

More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema

IEEE EuroS&P 2018

2018-04-26

Horst Görtz Institute for IT Security

Chair for Network and Data Security

Paul Rösler, Christian Mainka, Jörg Schwenk

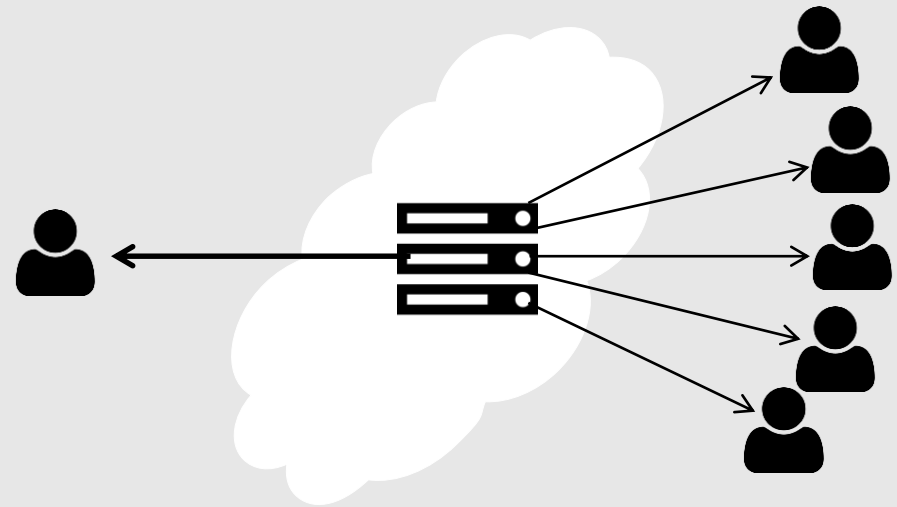
Secure Group Instant Messaging: End-to-End

- Dynamic group of users



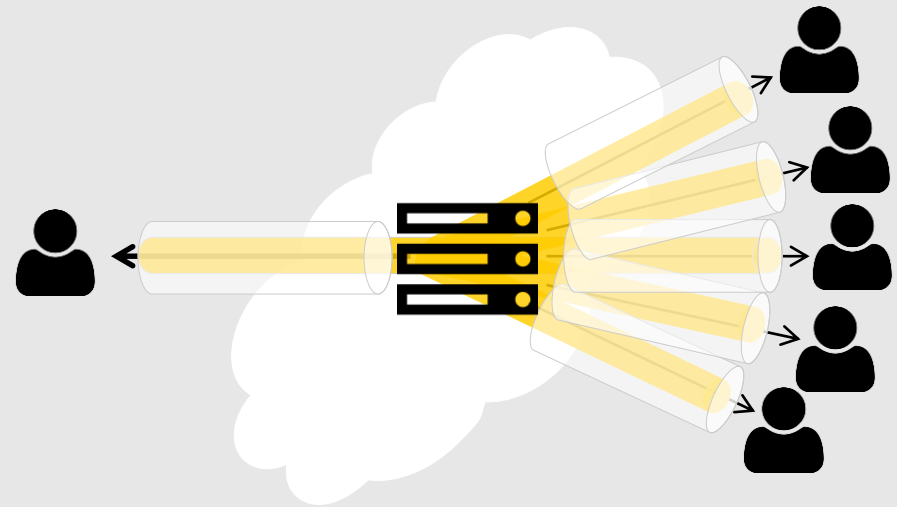
Secure Group Instant Messaging: End-to-End

- Dynamic group of users
- One central server (always online)



Secure Group Instant Messaging: End-to-End

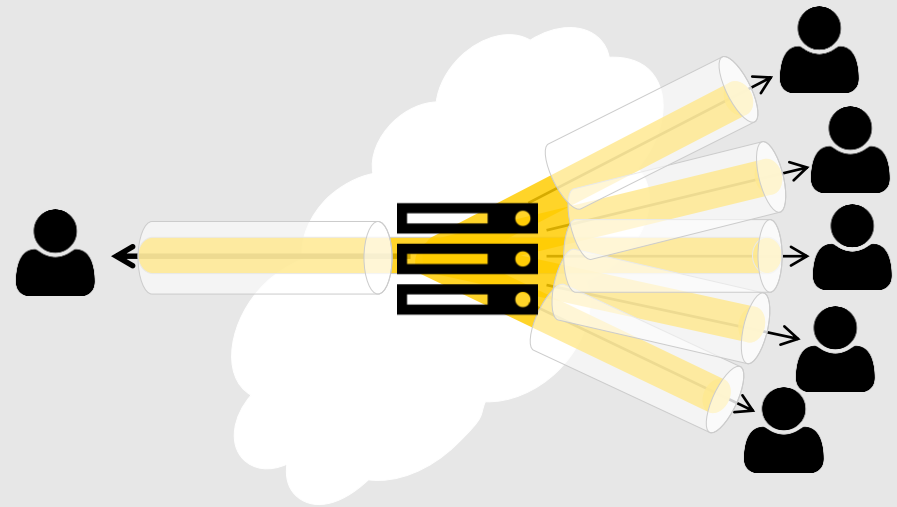
- Dynamic group of users
- One central server (always online)
- End-to-end protection within protected transport layer
- Server potentially malicious



Secure Group Instant Messaging: End-to-End

- Dynamic group of users
- One central server (always online)
- End-to-end protection within protected transport layer
- Server potentially malicious
- Multiple users + leaving/joining + users offline + forward secrecy/PCS

⇒ Security definition...



Secure Group Instant Messaging: End-to-End

- Dynamic group of users
- One central server (always online)
- End-to-end protection within protected transport layer
- Server potentially malicious
- Multiple users + leaving/joining + users offline + forward secrecy/PCS



⇒ Security definition vs. real world protocols

Agenda

- Security Model
- Issues of Modeling and Issues of Real World Protocols
 - Reliability vs. Instant Messaging
 - Post Compromise Security and Ratcheting

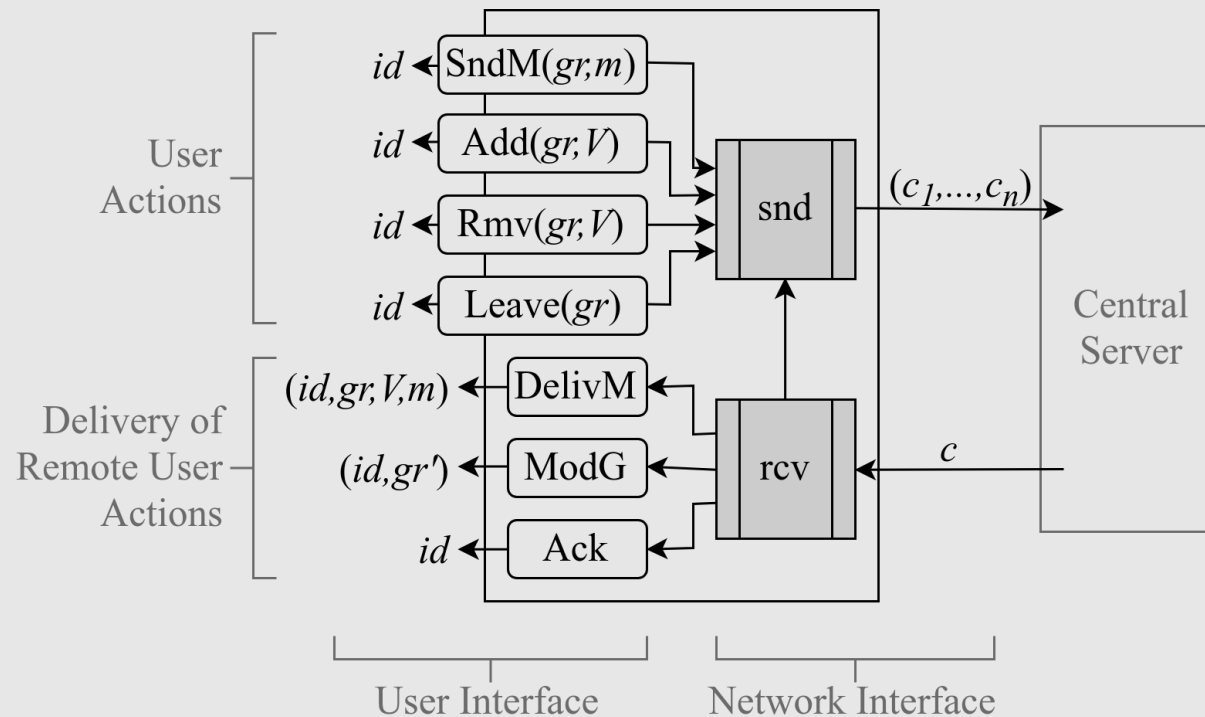
Secure Group Instant Messaging: Groups

Security Model

Reliability vs. Instant Messaging

PCS and Ratcheting

Asynchronous Group IM



Secure Group Instant Messaging: Two Parties

Security Model

Reliability vs. Instant Messaging

PCS and Ratcheting

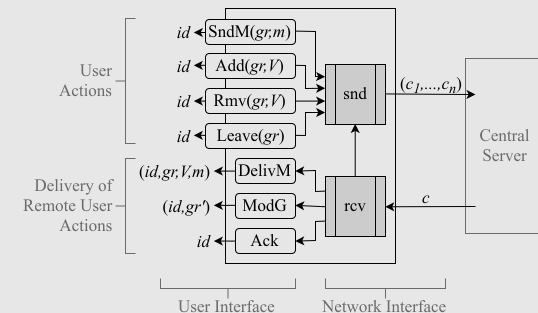
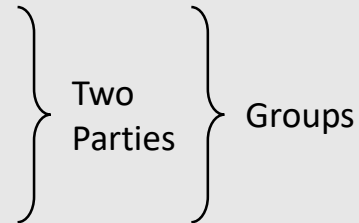
Asynchronous Group IM

Confidentiality

- Message Confidentiality

Integrity

- Message Authentication
- No Duplication



Secure Group Instant Messaging: Two Parties

Security Model

Reliability vs. Instant Messaging

PCS and Ratcheting

Asynchronous Group IM

Confidentiality

- Message Confidentiality

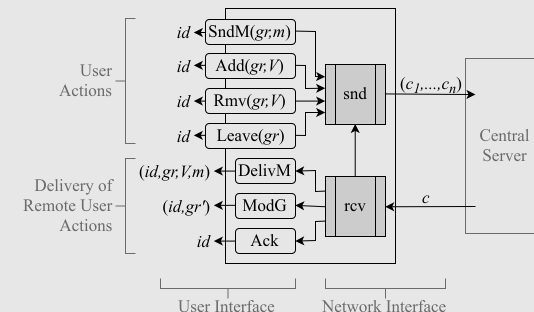
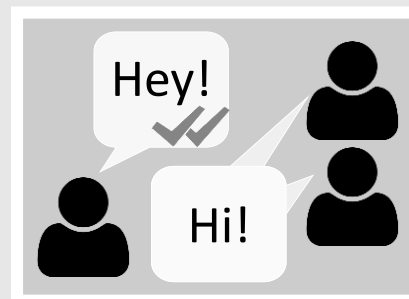
Integrity

- Message Authentication
- No Duplication
- **Traceable Delivery**

Two
Parties

Groups

“Only successful delivery is acknowledged”



Secure Group Instant Messaging: Groups

Security Model

Reliability vs. Instant Messaging

PCS and Ratcheting

Asynchronous Group IM

Confidentiality

- Message Confidentiality
- **Closeness**

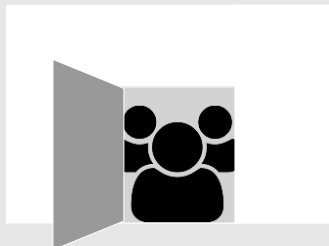
Integrity

- Message Authentication
- No Duplication
- **Traceable Delivery**
- No Creation

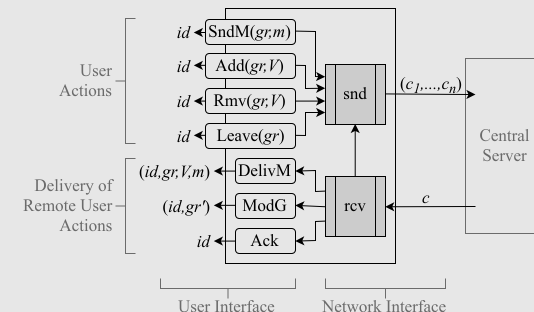
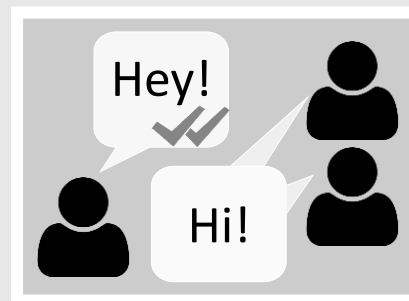
Two Parties

Groups

“Only group (admin) decides on membership”



“Only successful delivery is acknowledged”




Security Model: Malicious Server

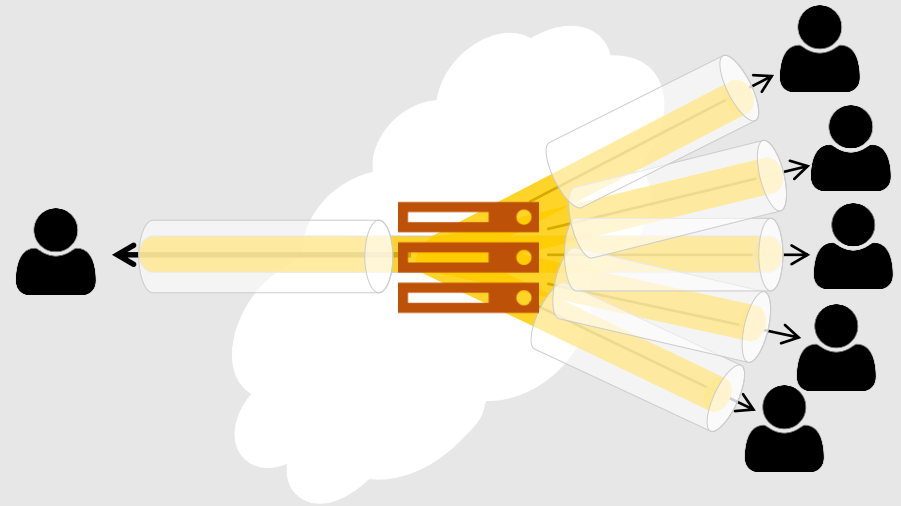
Security Model

Reliability vs. Instant Messaging

PCS and Ratcheting

Asynchronous Group IM

- Malicious Server 
 - Can decrypt transport layer protection
 - E.g. IM provider, TLS certificate forger on network, ...




Security Model: Malicious Server

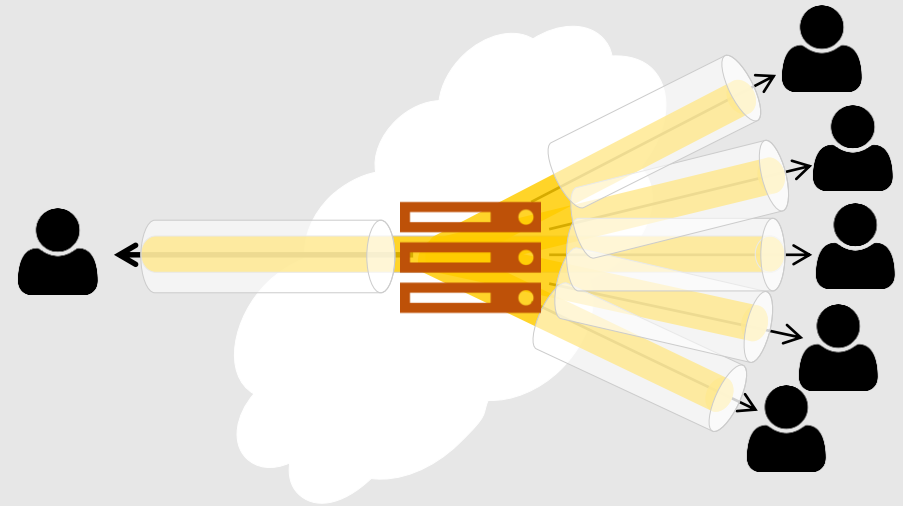
Security Model






Reliability vs. Instant Messaging

PCS and Ratcheting

Asynchronous Group IM

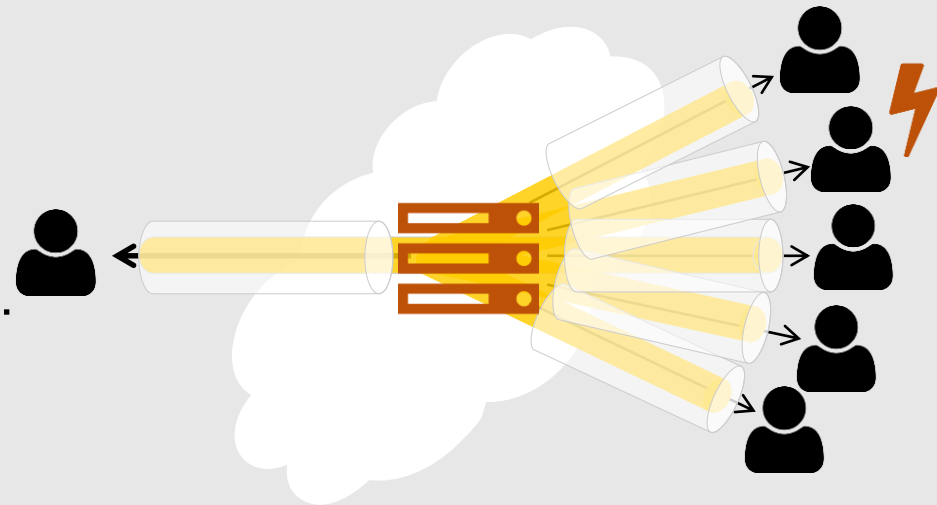
- Malicious Server 
 - Can decrypt transport layer protection
 - E.g. IM provider, TLS certificate forger on network, ...








Attackable by	Traceable Delivery	Closeness
		?
		

Security Model: Compromising Attacker

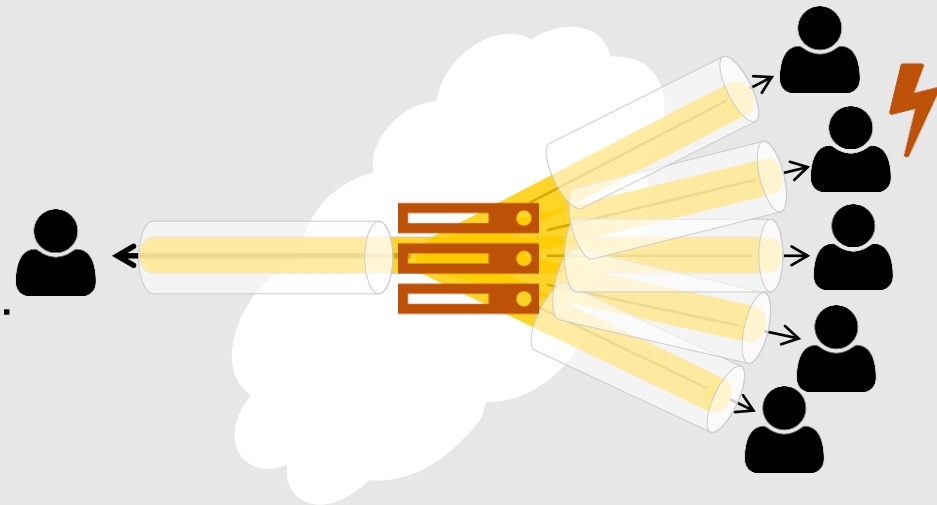
- Compromising Attacker ⚡
 - Access to members' secrets
 - E.g. access to device, cryptanalysis, ...



Attackable by	Traceable Delivery	Closeness
		?
		

Security Model: Compromising Attacker






- Compromising Attacker ⚡
 - Access to members' secrets
 - E.g. access to device, cryptanalysis, ...
- Advanced Goals:
 - Forward Secrecy



Secure → ⚡

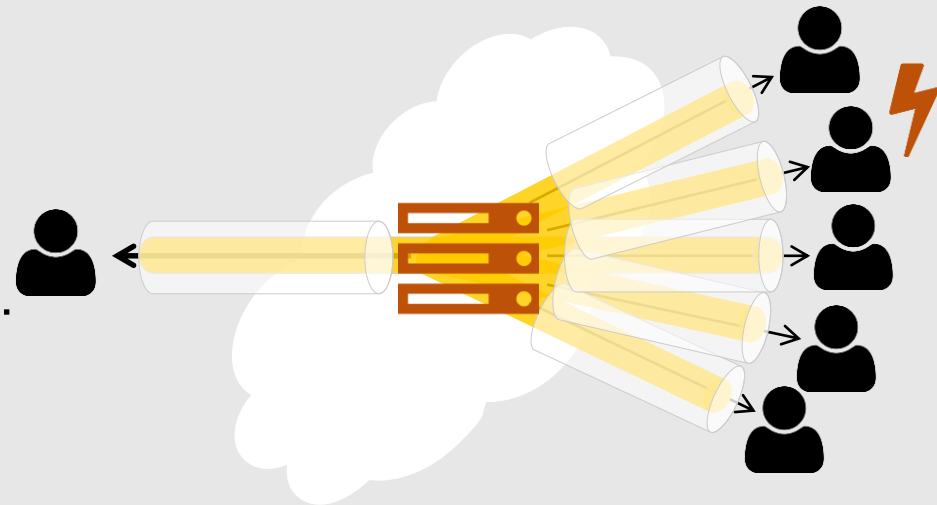
- Post Compromise Security
(aka Future Secrecy aka Backward Secrecy)

⚡ → Secure →

Attackable by	Traceable Delivery	Closeness
		?
		

Security Model: Compromising Attacker






- Compromising Attacker ⚡
 - Access to members' secrets
 - E.g. access to device, cryptanalysis, ...
- Advanced Goals:
 - Forward Secrecy



Secure → ⚡

- Post Compromise Security
(aka Future Secrecy aka Backward Secrecy)

⚡ → Secure →

Attackable by	Traceable Delivery	Closeness
		⚡ (PCS)
		

Security Model

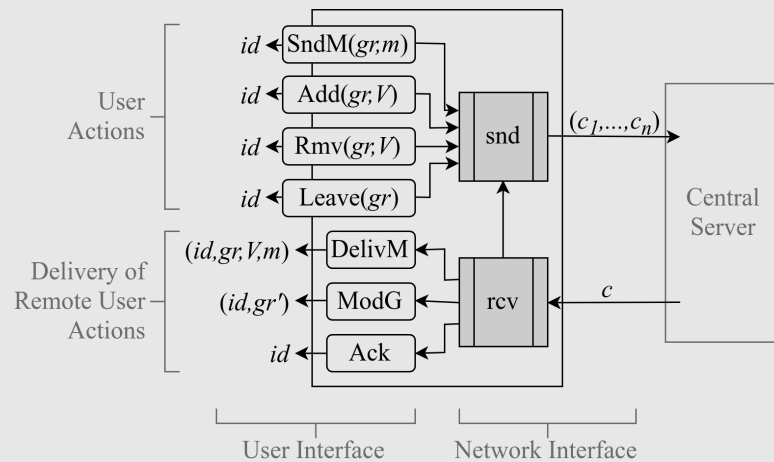
Security Model

Reliability vs. Instant Messaging

PCS and Ratcheting

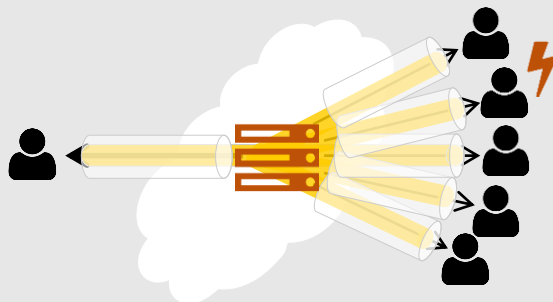
Asynchronous Group IM

Syntax



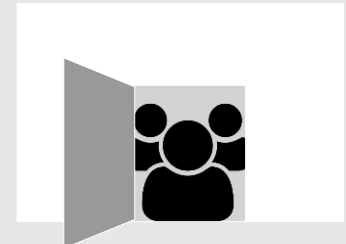
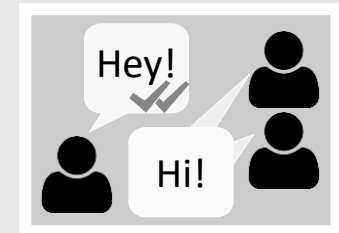
Adversaries

- Malicious Server
- Compromising Attacker



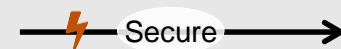
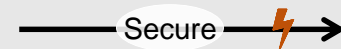
Security & Reliability Goals:

- Message Confidentiality
- Message Authentication
- No Duplication
- Traceable Delivery
- Closeness
- No Creation



Advanced Goals:

- Forward Secrecy
- Post Compromise Security



Security Model

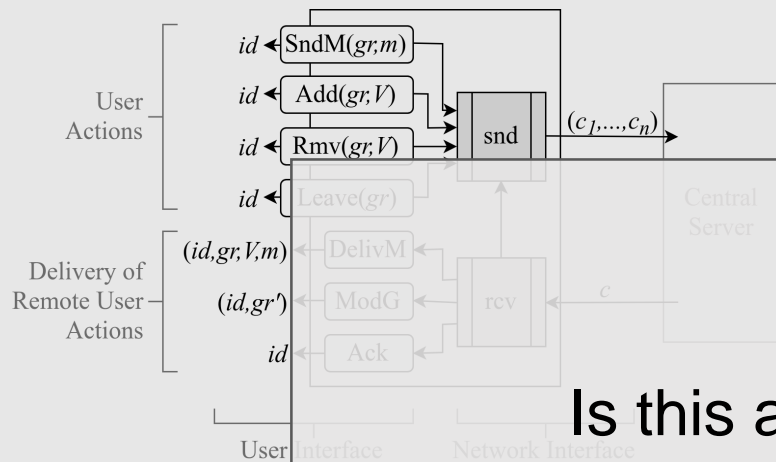
Security Model

Reliability vs. Instant Messaging

PCS and Ratcheting

Asynchronous Group IM

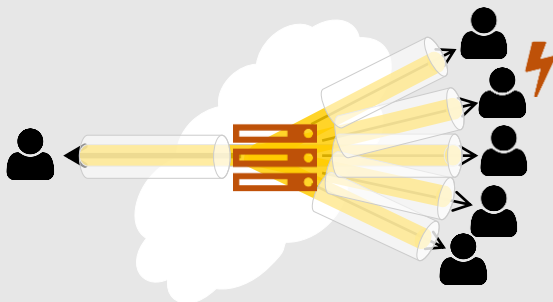
Syntax



Is this a good definition for
secure group instant messaging?

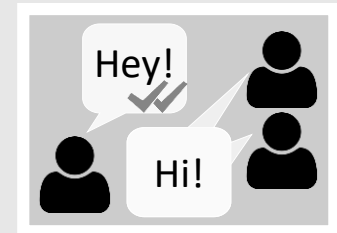
Adversaries

- Malicious Server
- Compromising Attacker

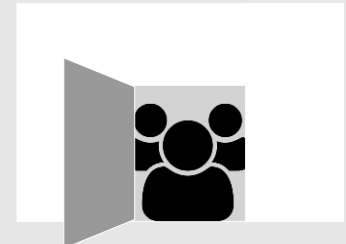


Security & Reliability Goals:

- Message Confidentiality
- Message Authentication

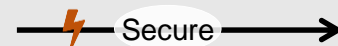
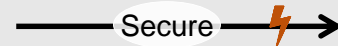


- No Duplication
- Traceable Delivery
- Closeness
- No Creation



Advanced Goals:

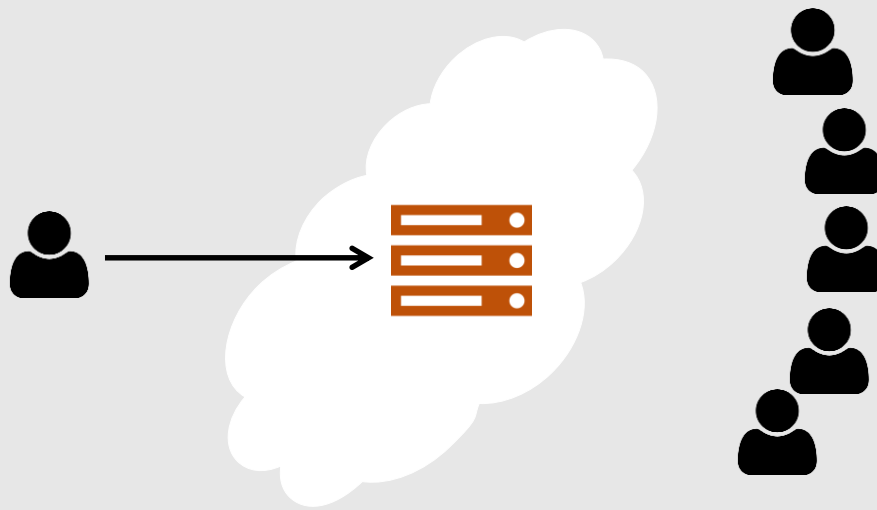
- Forward Secrecy
- Post Compromise Security



Reliability vs. Instant Messaging

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

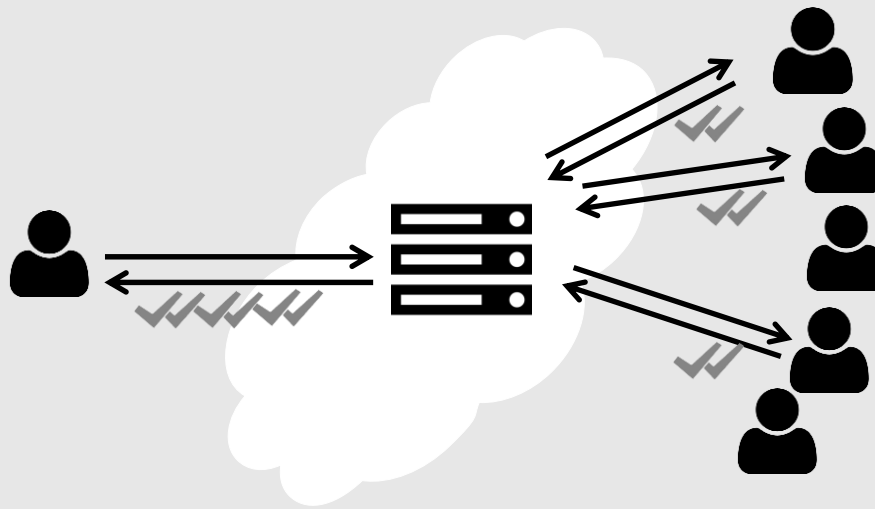
- Reliable delivery in centralized network impossible (Byzantine Agreement)



Reliability vs. Instant Messaging

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

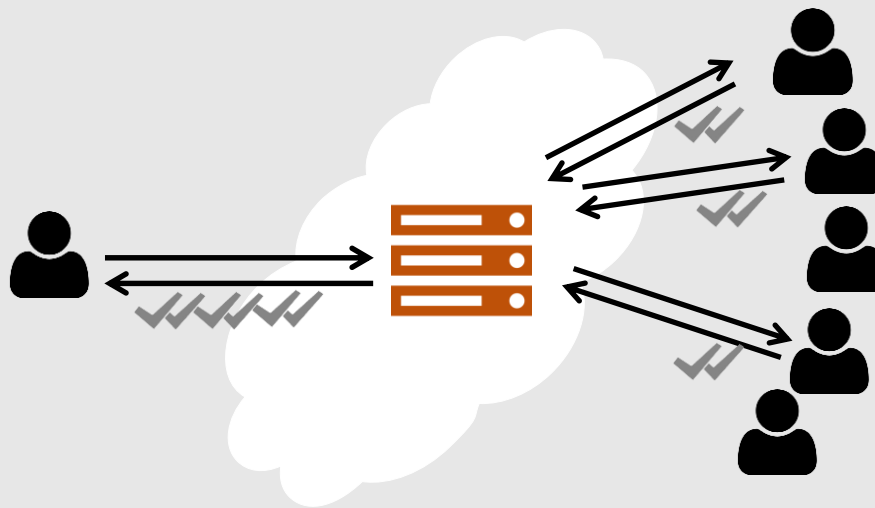
- Reliable delivery in centralized network impossible (Byzantine Agreement)
- Reliability of receipt status partially possible (Traceable Delivery)



Reliability vs. Instant Messaging

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

- Reliable delivery in centralized network impossible (Byzantine Agreement)
- Reliability of receipt status partially possible (Traceable Delivery)



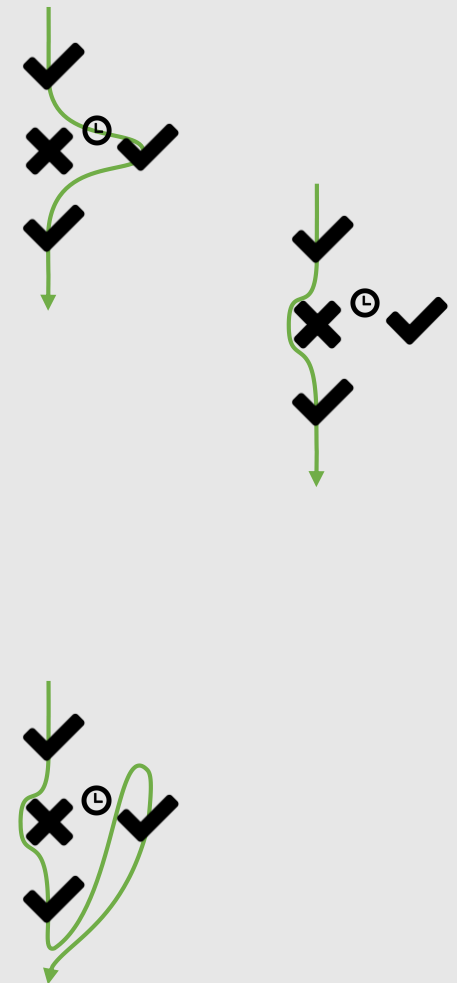
- Signal and WhatsApp sent acknowledgments *plain*



Order in Instant Messaging

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

- Ordering
 - With graphical user interface (out of scope)
 - Causality (m_i delivered if m_{i-1} delivered)
 - *Weak* causality (m_i delivered if not m_j delivered, $i < j$)
- Signal and WhatsApp deliver messages on receipt
 - Server can mix last 2000 messages in delivery
 - Allows to refer to specific messages



Order in Instant Messaging

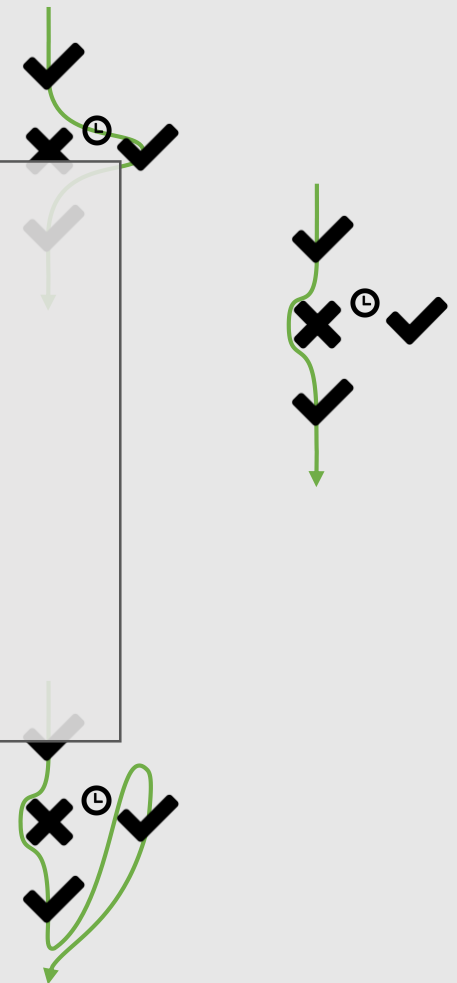
Security Model
Reliability vs. Instant Messaging
 PCS and Ratcheting
 Asynchronous Group IM

- Ordering

- With graphical user interface (out of scope)
- Causality (m_i delivered if m_{i-1} delivered)
- Weak causality (m_i delivered if not m_j delivered, $i < j$)

Have a look into the paper...

- Signal and WhatsApp deliver messages on receipt
 - Server can mix last 2000 messages in delivery
 - Allows to refer to specific messages

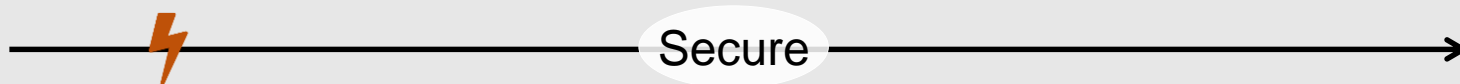


Post Compromise Security and Ratcheting

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

Post Compromise Security in Groups

- Recovery into secure state after its exposure



Post Compromise Security and Ratcheting

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

Post Compromise Security in Groups

- Recovery into secure state after its exposure
 - “Secure state”?
 - **Confidentiality** of messages after λ “group round trips”, λ constant



Post Compromise Security and Ratcheting

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

Post Compromise Security in Groups

- Recovery into secure state after its exposure
 - “Secure state”?
 - **Confidentiality** of messages after λ “group round trips”, λ constant
 - Can be scaled for different protocols

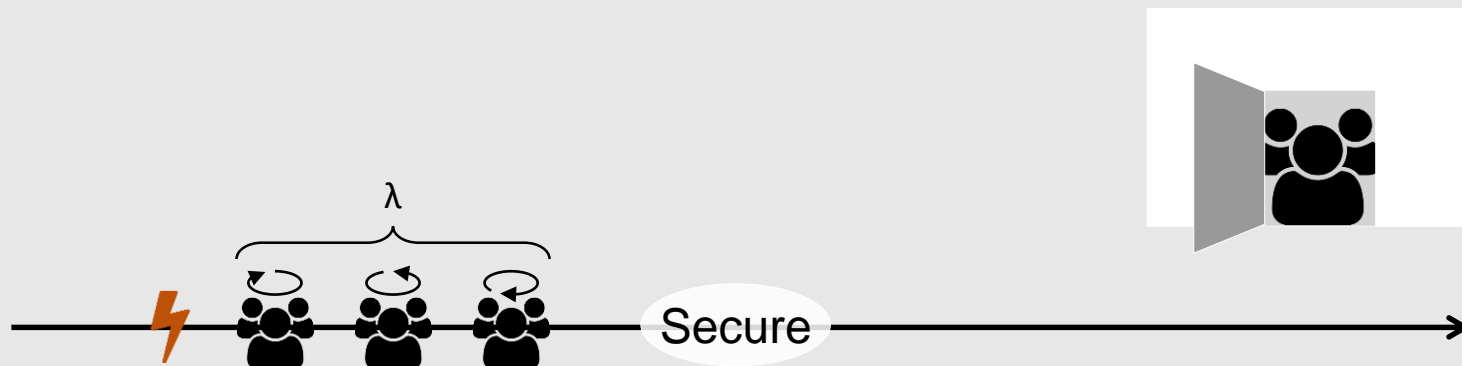


Post Compromise Security and Ratcheting

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

Post Compromise Security in Groups

- Recovery into secure state after its exposure
 - “Secure state”?
 - **Confidentiality** of messages after λ “group round trips”, λ constant
 - ⇒ **Closeness** of group after λ “group round trips”



Post Compromise Security and Ratcheting

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

Post Compromise Security in Groups

- Recovery into secure state after its exposure
 - “Secure state”?
 - **Confidentiality** of messages after λ “group round trips”, λ constant
 - ⇒ **Closeness** of group after λ “group round trips”

Ratcheting

- Continuous update of state secrets to reach PCS




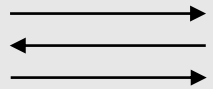
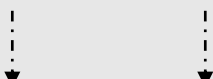
Post Compromise Security and Ratcheting

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

Post Compromise Security in Groups

- Recovery into secure state after its exposure
 - “Secure state”?
 - **Confidentiality** of messages after λ “group round trips”, λ constant
 - ⇒ **Closeness** of group after λ “group round trips”

Ratcheting

- Continuous update of state secrets to reach PCS 
 - Direct communication: Signal, [BCJ+ CRYPTO ‘17], [**PoeRoe ePrint ‘18**]
 - *Continuously redo key exchanges and mix* 
 - *In the meantime forward securely update secrets* 


Post Compromise Security and Ratcheting

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

Post Compromise Security in Groups

- Recovery into secure state after its exposure
 - “Secure state”?
 - **Confidentiality** of messages after λ “group round trips”, λ constant
 - ⇒ **Closeness** of group after λ “group round trips”

Ratcheting

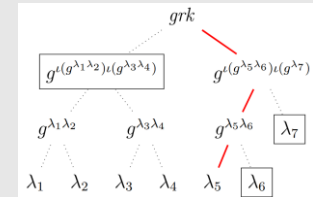
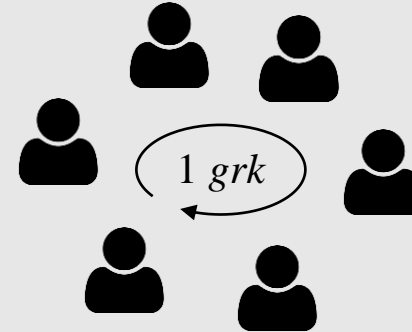
- Continuous update of state secrets to reach PCS 
 - Direct communication: Signal, [BCJ+ CRYPTO ‘17], [PoeRoe ePrint ‘18]
 - Groups?

Post Compromise Security and Ratcheting

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

Confidentiality via group key

→ Ratcheting of group key [CCG+ ePrint '17]



Post Compromise Security and Ratcheting

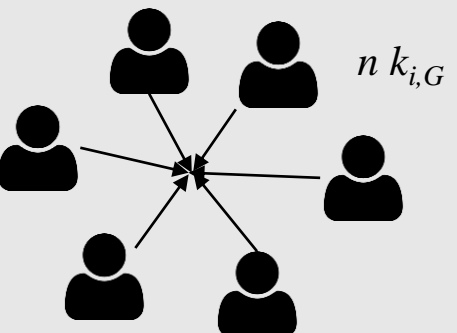
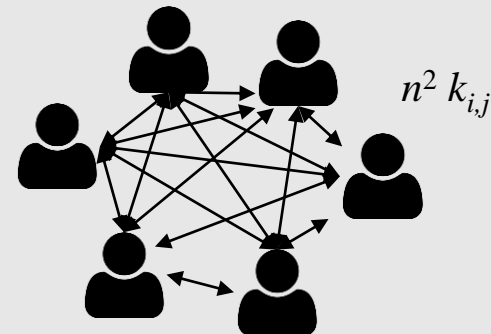
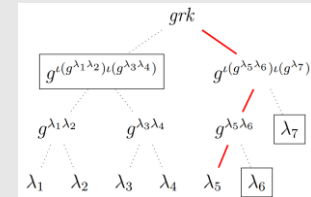
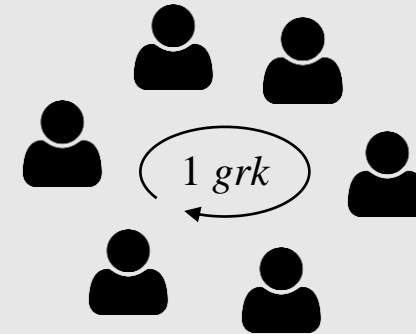
Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

Confidentiality via group key

→ Ratcheting of group key [CCG+ ePrint '17]

Confidentiality via direct channels

→ Ratcheting in direct channels



Post Compromise Security and Ratcheting

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

Confidentiality via group key

→ Ratcheting of group key [CCG+ ePrint '17]

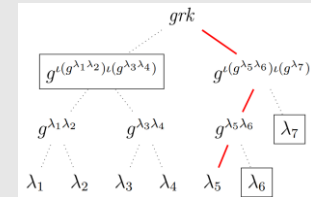
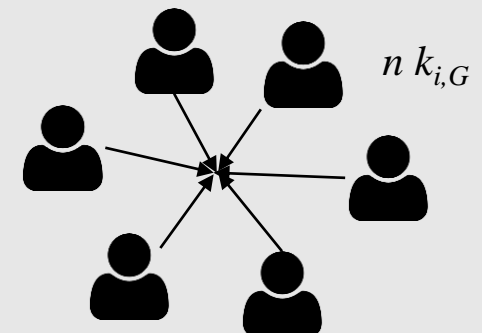
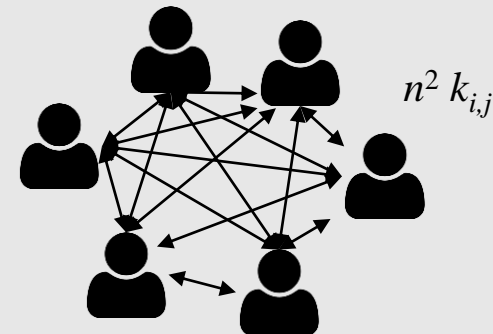
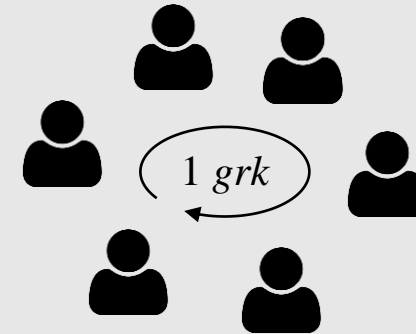
Confidentiality via direct channels

→ Ratcheting in direct channels

→ Group management PCS:

- Ticket approach

→ Related to group key exchange



Post Compromise Security and Ratcheting

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

Confidentiality via group key

→ Ratcheting of group key [CCG+ ePrint '17]

Confidentiality via direct channels

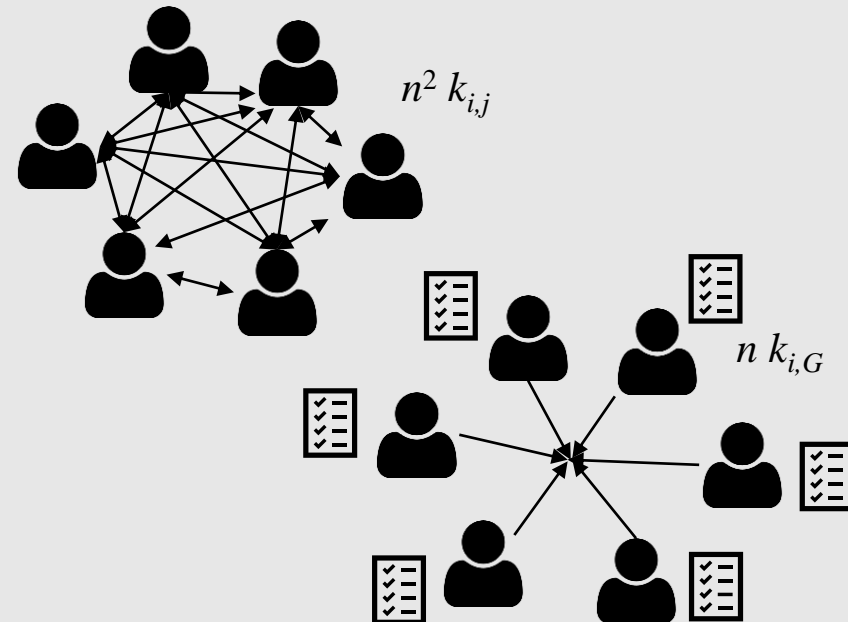
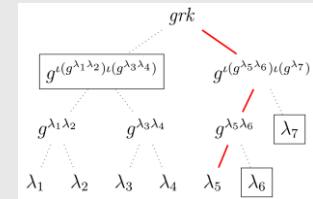
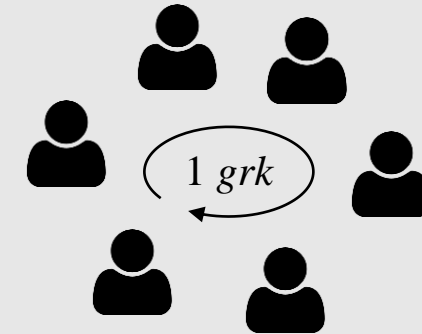
→ Ratcheting in direct channels

→ Group management PCS:

- Ticket approach

→ Related to group key exchange

- Guest list approach



Protocol Overview: Signal

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM



Protocol Overview: Signal

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM



Protocol Overview: Signal

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM



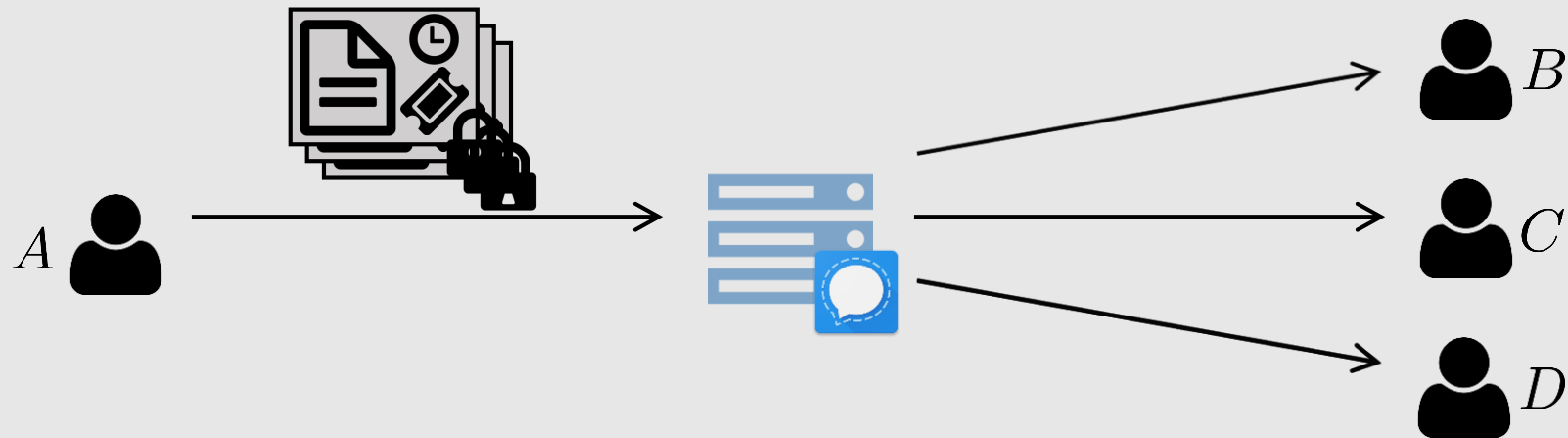
Protocol Overview: Signal

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM



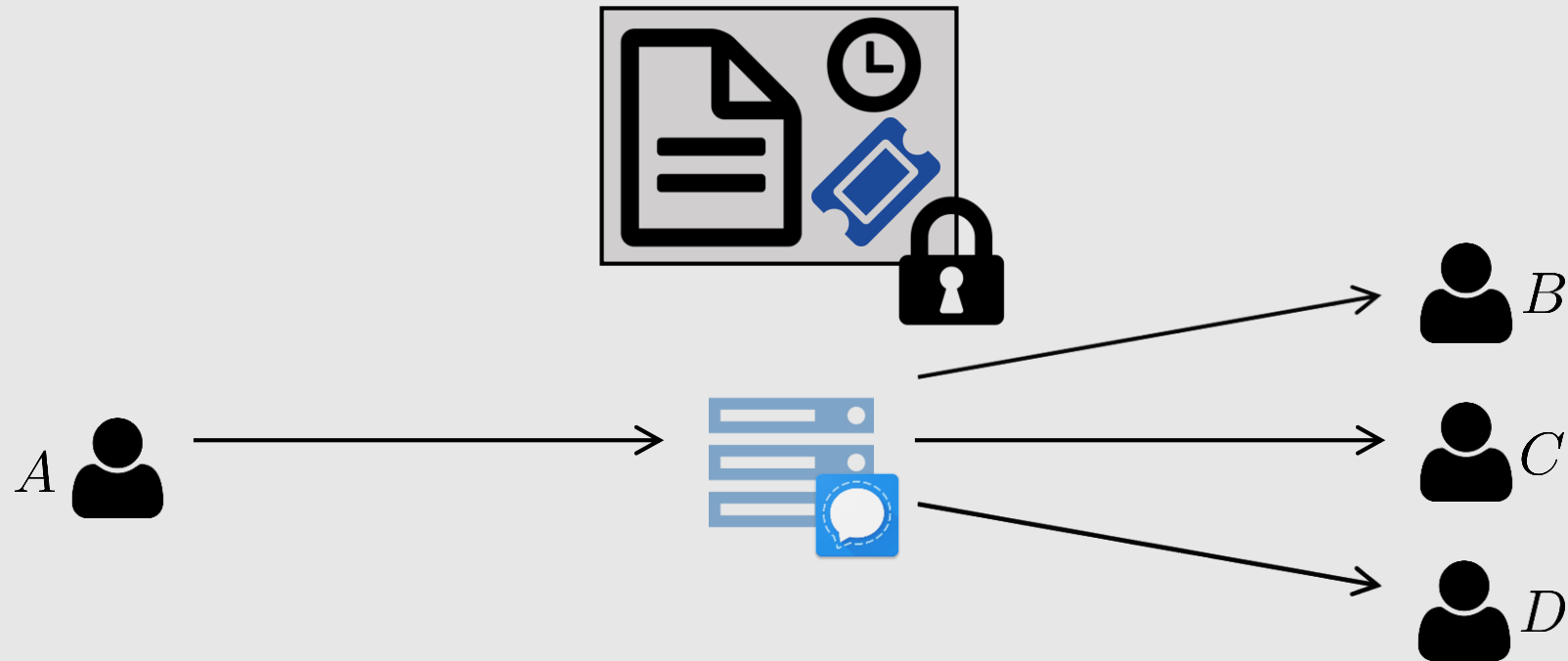
Protocol Overview: Signal

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM



Protocol Overview: Signal

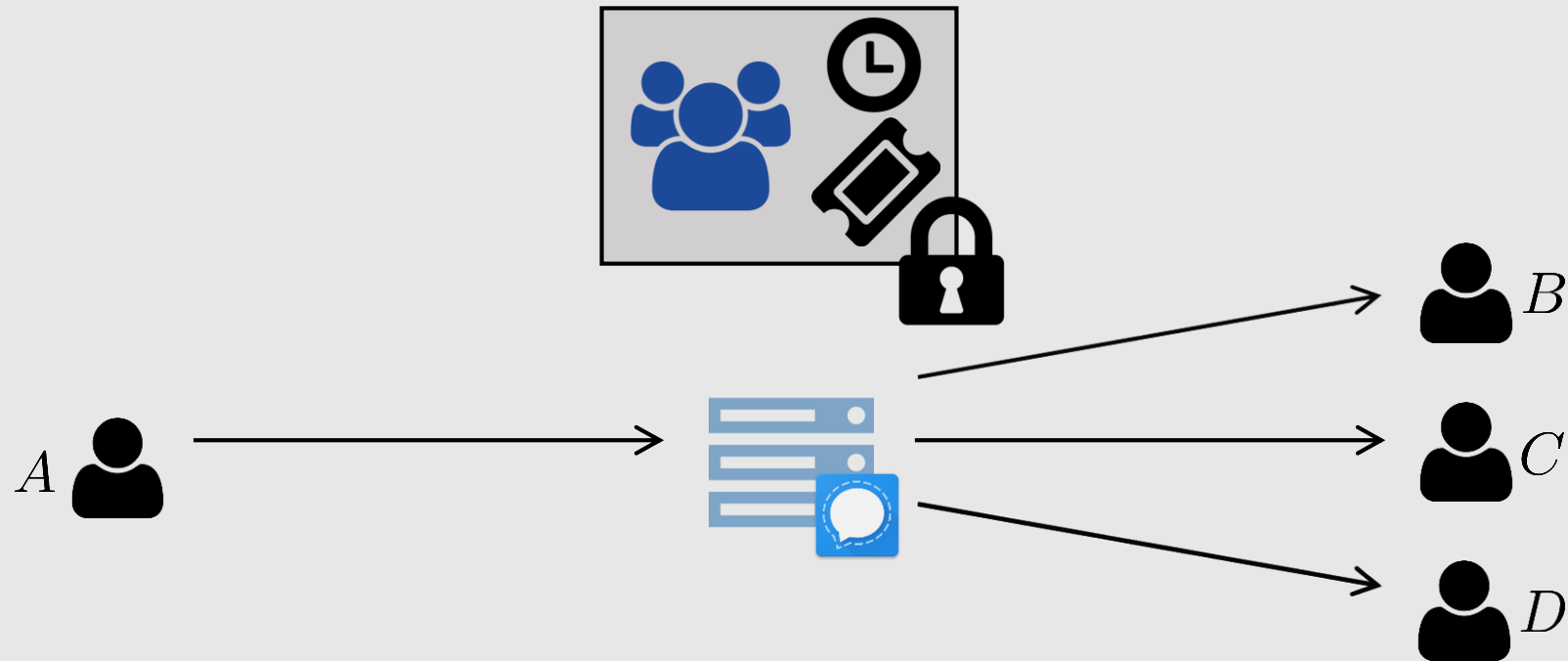
Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM



Sender in group?

Protocol Overview: Signal

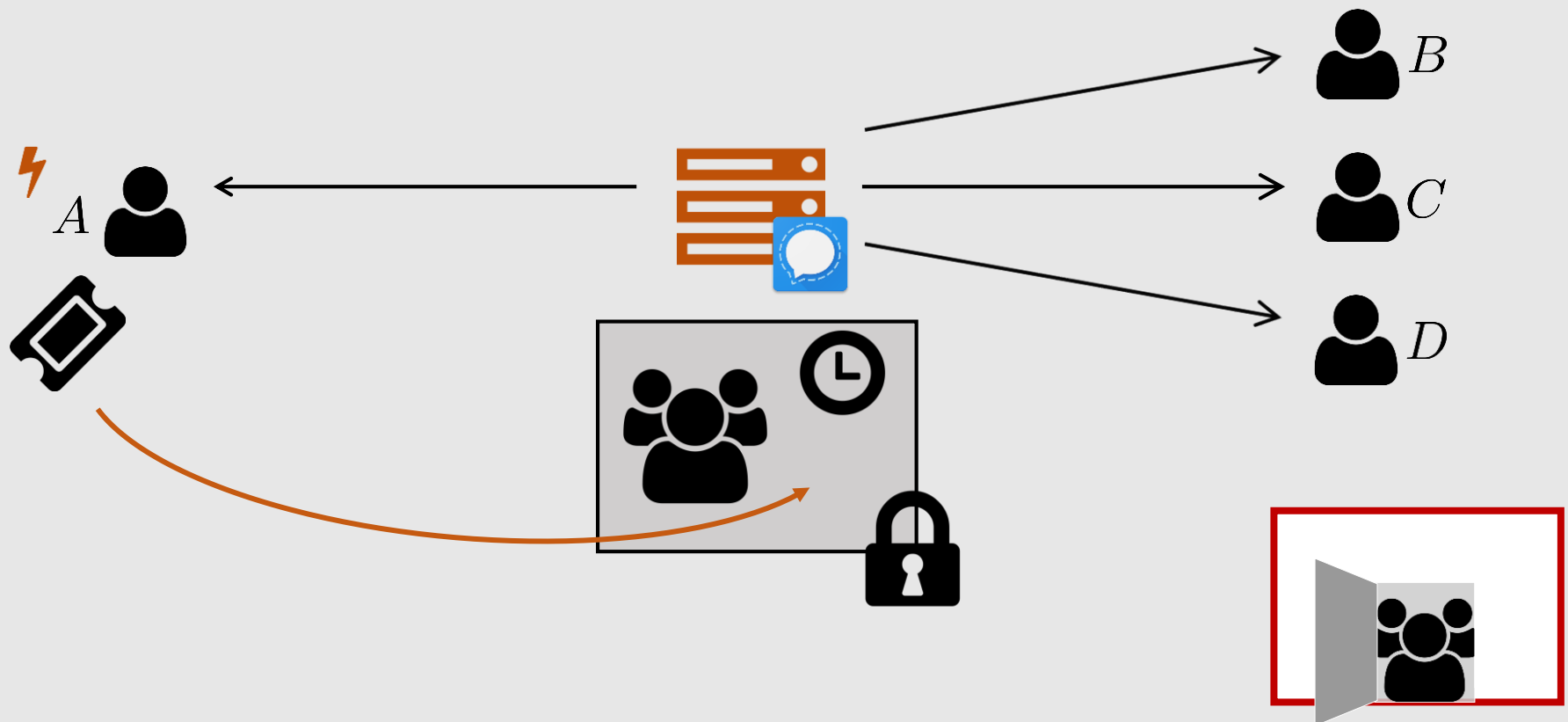
Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM



New receiver in group

Weaknesses: Signal

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM



Post Compromise Security and Ratcheting

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

Confidentiality via group key

→ Ratcheting of group key [CCG+ ePrint '17]

Confidentiality via direct channels

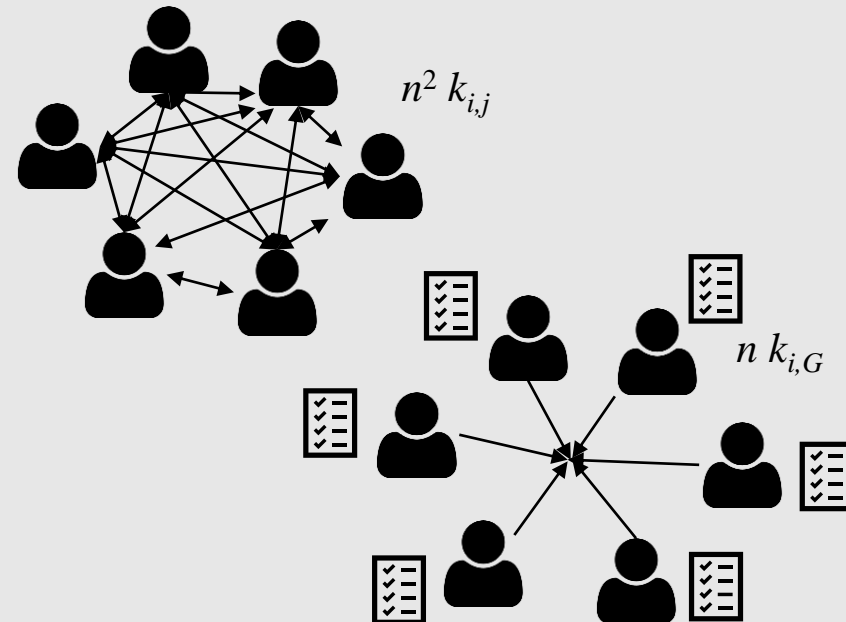
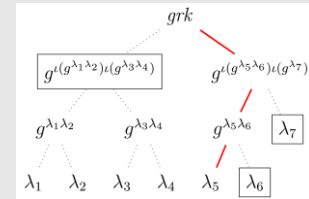
→ Ratcheting in direct channels

→ Group management PCS:

- Ticket approach

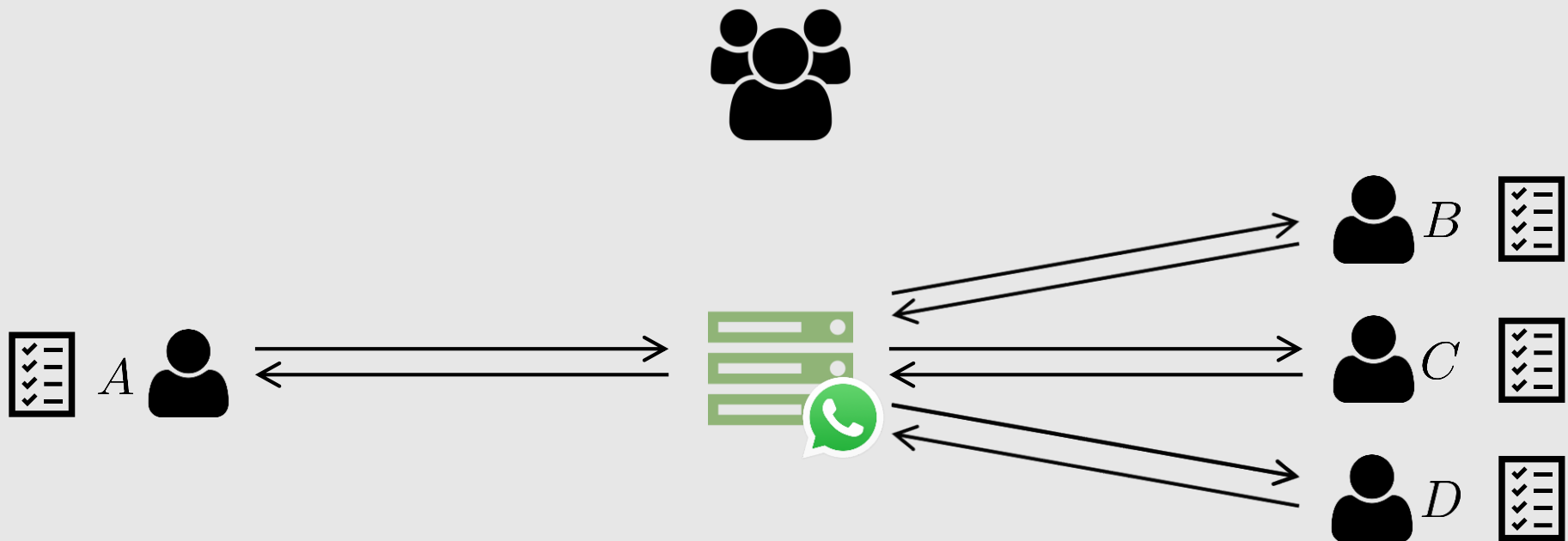
→ Related to group key exchange

- Guest list approach



Protocol Overview: WhatsApp

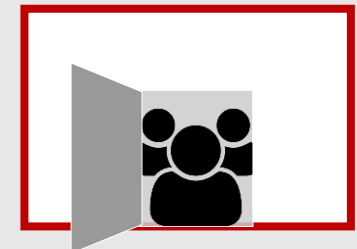
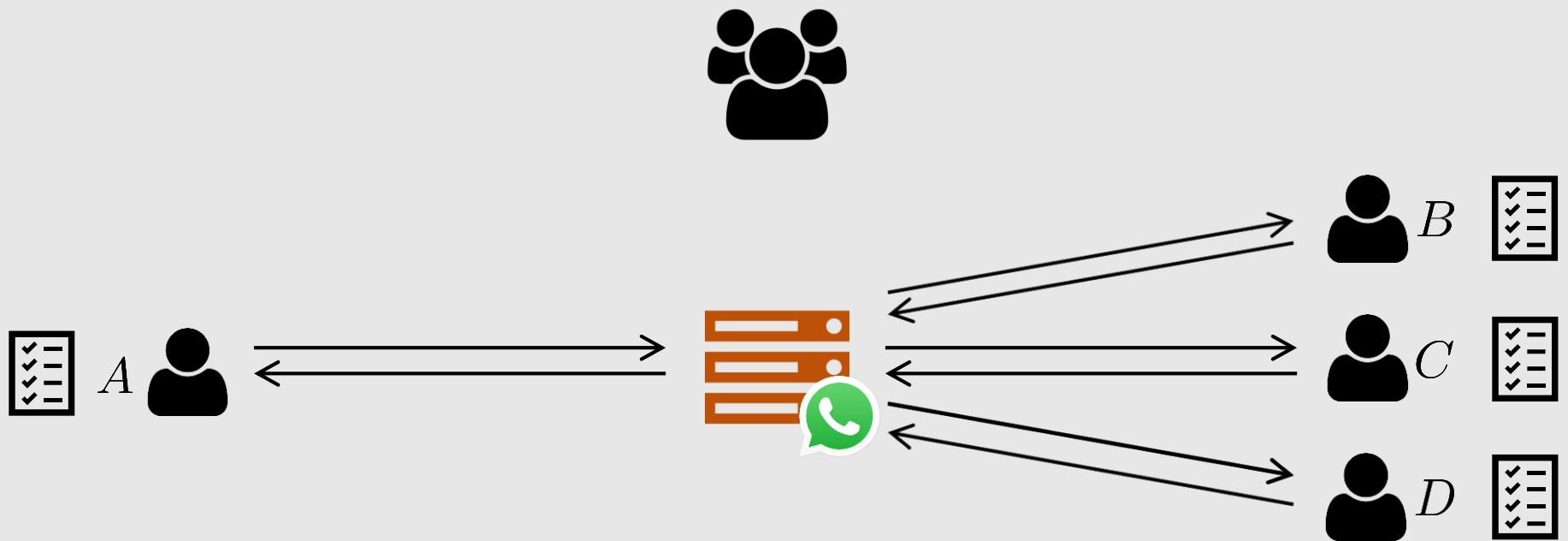
Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM



Sender in group?
& Receiver in group!

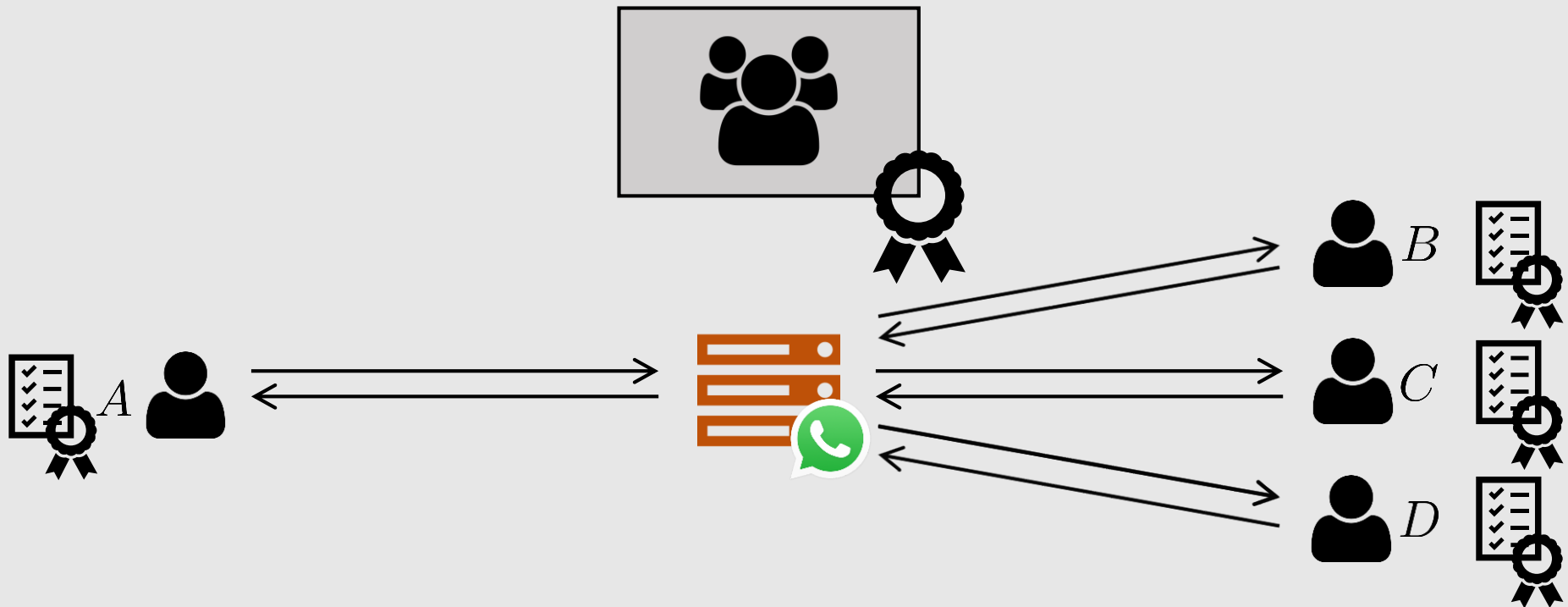
Protocol Overview: WhatsApp

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM



Protocol Overview: WhatsApp

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM



Post Compromise Security and Ratcheting

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

Confidentiality via group key

→ Ratcheting of group key [CCG+ ePrint '17]

Confidentiality via direct channels

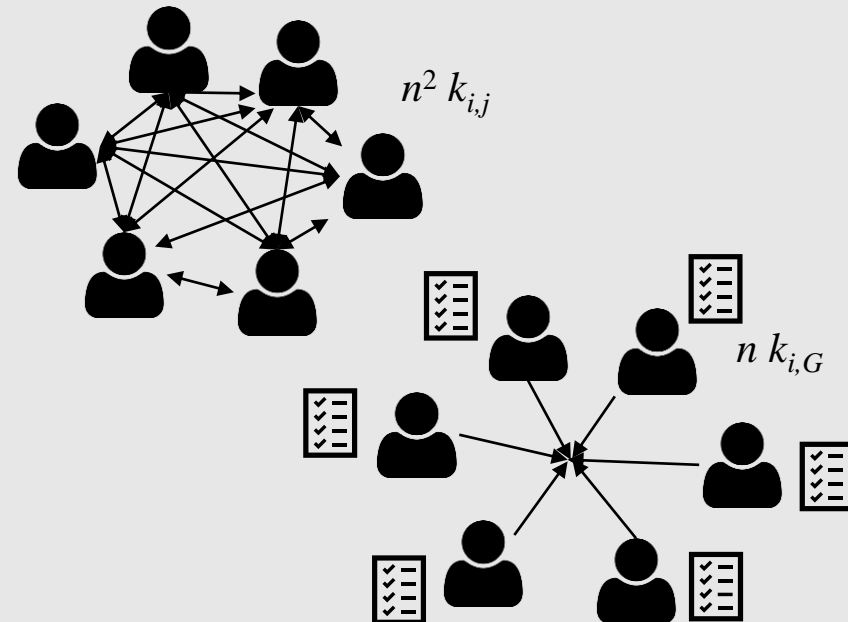
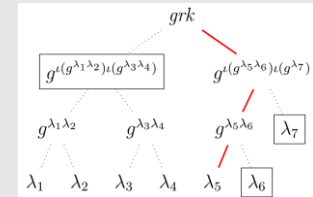
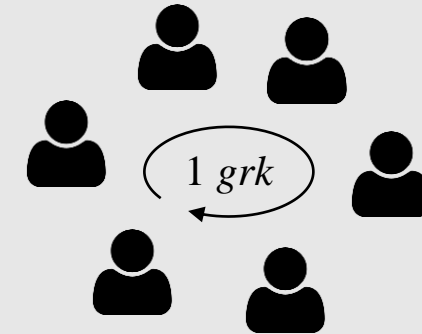
→ Ratcheting in direct channels

→ Group management PCS:

- Ticket approach

→ Related to group key exchange

- Guest list approach



Post Compromise Security and Ratcheting

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

Confidentiality via group key

→ Ratcheting of group key [CCG+ ePrint '17]

Confidentiality via direct channels

→ Ratcheting in direct channels

→ Group management PCS:

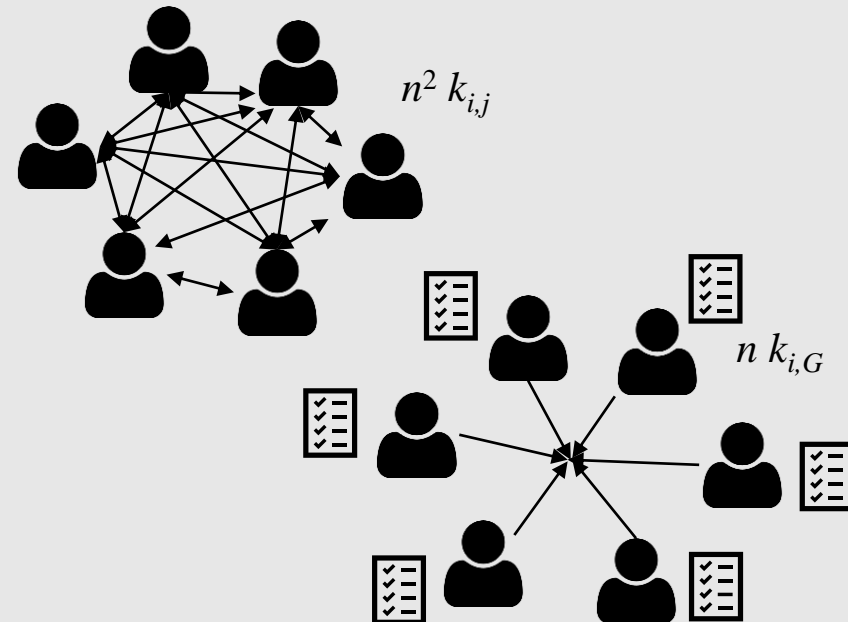
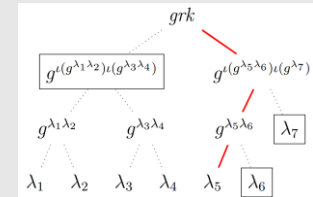
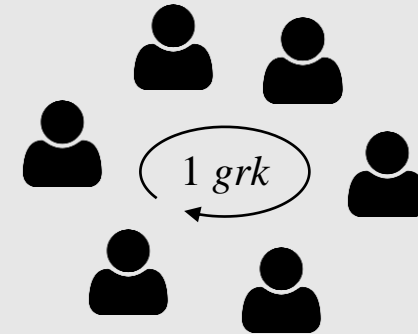
- Ticket approach

→ Related to group key exchange

- Guest list approach

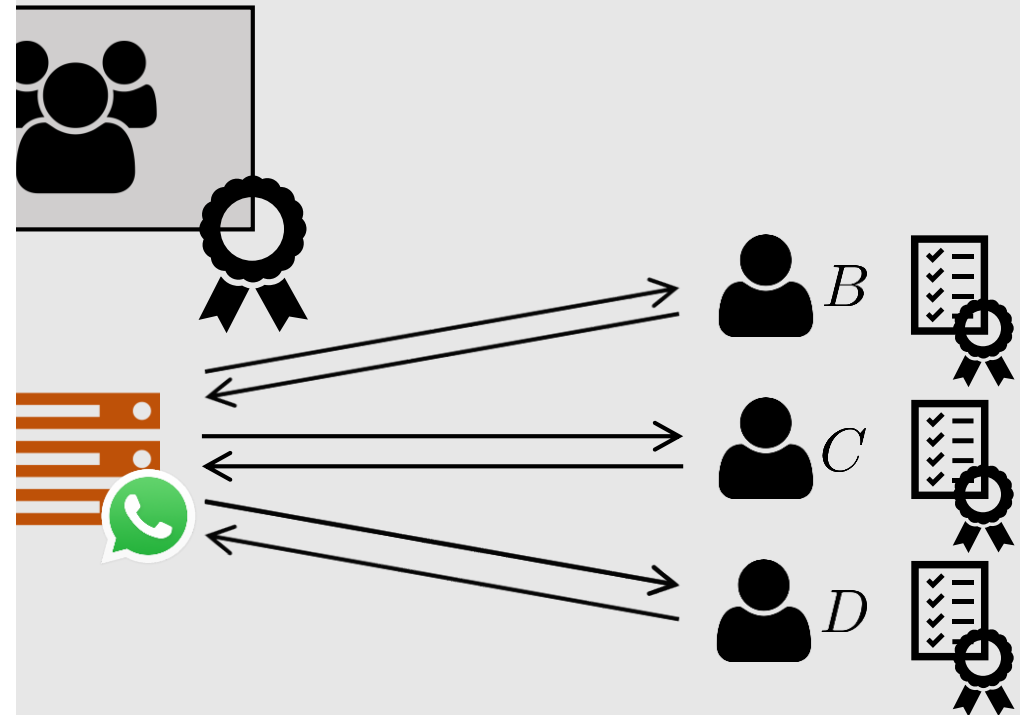
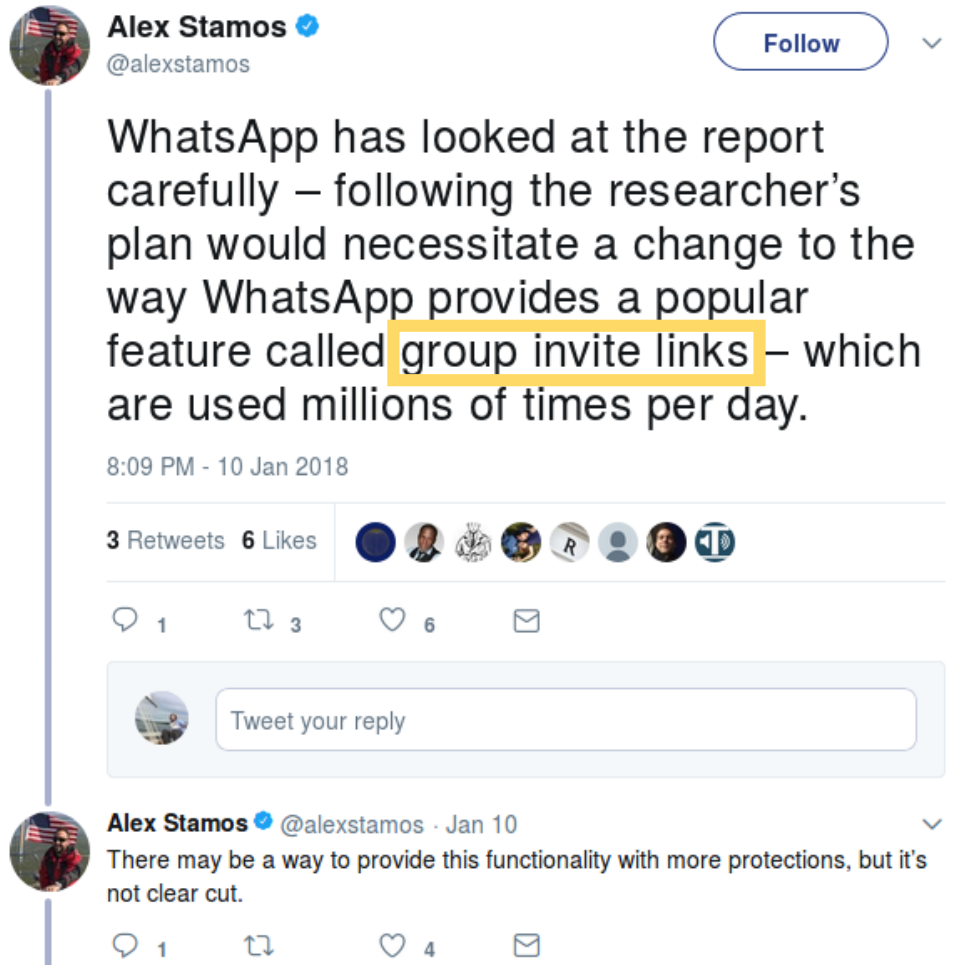
→ No complex group key ratcheting

→ Problems in asynchronous federated environment



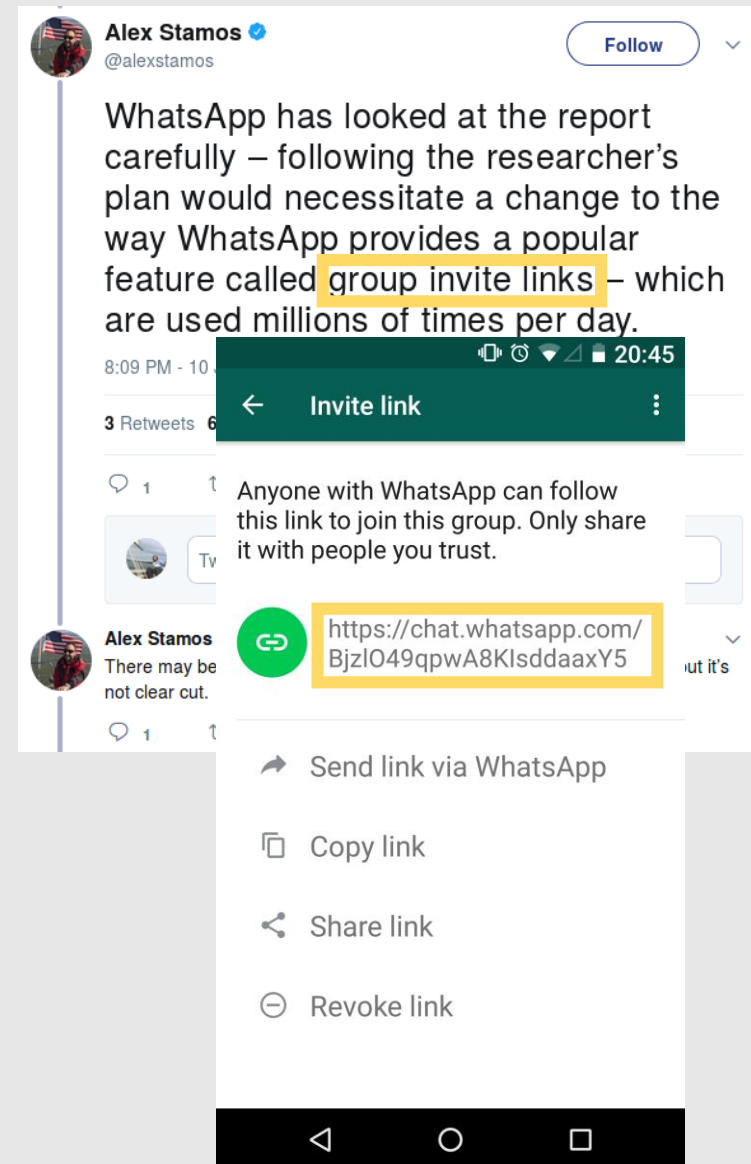
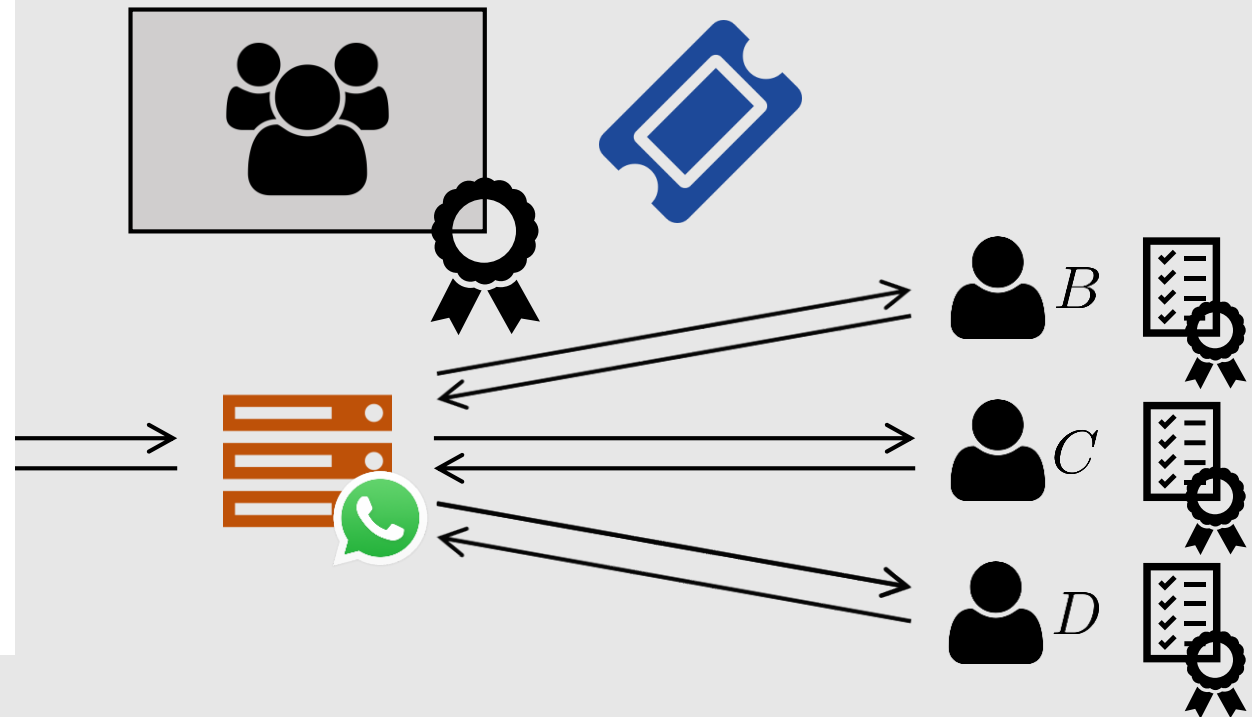
Protocol Overview: WhatsApp

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM



Protocol Overview: WhatsApp

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM



Post Compromise Security and Ratcheting

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

Confidentiality via group key

→ Ratcheting of group key [CCG+ ePrint '17]

Confidentiality via direct channels

→ Ratcheting in direct channels

→ Group management PCS:

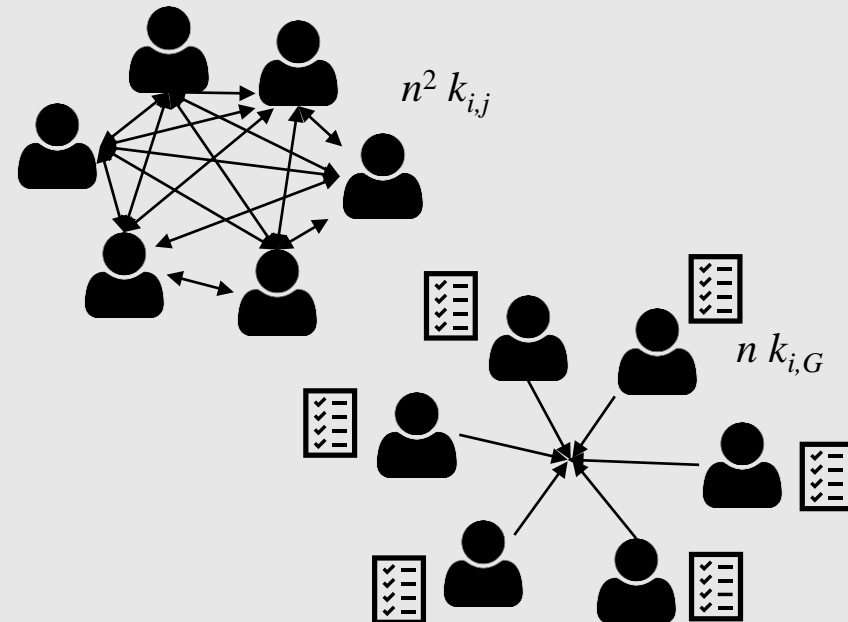
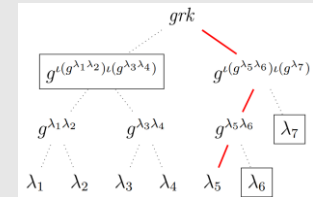
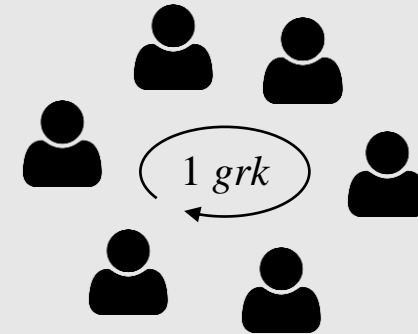
- Ticket approach

→ Related to group key exchange

- Guest list approach

→ No complex group key ratcheting

→ Problems in asynchronous federated environment



Complexity of Dynamic Groups in Asynchronous Networks

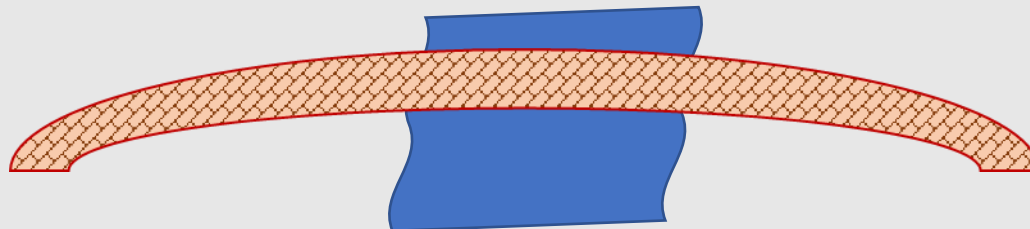
Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

Practice

- Dynamic group IM
- Ratcheting
- Concurrency
- Special ordering
- Trace delivery

Theory

- Dynamic group key exchange
- Static group key ratcheting
- Definitions of reliability



Complexity of Dynamic Groups in Asynchronous Networks

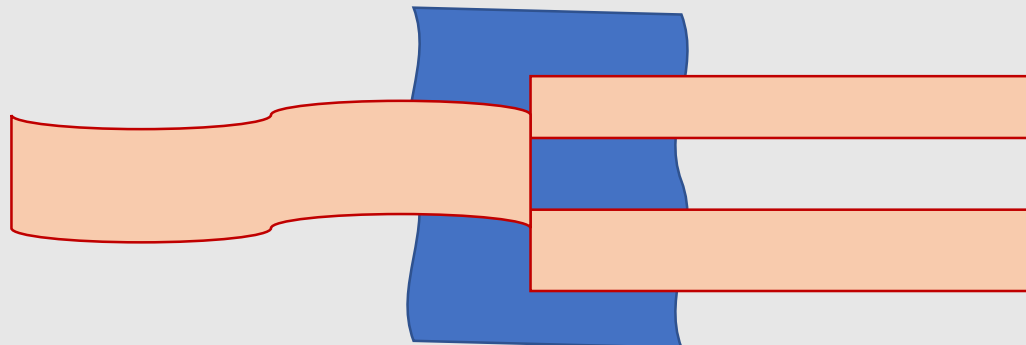
Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

Practice

- Dynamic group IM
- Ratcheting
- Concurrency
- Special ordering
- Trace delivery

Theory

- Dynamic group key exchange
 - Synchronous communication
- Static group key ratcheting
 - No concurrency
- Definitions of reliability
 - Incompatible with IM



Complexity of Dynamic Groups in Asynchronous Networks

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

Practice

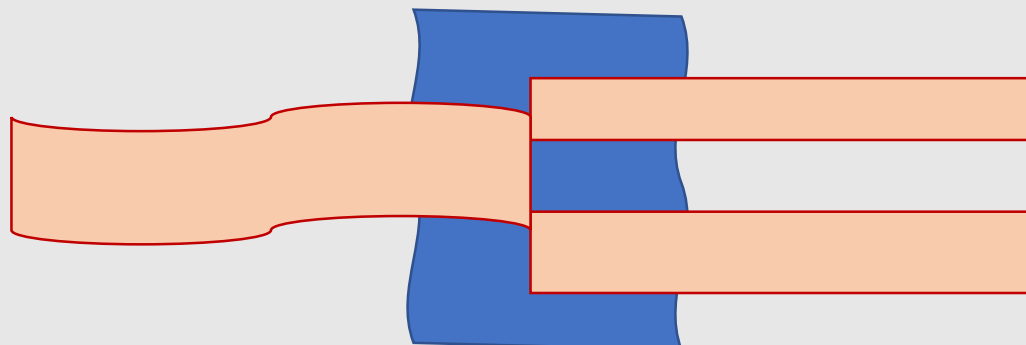
- Dynamic group IM
- Ratcheting
- Concurrency
- Special ordering
- Trace delivery

Theory

- Dynamic group key exchange
- Synchronous communication
- Static group key ratcheting
- No concurrency
- Definition of reliability
- Incompatible with IM

We

- Propose a model capturing relevant security notions
- Analyzed real world w.r.t. to this model
- Propose measures for enhancing real world



Complexity of Dynamic Groups in Asynchronous Networks

Security Model
Reliability vs. Instant Messaging
PCS and Ratcheting
Asynchronous Group IM

Practice

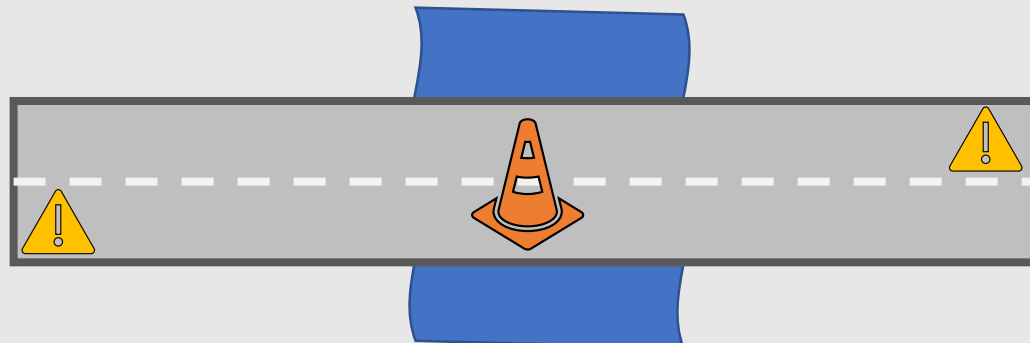
- Dynamic group IM
- Ratcheting
- Concurrency
- Special ordering
- Trace delivery

Theory

- Dynamic group key exchange
- Synchronous communication
- Static group key ratcheting
- No concurrency
- Definition of reliability
- Incompatible with IM








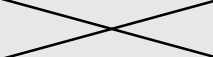




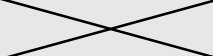




We

- Propose a model capturing relevant security notions
- Analyzed real world w.r.t. to this model
- Propose measures for enhancing real world



Summary

- First security model for group instant messaging
 - Captures security and *reliability*
- Description (\Rightarrow reverse engineering) of three major IM protocols
- Application of model to protocols
 - Revelation of discrepancies between security definition and protocols:

	Closeness	Forward Secrecy	Future Secrecy	Traceable Delivery	No Duplication	No Creation
						
						
						

ia.cr/2017/713

@roeslpa