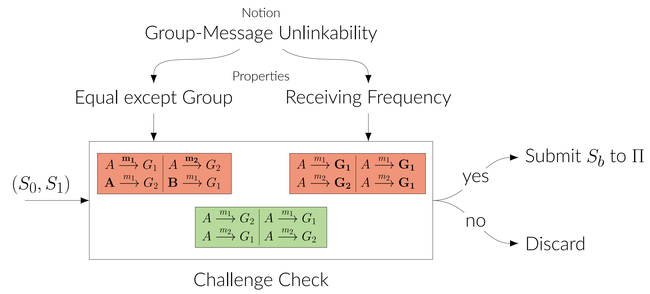


How to Formalize Privacy Goals?

Kuhn et al. [5]: framework of formal privacy notions through indistinguishability games (IND-CPA-like):



- Concrete Privacy notions are defined by *properties*
  - Specify which information may be disclosed
  - Disclosable information has to be identical in both scenarios



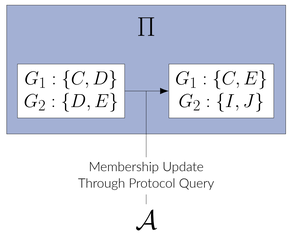
Changes for Group Communication

Communication Format

$A \xrightarrow{m} G$

Receiver ⇒ Group ID

Membership Management

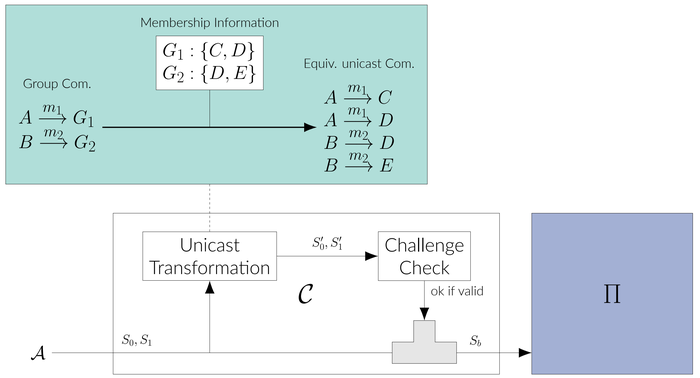


New Notions

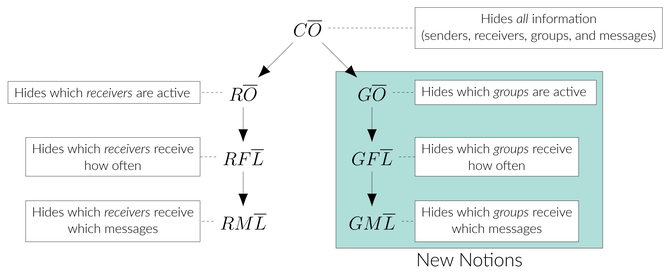
- To cover link between groups and messages
- See hierarchy on the left

Unicast Transformation

- Notions with individual receiver-related properties (e.g., "Which client receives how often?") cannot be checked directly from submitted communications.
- Instead: Challenge check based on *unicast transformation*



Partial Hierarchy



Future Work

- Further privacy notions (e.g., *membership*-related)
- Protocol analysis

Acknowledgments & References

This work was supported by funding of the Helmholtz Association (HGF) through the Competence Center for Applied Security Technology (KASTEL).

[1] D. Wolinsky *et al.*, "Dissent in numbers: Making strong anonymity scale," in *USENIX OSDI*, 2012.

[2] R. Cheng *et al.*, "Talek: a private publish-subscribe protocol," tech. rep., Technical Report. University of Washington, 2016.

[3] I. Abraham *et al.*, "Blinder: Mpc based scalable and robust anonymous committed broadcast.," *IACR Cryptol. ePrint Arch.*, 2020.

[4] H. Corrigan-Gibbs *et al.*, "Riposte: An anonymous messaging system handling millions of users," in *IEEE S&P*, 2015.

[5] C. Kuhn *et al.*, "On privacy notions in anonymous communication," *Proceedings on Privacy Enhancing Technologies*, 2019.