Message Injection Attacks Against Signal

Kien Tuong Truong[1], **Noemi Terzo[2]**, Kenny Paterson[1]

[1] ETH Zurich
[2] Max Planck Institute for Security and Privacy

What is “Signal”?

The app?

Signal

The PQXDH Key Agreement Protocol

Revision 3, 2023-05-24, Last Updated: 2024-01-23 [PDF]

Ehren Kret, Rolfe Schmidt

The Double Ratchet Algorithm

Revision 4, 2025-11-04 [PDF]

Trevor Perrin (editor), Moxie Marlinspike, Rolfe Schmidt (revision 3+)

A set of protocols?

Signal

Private Group Messaging

moxie0 on 05 May 2014

The X3DH Key Agreement Protocol

Revision 1, 2016-11-04 [PDF]

Moxie Marlinspike, Trevor Perrin (editor)

Signal

The Sesame Algorithm: Session Management for Asynchronous Message Encryption

Comprehensive Deniability Analysis of Signal Handshake Protocols: X3DH, PQXDH to Fully Post-Quantum with Deniable Ring Signatures

Shuichi Katsumata [1,2] *Guilhem Niot* [1,3] *Ida Tucker* [1]
Thom Wiggers [1]
[1] *PQShield*
[2] *AIST*
[3] *Univ Rennes, CNRS, IRISA*

Formal verification of the PQXDH Post-Quantum key agreement protocol for end-to-end secure messaging

Karthikeyan Bhargavan, *Cryspen;* Charlie Jacomme, *Inria Nancy Grand-Est, Université de Lorraine, LORIA, France;* Franziskus Kiefer, *Cryspen;* Rolfe Schmidt, *Signal Messenger*

Automated Verification for Secure Messaging Protocols and their Implementations: A Symbolic and Computational Approach

Nadim Kobeissi, INRIA Paris
Karthikeyan Bhargavan, INRIA Paris
Bruno Blanchet, INRIA Paris

Security Analysis of Signal's **PQXDH** Handshake

Rune Fiedler[1(✉)] and Felix Günther[2]

[1] Cryptoplexity, Technische Universität Darmstadt, Darmstadt, Germany
rune.fiedler@cryptoplexity.de
[2] IBM Research Europe – Zurich, Rüschlikon, Switzerland
mail@felixguenther.info

A Formal Security Analysis of the Signal Messaging Protocol
(Extended abstract: full version available at [10])

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

University of Oxford, UK katriel.cohn-gordon@cs.ox.ac.uk, cas.cremers@cs.ox.ac.uk, luke.garratt@cs.ox.ac.uk
†Royal Holloway, University of London, UK benjamin.dowling@rhul.ac.uk
‡McMaster University, Canada stebilad@mcmaster.ca

A More Complete Analysis of the Signal Double Ratchet Algorithm

Alexander Bienstock[1(✉)], Jaiden Fairoze[2], Sanjam Garg[2,3], Pratyay Mukherjee[4], and Srinivasan Raghuraman[5]

[1] New York University, New York, USA
abienstock@cs.nyu.edu
[2] UC Berkeley, Berkeley, USA
[3] NTT Research, Sunnyvale, USA
[4] Swirlds Labs, Dallas, USA
[5] Visa Research, Palo Alto, USA

What does it mean to "formally analyze" Signal?

A Deniability Analysis of Signal's Initial Handshake PQXDH

Rune Fiedler, Technische Universität Darmstadt, Darmstadt, Germany, rune.fiedler@cryptoplexity.de
Christian Janson, Technische Universität Darmstadt, Darmstadt, Germany, christian.janson@cryptoplexity.de

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

Cas Cremers, *CISPA Helmholtz Center for Information Security*
Charlie Jacomme*, *Inria Paris, France*
Aurora Naska, *CISPA Helmholtz Center for Information Security*

Clone Detection in Secure Messaging: Improving Post-Compromise Security in Practice

Cas Cremers, CISPA Helmholtz Center for Information Security, Saarbrücken, Germany, cremers@cispa.saarland
Jaiden Fairoze, CISPA Helmholtz Center for Information Security, Saarbrücken, Germany, jfairoze@student.unimelb.edu.au
Benjamin Kiesl, CISPA Helmholtz Center for Information Security, Saarbrücken, Germany, benjamin.kiesl@cispa.saarland
Aurora Naska, CISPA Helmholtz Center for Information Security, Saarbrücken, Germany, s8aunask@stud.uni-saarland.de

The Signal Private Group System and Anonymous Credentials Supporting Efficient Verifiable Encryption *

Melissa Chase, Microsoft Research, Redmond, Washington, USA, melissac@microsoft.com
Trevor Perrin, Signal Technology Foundation, USA, trevp@signal.org
Greg Zaverucha, Microsoft Research, Redmond, Washington, USA, gregz@microsoft.com

Analyzing Group Chat Encryption in MLS, Session, Signal, and Matrix

Joseph Jaeger and Akshaya Kumar

School of Cybersecurity and Privacy
Georgia Institute of Technology, Atlanta, Georgia, US
{josephjaeger,akshayakumar}@gatech.edu

WhatsUpp with Sender Keys? Analysis, Improvements and Security Proofs

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

[1] IMDEA Software Institute, Spain
[2] Universidad Politécnica de Madrid, Spain
[3] EPFL, Switzerland
[4] Max Planck Institute for Security and Privacy, Germany
[5] Ruhr University Bochum, Germany

The Double Ratchet: Security Notions, Proofs, and Modularization for the Signal Protocol

Joël Alwen*, Wickr Inc., jalwen@wickr.com
Sandro Coretti†, New York University, corettis@nyu.edu
Yevgeniy Dodis‡, New York University, dodis@cs.nyu.edu

February 21, 2020

What don't we know about Signal?

Comprehensive Deniability Analysis of Signal Handshake Protocols: X3DH, PQXDH to Fully Post-Quantum with Deniable Ring Signatures

Shuichi Katsumata [1,2] *Guilhem Niot* [1,3] *Ida Tucker* [1]
Thom Wiggers [1]
[1] *PQShield*
[2] *AIST*
[3] *Univ Rennes, CNRS, IRISA*

Formal verification of the PQXDH Post-Quantum key agreement protocol for end-to-end secure messaging

Karthikeyan Bhargavan, *Cryspen;* Charlie Jacomme, *Inria Nancy Grand-Est, Université de Lorraine, LORIA, France;* Franziskus Kiefer, *Cryspen;* Rolfe Schmidt, *Signal Messenger*

Automated Verification for Secure Messaging Protocols and their Implementations: A Symbolic and Computational Approach

Nadim Kobeissi, INRIA Paris
Karthikeyan Bhargavan, INRIA Paris
Bruno Blanchet, INRIA Paris

Security Analysis of Signal's **PQXDH** Handshake

Rune Fiedler[1(✉)] and Felix Günther[2]
[1] Cryptoplexity, Technische Universität Darmstadt, Darmstadt, Germany
rune.fiedler@cryptoplexity.de
[2] IBM Research Europe – Zurich, Rüschlikon, Switzerland
mail@felixguenther.info

A Formal Security Analysis of the Signal Messaging Protocol

(Extended abstract: full version available at [10])

Katriel Cohn-Gordon*, Cas Cremers*, Benjamin Dowling†, Luke Garratt*, Douglas Stebila‡
*University of Oxford, UK — katriel.cohn-gordon@cs.ox.ac.uk, cas.cremers@cs.ox.ac.uk, luke.garratt@cs.ox.ac.uk
†Royal Holloway, University of London, UK — benjamin.dowling@rhul.ac.uk
‡McMaster University, Canada — stebilad@mcmaster.ca

A More Complete Analysis of the Signal Double Ratchet Algorithm

Alexander Bienstock[1(✉)], Jaiden Fairoze[2], Sanjam Garg[2,3], Pratyay Mukherjee[4], and Srinivasan Raghuraman[5]
[1] New York University, New York, USA
abienstock@cs.nyu.edu
[2] UC Berkeley, Berkeley, USA
[3] NTT Research, Sunnyvale, USA
[4] Swirlds Labs, Dallas, USA
[5] Visa Research, Palo Alto, USA

A Deniability Analysis of Signal's Initial Handshake PQXDH

Rune Fiedler, Technische Universität Darmstadt, Darmstadt, Germany, rune.fiedler@cryptoplexity.de
Christian Janson, Technische Universität Darmstadt, Darmstadt, Germany, christian.janson@cryptoplexity.de

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

Cas Cremers, *CISPA Helmholtz Center for Information Security*
Charlie Jacomme*, *Inria Paris, France*
Aurora Naska, *CISPA Helmholtz Center for Information Security*

Clone Detection in Secure Messaging: Improving Post-Compromise Security in Practice

Cas Cremers, CISPA Helmholtz Center for Information Security, Saarbrücken, Germany, cremers@cispa.saarland
Jaiden Fairoze, CISPA Helmholtz Center for Information Security, Saarbrücken, Germany, jfairoze@student.unimelb.edu.au
Benjamin Kiesl, CISPA Helmholtz Center for Information Security, Saarbrücken, Germany, benjamin.kiesl@cispa.saarland
Aurora Naska, CISPA Helmholtz Center for Information Security, Saarbrücken, Germany, s8aunask@stud.uni-saarland.de

The Signal Private Group System and Anonymous Credentials Supporting Efficient Verifiable Encryption *

Melissa Chase, Microsoft Research, Redmond, Washington, USA, melissac@microsoft.com
Trevor Perrin, Signal Technology Foundation, USA, trevp@signal.org
Greg Zaverucha, Microsoft Research, Redmond, Washington, USA, gregz@microsoft.com

Analyzing Group Chat Encryption in MLS, Session, Signal, and Matrix

Joseph Jaeger and Akshaya Kumar
School of Cybersecurity and Privacy
Georgia Institute of Technology, Atlanta, Georgia, US
{josephjaeger,akshayakumar}@gatech.edu

The Double Ratchet: Security Notions, Proofs, and Modularization for the Signal Protocol

Joël Alwen*, Wickr Inc., jalwen@wickr.com
Sandro Coretti†, New York University, corettis@nyu.edu
Yevgeniy Dodis‡, New York University, dodis@cs.nyu.edu

February 21, 2020

WhatsUpp with Sender Keys? Analysis, Improvements and Security Proofs

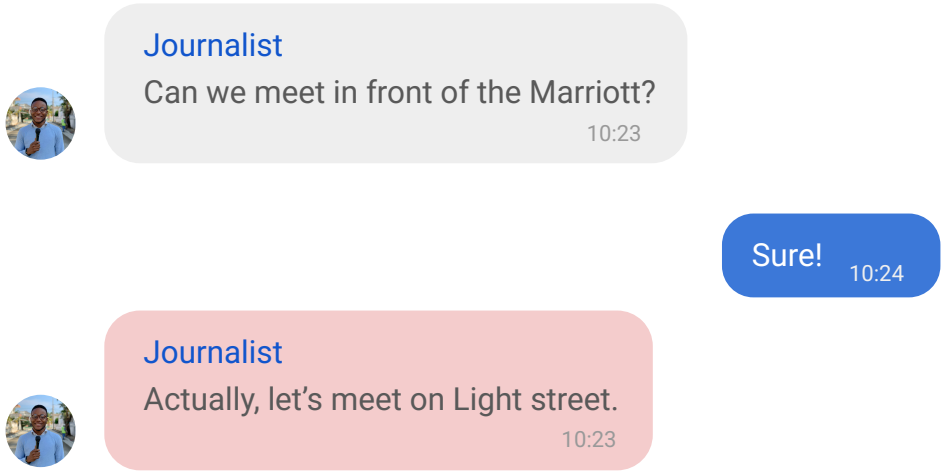
David Balbás[1,2] *, Daniel Collins[3] **, and Phillip Gajland[4,5] ***
[1] IMDEA Software Institute, Spain
[2] Universidad Politécnica de Madrid, Spain
[3] EPFL, Switzerland
[4] Max Planck Institute for Security and Privacy, Germany
[5] Ruhr University Bochum, Germany

Our Contributions

Two attacks that allow a malicious server to inject arbitrary messages in a conversation, undetected

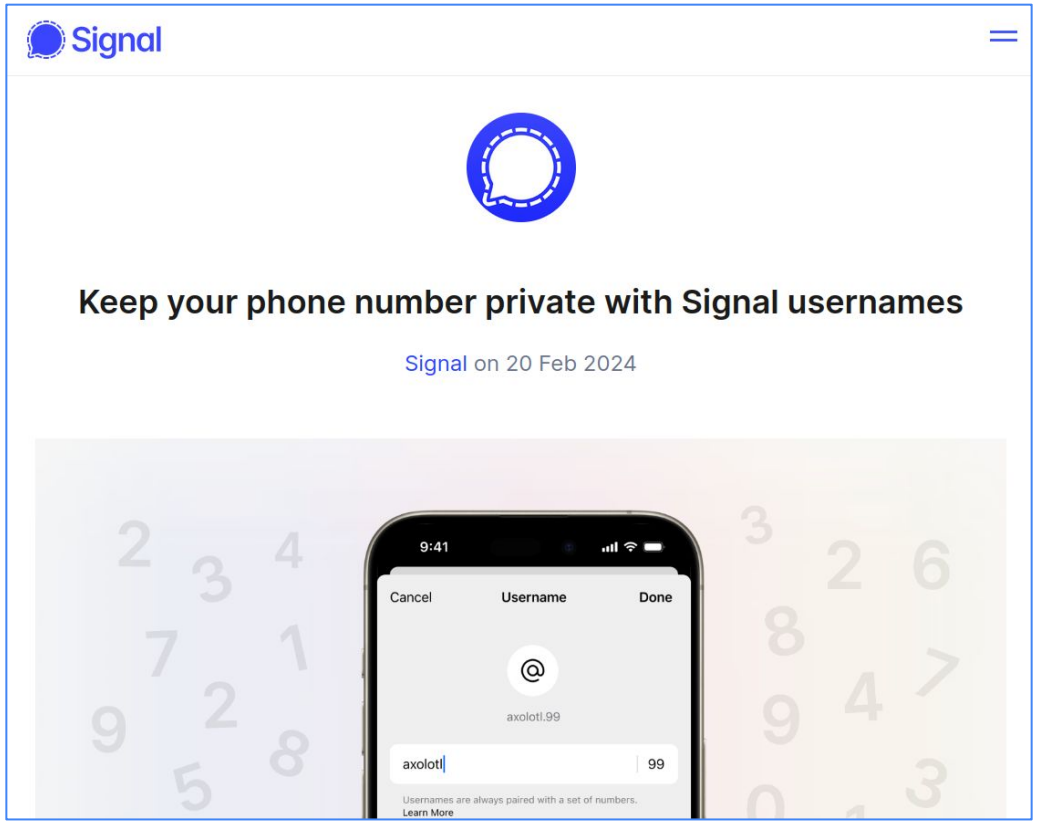
and

Detailed descriptions of protocols that were never analyzed and that affect the security of conversations in Signal.

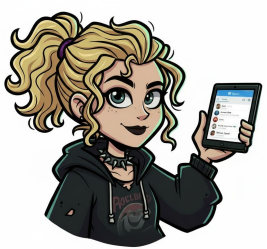


Attack 1: Usernames and Session Handling

Introduction of usernames in Signal



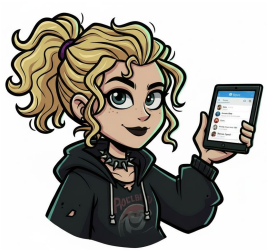
Phone Numbers vs Usernames

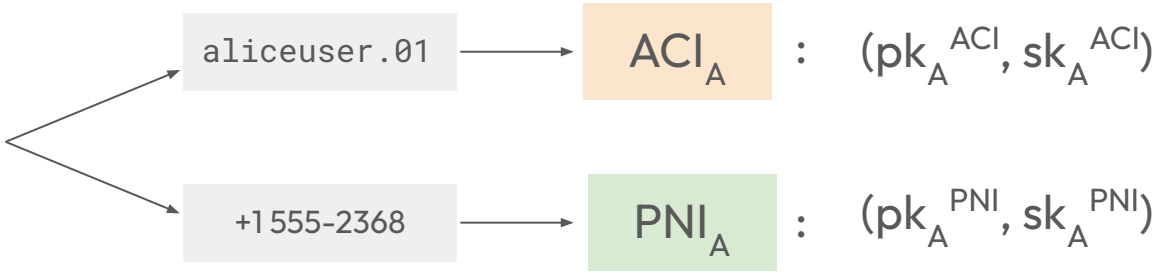


+1 555-2368 → PNI_A : (pk_A^{PNI}, sk_A^{PNI})

PNI: Phone Number Identifier

Phone Numbers vs Usernames

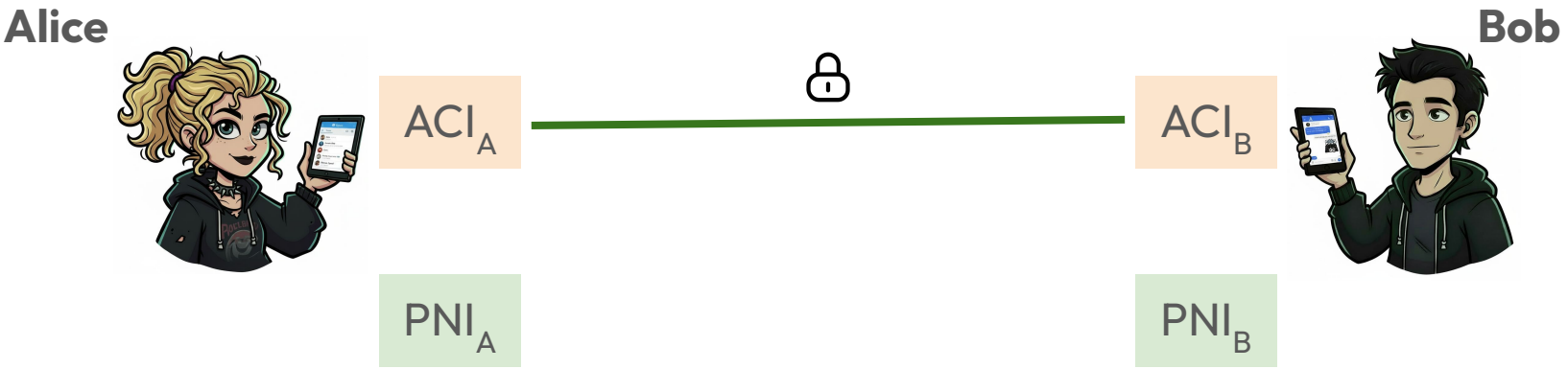




PNI: Phone Number Identifier

ACI: Account Identifier

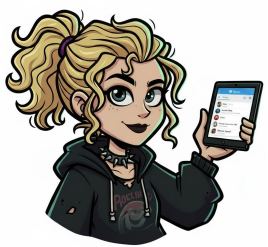
ACIs, PNIs and sessions



ACI_A — ACI_B session: by username

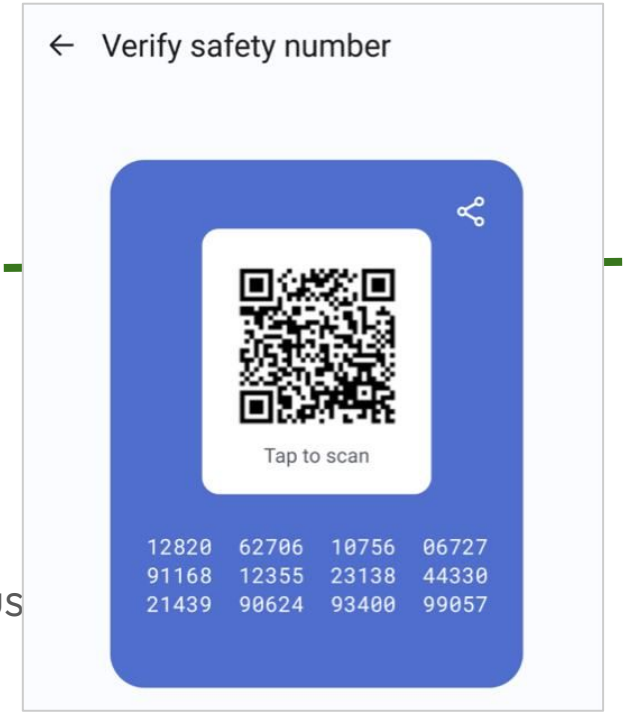
ACIs, PNIs and sessions

Alice



ACI_A

PNI_A



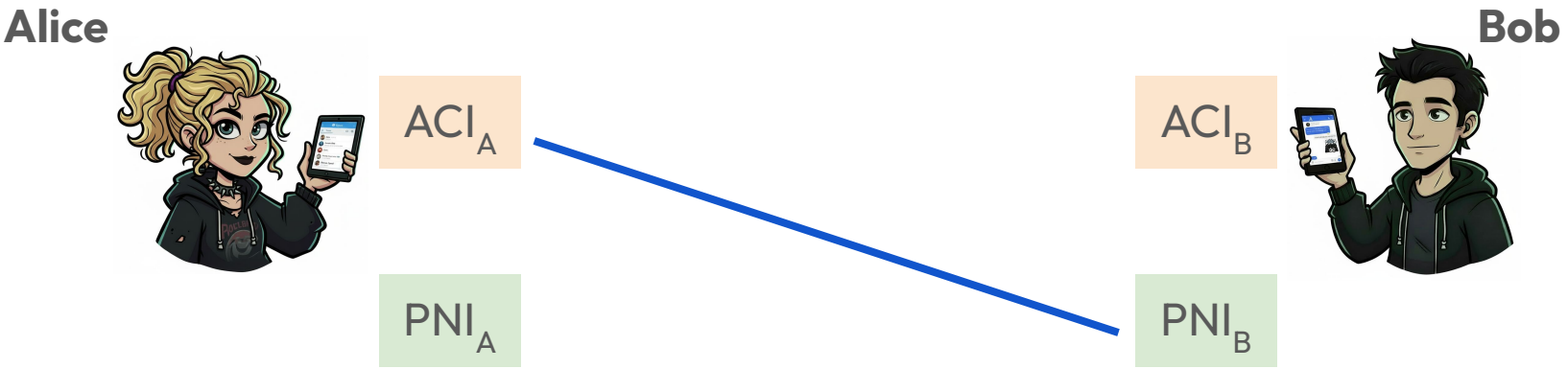
ACI_B

PNI_B

Bob

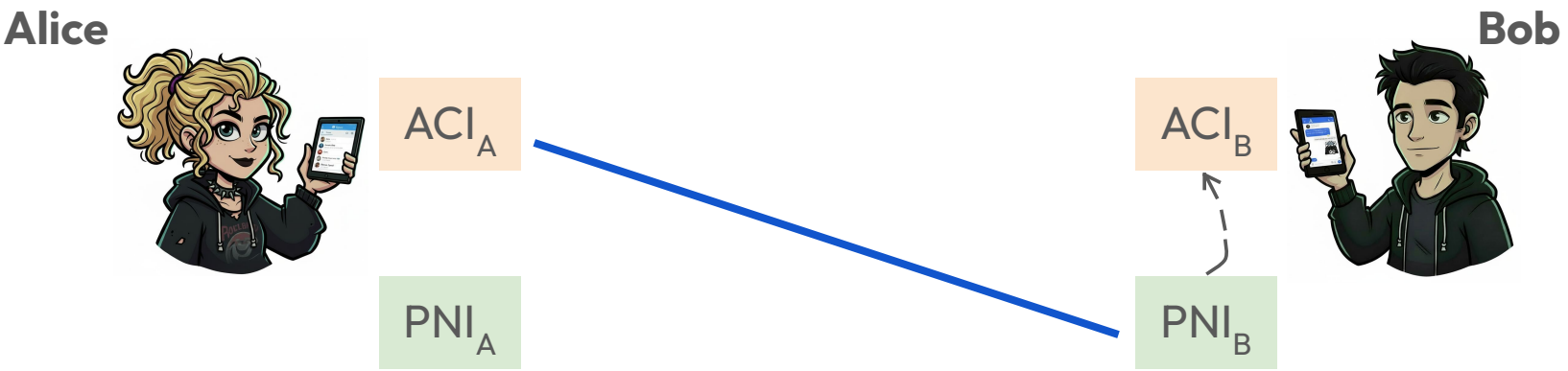
ACI_A — ACI_B session: by us

ACIs, PNIs and sessions



ACI_A — PNI_B session: by phone number

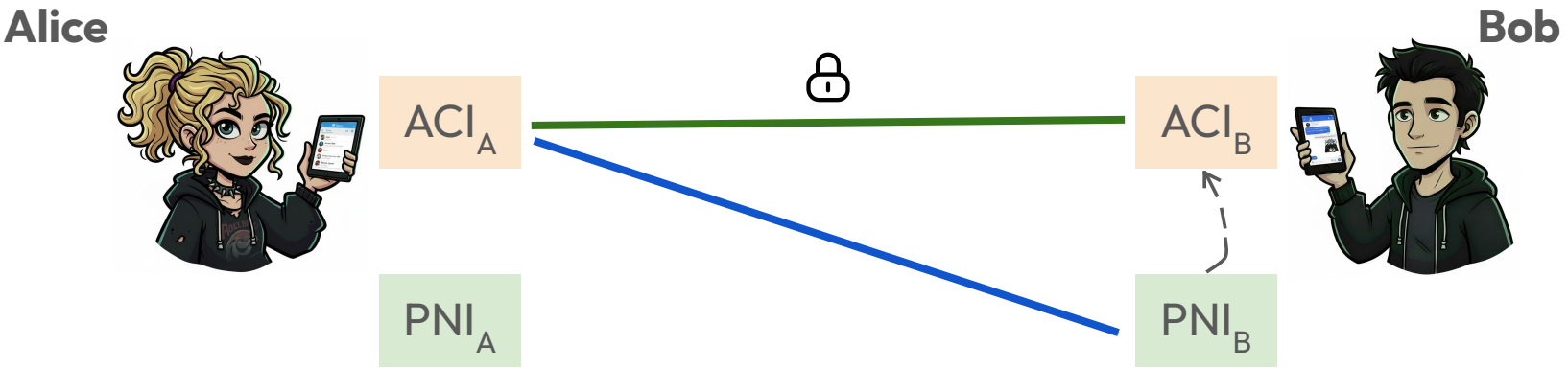
ACIs, PNIs and sessions



ACI_A — PNI_B session: by phone number

upgrade to ACI...

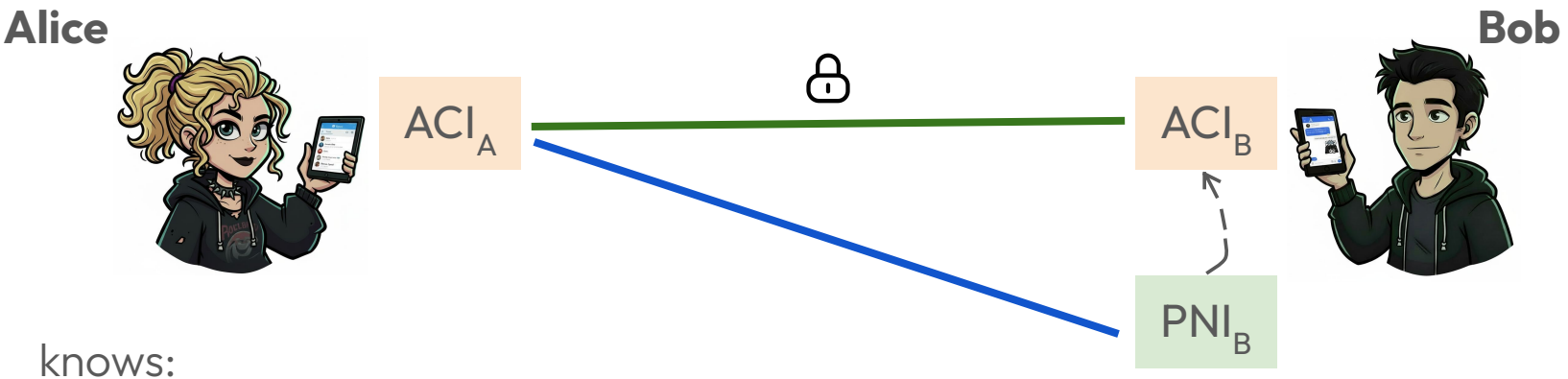
ACIs, PNIs and sessions



ACI$_A$ — PNI$_B$ session: by phone number

upgrade to ACI... new ACI$_A$ — ACI$_B$ session!

“PNI-to-ACI” protocol



knows:

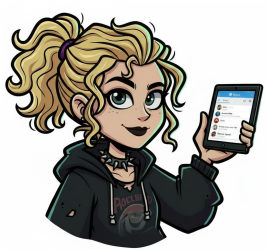
PNI_B , pk_B^{PNI}

merges ACI_B, pk_B^{ACI}, PNI_B, pk_B^{PNI}

signs pk_B^{ACI} with sk_B^{PNI}

Involved protocols: X3DH, Double Ratchet, Sesame

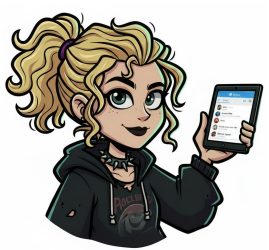
“PNI-to-ACI” protocol

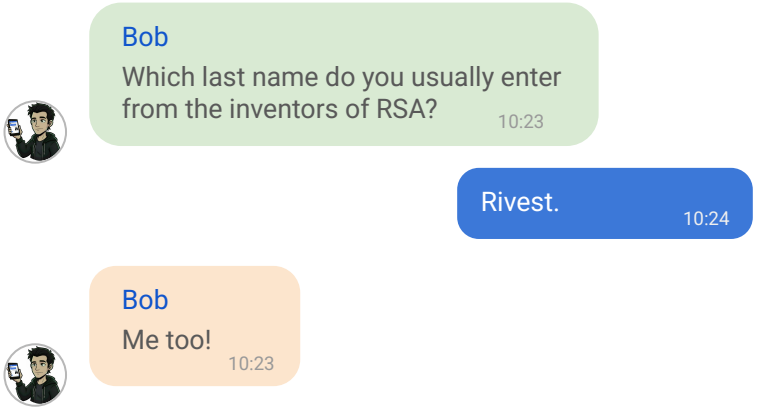


…	…	…	…	…	…
+1 555-1259	bobsignal.03	PNI_B	pk_B^{PNI}	ACI_B	pk_B^{ACI}
NULL	charlie.42	NULL	NULL	ACI_C	pk_C^{ACI}
…	…	…	…	…	…

The two identities are not cryptographically linked:
they are merged into the same database row.

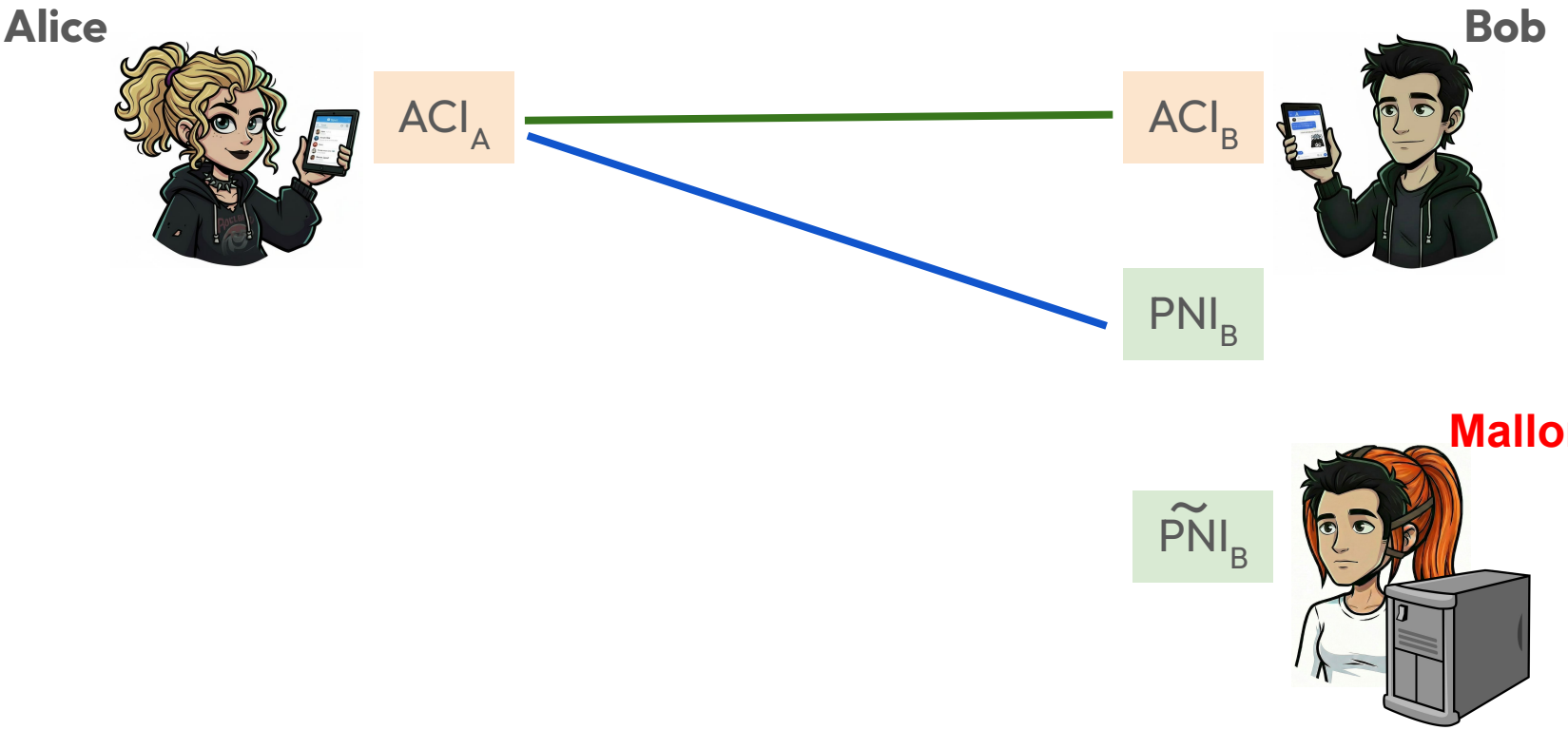
“PNI-to-ACI” protocol



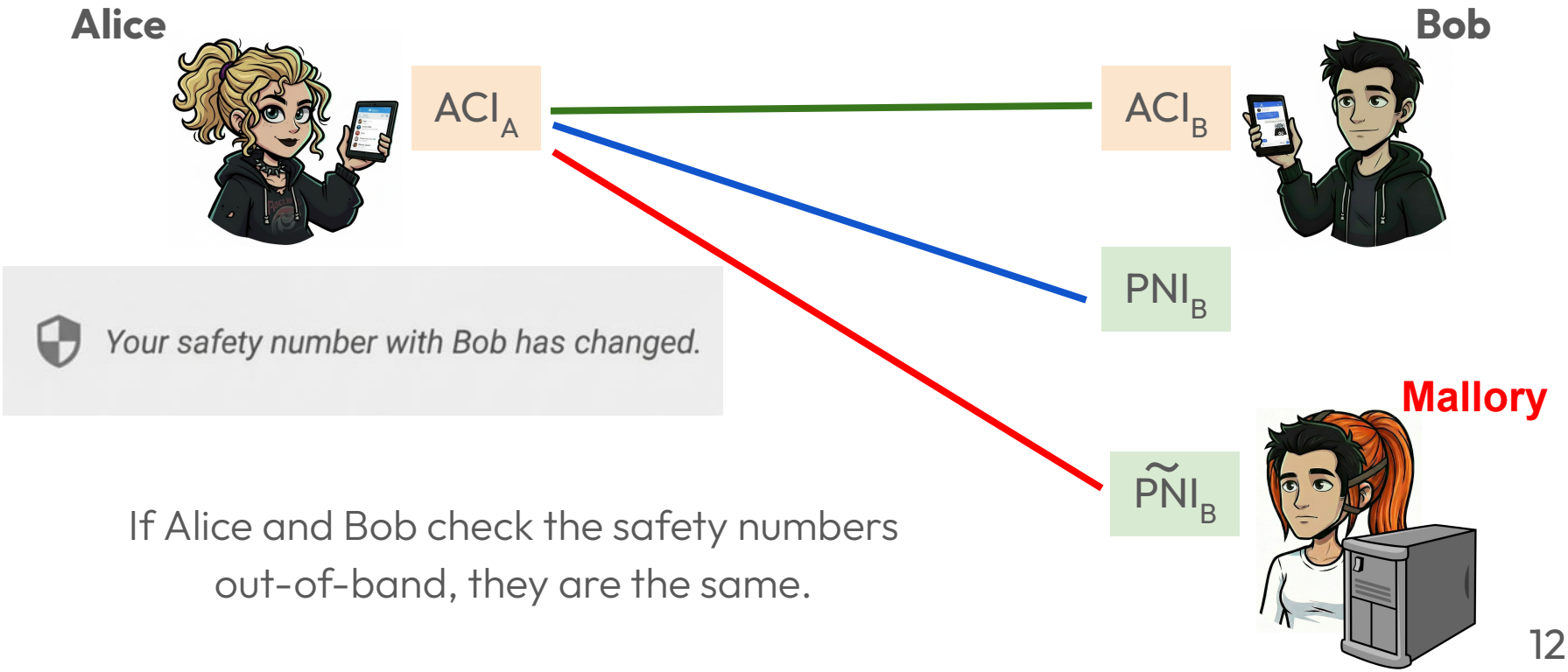


After linking, any message with PNI_B or ACI_B as a source will be **displayed in the same conversation.**

The First Attack

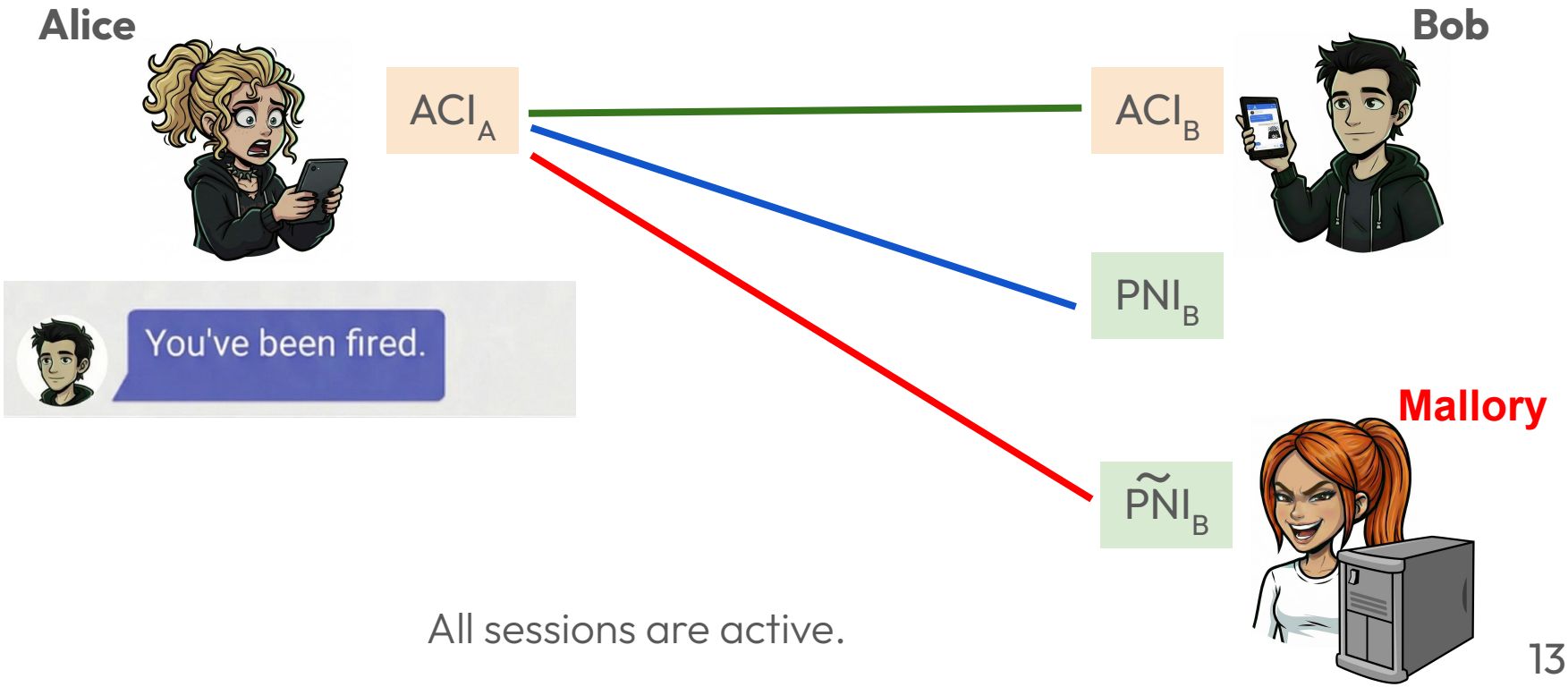


The First Attack



If Alice and Bob check the safety numbers out-of-band, they are the same.

The First Attack



All sessions are active.

Attack 2: Sealed Sender and Plaintext Messages

Injecting Messages

In Signal, a malicious server can send a message on behalf of anyone, as the sender field is not authenticated...

...but it cannot forge valid ciphertexts!

Injecting Messages

Plaintext content is allowed, but only to **encode errors.**

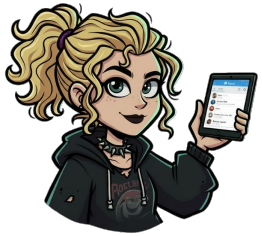
Issue 1: Sealed Sender does not authenticate

The Signal server signs (pk_A, ACI_A) to certify the association

pk_A

Reveals the sender identity to Bob

pk_B



$PKE.Enc(pk_B, msg=pk_A||ACI_A||cert)$

$AuthPKE.Enc(pk_B, sender\_pk=pk_A, msg=m)$

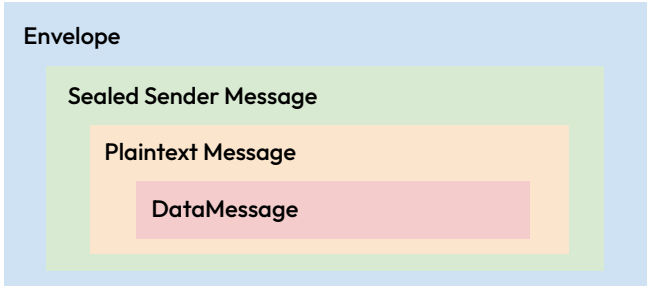
Wraps m and ensures it was sent by Alice

Wants to wrap msg m

Unfortunately, cert doesn't provide much if the server is malicious…

A malicious server can send a message on behalf of **anyone**.

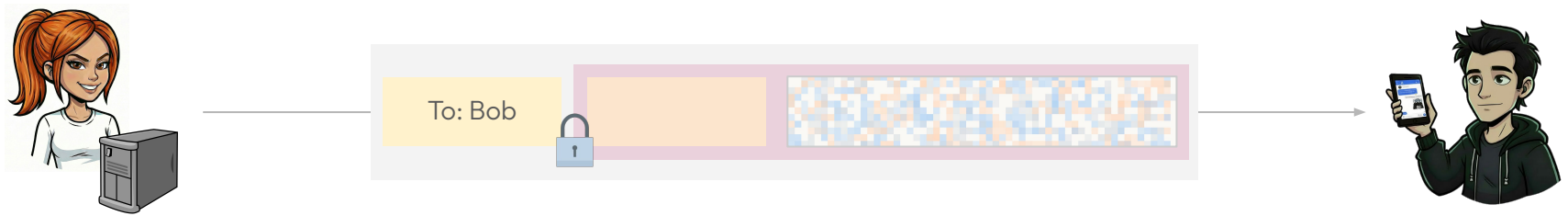
Issue 2: Sealed Sender does not validate plaintext content



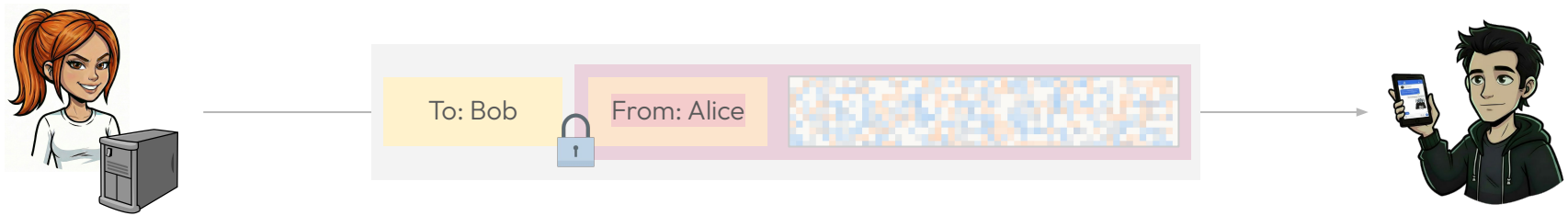
...due to **incorrect validation**, plaintext content for text messages is accepted if using Sealed Sender.

A malicious server can inject **arbitrary messages**.

Combining the Two Issues



Combining the Two Issues



The server can send messages as any user…

Combining the Two Issues

The server can send messages as any user…

… and send plaintext content, bypassing authentication!

Conclusions

Signal is an app...

Its cryptography should be studied at the system level

Signal

The PQXDH Key Agreement Protocol

Revision 3, 2023-05-24, Last Updated: 2024-01-23 [PDF]

Ehren Kret, Rolfe Schmidt

The Double Ratchet Algorithm

Revision 4, 2025-11-04 [PDF]

Trevor Perrin (editor), Moxie Marlinspike, Rolfe Schmidt (revision 3+)

...AND a set of protocols

Signal

Private Group Messaging

moxie0 on 05 May 2014

The X3DH Key Agreement Protocol

Revision 1, 2016-11-04 [PDF]

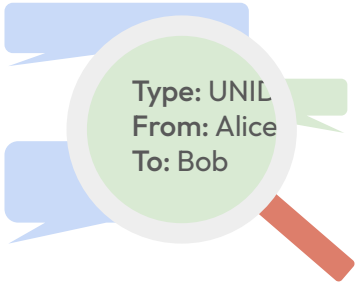
Moxie Marlinspike, Trevor Perrin (editor)

Signal

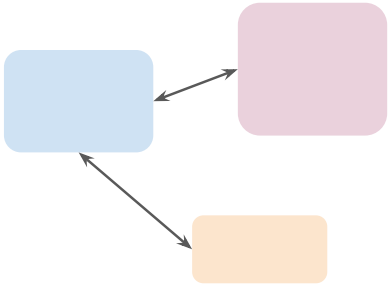
The Sesame Algorithm: Session Management for Asynchronous Message Encryption

Could we have spotted this earlier?

Formal analyses *could* have spotted these attacks...



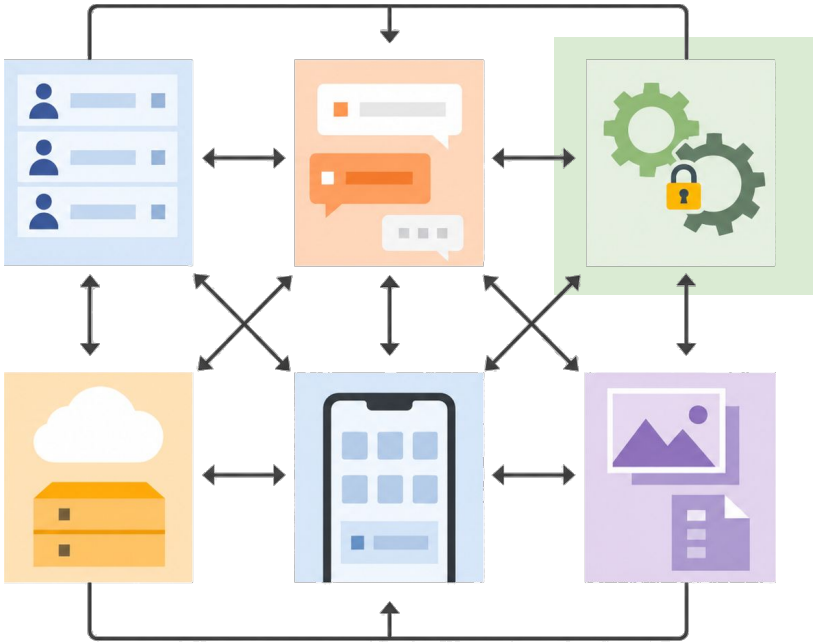
...but only if they captured the system in enough detail



...and only if they captured the interaction between all protocols

...but our techniques do not seem mature enough to capture this level of complexity yet.

For vendors



There's no such thing as a cryptographic core. Everything in the application is security-relevant.

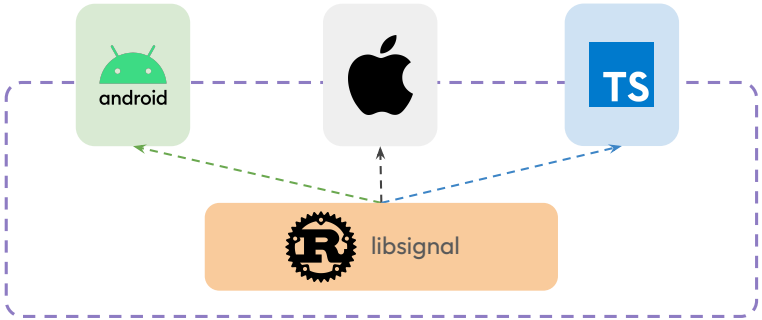
Audit your cryptography and the rest of your code together.

Platform-Dependent Logic

Attack 1 affects Android and Desktop.

Attack 2 affects only Android.

Avoid scattering cryptographic logic across modules and platforms.



- We analysed Signal in the **malicious server setting.**
- We found **two attacks which violate conversation integrity.**
- Signal for iOS was unaffected by both attacks.
  Signal Desktop was unaffected by the second attack.
- Both attacks were **patched very quickly by the Signal team**, whom we thank for the smooth disclosure procedure.

kitruong@ethz.ch
https://ktruong.dev

noemi.terzo@mpi-sp.org
https://nterzo.sh

ePrint Link