

# Loose Ends of the Wire



Finding the Ends in E2E Encryption

---

Matteo Scarlata, Kien Tuong Truong, Andreas Tsouloupas

matteo.scarlata@inf.ethz.ch

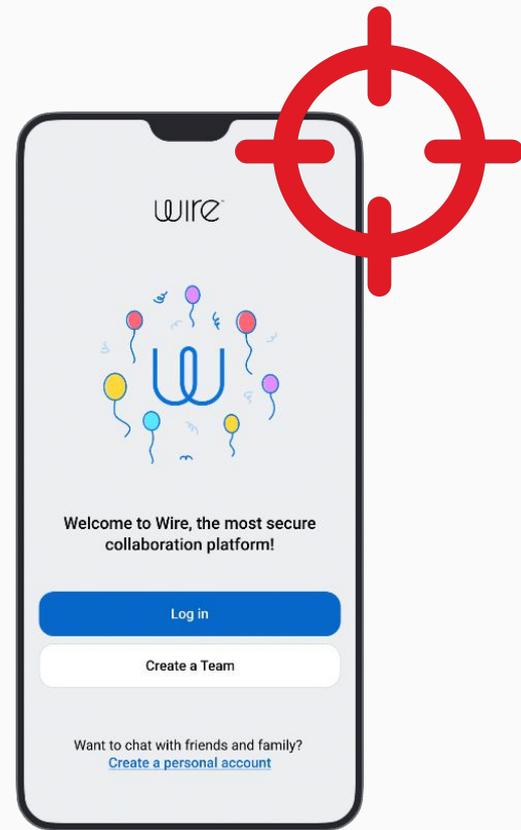
Applied Cryptography Group, D-INFK, ETH Zurich

- 1. Key Exchange +
- Messaging Channel +
- ???
- ???
- ???

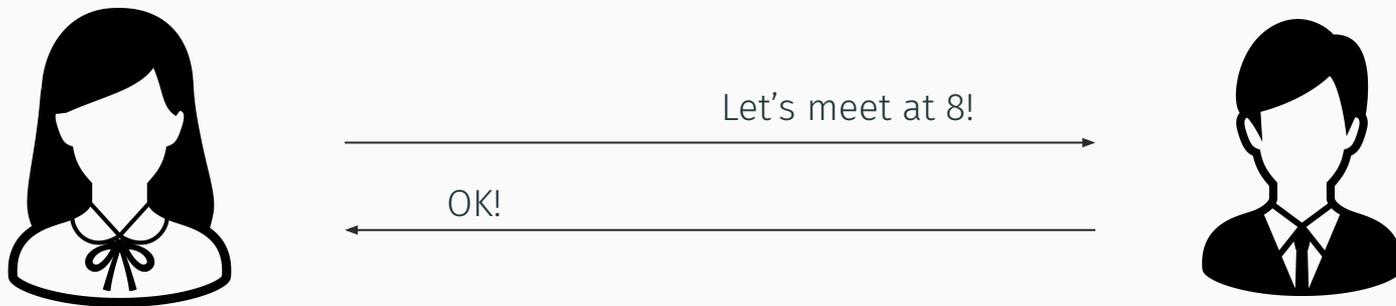
---

## Secure Messaging

2.

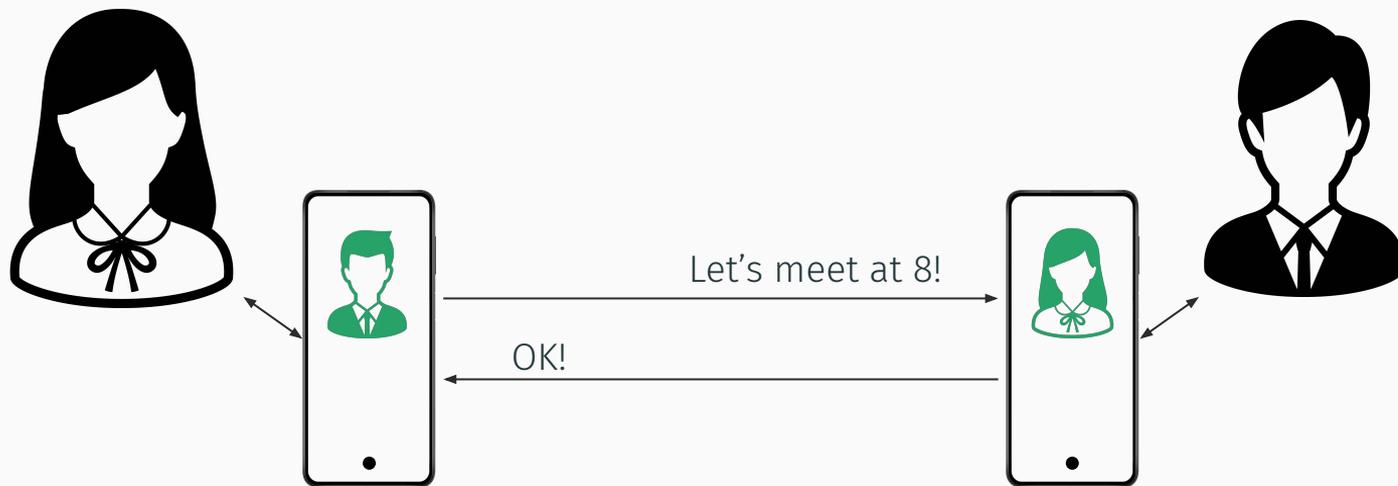


# End-to-End Security

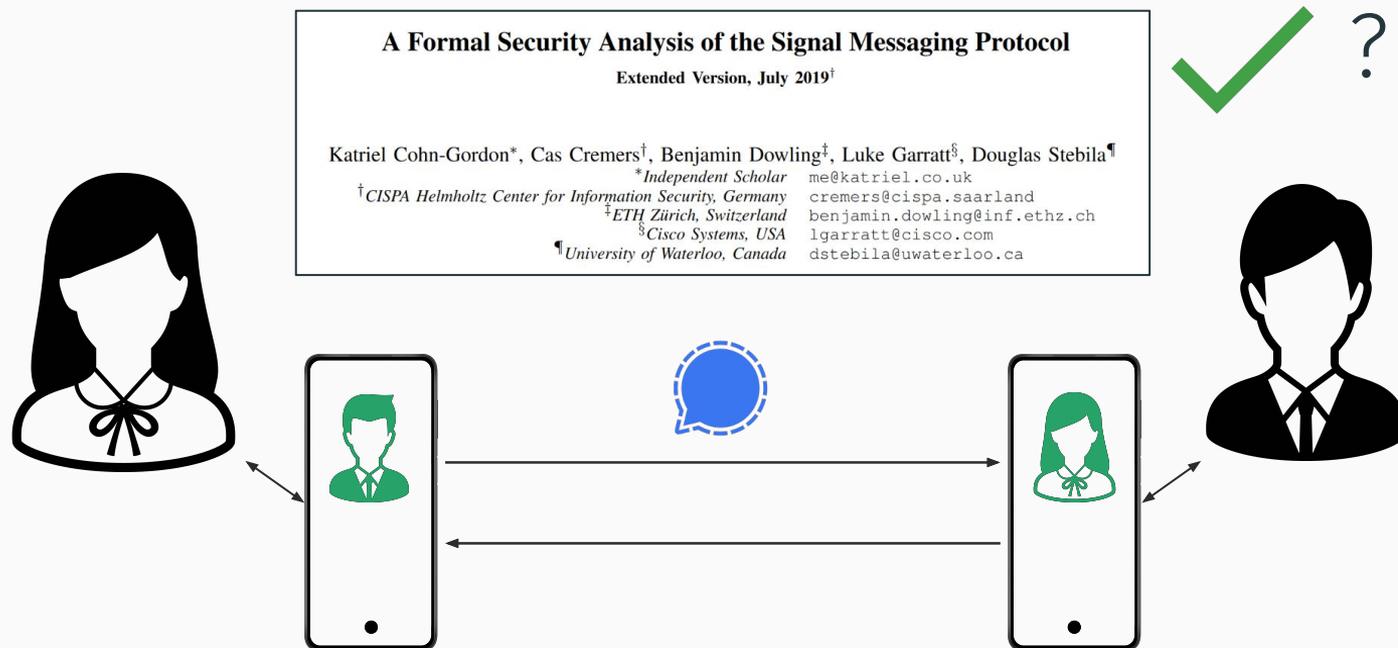


*“Only the end points should have access to the plaintext”*

# End-to-End Security: Secure Messaging



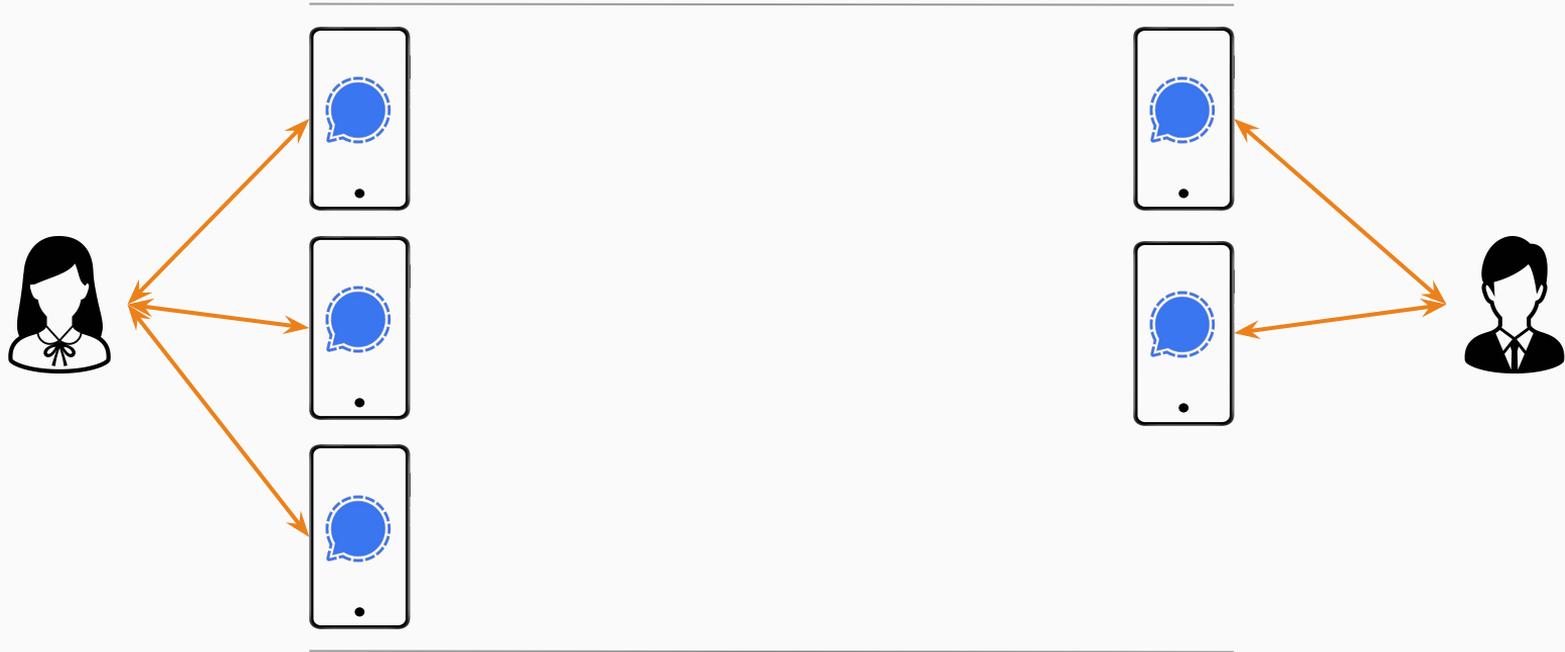
# End-to-End Security: Secure Messaging



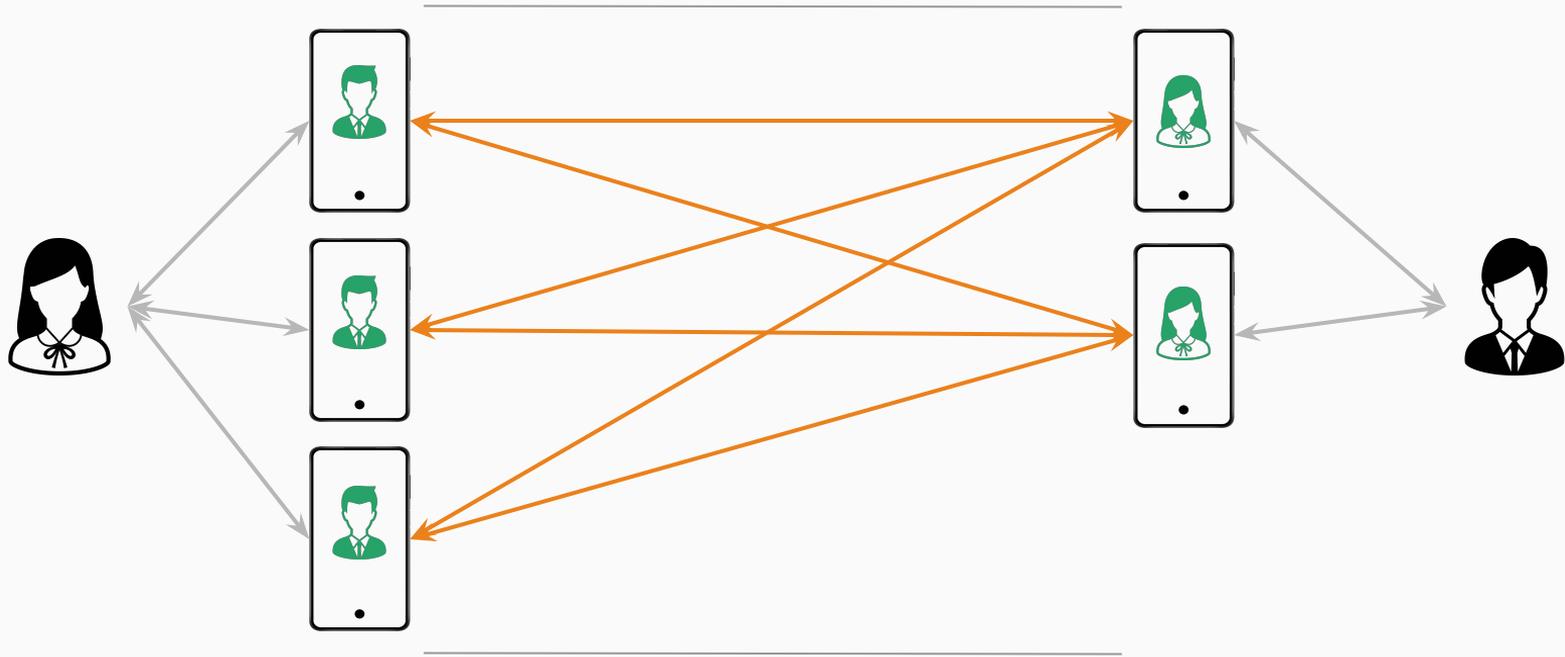
# Secure Messaging



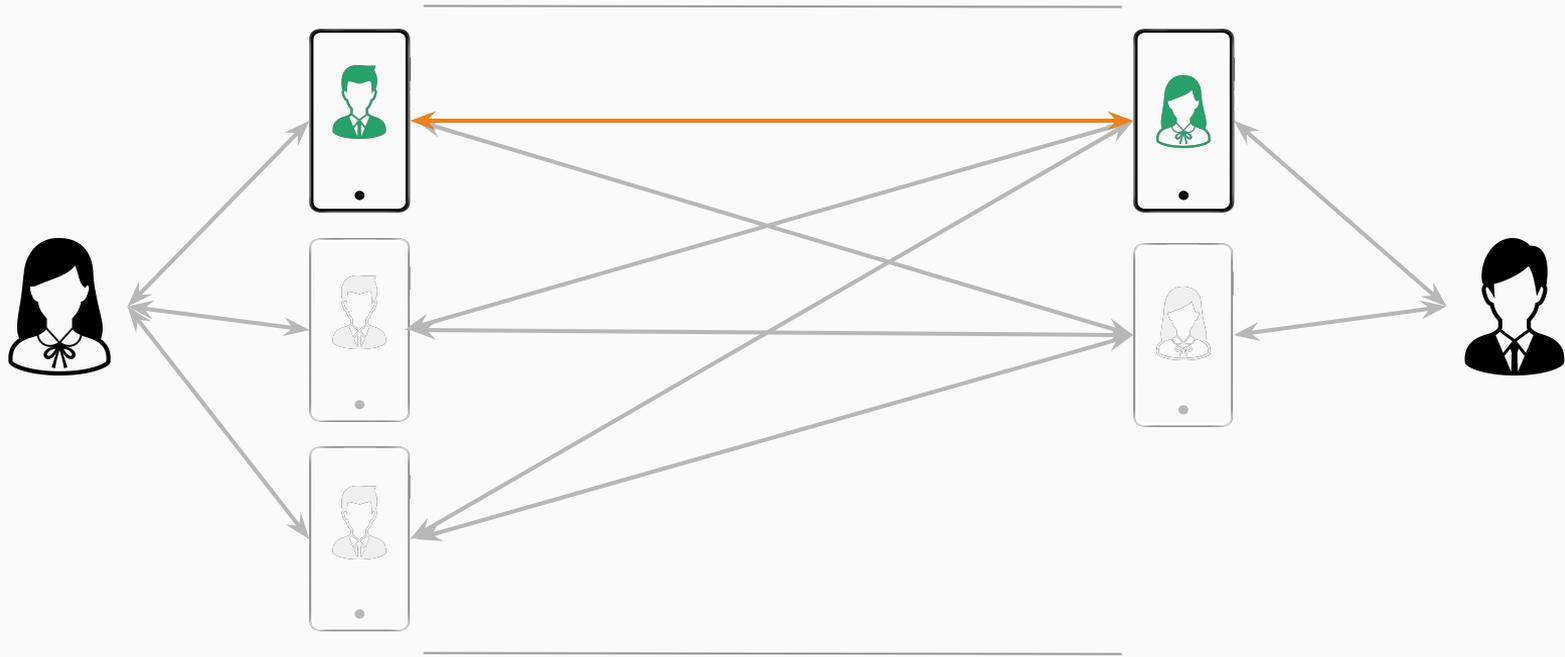
# UI



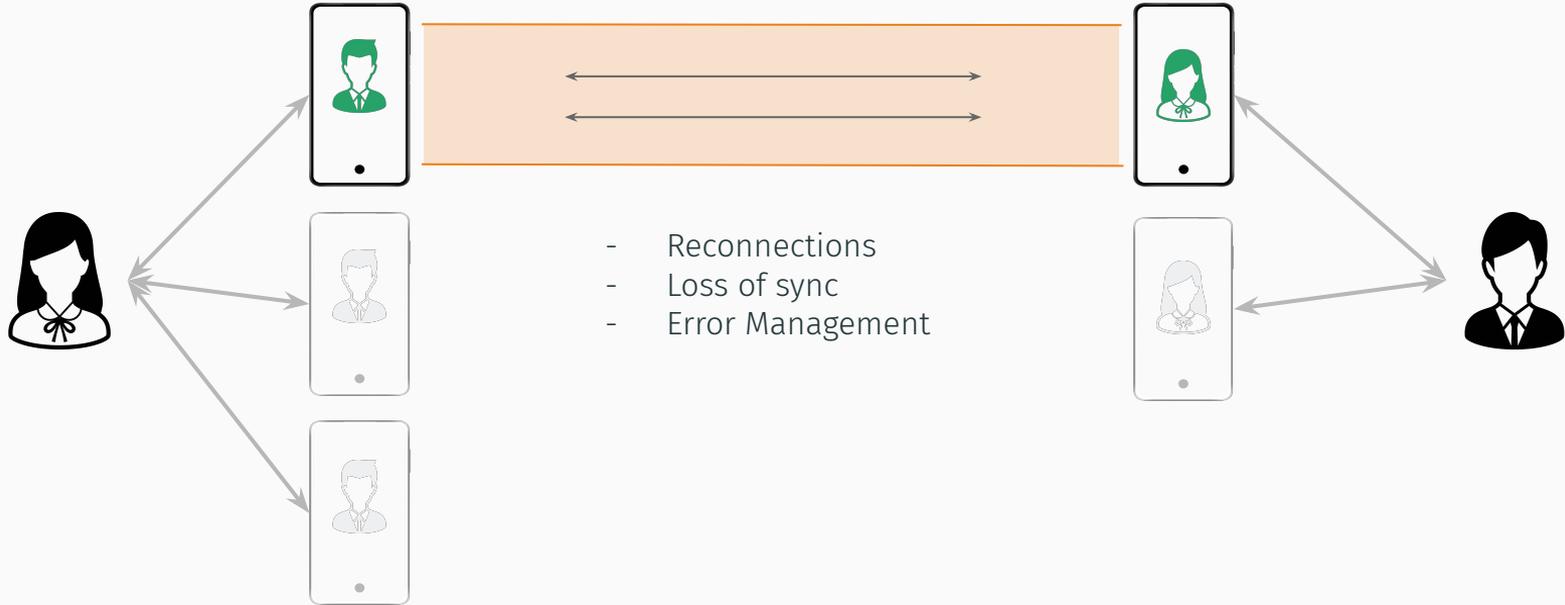
# Chat



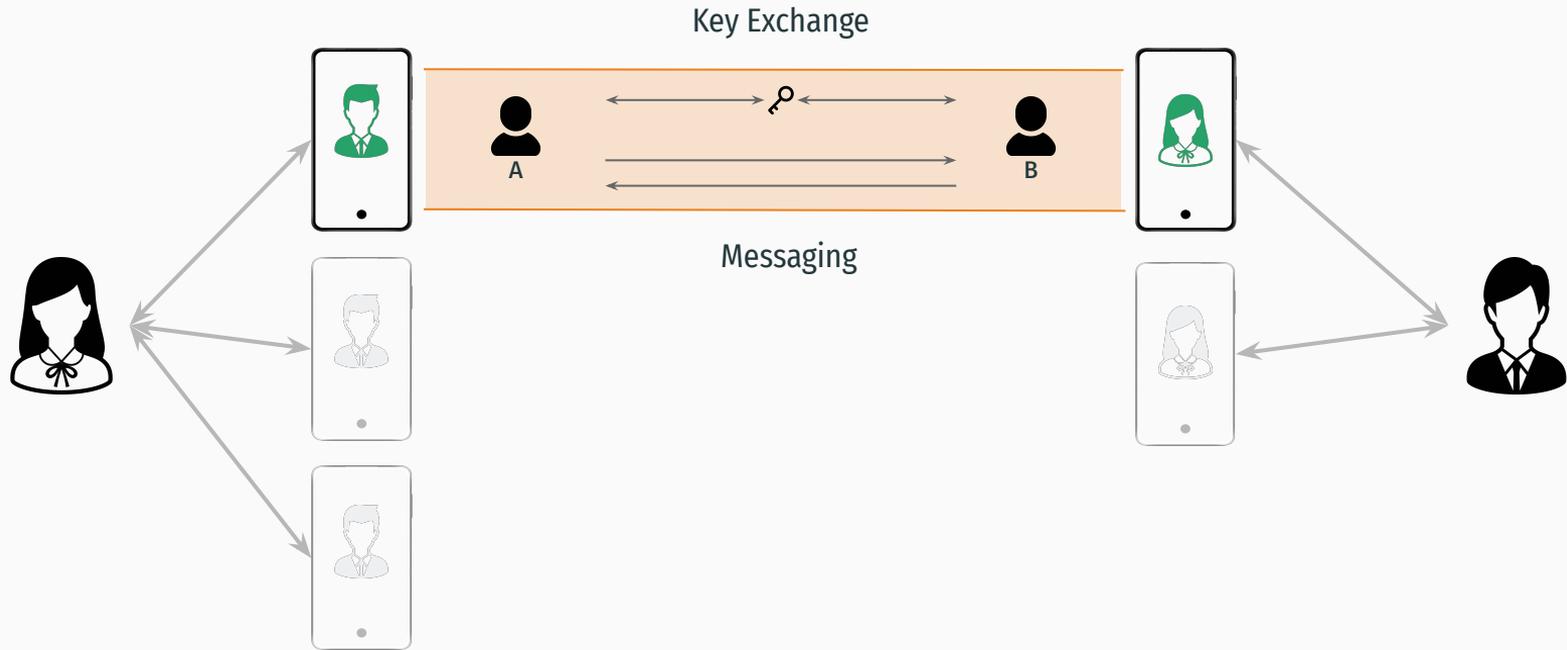
# Chat



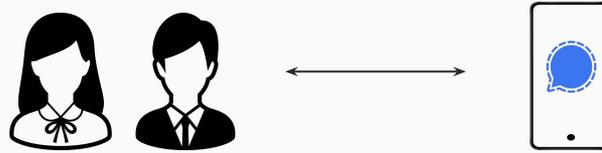
# Conversation



# Session

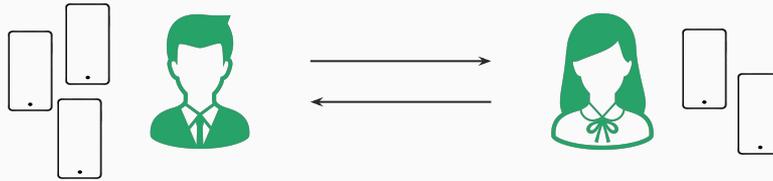


Signal.apk

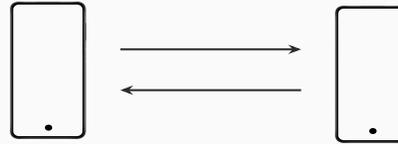


Client-side fan-out

Sender key

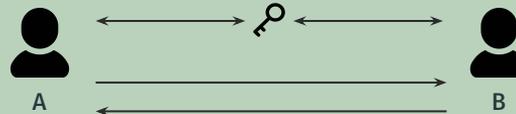


Sesame



X3DH

Double Ratchet



**A Formal Security Analysis of the Signal Messaging Protocol**

Extended Version, July 2019<sup>1</sup>

Katriel Cohn-Gordon<sup>\*</sup>, Cas Cremers<sup>†</sup>, Benjamin Dowling<sup>‡</sup>, Luke Garratt<sup>§</sup>, Douglas Stebila<sup>¶</sup>

<sup>\*</sup>Independent Scholar

<sup>†</sup>me@katriel.co.uk

<sup>‡</sup>CISPA Helmholtz Center for Information Security, Germany

<sup>§</sup>cremers@cispa.saarland

<sup>¶</sup>ETH Zürich, Switzerland

<sup>‡</sup>benjamin.dowling@inf.ethz.ch

<sup>§</sup>Cisco Systems, USA

<sup>§</sup>lgarratt@cisco.com

<sup>¶</sup>University of Waterloo, Canada

<sup>¶</sup>dstebla@uwaterloo.ca

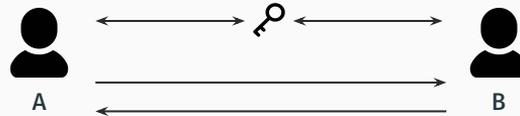
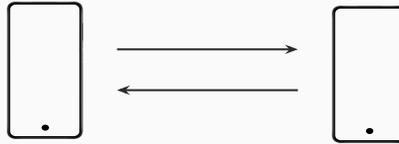
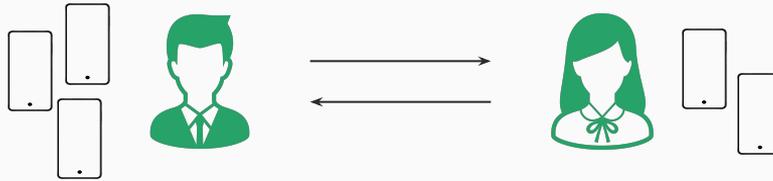
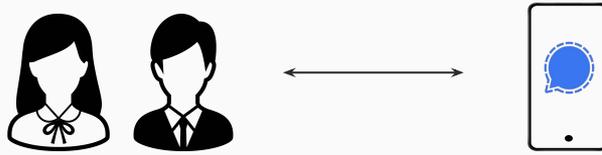
wire™



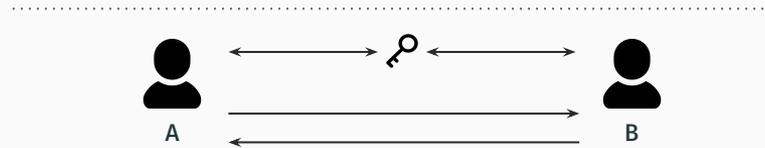
Deutscher Bundestag

*"Most of the world's G7 governments (5 out of 7) trust Wire to protect their communications"*

wire™



# Session



# The Case of Wire: Session Level - Key Exchange

“XPDH”



A

Initiator

$idk^A, idpk^A$

$ek^A, epk^A$

Responder

$idk^B, idpk^B$

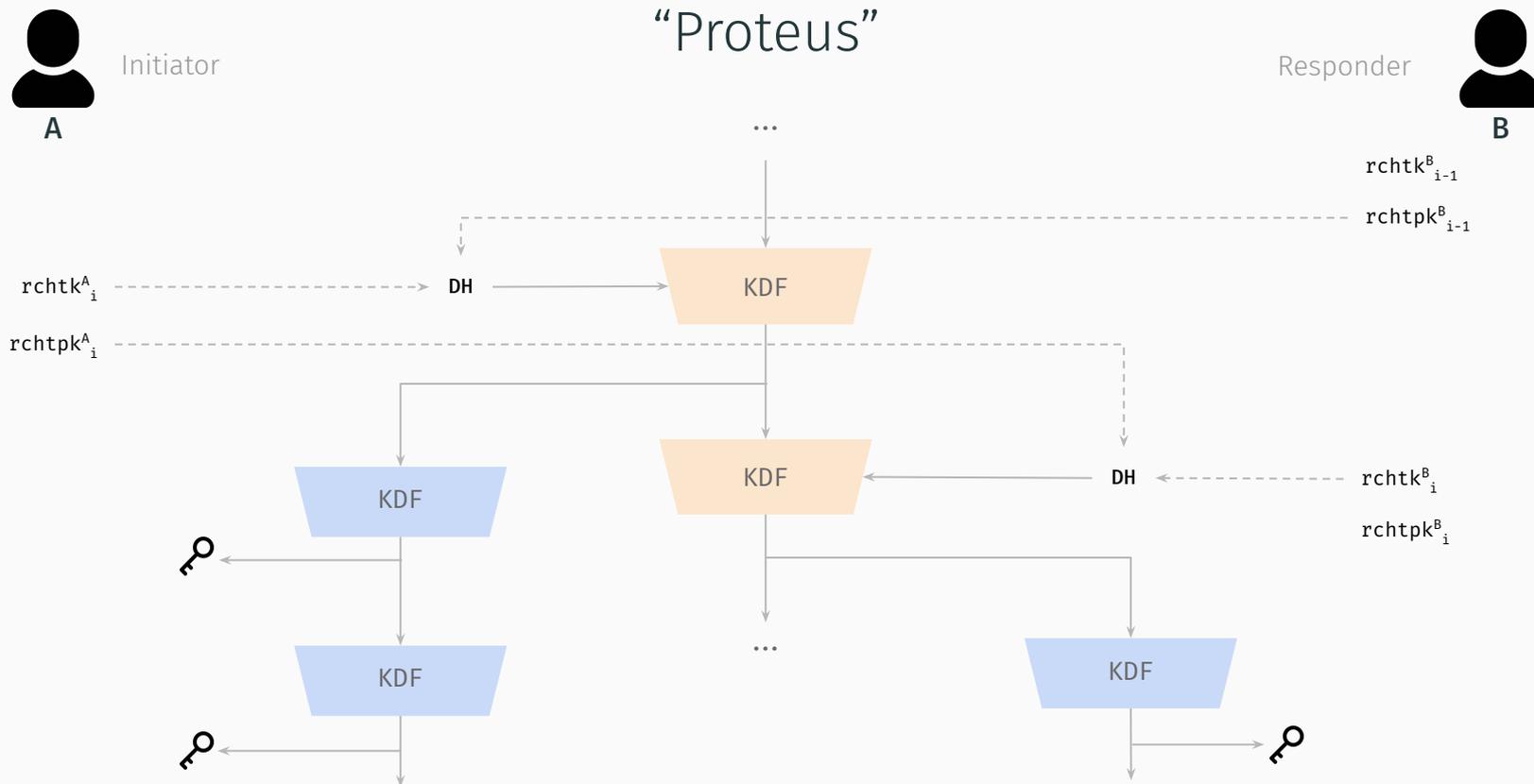
$prek^B, prepk^B_i$



B

$$K = DH(idk^A, prek^B) \parallel DH(ek^A, idpk^B) \parallel DH(ek^A, prepk^B)$$

# The Case of Wire: Session Level - Messaging



# The Case of Wire: Session Level

wire™



XPDH

≈

X3DH

Proteus

≈

Double Ratchet

## A Formal Security Analysis of the Signal Messaging Protocol

Extended Version, July 2019<sup>i</sup>

Katriel Cohn-Gordon\*, Cas Cremers<sup>†</sup>, Benjamin Dowling<sup>‡</sup>, Luke Garratt<sup>§</sup>, Douglas Stebila<sup>¶</sup>

<sup>\*</sup>Independent Scholar

me@katriel.co.uk

<sup>†</sup>CISPA Helmholtz Center for Information Security, Germany

cremers@cispa.saarland

<sup>‡</sup>ETH Zürich, Switzerland

benjamin.dowling@inf.ethz.ch

<sup>§</sup>Cisco Systems, USA

lgarratt@cisco.com

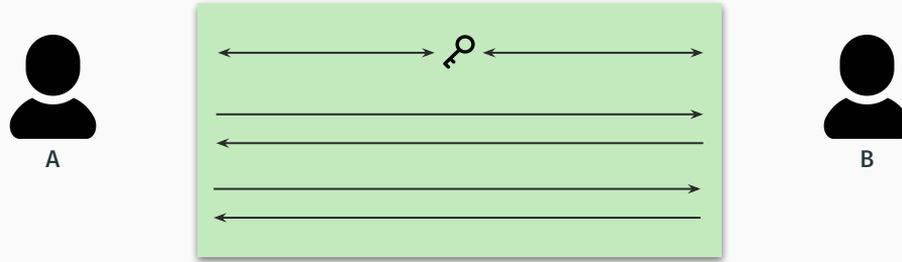
<sup>¶</sup>University of Waterloo, Canada

dstebila@uwaterloo.ca

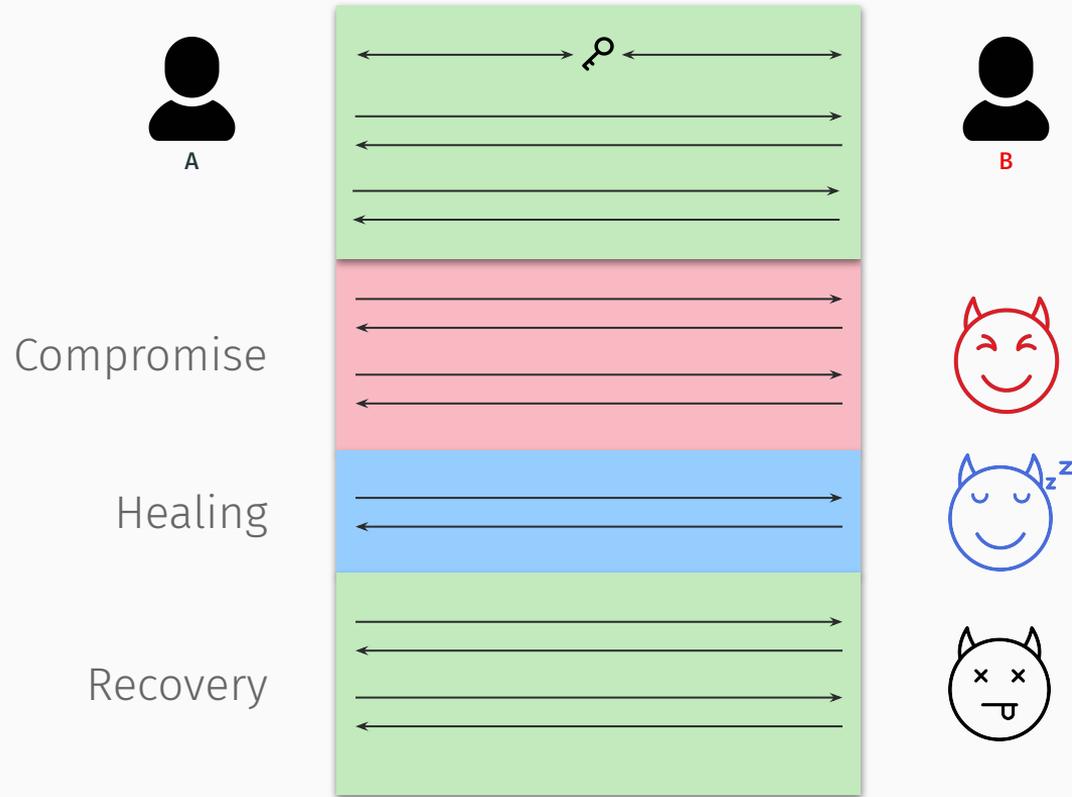


\*: prekeys not signed,  
no responder ephemerals

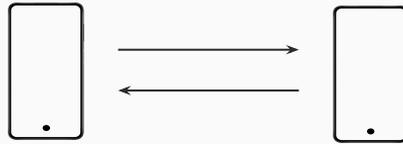
# Post-Compromise Security



# Post-Compromise Security



Conversation



Session



# The Case of Wire: Conversation Level

XPDH



PreKeyMessage

$\text{tag}_1, \text{idpk}^A, \#\text{prek}^B, \text{epk}^A$



→  $\text{tag}_1$ :

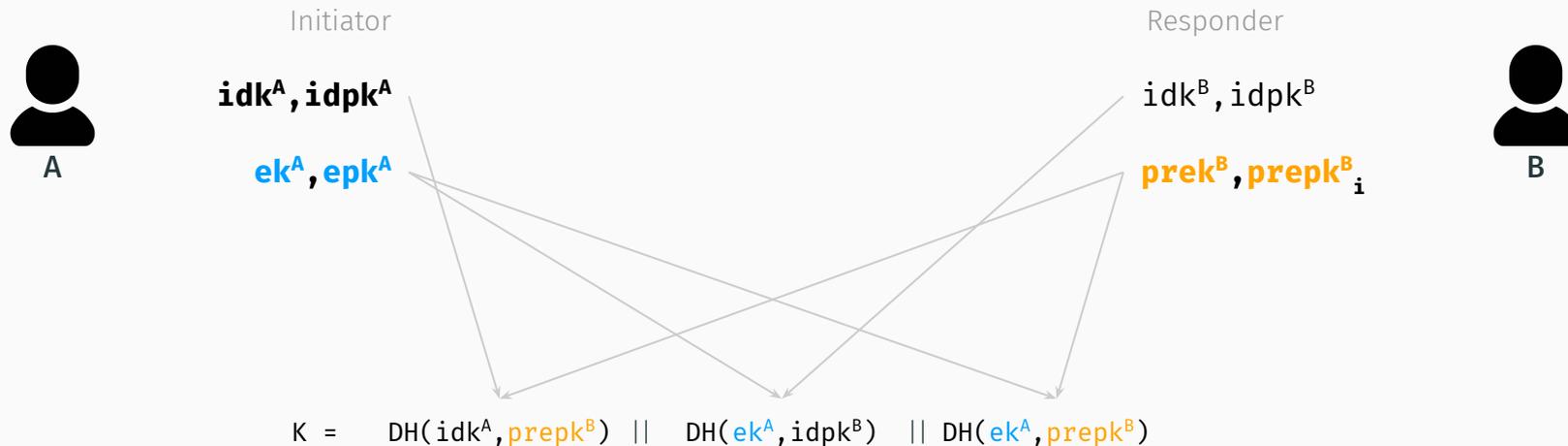


→  $\text{tag}_1$ :



# The Case of Wire: Session Level - Key Exchange

“XPDH”



# The Case of Wire: Conversation Level



CipherMessage

$tag_1$ , ctxt



# The Case of Wire: Conversation Level



# The Case of Wire: Conversation Level



PreKeyMessage

$tag_2, idpk^A, \#prek^B, epk^A$



# The Case of Wire: Conversation Level



CipherMessage

$tag_2, ctxt$



$tag_1$ :

→  $tag_2$ :

$tag_1$ :

→  $tag_2$ :

# The Case of Wire: Conversation Level



CipherMessage

$\text{tag}_1, \text{ctxt}$



$\text{tag}_1$ :

→  $\text{tag}_2$ :

$\text{tag}_1$ :

→  $\text{tag}_2$ :

# The Case of Wire: Conversation Level



CipherMessage

$tag_1, \text{ctxt}$



# The Case of Wire: Conversation Level



CipherMessage

$tag_1$ , ctxt



# The Case of Wire: Conversation Level



CipherMessage

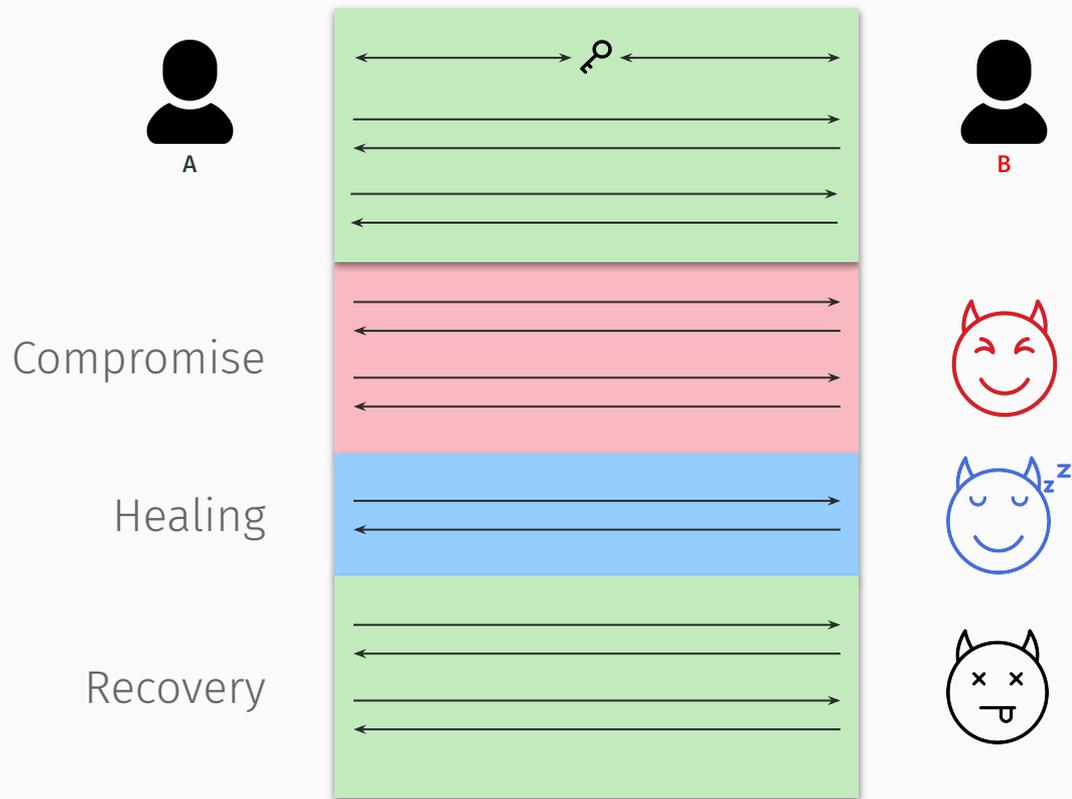
$tag_1$ , ctxt



# Session Security to Conversation Security



# Post-Compromise Security



# The Case of Wire: Post-Compromise Security



$idk^A, idpk^A$



$idk^B, idpk^B$



# The Case of Wire: Post-Compromise Security



$idk^A, idpk^A$



$idk^B, idpk^B$



# The Case of Wire: Post-Compromise Security



$idk^A, idpk^A$

→  $tag_1$ :



$idk^B, idpk^B$



→  $tag_1$ :



# The Case of Wire: Post-Compromise Security



# The Case of Wire: Post-Compromise Security



# The Case of Wire: Post-Compromise Security

## A Formal Security Analysis of the Signal Messaging Protocol

Extended Version, July 2019<sup>†</sup>

Katriel Cohn-Gordon\*, Cas Cremers<sup>‡</sup>, Benjamin Dowling<sup>‡</sup>, Luke Garratt<sup>§</sup>, Douglas Stebila<sup>¶</sup>

*\*Independent Scholar*

*me@katriel.co.uk*

<sup>†</sup>*CISPA Helmholtz Center for Information Security, Germany*

*cremers@cispa.saarland*

<sup>‡</sup>*ETH Zürich, Switzerland*

*benjamin.dowling@inf.ethz.ch*

<sup>§</sup>*Cisco Systems, USA*

*lgarratt@cisco.com*

<sup>¶</sup>*University of Waterloo, Canada*

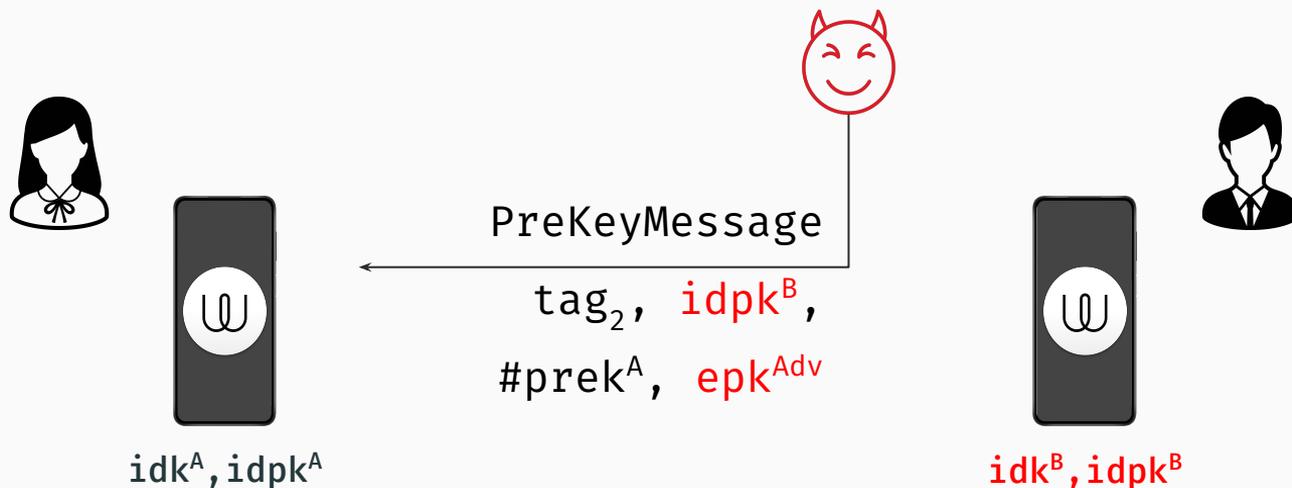
*dstebila@uwaterloo.ca*



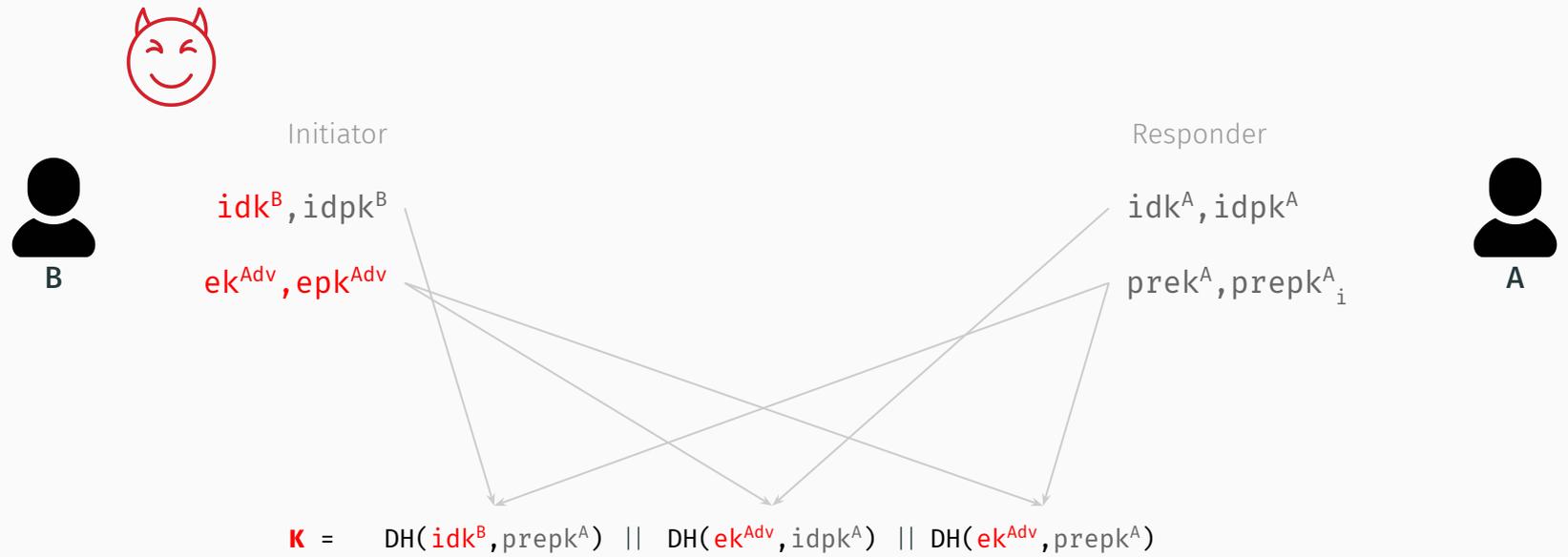
# The Case of Wire: Post-Compromise Security



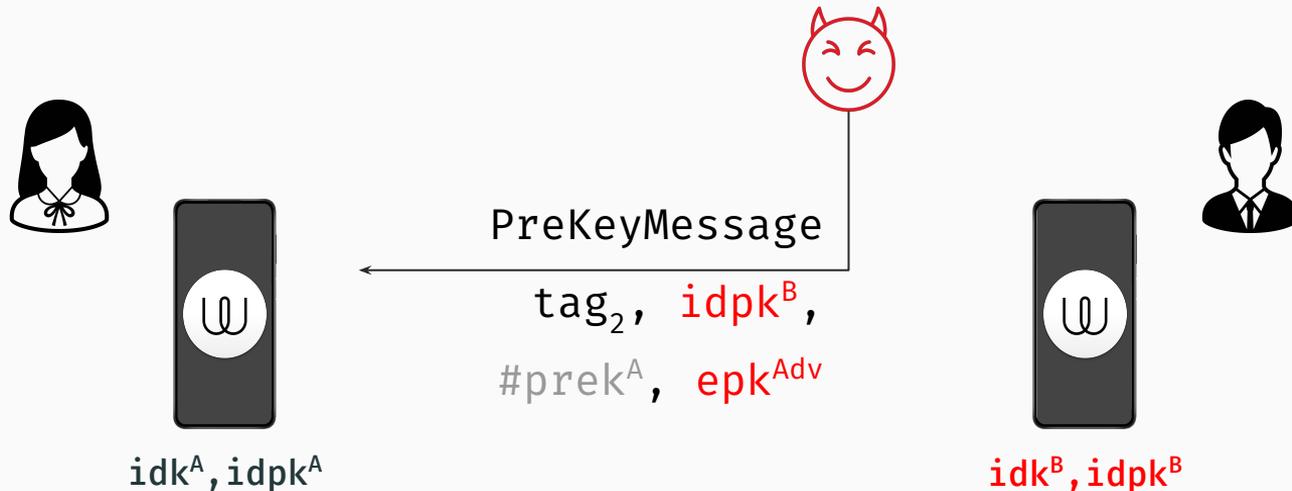
# The Case of Wire: Post-Compromise Security



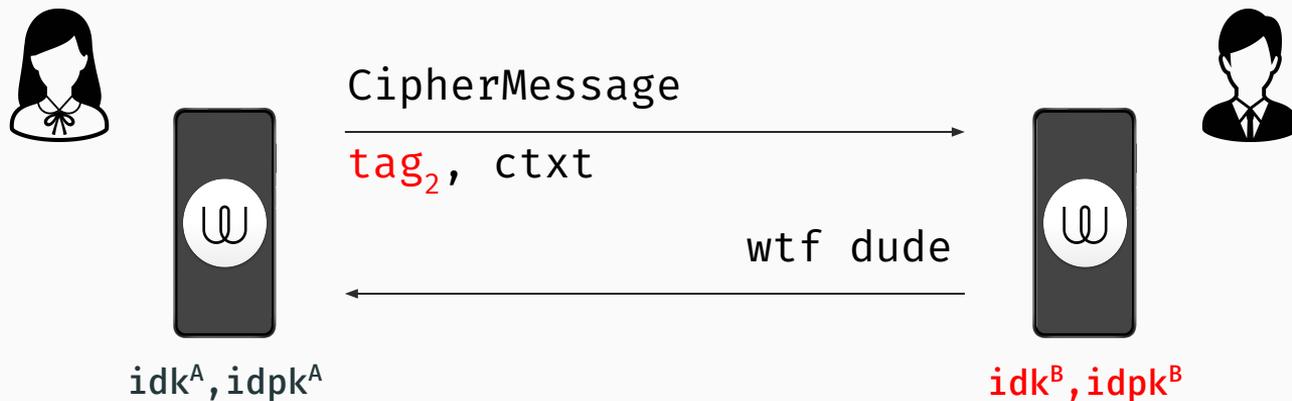
# Reminder: XPDH



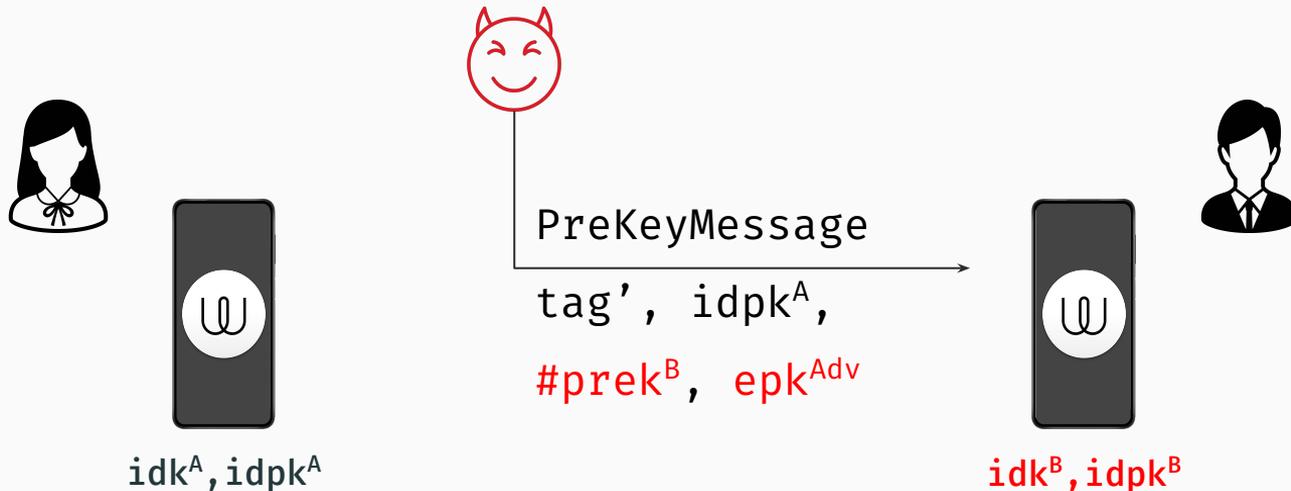
# The Case of Wire: Post-Compromise Security



# The Case of Wire: Post-Compromise Security



# The Case of Wire: Conversation Level PCS

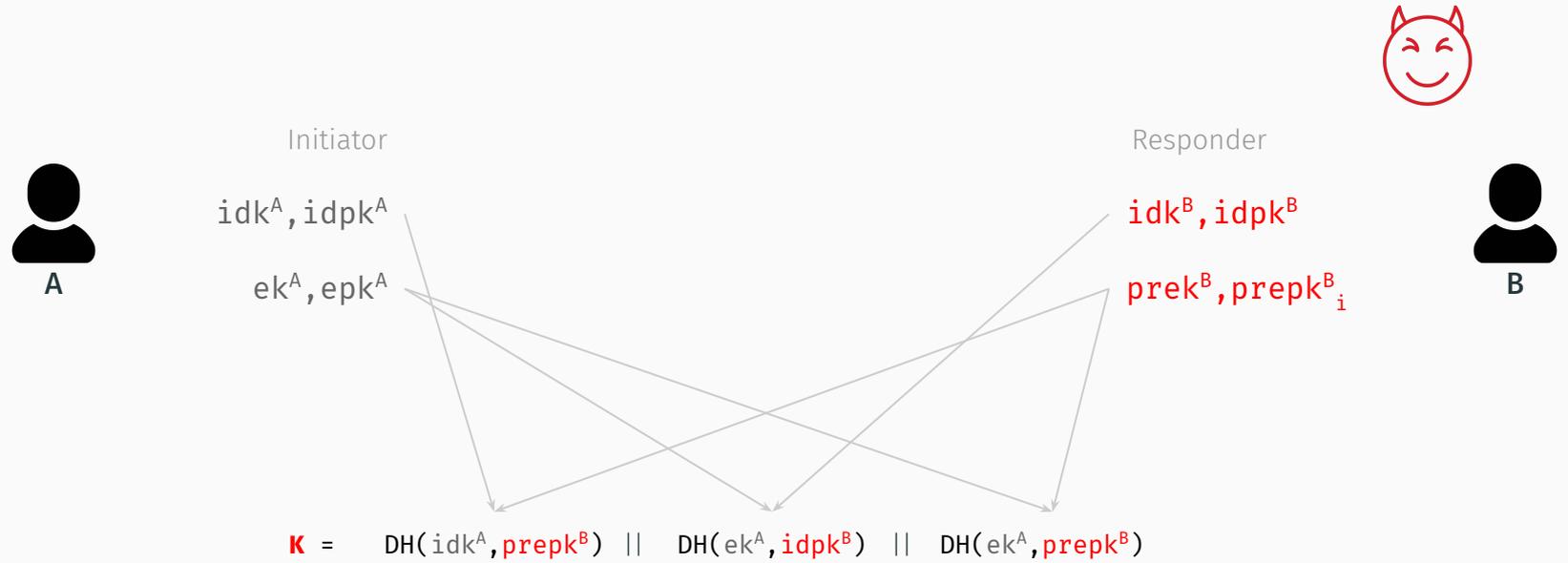


$tag_1$ : 

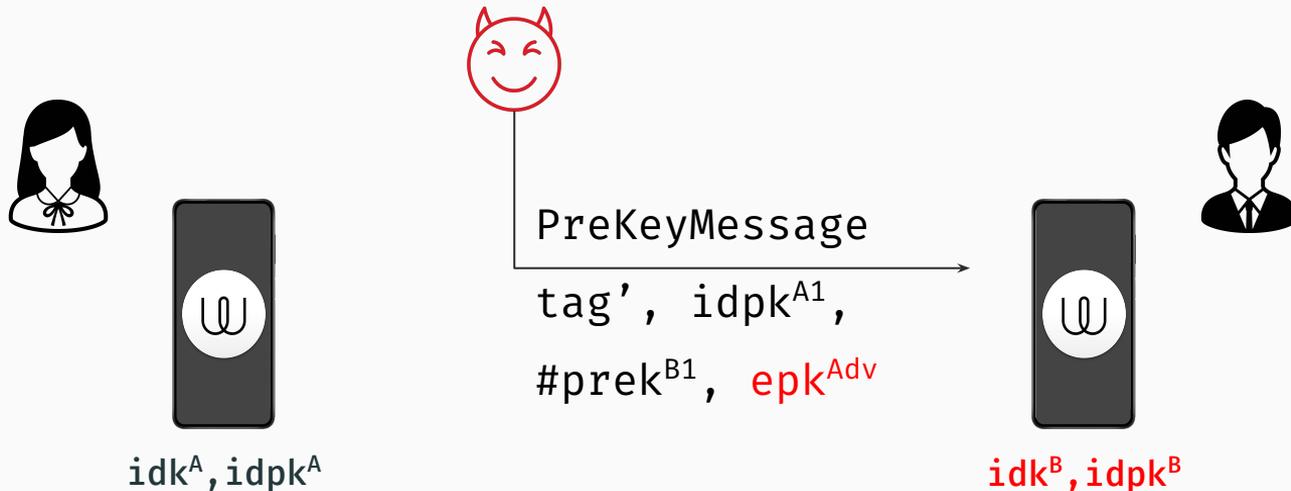
$\rightarrow tag_1$ : 

$\rightarrow tag_2$ : 

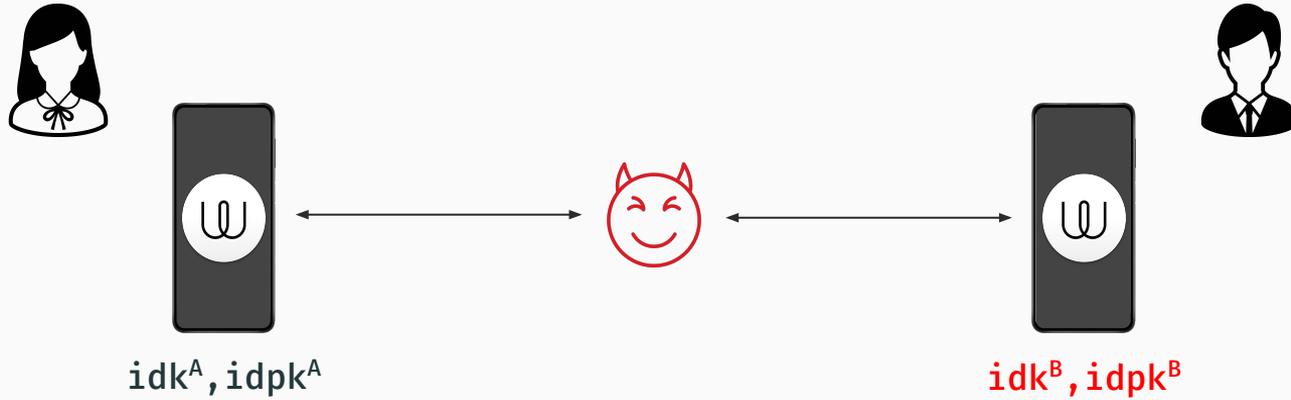
# Reminder: XPDH



# The Case of Wire: Conversation Level PCS



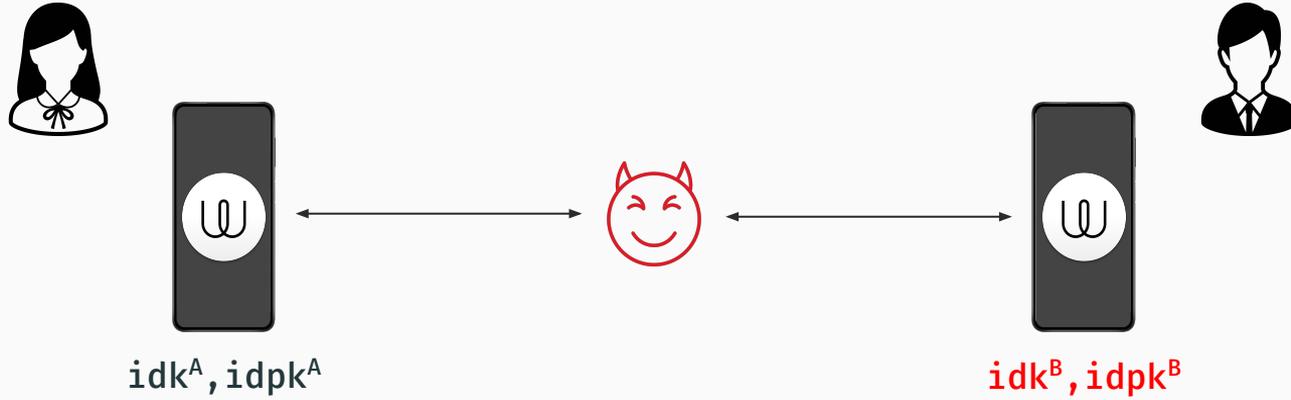
# The Case of Wire: Conversation Level PCS



# The Case of Wire: Conversation Level PCS



# The Case of Wire: Conversation Level PCS



# The Case of Wire: Conversation Level

XPDH

+

Proteus



**PCS**

# The Case of Wire: Conversation Level

VDDH

X3DH

+

DR

+

Sesame

⇓

**NO PCS\***

## Formal Analysis of Session-Handling in Secure Messaging: Lifting Security from Sessions to Conversations

February 20, 2023 - v2.0

Cas Cremers  
*CISPA Helmholtz Center for  
Information Security*  
Saarbrücken, Germany  
*cremers@cispa.de*

Charlie Jacomme\*  
*Inria Paris, France*  
*charlie.jacomme@inria.fr*

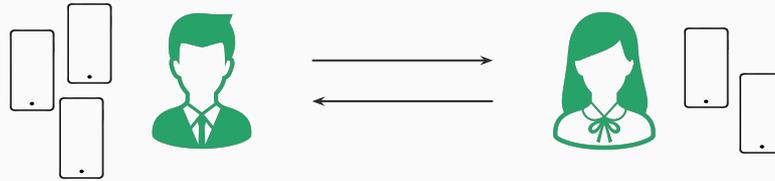
Aurora Naska  
*CISPA Helmholtz Center for  
Information Security*  
Universität des Saarlandes  
Saarbrücken, Germany  
*aurora.naska@cispa.de*

management

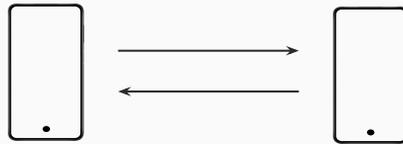
⇓

**NO PCS**

Chat



Conversation



Session

XPDH

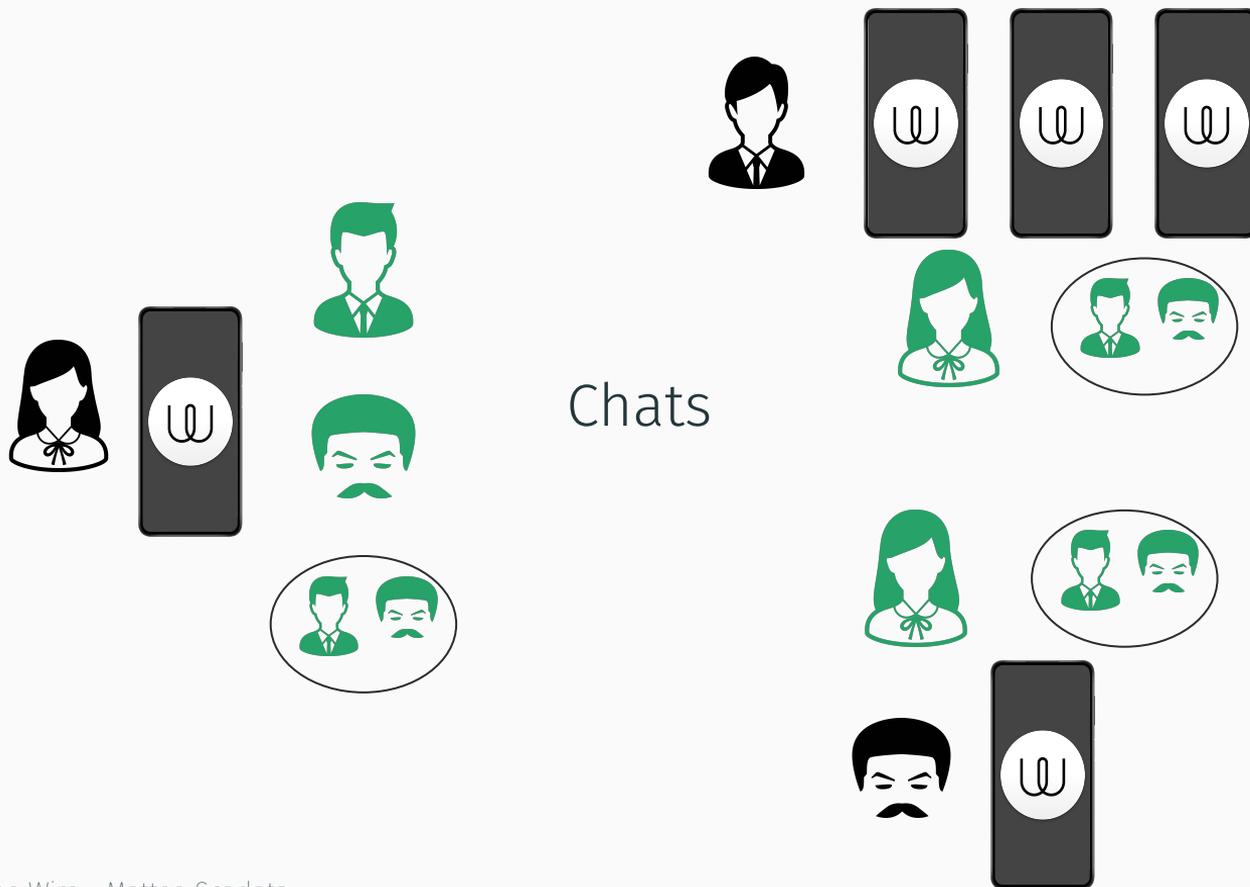


# The Case of Wire: Chat Level

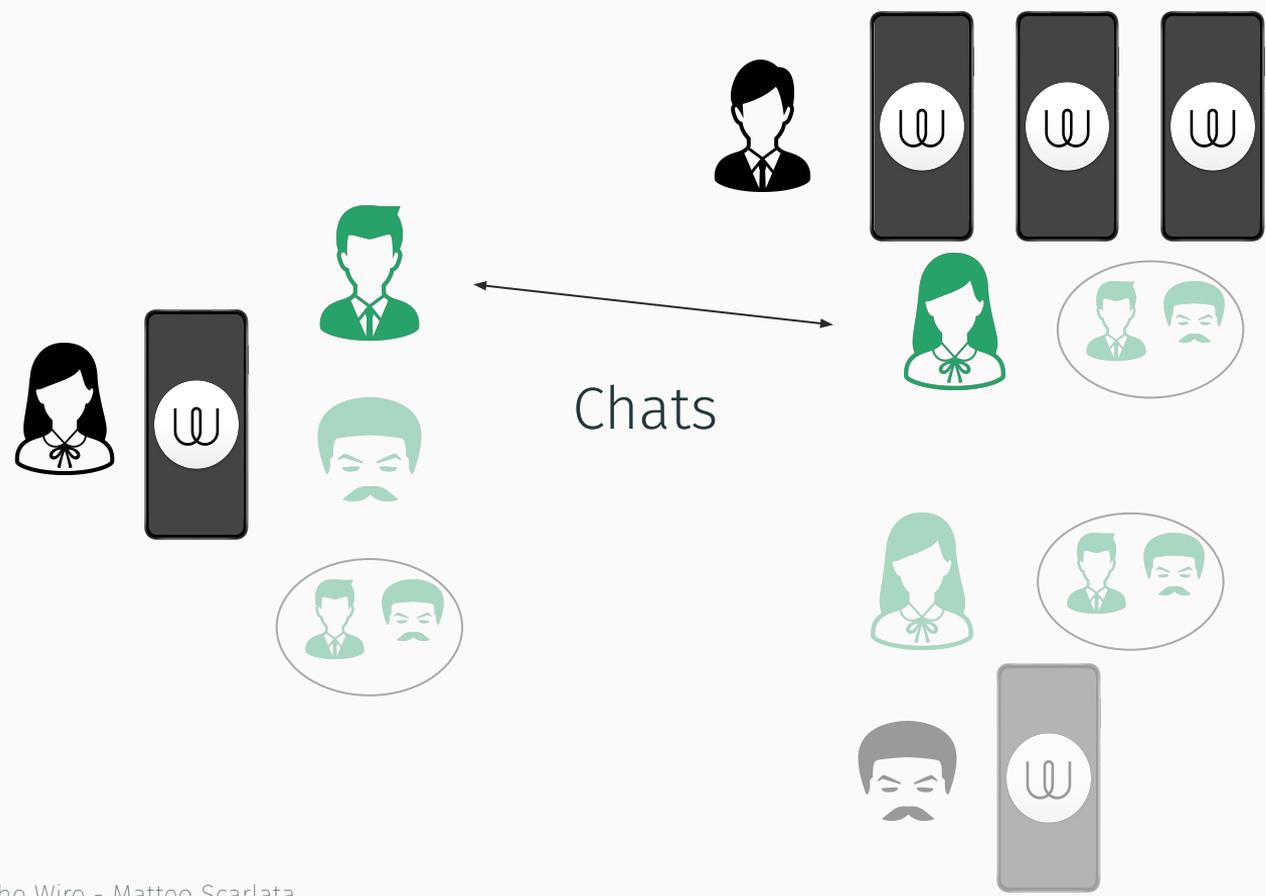


The screenshot displays the Wire chat application interface. On the left, a vertical sidebar for user Alice shows a list of contacts: Bob (highlighted in blue), Charlie, and Group Chat 1. The main chat area on the right is titled 'Bob' and features a search icon, video call, voice call, and info icons at the top. The contact's name 'Bob' and handle '@bob' are displayed above a large green circular profile picture. At the bottom, there is a 'Type a message' input field and a row of icons for emojis, photos, attachments, voice recording, and a send button.

# Chat Level Security



# Chat Level Security

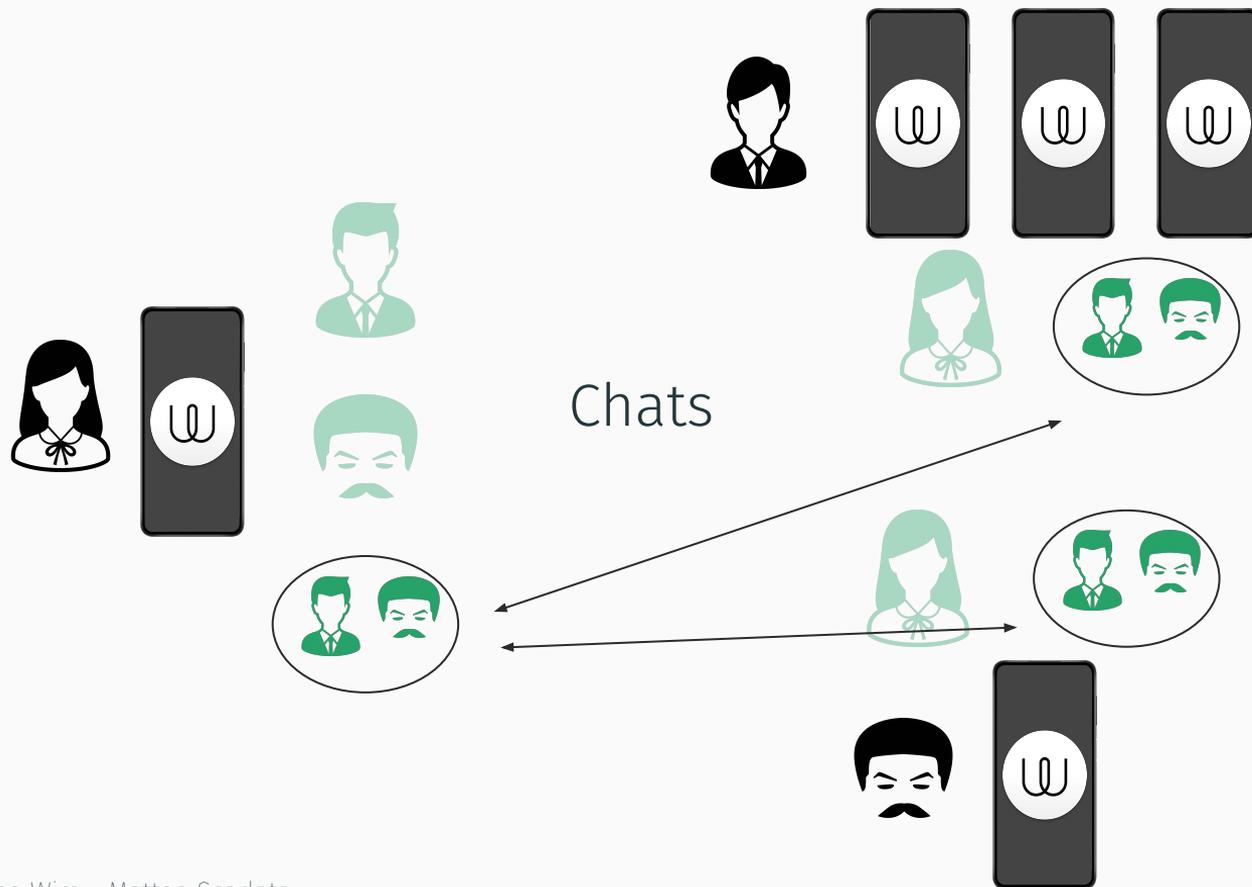


## Consistent view

Hi Alice!  
I like  
pineapple pizza

Hi Bob!  
That's not a  
crime

# Chat Level Security



## Consistent view

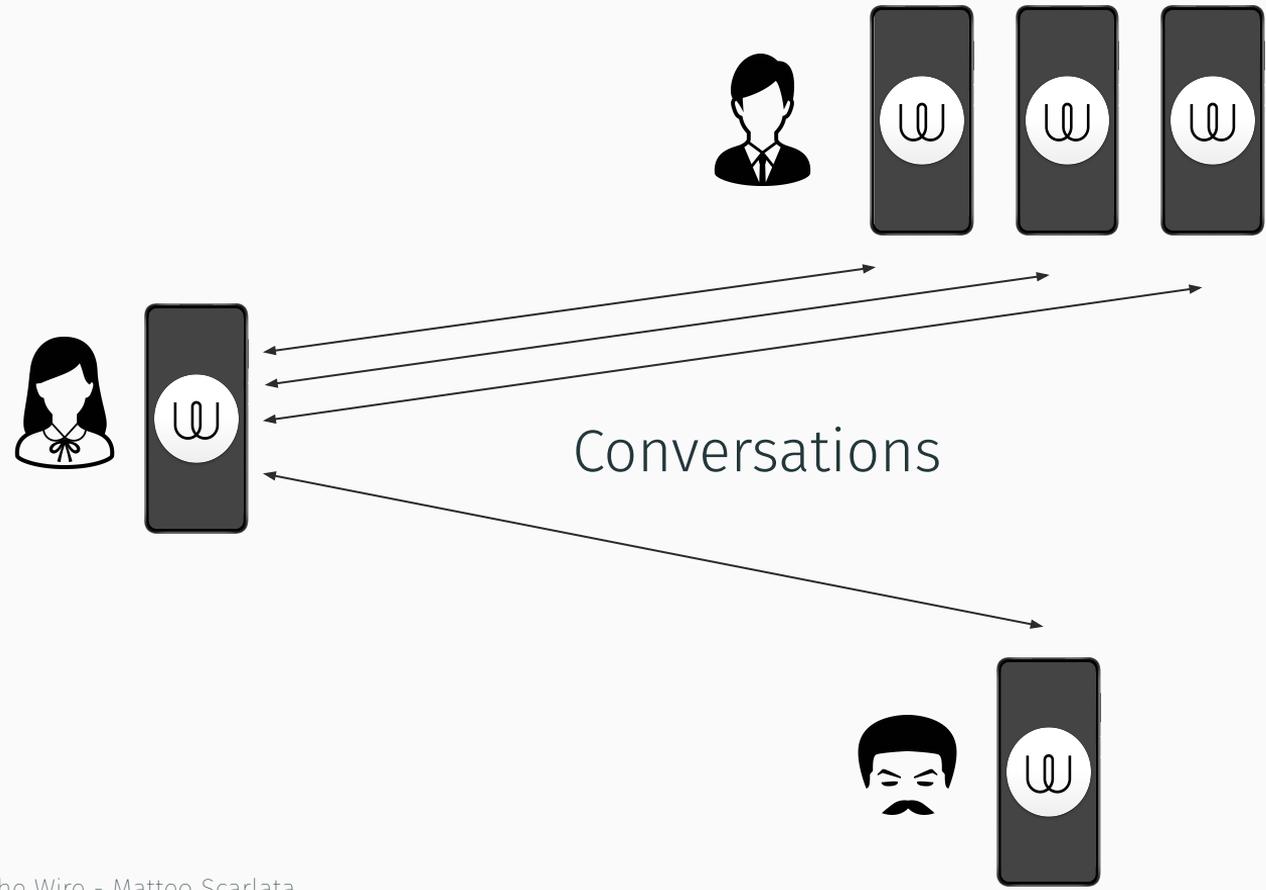
A: we meet at 8

B: let's do 9

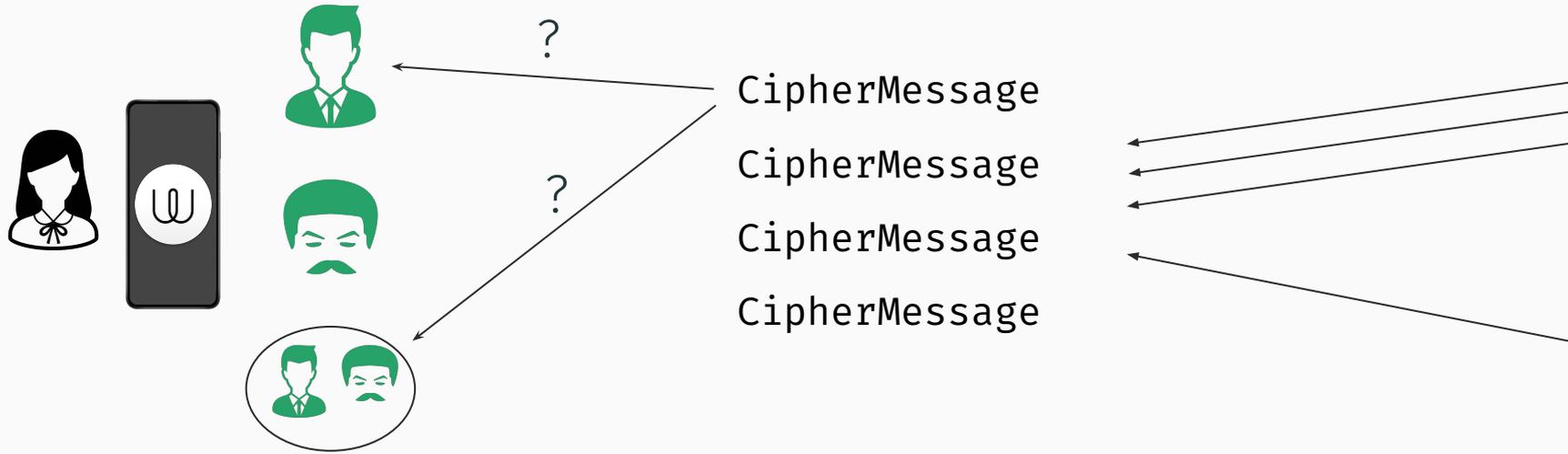
C: yes

A: ok

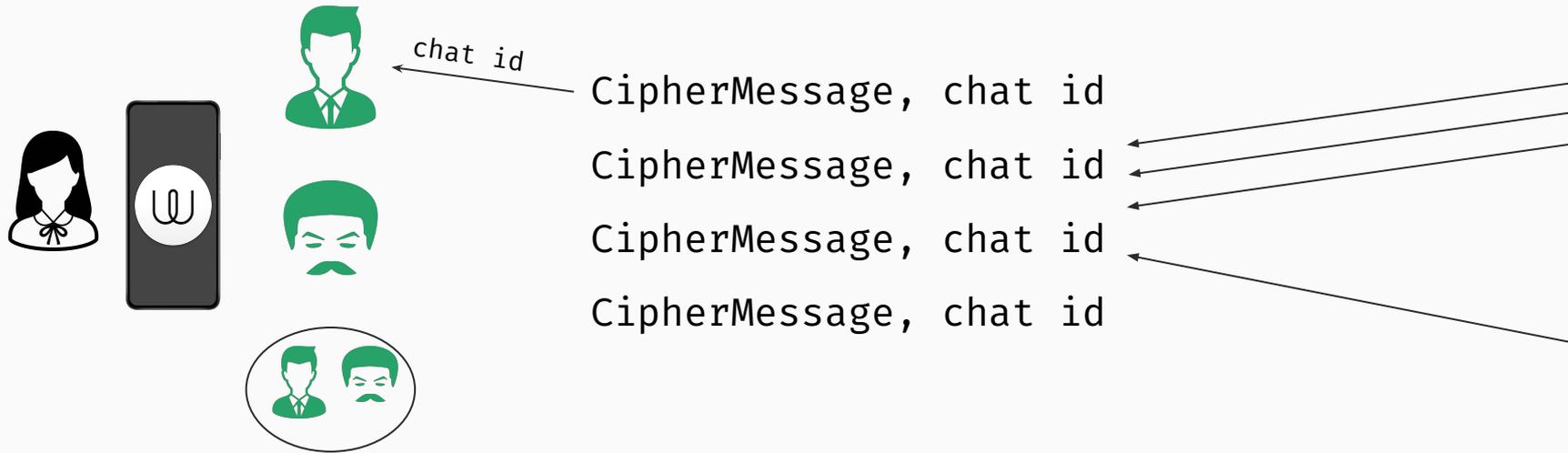
# The Case of Wire: Chat Level



# The Case of Wire: Chat Level



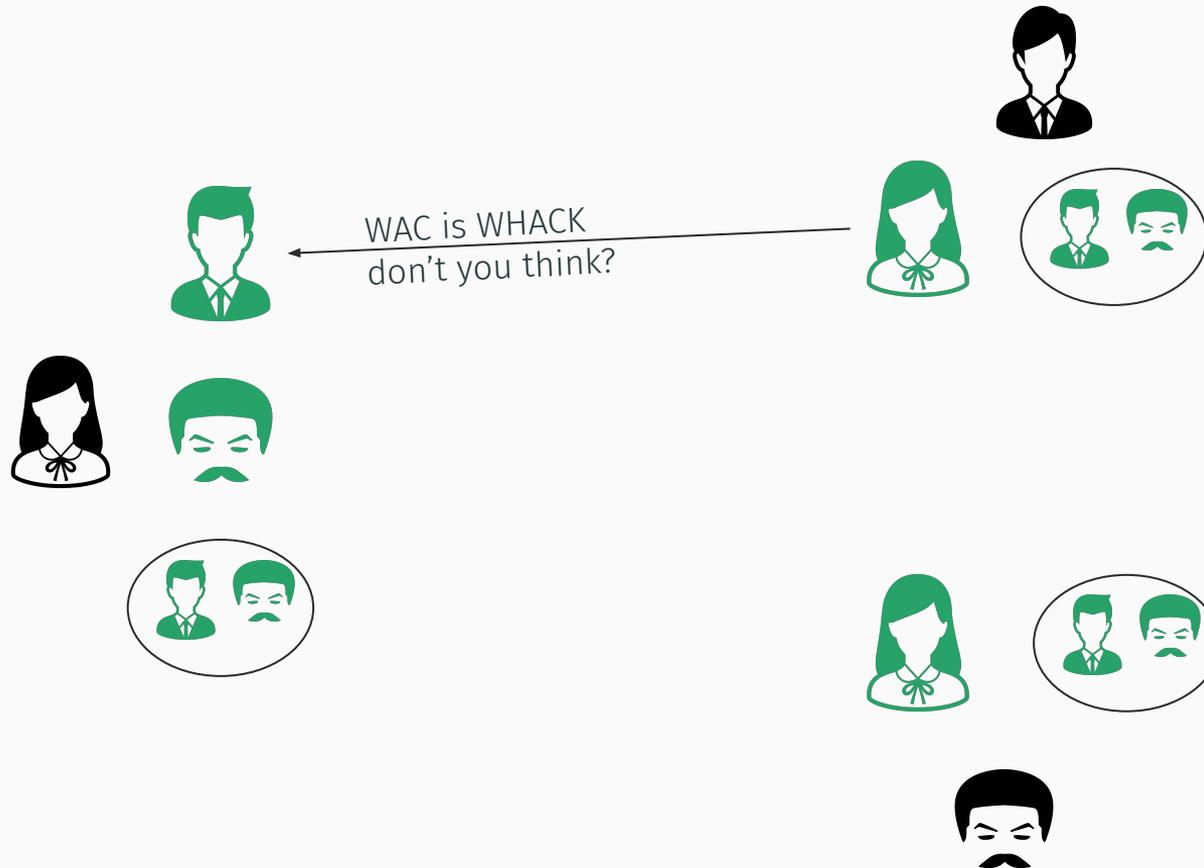
# The Case of Wire: Chat Level



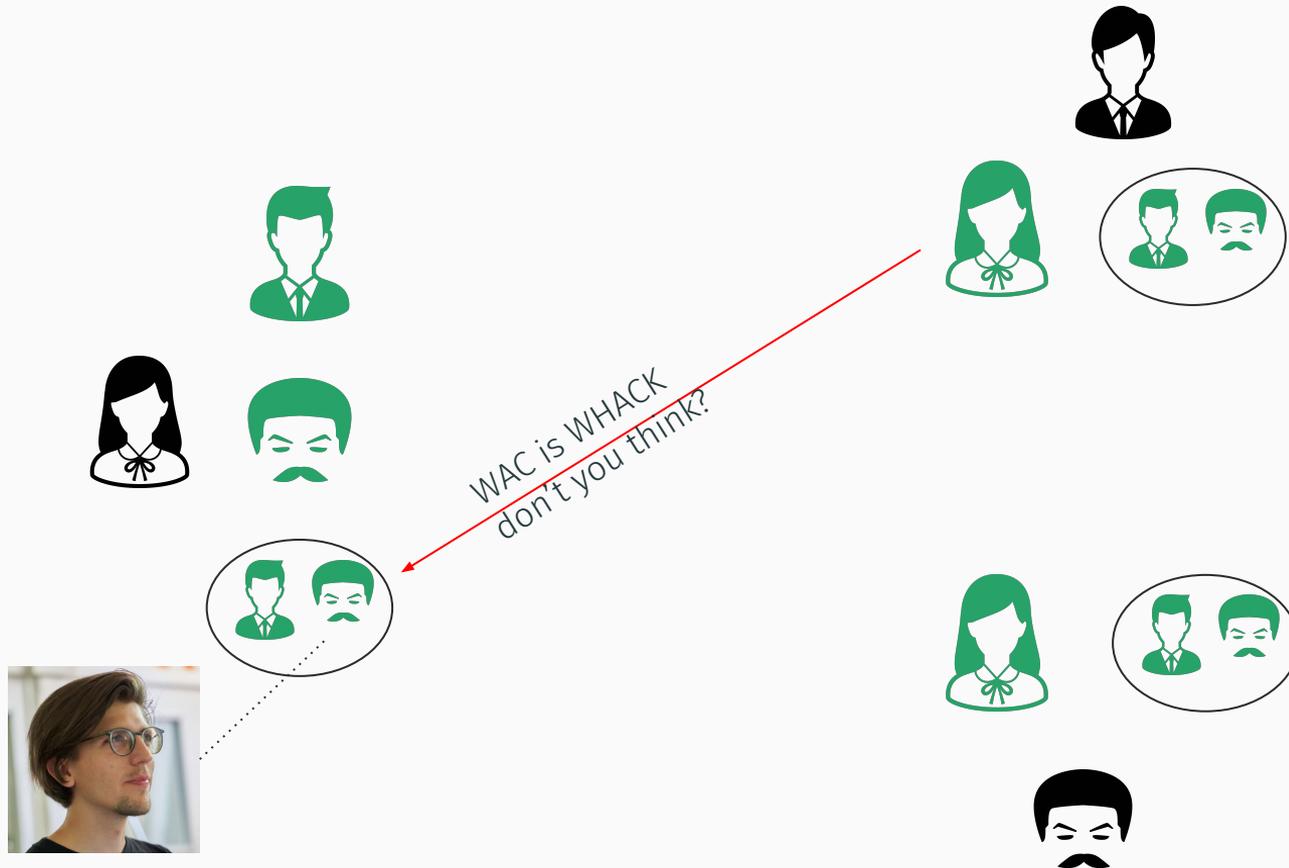
# The Case of Wire: Chat Level



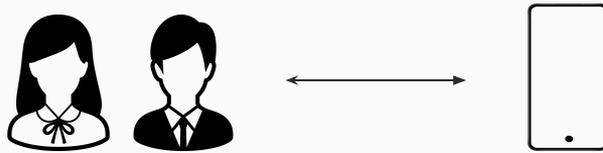
# The Case of Wire: Chat Level



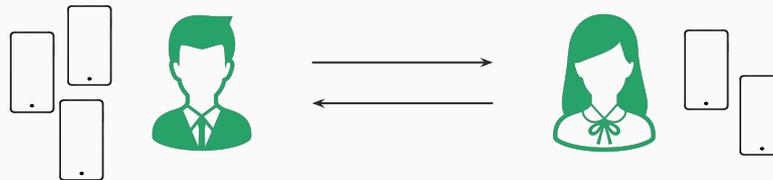
# The Case of Wire: Chat Level



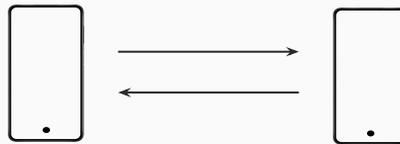
UI



Chat



Conversation

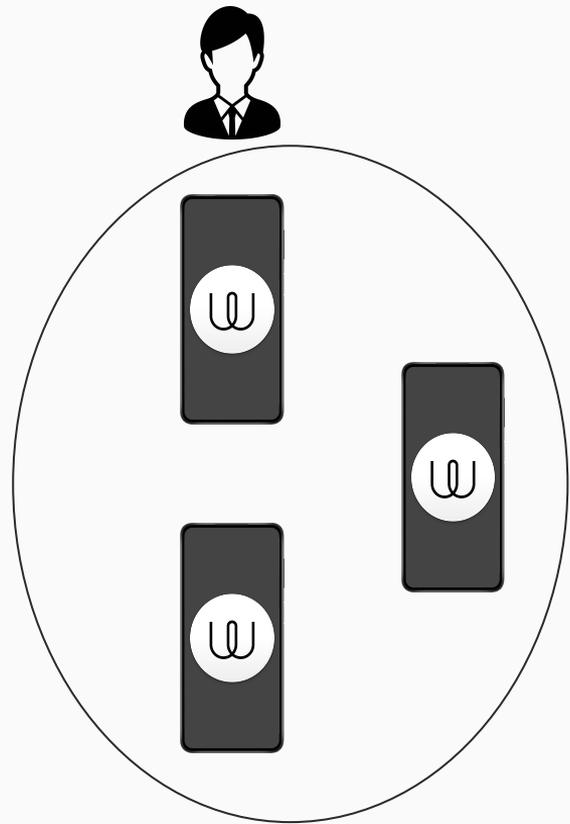
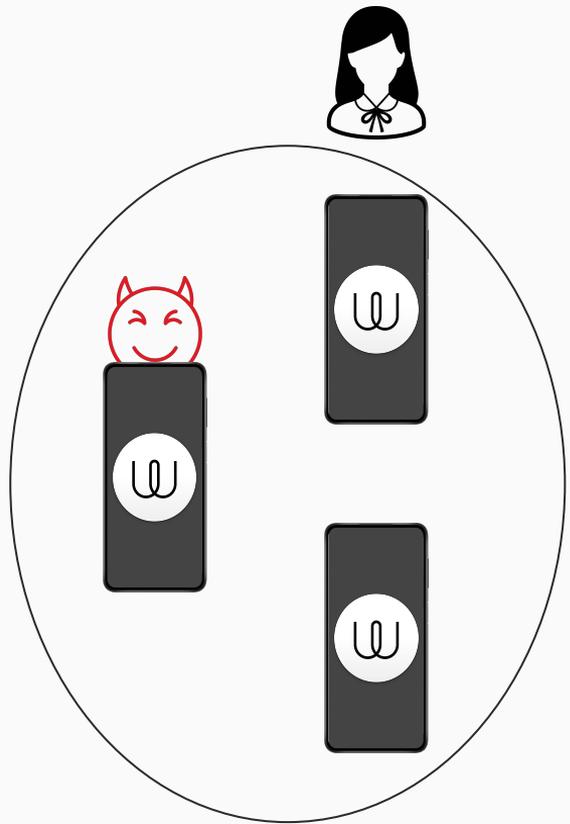


Session

XPDH



# The Case of Wire: UI Level



# The Case of Wire: UI Level



## Your connection is not private

Attackers might be trying to steal your information from **wrong.host.badssl.com** (for example, passwords, messages or credit cards). [Learn more](#)

NET::ERR\_CERT\_COMMON\_NAME\_INVALID

Advanced

Back to safety

# The Case of Wire: UI Level

## feat: Dialog informin conversation was degraded (WPB-1771)

 Merged mchenani merged 9 commits into `develop` from `feat/dialog_informin_conversation_was_degraded`  on Nov 17, 2023

 Conversation 13

 Commits 9

 Checks 12

 Files changed 13



**borichellow** commented on Nov 15, 2023 • edited by github-actions  

Contributor ...

 [WPB-1771](#) [Proteus] Add dialog to confirm sending a message in a degraded conversation

# The Case of Wire: Disclosure

- Disclosed on 13/11/2023, response on 15/11/2023
- UI vulnerability fixed on 17/11/2023
- PCS and group id auth not fixed!
  - Wire to switch to MLS in late 2024

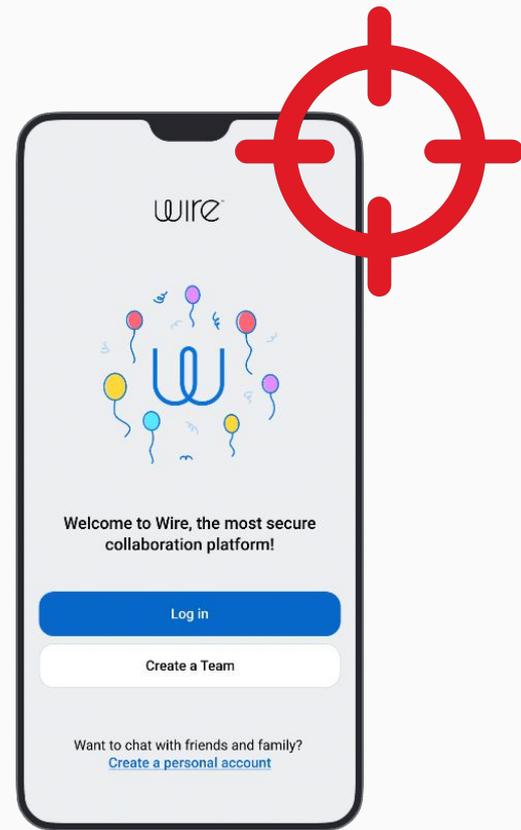
# Lessons

- 1. Key Exchange +
- Messaging Channel +
- Conversations +
- Chats +
- UI =

---

## Secure Messaging

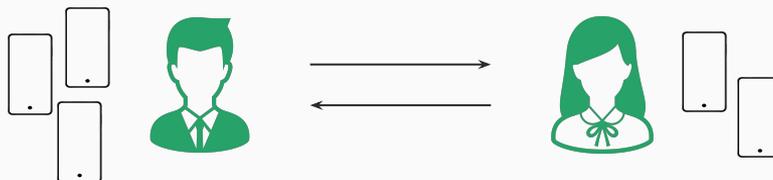
2.



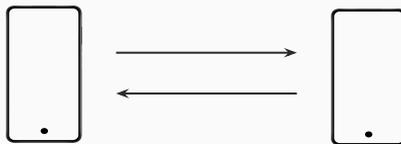
UI



Chat



Conversation



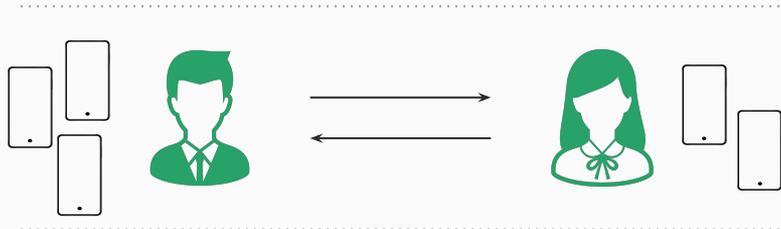
Session



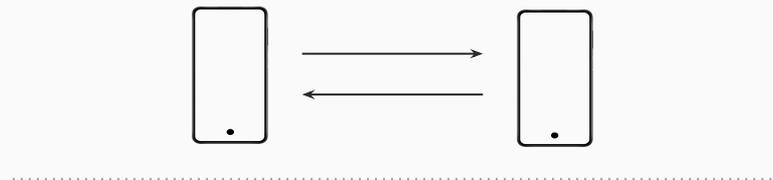
UI



Chat



Conversation

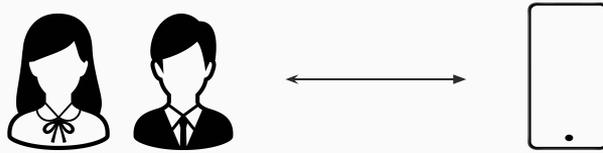


Session

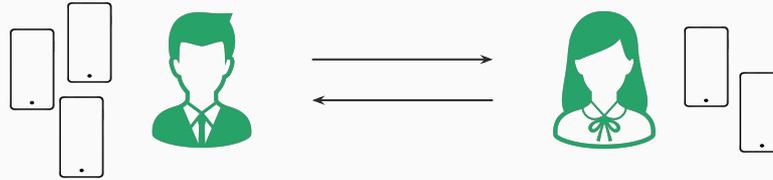


Models?

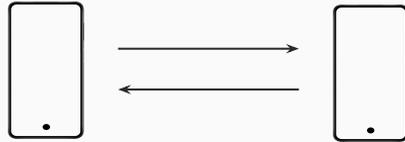
UI



Chat



Conversation



Session

XPDH



**WhatsApp with Sender Keys?  
Analysis, Improvements and Security Proofs**

David Balbás<sup>1,2</sup> \*, Daniel Collins<sup>3</sup> \*\*, and Phillip Gajland<sup>4,5</sup> \*\*\*

**There Can Be No Compromise:  
The Necessity of Ratcheted Authentication in  
Secure Messaging**

Benjamin Dowling<sup>1</sup> and Britta Hale<sup>2\*</sup>

<sup>1</sup> Department of Computer Science, ETH Zurich  
benjamin.dowling@inf.ethz.ch  
<sup>2</sup> Department of Computer Science, NPS, Naval Postgraduate School  
britta.hale@nps.edu

**Formal Analysis of  
Lifting Security**

Cas Cremers  
CISPA Helmholtz Center for Information Security  
Saarbrücken, Germany  
cremers@cispa.de

charlie.jacome@univ.fr  
Information Security  
Universität des Saarlandes  
Saarbrücken, Germany  
aurora.naska@cispa.de

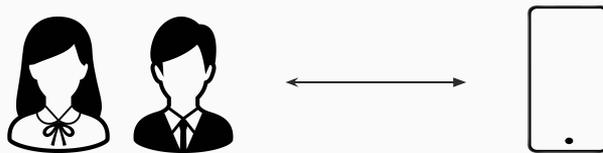
**A Formal Security Analysis of the Signal Messaging Protocol**  
Extended Version, July 2019<sup>1</sup>

Katriel Cohn-Gordon<sup>1</sup>, Cas Cremers<sup>1</sup>, Benjamin Dowling<sup>1</sup>, Luke Garratt<sup>1</sup>, Douglas Stebila<sup>1</sup>

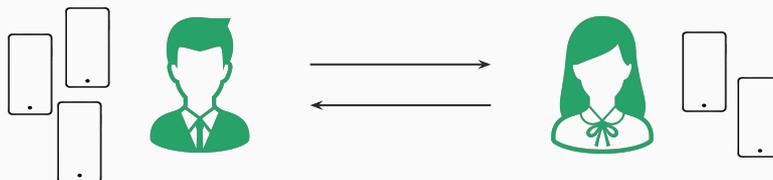
<sup>1</sup>CISPA Helmholtz Center for Information Security, Germany  
cremers@cispa.saarland  
benjamin.dowling@inf.ethz.ch  
lgarratt@cisco.com  
dstebila@uwaterloo.ca

<sup>2</sup>ETH Zurich, Switzerland  
<sup>3</sup>Cisco Systems, USA  
<sup>4</sup>University of Waterloo, Canada

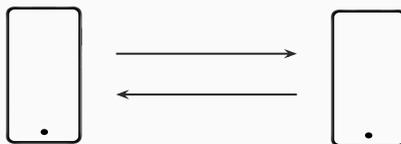
UI



Chat



Conversation



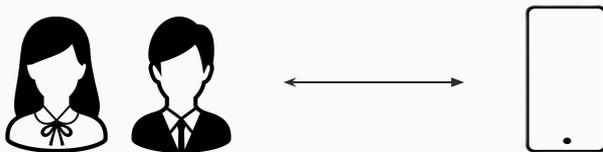
Processes?

Session

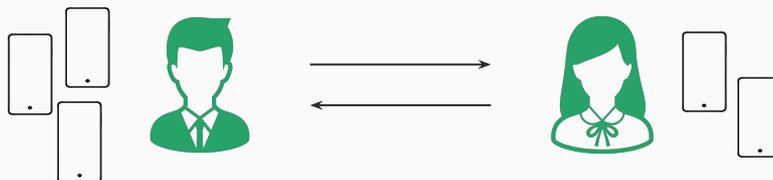
XPDH



UI

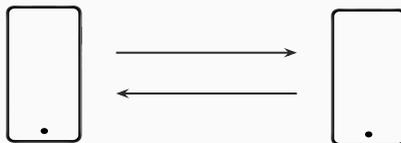


Chat



Questions?

Conversation



Matteo Scarlata  
scmatteo@ethz.ch

Session

XPDH



<https://www.svgrepo.com/>