

# Consequences of Complexity in Group Instant Messaging using the Example of WhatsApp and Signal

RuhrSec 2018

**2018-05-18**

**Horst Görtz Institute for IT Security**

Chair for Network and Data Security

**Paul Rösler**, Christian Mainka, Jörg Schwenk

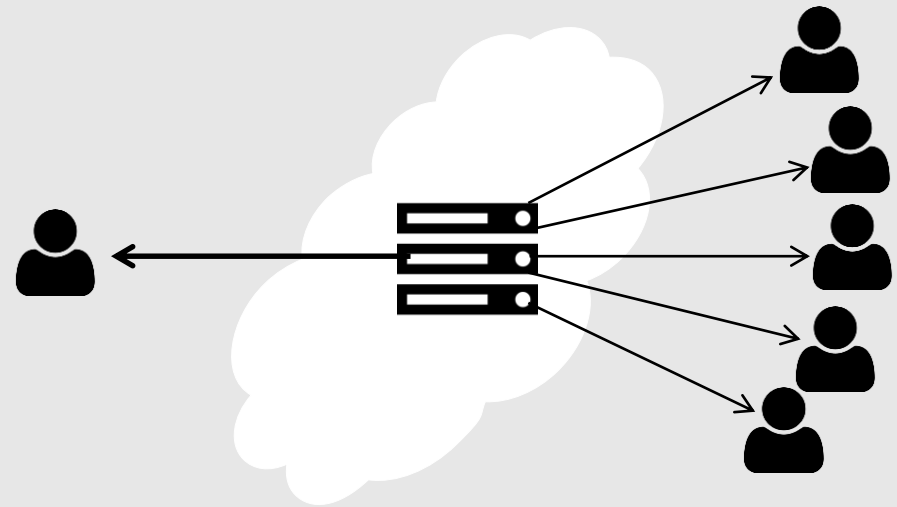
# Secure Group Instant Messaging: End-to-End

- Dynamic group of users



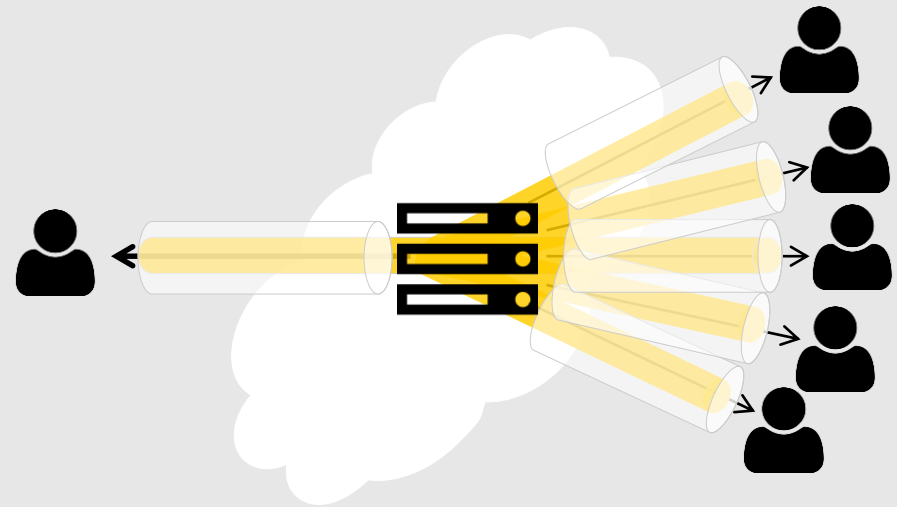
# Secure Group Instant Messaging: End-to-End

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



# Secure Group Instant Messaging: End-to-End

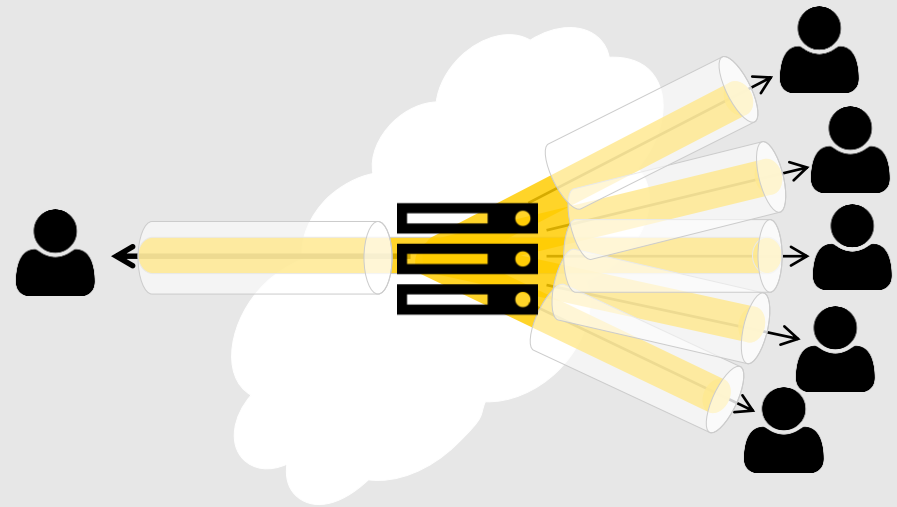
- Dynamic group of users
- One central server (always online)
- End-to-end protection within protected transport layer
- Server potentially malicious



# 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

# History of our Work

## More is Less: How Group Chats Weaken the Security of Instant Messengers Signal, WhatsApp, and Threema

Paul Rösler, Christian Mainka, Jörg Schwenk  
{firstname.lastname}@rub.de  
Chair for Network and Data Security  
Ruhr-University Bochum

July 24, 2017

### Abstract

Secure Instant Messaging (SIM) is utilized in two variants: one-to-one communication and group communication. While the first variant has received much attention lately (Frosch et al., EuroS&P16; Cohn-Gordon et al., EuroS&P17; Kobeissi et al., EuroS&P17), little is known about the cryptographic mechanisms and security guarantees of SIM group communication.

In this paper, we investigate group communication security mechanisms of three main SIM applications: Signal, WhatsApp, and Threema. We first provide a comprehensive and realistic attacker model for analyzing group SIM protocols regarding security and reliability. We then describe and analyze the group protocols used in Signal, WhatsApp, and Threema. By applying our model, we reveal multiple weaknesses, and propose generic countermeasures to enhance the protocols regarding the required security and reliability goals. Our systematic analysis reveals that (1) the *communications' integrity* – represented by the integrity of all exchanged messages – and (2) the *groups' closeness* – represented by the members' ability of managing the group – are not end-to-end protected.

We additionally show that strong security properties, such as Future Secrecy which is a core part of the one-to-one communication in the Signal protocol, do not hold for its group communication.

# History of our Work

## Real World Crypto 2018

### Program

All going well with technology we plan to live stream the event, and keep a permanent record of talks at the RWC YouTube channel

<https://www.youtube.com/c/RealWorldCrypto>

Wednesday Jan. 10, 2018	
Session 5: Usability and privacy <span>session chair: Ian Goldberg</span>	
3:45pm	<b>Comparing the usability of cryptographic APIs</b> <i>Yasemin Acar (Leibniz University Hannover)</i>
4:15pm	<b>Is Certificate Transparency usable?</b> <i>Emily Stark (Google)</i>
4:45pm	<b>On the end-to-end security of group chats</b> <i>Paul Rösler (U. Bochum), Christian Mainka (U. Bochum), Jörg Schwenk (U. Bochum)</i>
5:10pm	<b>Privacy-preserving search of similar patients in genomic data</b> <i>Gilad Asharov (Cornell Tech), Shai Halevi (IBM), Yehuda Lindell (Bar-Ilan University), Tal Rabin (IBM)</i>
5:35pm	<b>End of day one</b>
5:45pm	<b>Reception</b>



# History of our Work

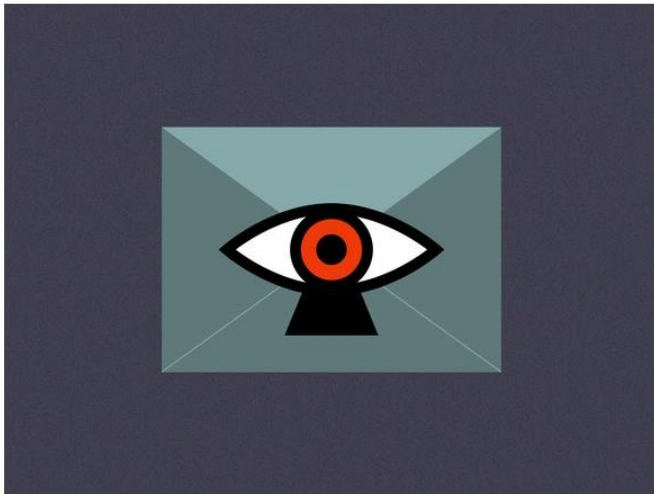


# History of our Work

**WIRED** WhatsApp Security Flaws Could Allow Snoops to Slide Into Group Chats

ANDY GREENBERG SECURITY 01.10.18 07:00 AM

## WHATSAPP SECURITY FLAWS COULD ALLOW SNOOPS TO SLIDE INTO GROUP CHATS



Millions of people trust WhatsApp's end-to-end encryption. But security researchers say a flaw could put some group chats at risk of infiltration. [HOTLITTLEPOTATO](#)

When WhatsApp added end-to-end encryption to every conversation for its billion users two years ago, the mobile messaging giant significantly raised the bar for the privacy of digital communications worldwide. But one of the tricky



## A Few Thoughts on Cryptographic Eng

*Some random thoughts about crypto. Notes from a course I teach. Pictures of my dachshund*

Matthew Green in attacks, messaging January 10, 2018 1,984 Words

## Attack of the Week: Group Messaging in WhatsApp and Signal

If you've read this blog before, you know that secure messaging is one of my favorite topics. However, recently I've been a bit disappointed. My sadness comes from the fact that lately these systems have been getting *too damned good*. That is, I was starting to believe that most of the interesting problems had finally been solved.

If nothing else, today's post helped disabuse me of that notion.

This result comes from a new paper by Rösler, Mainka and Schwenk from Ruhr-



Matthew Green

I'm a cryptographer and professor at Johns Hopkins University. I've designed and analyzed cryptographic systems used in wireless networks, payment systems and digital content protection platforms. In my research I look at the various ways cryptography can be used



# History of our Work

**SPIEGEL ONLINE** DER SPIEGEL SPIEGEL TV 🔍 Anmelden

☰ Menü | Politik | Meinung | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | mehr▼

**NETZWELT** Schlagzeilen | Wetter | DAX 13.231,42 | TV-Programm | Abo

Nachrichten > Netzwelt > Apps > WhatsApp > WhatsApp-Gruppenchats: Schwachstelle im Verschlüsselungs-Protokoll

**WhatsApp**  
**Schwachstelle in Verschlüsselung von Gruppenchats**

Deutscher Forscher haben eine Sicherheitslücke in WhatsApp entdeckt, mit der sich die Ende-zu-Ende-Verschlüsselung von Gruppenchats aushebeln ließe. WhatsApp-Mutter Facebook hält das Angriffsszenario für unrealistisch.

 Von Patrick Beuth ▼



WhatsApp-Messenger DPA

# History of our Work

**SPIEGEL ONLINE** DER SPIEGEL SPIEGEL TV

Menü | Politik Meinung Wirtschaft Panorama Sport Kultur Netzwelt Wissenschaft mehr▼

**NETZWELT**

Nachrichten > Netzwelt >

**Handelsblatt**

amm | Abo

FINANZEN UNTERNEHMEN POLITIK **TECHNIK** SPORT VIDEO AUTO PA

IT + Internet Gadgets Forschung + Innovation ▼ Medizin Ene

**WhatsApp Schwach!**

**Deutscher Forscher**

**Verschlüsselung von Gruppenchats**

**für unrealistisch.**

Handelsblatt > Technik > IT + Internet > Facebook-Tochter: Deutsche Forscher finden Sicherheitslücke bei WhatsApp

**Ende-sszenario**

**VERSCHLÜSSELUNG UMGANGEN**

Von Patrick

**Forscher finden Sicherheitslücke bei WhatsApp**

von: Johannes Steger  
 Datum: 11.01.2018 14:11 Uhr

Forscher haben herausgefunden, wie die Verschlüsselung bei Gruppenchats theoretisch umgangen werden kann und heimlich neue Mitglieder beitreten könnten. Das Problem ließe sich einfach beheben.

f Facebook t Twitter g+ Google+ x Xing in LinkedIn

0  
3



WhatsApp-Messenger

# History of our Work

**SPIEGEL ONLINE** DER SPIEGEL SPIEGEL TV Suche Anmelden

Menü | Politik | Meinung | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | mehr▼

**NETZWELT** Handelsblatt amm | Abo

Nachrichten > Netzwelt >

**WhatsApp Schwachstelle** IT + In

Deutscher Forschung: Verschlüsselung von Gruppenchats für unrealistisch.

Von Patrick Forscher finden Schwachstelle bei WhatsApp

von: Johannes Steger  
Datum: 11.01.2018 14:11 Uhr

Forscher haben herausgefunden, dass Gruppenchats theoretisch umgangen werden können, wenn neue Mitglieder beitreten könnten. Das ist ein Problem, das bisher unbeachtet blieb.

**VERSCHLÜSSELUNG UMGANGEN**

**Security researchers flag invite bug in WhatsApp group chats**

Posted yesterday by [Natasha Lomas \(@riptari\)](#)

encryption  
computer security  
vulnerability  
WhatsApp  
Europe

**Popular Posts**

- The quantum computing apocalypse is imminent
- Google shuts down its CES booth because it's not waterproof
- Nvidia CEO clarifies its GPUs are 'absolutely' immune to Meltdown and ...
- Confide makes its iOS messaging app

**Crunchbase**

**WhatsApp**

FOUNDED 2009

**OVERVIEW**

WhatsApp Messenger is a cross-platform mobile messaging app which allows you to exchange messages without having to pay for SMS. WhatsApp Messenger is available for iPhone, [BlackBerry] (/organization/blackberry), Android, Windows Phone and [Nokia] (/organization/nokia) and yes, those phones can all message each other! Because WhatsApp Messenger uses the same internet data plan that you use for email ...

**LOCATION**

Santa Clara, California

**CATEGORIES**

Subscription Service, Android, Messaging, Mobile

**FOUNDERS**

Brian Acton, Jan Koum

**WhatsApp-Messenger**



# History of our Work

**SPIEGEL ONLINE** DER SPIEGEL SPIEGEL TV Suche Anmelden

Menü | Politik | Meinung | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | mehr▼

**NETZWELT**

Nachrichten > Netzwelt >

**Handelsblatt** amm | Abo

FINANZEN | UNTERNEHMEN | POLITIK | **TECHNIK** | SPORT | VIDEO | AUTO | PA

IT + In

Got a tip? **Let us know.**

News ▾ Video ▾ Events ▾

**WhatsApp Schwachstelle bei Verschlüsselung von Gruppenchats**

Deutscher Forscher: Verschlüsselung von Gruppenchats ist für unrealistisch.

Von Patrick

Forscher finden Schwachstelle bei WhatsApp

von: Johannes Steger  
Datum: 11.01.2018 14:11 Uhr

Forscher haben herausgefunden, dass Gruppenchats theoretisch umgangen werden können, wenn neue Mitglieder beitreten könnten. Das behebene.

Facebook Twitter Google+

WhatsApp-Messenger

**TC WINTER**

encryption  
computer security  
vulnerability  
WhatsApp  
Europe

**Security research in group chats**

Posted yesterday by Natas

Popular Posts

The quantum computing apocalypse is imminent

Google shuts down its CES booth because it's not waterproof

Nvidia CEO clarifies its GPUs are 'absolutely' immune to Meltdown and ...

Confide makes its iOS messaging app

**Süddeutsche Zeitung**  
SZ.de Zeitung Magazin

Wirtschaft | Panorama | Sport | München | Bayern | Kultur | Gesellschaft | Wissen | Digital | Karriere | Reisen

IT-Sicherheit > Ungebetene Gäste in Whatsapp-Gruppenchats

11. Januar 2018, 15:08 Uhr IT-Sicherheit

**Wie Fremde sich in Whatsapp-Gruppenchats einladen können**

**WhatsApp group**

cross-platform mobile messaging app that lets you to exchange messages and pay for SMS. WhatsApp is available on iPhone, [BlackBerry] Android, Windows Phone (Nokia) and yes, those who use other! Because the same internet data

- Deutsche Forscher haben eine Schwachstelle im Messenger WhatsApp entdeckt.
- Ein Angreifer, der den Server von WhatsApp kontrolliert, kann ein neues Mitglied in einen Gruppenchat einschleusen.
- Es gibt sehr hohe Hürden. Ein Angriff wäre nur für versierte Profis oder Regierungen möglich.

id, Messaging, Mobile

# History of our Work

**SPIEGEL ONLINE** DER SPIEGEL SPIEGEL TV

Menü | Politik | Meinung | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | mehr▼

**NETZWELT**

Nachrichten > Netzwelt >

**WhatsApp Schwachstelle**

Deutscher Forscher: Verschlüsselung von Gruppenchats für unrealistisch.

Von Patrick

**Forscher finden Schwachstelle bei WhatsApp**

von: Johannes Steger  
Datum: 11.01.2018 14:11 Uhr

Forscher haben herausgefunden, dass Gruppenchats theoretisch umgangen werden können, wenn neue Mitglieder beitreten könnten. Dies könnte zu Sicherheitsproblemen führen.

VERSCHLÜSSELUNG UMGANGEN

TC WINTER

Got a tip? Let us know.

News Video Events

encryption  
computer security  
vulnerability  
WhatsApp  
Europe

Popular Posts

The quantum computing apocalypse is imminent

Google shuts down its CES booth because it's not waterproof

Nvidia CEO clarifies its GPUs are 'absolutely' immune to Meltdown and ...

Confide makes its iOS messaging app

**The Telegraph** HOME NEWS

**Technology**

News | Reviews | Opinion | Internet security | Social media | Apple | Google | New

Technology

**WhatsApp 'bug' raises questions over group message privacy**

11. Januar 2018, 15:08 Uhr IT-Sicherheit

**Wie Fremde sich in WhatsApp Gruppenchats einmischen könnten**

WhatsApp is a popular messaging service. CREDIT: REUTERS

By Margi Murphy  
10 JANUARY 2018 • 5:39PM

WhatsApp backdoor that could allow someone to plant moles into group conversations has been revealed by security researchers, raising questions over the security of users' conversations.

- Deutsche Forscher haben eine Schwachstelle entdeckt.
- Ein Angreifer, der den Server kontrolliert, könnte ein Mitglied in einen Gruppenchat einschleusen.
- Es gibt sehr hohe Hürden. Ein Angriff wäre nur für versierte Profis oder Regierungen möglich.

id, Messaging, Mobile

# History of our Work

From Paul Rösler★  
Subject **Re: WhatsApp / Artikel Welt.de**  
To [REDACTED]@welt.de★  
Enigmil Good signature from Paul Rösler (university) <paul.roesler@rub.de>  
Key ID: 0x9C6B3746 / Signed on: 11.01.18, 13:48

Hallo Herr W [REDACTED],

ich möchte der Mail voranstellen, dass ich einen gewissen negativen Respekt vor der Zusammenarbeit mit dem Axel-Springer Verlag habe. Es freut mich, dass sie darüber informieren möchten. Um aber zu verhindern, dass die Ergebnisse in einer reißerischen Überschrift aufgedreht werden möchte ich Sie ausdrücklich darum bitten, die Informationen sachlich zu verwenden. Bitte nehmen Sie das nicht als persönlichen Angriff auf.

On 11.01.2018 11:46, W [REDACTED] wrote:  
ich bin Redakteur der WELT und plane einen Artikel über das WhatsApp-Sicherheitsthema zu veröffentlichen. Hätten Sie Zeit mir bis morgen Mittag ein paar Fragen zu beantworten? Gerne auch telefonisch.

Ich bin bis Samstag in Zürich auf der RWC Konferenz. Das Programm geht heute bis kurz nach 5, sodass ich wahrscheinlich gegen halb 6 erreichbar wäre. Meine Handy Nr. ist +491 [REDACTED].

Und zwar geht es im Grunde um das Hauptproblem, was Sie und Ihre Mitarbeiter herausgefunden haben, was die größte Gefahr ist und die Reaktion von Facebook.

Um einen ersten Eindruck zu bekommen, sind der Wired Artikel und der Blog Post von Matthew Green sehr verständlich. Wir haben auch einen eigenen Blog Post geschrieben und wenn sie die Probleme vollständig



# History of our Work

From Paul Rösler★  
 Subject Re: WhatsApp / Artikel Welt.de  
 To [REDACTED]@welt.de★  
 Enigmil Good signature from Paul Rösler (university) <paul.roesler@rub.de>  
 Key ID: 0x9C6B3746 / Signed on: 11.01.18, 13:48

Hallo Herr W[REDACTED],

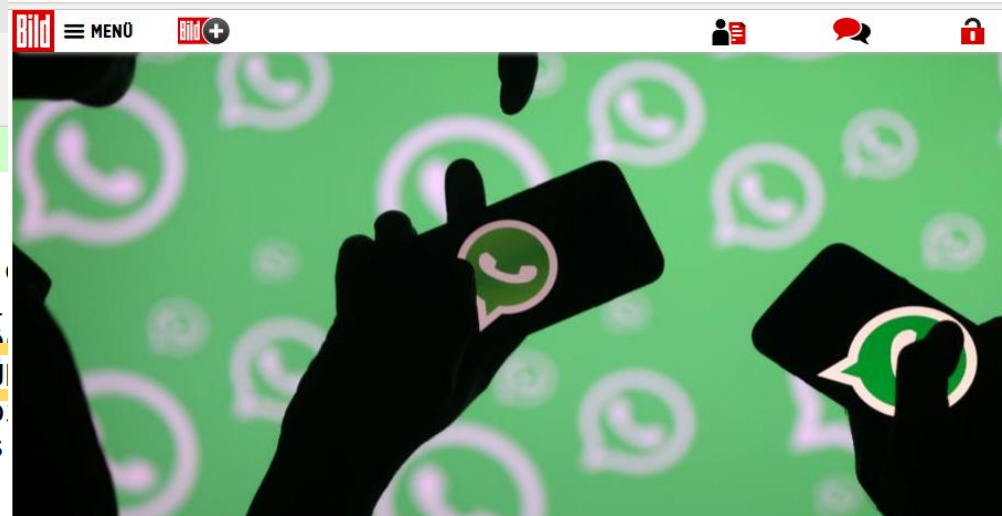
ich möchte der Mail voranstellen, dass ich Respekt vor der Zusammenarbeit mit dem Axel freut mich, dass sie darüber informieren mö dass die Ergebnisse in einer reißerischen Ü werden möchte ich Sie ausdrücklich darum b sachlich zu verwenden Bitte nehmen Sie das Angriff auf.

On 11.01.2018 11:46, W[REDACTED], Jan-Titus  
 ich bin Redakteur der WELT und plane einen WhatsApp-Sicherheitsthema zu veröffentlichen morgen Mittag ein paar Fragen zu beantworten

Ich bin bis Samstag in Zürich auf der RWC K heute bis kurz nach 5, sodass ich wahrscheinlich wäre. Meine Handy Nr. ist +491[REDACTED].

Und zwar geht es im Grunde um das Hauptpro Mitarbeiter herausgefunden haben, was die Reaktion von Facebook.

Um einen ersten Eindruck zu bekommen, sind Blog Post von Matthew Green sehr verständlich eigenen Blog Post geschrieben und wenn sie



Unbefugte könnten sich in WhatsApp-Gruppen einschleichen, mahnen Sicherheitsforscher  
 Foto: DADO RUVIC / Reuters



ANZEIGE

12.01.2018 - 10:07 Uhr

**Es ist eine Horror-Vorstellung: Fremde können sich in Gruppenchats bei WhatsApp schleichen, dort private Gespräche verfolgen und diese sogar manipulieren. Eine Sicherheitslücke macht dies theoretisch möglich, das haben Sicherheitsforscher aus Deutschland herausgefunden.**

Laut den Experten der Ruhr-Universität Bochum sind die Chats trotz Verschlüsselung angreifbar, wenn Hacker sich Zugriff auf die WhatsApp-Server verschaffen. Sie könnten dann Einladungen zu Gruppen-Chats fälschen und sich so in beliebige Chat-Gruppen einschleichen, ohne tatsächlich eine Einladung erhalten zu haben.

# History of our Work



**THE Sun** THE SUN, A NEWS UK COMPANY

SPORT TV & SHOWBIZ NEWS FABULOUS MONEY MOTORS TRAVEL

All Tech Science Phones & Gadgets Gaming

## WHO'S WATCHING? New WhatsApp bug could expose your group chat messages to hackers – we reveal how to stay safe

Researchers say WhatsApp users could be vulnerable to cyber-attack, as a new exploit reveals sneaky way of hacking your private group chats

By Sean Keach  
11th January 2018, 10:32 am | Updated: 11th January 2018, 2:32 pm

COMMENT NOW

PRIVATE messages sent by WhatsApp users could be exposed thanks to a new software bug.

Researchers have revealed how hackers could break into the popular messaging app and read your conversations.




**Bild** MENO



## Unbefugte könnten sich in WhatsApp-Gruppen einschleichen, mahnen Sicherheitsforscher

Foto: DADO RUVIC / Reuters

Teilen Twittern G+ Email Warnung

ANZEIGE

**12.01.2018 - 10:07 Uhr**

**Es ist eine Horror-Vorstellung: Fremde können sich in Gruppenchats bei WhatsApp schleichen, dort private Gespräche verfolgen und diese sogar manipulieren. Eine Sicherheitslücke macht dies theoretisch möglich, das haben Sicherheitsforscher aus Deutschland herausgefunden.**

Laut den Experten der Ruhr-Universität Bochum sind die Chats trotz Verschlüsselung angreifbar, wenn Hacker sich Zugriff auf die WhatsApp-Server verschaffen. Sie könnten dann Einladungen zu Gruppen-Chats fälschen und sich so in beliebige Chat-Gruppen einschleichen, ohne tatsächlich eine Einladung erhalten zu haben.



# History of our Work



**THE Sun** THE SUN, A NEWS UK COMPANY

SPORT TV & SHOWBIZ NEWS FABULOUS MONEY MOTORS TRAVEL

All Tech Science Phones & Gadgets Gaming

## WHO'S WATCHING? New WhatsApp bug could expose your group chat messages to hackers – we reveal how to stay safe

Researchers say WhatsApp users could be vulnerable to cyber-attack, as a new exploit reveals sneaky way of hacking your private group chats

By Sean Keach  
11th January 2018, 10:32 am | Updated: 11th January 2018, 2:32 pm

COMMENT NOW

PRIVATE messages sent by WhatsApp users could be exposed thanks to a new software bug.

Researchers have revealed how hackers could break into the popular messaging app and read your conversations.




Unbefugte könnten sich in 1  
Foto: DADO RUVIC / Reuters



12.01.2018 - 10:07 Uhr  
Es ist eine Horror-Vorst  
schleichen, dort private  
Sicherheitslücke macht  
Deutschland herausgef

Laut den Experten der R  
angreifbar, wenn Hacke  
Einladungen zu Grupper  
ohne tatsächlich eine Einladuung erhalten zu haben.



Resources Industry Voice SMB Spotlight

**the INQUIRER**

News Artificial Intelligence Internet of Things Open Source Hardware Software Security

## WhatsApp bug lets anyone easily infiltrate private group chats

Facebook-owned messaging outfit shrugs off the issue

Security

Carly Page  
@CarlyPage\_  
11 January 2018

0 Comments



WhatsApp bug lets anyone easily infiltrate private group chats

**FACEBOOK-OWNED** WhatsApp suffers from a flaw that makes it possible for anyone to infiltrate private group chats without admin permission.

The vulnerability was outed by a bunch of cryptographers from Ruhr University Bochum in Germany, who announced their findings at the 'Real World Crypto Security

# History of our Work

**THE Sun** THE SUN, A NEWS UK COMPANY

**Bild** MENO

Resources Industry Voice SMB Spotlight

**the INQUIRER**

en Source Hardware Software Security

**MailOnline** Science & Tech

All Tech Science Phones & Gadgets Gaming

Home News U.S. Sport TV&Showbiz Australia Femail Health Science Money Video Travel Fashion Finder

Latest Headlines Science Pictures Discounts Login

## WHO'S WATCHING? New WhatsApp bug could expose your group chat messages to hackers – we reveal how to stay safe

Researchers say WhatsApp users could be vulnerable to attack, as a new exploit reveals sneaky way of hacking private group chats

By Sean Keach  
11th January 2018, 10:32 am | Updated: 11th January 2018, 2:32 pm

Twitter Facebook

**PRIVATE** messages sent by WhatsApp users could be exposed thanks to software bug.

Researchers have revealed how hackers could break into the popular messenger and read your conversations.

### Massive WhatsApp security flaw lets ANYONE spy on conversations by secretly adding members to private group chats (but Facebook says it won't fix the problem)

- Security experts have found a way around WhatsApp's end-to-end encryption
- Hackers can insert people into WhatsApp groups without admin permission
- Facebook, which owns WhatsApp, said it does not intend to fix the issue
- It added that group chats 'remain protected' by the app's encryption

By **HARRY PETTIT FOR MAILONLINE**  
PUBLISHED: 10:11 GMT, 11 January 2018 | UPDATED: 12:15 GMT, 11 January 2018

Facebook Share Twitter Pinterest Google+ Email RSS 160 shares 64 View comments

A huge WhatsApp design flaw that allows anyone to infiltrate private group chats has been uncovered by security researchers.

Despite the service's end-to-end encryption, experts say hackers can insert people

anyone easily join group chats

shrugs off the issue

Facebook

Today's headlines Most Read

- Incredible NASA images show exposed 'underground ice cliffs' on Mars in discovery that could provide...
- How clean is YOUR air? UK pollution hotspots are revealed using a new tool that lets you check toxic...
- Flashing fake eyelashes fitted with tiny LEDs could be the next high-tech beauty trend, but would you wear...
- General Motors says it will mass produce a self-driving car WITHOUT a steering wheel or pedals in 2019
- Little-known deep sea volcanic eruption that took place just 600 miles from New Zealand was the world's...
- Could dogs one day speak 'human'? Pet translator that converts growls and barks into English could be...

# History of our Work

**Y Hacker News** new | comments | show | ask | jobs | submit

login

▲ moxie 2 days ago | parent | favorite | on: WhatsApp Encryption Security Flaws Could Allow Sno...

Here's how WhatsApp group messaging works: membership is maintained by the server. Clients of a group retrieve membership from the server, and clients encrypt all messages they send e2e to all group members.

If someone hacks the WhatsApp server, they can obviously alter the group membership. If they add themselves to the group:

1. The attacker will not see any past messages to the group; those were e2e encrypted with keys the attacker doesn't have.
2. All group members will see that the attacker has joined. There is no way to suppress this message.

Given the alternatives, I think that's a pretty reasonable design decision, and I think this headline pretty substantially mischaracterizes the situation. I think it would be better if the server didn't have metadata visibility into group membership, but that's a largely unsolved problem, and it's unrelated to confidentiality of group messages.

In contrast Telegram does *no encryption at all* for group messages, even though it advertises itself as an encrypted messenger, and even though telegram users think that group chats are somehow secure. An attacker who compromises the Telegram server can, undetected, recover every message that was sent in the *past* and receive all messages transmitted in the *future* without anyone receiving any notification at all.

There's no way to publish an academic paper about that, though, because there's no "attack" to describe, because there's no encryption to begin with. Without a paper there will be no talks at conferences, which means there will be no inflammatory headlines like this one.

To me, this article reads as a better example of the problems with the security industry and the way security research is done today, because I think the lesson to anyone watching is clear: don't build security into your products, because that makes you a target for researchers, even if you make the right decisions, and regardless of whether their research is practically important or not. It's much more effective to be Telegram: just leave cryptography out of everything, except for your marketing.



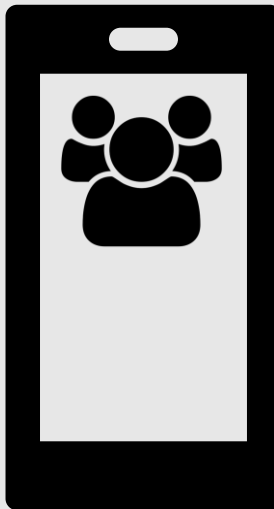
# Agenda

- Methodology
- Security Model
  - Issues of Modeling and Protocols
    - Reliability vs. Instant Messaging
    - Post Compromise Security and Ratcheting
- Overview and Standardization

# Methodology

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

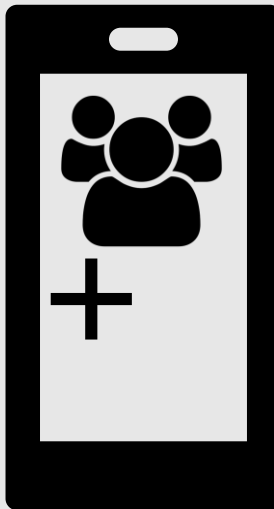
- Define
  - Syntax (=API)



# Methodology

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

- Define
  - Syntax (=API)

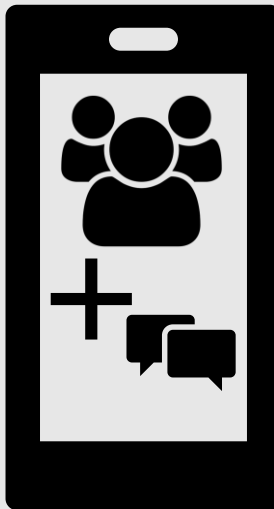




# Methodology

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

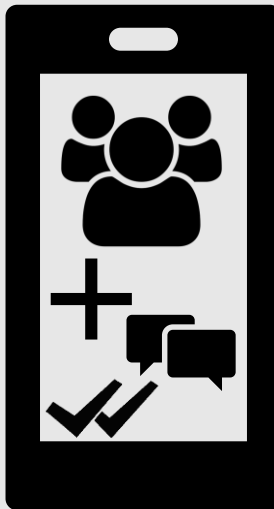
- Define
  - Syntax (=API)



# Methodology

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

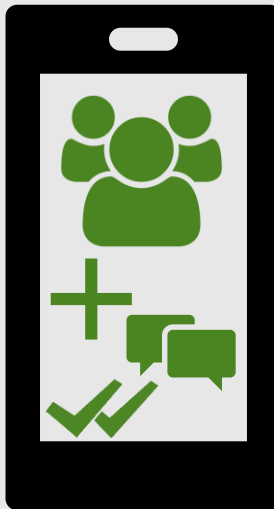
- Define
  - Syntax (=API)



# Methodology

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

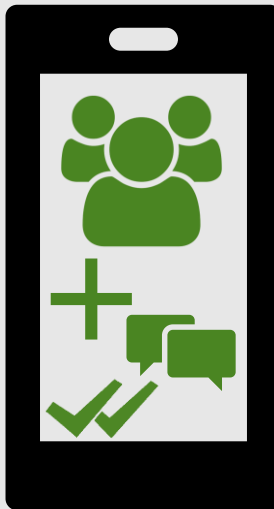
- Define
  - Syntax (=API)
  - Security goals



# Methodology

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

- Define
  - Syntax (=API)
  - Security goals
  - Attacker capabilities



# Methodology

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

- Define
  - Syntax (=API)
  - Security goals
  - Attacker capabilities
- Analyze
  - Key distribution



# Methodology

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

- Define
  - Syntax (=API)
  - Security goals
  - Attacker capabilities
- Analyze
  - Key distribution
  - Messaging protocols
    - Key computation



# Methodology

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

- Define
  - Syntax (=API)
  - Security goals
  - Attacker capabilities
- Analyze
  - Key distribution
  - Messaging protocols
    - Key computation
  - Group management



# Methodology

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

- Define
  - Syntax (=API)
  - Security goals
  - Attacker capabilities
- Analyze
  - Key distribution
  - Messaging protocols
    - Key computation
  - Group management
  - Reliability protocols

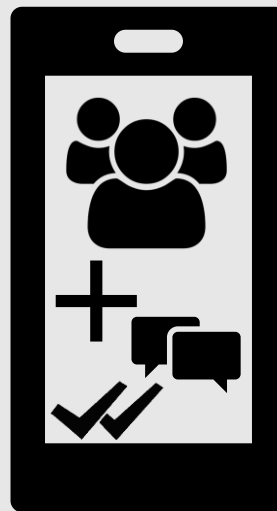




# Methodology

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

- Define
  - Syntax (=API)
  - Security goals
  - Attacker capabilities



- Analyze
  - Key distribution
  - Messaging protocols
    - Key computation
  - Group management
  - Reliability protocols
  - WhatsApp: Alternative client
  - Signal: Android in Java
  - Threema: Alternative client

# Methodology

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

- Define
    - Syntax (=API)
    - Security goals
    - Attacker capabilities
  - Analyze
    - Key distribution
    - Messaging protocols
    - Key computation
    - Group management
    - Reliability protocols
- Focus: cryptographic protocols
- Out of scope: implementations  
(future work for you?! 😊)



- WhatsApp: Alternative client
- Signal: Android in Java
- Threema: Alternative client

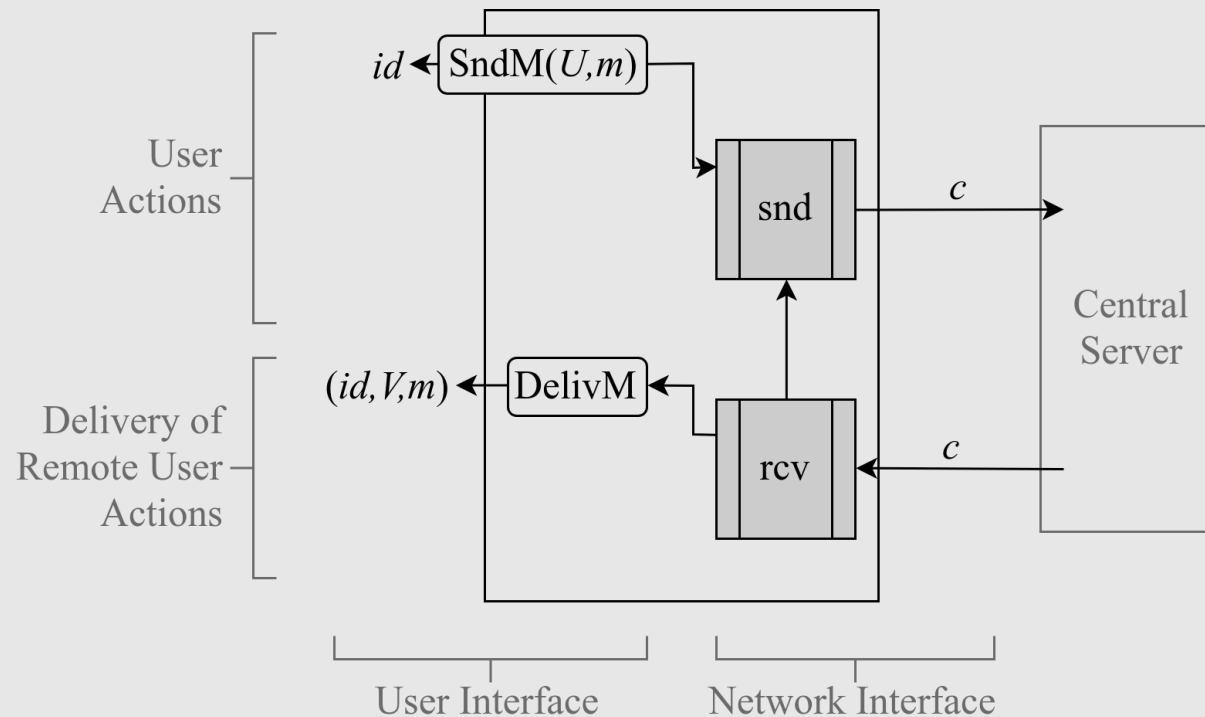
# Secure Group Instant Messaging: Two Parties

## Security Model

Reliability vs. Instant Messaging

PCS and Ratcheting

Asynchronous Group IM



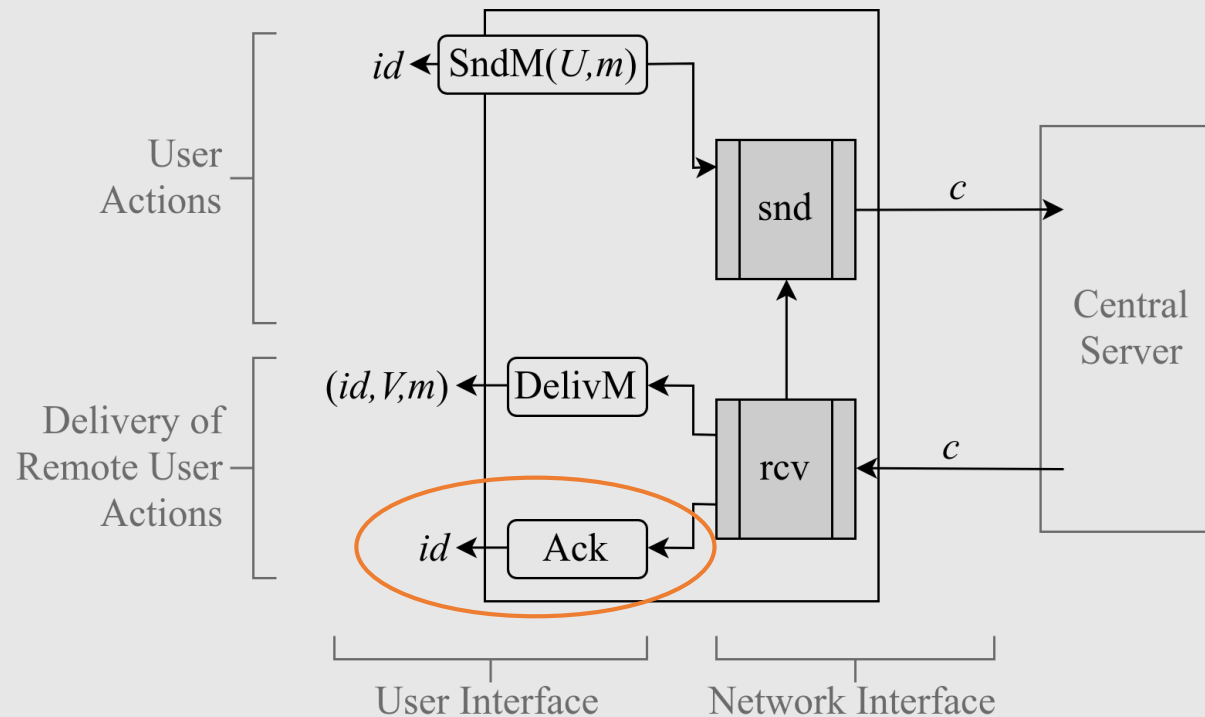
# Secure Group Instant Messaging: Two Parties

## Security Model

Reliability vs. Instant Messaging

PCS and Ratcheting

Asynchronous Group IM



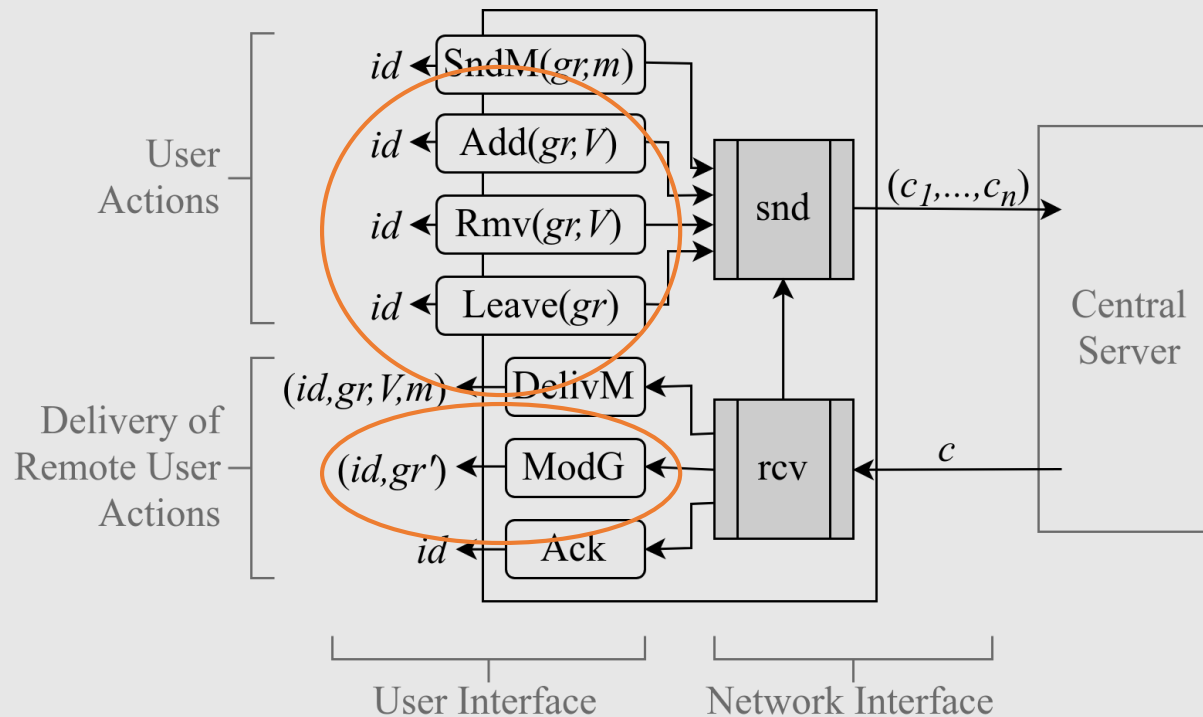
# Secure Group Instant Messaging: Groups

## 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

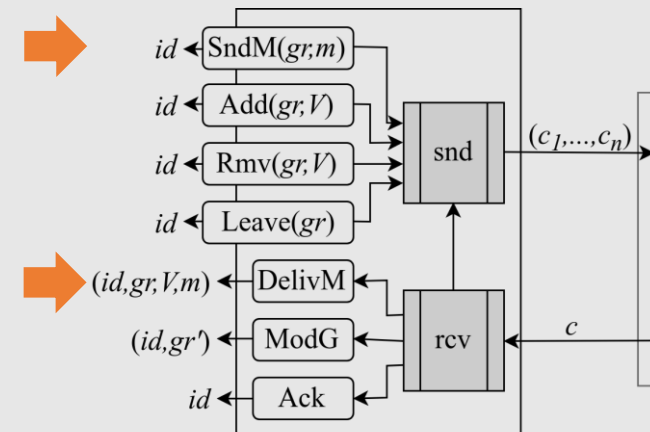
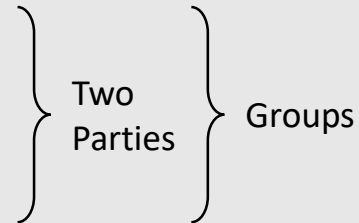
Asynchronous Group IM

## 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

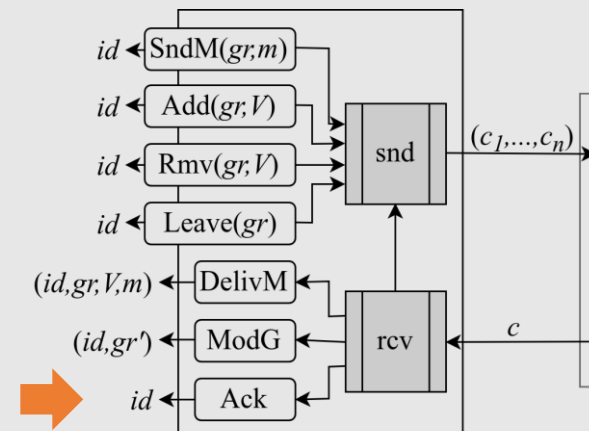
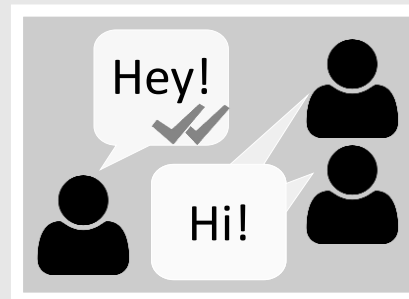
## Integrity

- 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**

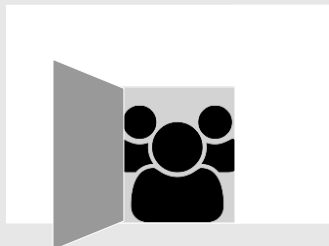
## Integrity

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

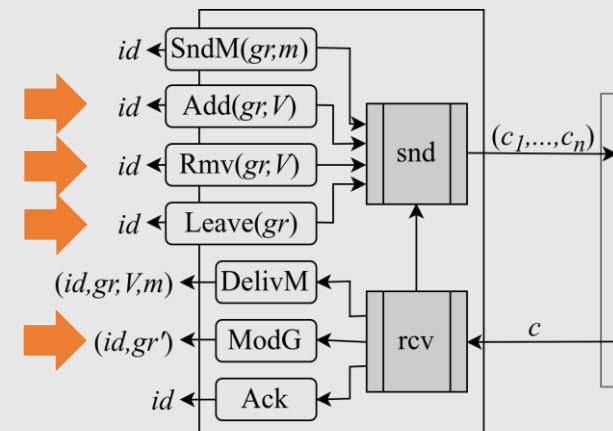
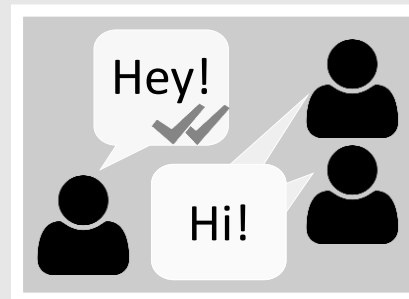
Two  
Parties

Groups

“Only group (admin) decides on membership”



“Only successful delivery is acknowledged”






# Security Model: Malicious Server

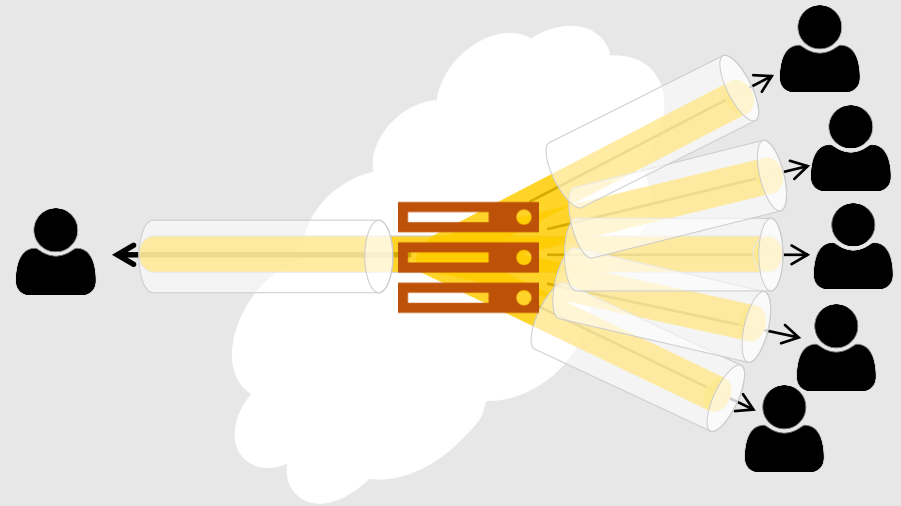
## Security Model

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 protection
- E.g. IM provider, TLS forger on network,

**Support The Guardian**

**The Guardian**

News Opinion Sport Culture Lifestyle

US World Environment Soccer **US politics** Business Tech Science More

TOP SECRET//SI//ORCON//NOFORN

PRISM

PRISM/US-984XN  
Overview

OR

*The SIGAD Used Most in NSA Reporting*  
Overview

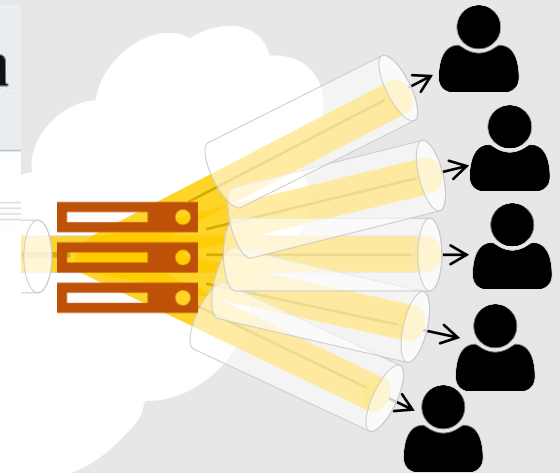
PRISM Collection Manager, S35333

April 2013

Glenn Greenwald on security and liberty

### NSA Prism program taps in to user data of Apple, Google and others


- Top-secret Prism program claims direct access to servers of firms including Google, Apple and Facebook
- Companies deny any knowledge of program in operation since 2007
- Obama orders US to draw up overseas target list for cyber-attacks



# Security Model: Malicious Server

## Security Model

Reliability vs. Instant Messaging  
PCS and Ratcheting  
Asynchronous Group IM

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



**Bloomberg** Telegram Loses Bid to Block Russia From Encryption Keys

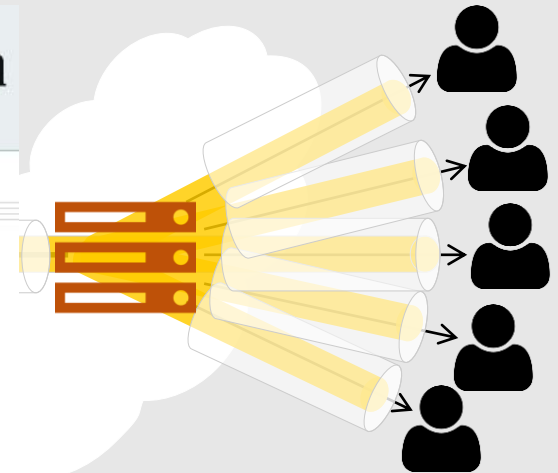
## Telegram Loses Bid to Block Russia From Encryption Keys

By Ilya Khrennikov

March 20, 2018, 12:04 PM GMT+1 Updated on March 20, 2018, 4:27 PM GMT+1

- Messaging service plans to appeal Russian court's decision
- Regulators could block Telegram service if it fails to comply

Telegram, the encrypted messaging app that's prized by those seeking privacy, lost a bid before Russia's Supreme Court to block security services from getting access to users' data, giving President Vladimir Putin a victory in his effort to keep tabs on electronic communications.



data of

ers of

on

ier-


# Security Model: Malicious Server

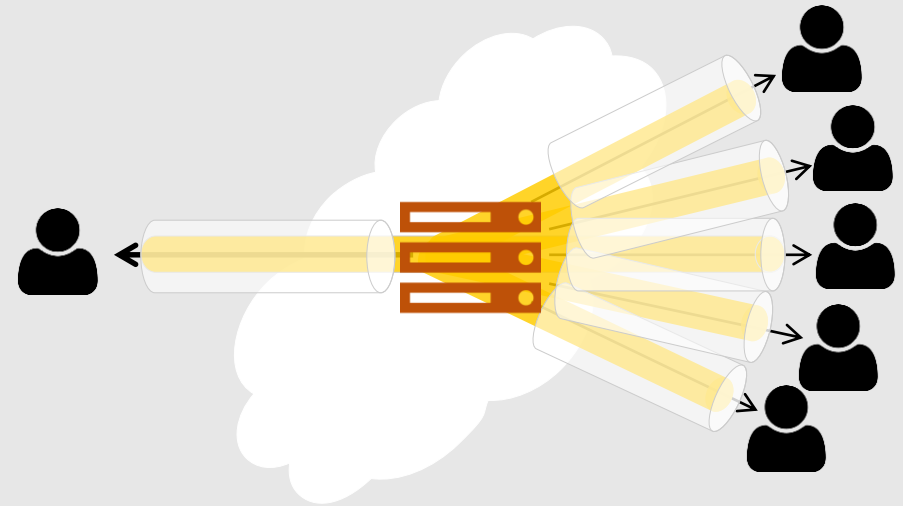
## Security Model






Reliability vs. Instant Messaging

PCS and Ratcheting

Asynchronous Group IM

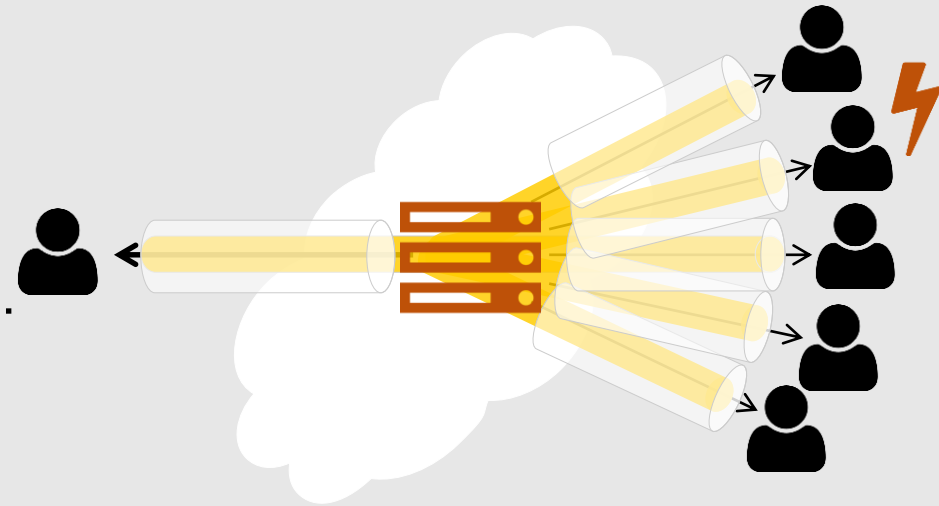
- Malicious Server 
  - Can decrypt transport layer protection
  - E.g. IM provider, TLS certificate forger on network, ...








Attackable by	Traceable Delivery	Closeness
		?
		

# Security Model: Compromising Attacker

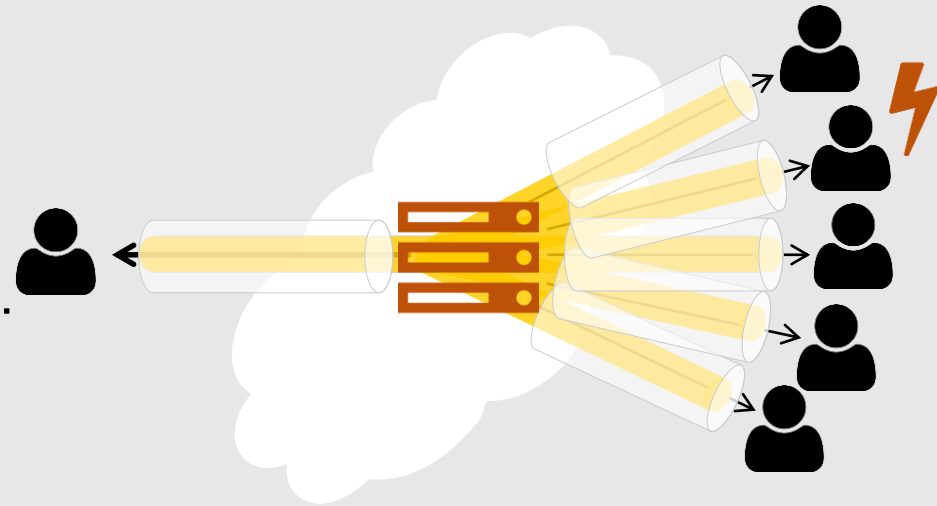
- Compromising Attacker ⚡
  - Access to members' secrets
  - E.g. access to device, cryptanalysis, ...



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 → ⚡

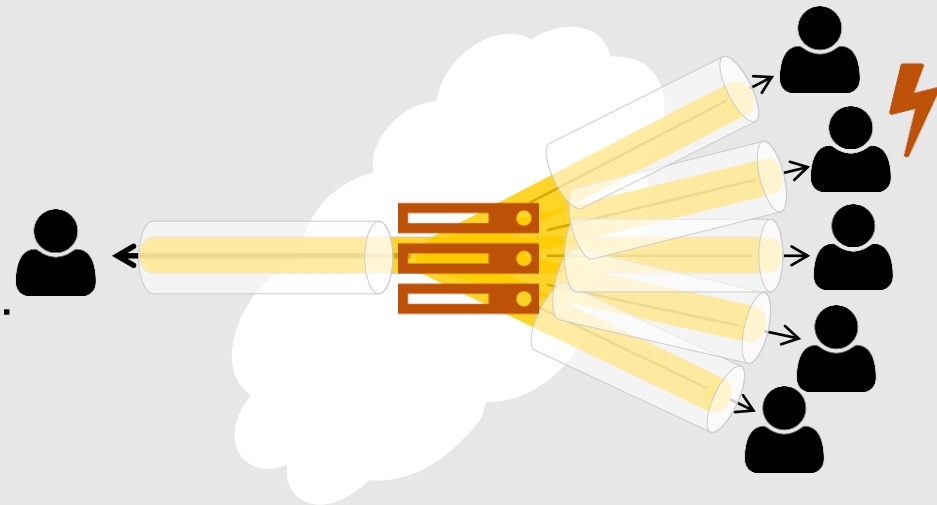
- Post Compromise Security  
(aka Future Secrecy aka Backward Secrecy → cf. [CCG CSF '16])

⚡ → 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 → cf. [CCG CSF '16])

⚡ → Secure →

Attackable by	Traceable Delivery	Closeness
		⚡ (PCS)
		

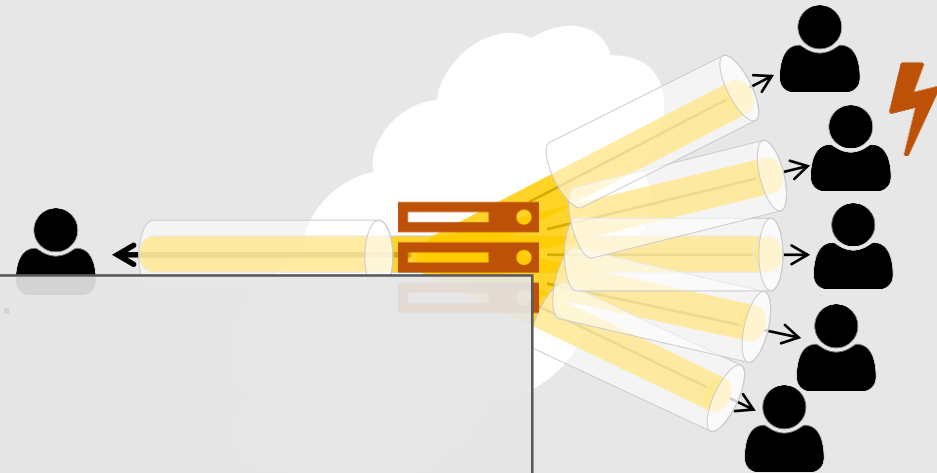
# Security Model: Compromising Attacker

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

- Advanced Goals:
  - Forward Secrecy






Remark:  
Email is also asynchronous

- Post Compromise Security  
(aka Future Secrecy aka Backward Secrecy → cf. [CCG CSF '16])



Secure → ⚡

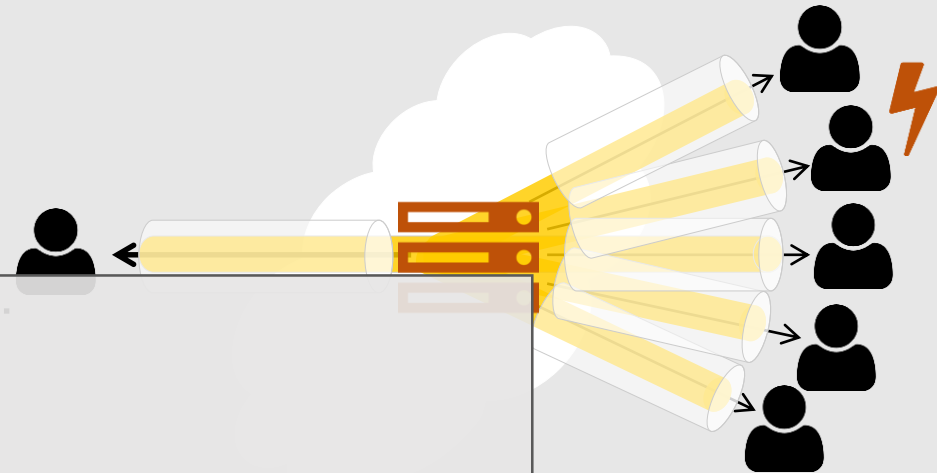
⚡ Secure →

Attackable by	Traceable Delivery	Closeness
		⚡ (PCS)
		



# Security Model: Compromising Attacker

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








- Advanced Goals:
    - Forward Secrecy
- Remark:  
Email is also asynchronous  
Email has **neither FS nor PCS**



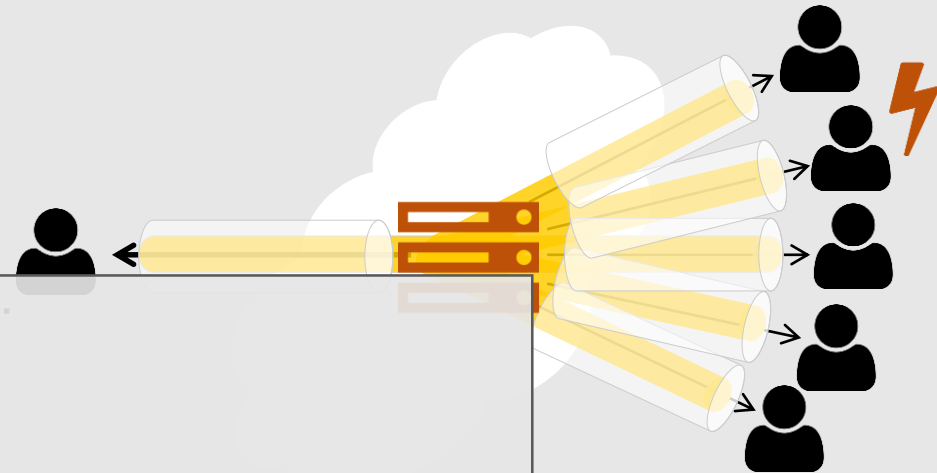
- Post Compromise Security  
(aka Future Secrecy aka Backward Secrecy → cf. [CCG CSF '16])



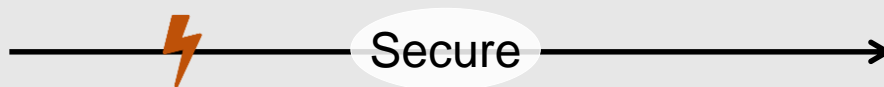
Attackable by	Traceable Delivery	Closeness
		⚡ (PCS)
		






# Security Model: Compromising Attacker

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



- Advanced Goals:
  - Forward Secrecy
- Remark:
  - Email is also asynchronous
  - Email has **neither FS nor PCS**
  - Email has even **no authentication**
- Post Compromise Security  
(aka Future Secrecy aka Backward Secrecy → cf. [CCG CSF '16])



Attackable by	Traceable Delivery	Closeness
		⚡ (PCS)
		

# Security Model

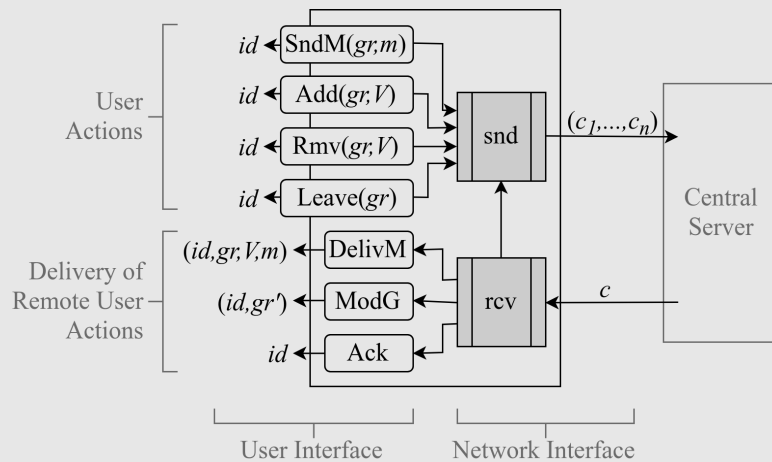
## Security Model

Reliability vs. Instant Messaging

PCS and Ratcheting

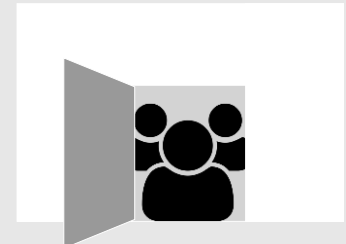
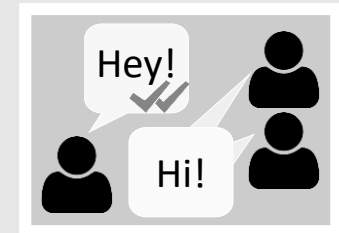
Asynchronous Group IM

## Syntax



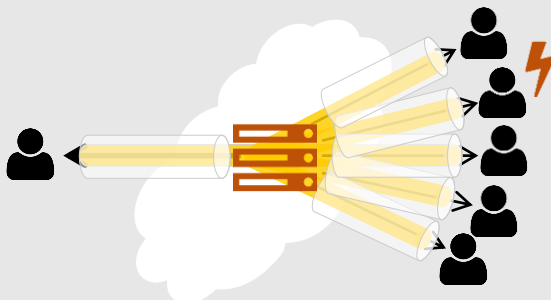
## Security & Reliability Goals:

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



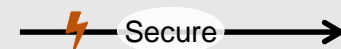
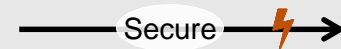
## Adversaries

- Malicious Server
- Compromising Attacker



## Advanced Goals:

- Forward Secrecy
- Post Compromise Security



# Security Model

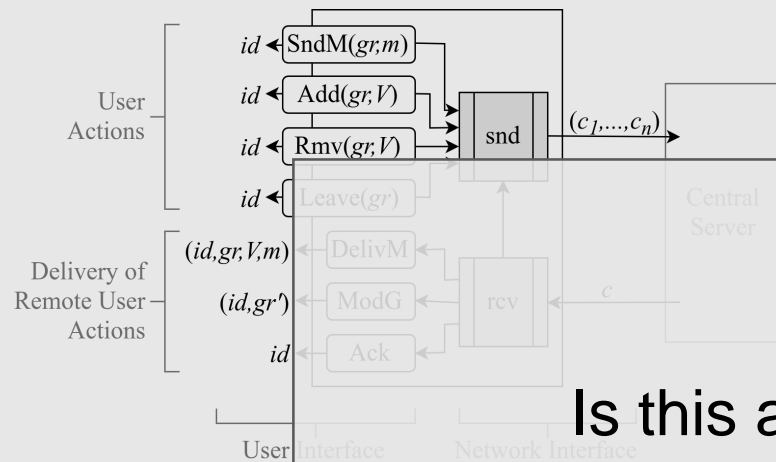
## Security Model

Reliability vs. Instant Messaging

PCS and Ratcheting

Asynchronous Group IM

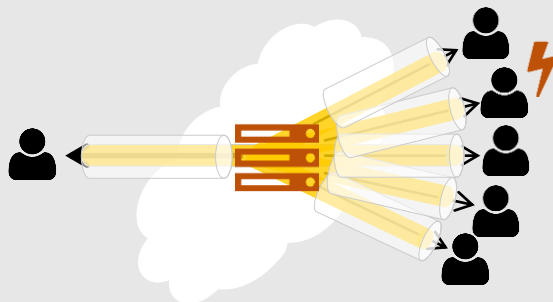
## Syntax



Is this a good definition for *secure group instant messaging*?

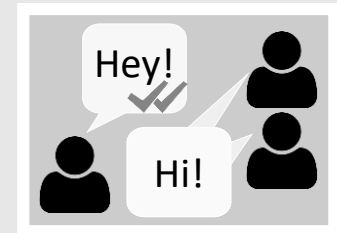
## Adversaries

- Malicious Server
- Compromising Attacker

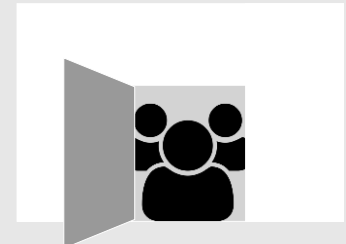


## Security & Reliability Goals:

- Message Confidentiality
- Message Authentication

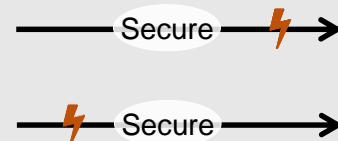


- No Duplication
- Traceable Delivery
- Closeness
- No Creation



## Advanced Goals:

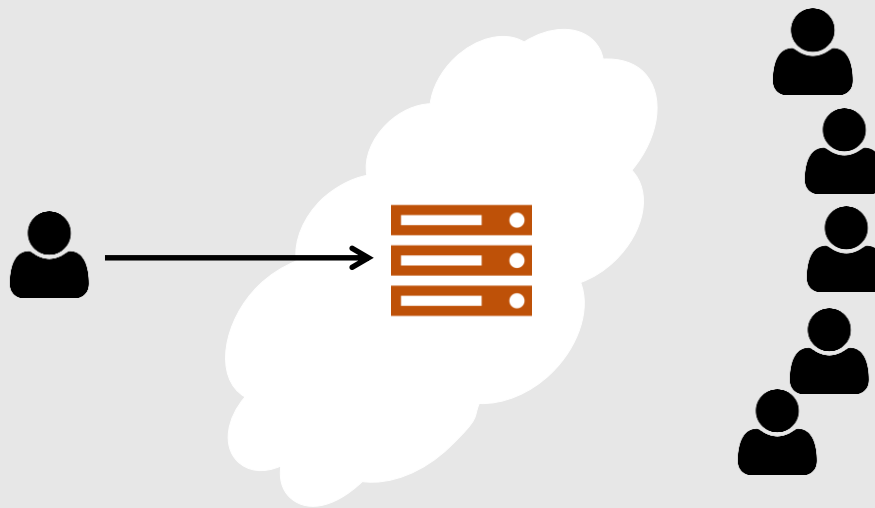
- Forward Secrecy
- Post Compromise Security



# Reliability vs. Instant Messaging

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

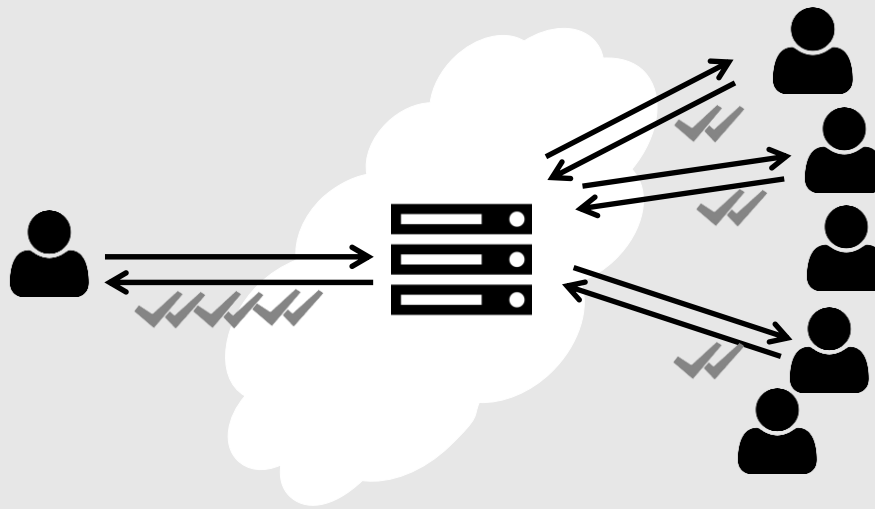
- Reliable delivery in centralized network impossible (Byzantine Agreement)



# Reliability vs. Instant Messaging

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

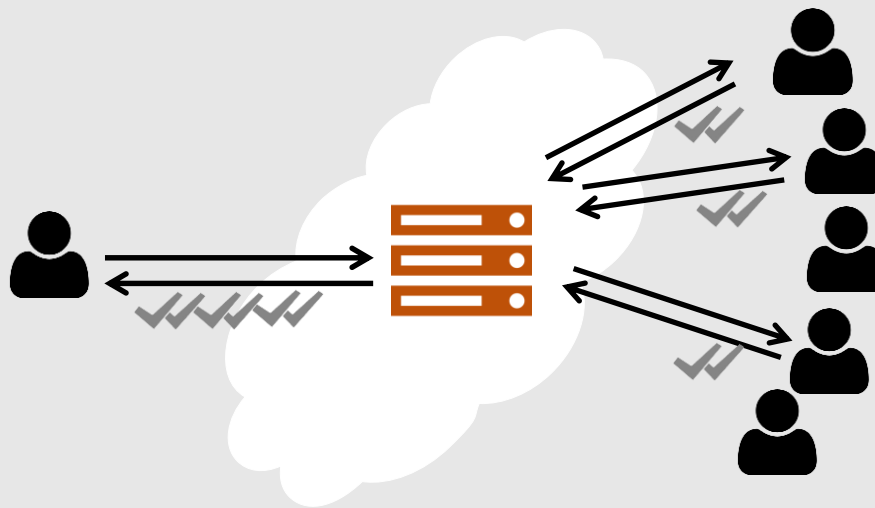
- Reliable delivery in centralized network impossible (Byzantine Agreement)
- Reliability of receipt status partially possible (Traceable Delivery)



# 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

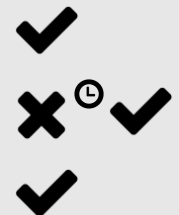
- Reliable delivery in centralized network impossible (Byzantine Agreement)
- Reliability of receipt status partially possible (Traceable Delivery)
- Ordering
  - With graphical user interface (out of scope)
    - *“we feel [...] difficult to build [...] UX which provides transcript consistency”* (Moxie Marlinspike)



# Order in 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)
- Ordering
  - With graphical user interface (out of scope)
    - “we feel [...] difficult to build [...] UX which provides transcript consistency” (Moxie Marlinspike)
- Causality
- *Weak* causality

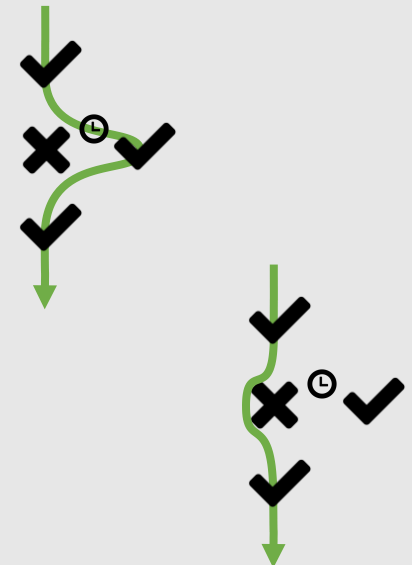




# Order in Instant Messaging

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

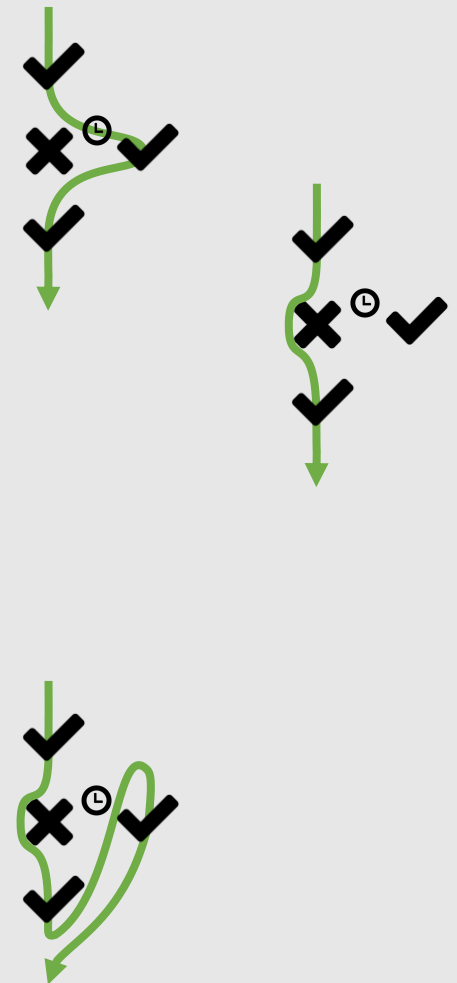
- Reliable delivery in centralized network impossible (Byzantine Agreement)
- Reliability of receipt status partially possible (Traceable Delivery)
- Ordering
  - With graphical user interface (out of scope)
    - “we feel [...] difficult to build [...] UX which provides transcript consistency” (Moxie Marlinspike)
  - Causality ( $m_i$  delivered if  $m_{i-1}$  delivered)
    - Withholding newer messages after message loss
  - Weak causality ( $m_i$  delivered if not  $m_j$  delivered,  $i < j$ )
    - Accepts message loss; prevents reordering



# Order in Instant Messaging

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

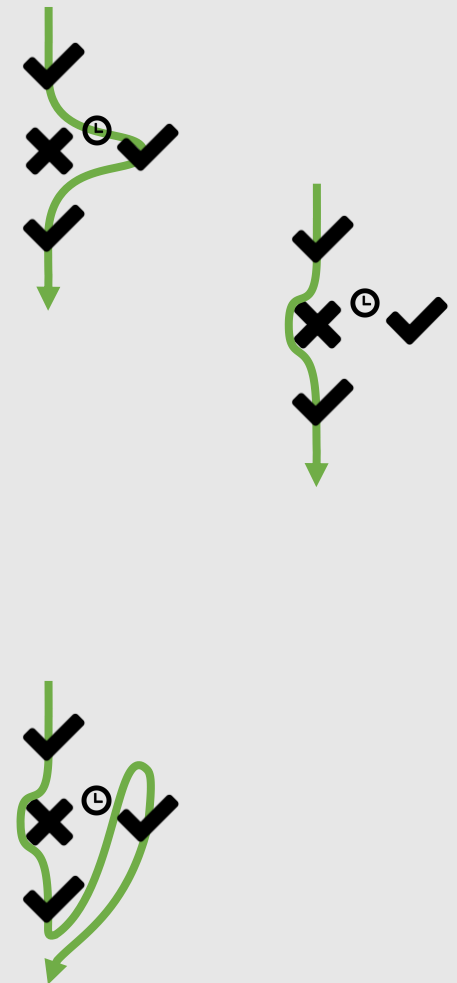
- Ordering
  - With graphical user interface (out of scope)
  - Causality ( $m_i$  delivered if  $m_{i-1}$  delivered)
  - *Weak* causality ( $m_i$  delivered if not  $m_j$  delivered,  $i < j$ )
- Signal and WhatsApp deliver messages on receipt
  - Server can mix last 2000 messages in delivery
  - Allows 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,  $i < j$ )
- Signal and WhatsApp deliver messages on receipt
  - Server can mix last 2000 messages in delivery
  - Allows to refer to specific messages
- No distinct solution in IM?!

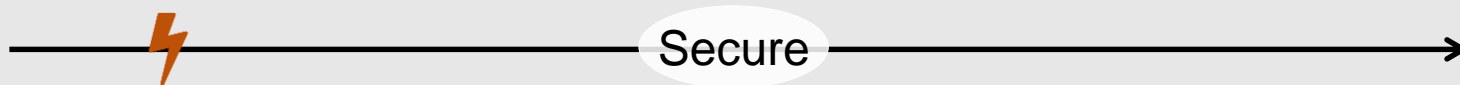


# Post Compromise Security and Ratcheting

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  $\lambda$  “group round trips”,  $\lambda$  constant

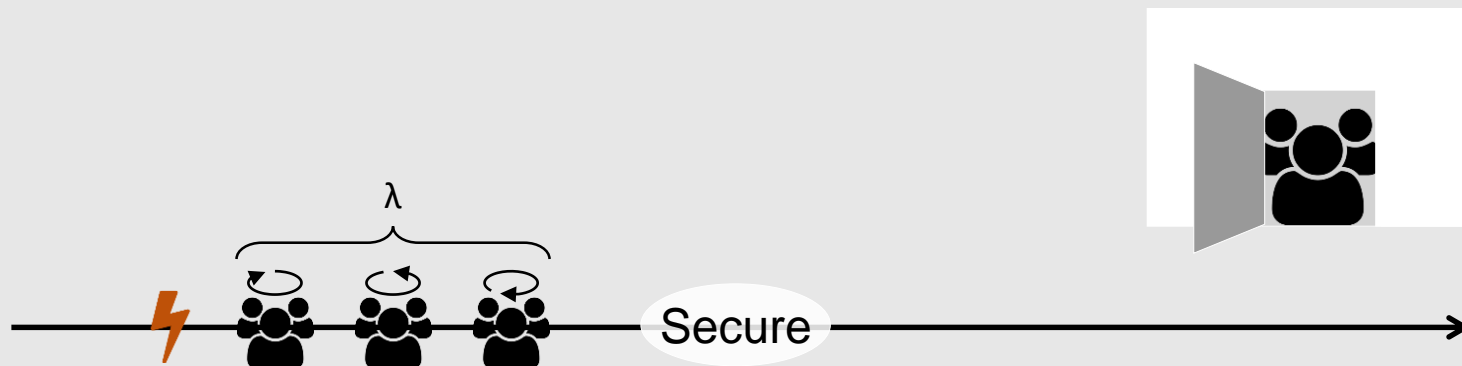


# Post Compromise Security and Ratcheting

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  $\lambda$  “group round trips”,  $\lambda$  constant
    - ⇒ **Closeness** of group after  $\lambda$  “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

- **Confidentiality** of messages after  $\lambda$  “group round trips”,  $\lambda$  constant  
 $\Rightarrow$  **Closeness** of group after  $\lambda$  “group round trips”

## Ratcheting

- Continuous update of state secrets to reach PCS

# Post Compromise Security and Ratcheting

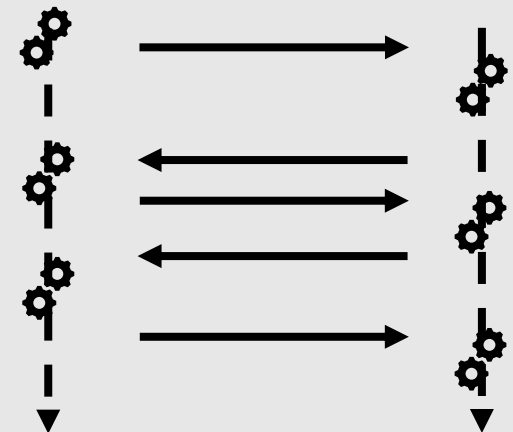
Security Model  
Reliability vs. Instant Messaging  
**PCS and Ratcheting**  
Asynchronous Group IM

## Post Compromise Security in Groups

- **Confidentiality** of messages after  $\lambda$  “group round trips”,  $\lambda$  constant  
⇒ **Closeness** of group after  $\lambda$  “group round trips”

## Ratcheting

- Continuous update of state secrets to reach PCS  
→ Pair-wise communication: Signal, [BCJ+ Crypto ‘17], [**PoeRoe Crypto ‘18**]
- *Continuously redo key exchanges and mix*  
+ *Forward secure state update*



# Post Compromise Security and Ratcheting

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

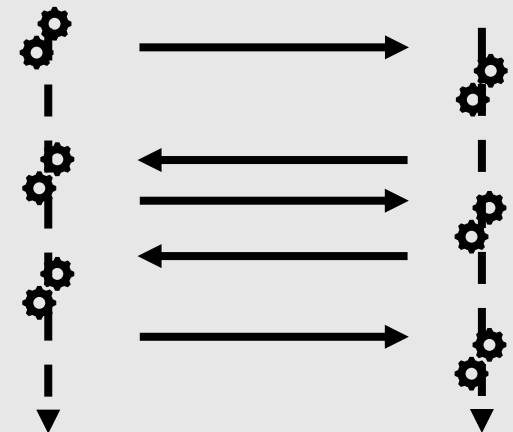
## Post Compromise Security in Groups

- **Confidentiality** of messages after  $\lambda$  “group round trips”,  $\lambda$  constant  
⇒ **Closeness** of group after  $\lambda$  “group round trips”

## Ratcheting

- Continuous update of state secrets to reach PCS  
→ Pair-wise communication: Signal, [BCJ+ Crypto ‘17], [**PoeRoe Crypto ‘18**]
- *Continuously redo key exchanges and mix*  
+ *Forward secure state update*

→ Groups?!

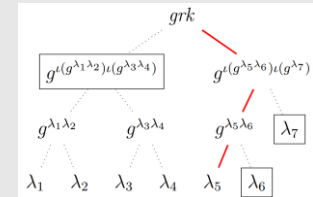
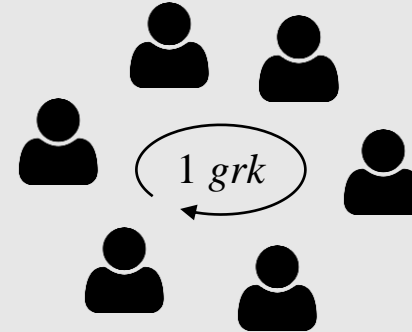


# Post Compromise Security and Ratcheting

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

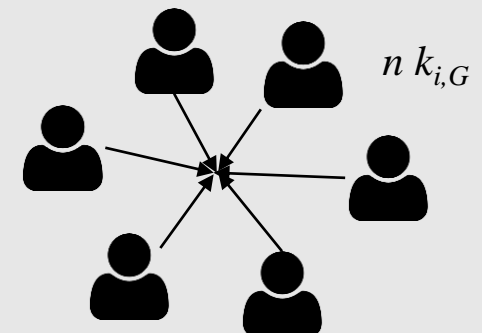
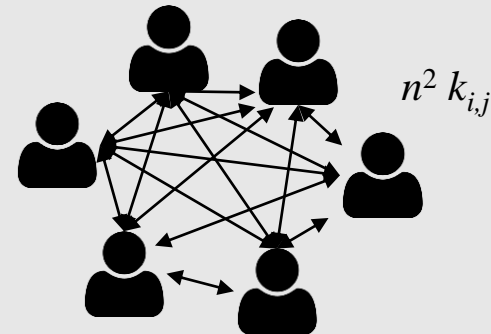
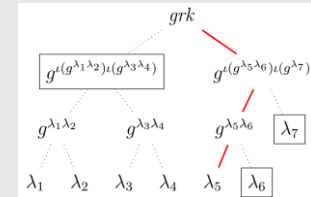
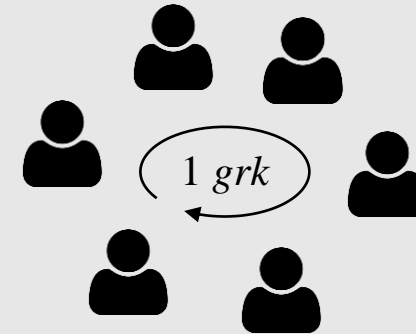
Security Model  
Reliability vs. Instant Messaging  
**PCS and Ratcheting**  
Asynchronous Group IM

## 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]

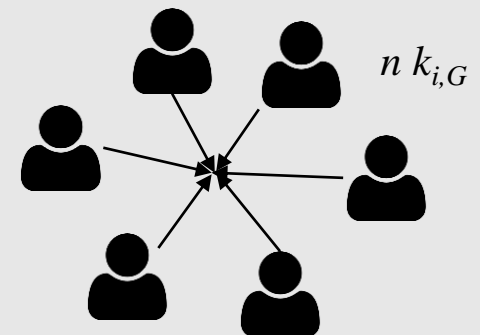
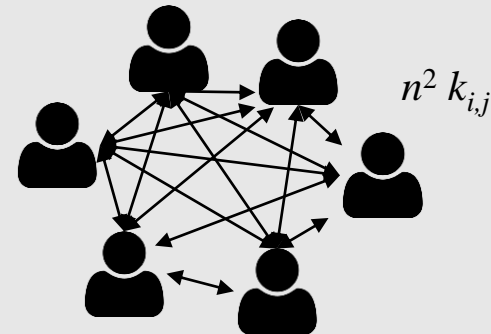
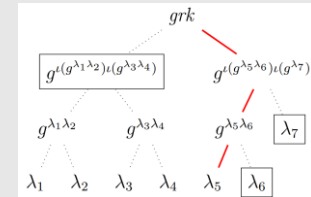
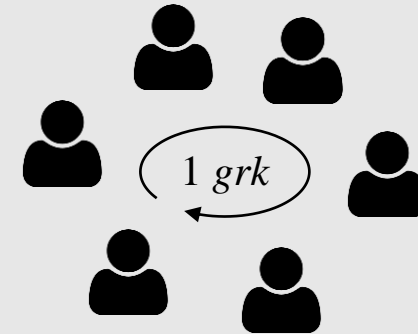
## Confidentiality via direct channels

→ 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

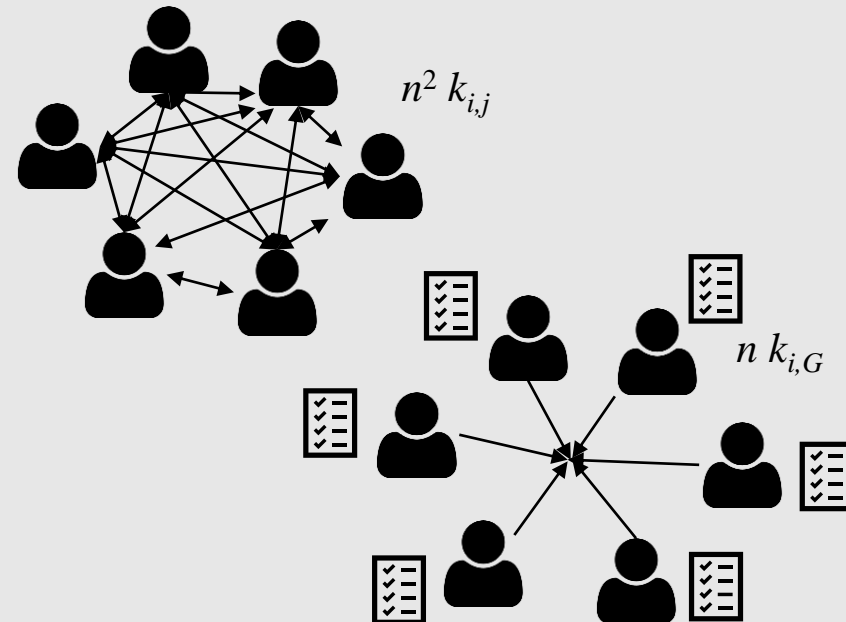
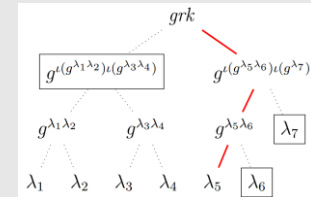
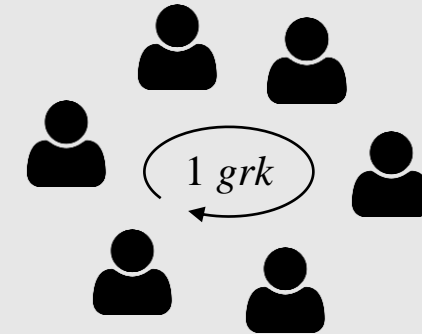
→ Ratcheting in direct channels

→ 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

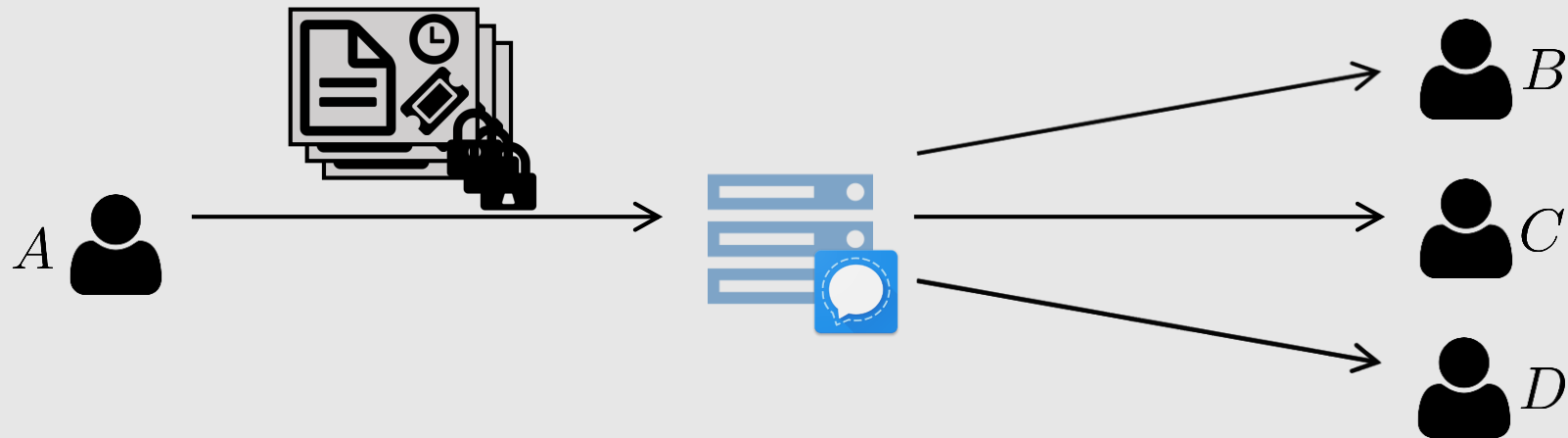
Security Model  
Reliability vs. Instant Messaging  
**PCS and Ratcheting**  
Asynchronous Group IM





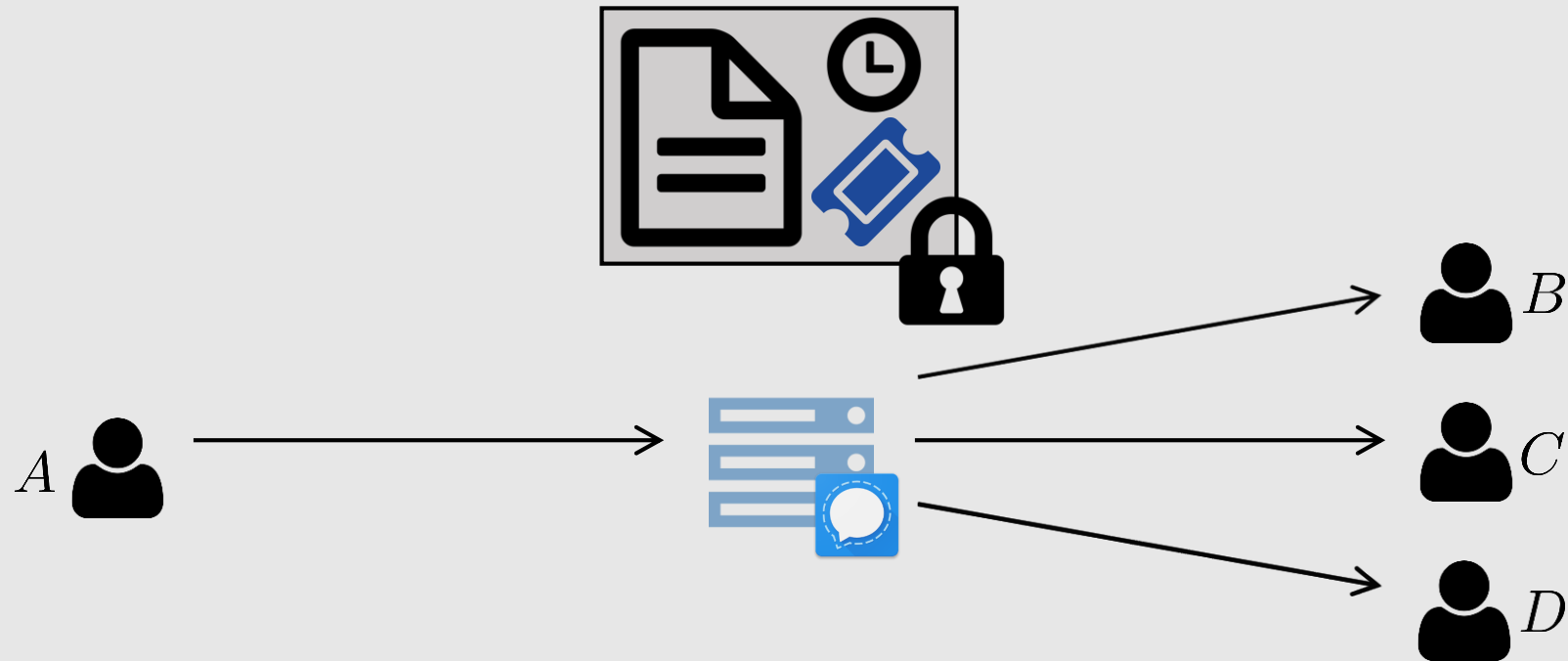
# Protocol Overview: Signal

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



# Protocol Overview: Signal

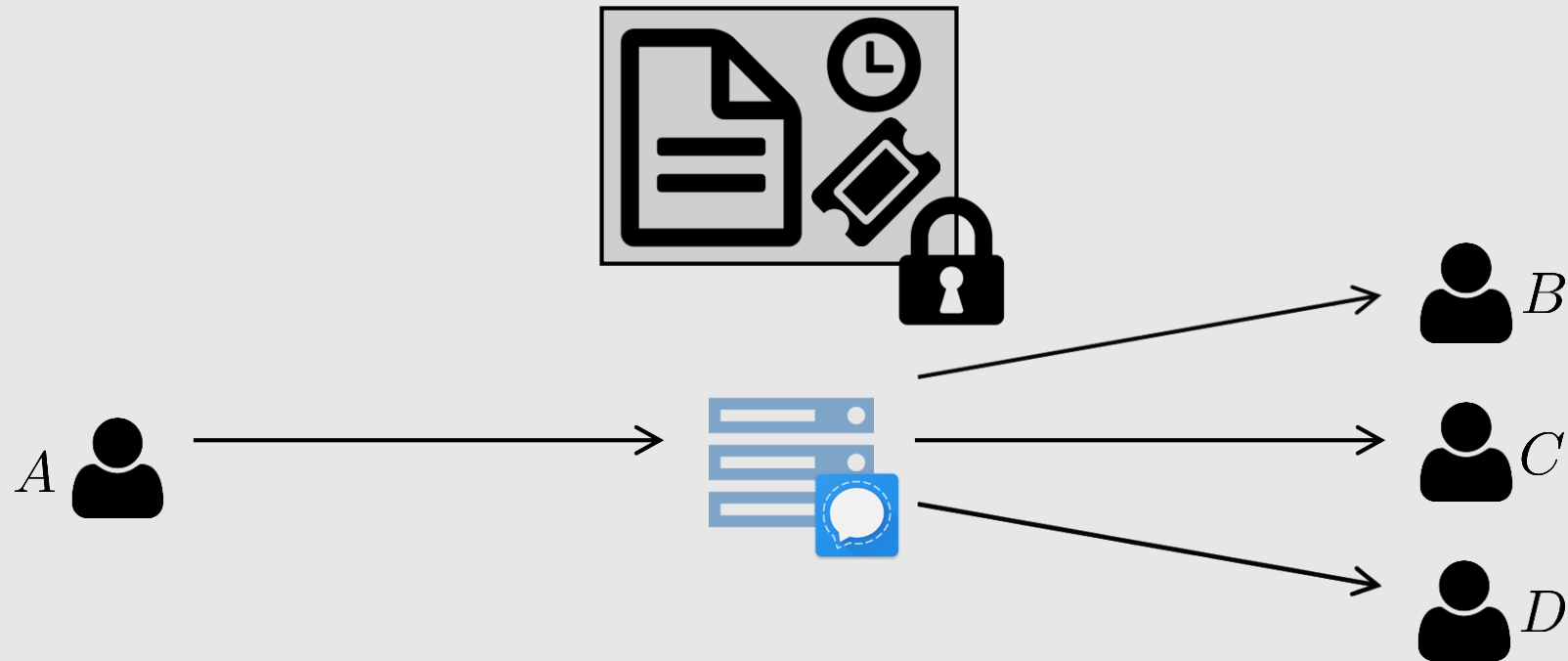
Security Model  
Reliability vs. Instant Messaging  
**PCS and Ratcheting**  
Asynchronous Group IM



Sender in group?

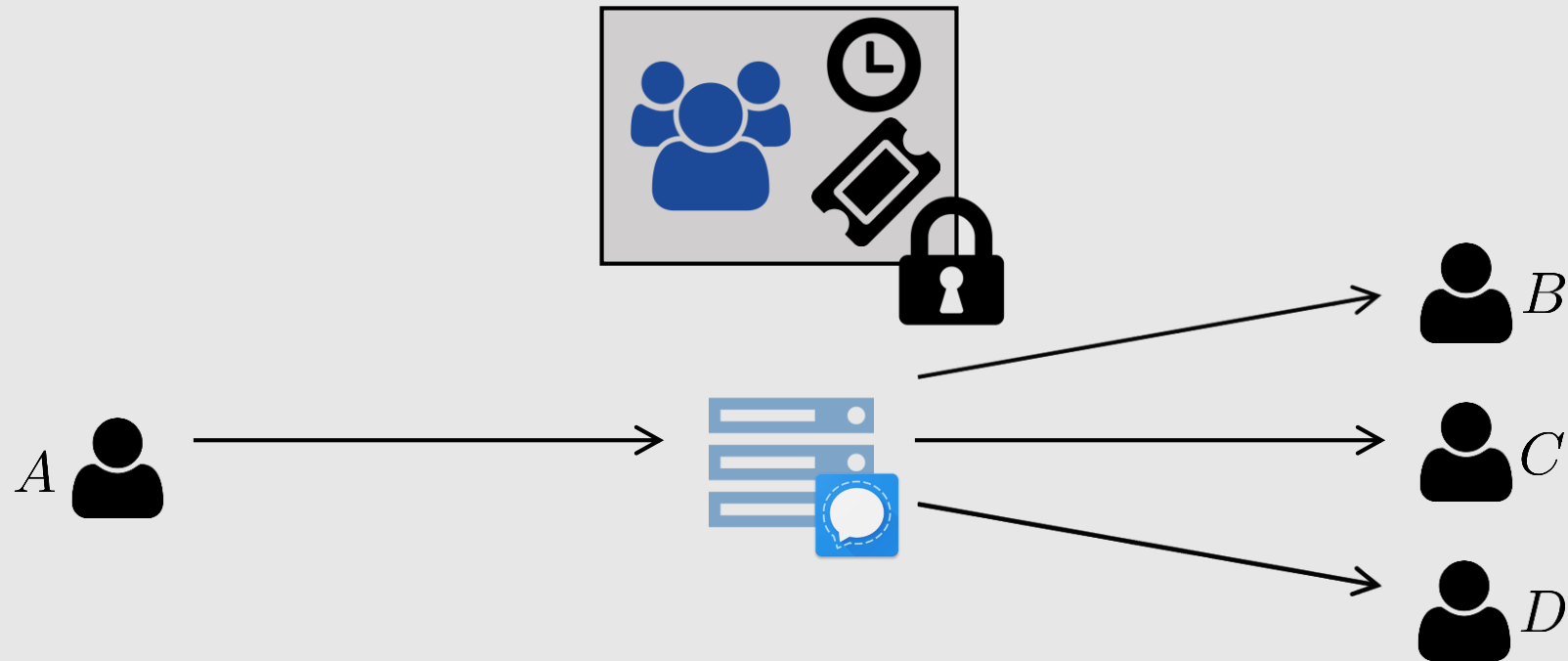
# Protocol Overview: Signal

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



# Protocol Overview: Signal

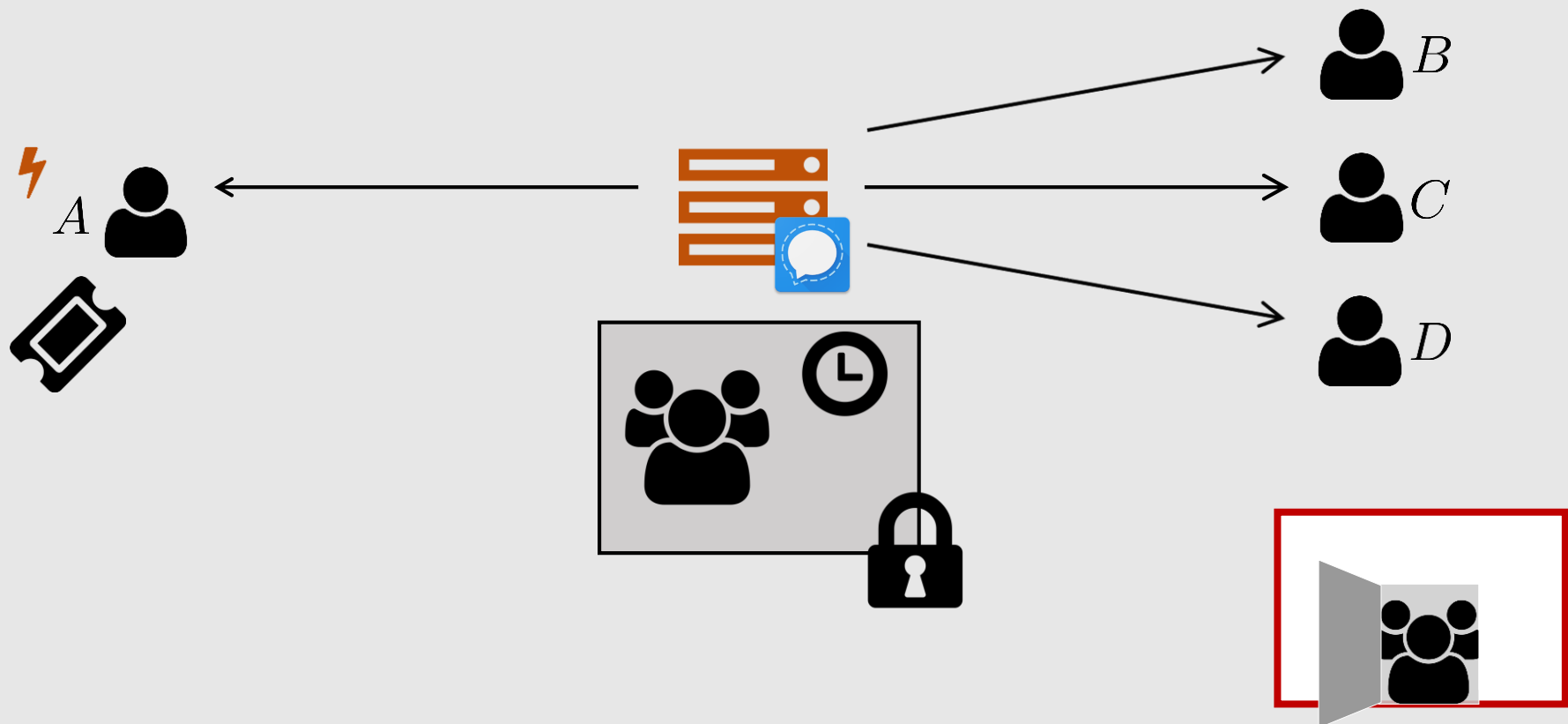
Security Model  
Reliability vs. Instant Messaging  
**PCS and Ratcheting**  
Asynchronous Group IM



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:

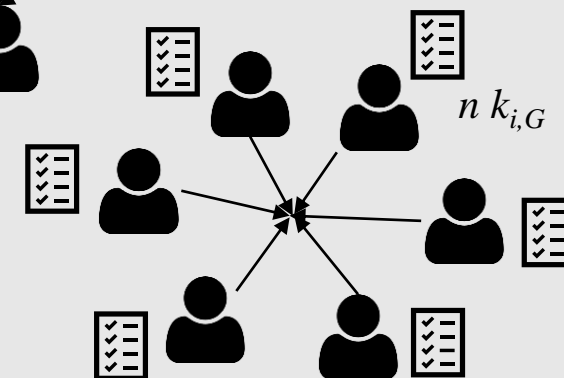
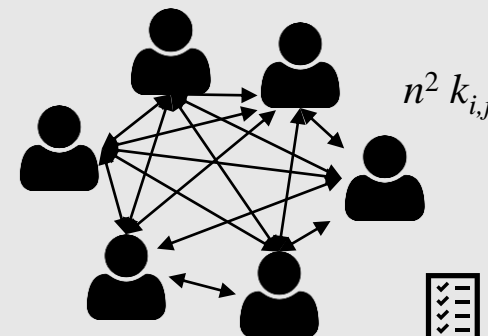
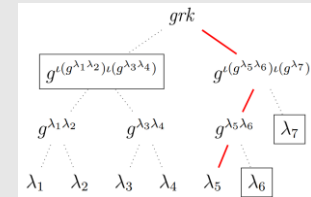
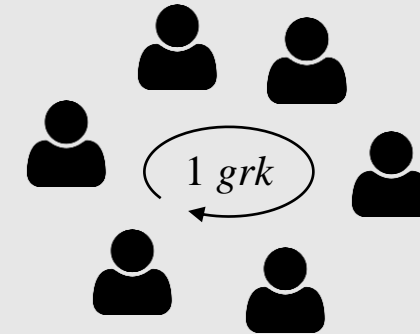


- Ticket approach



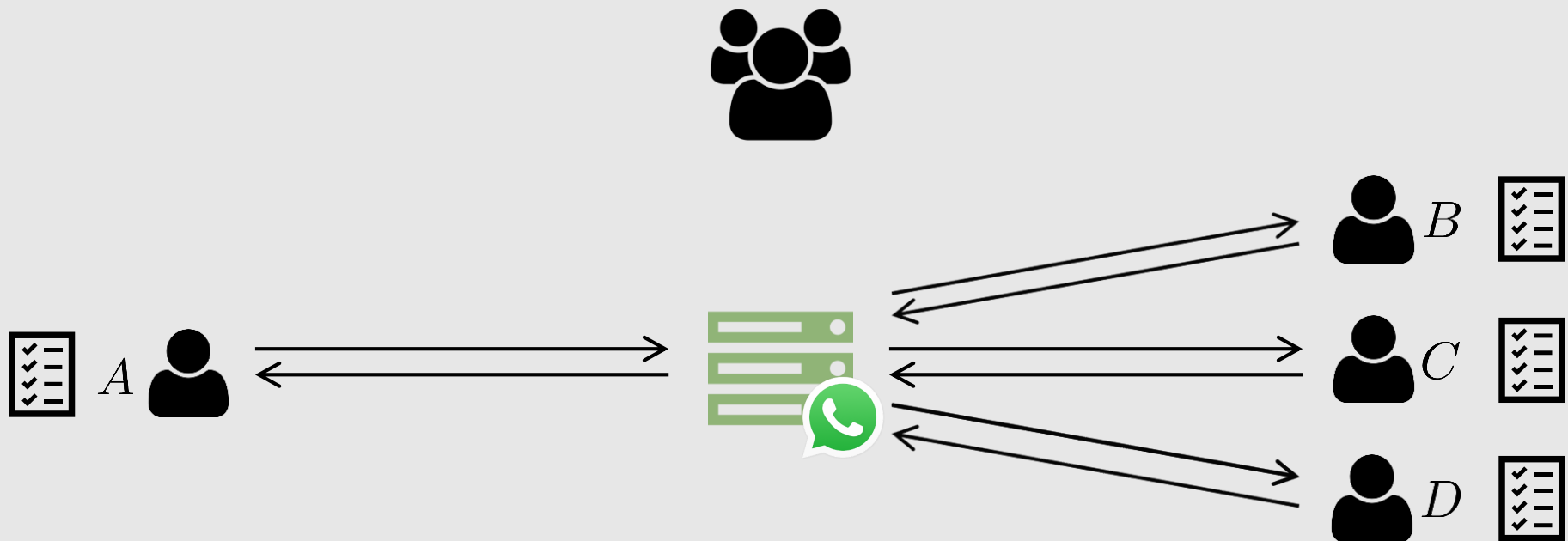
→ Related to group key exchange

- Guest list approach



# Protocol Overview: WhatsApp

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

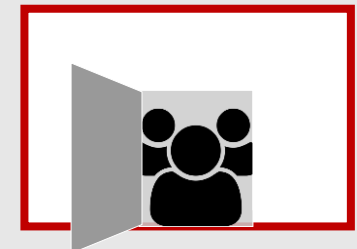
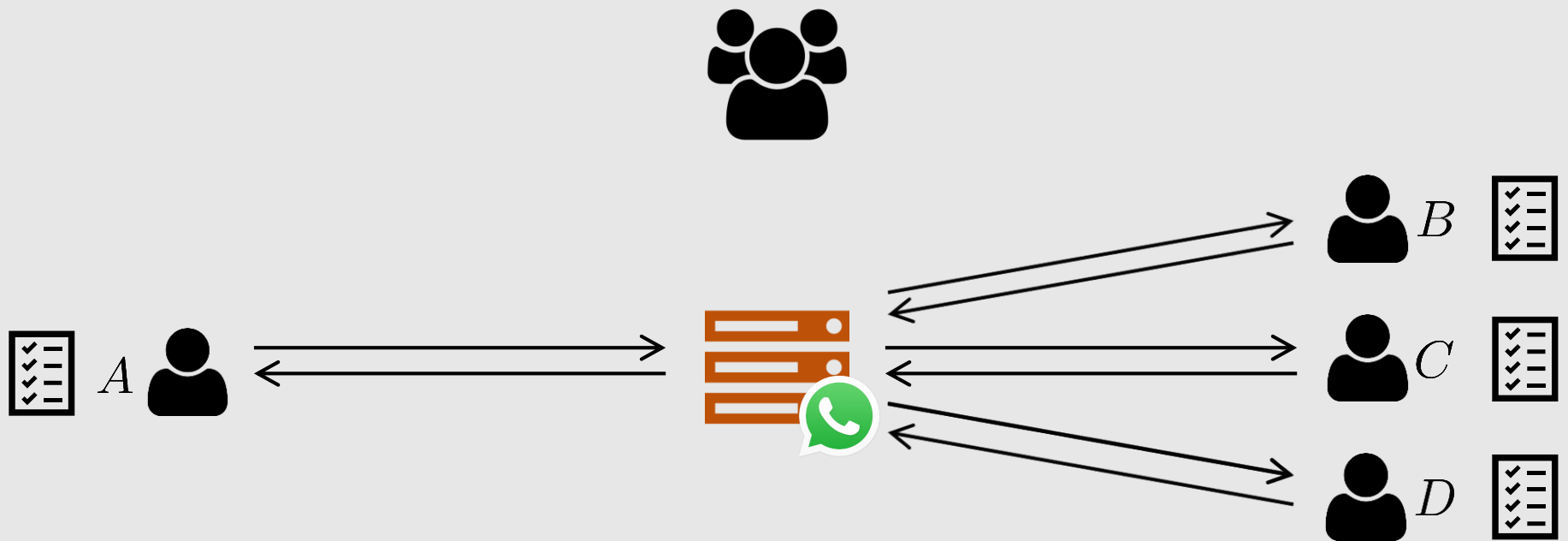


Sender in group?  
& Receiver in group!



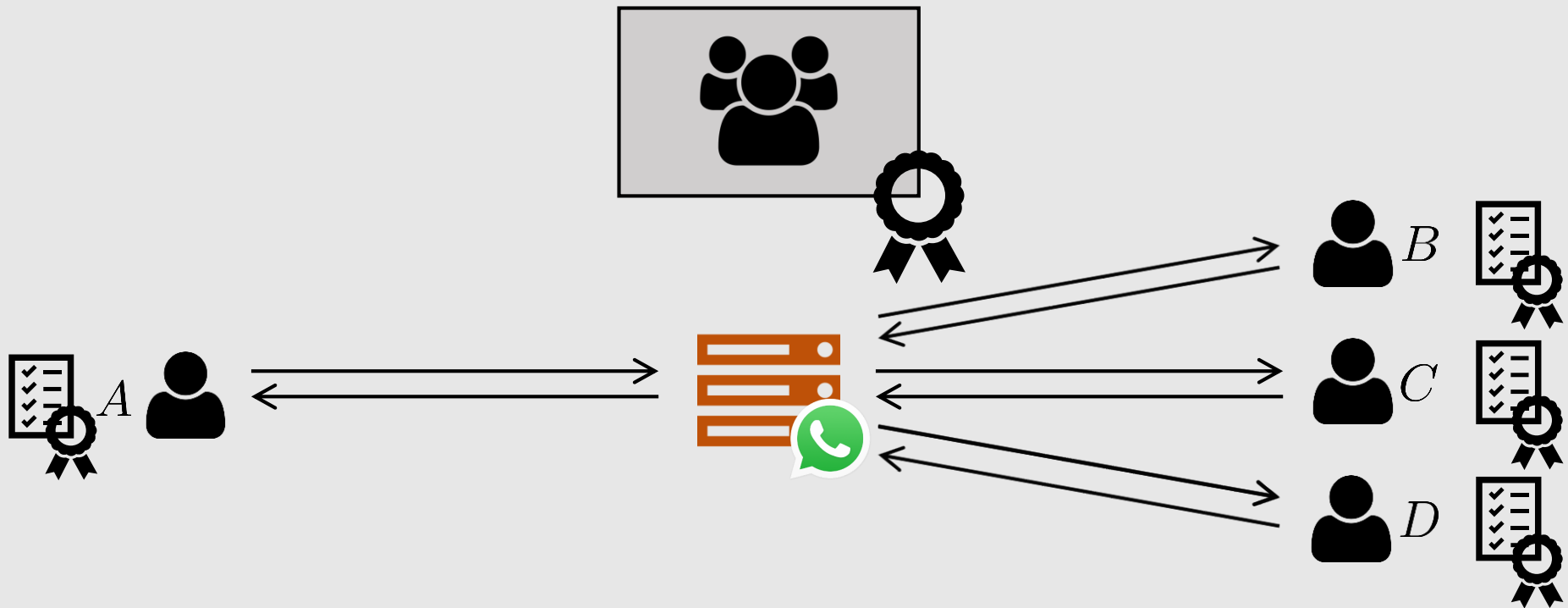
# Protocol Overview: WhatsApp

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

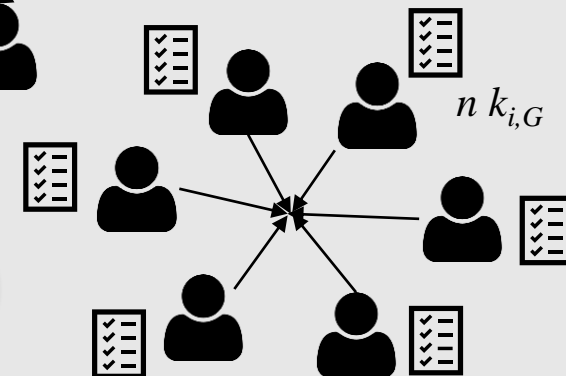
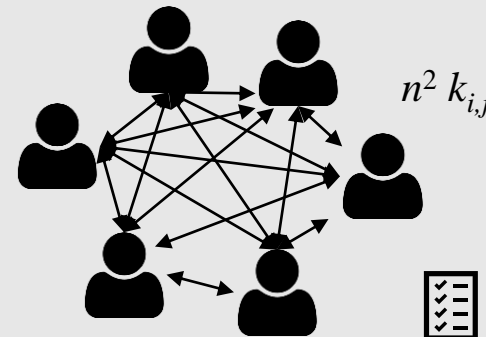
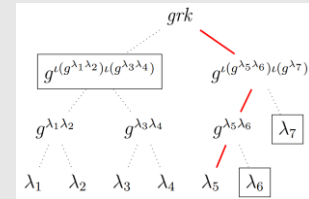
→ Group management PCS:

- 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:

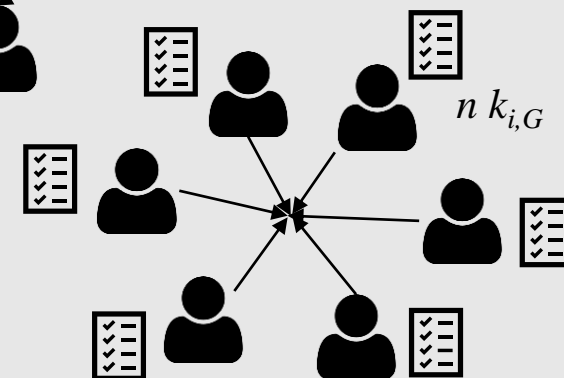
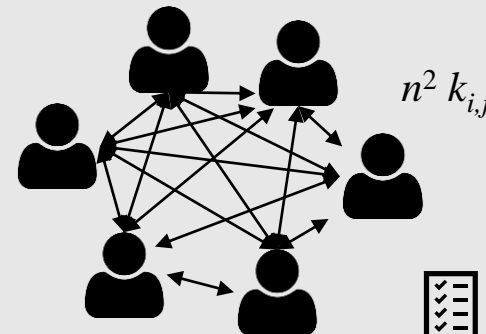
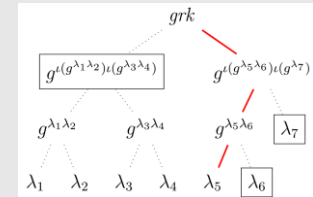
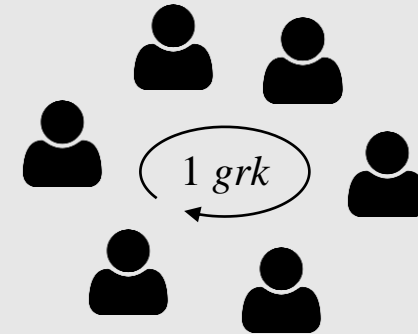
- Ticket approach

→ Related to group key exchange

- Guest list approach

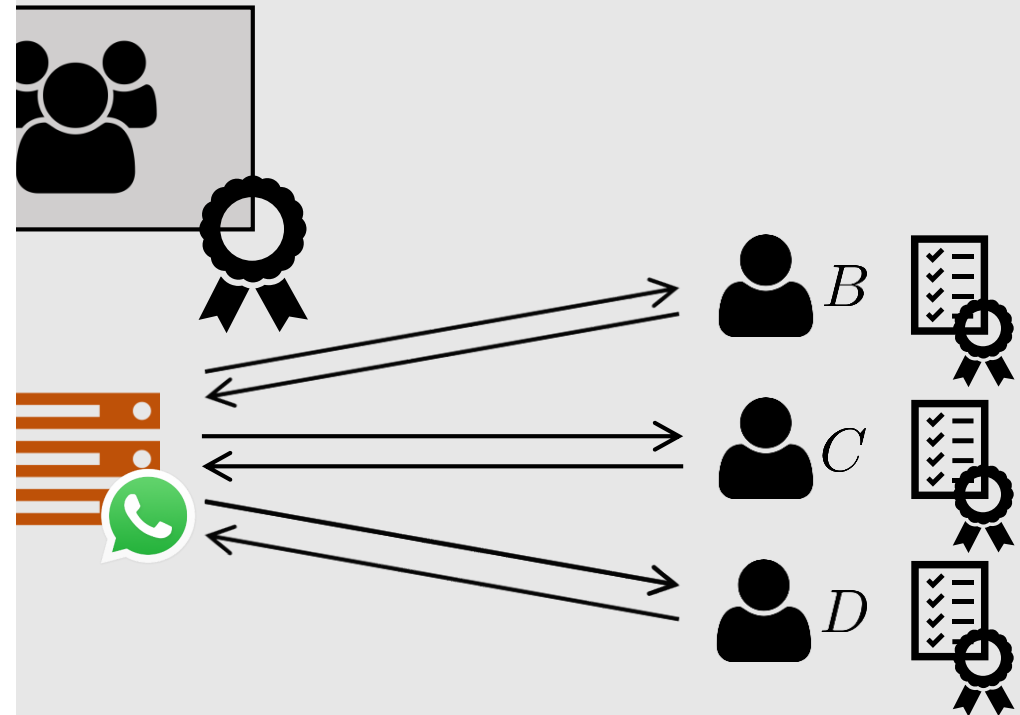
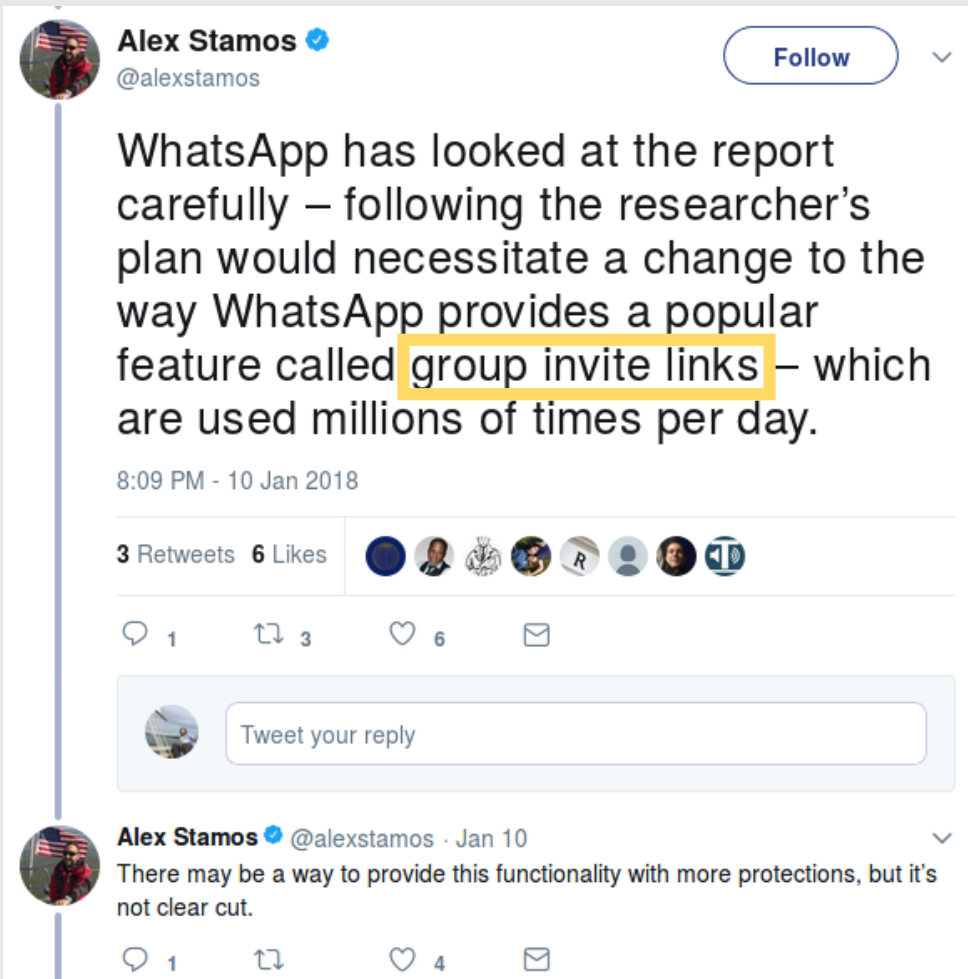
→ No complex group key ratcheting

→ Problems in asynchronous federated environment



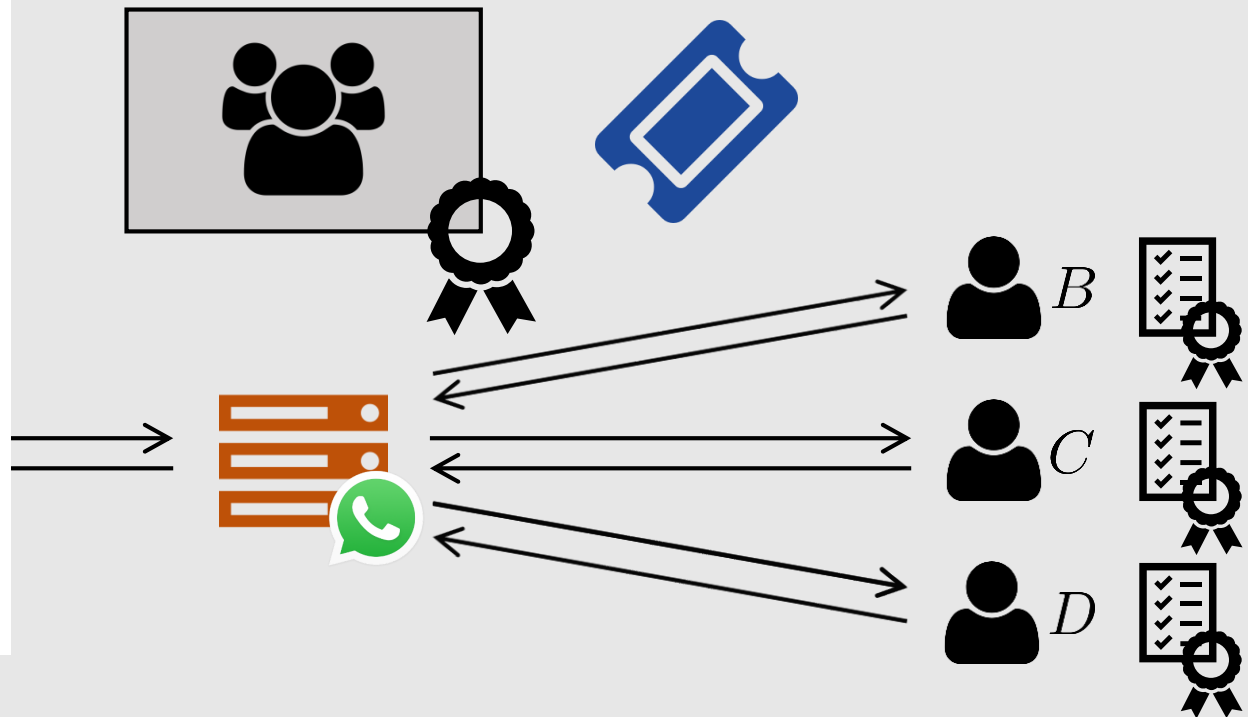
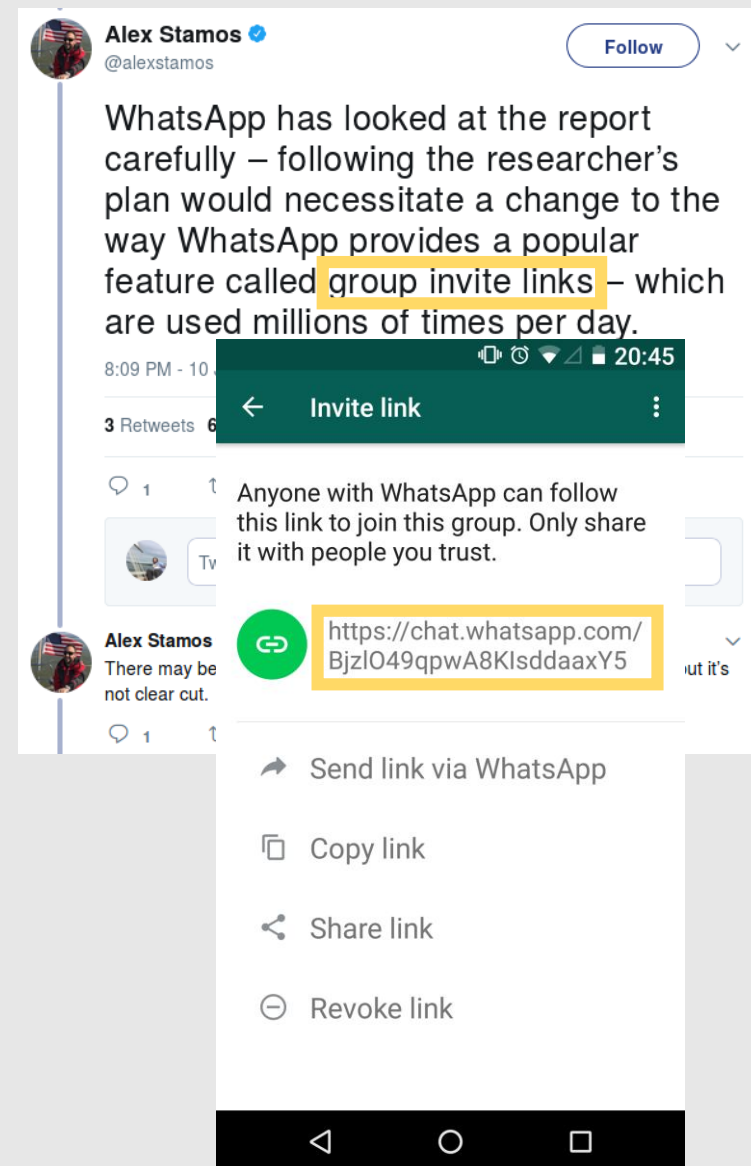
# Protocol Overview: WhatsApp

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:

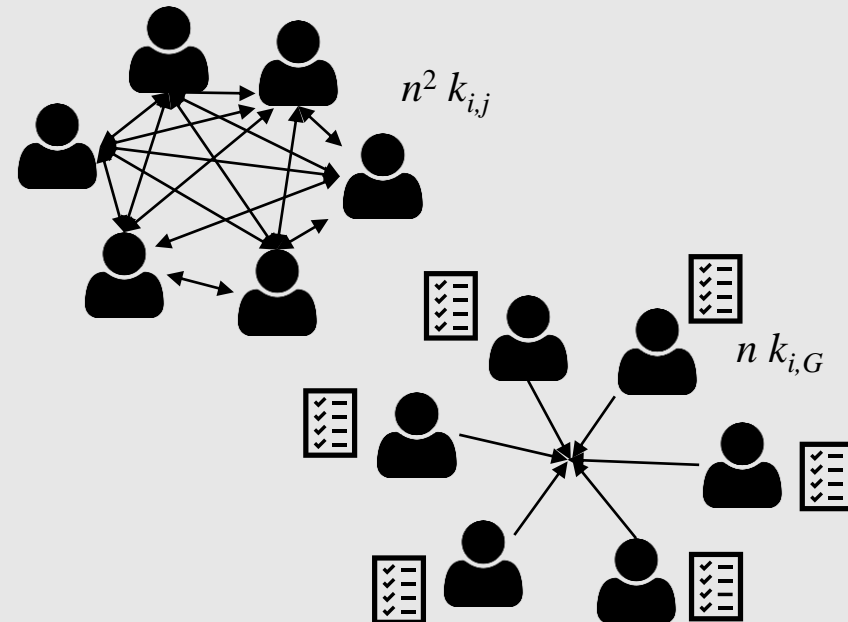
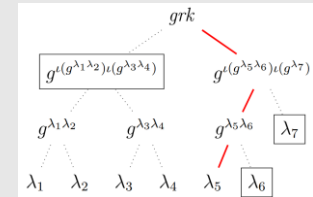
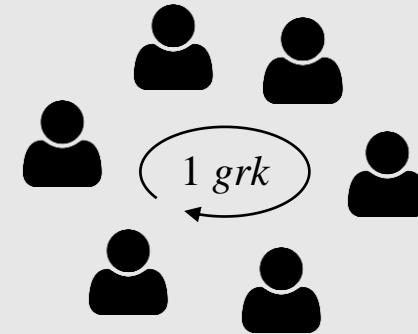
- Ticket approach

→ 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

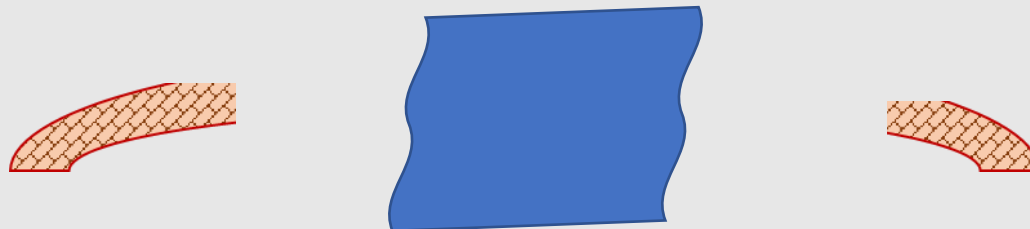
Security Model  
Reliability vs. Instant Messaging  
PCS and Ratcheting  
**Asynchronous Group IM**

## Practice

- Dynamic group IM

## Theory

- Dynamic group key exchange



# Complexity of Dynamic Groups in Asynchronous Networks

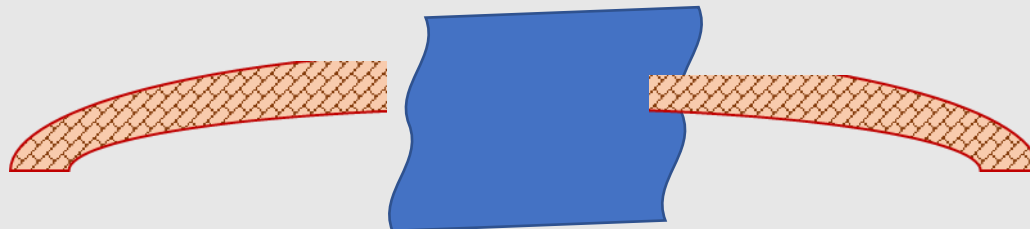
Security Model  
Reliability vs. Instant Messaging  
PCS and Ratcheting  
**Asynchronous Group IM**

## Practice

- Dynamic group IM
- Ratcheting
- Concurrency

## Theory

- Dynamic group key exchange
- Static group key ratcheting



# Complexity of Dynamic Groups in Asynchronous Networks

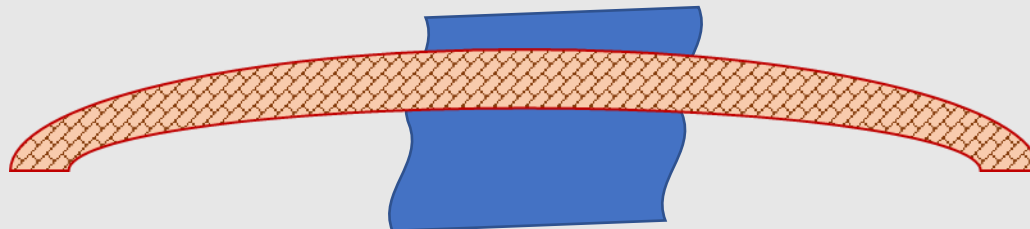
Security Model  
Reliability vs. Instant Messaging  
PCS and Ratcheting  
**Asynchronous Group IM**

## 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

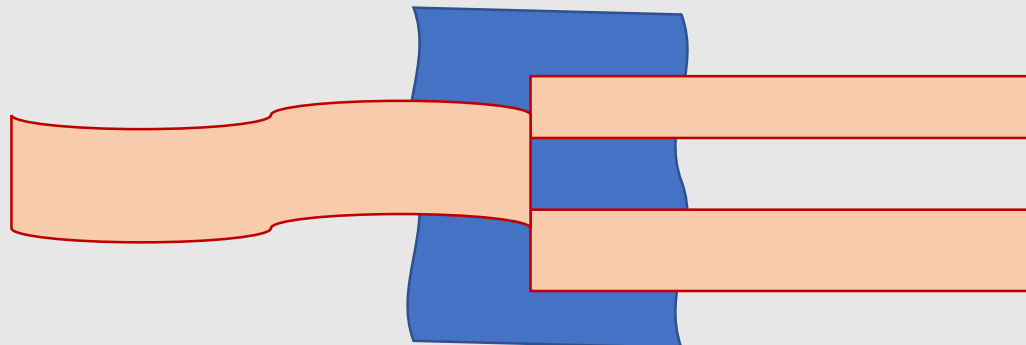
Security Model  
Reliability vs. Instant Messaging  
PCS and Ratcheting  
**Asynchronous Group IM**

## 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 delivery

- Trace delivery

## Theory

- Dynamic group key exchange

- Synchronous communication

- Static group key ratcheting

- No concurrency

- Definition of reliability

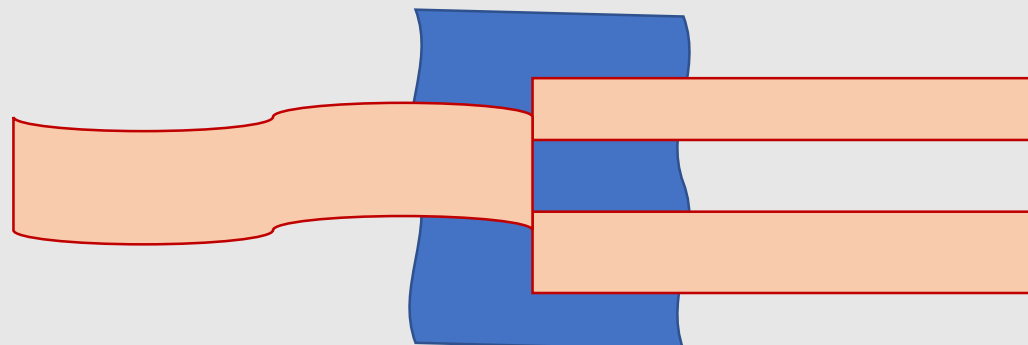
- Incompatible with IM

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

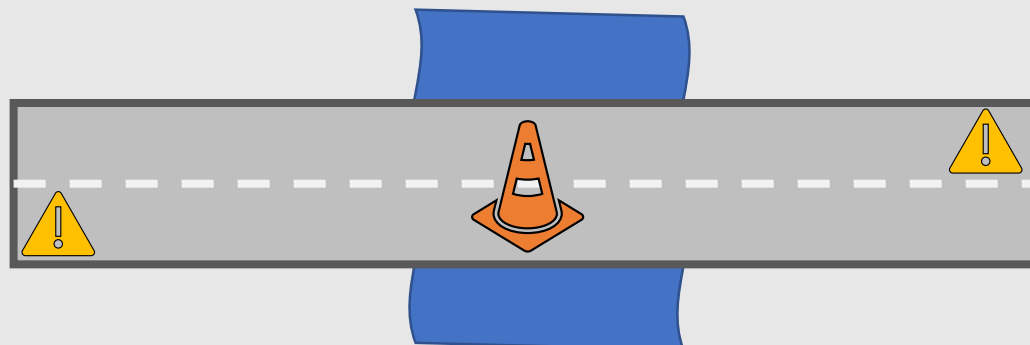
- Incompatible with IM

We

- Propose a model capturing relevant security notions

- Analyzed real world w.r.t. to this model

- Propose measures for enhancing real world



# Complexity of Dynamic Groups in Asynchronous Networks

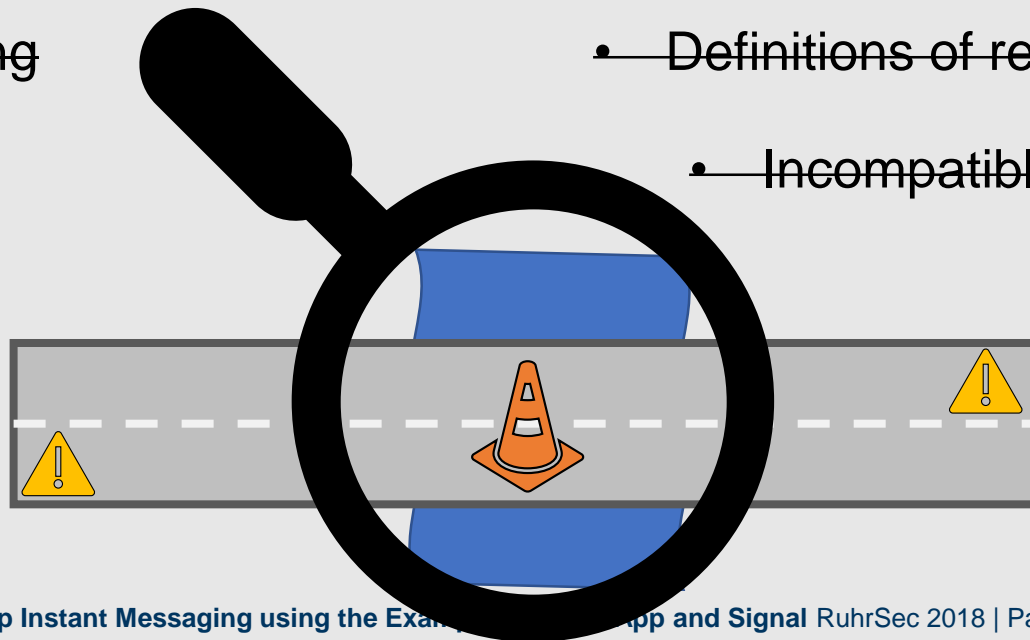
Security Model  
Reliability vs. Instant Messaging  
PCS and Ratcheting  
**Asynchronous Group IM**

## 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**

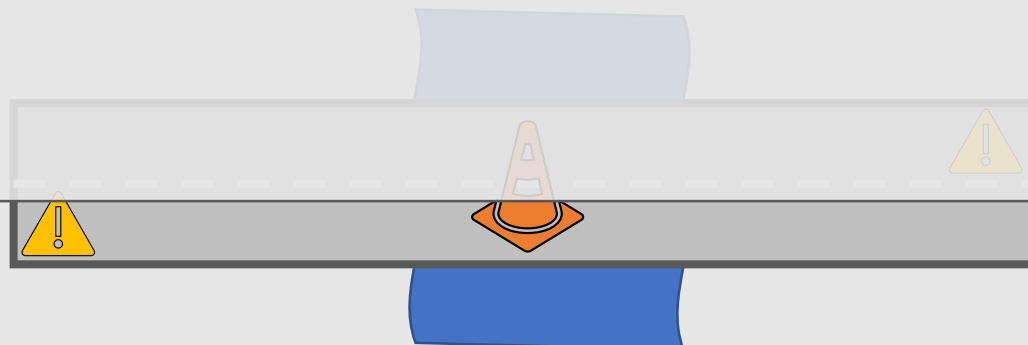
## Practice

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

## Theory

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

TLS ↔ Key Exchange + Channel  
(~ACCE?!)



# Complexity of Dynamic Groups in Asynchronous Networks

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

## Practice

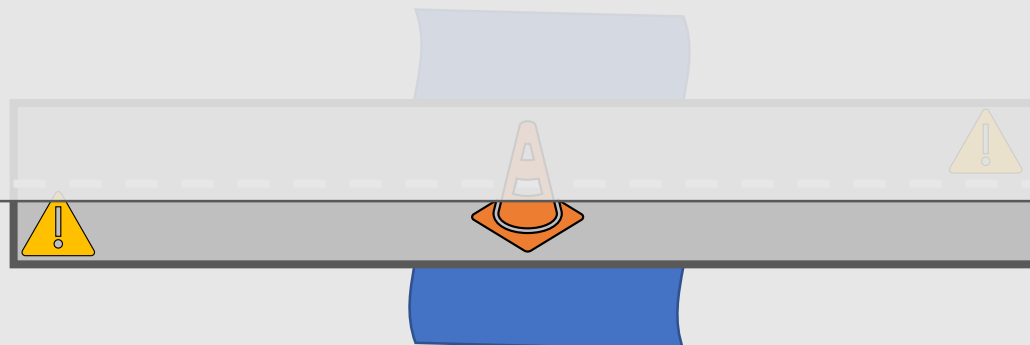
- Dynamic group IM
- Ratcheting
- ~~Concurrency~~
- ~~Special ordering~~
- ~~Trace delivery~~

## Theory

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

TLS  $\leftrightarrow$  Key Exchange + Channel  
(~ACCE?!)

MLS  $\leftrightarrow$  Group KE + Channel (+ 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~~ ⇒ Formulate ideal world before real world is fixed...

## Theory

- Dynamic group key exchange

TLS ↔ Key Exchange + Synchronous communication

(~ACCE?!)

- ~~Static group key ratcheting~~

MLS ↔ Group KE + Channel (+ Reliability?)








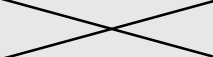




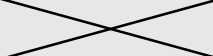




+ ...?!

- ~~Definitions of reliability~~



# 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:








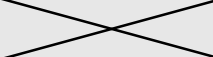




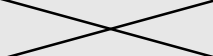




	Closeness	Forward Secrecy	Future Secrecy	Traceable Delivery	No Duplication	No Creation
						
						
						

[ia.cr/2017/713](https://ia.cr/2017/713)

@roeslpa

# 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
						
						
						

- Probably not the only protocol/implementation weaknesses
- Signal still **very** secure! WhatsApp brought E2E encryption to  $10^9$  users!

[ia.cr/2017/713](https://ia.cr/2017/713)

@roeslpa