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 +

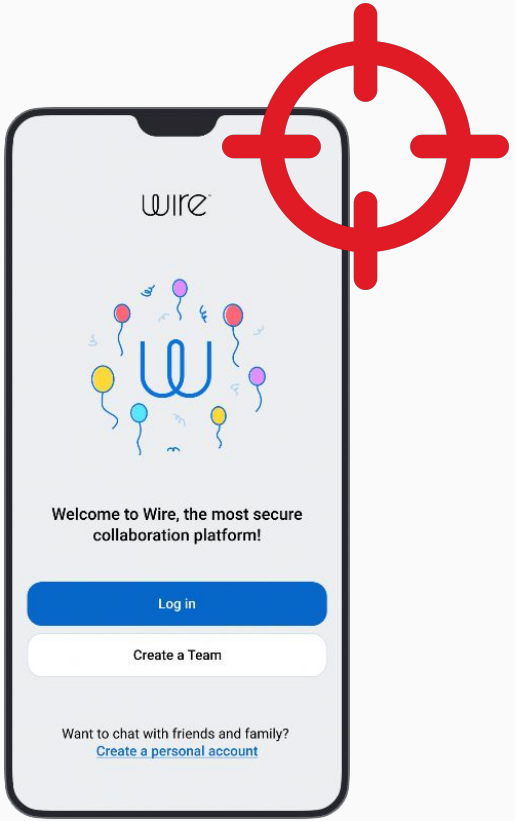
   ??? +

   ??? +

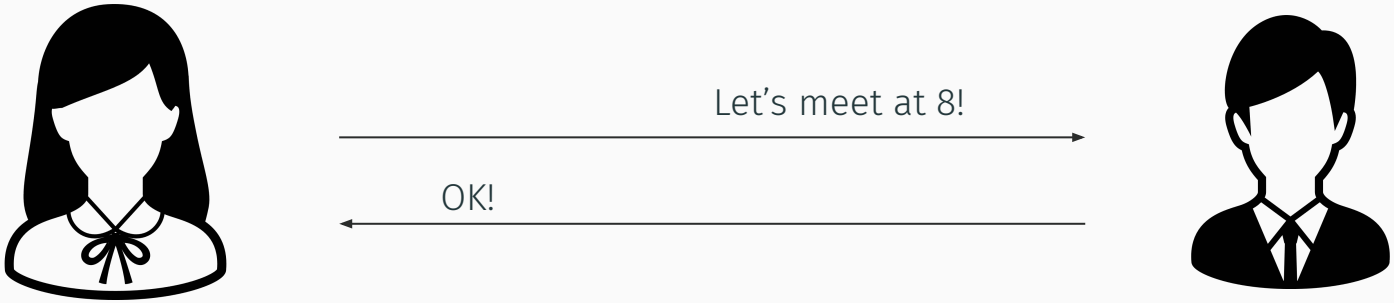
   ??? =

Secure Messaging

2.

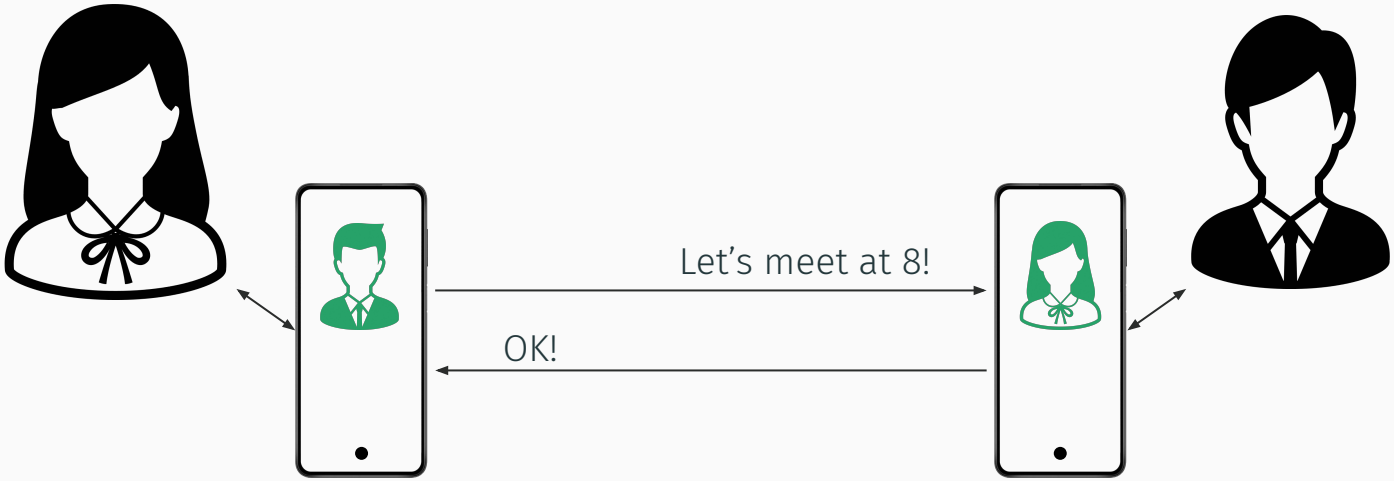


End-to-End Security

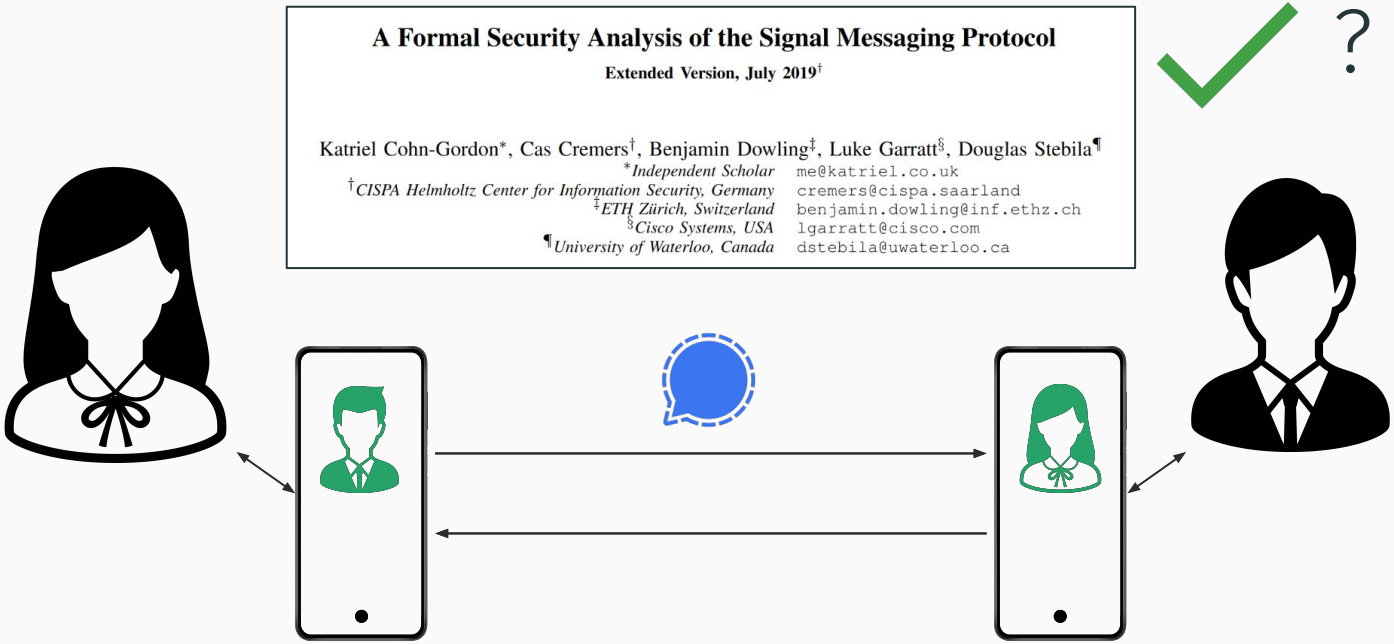


“Only the end points should have access to the plaintext”

End-to-End Security: Secure Messaging

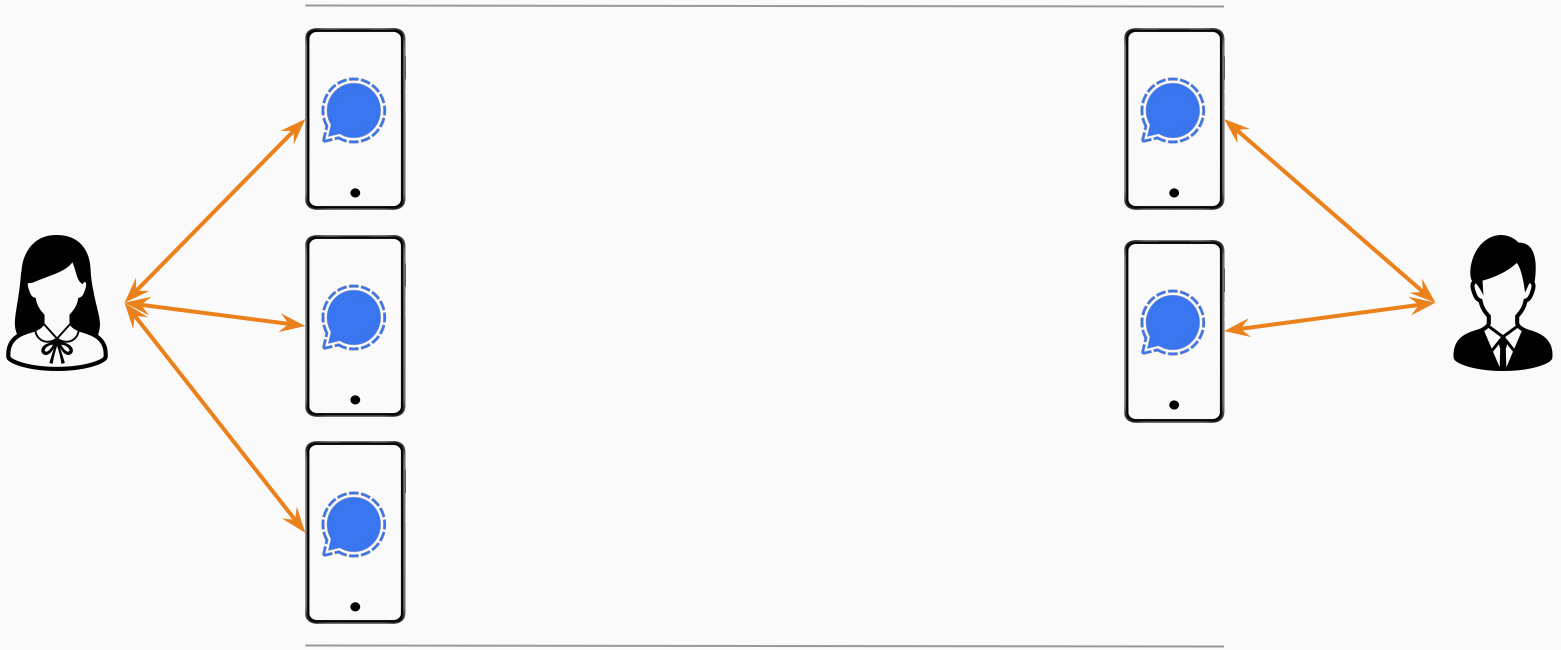


End-to-End Security: Secure Messaging

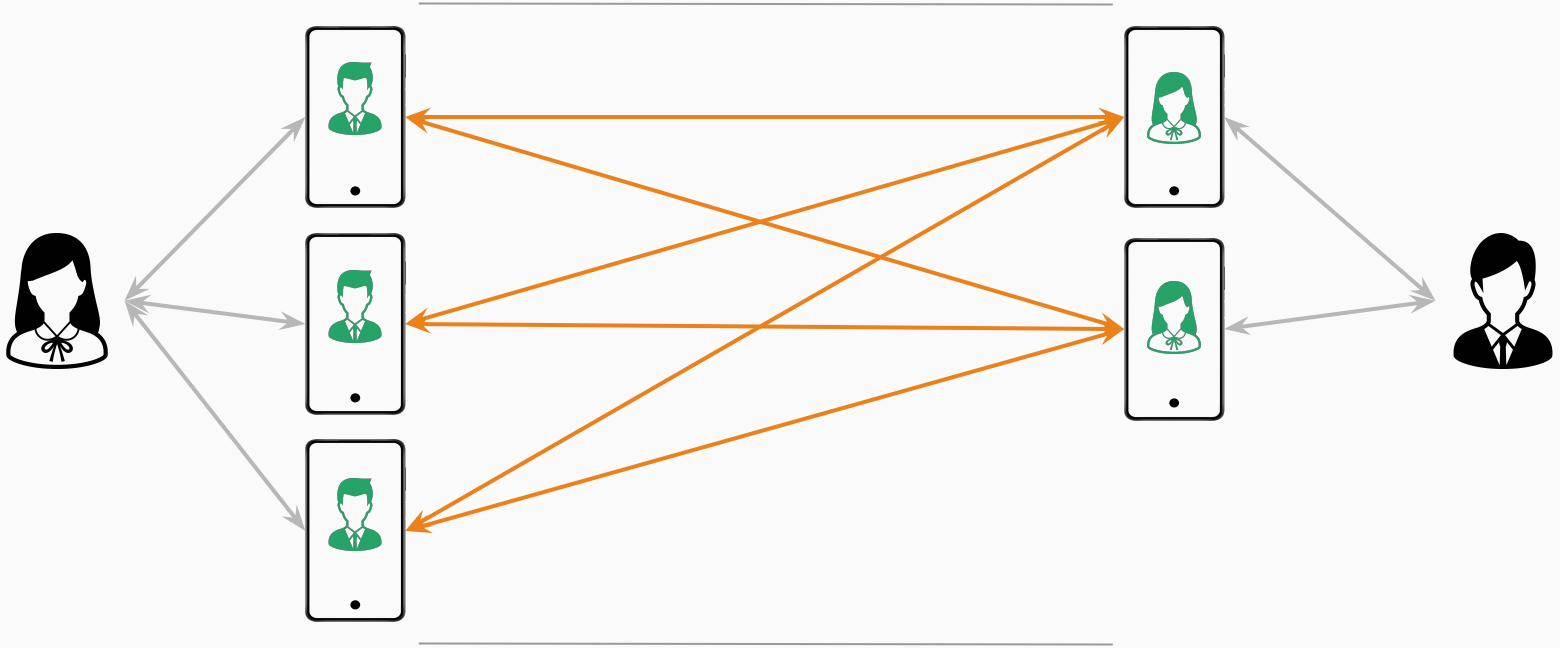


Secure Messaging

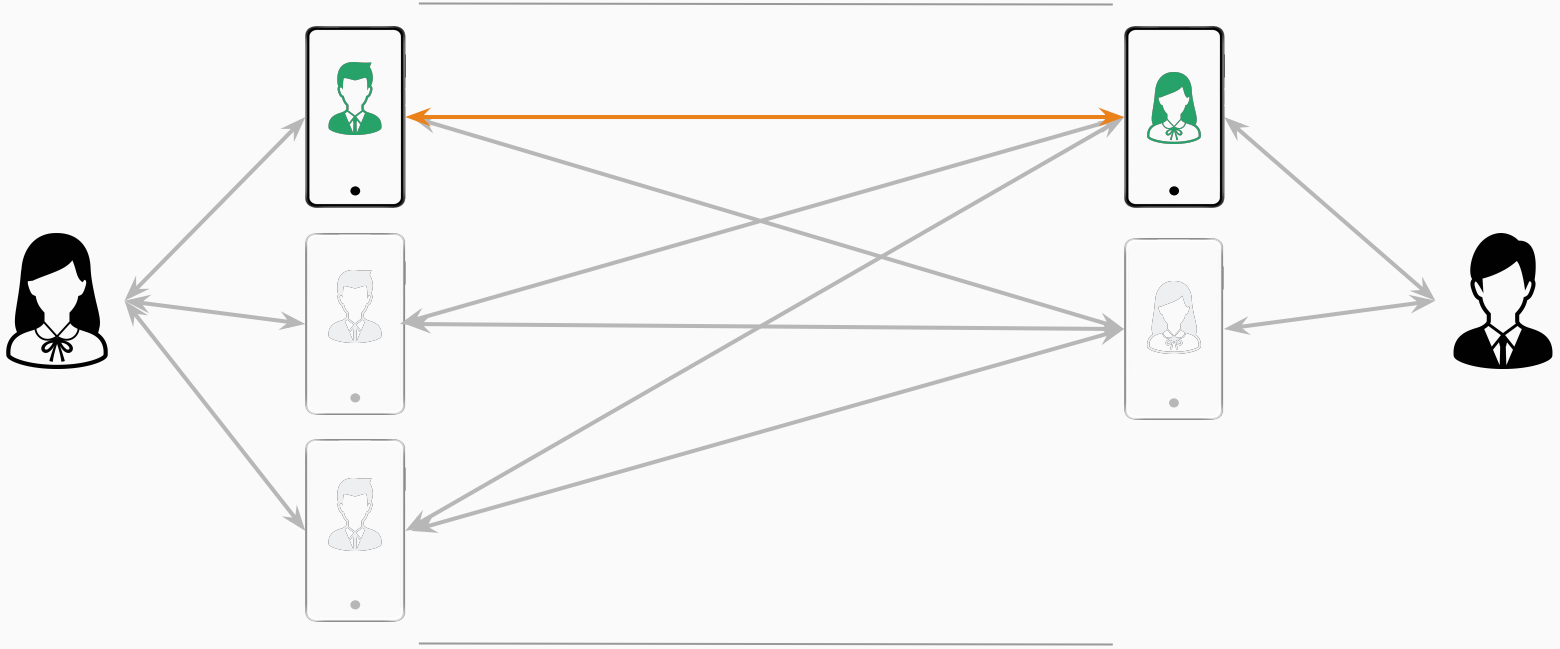
UI



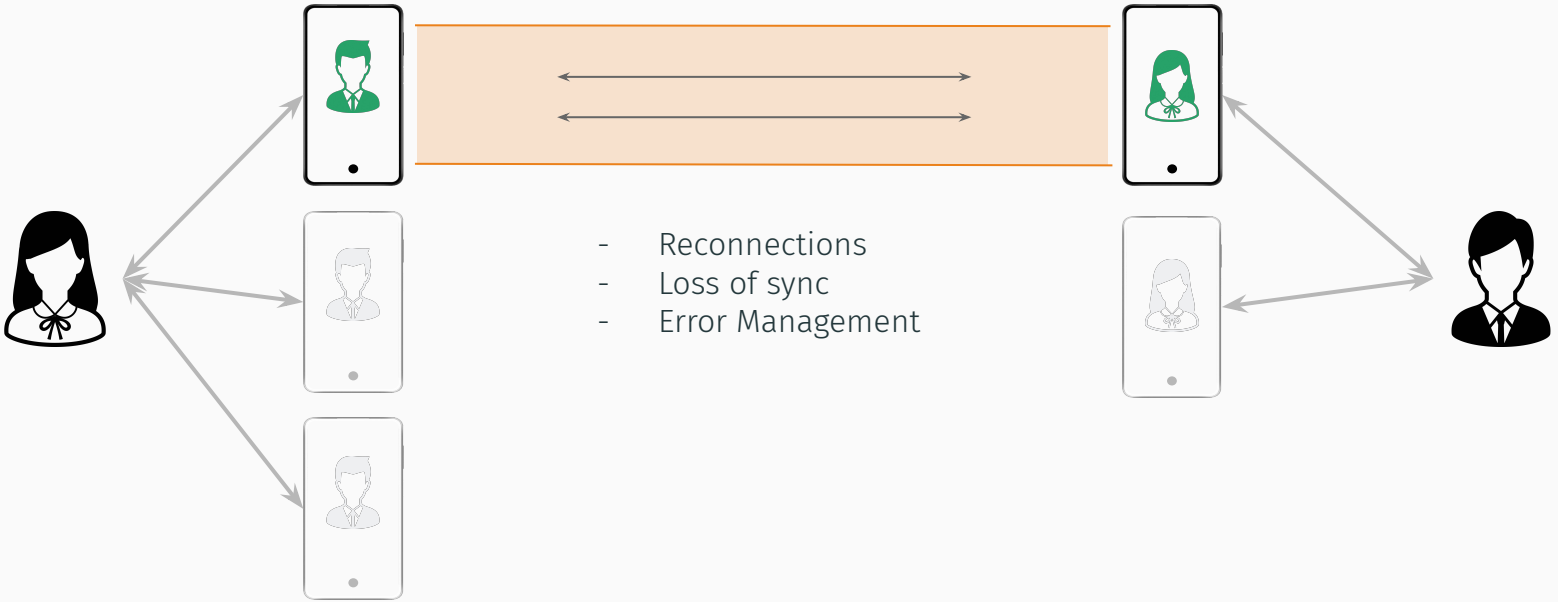
Chat



Chat

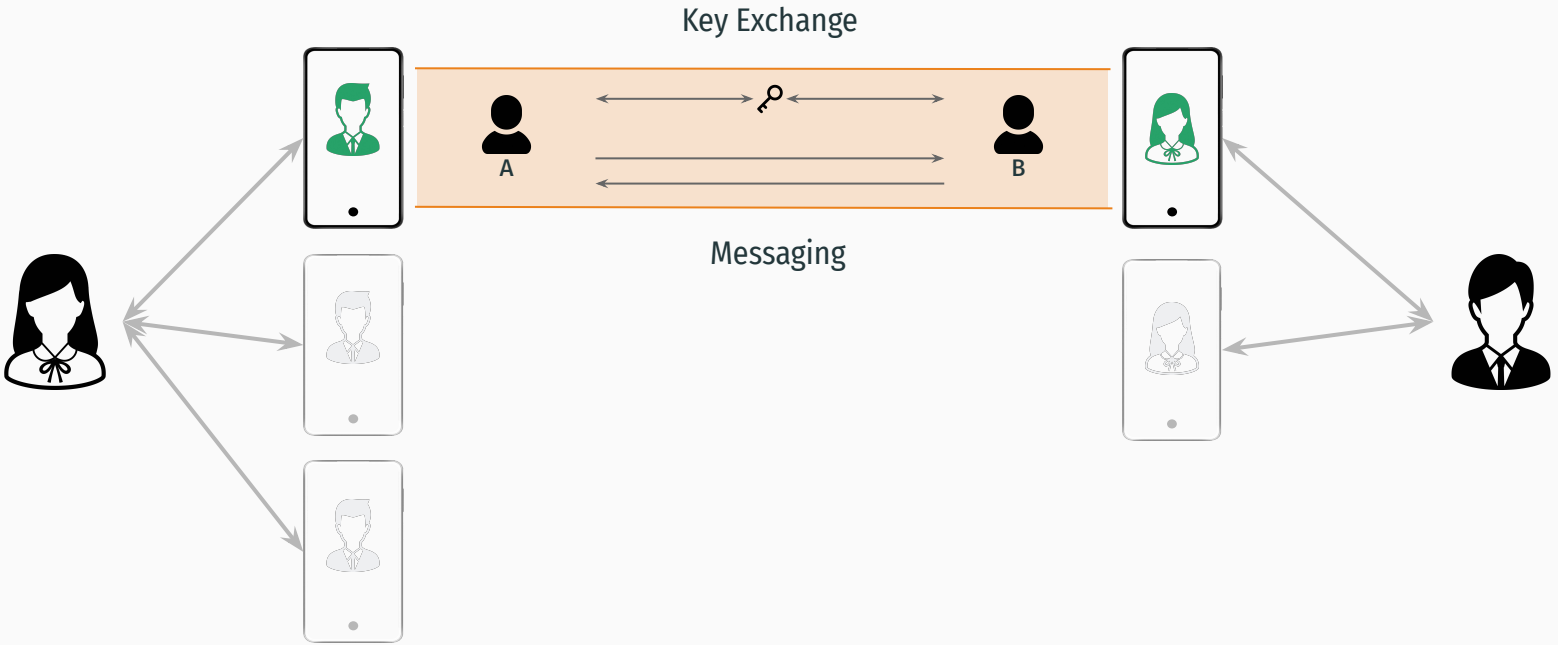


Conversation



- Reconnections
- Loss of sync
- Error Management

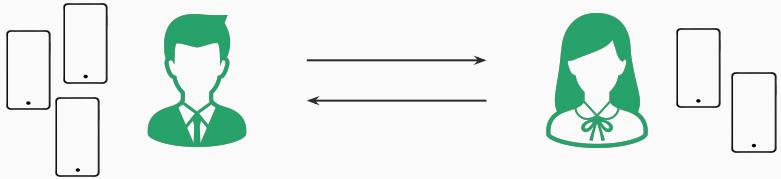
Session



Signal.apk

Client-side fan-out

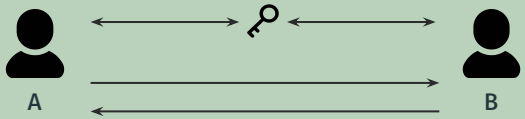
Sender key



Sesame

X3DH

Double Ratchet



A Formal Security Analysis of the Signal Messaging Protocol

Extended Version, July 2019[†]

Katriel Cohn-Gordon*, Cas Cremers[†], Benjamin Dowling[‡], Luke Garratt[§], Douglas Stebila[¶]

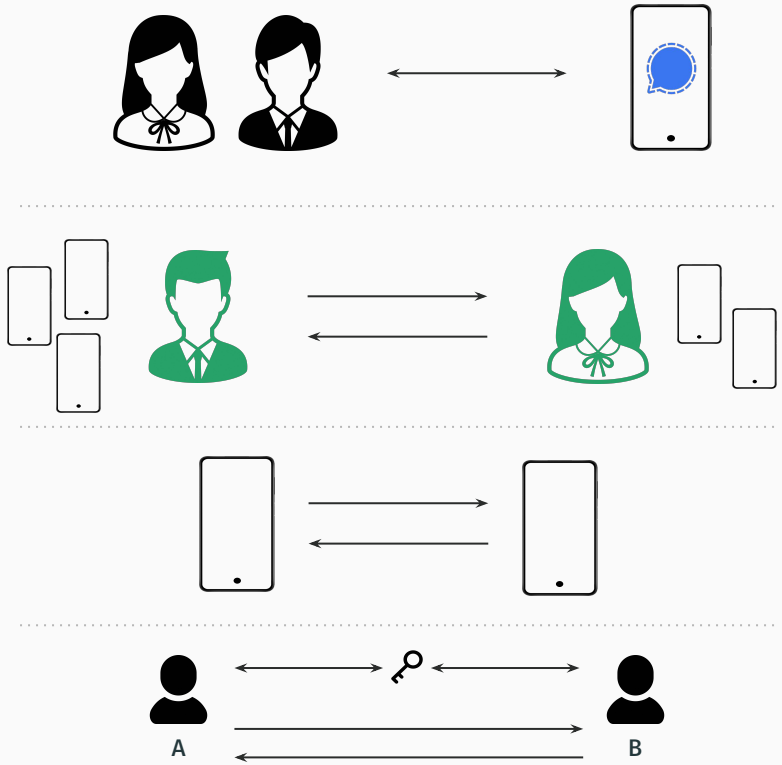
*Independent Scholar me@katriel.co.uk
[†]CISPA Helmholtz Center for Information Security, Germany cremers@cispa.saarland
[‡]ETH Zürich, Switzerland benjamin.dowling@inf.ethz.ch
[§]Cisco Systems, USA lgarratt@cisco.com
[¶]University of Waterloo, Canada dstebila@uwaterloo.ca

The Case of Wire

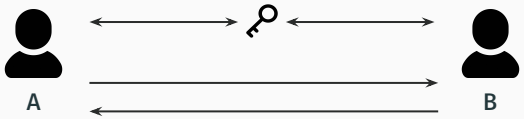
Deutscher Bundestag

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

wire™

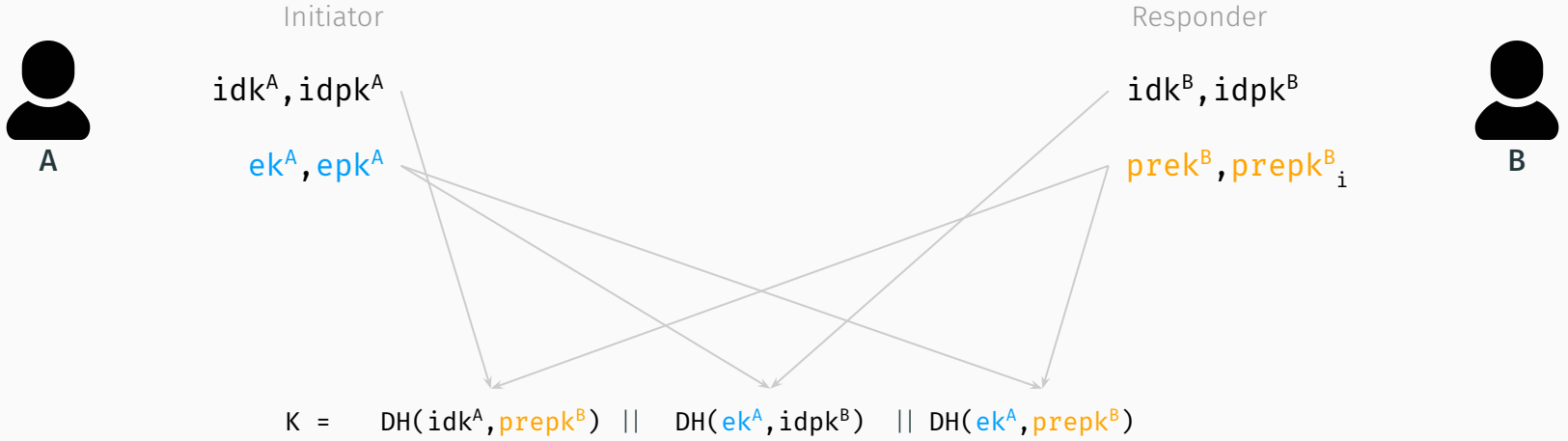


Session

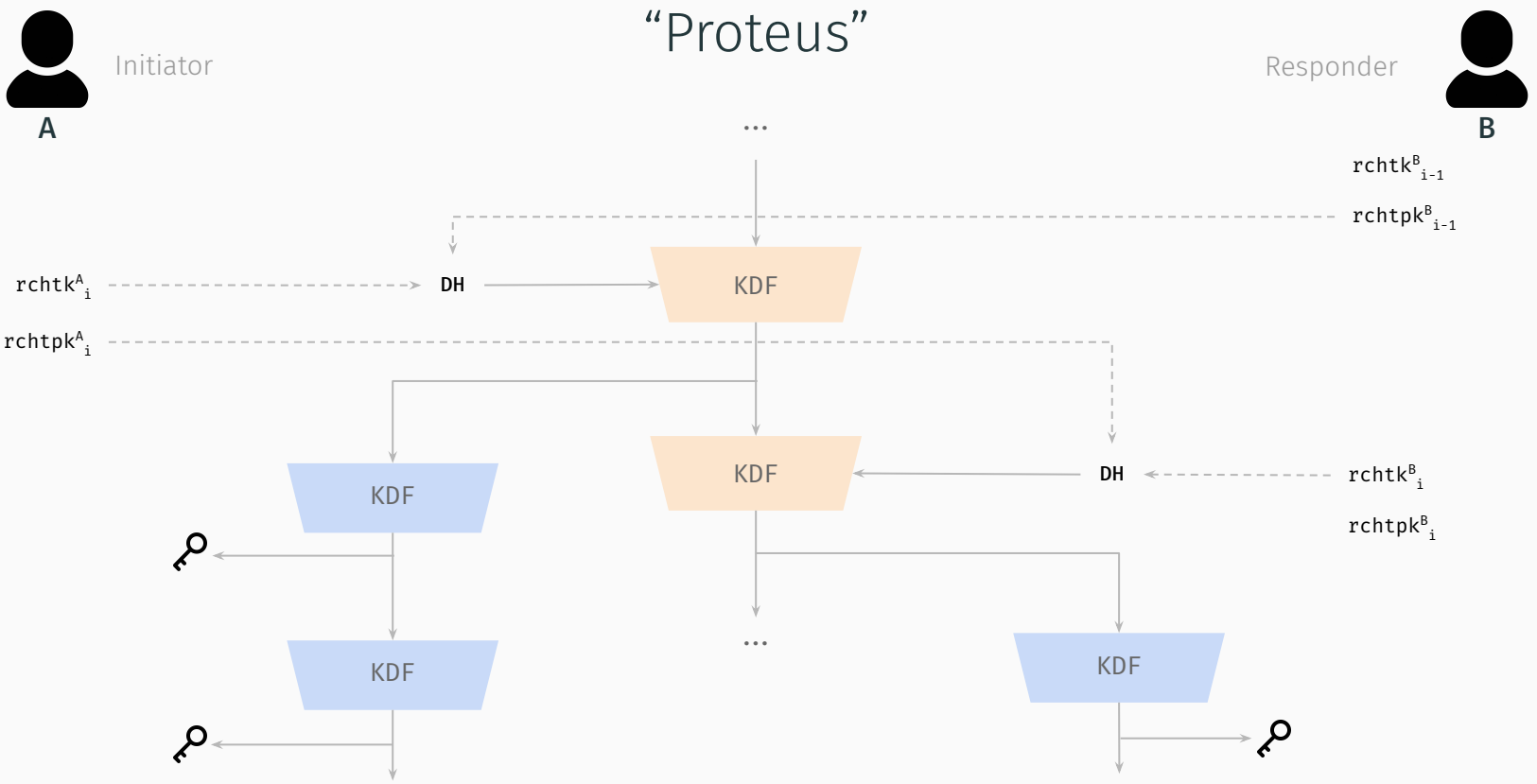


The Case of Wire: Session Level - Key Exchange

"XPDH"



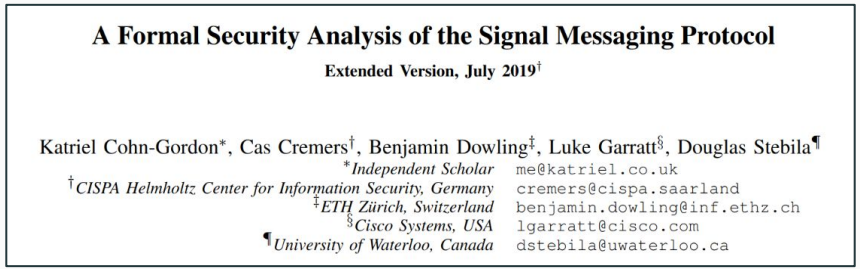
The Case of Wire: Session Level - Messaging



The Case of Wire: Session Level

XPDH ≈ X3DH

Proteus ≈ Double Ratchet



A Formal Security Analysis of the Signal Messaging Protocol

Extended Version, July 2019†

Katriel Cohn-Gordon*, Cas Cremers†, Benjamin Dowling‡, Luke Garratt§, Douglas Stebila¶

*Independent Scholar me@katriel.co.uk

†CISPA Helmholtz Center for Information Security, Germany cremers@cispa.saarland

‡ETH Zürich, Switzerland benjamin.dowling@inf.ethz.ch

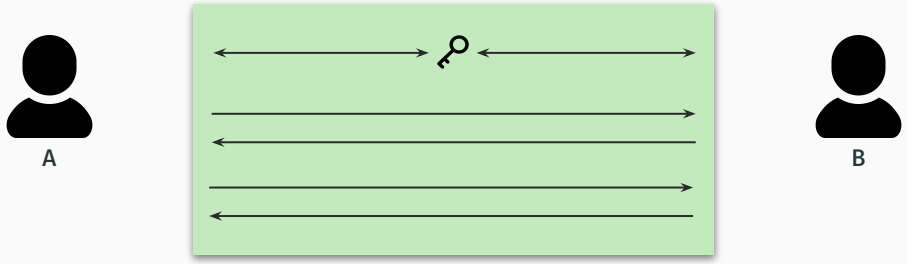
§Cisco Systems, USA lgarratt@cisco.com

¶University of Waterloo, Canada dstebila@uwaterloo.ca

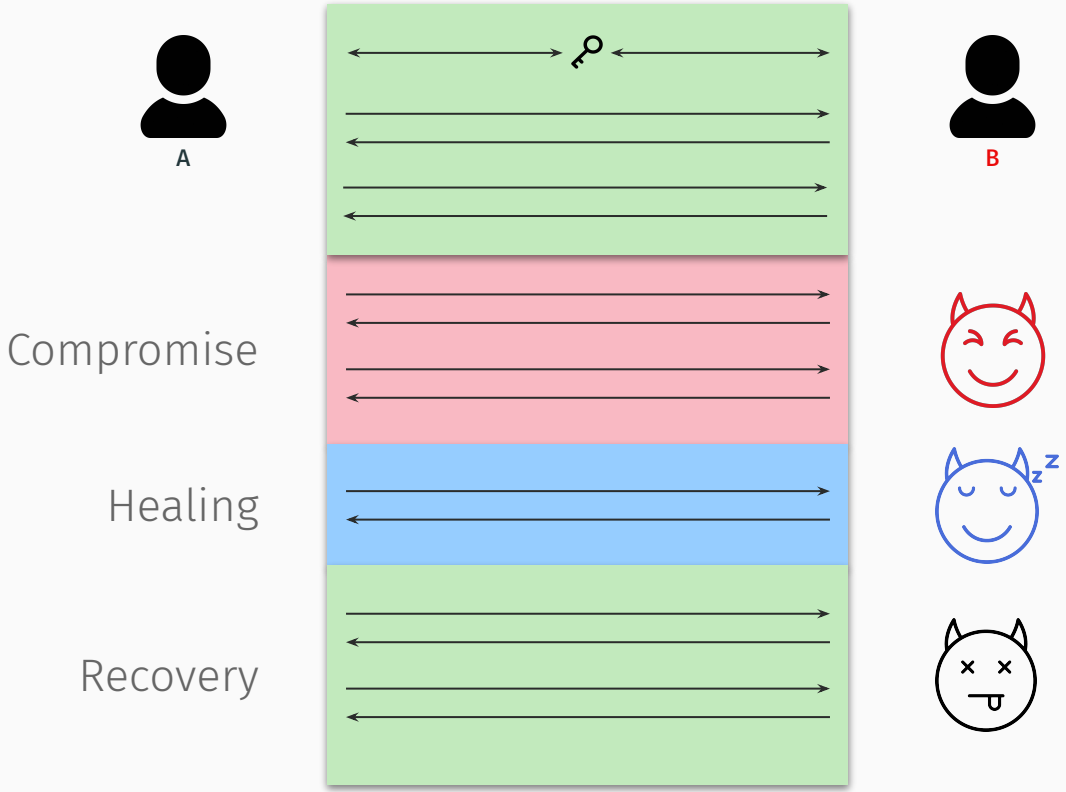
*

*: prekeys not signed,
no responder ephemerals

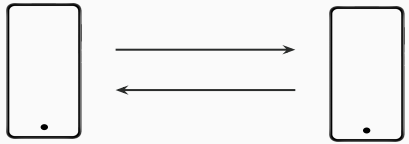
Post-Compromise Security



Post-Compromise Security



Conversation



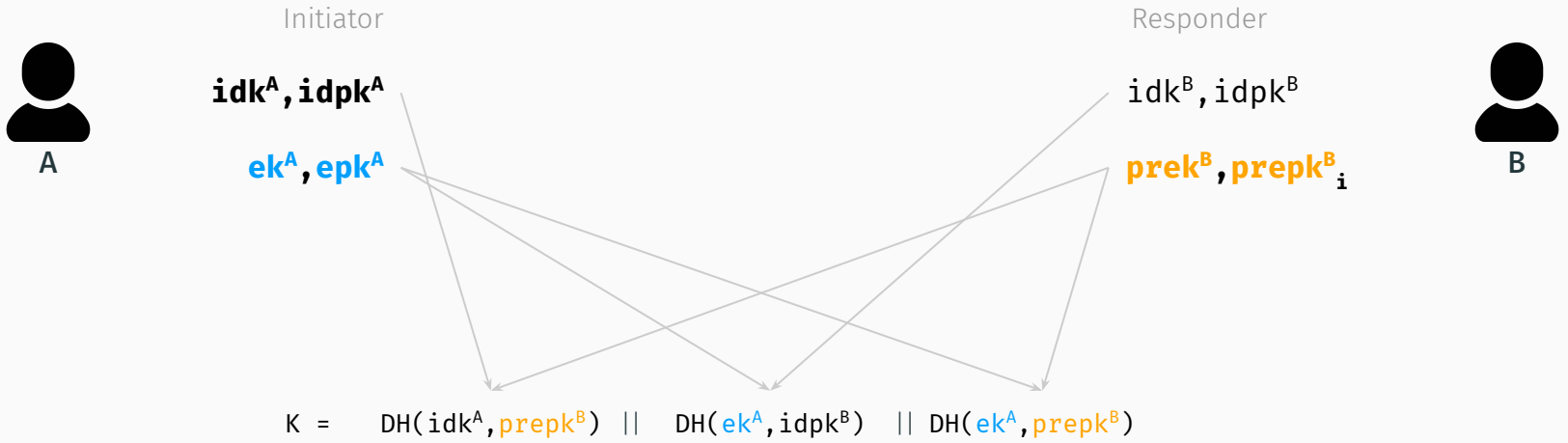
Session

XPDH

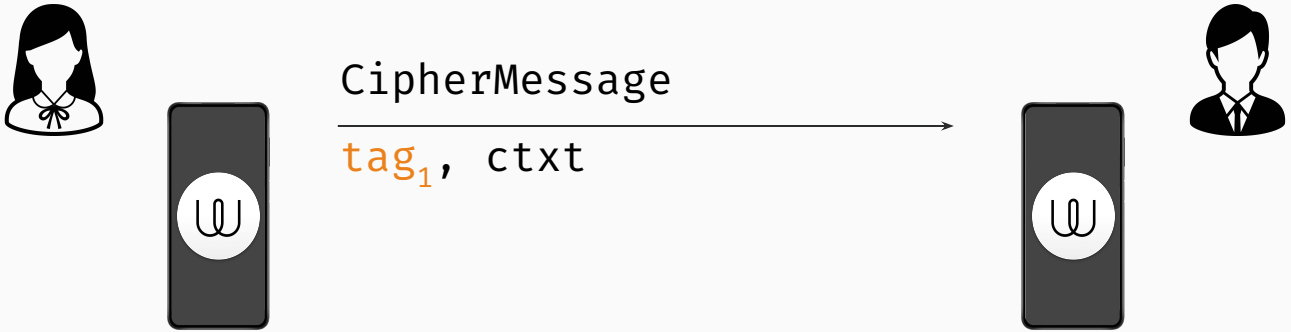
The Case of Wire: Conversation Level

The Case of Wire: Session Level - Key Exchange

"XPDH"



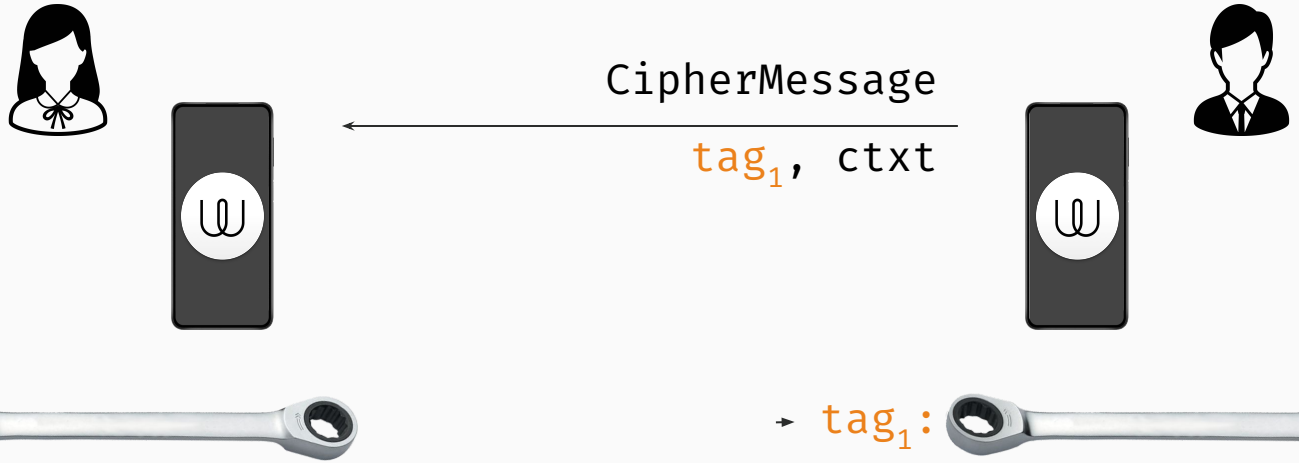
The Case of Wire: Conversation Level



- tag_1: 

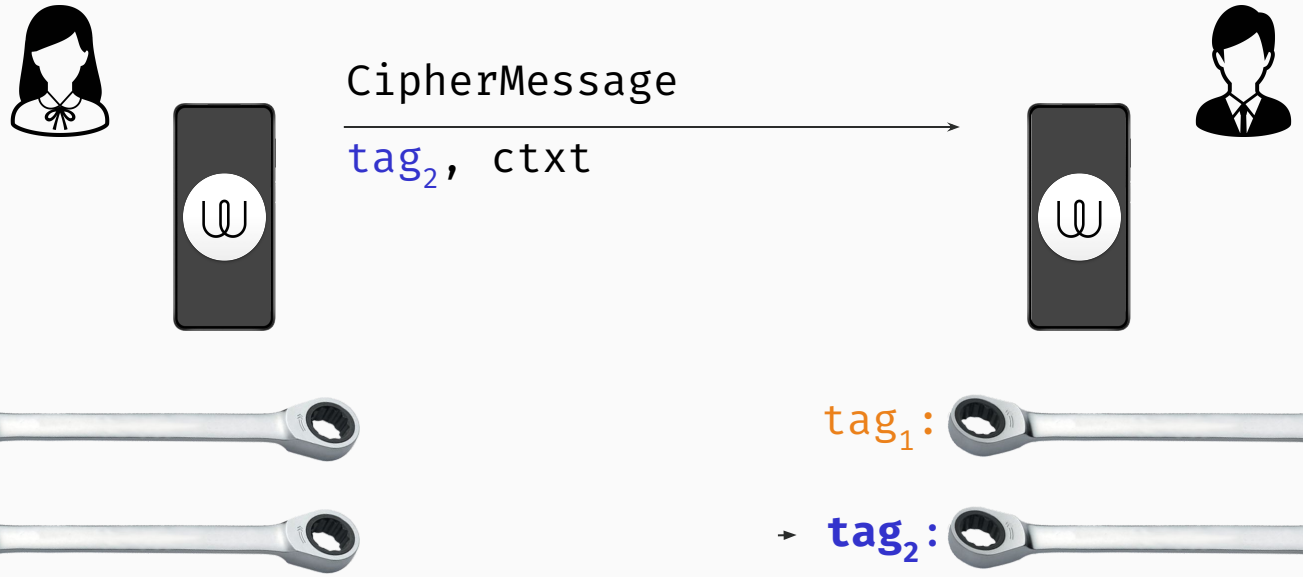
- tag_1: 

The Case of Wire: Conversation Level

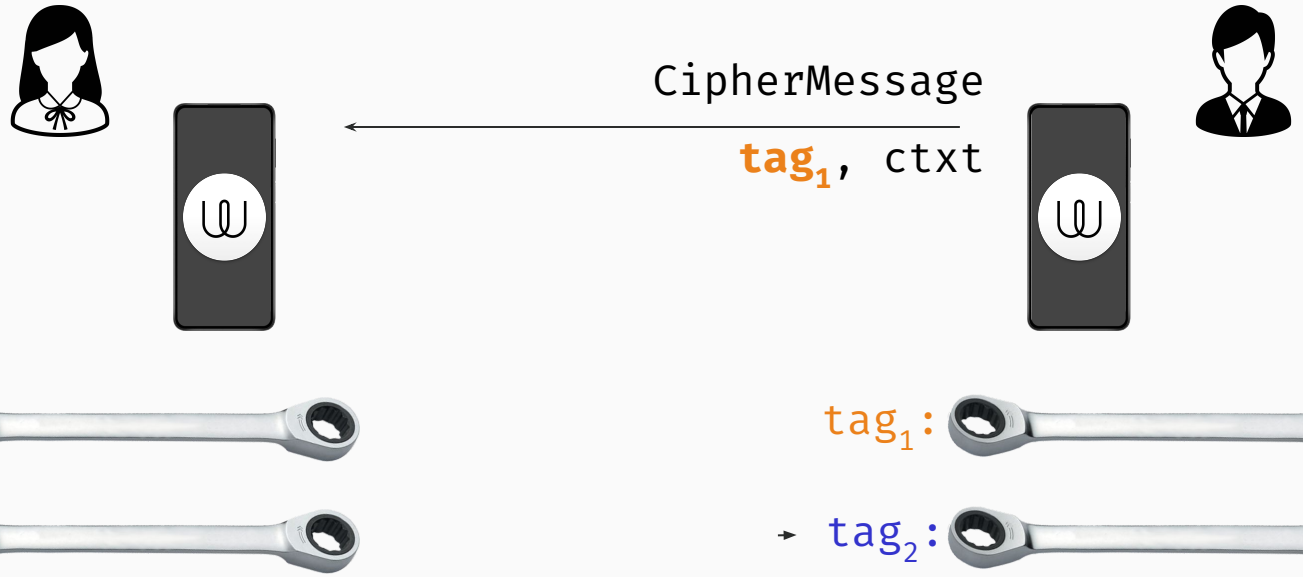


The Case of Wire: Conversation Level

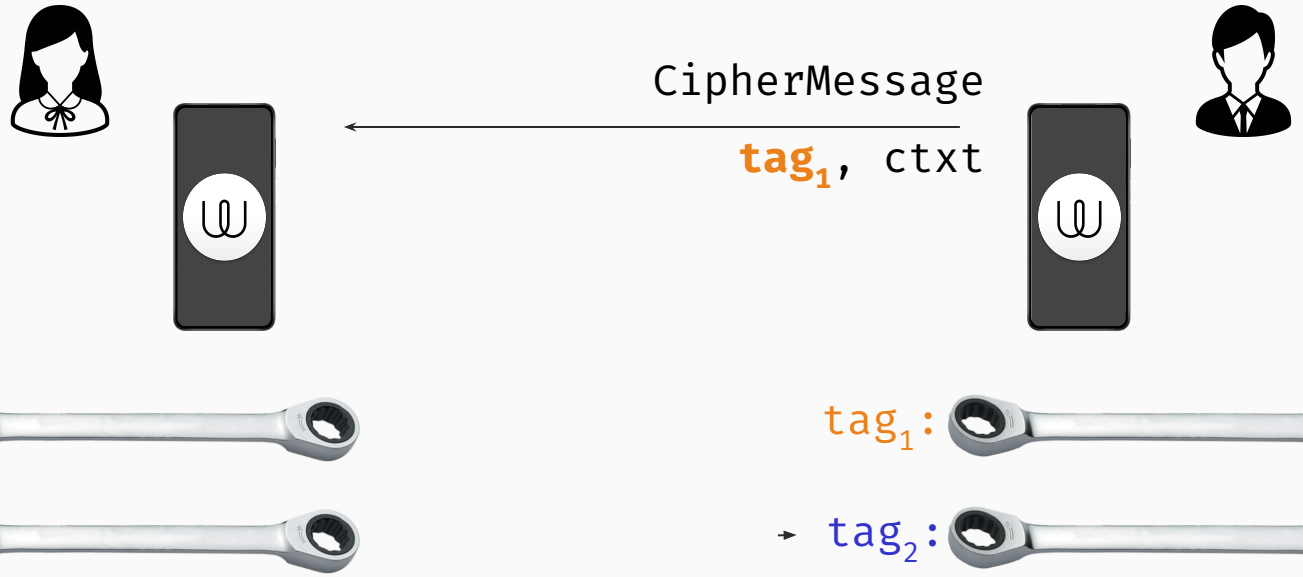
The Case of Wire: Conversation Level



The Case of Wire: Conversation Level



The Case of Wire: Conversation Level

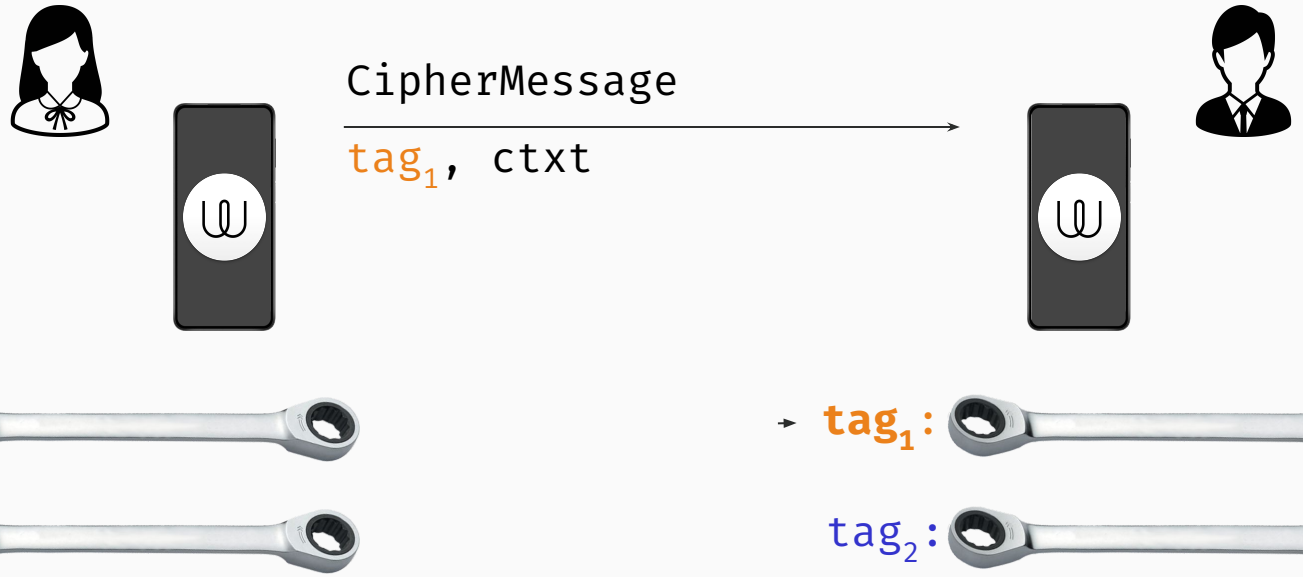


The Case of Wire: Conversation Level

- tag_1:
- tag_2:

- tag_1:
- tag_2:

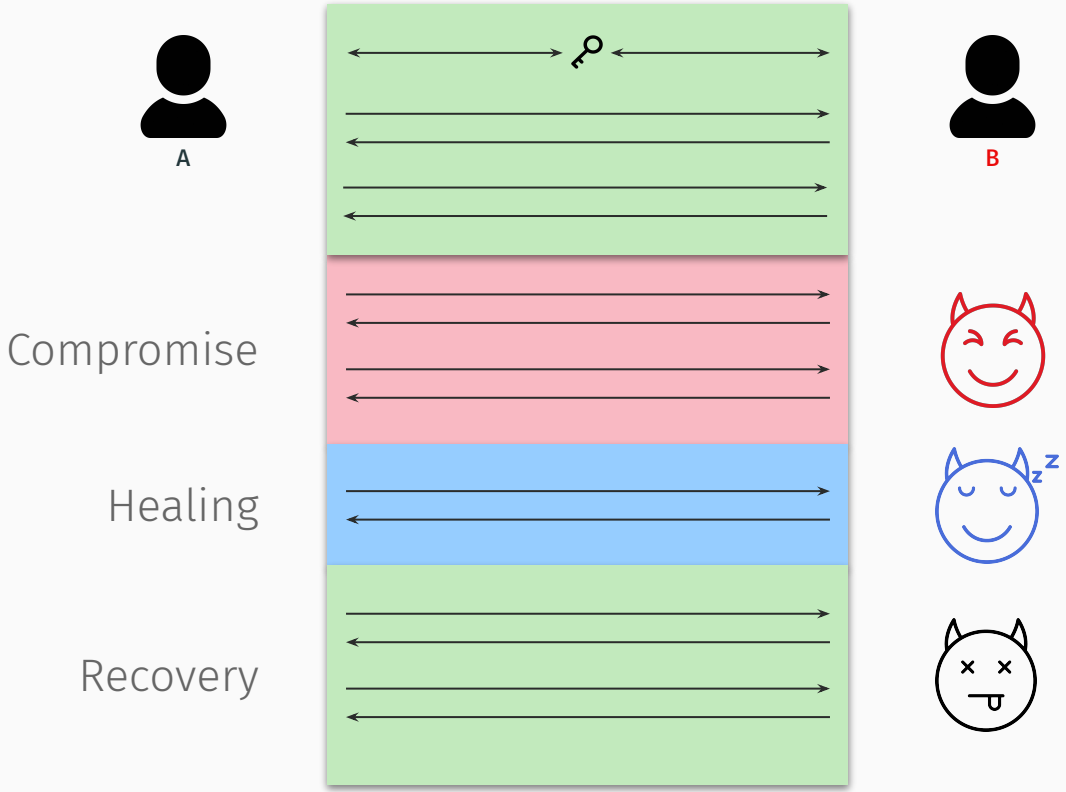
The Case of Wire: Conversation Level



Session Security to Conversation Security

≈

Post-Compromise Security



The Case of Wire: Post-Compromise Security

$\texttt{idk}^{A}, \texttt{idpk}^{A}$

$\texttt{idk}^{B}, \texttt{idpk}^{B}$

- $\texttt{tag}_1$: 

- $\texttt{tag}_1$: 

The Case of Wire: Post-Compromise Security

$\texttt{idk}^{A}, \texttt{idpk}^{A}$

$\texttt{idk}^{B}, \texttt{idpk}^{B}$

- $\texttt{tag}_1$: 

- $\texttt{tag}_1$: 

The Case of Wire: Post-Compromise Security

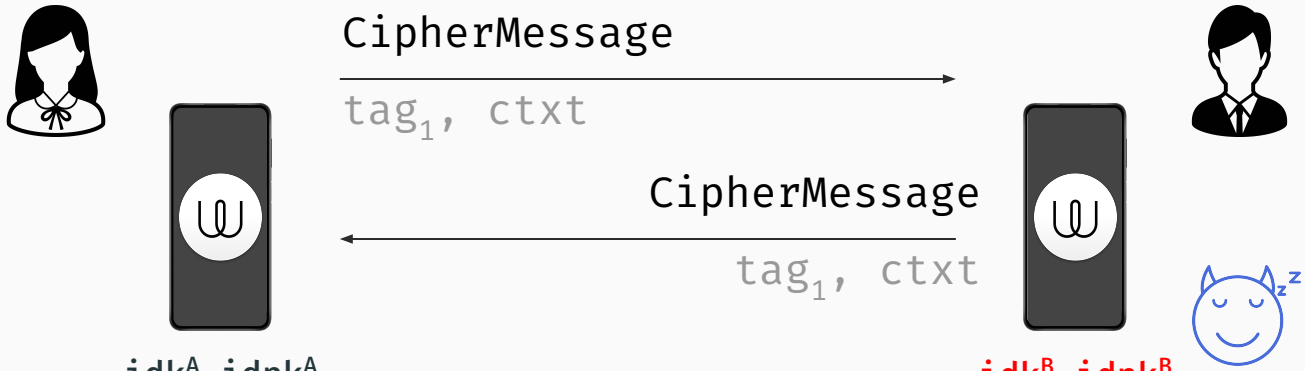
$idk^A, idpk^A$

- tag_1: 

$idk^B, idpk^B$

- tag_1: 

The Case of Wire: Post-Compromise Security



- tag_1:

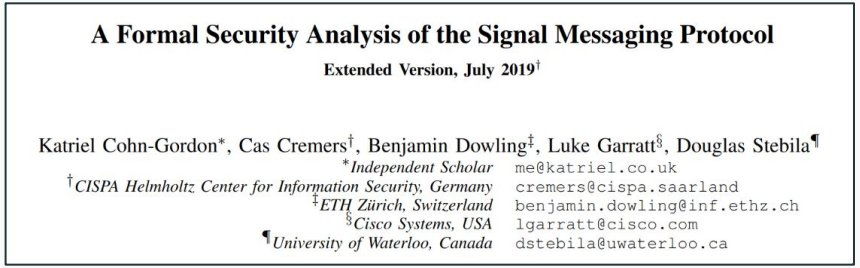
- tag_1:

The Case of Wire: Post-Compromise Security

- tag_1:

- tag_1:

The Case of Wire: Post-Compromise Security



A Formal Security Analysis of the Signal Messaging Protocol

Extended Version, July 2019[†]

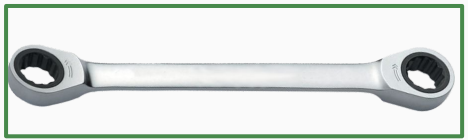
Katriel Cohn-Gordon[*], Cas Cremers[†], Benjamin Dowling[‡], Luke Garratt[§], Douglas Stebila[¶]

[*]*Independent Scholar* me@katriel.co.uk
[†]*CISPA Helmholtz Center for Information Security, Germany* cremers@cispa.saarland
[‡]*ETH Zürich, Switzerland* benjamin.dowling@inf.ethz.ch
[§]*Cisco Systems, USA* lgarratt@cisco.com
[¶]*University of Waterloo, Canada* dstebila@uwaterloo.ca

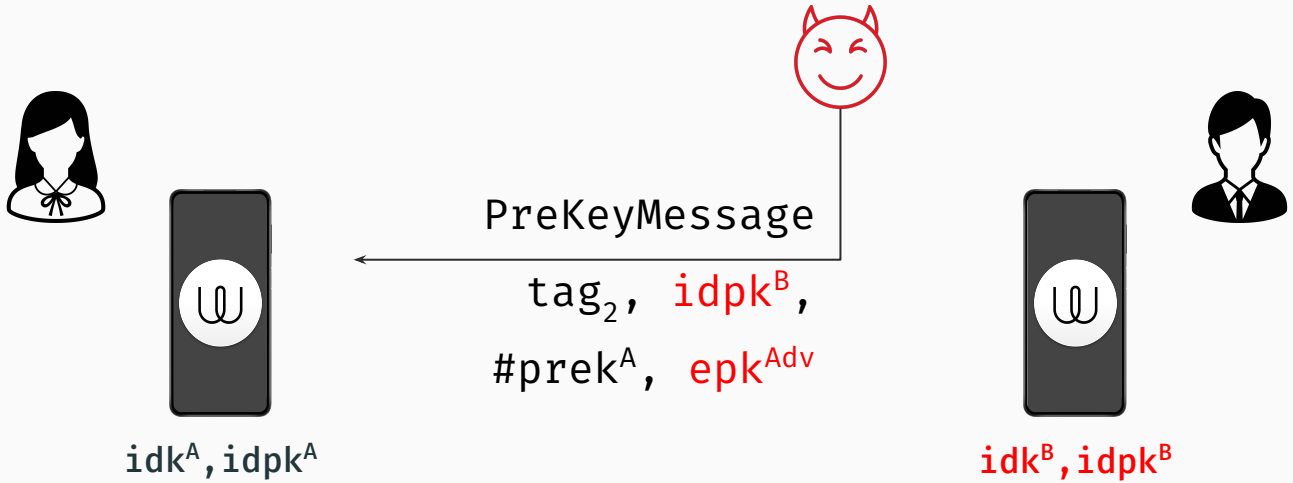
The Case of Wire: Post-Compromise Security

- tag_1:

- tag_1:



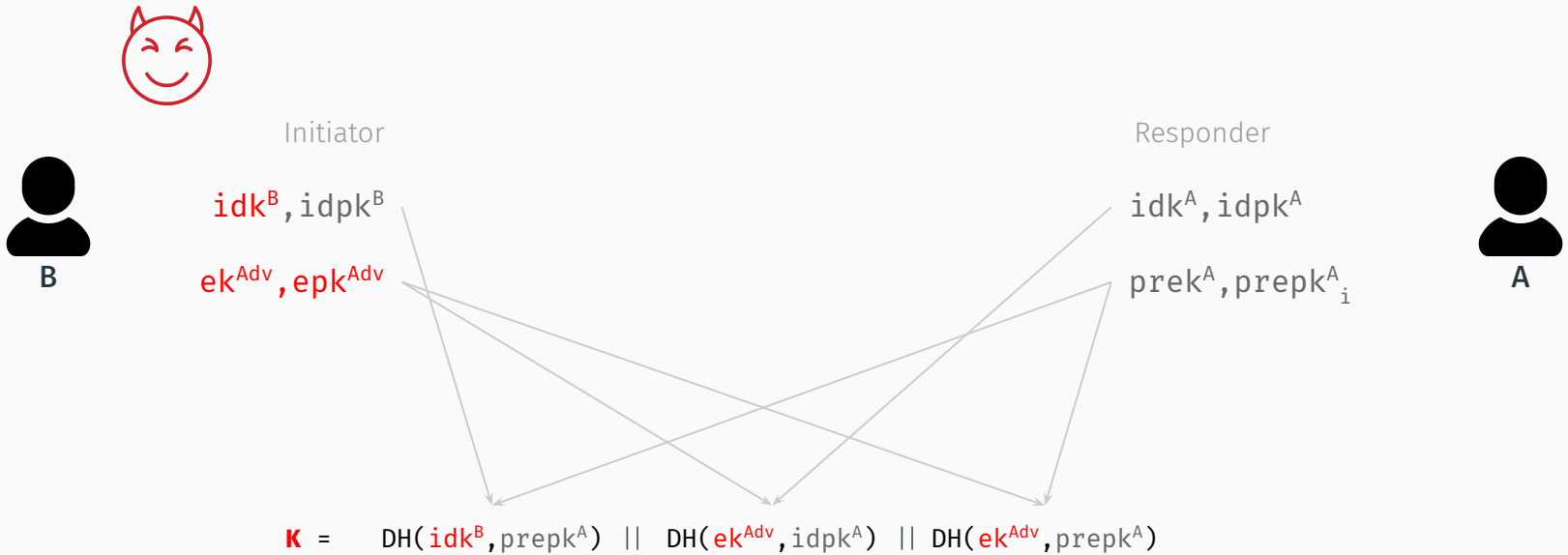
The Case of Wire: Post-Compromise Security



- tag$_1$: 

- tag$_1$: 

Reminder: XPDH



The Case of Wire: Post-Compromise Security

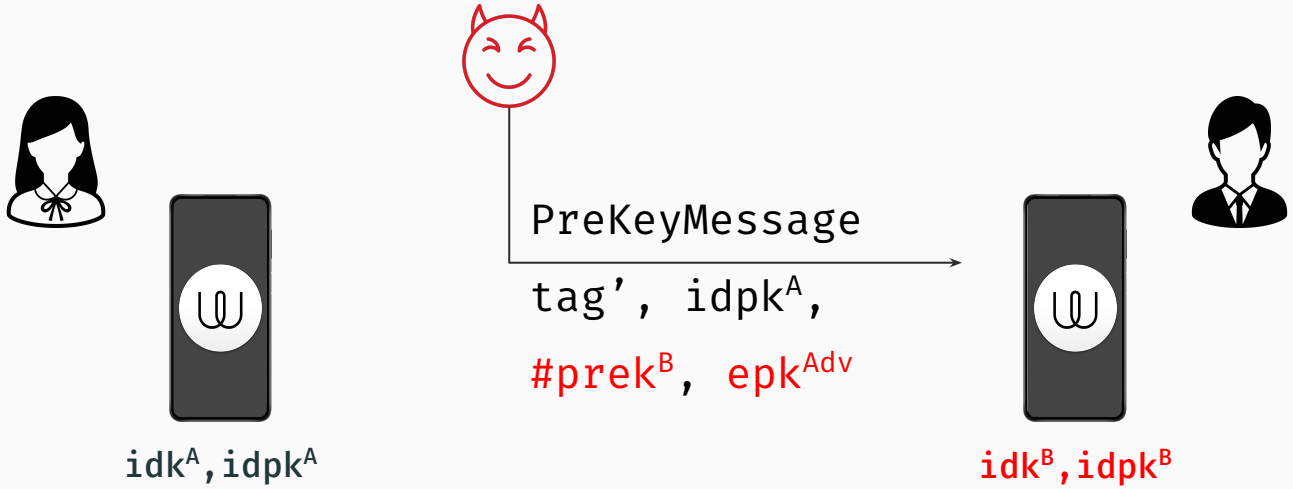
tag$_1$: 

→ tag$_2$: 

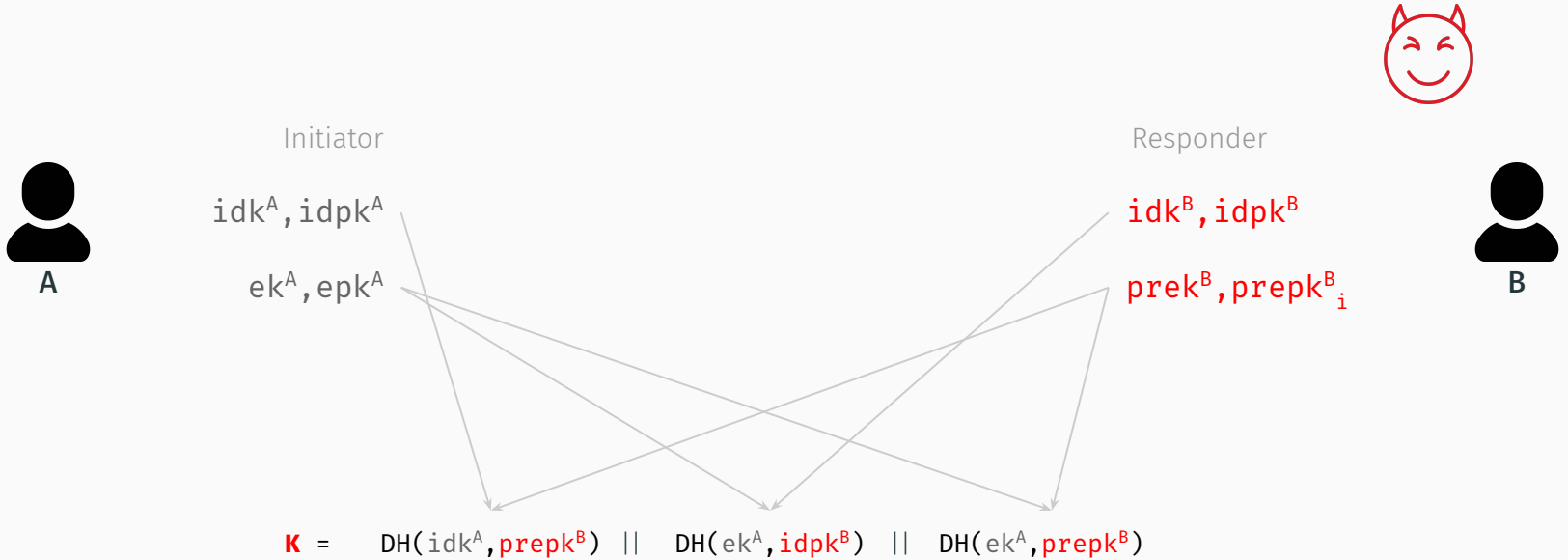
tag$_1$: 

The Case of Wire: Post-Compromise Security

The Case of Wire: Conversation Level PCS

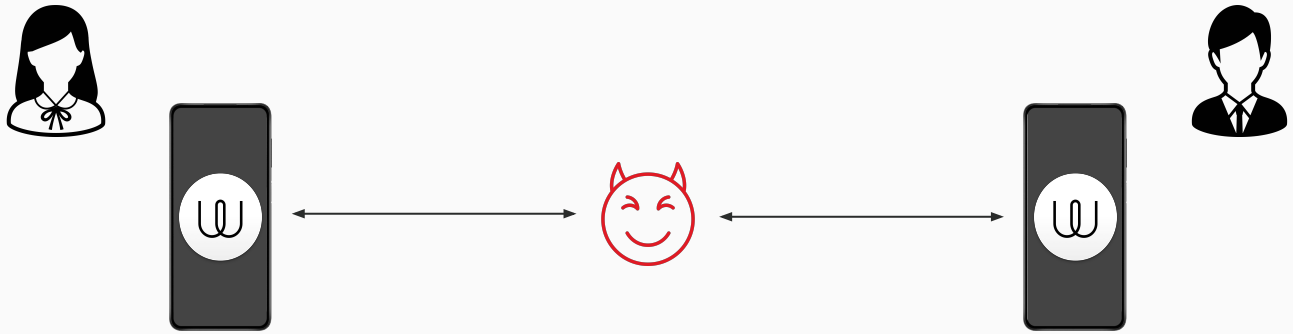


Reminder: XPDH



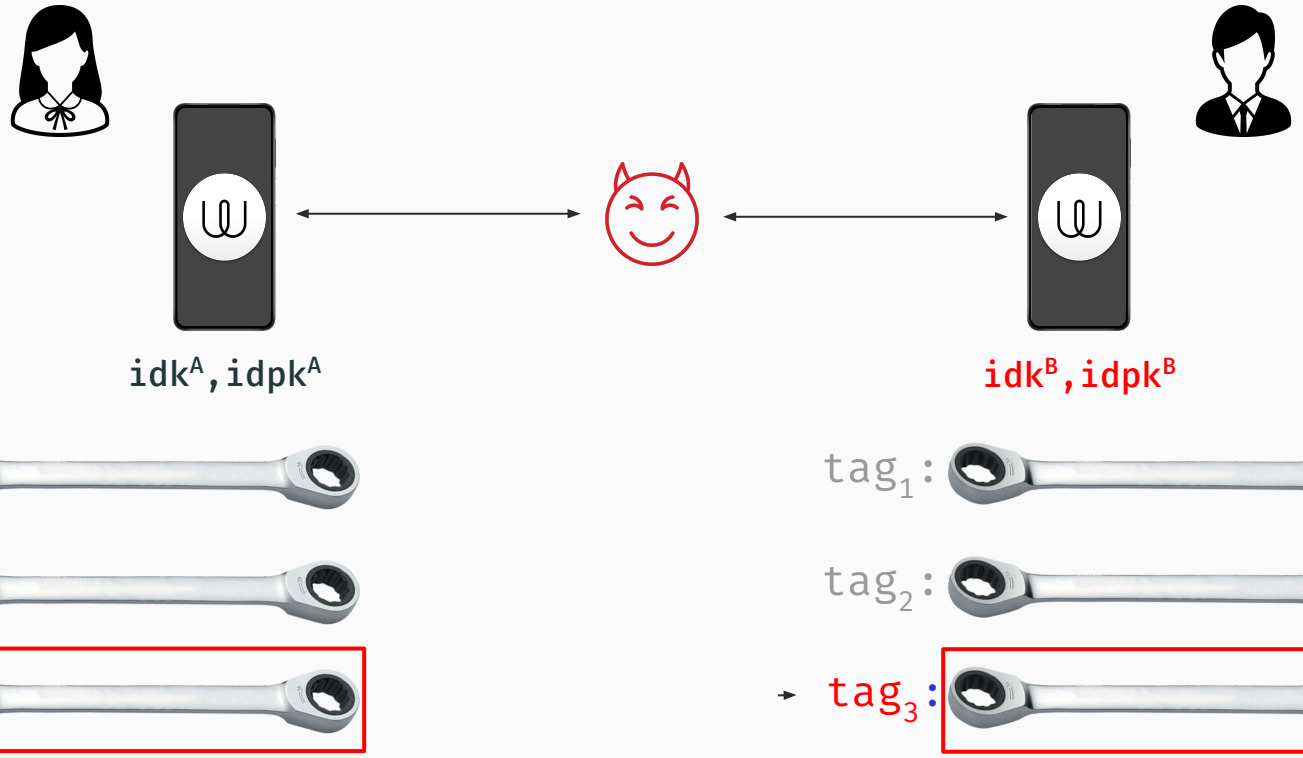
The Case of Wire: Conversation Level PCS

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

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

X3DH

+

DR

+

Sesame

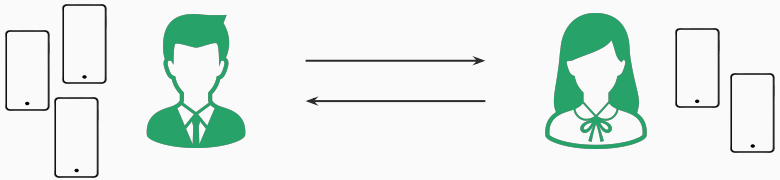
⇓

NO PCS

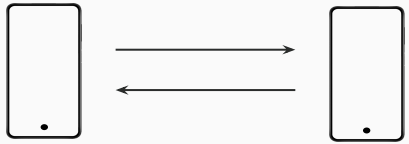
⇓

NO PCS*

Chat



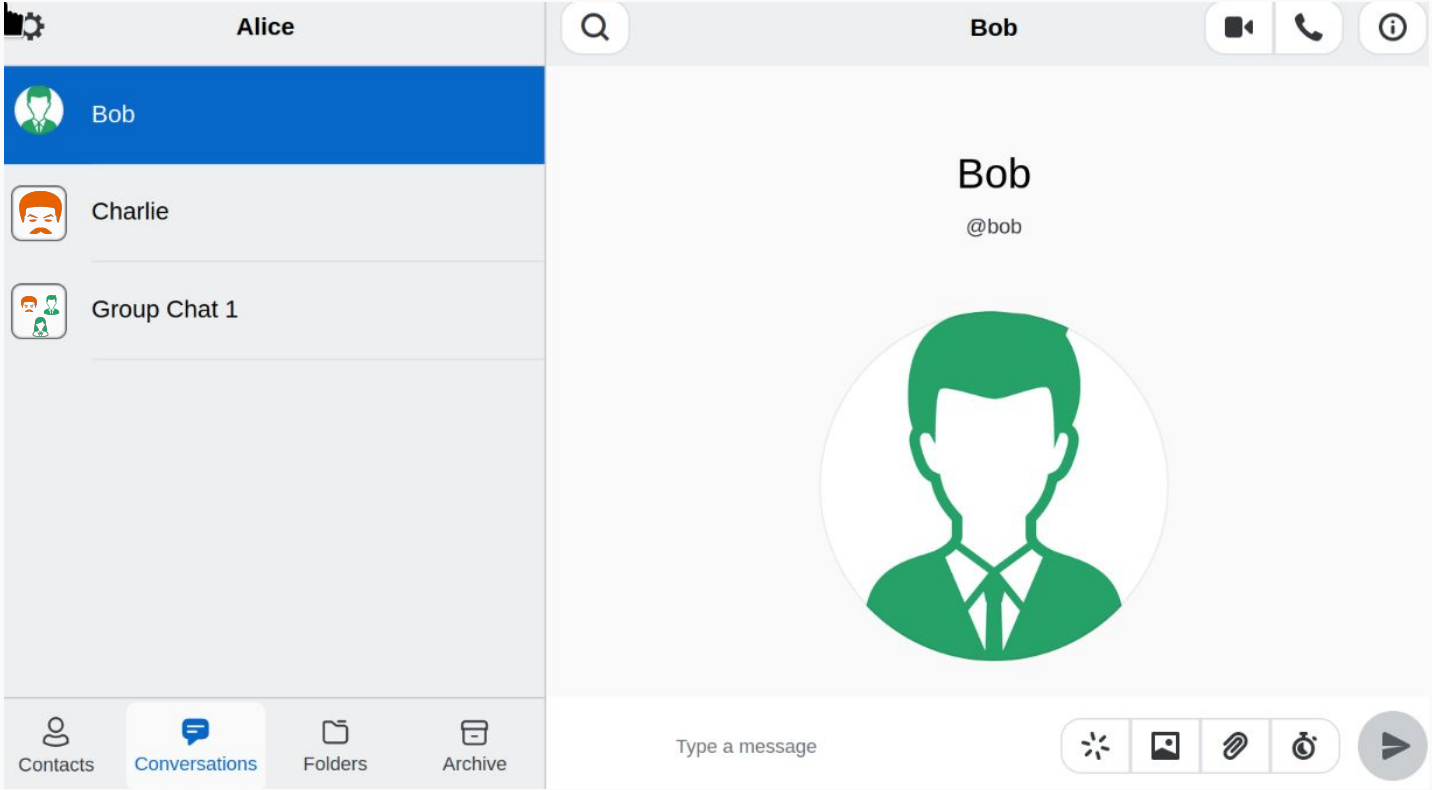
Conversation



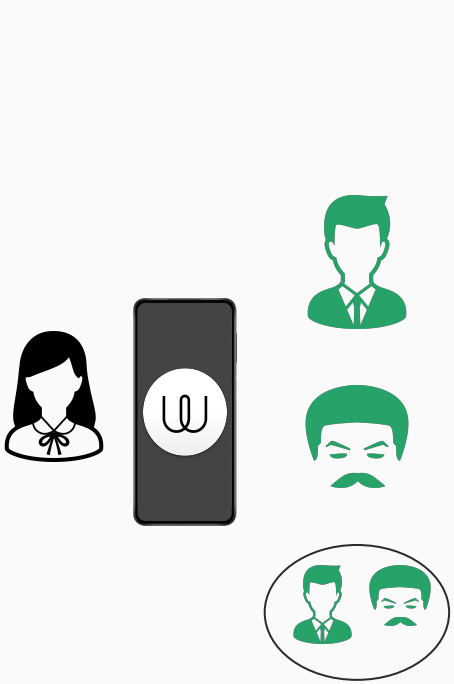
Session

XPDH

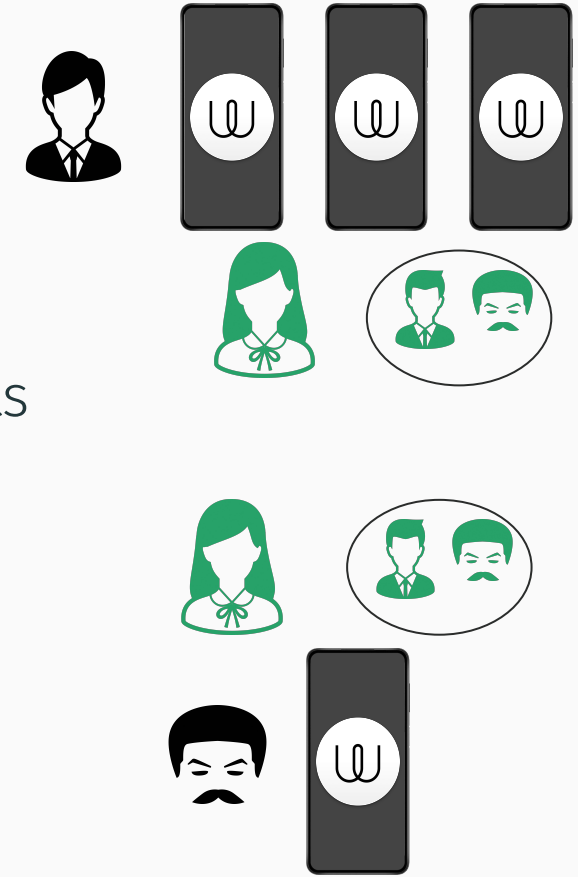
The Case of Wire: Chat Level



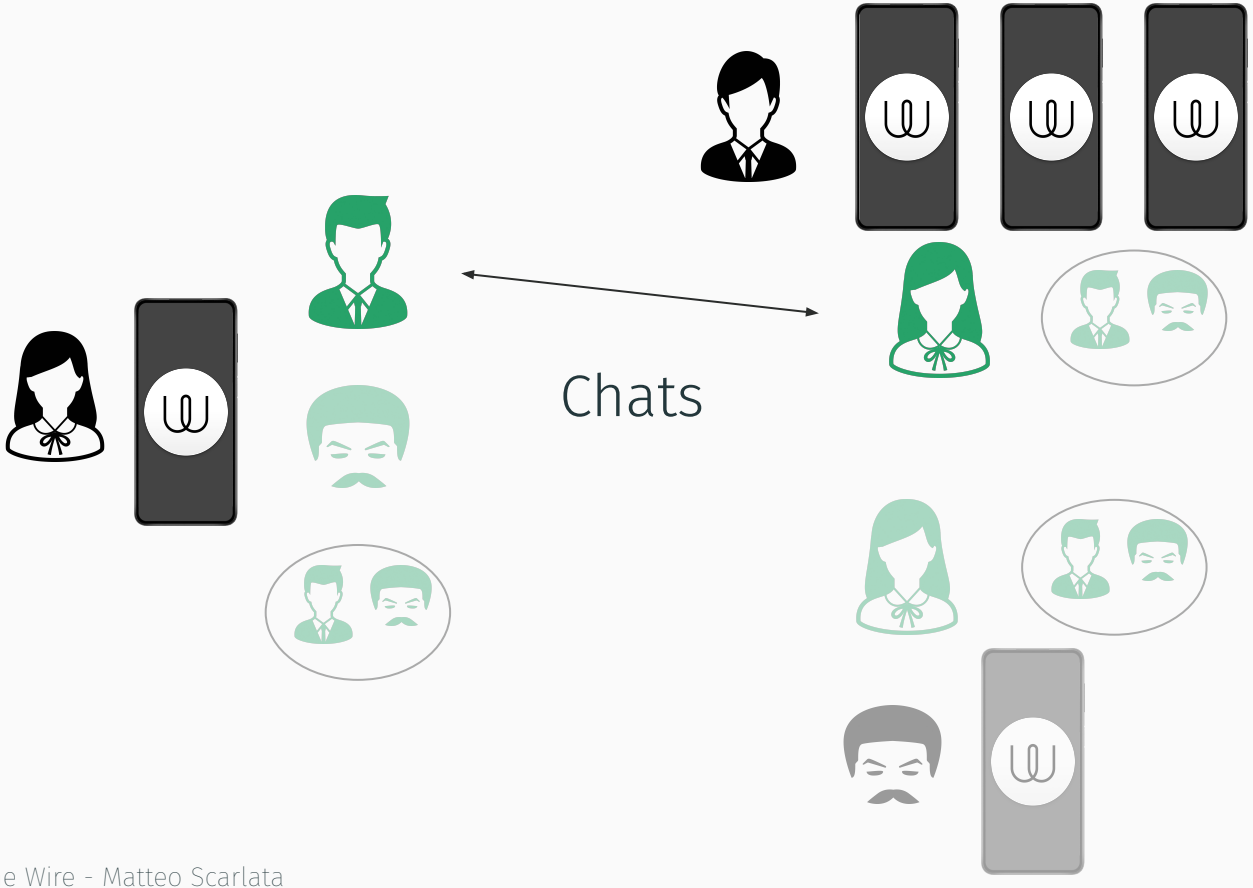
Chat Level Security



Chats



Chat Level Security

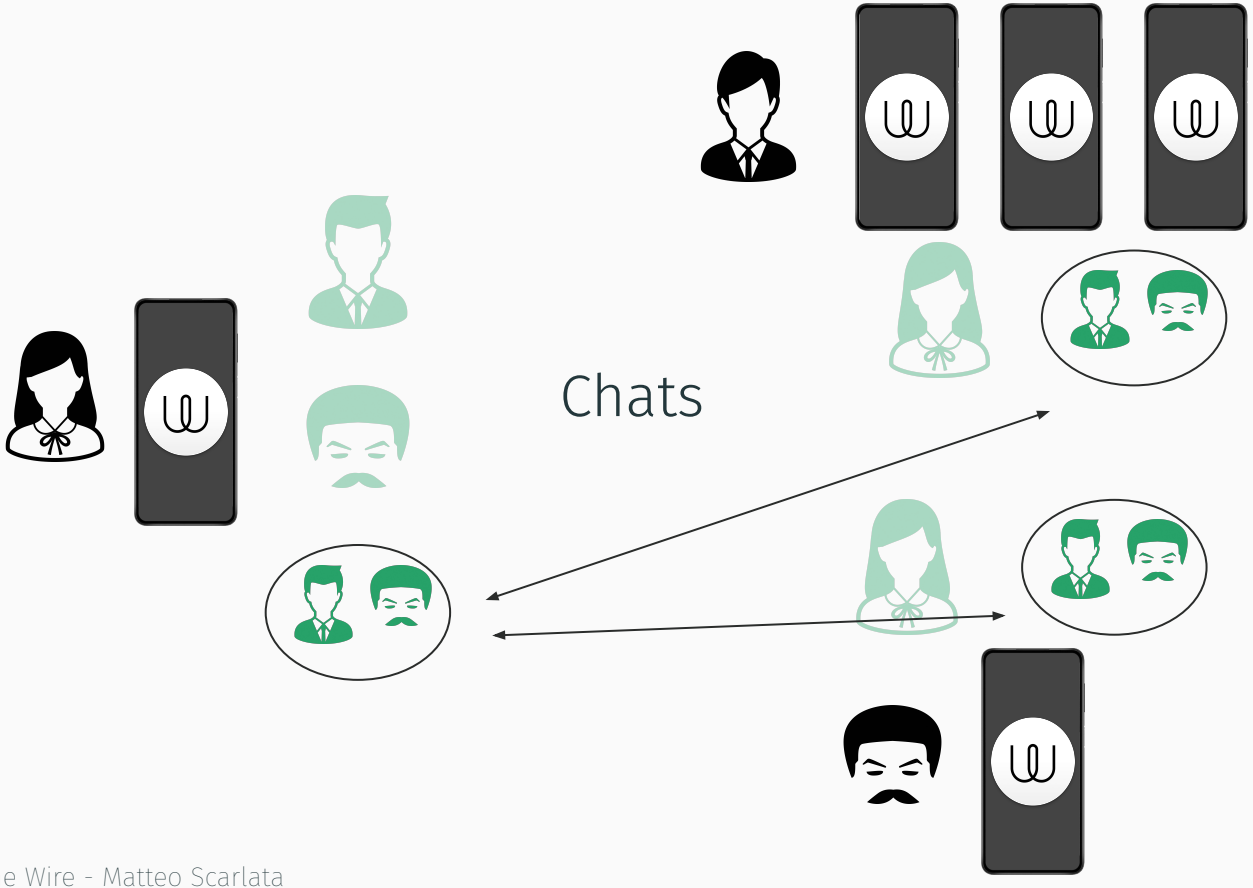


Consistent view

Hi Alice!
I like
pineapple pizza

Hi Bob!
That's not a
crime

Chat Level Security



Consistent view

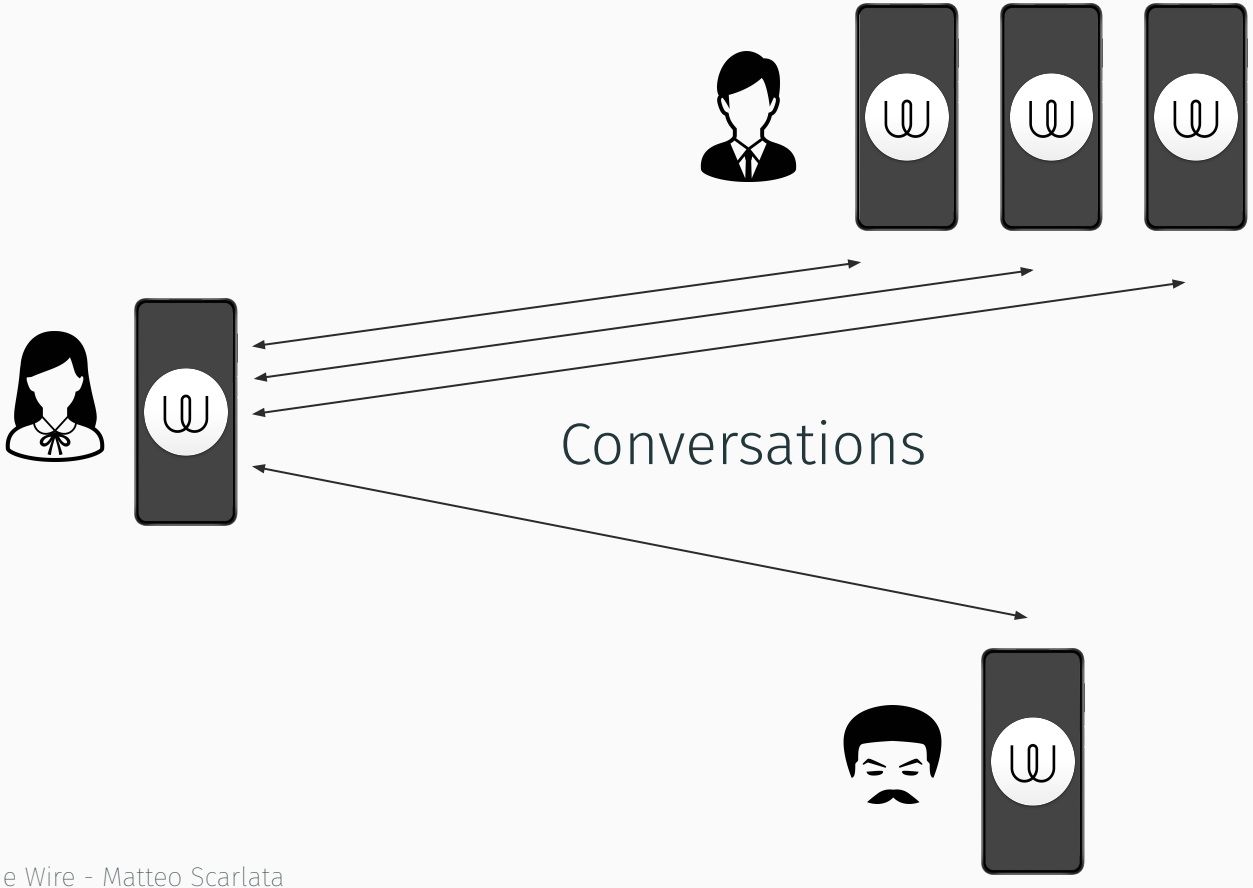
A: we meet at 8

B: let's do 9

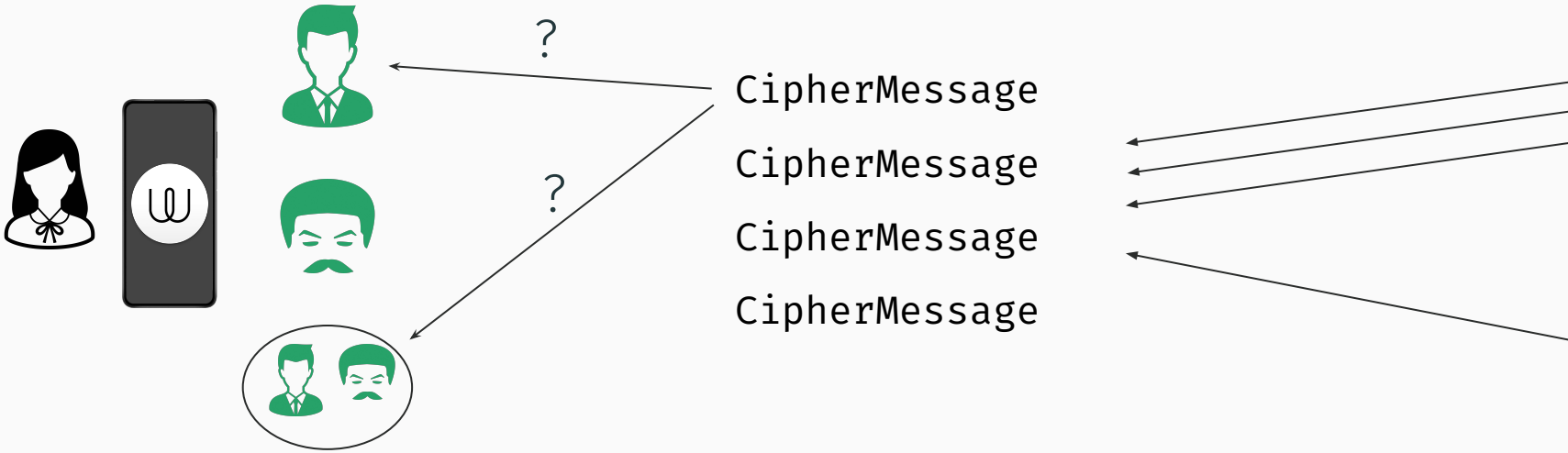
C: yes

A: ok

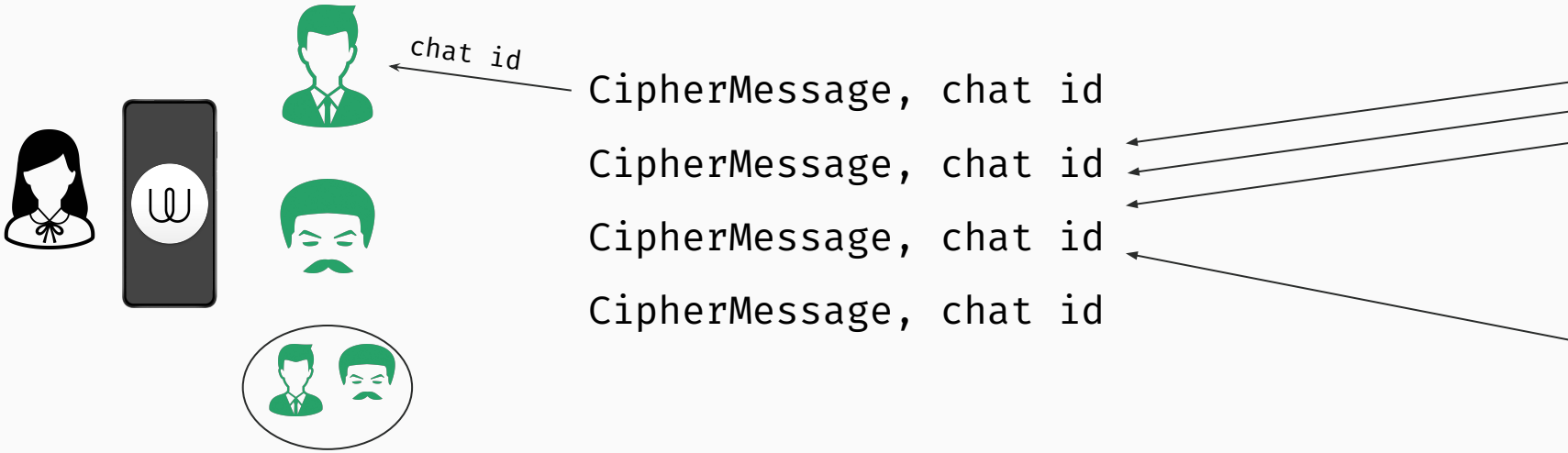
The Case of Wire: Chat Level



The Case of Wire: Chat Level

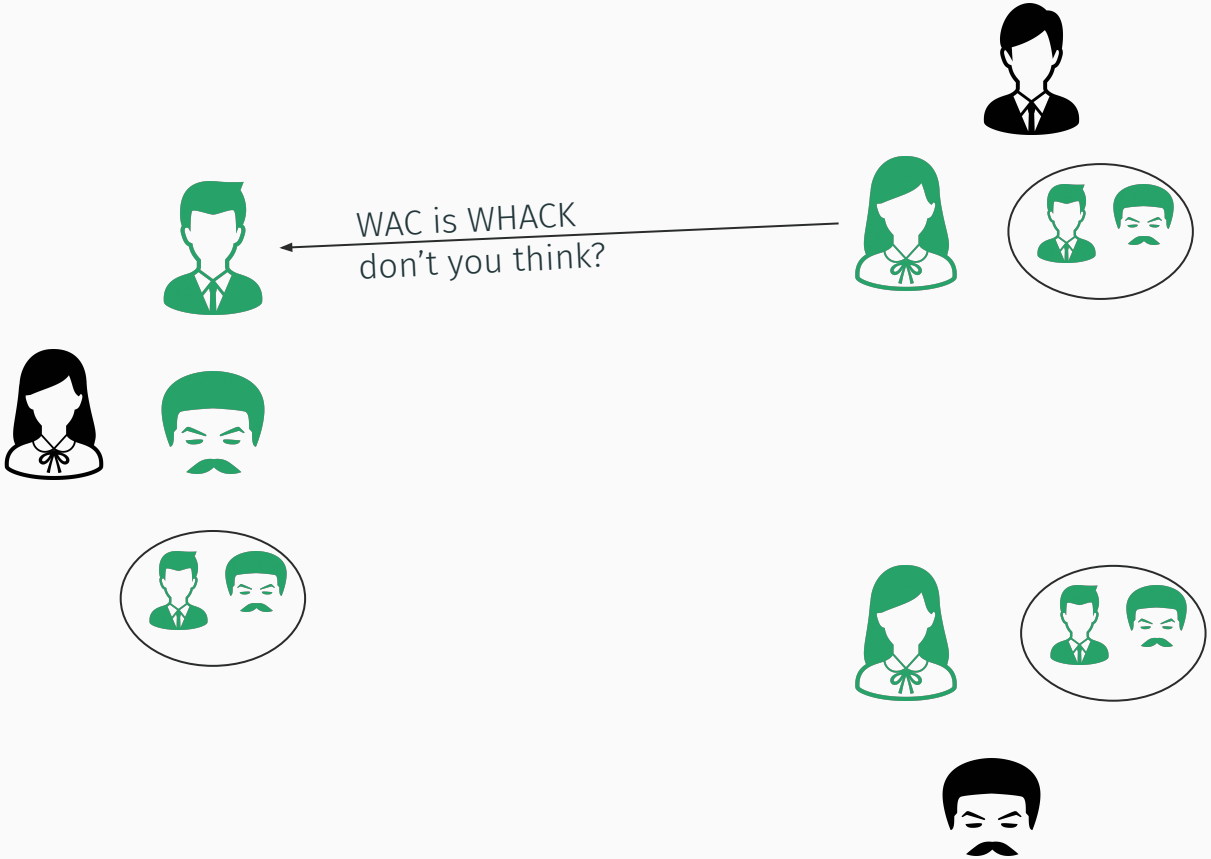


The Case of Wire: Chat Level

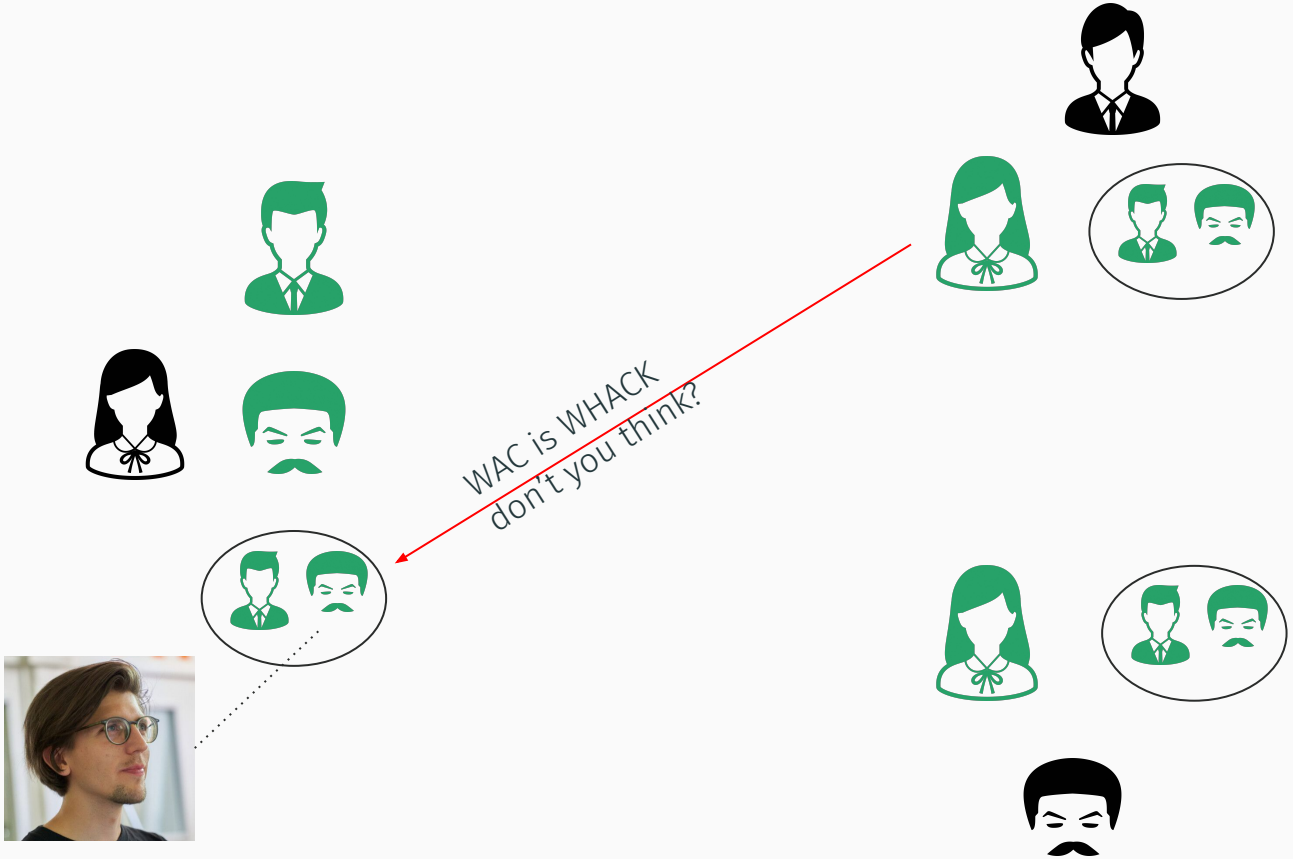


The Case of Wire: Chat Level

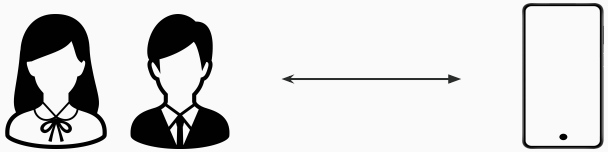
The Case of Wire: Chat Level



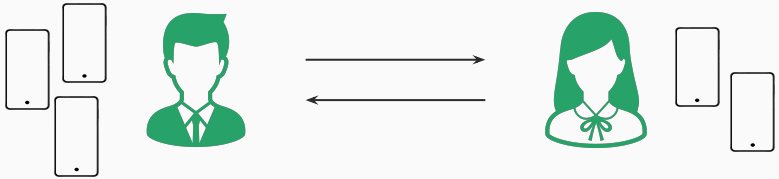
The Case of Wire: Chat Level



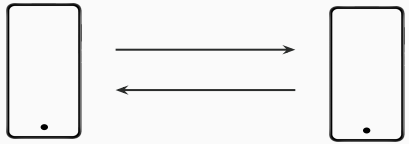
UI



Chat



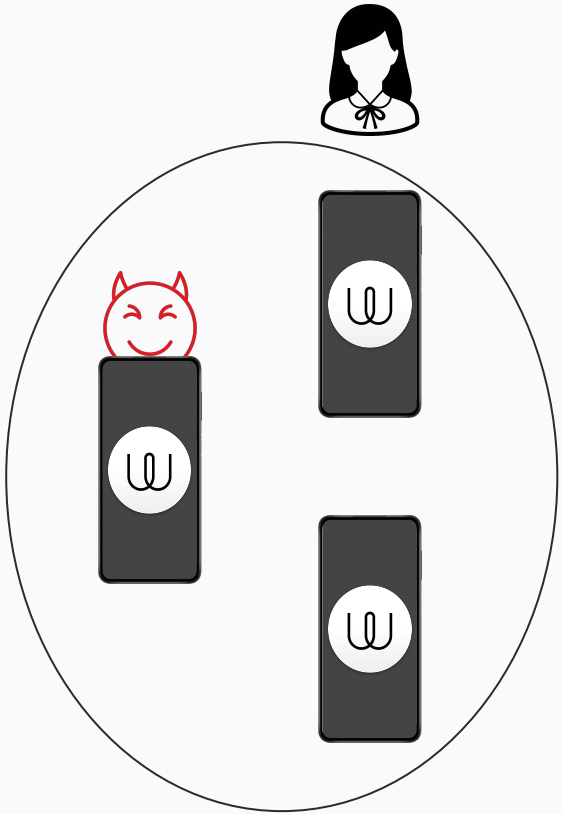
Conversation

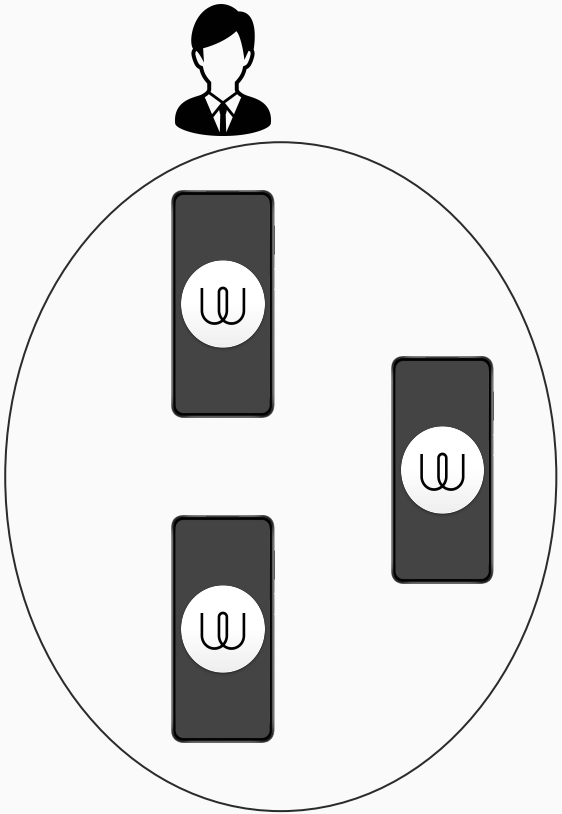


Session

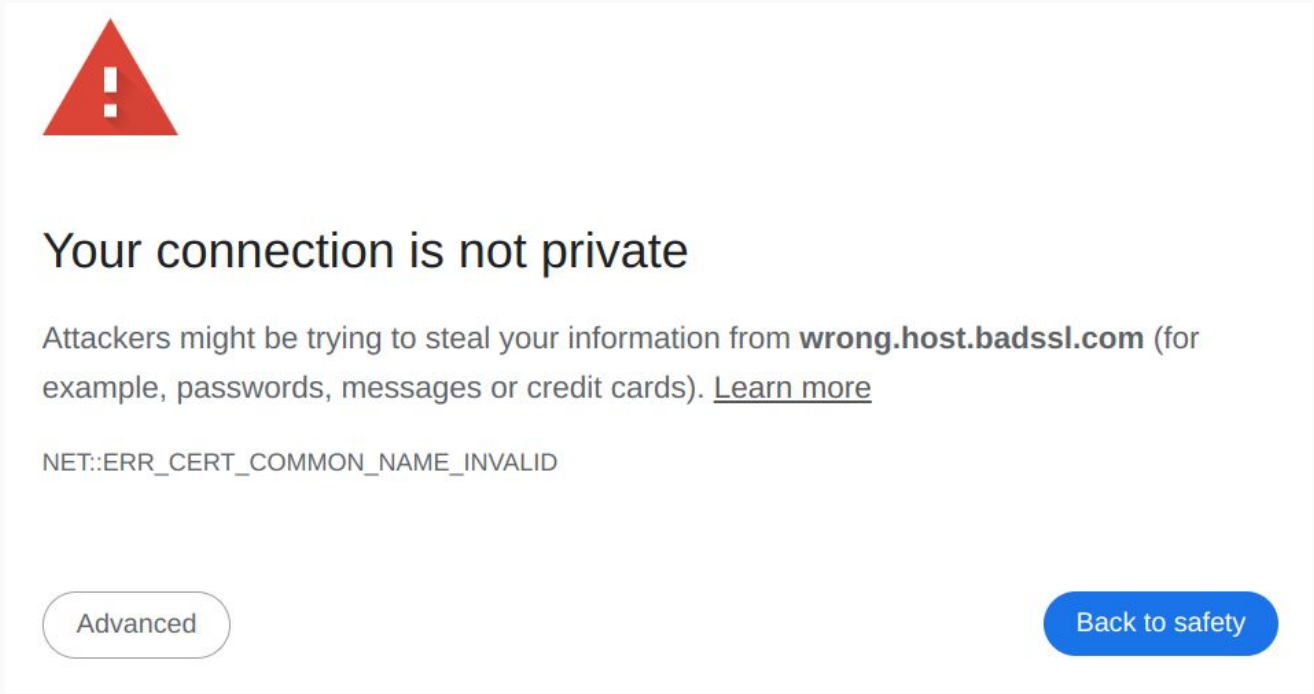
XPDH

The Case of Wire: UI Level

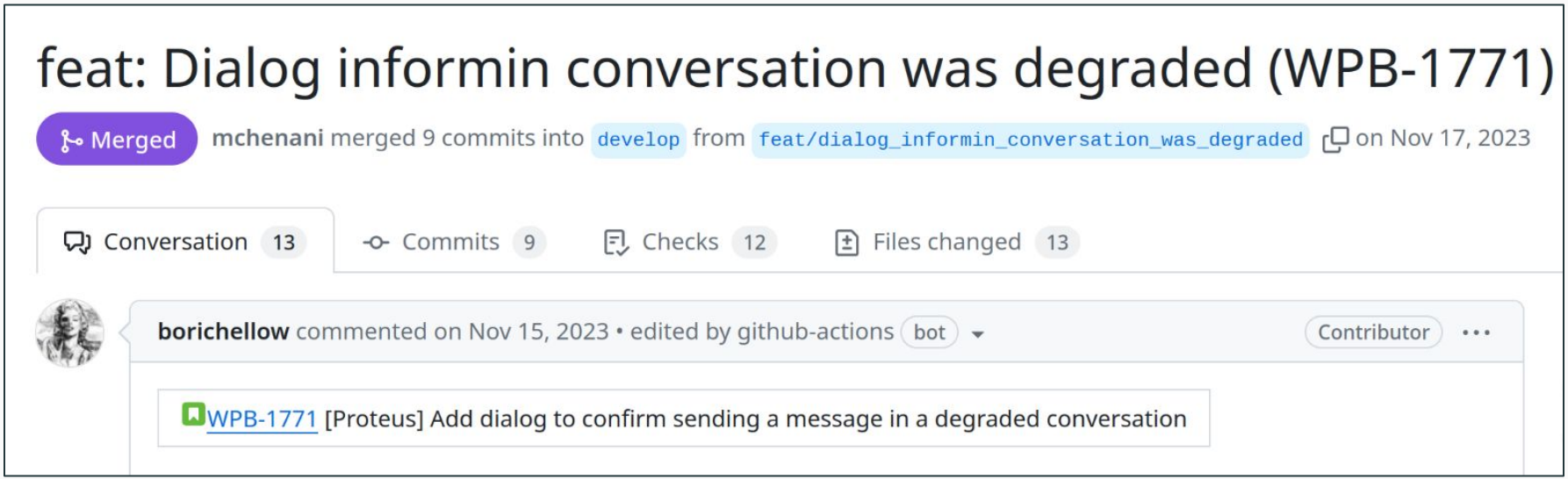




The Case of Wire: UI Level



The Case of Wire: UI Level



The Case of Wire: Disclosure

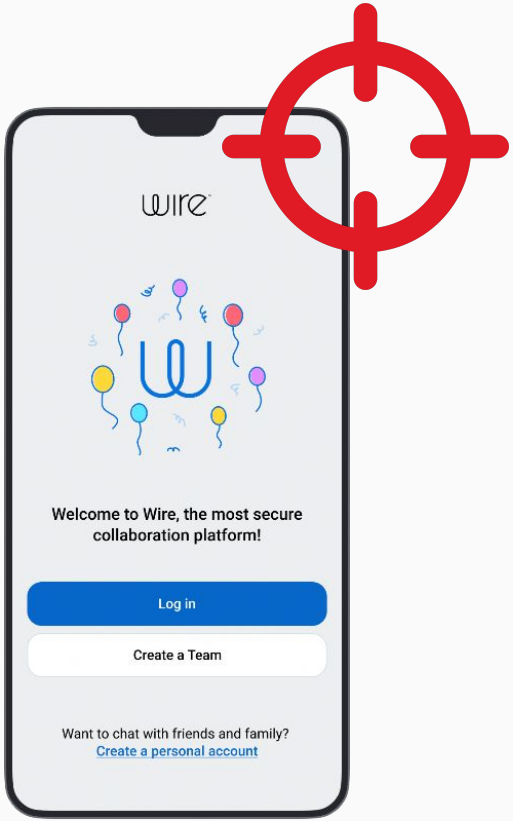
- Disclosed on 13/11/2023, response on 15/11/2023
- UI vulnerability fixed on 17/11/2023
- PCS and group id auth not fixed!
  - Wire to switch to MLS in late 2024

Lessons

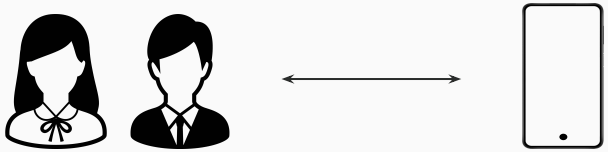
1. Key Exchange +
   Messaging Channel +
   Conversations +
   Chats +
   UI =

Secure Messaging

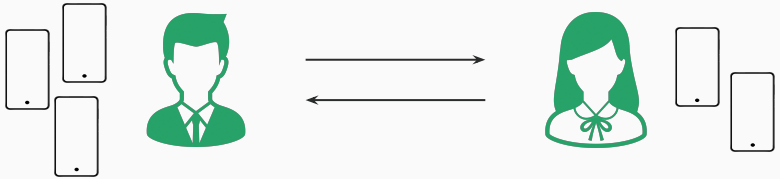
2.



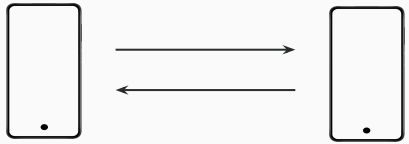
UI



Chat



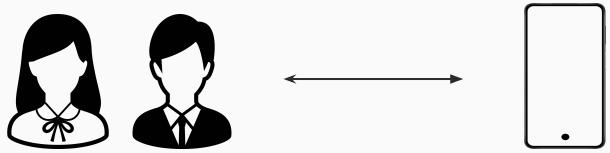
Conversation



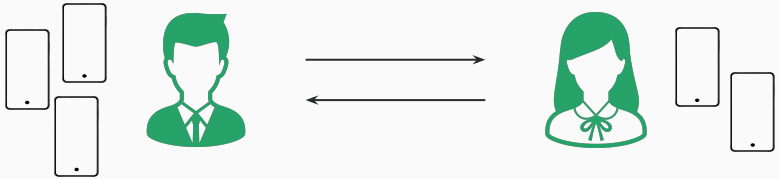
Session

XPDH

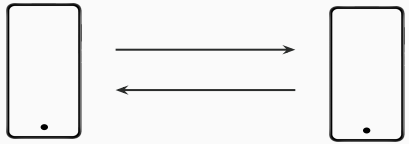
UI



Chat



Conversation

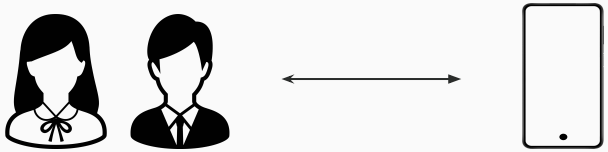


Session

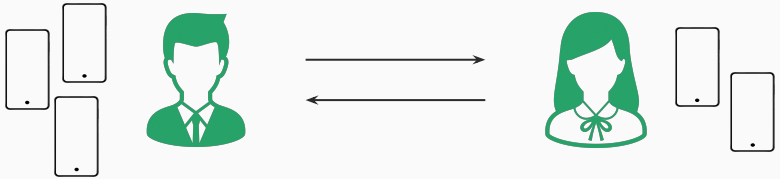
XPDH

Models?

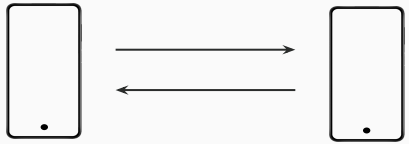
UI



Chat



Conversation



Session

XPDH

WhatsUpp with Sender Keys?
Analysis, Improvements and Security Proofs

David Balbás[1,2] *, Daniel Collins[3] **, and Phillip Gajland[4,5] ***

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

Benjamin Dowling[1] and Britta Hale[2]*

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

Formal Analysis o
Lifting Securi

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

charlie.jacomme@inria.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†

Katriel Cohn-Gordon*, Cas Cremers†, Benjamin Dowling‡, Luke Garratt§, Douglas Stebila¶

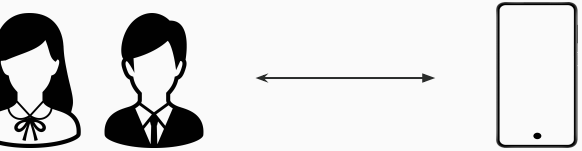
*Independent Scholar me@katriel.co.uk
†CISPA Helmholtz Center for Information Security, Germany cremers@cispa.saarland
‡ETH Zürich, Switzerland benjamin.dowling@inf.ethz.ch
§Cisco Systems, USA lgarratt@cisco.com
¶University of Waterloo, Canada dstebila@uwaterloo.ca

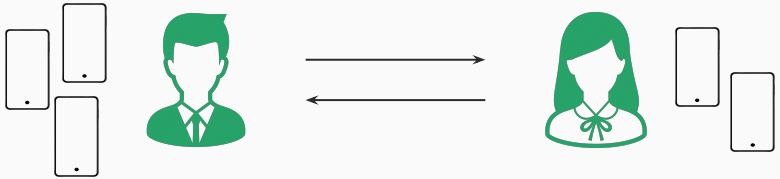
UI

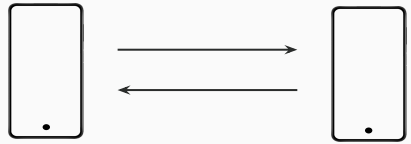
Chat

Conversation

Session



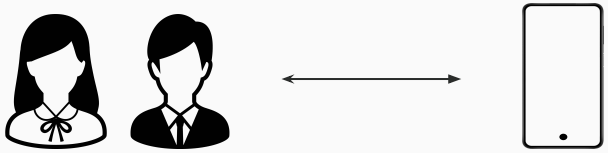




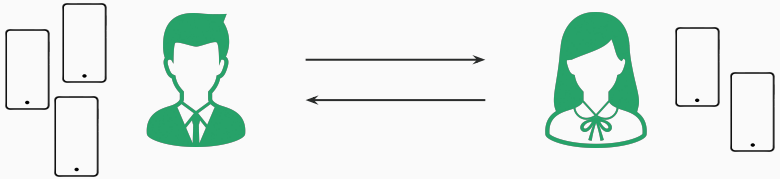
XPDH

Processes?

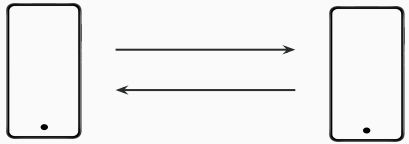
UI



Chat



Conversation



Session

XPDH

Questions?

Matteo Scarlata
scmatteo@ethz.ch

Assets

https://www.svgrepo.com/