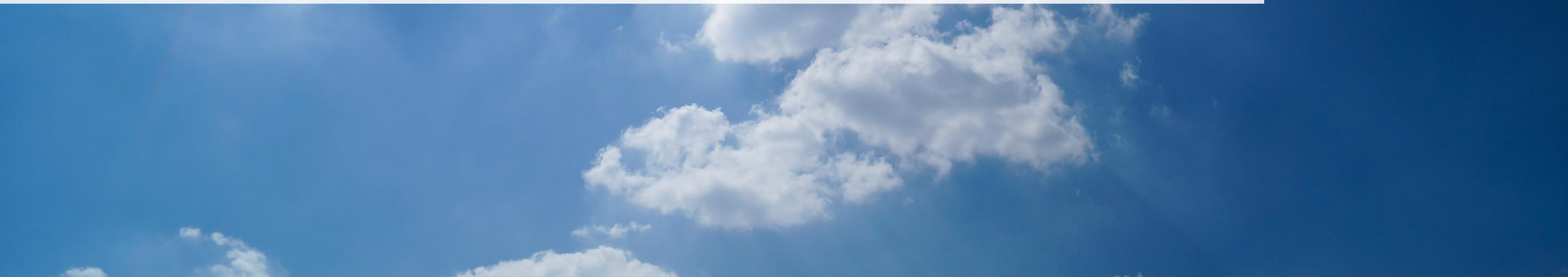
Security of Modern Messengers

Inaugural Lecture

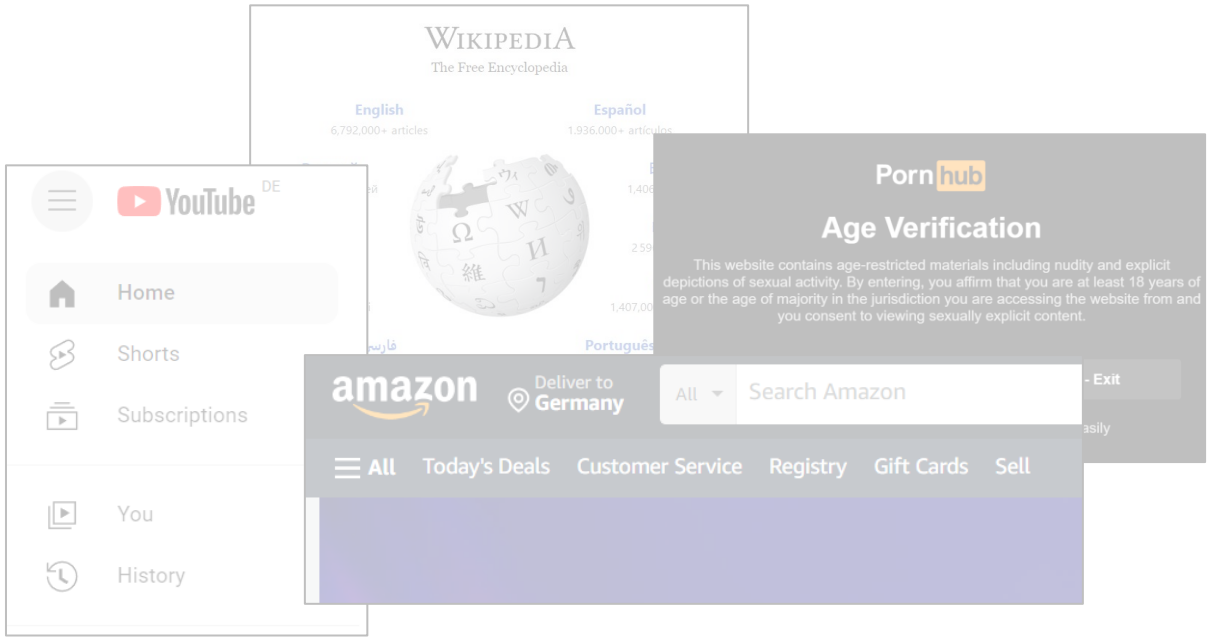
May 24

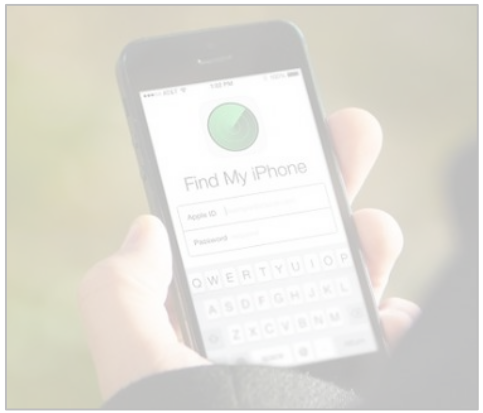
Real-World Cryptography Group
FAU Erlangen-Nürnberg, Germany

Paul Rösler

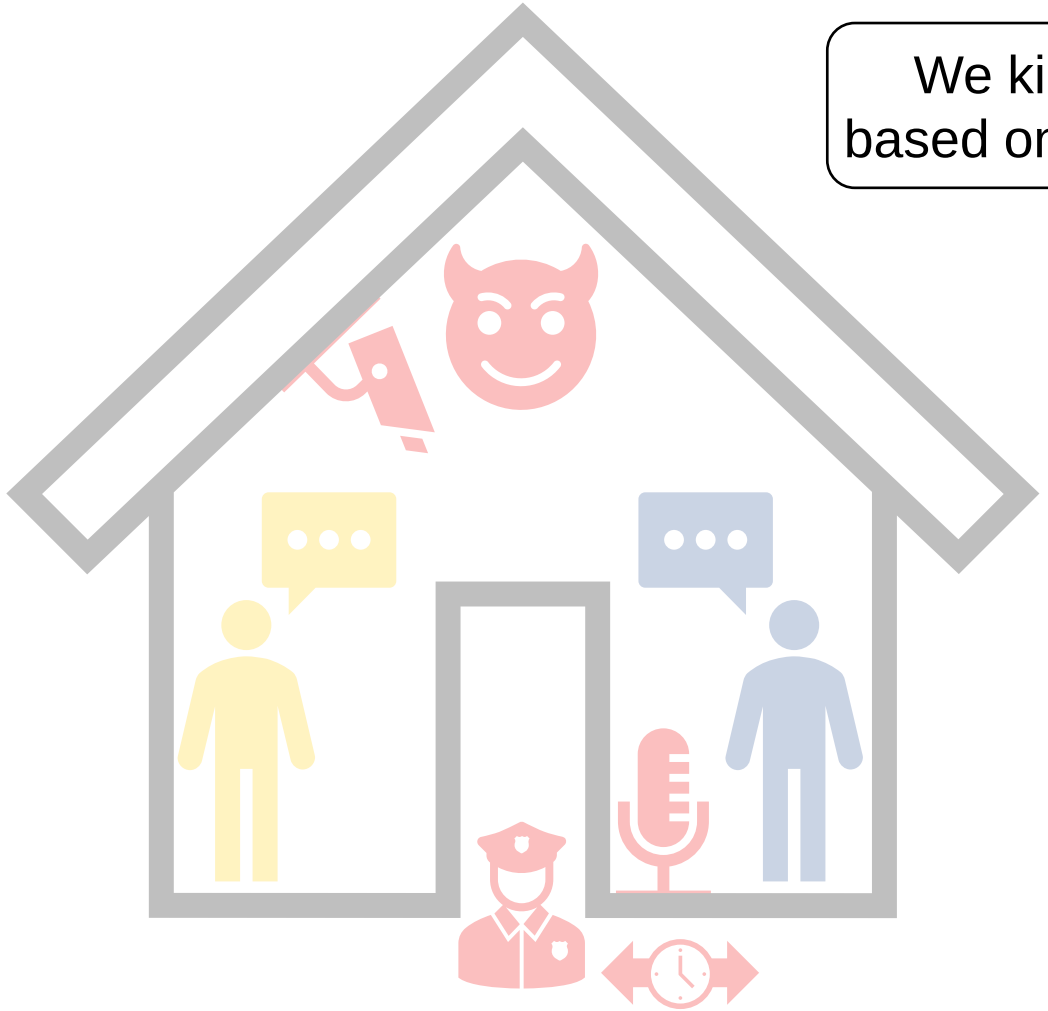


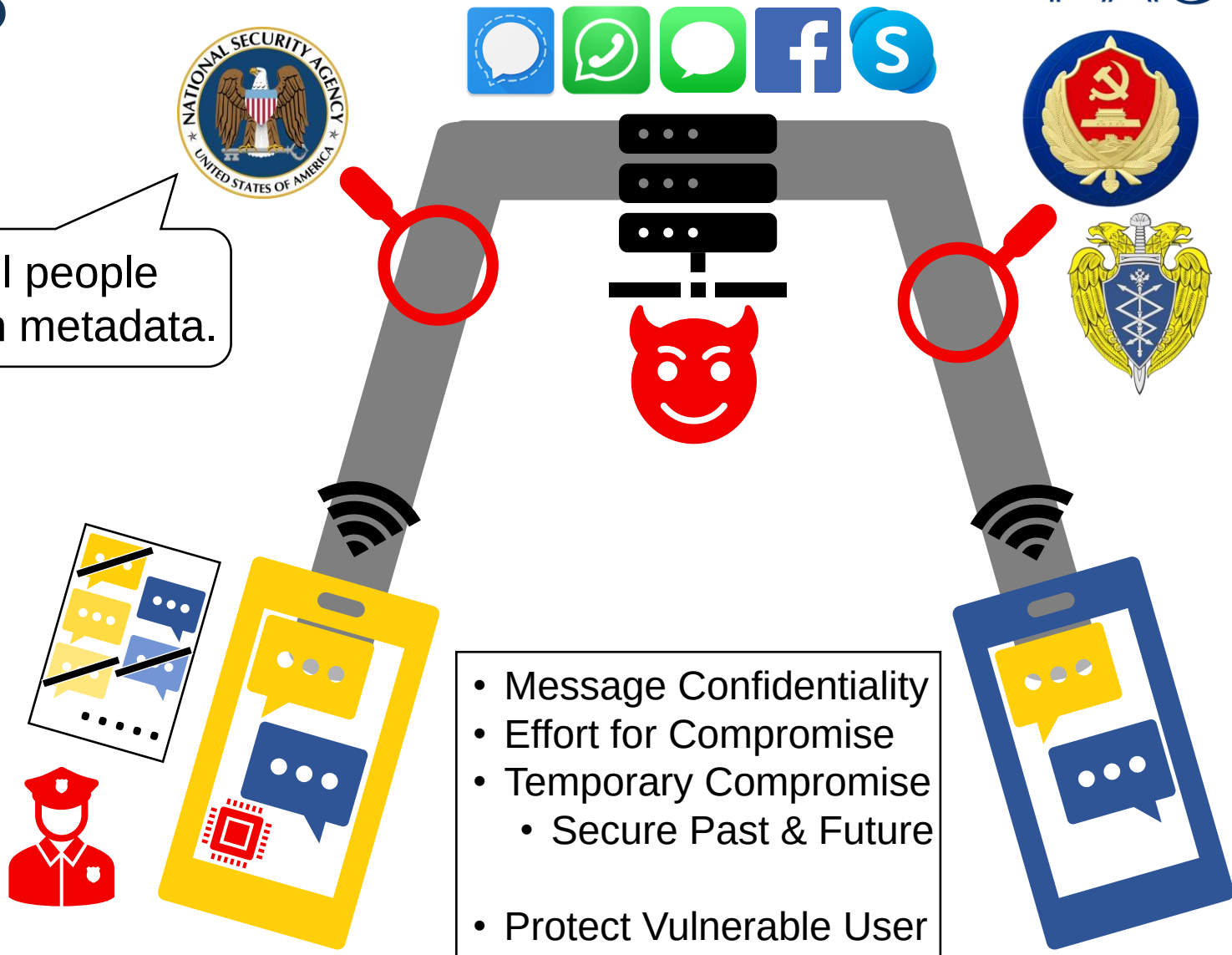
Where is Cryptography?





Why Cryptography?





- Message Confidentiality
- Effort for Compromise
- Temporary Compromise
  - Secure Past & Future
- Protect Vulnerable User
  → Protect all Users
- Privacy

Messaging: Environment

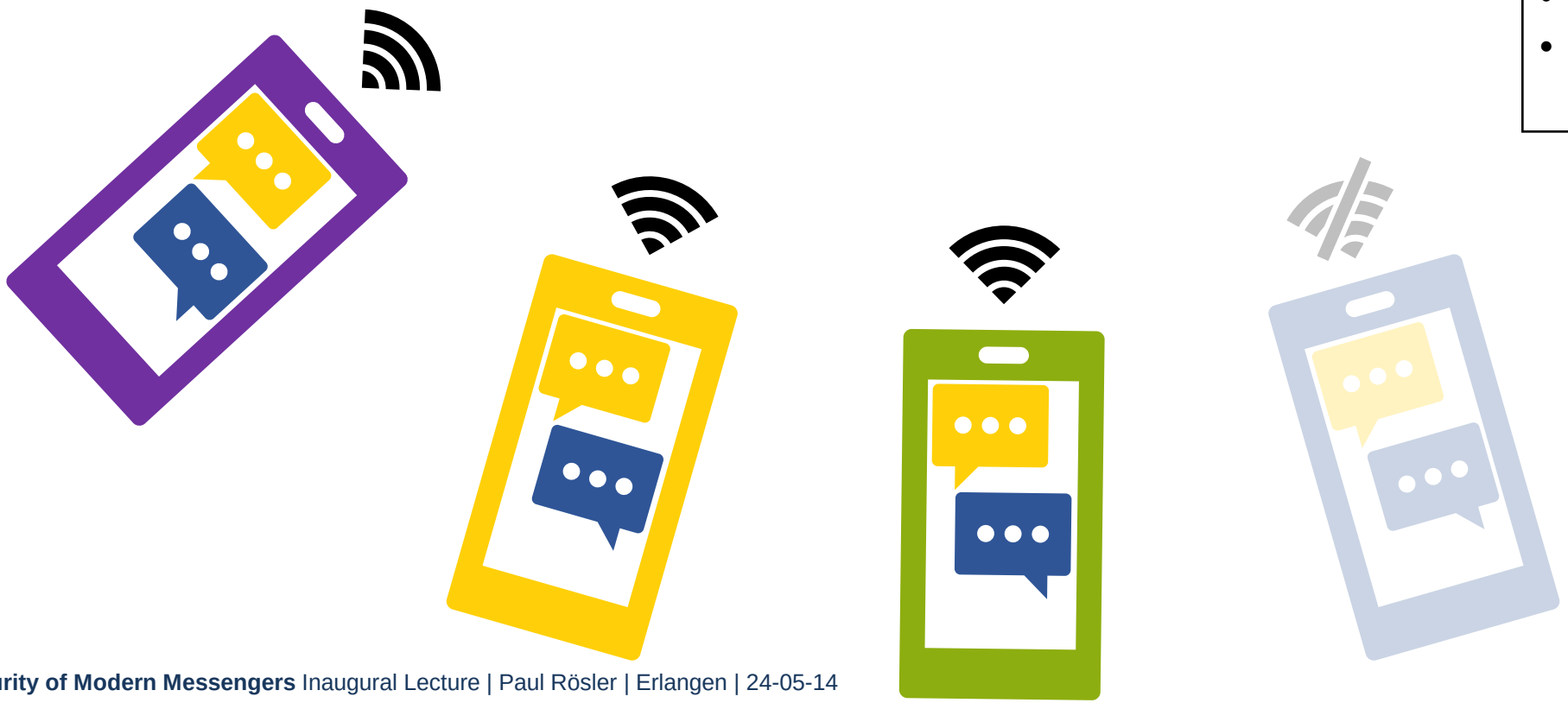
Centralized
- Contact Discovery
- Feature (R-)Evolution
- Security Updates
- Cost Reduction

- Network Effect: Lock-In
- Monoculture
- Monopoly

Messaging: Environment

Asynchronous
- Immediate Sending
- Independent Activity
- Instant Delivery

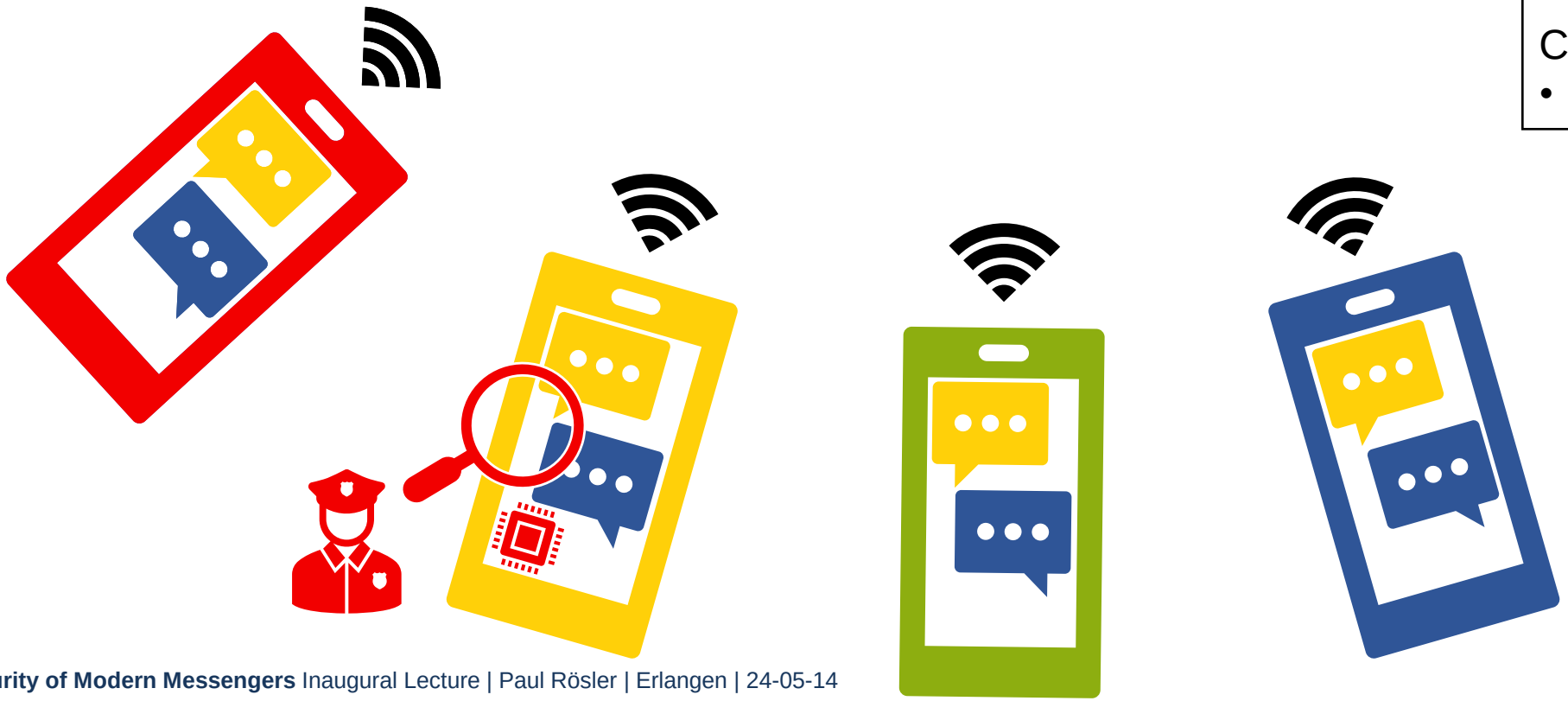
Groups
- Dynamic Membership
- Efficient Communication



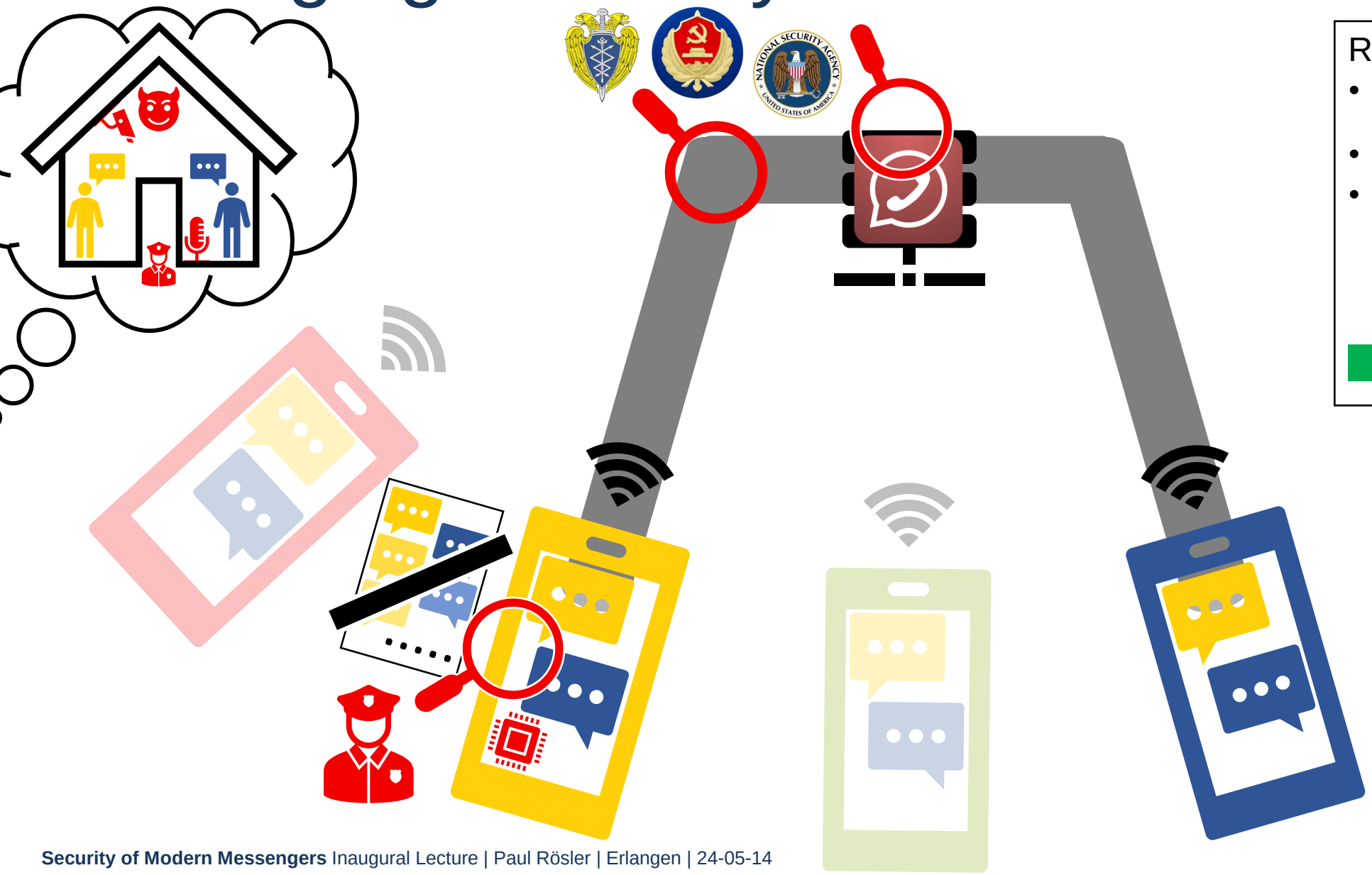
Messaging: Attackers

Attackers
- Internet
- Service Provider
- Intelligence Agencies
- Group Members
- Police

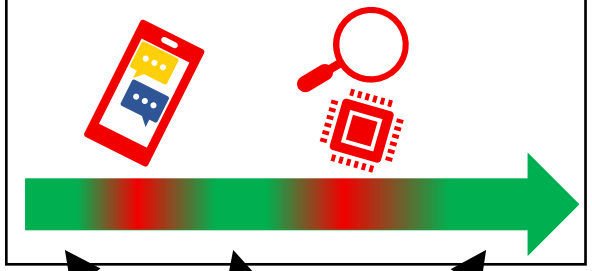
Compromise Secrets
- Virus, Bug, Seizure, …



Messaging: Security

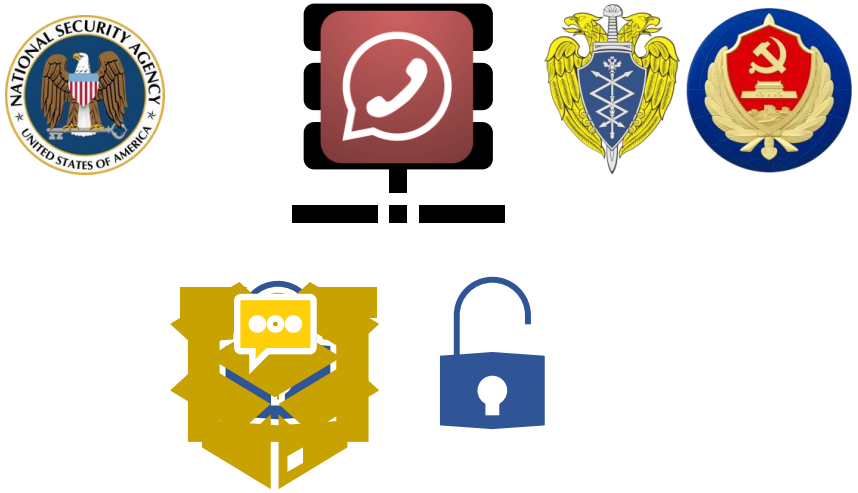


Requirements
- Confidential
- For Honest Members
- With Fresh Secrets



Secure

Secure Messaging: Intuition



Confidential ✓

Secure Messaging: Intuition

Confidential ✓

Problem: Compromise leaks all messages

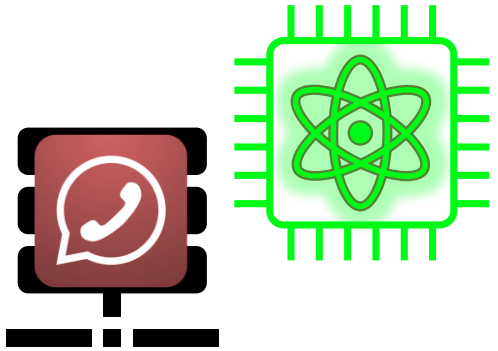
Secure Messaging: Intuition

Secure Messaging: Intuition

Confidential ✓

Secure Past & Future ✓

Secure Messaging: Cryptography



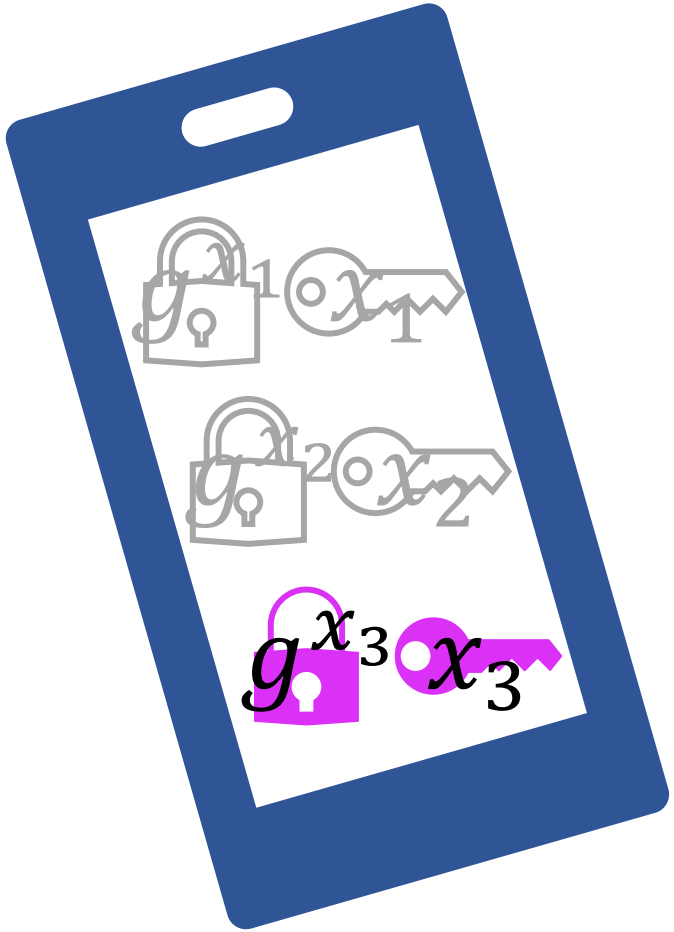
$g^{y_1}, g^{x_1 y_1} + m_1$ g^{x_1}

$g^{y_2}, g^{x_2 y_2} + m_2$ g^{x_2} x_2

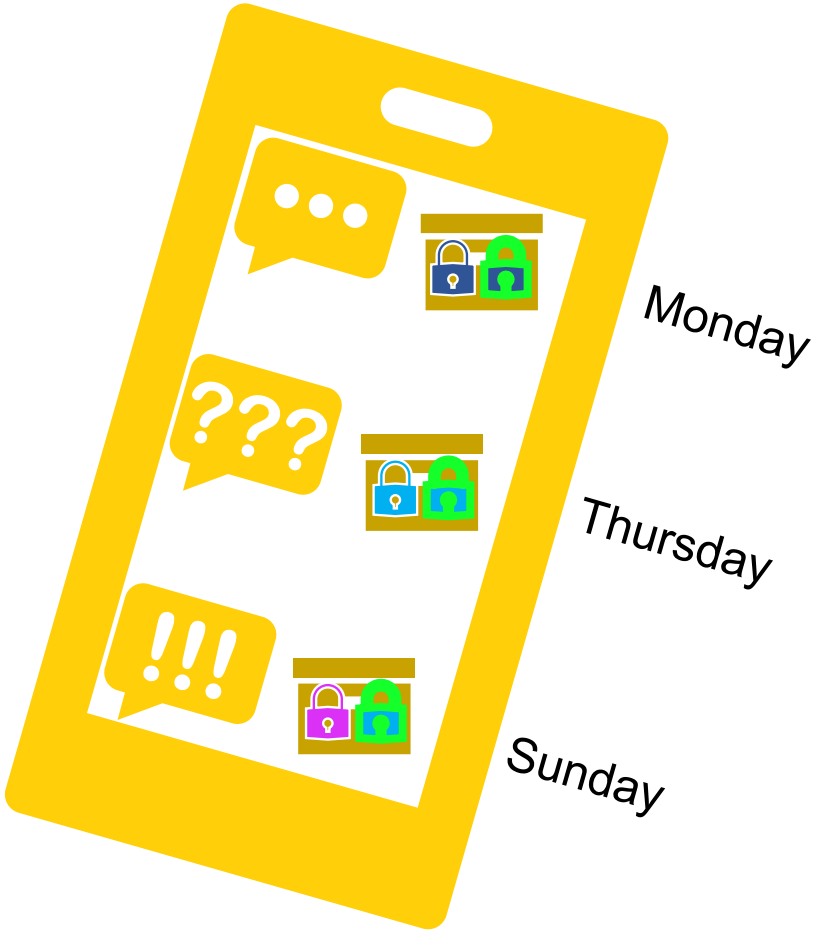
$g^{y_3}, g^{x_3 y_3} + m_3$ g^{x_3}

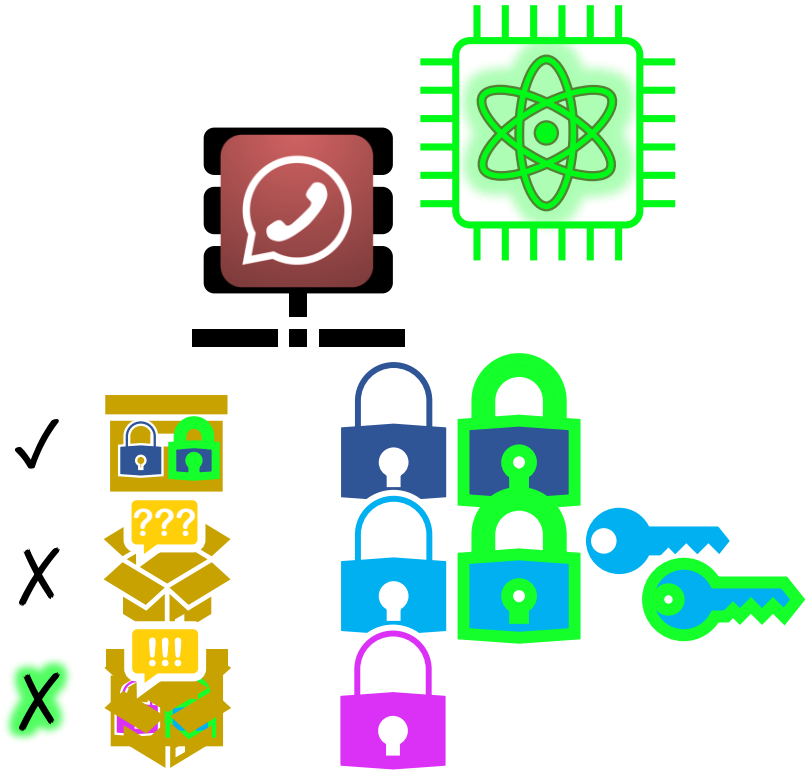
$g^x \rightarrow x$ ~~hard~~

$g^x = \underbrace{938..527}_{40 \text{ digits}}$



Secure Messaging: Post-Quantum



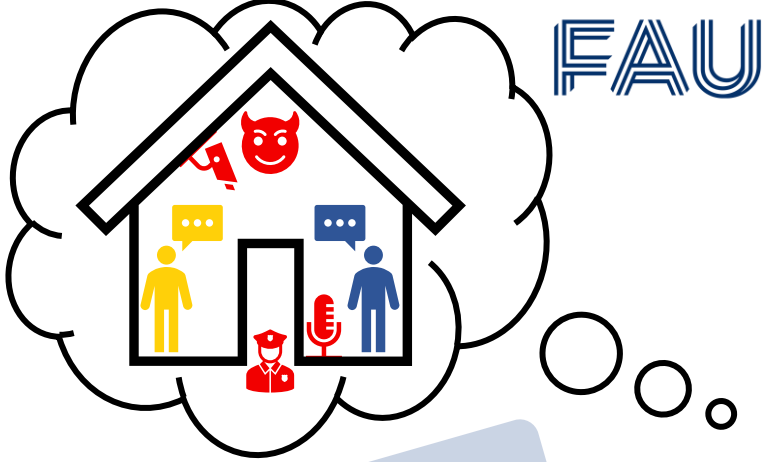


Confidential ✓

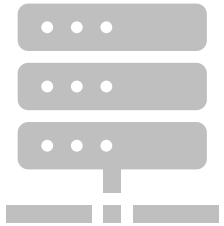
Secure Past & Future ✓

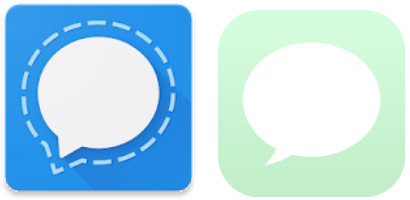
Delayed Post-Quantum Secure ✓

Secure Messaging: Deployment

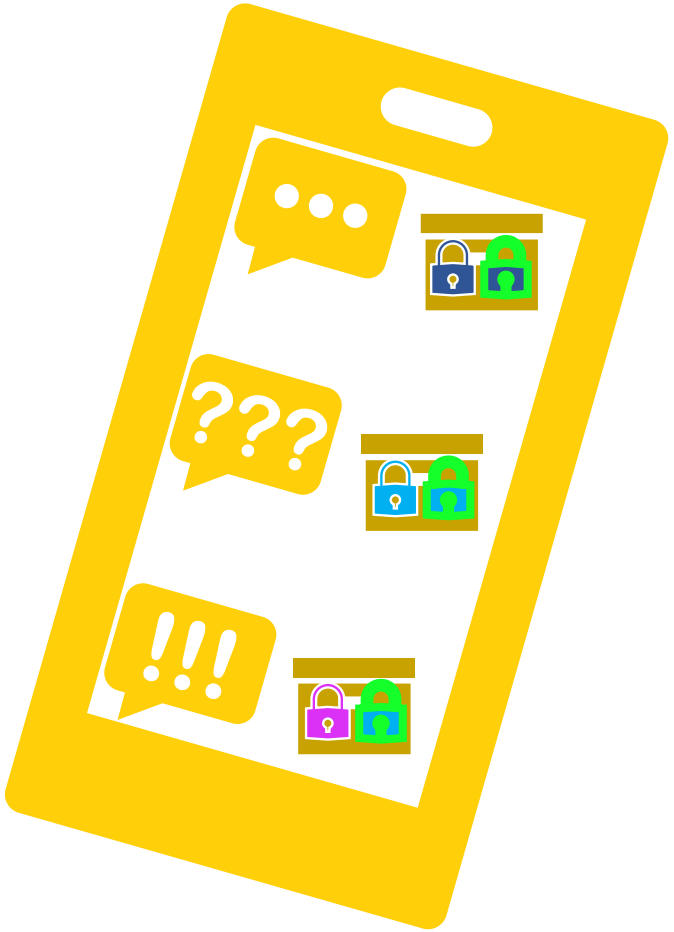


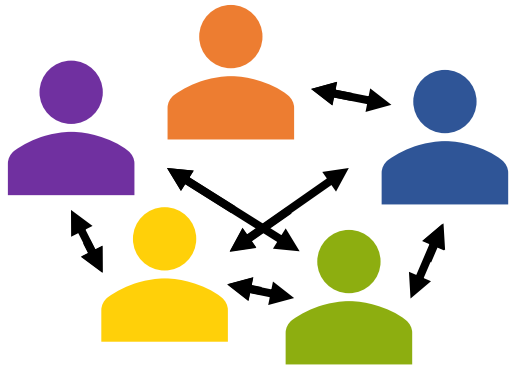
We kill people based on metadata.



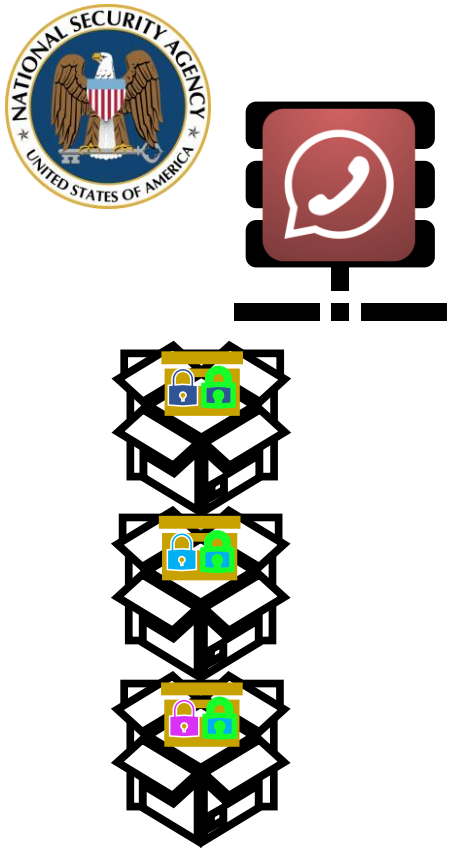


Secure Messaging: Privacy

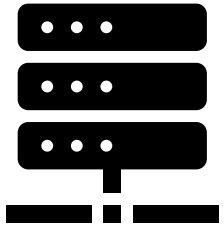




Secure Messaging: Privacy



Secure Messaging: Open Problems

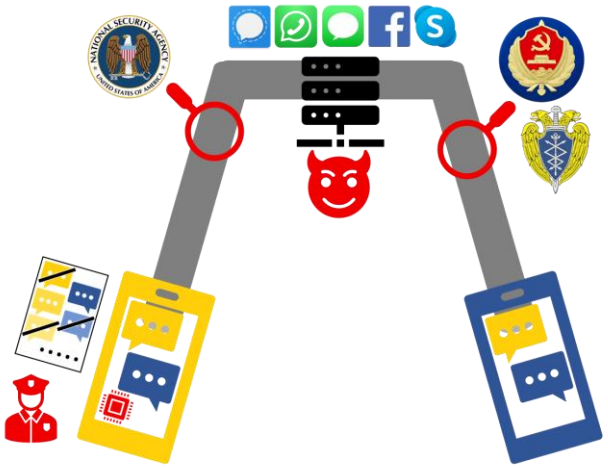


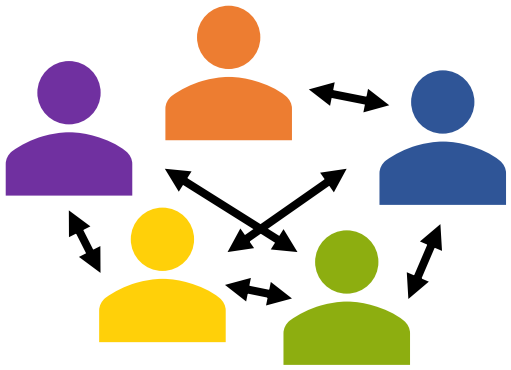
Privacy
- For Past & Future
- Efficient Decryption
- Abuse Prevention
- Spam Detection

Interoperability, …

Cybercrime and Forensic Computing
Research Training Group 2475

Summary





roeslpa.de