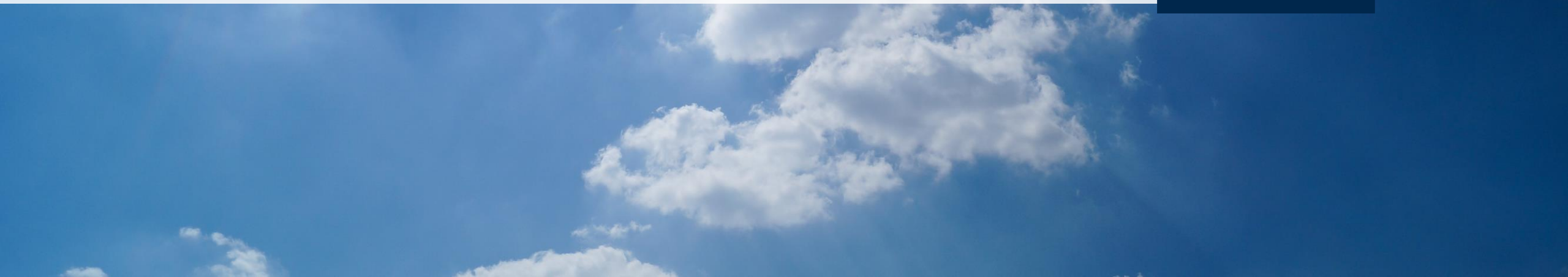
ASMesh: Secure Messaging in Mesh Networks Using Stronger, Anonymous Double Ratchet

ACM CCS 2023

February 23

Real-World Cryptography Group
FAU Erlangen-Nürnberg, Germany

Alexander Bienstock, **Paul Rösler**, Yi Tang



Mesh Messaging

INTERNET NEWS MARCH 15, 2021 / 11:12 PM / UPDATED 2 YEARS AGO

Encrypted messaging app Signal stops working in China

Signal

Help people in Iran reconnect to Signal – a request to our community

Forbes

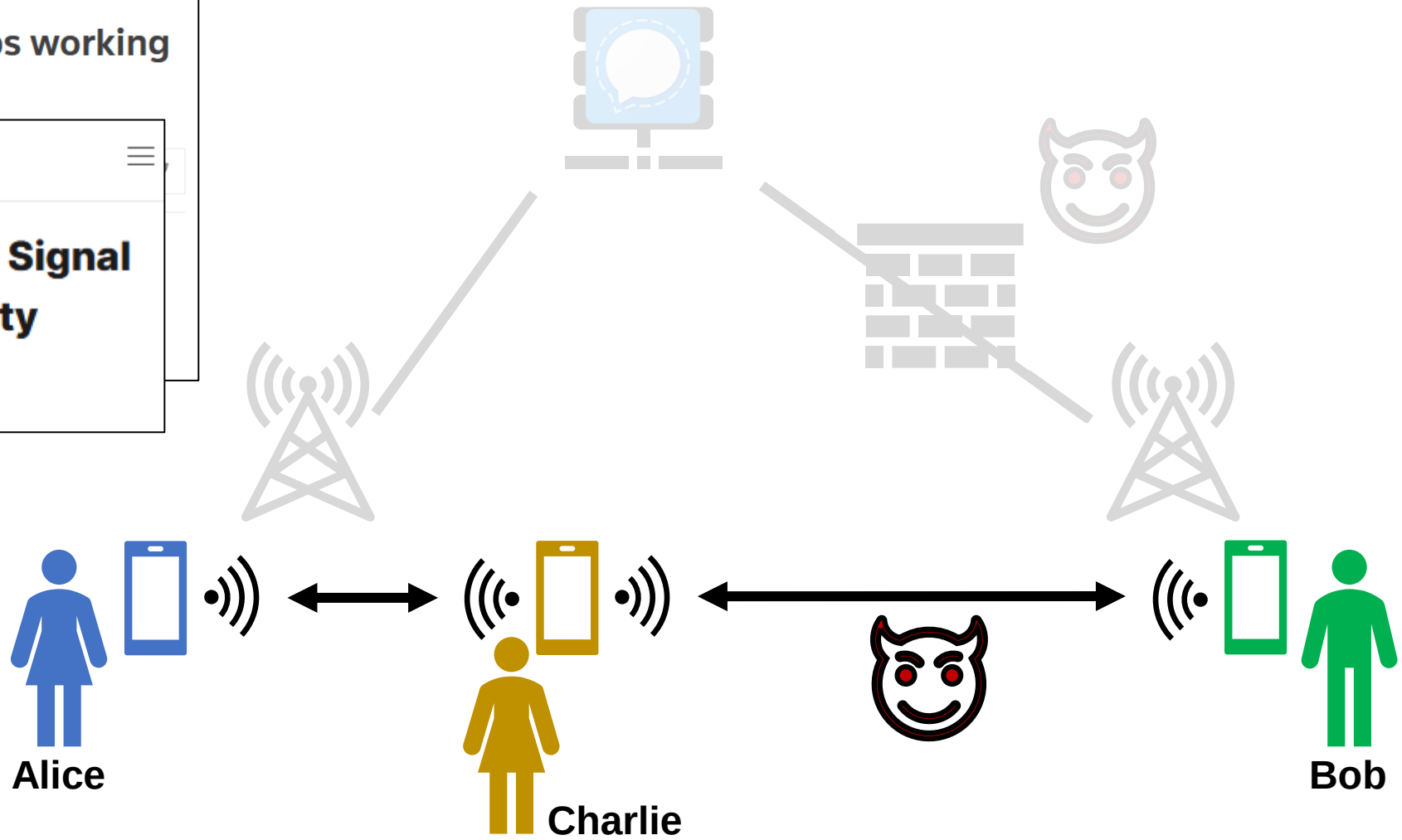
CONSUMER TECH

Hong Kong Protestors Using Mesh Messaging App China Can't Block: Usage Up 3685%

John Koetsier Senior Contributor
John Koetsier is a journalist, analyst, author, and speaker.

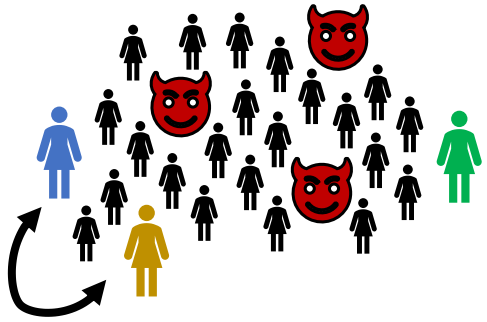
Follow

Sep 2, 2019, 01:23pm EDT



Mesh Messaging

- Vulnerable victims
- Strong adversaries
  But: Not ubiquitous
- Low bandwidth
- High latency
- Low memory

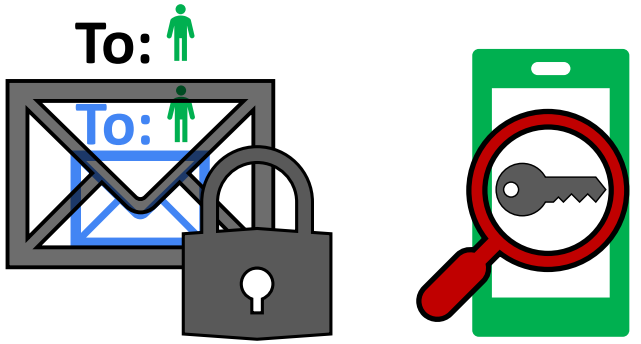


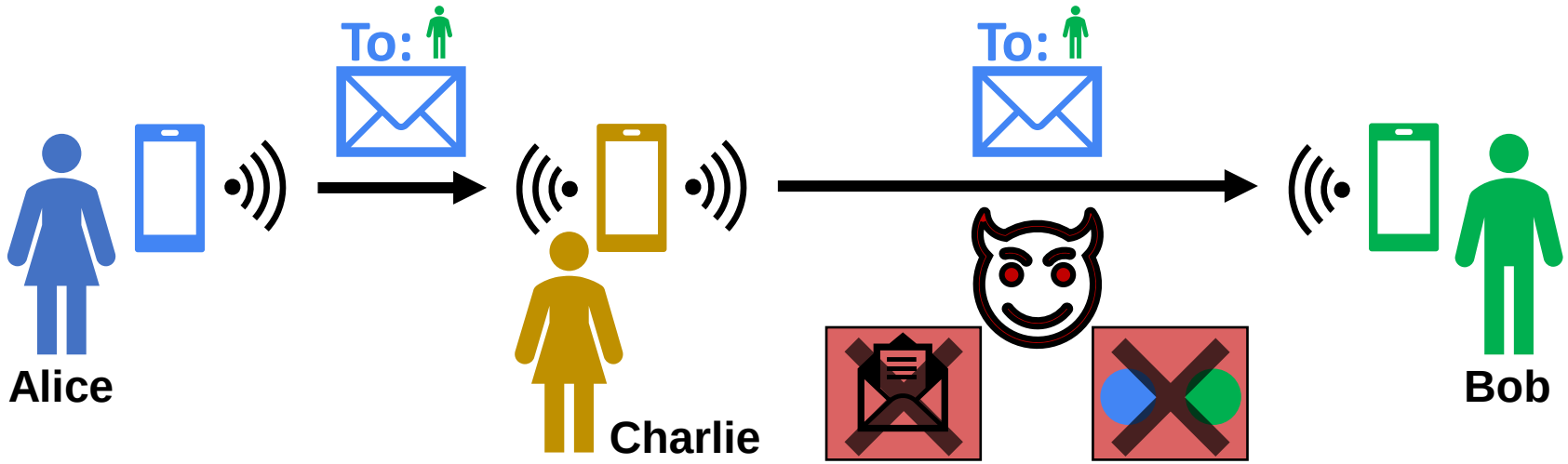
- **No Definitions**
- **No Provably Secure Constructions**

Confidentiality & Anonymity

- Sender Anonymity
- Receiver Anonymity

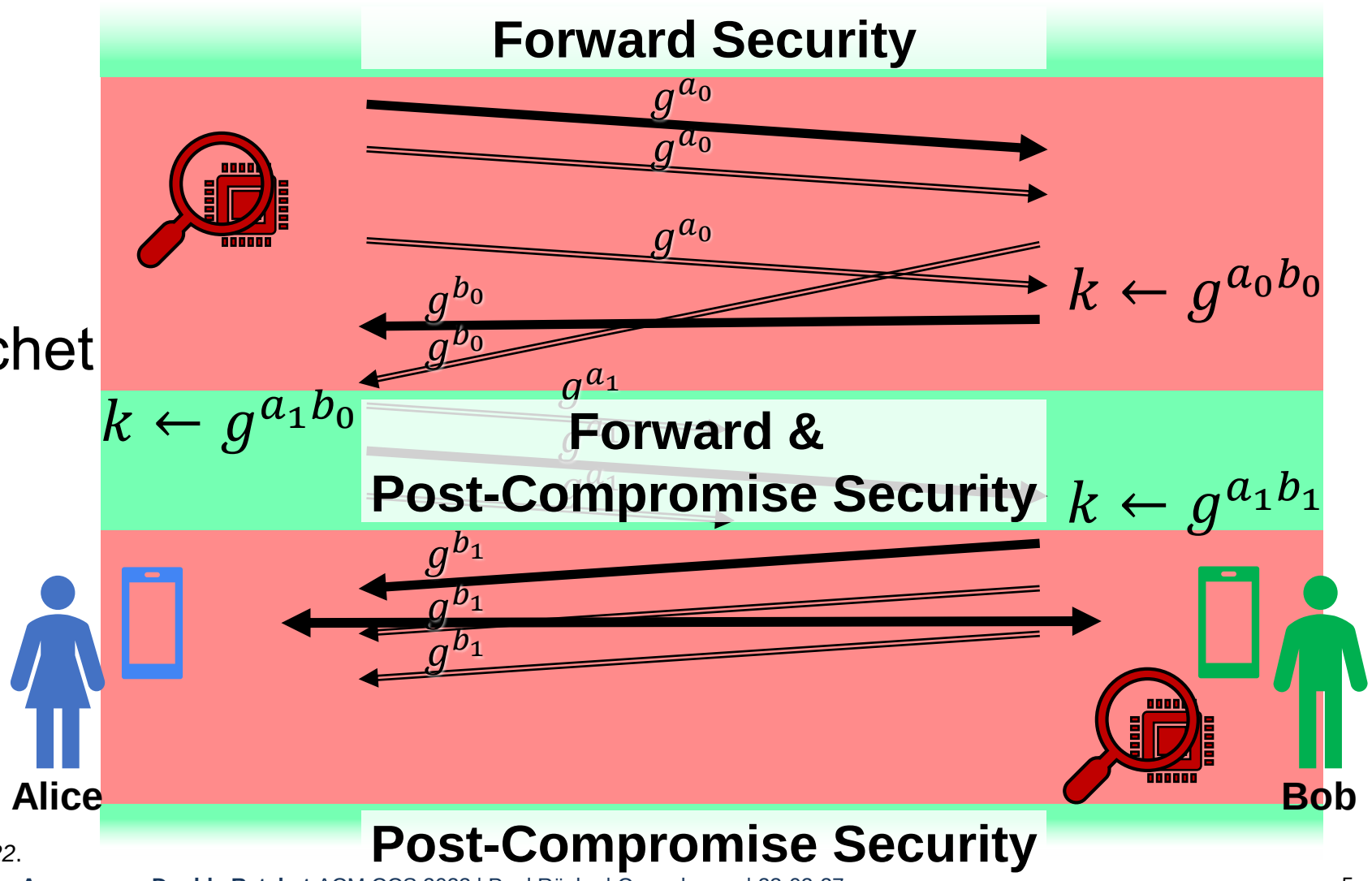
- Available option:
  Signal's Sealed *Sender*
- Receiver corruption
  ⇒ Anonymity lost





Corruption: Forward & Post-Compromise Security

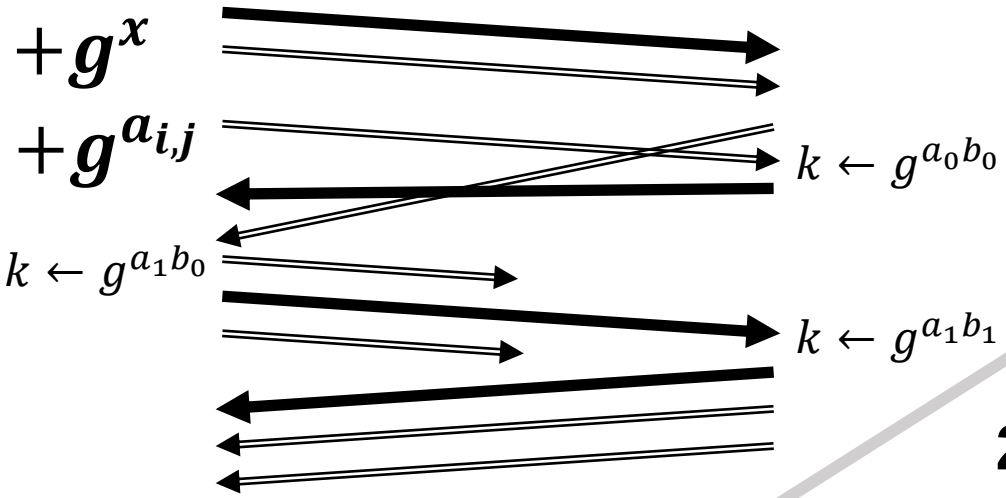
- Continuously refresh local secrets
- Available options:
  - Signal's Double Ratchet
  - MLS Standard
    - → Preliminary wrapper [HKP'22]
- Both non-anonymous



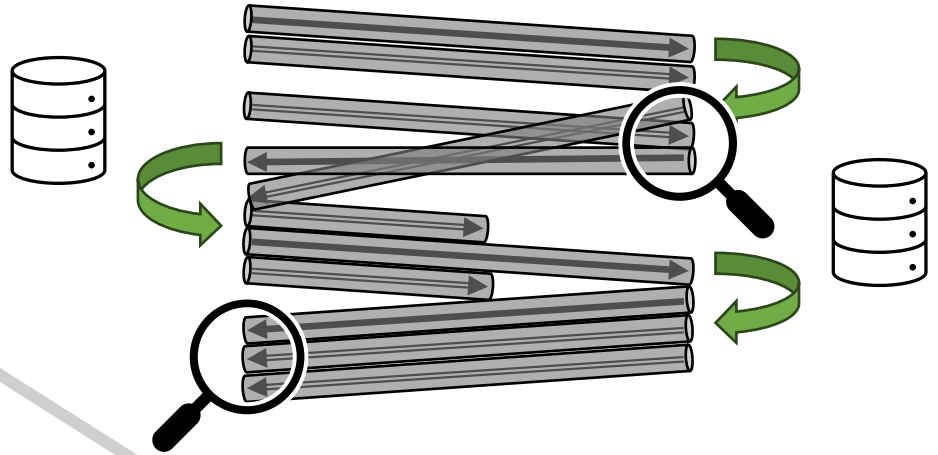
[HKP'22]: Hashimoto, Katsumata, and Prest. *ACM CCS 2022*.

Contributions

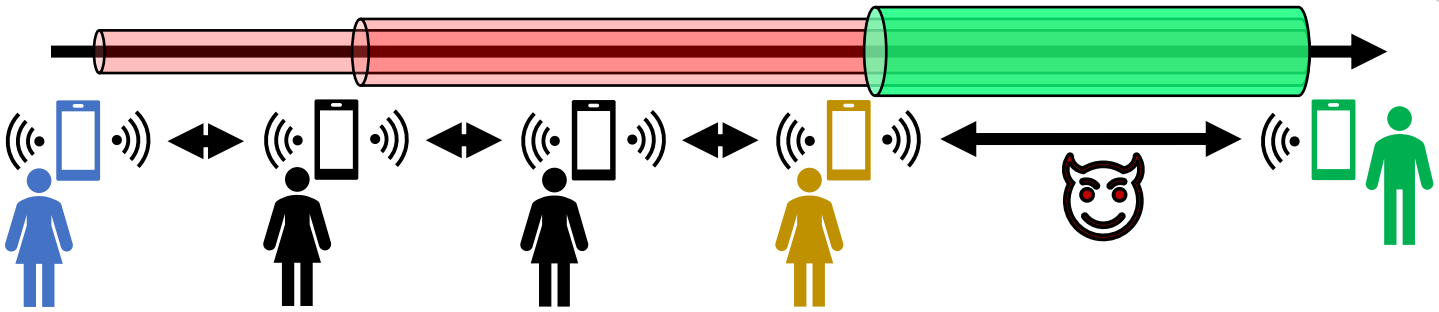
1. Stronger Double Ratchet



3. Message Anonymizer

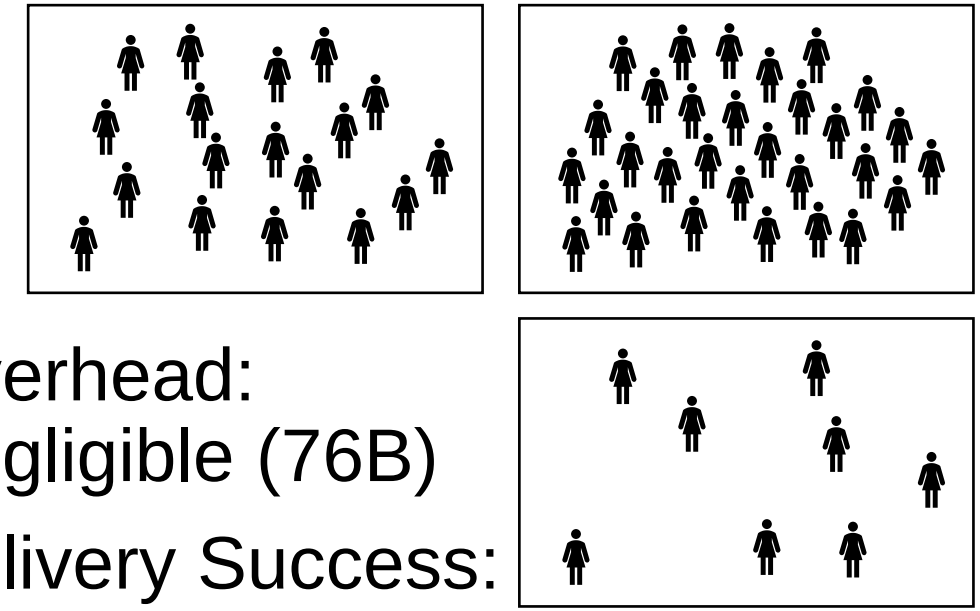


2. In-Flight PCS via Contact Cooperation

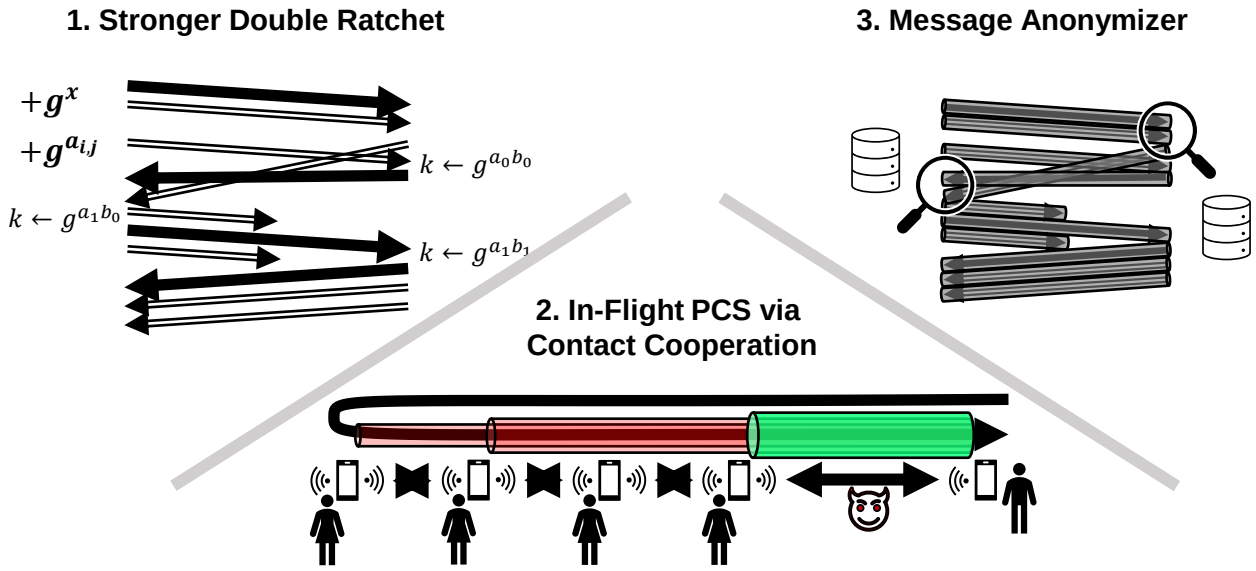


Performance & Overview

- Code and 3 Simulated Networks



- Overhead: Negligible (76B)
- Delivery Success: > 90%
- Strong Generic Anonymity
- Stronger FS & PCS



Paper: ia.cr/2023/1053
Code: github.com/meshmessaging/ASMesh