RUHR-UNIVERSITÄT BOCHUM

RUB

On the End-to-End Security of Group Chats

Real World Crypto 2018

2018-01-10

Horst Görtz Institute for IT Security
Chair for Network and Data Security
Paul Rösler, Christian Mainka, Jörg Schwenk

RUHR-UNIVERSITÄT BOCHUM

On the End-to-End Security of Group Chats

Real World Crypto 2018

2018-01-10

Horst Görtz Institute for IT Security
Chair for Network and Data Security
Paul Rösler, Christian Mainka, Jörg Schwenk

Or:

Why what ☎ is doing is 👍

RUHR-UNIVERSITÄT BOCHUM

RUB

On the End-to-End Security of Group Chats

Real World Crypto 2018

2018-01-10

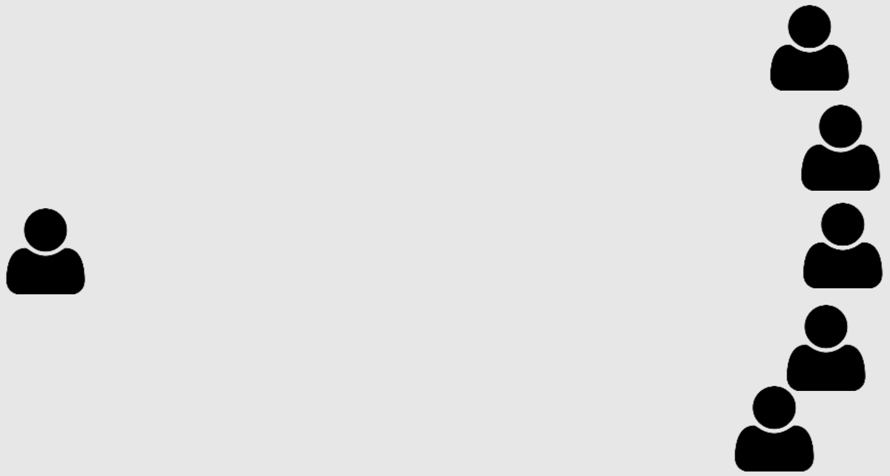
Horst Görtz Institute for IT Security
Chair for Network and Data Security
Paul Rösler, Christian Mainka, Jörg Schwenk

Or:

Why what 📞 is doing is 👎 (in 👥)

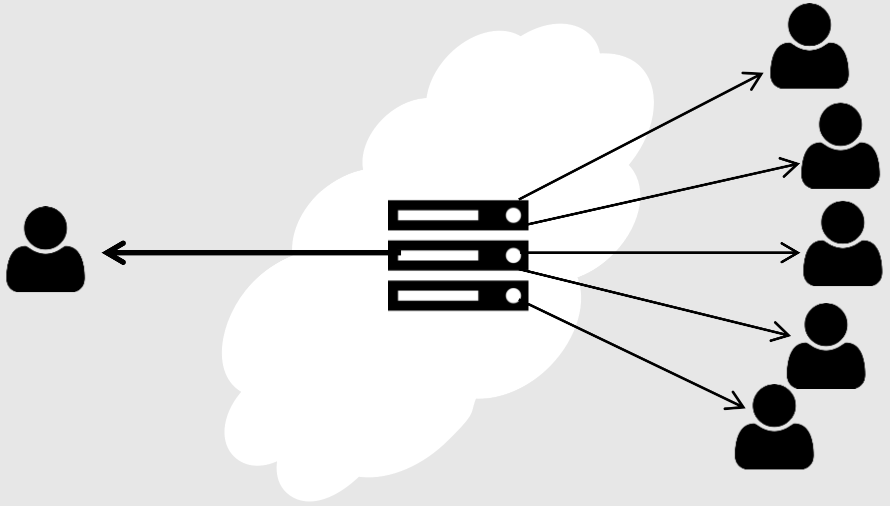
Secure Group Instant Messaging: End-to-End

- Dynamic group of users



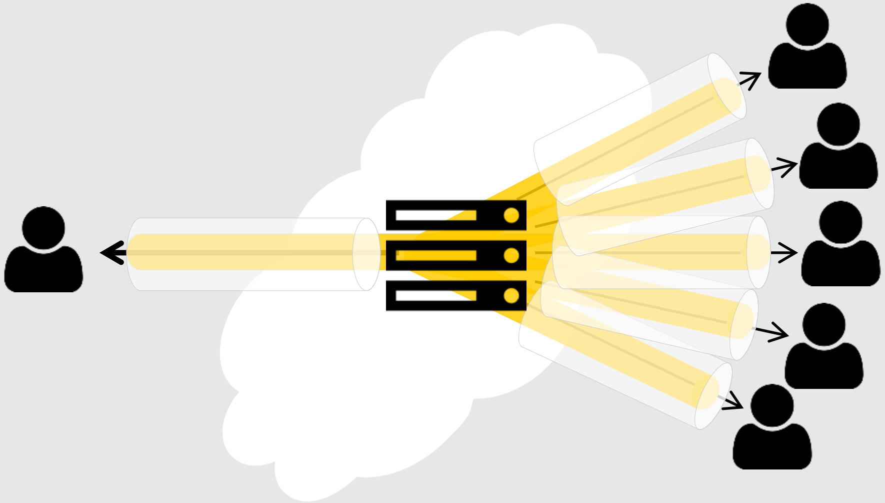
Secure Group Instant Messaging: End-to-End

- Dynamic group of users
- One central server



Secure Group Instant Messaging: End-to-End

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



Agenda

- Security Model
- Protocol Overview and Weaknesses
  - Signal
  - WhatsApp
  - (Threema)
- Problems and Solutions
  - Traceable Delivery
  - Closeness

Secure Group Instant Messaging: Two Parties

Confidentiality

- Message Confidentiality

Integrity

- Message Authentication } Two Parties } Groups

Secure Group Instant Messaging: Two Parties

Confidentiality

- Message Confidentiality

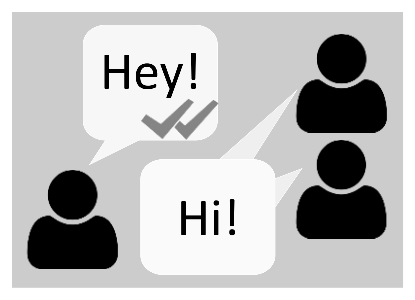
Integrity

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

Two Parties

Groups

“Only successful delivery is acknowledged”



Secure Group Instant Messaging: Groups

Confidentiality

- Message Confidentiality
- **Closeness**

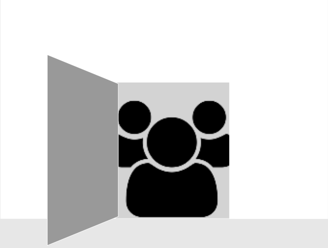
Integrity

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

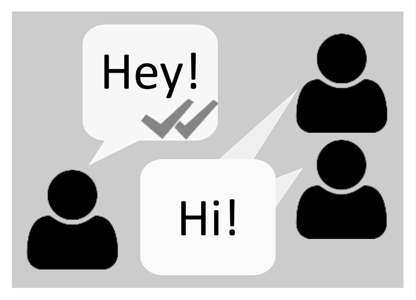
Two Parties

Groups

“Only group (admin) decides on membership”

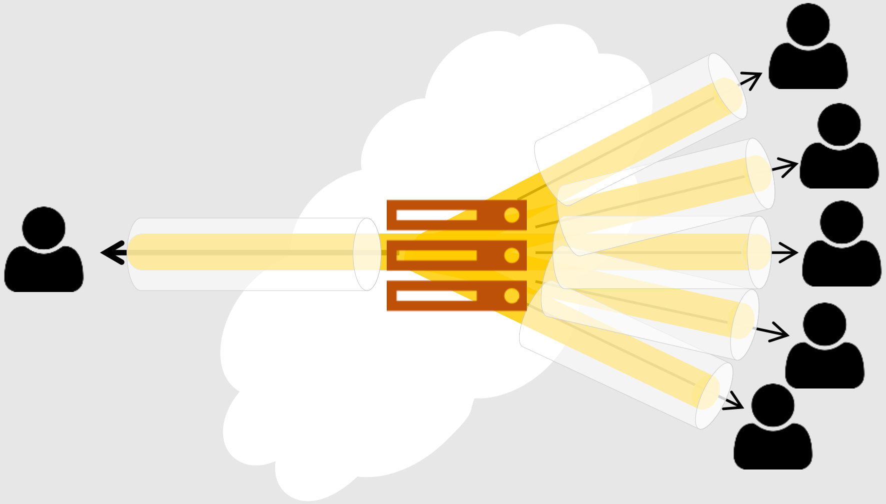


“Only successful delivery is acknowledged”



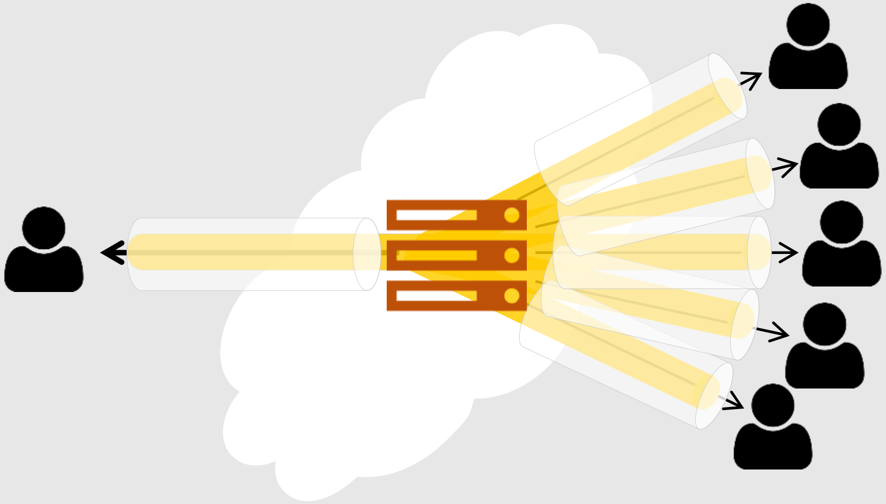
Security Model: Malicious Server

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



Security Model: Malicious Server

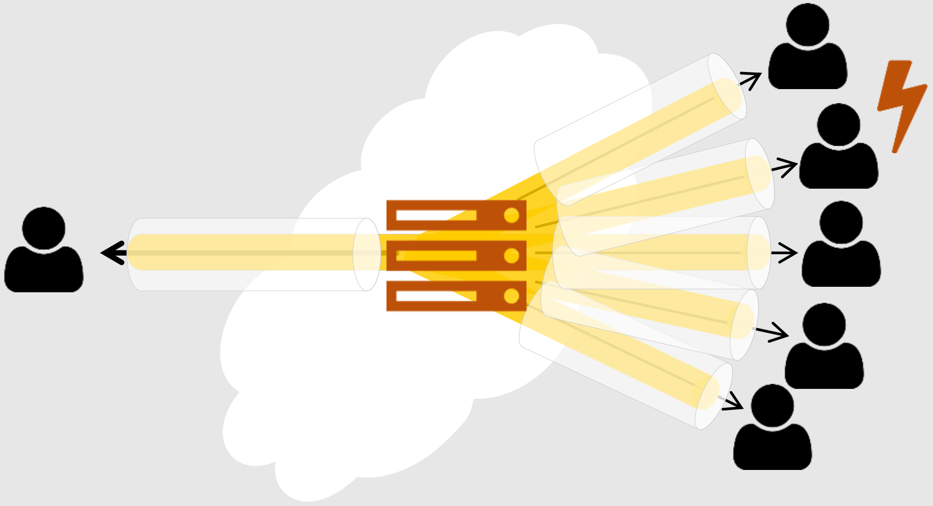
- Malicious Server ☰
  - Can decrypt transport layer protection
  - E.g. IM provider, TLS certificate forger on network, ...



Attackable by	Traceable Delivery	Closeness
💬	☰	?
📞	☰	☰

Security Model: Compromising Attacker

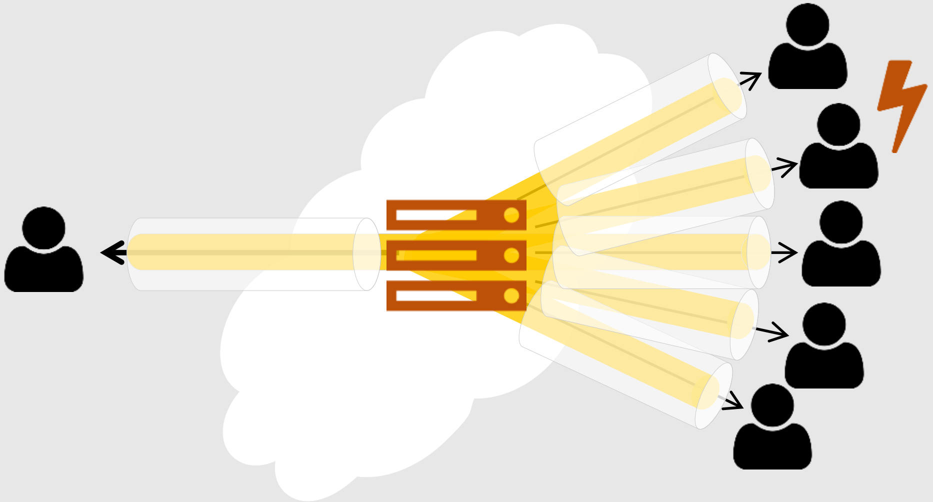
- Compromising Attacker ϟ
  - Access to members’ secrets
  - E.g. access to device, cryptanalysis, …



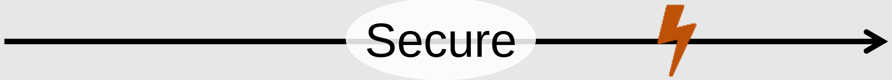
Attackable by	Traceable Delivery	Closeness
💬	🗄	?
📞	🗄	🗄

Security Model: Compromising Attacker

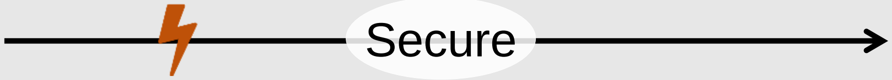
- Compromising Attacker ⚡
  - Access to members’ secrets
  - E.g. access to device, cryptanalysis, …



- Advanced Goals:
  - Forward Secrecy



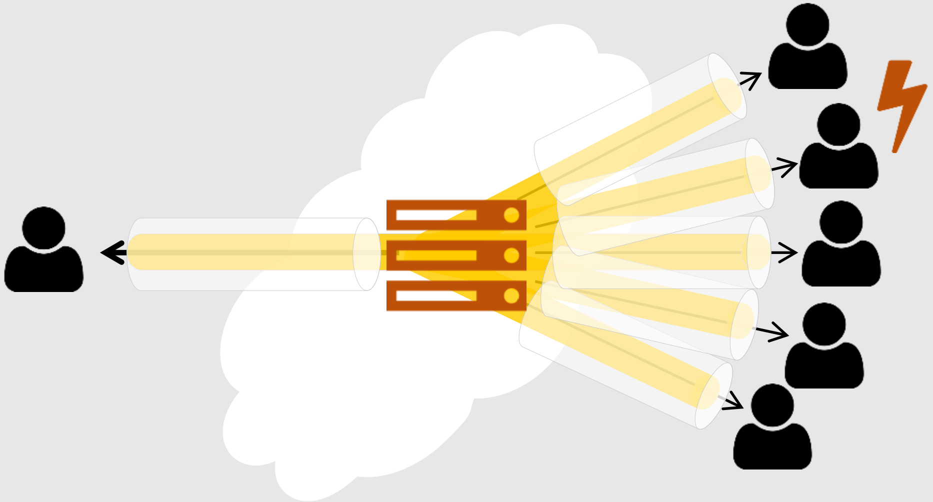
  - Future Secrecy
    (aka Post Compromise Security aka Backward Secrecy)



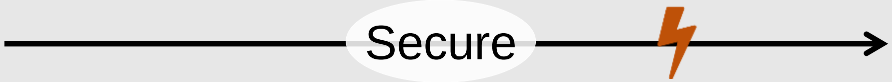
Attackable by	Traceable Delivery	Closeness
💬	🗄	?
📞	🗄	🗄

Security Model: Compromising Attacker

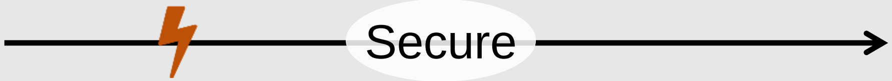
- Compromising Attacker ⚡
  - Access to members’ secrets
  - E.g. access to device, cryptanalysis, …



- Advanced Goals:
  - Forward Secrecy



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



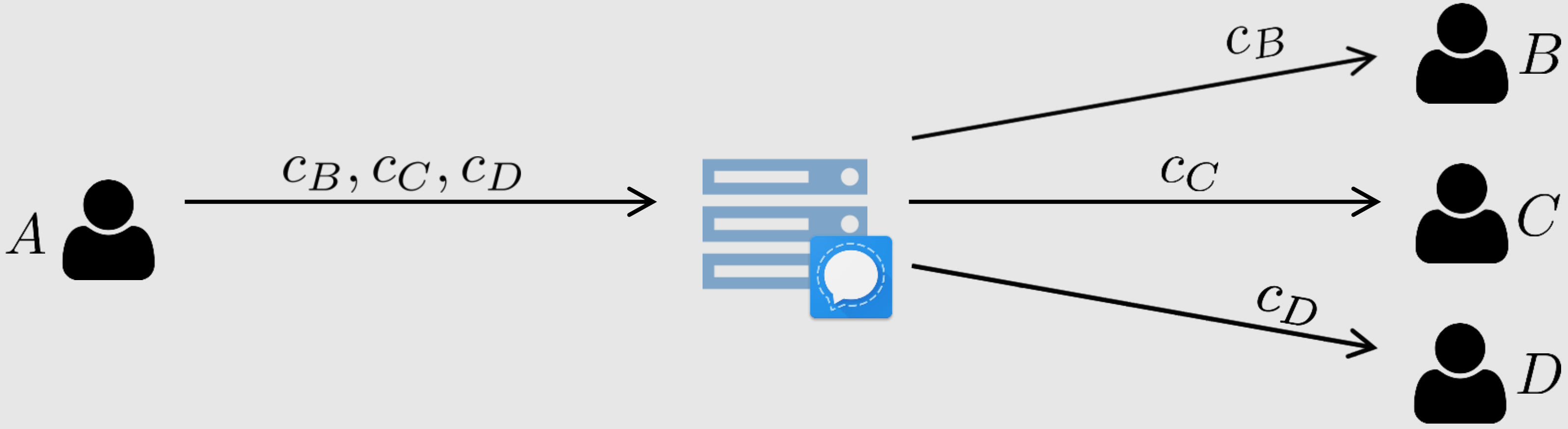
Attackable by	Traceable Delivery	Closeness
💬	🗄	⚡ (Fut. Sec.)
📞	🗄	🗄

Protocol Overview: Signal

- Ciphertexts c (ID static)

$$\forall i \in G \setminus \{A\}\colon$$
$$c_i \leftarrow \mathrm{E}_A(i; ID_G, t, m)$$

$$G = \{A, B, C, D\}$$

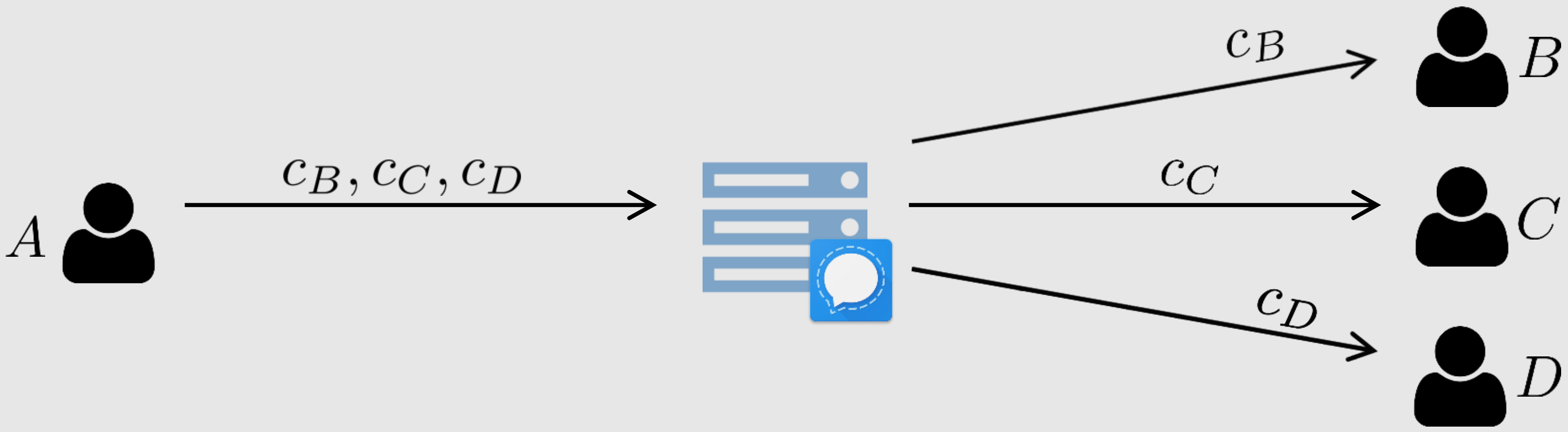


Protocol Overview: Signal

- Ciphertexts c (ID static)

$$\forall i \in G \setminus \{A\}:$$
$$c_i \leftarrow \mathrm{E}_A(i; ID_G, t, m)$$

$$G = \{A, B, C, D\}$$



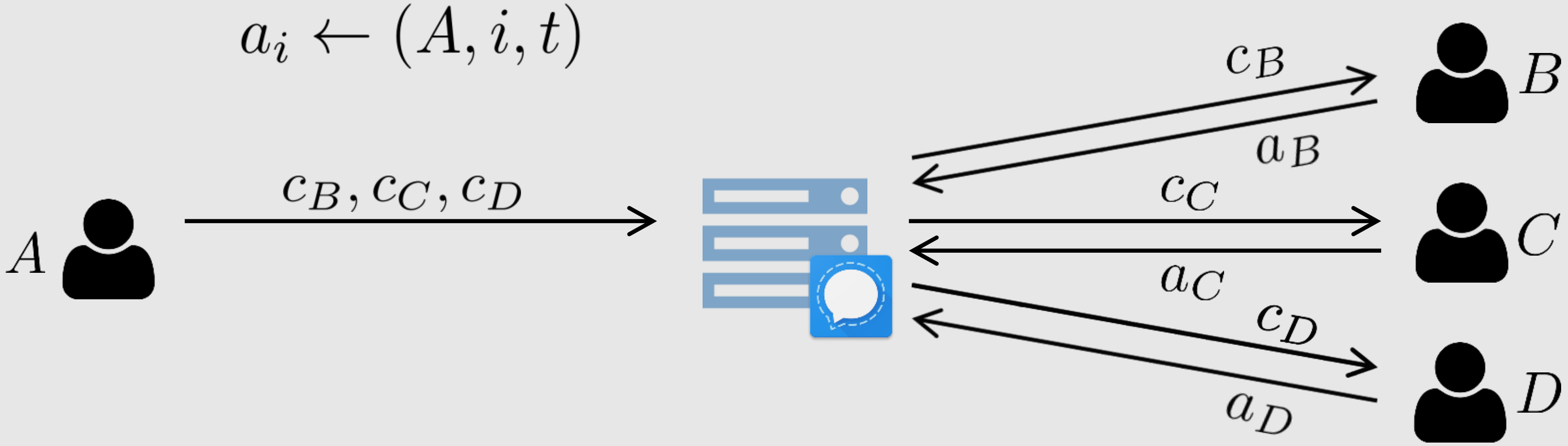
- Forward and future secure key streams of *direct* communication
- Group ID as proof of membership

Protocol Overview: Signal

- Ciphertexts c (ID static)
- Acks a (plain)

$$\forall i \in G \setminus \{A\}:$$
$$c_i \leftarrow \mathrm{E}_A(i; ID_G, t, m)$$
$$a_i \leftarrow (A, i, t)$$

$$G = \{A, B, C, D\}$$



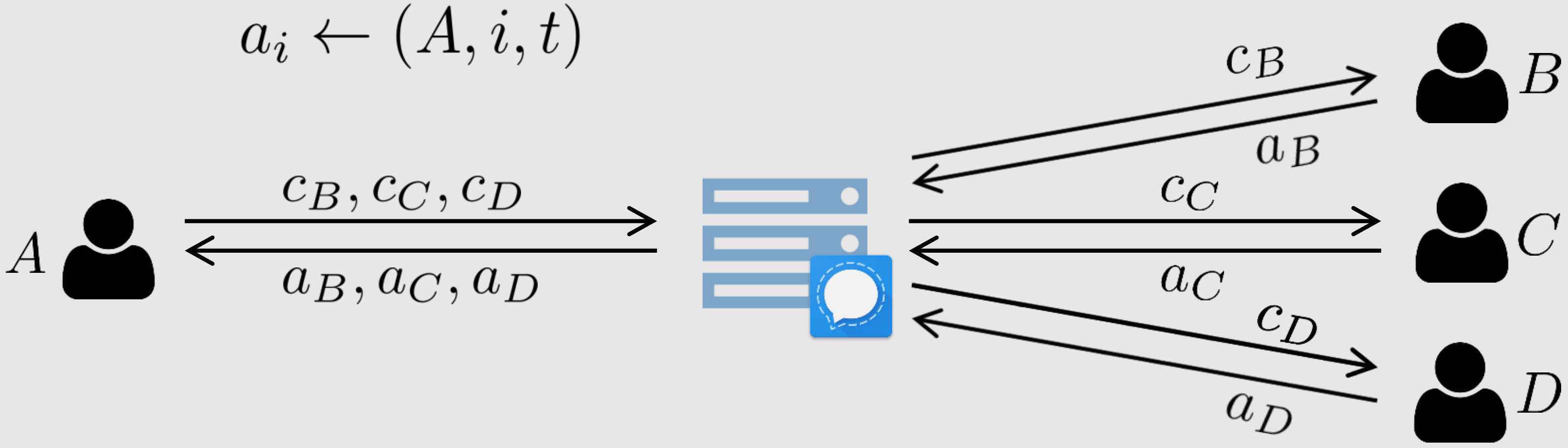
- Forward and future secure key streams of *direct* communication
- Group ID as proof of membership

Protocol Overview: Signal

- Ciphertexts c (ID static)
- Acks a (plain)

$$\forall i \in G \setminus \{A\}:$$
$$c_i \leftarrow \mathrm{E}_A(i; ID_G, t, m)$$
$$a_i \leftarrow (A, i, t)$$

$$G = \{A, B, C, D\}$$



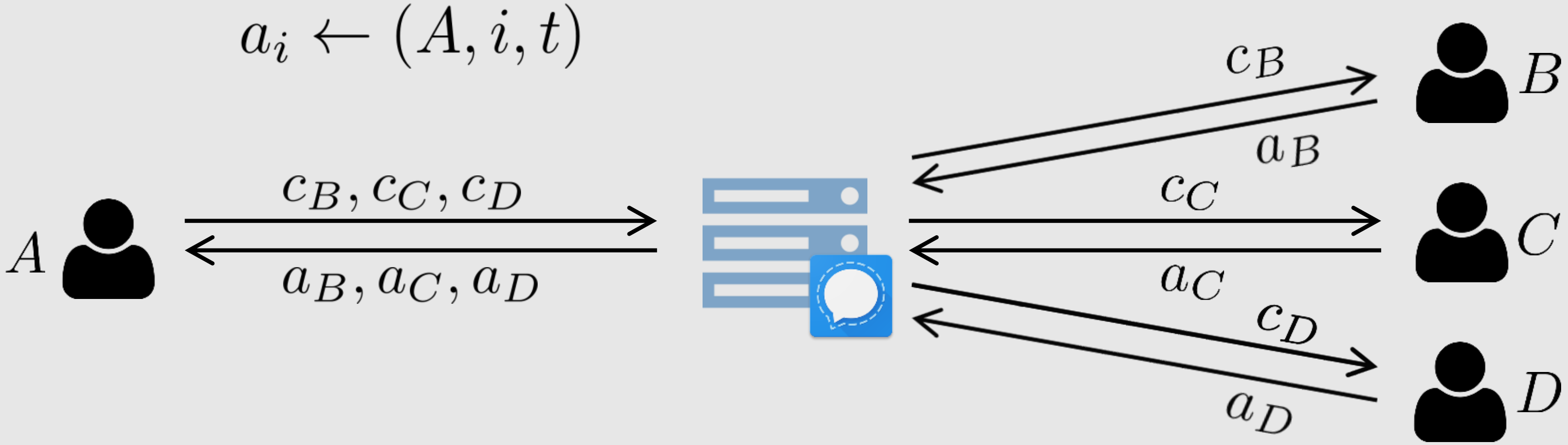
- Forward and future secure key streams of *direct* communication
- Group ID as proof of membership

Protocol Overview: Signal

- Ciphertexts c (ID static)
- Acks a (plain)
- Group update as message m

$$\forall i \in G \setminus \{A\}:$$
$$c_i \leftarrow \mathrm{E}_A(i; ID_G, t, m)$$
$$a_i \leftarrow (A, i, t)$$

$$G = \{A, B, C, D\}$$



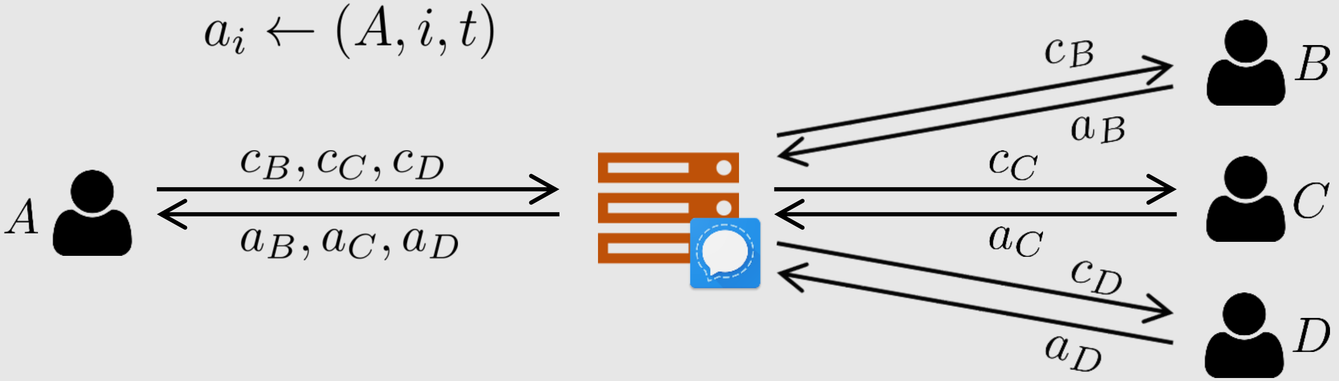
- Forward and future secure key streams of *direct* communication
- Group ID as proof of membership

Weaknesses: Signal

- Ciphertexts c (ID static)
- Acks a (plain)
- Group update as message m

$\forall i \in G \setminus \{A\}$:
$c_i \leftarrow \mathrm{E}_A(i; ID_G, t, m)$
$a_i \leftarrow (A, i, t)$

$G = \{A, B, C, D\}$



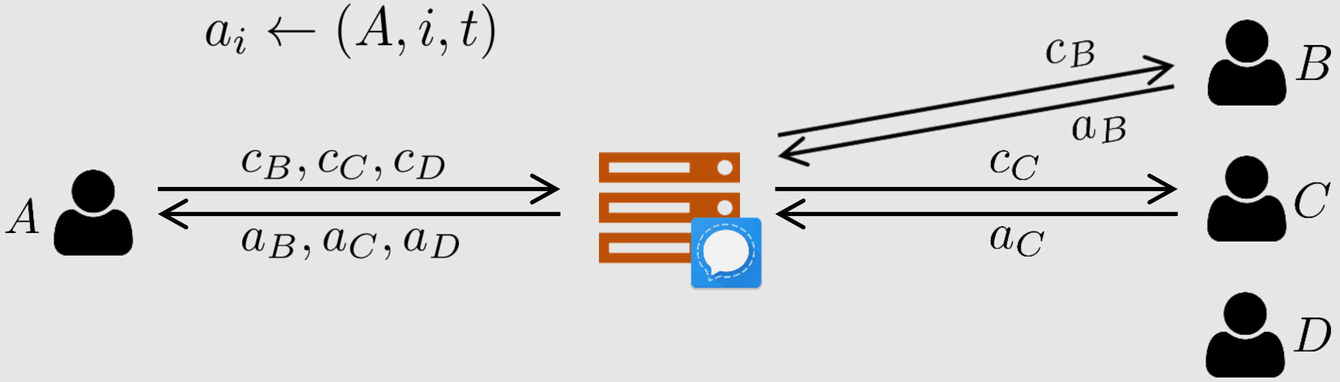
- Forward and future secure key streams of *direct* communication
- Group ID as proof of membership

Weaknesses: Signal

- Ciphertexts c (ID static)
- Acks a (plain)
- Group update as message m

$\forall i \in G \setminus \{A\}$:
$c_i \leftarrow \mathrm{E}_A(i; ID_G, t, m)$
$a_i \leftarrow (A, i, t)$

$G = \{A, B, C, D\}$



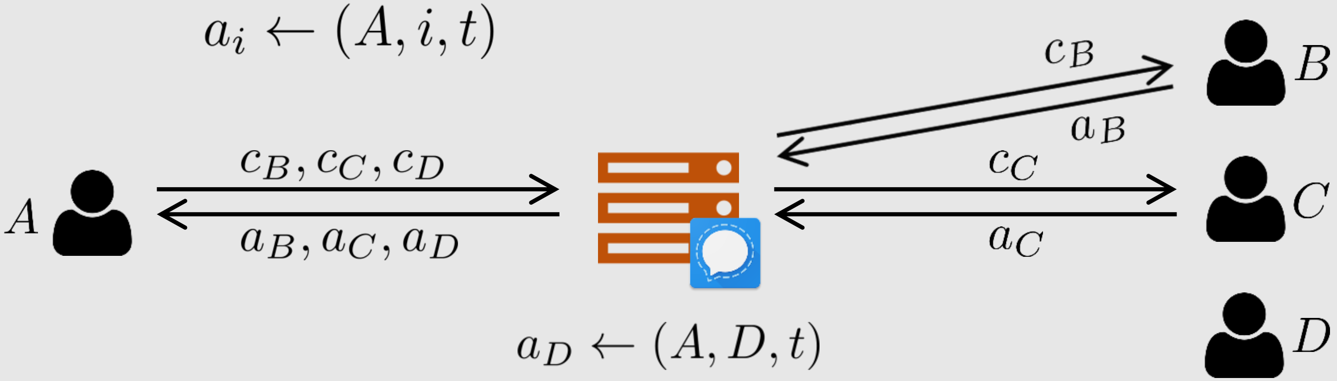
- Forward and future secure key streams of *direct* communication
- Group ID as proof of membership

Weaknesses: Signal

- Ciphertexts c (ID static)
- Acks a (plain)
- Group update as message m

$\forall i \in G \setminus \{A\}$:
$c_i \leftarrow \mathrm{E}_A(i; ID_G, t, m)$
$a_i \leftarrow (A, i, t)$

$G = \{A, B, C, D\}$



$a_D \leftarrow (A, D, t)$

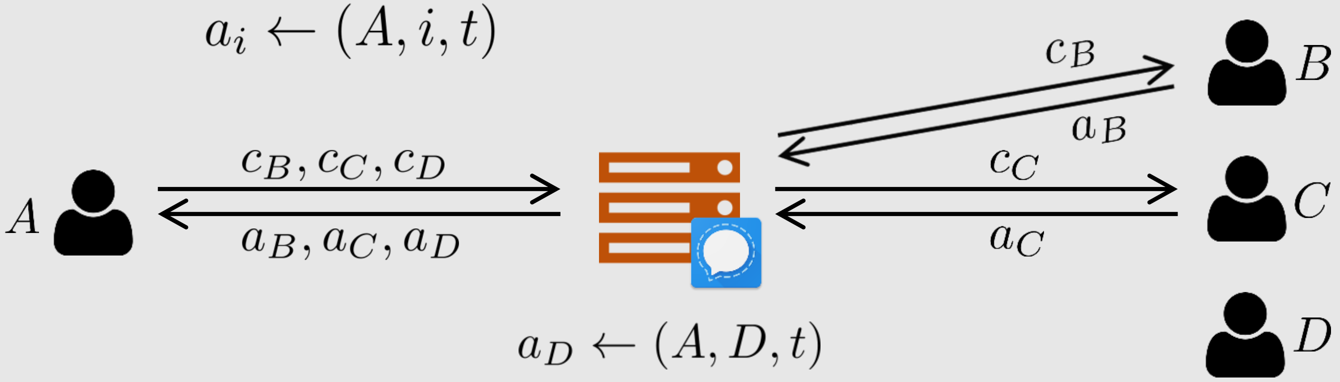
- Forward and future secure key streams of *direct* communication
- Group ID as proof of membership

Weaknesses: Signal

- Ciphertexts c (ID static)
- Acks a (plain)
- Group update as message m

$$\forall i \in G \setminus \{A\}:$$
$$c_i \leftarrow \mathrm{E}_A(i; ID_G, t, m)$$
$$a_i \leftarrow (A, i, t)$$

$$G = \{A, B, C, D\}$$



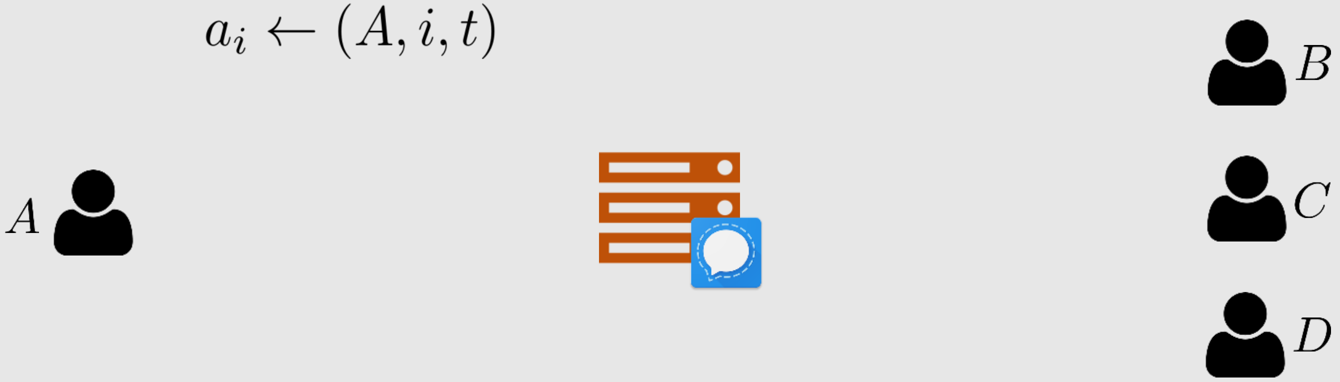
- Forward and future secure key streams of *direct* communication
- Group ID as proof of membership
- Traceable delivery by ack forgery *

Weaknesses: Signal

- Ciphertexts c (ID static)
- Acks a (plain)
- Group update as message m

$$\forall i \in G \setminus \{A\}:$$
$$c_i \leftarrow \mathrm{E}_A(i; ID_G, t, m)$$
$$a_i \leftarrow (A, i, t)$$

$$G = \{A, B, C, D\}$$



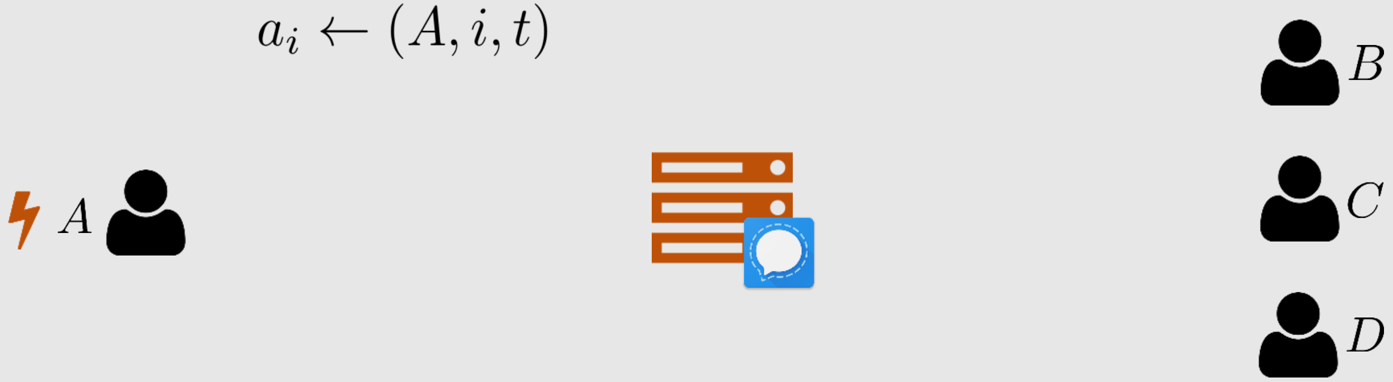
- Forward and future secure key streams of *direct* communication
- Group ID as proof of membership
- Traceable delivery by ack forgery *

Weaknesses: Signal

- Ciphertexts c (ID static)
- Acks a (plain)
- Group update as message m

$$\forall i \in G \setminus \{A\}:$$
$$c_i \leftarrow \mathrm{E}_A(i; ID_G, t, m)$$
$$a_i \leftarrow (A, i, t)$$

$$G = \{A, B, C, D\}$$



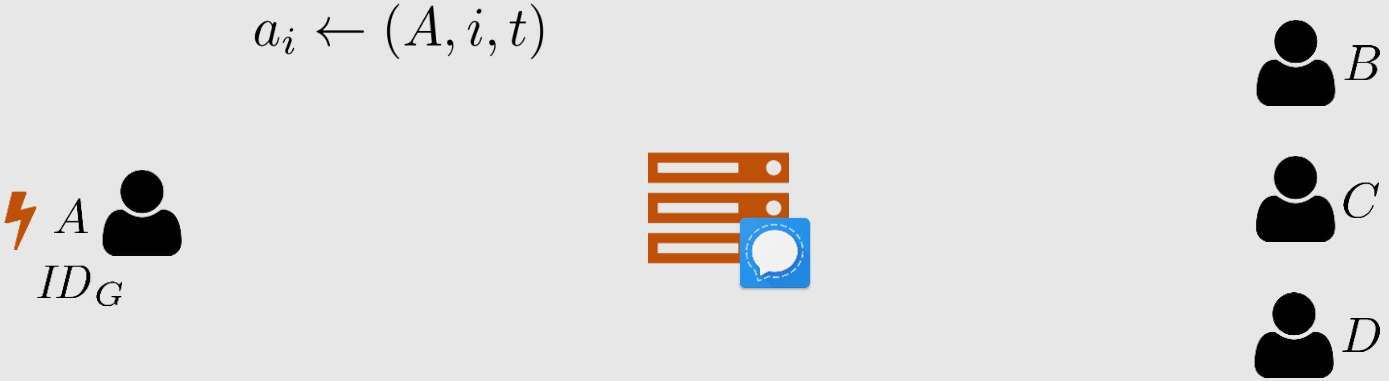
- Forward and future secure key streams of *direct* communication
- Group ID as proof of membership
- Traceable delivery by ack forgery *

Weaknesses: Signal

- Ciphertexts c (ID static)
- Acks a (plain)
- Group update as message m

$\forall i \in G \setminus \{A\}$:
$c_i \leftarrow \mathrm{E}_A(i; ID_G, t, m)$
$a_i \leftarrow (A, i, t)$

$G = \{A, B, C, D\}$



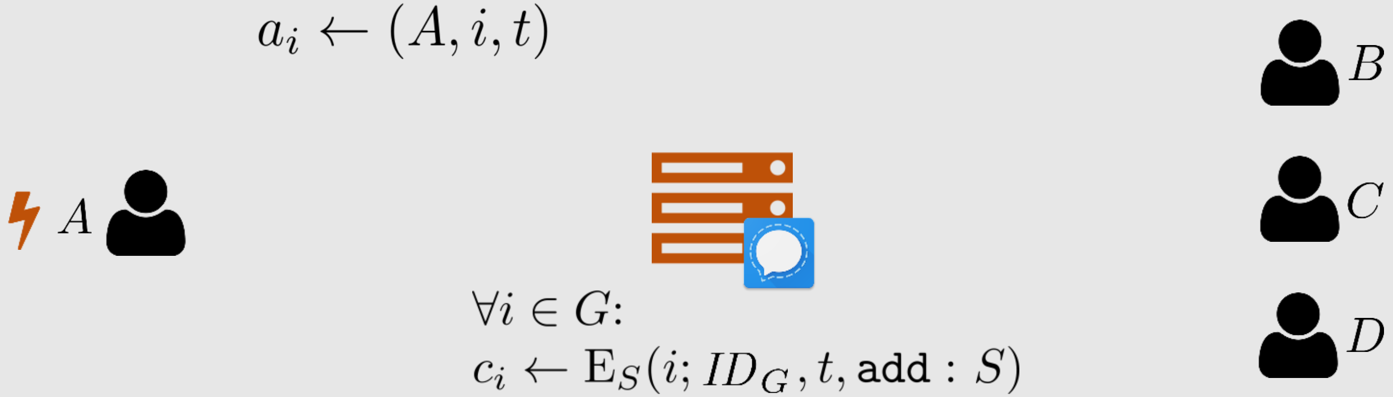
- Forward and future secure key streams of *direct* communication
- Group ID as proof of membership
- Traceable delivery by ack forgery *

Weaknesses: Signal

- Ciphertexts c (ID static)
- Acks a (plain)
- Group update as message m

$\forall i \in G \setminus \{A\}$:
$c_i \leftarrow \mathrm{E}_A(i; ID_G, t, m)$
$a_i \leftarrow (A, i, t)$

$G = \{A, B, C, D\}$

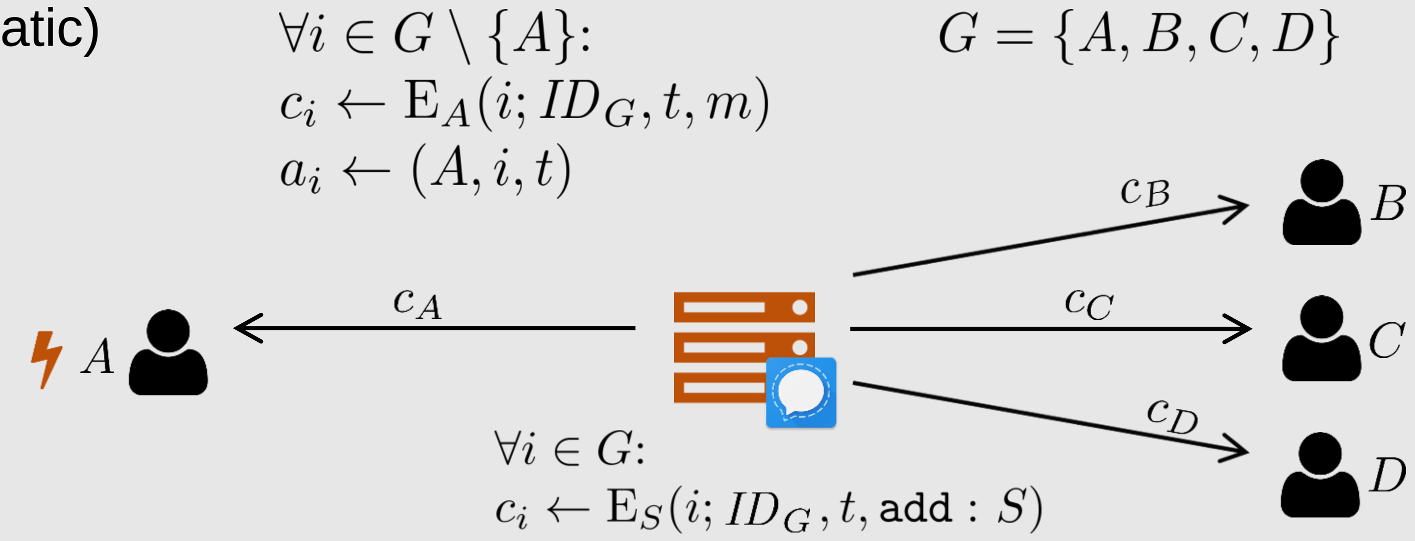


$\forall i \in G$:
$c_i \leftarrow \mathrm{E}_S(i; ID_G, t, \texttt{add}: S)$

- Forward and future secure key streams of *direct* communication
- Group ID as proof of membership
- Traceable delivery by ack forgery *

Weaknesses: Signal

- Ciphertexts c (ID static)
- Acks a (plain)
- Group update as message m


$\forall i \in G \setminus \{A\}$:
$c_i \leftarrow \mathrm{E}_A(i; ID_G, t, m)$
$a_i \leftarrow (A, i, t)$
$G = \{A, B, C, D\}$
c_B
B
c_A
A
c_C
C
c_D
D
$\forall i \in G$:
$c_i \leftarrow \mathrm{E}_S(i; ID_G, t, \mathtt{add} : S)$

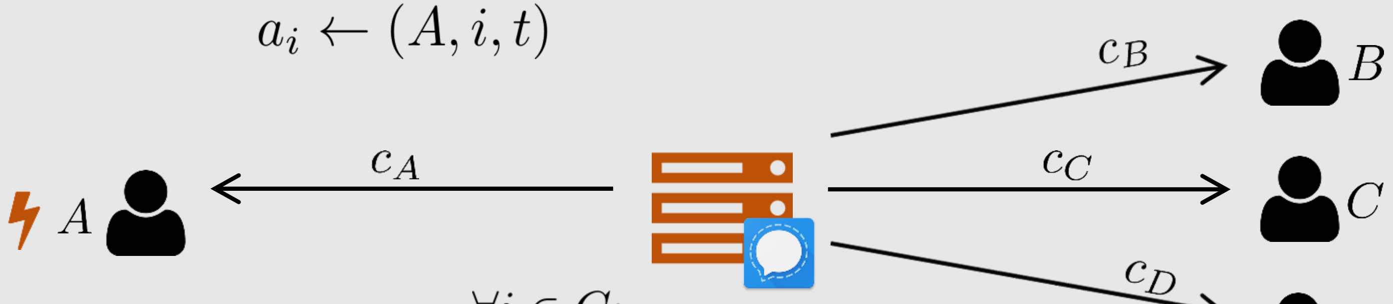
- Forward and future secure key streams of *direct* communication
- Group ID as proof of membership
- Traceable delivery by ack forgery *

Weaknesses: Signal

- Ciphertexts c (ID static)
- Acks a (plain)
- Group update as message m

$\forall i \in G \setminus \{A\}$:
$c_i \leftarrow \mathrm{E}_A(i; ID_G, t, m)$
$a_i \leftarrow (A, i, t)$

$G = \{A, B, C, D\}$



$\forall i \in G$:
$c_i \leftarrow \mathrm{E}_S(i; ID_G, t, \mathsf{add}: S)$

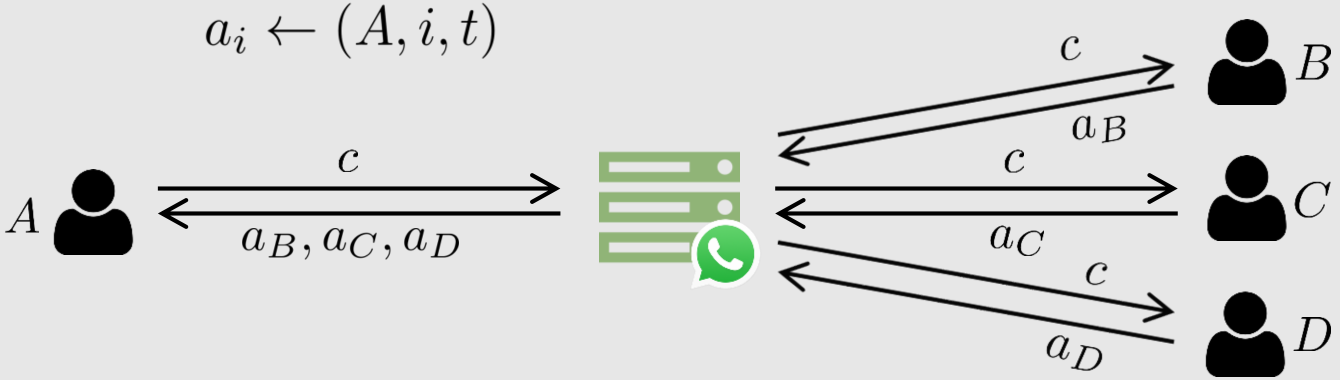
- Forward and future secure key streams of *direct* communication
- Group ID as proof of membership
- 🗄 Traceable delivery by ack forgery *
- ⚡ Closeness by using compromised group ID

Protocol Overview: WhatsApp

$$\begin{aligned} &\forall i \in G \setminus \{A\}: \\ &c \leftarrow \mathrm{E}_A(\mathbf{G}; m), t \\ &a_i \leftarrow (A, i, t) \end{aligned}$$

$$G = \{A, B, C, D\}$$

- **Group updates plain via server**



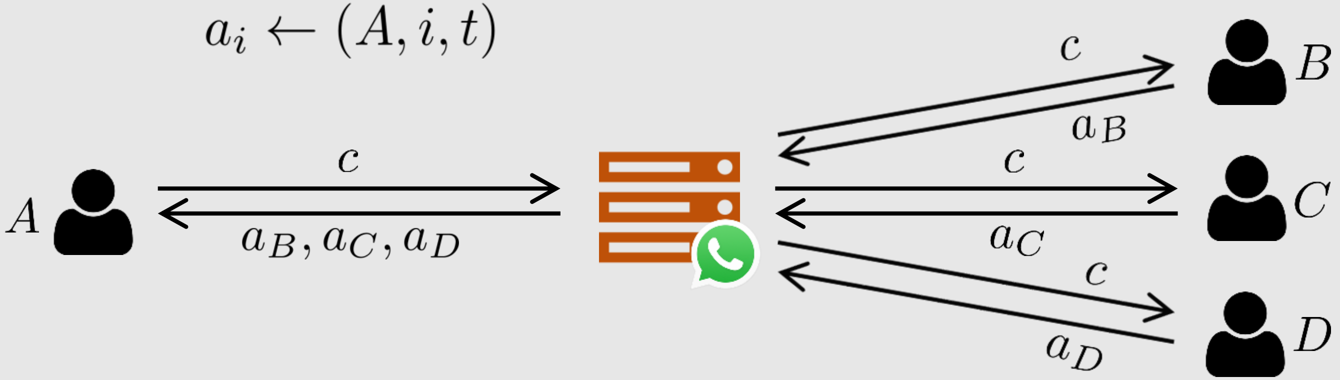
- Forward secure key streams for each group (and sender)

Weaknesses: WhatsApp

$$\forall i \in G \setminus \{A\}:$$
$$c \leftarrow \mathrm{E}_A(\mathbf{G}; m), t$$
$$a_i \leftarrow (A, i, t)$$

$$G = \{A, B, C, D\}$$

- **Group updates plain via server**



- Forward secure key streams for each group (and sender)

- Traceable delivery by ack forgery *
- Closeness by group update forgery

Problems & Solutions: Traceable Delivery

- Acks are not authenticated

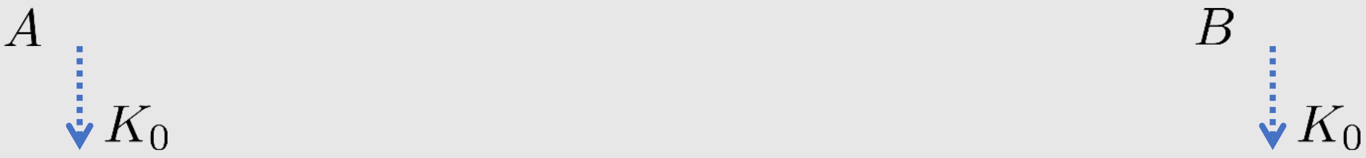
  → Explicit authentication by delivering as content message (AE) or signing

Problems & Solutions: Traceable Delivery

- Acks are not authenticated

  → Explicit authentication by delivering as content message (AE) or signing

- * For Signal and WhatsApp with key stream (stateful encryption):
  - Key omissions in key stream are ignored

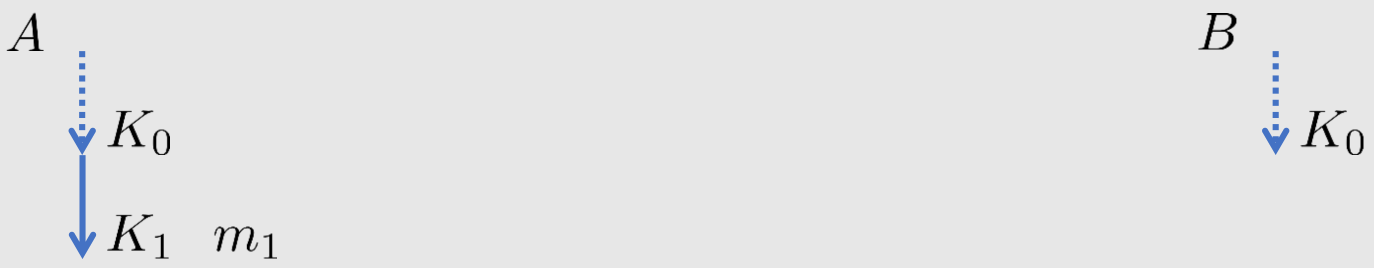


Problems & Solutions: Traceable Delivery

- Acks are not authenticated

  → Explicit authentication by delivering as content message (AE) or signing

- * For Signal and WhatsApp with key stream (stateful encryption):
  - Key omissions in key stream are ignored

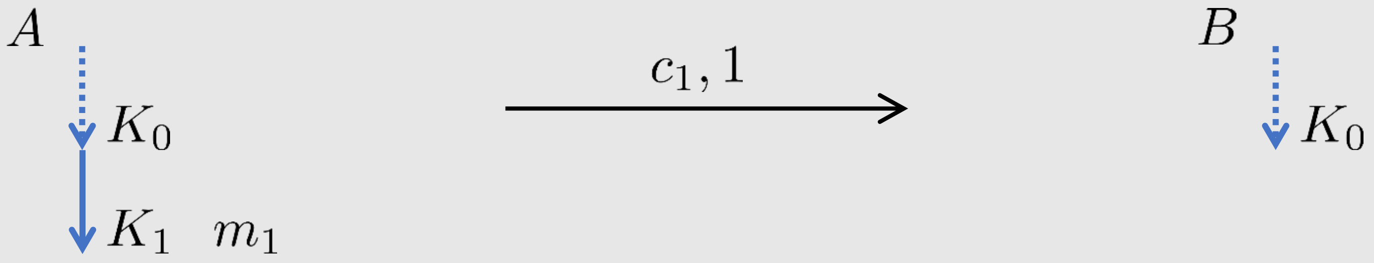


Problems & Solutions: Traceable Delivery

- Acks are not authenticated

  → Explicit authentication by delivering as content message (AE) or signing

- * For Signal and WhatsApp with key stream (stateful encryption):
  - Key omissions in key stream are ignored

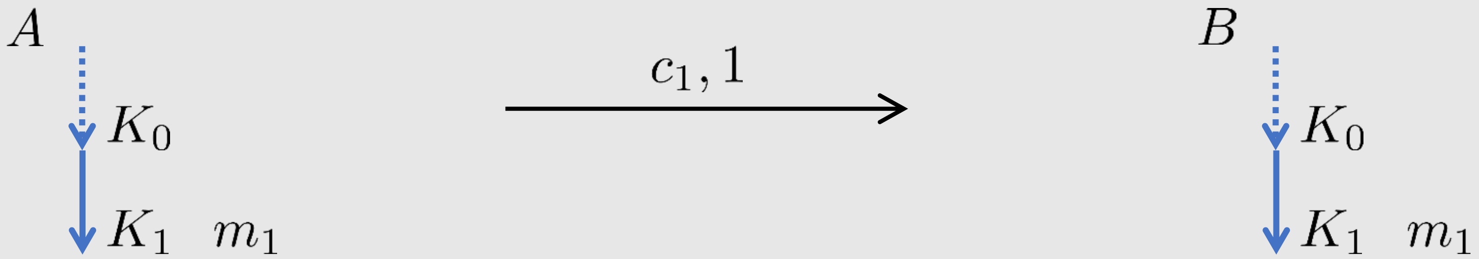


Problems & Solutions: Traceable Delivery

- Acks are not authenticated

  → Explicit authentication by delivering as content message (AE) or signing

- * For Signal and WhatsApp with key stream (stateful encryption):
  - Key omissions in key stream are ignored

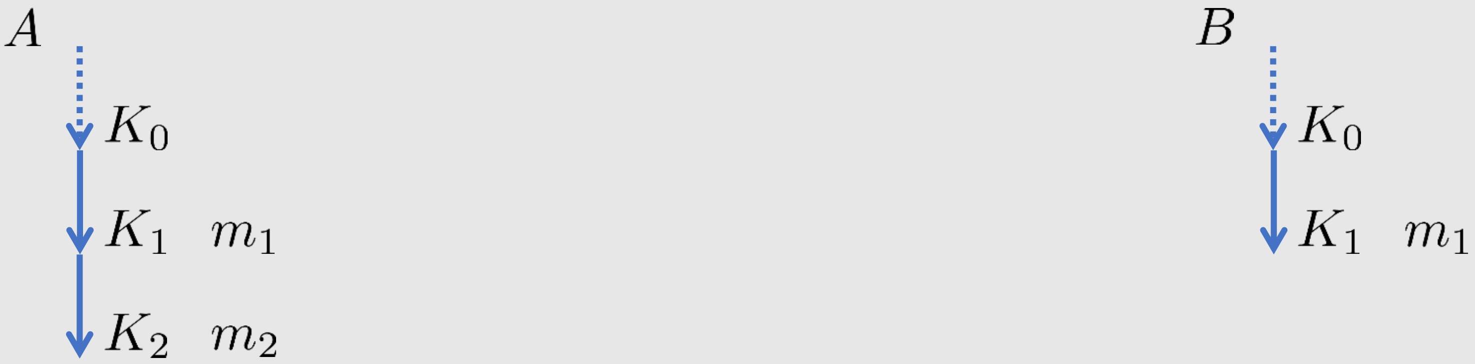


Problems & Solutions: Traceable Delivery

- Acks are not authenticated

  → Explicit authentication by delivering as content message (AE) or signing

- * For Signal and WhatsApp with key stream (stateful encryption):
  - Key omissions in key stream are ignored

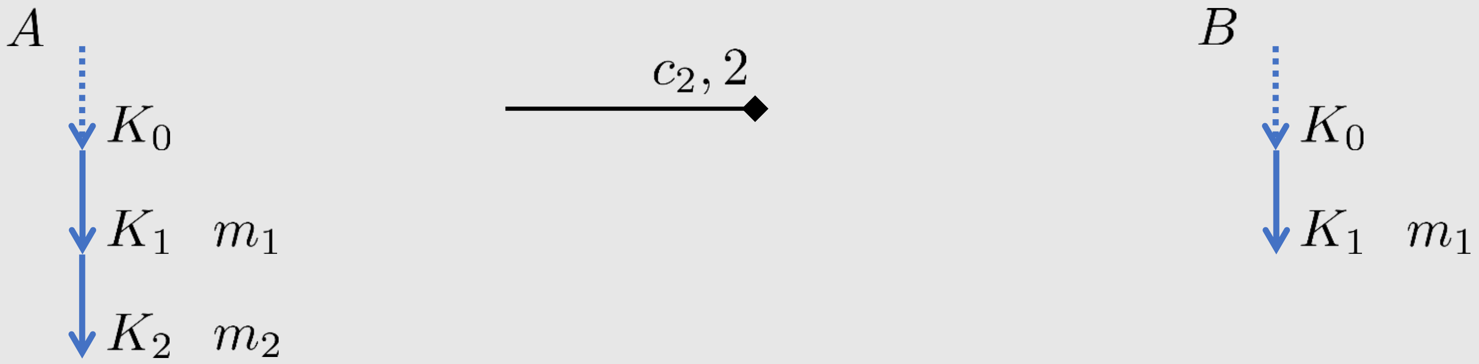


Problems & Solutions: Traceable Delivery

- Acks are not authenticated

  → Explicit authentication by delivering as content message (AE) or signing

- * For Signal and WhatsApp with key stream (stateful encryption):
  - Key omissions in key stream are ignored

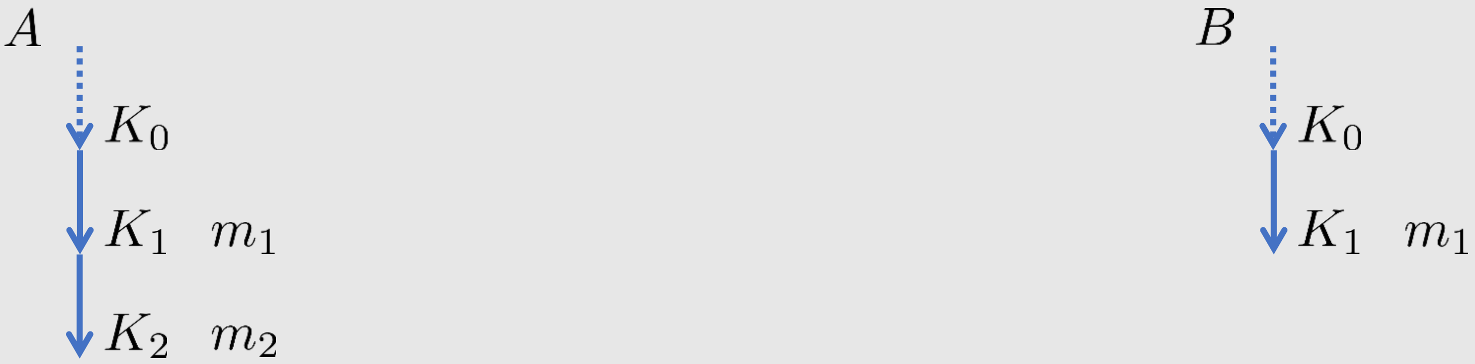


Problems & Solutions: Traceable Delivery

- Acks are not authenticated

  → Explicit authentication by delivering as content message (AE) or signing

- * For Signal and WhatsApp with key stream (stateful encryption):
  - Key omissions in key stream are ignored

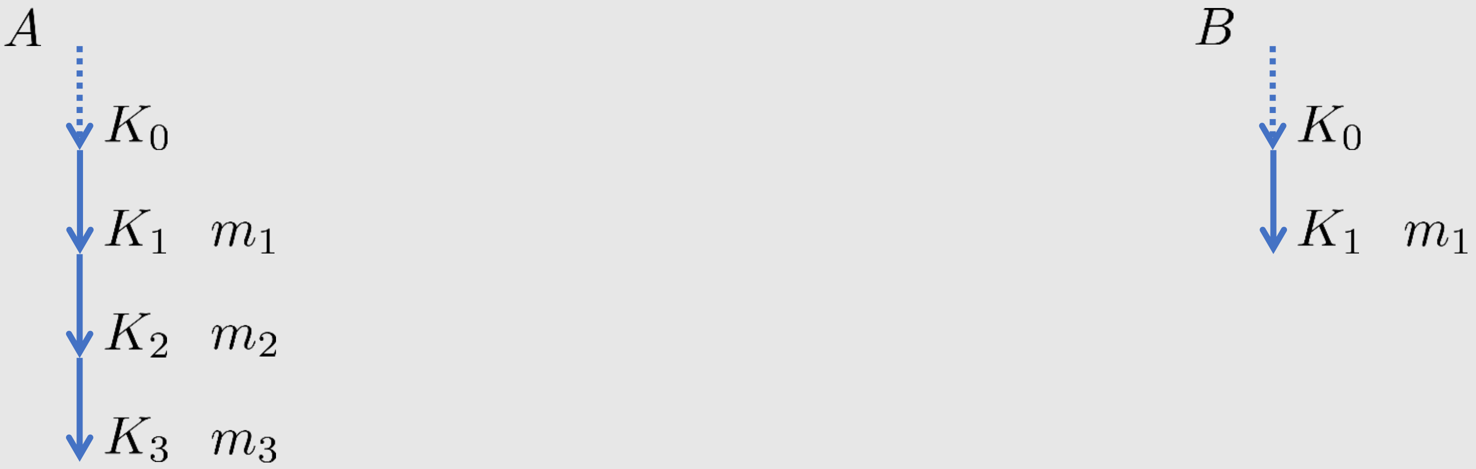


Problems & Solutions: Traceable Delivery

- Acks are not authenticated

  → Explicit authentication by delivering as content message (AE) or signing

- * For Signal and WhatsApp with key stream (stateful encryption):
  - Key omissions in key stream are ignored

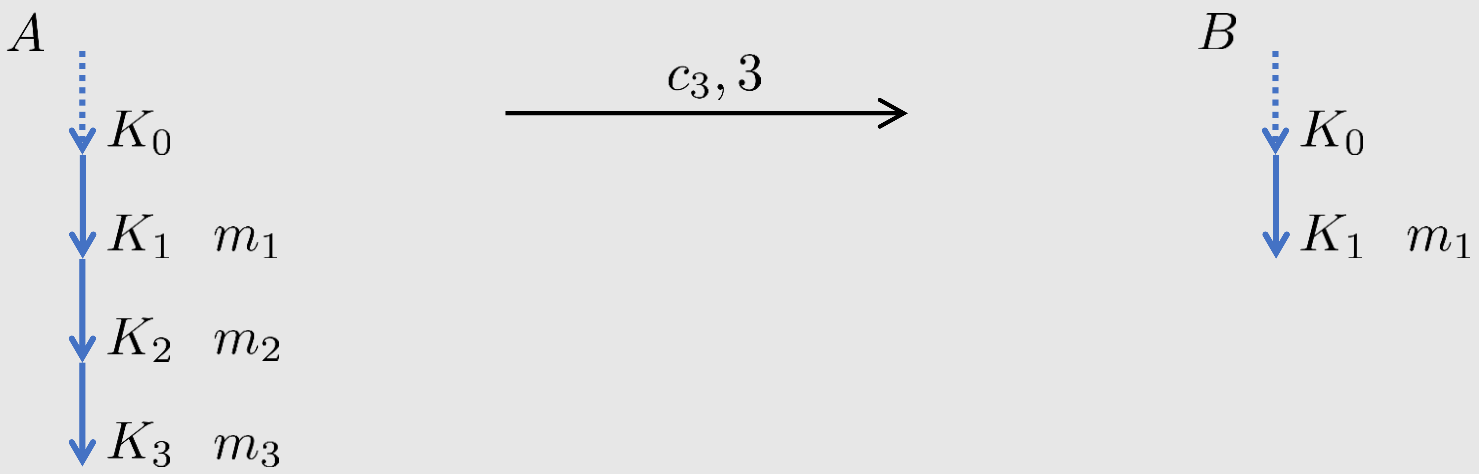


Problems & Solutions: Traceable Delivery

- Acks are not authenticated

  → Explicit authentication by delivering as content message (AE) or signing

- * For Signal and WhatsApp with key stream (stateful encryption):
  - Key omissions in key stream are ignored

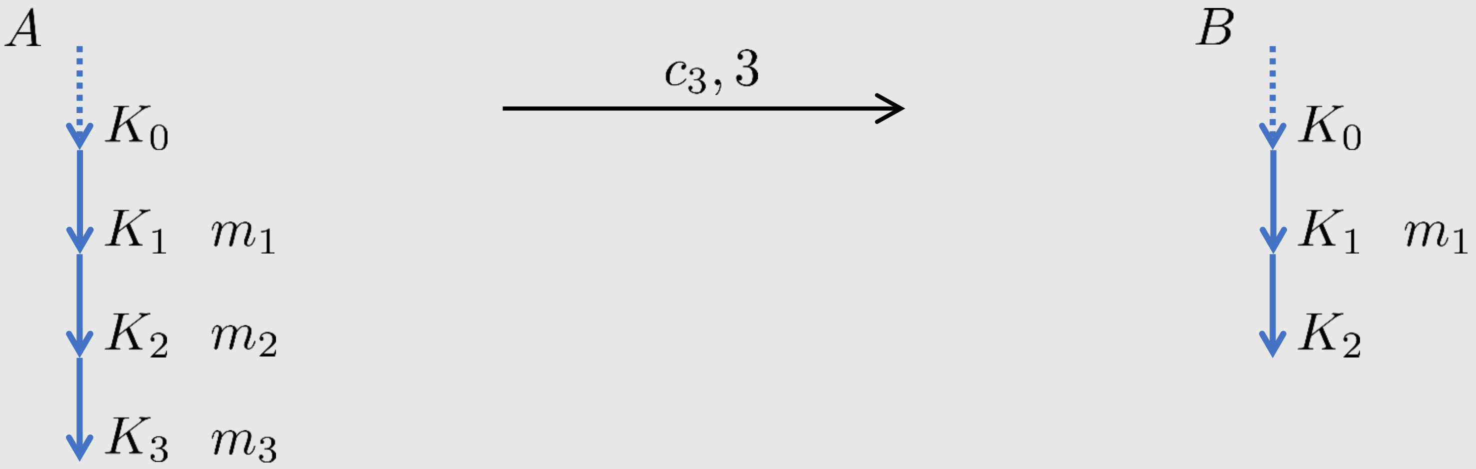


Problems & Solutions: Traceable Delivery

- Acks are not authenticated

  → Explicit authentication by delivering as content message (AE) or signing

- * For Signal and WhatsApp with key stream (stateful encryption):
  - Key omissions in key stream are ignored

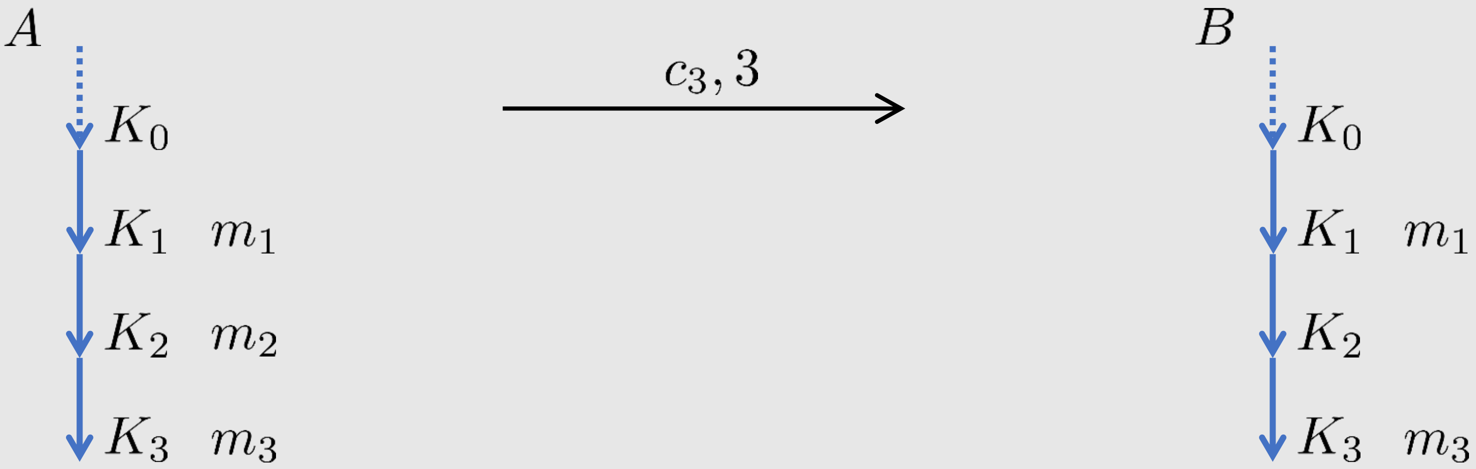


Problems & Solutions: Traceable Delivery

- Acks are not authenticated

  → Explicit authentication by delivering as content message (AE) or signing

- * For Signal and WhatsApp with key stream (stateful encryption):
  - Key omissions in key stream are ignored



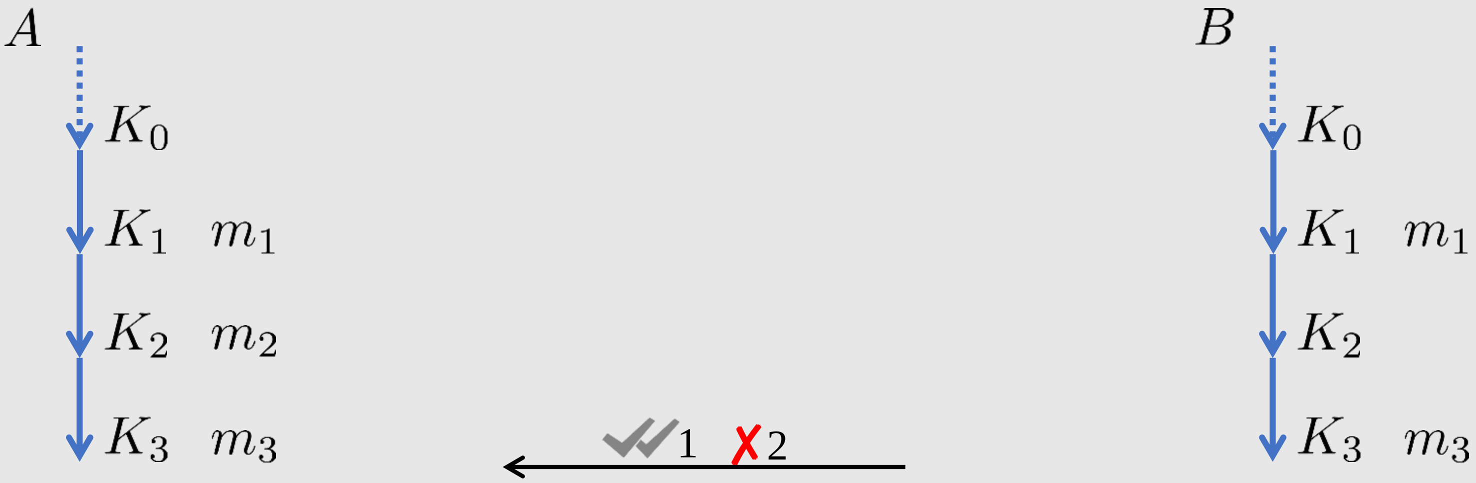
Problems & Solutions: Traceable Delivery

- Acks are not authenticated

  → Explicit authentication by delivering as content message (AE) or signing

- * For Signal and WhatsApp with key stream (stateful encryption):
  - Key omissions in key stream are ignored

  → Ack newest in order received message (e.g., with content messages)
  → Send negative ack (NACK) on key omission



Problems …: Closeness

Receiving according to …

- Guest list approach
  - WhatsApp: updates sent plain
- Ticket approach
  - Signal: updates accepted if group ID in message

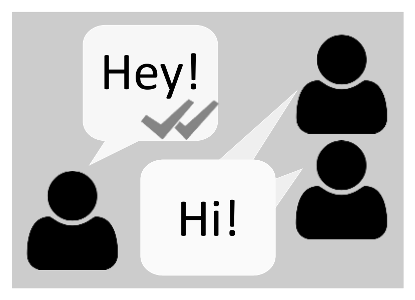
Problems …: Closeness

Receiving according to …

- Guest list approach
  - WhatsApp: updates sent plain
    - Manipulable by server
- Ticket approach
  - Signal: updates accepted if group ID in message
    - Static group ID ⇒ not (future) secure against compromising attacker

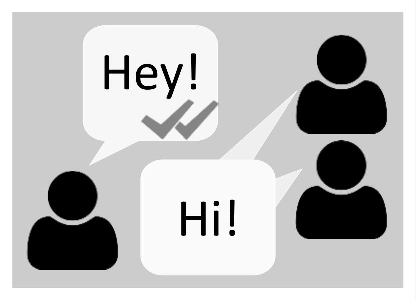
… and Solutions: Closeness

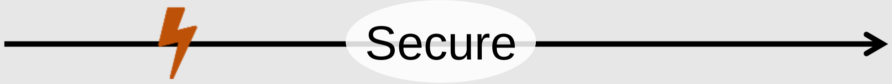
- Guest list approach
  - Authentic update messages
  - Causality [MarPoe ePrint ‘17]
    - Not desired: “*reordered, delayed, or lost in normal operation*” (Moxie Marlinspike)
  - At least traceable delivery
- Ticket approach



… and Solutions: Closeness

- Guest list approach
  - Authentic update messages
  - Causality [MarPoe ePrint ‘17]
    - Not desired: “*reordered, delayed, or lost in normal operation*” (Moxie Marlinspike)
  - At least traceable delivery
- Ticket approach
  - At least traceable delivery
  - Future secrecy also for group secret (in addition to pairwise channels)
    - Group key exchange: [KimPerTsu TISSEC ’04], [CCGMM ePrint ‘17]





Summary

- First security model for group instant messaging
  - Captures security and *reliability*
- Description (⇒ 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**