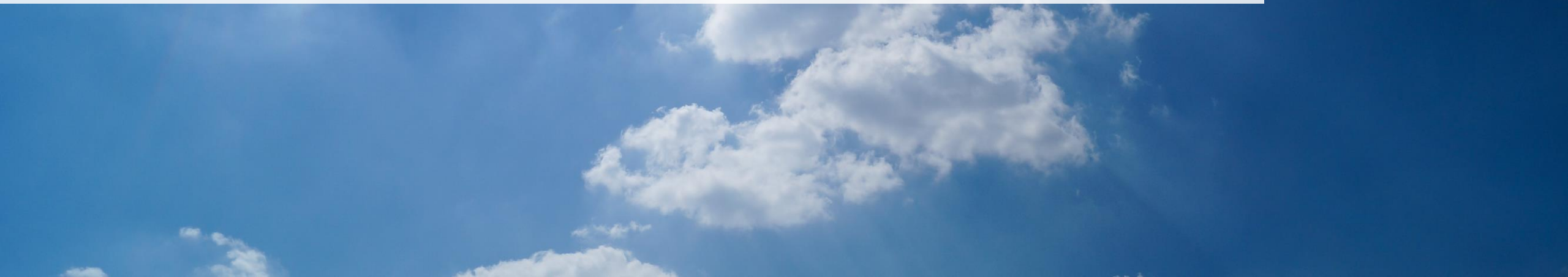
Taming Complexity of Messaging to understand its Security

ZISC Lunch Seminar

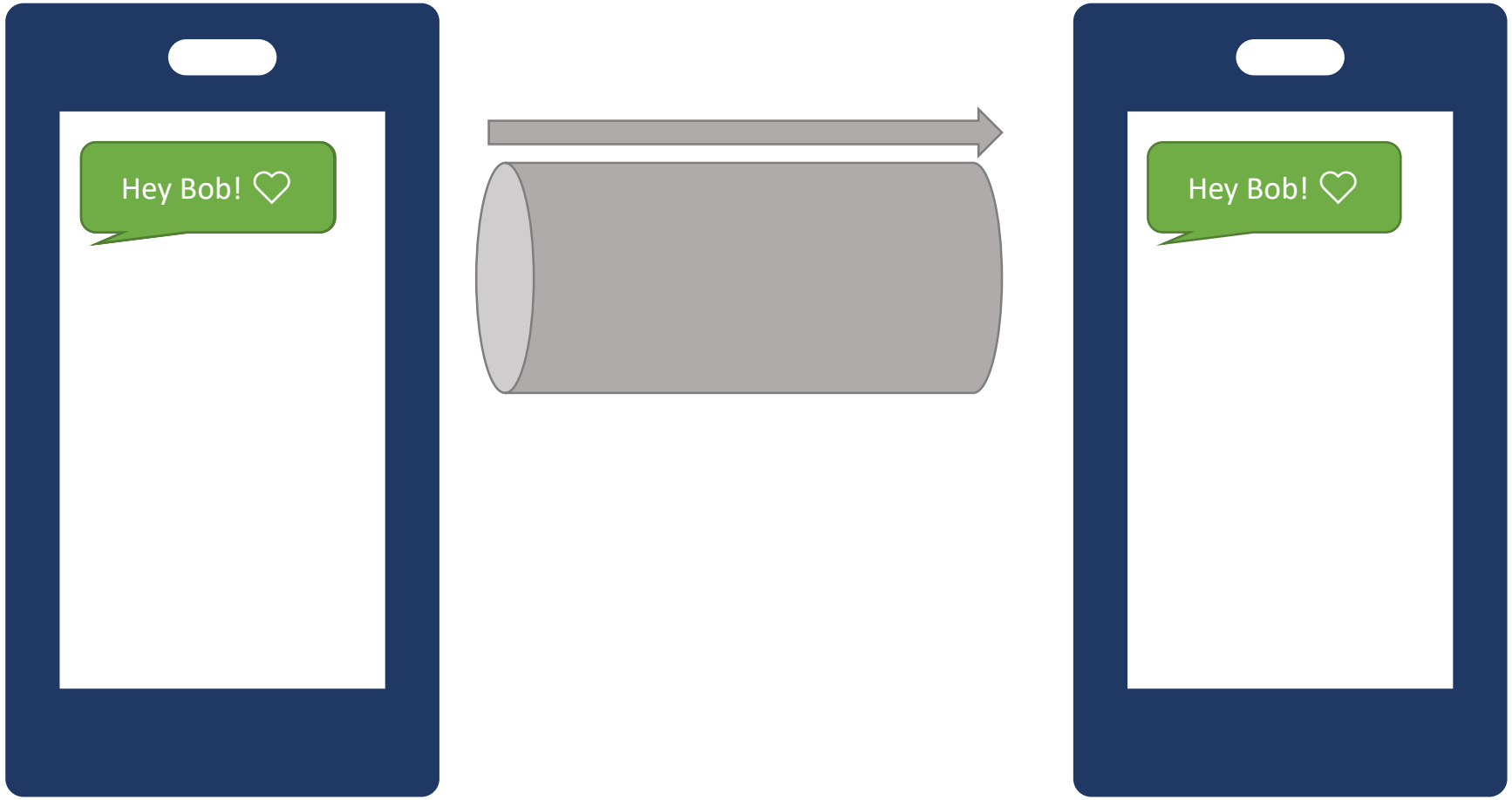
2019-10-10

Horst Görtz Institute for IT Security
Chair for Network and Data Security
Ruhr University Bochum
Paul Rösler



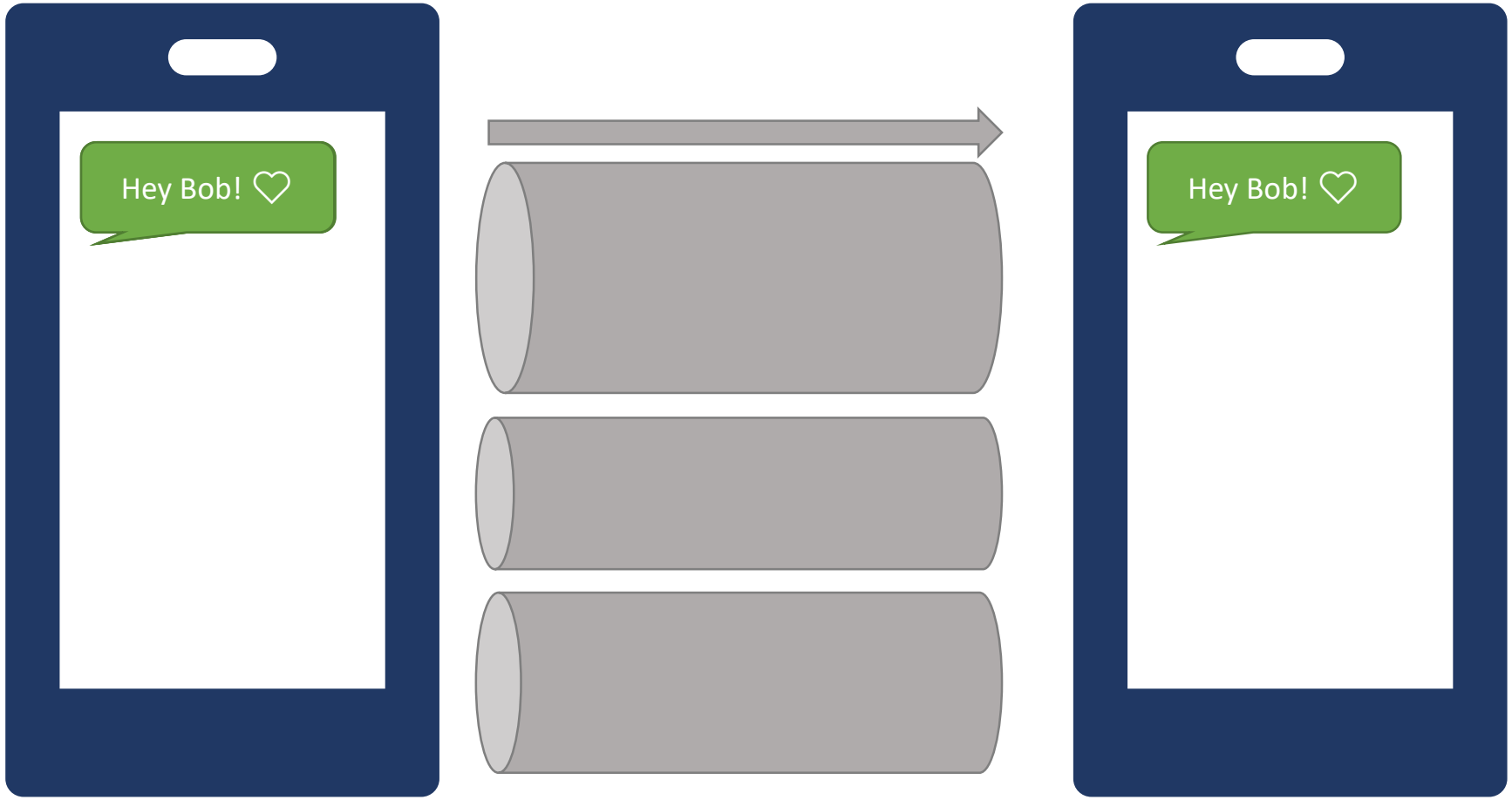
Messaging is complex

- (Asynchronous) session initialization
- “Secure” channel



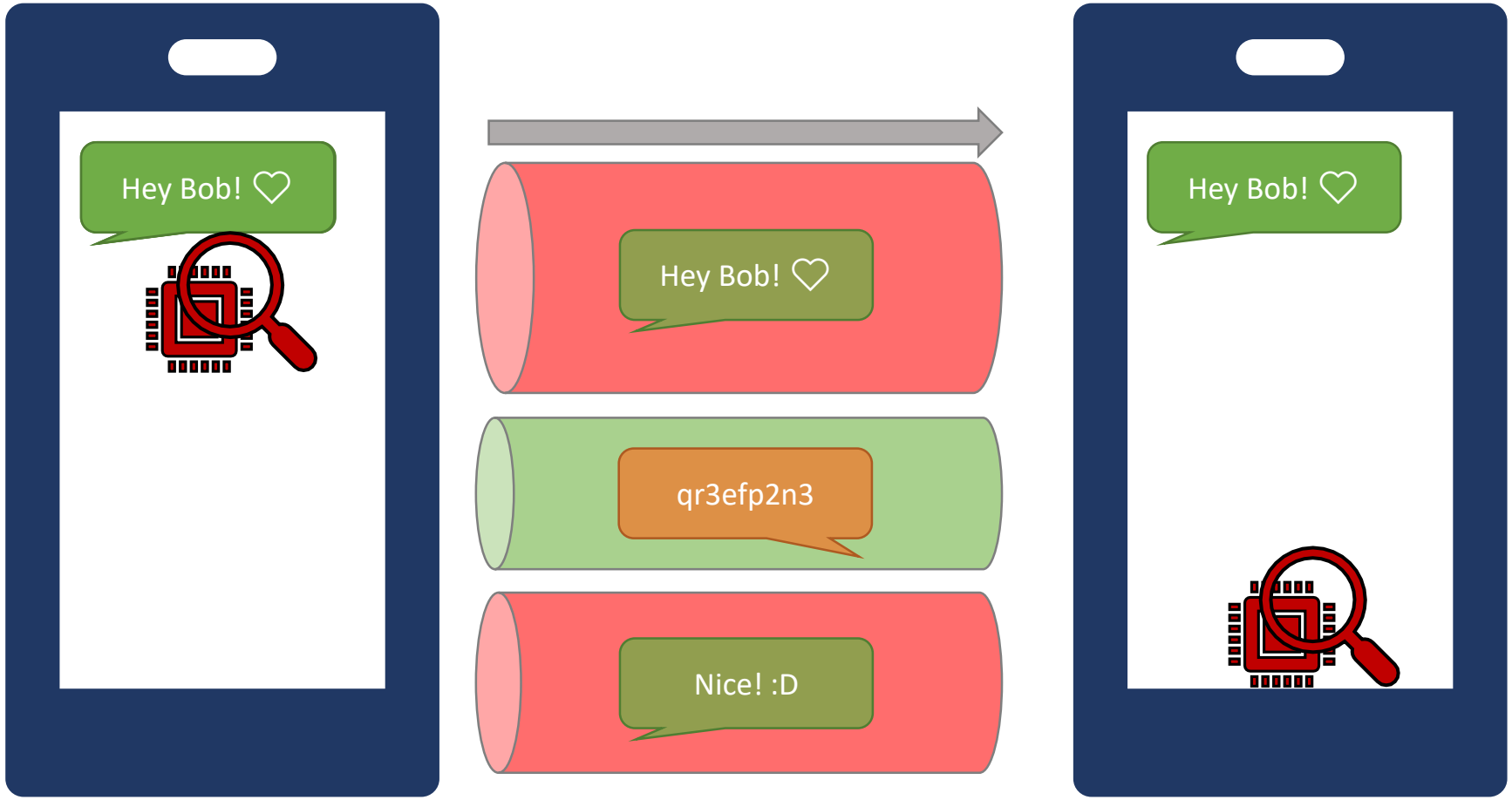
Messaging is complex

- (Asynchronous) session initialization
- “Secure” channel
- Strong security



Messaging is complex

- (Asynchronous) session initialization
- “Secure” channel
- Strong security

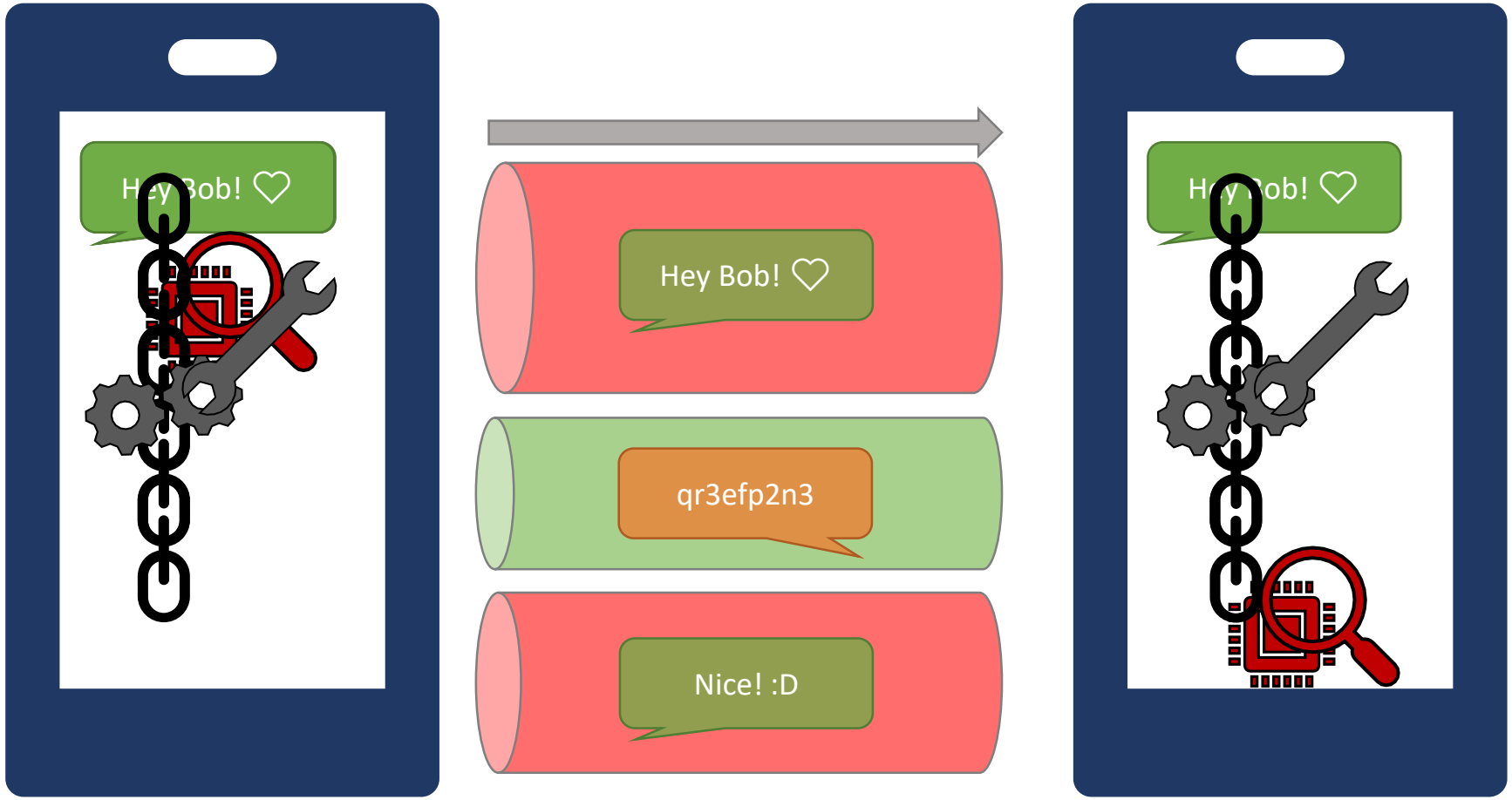


Messaging is complex

- (Asynchronous) session initialization
- “Secure” channel
- Strong security

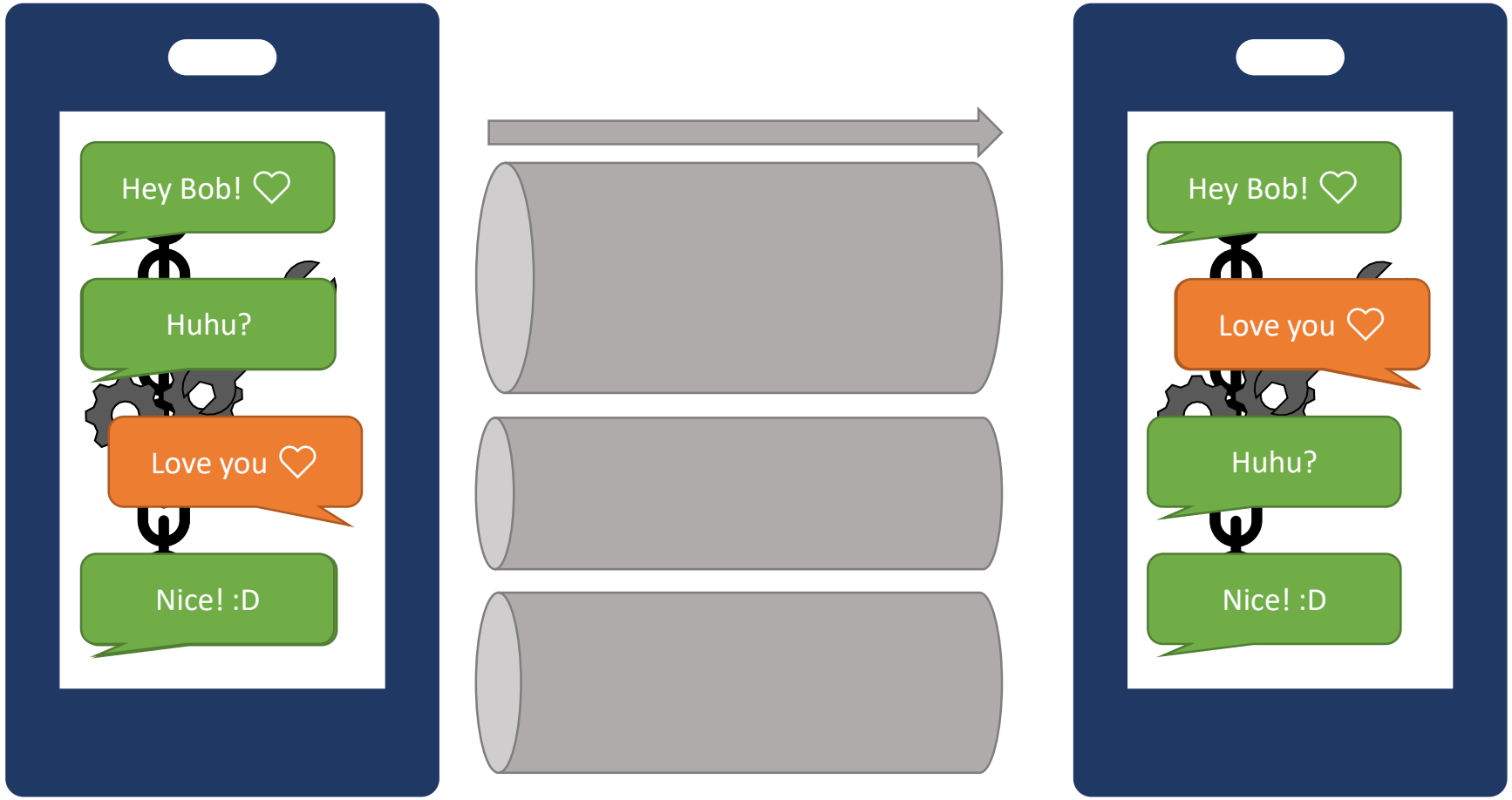
  “Ratchet”-Mechanism:
  - Invalidate old secrets
  - Sample and include new secrets
  - Origin:

  Simple construction:
  - Repetition and mix of key exchanges



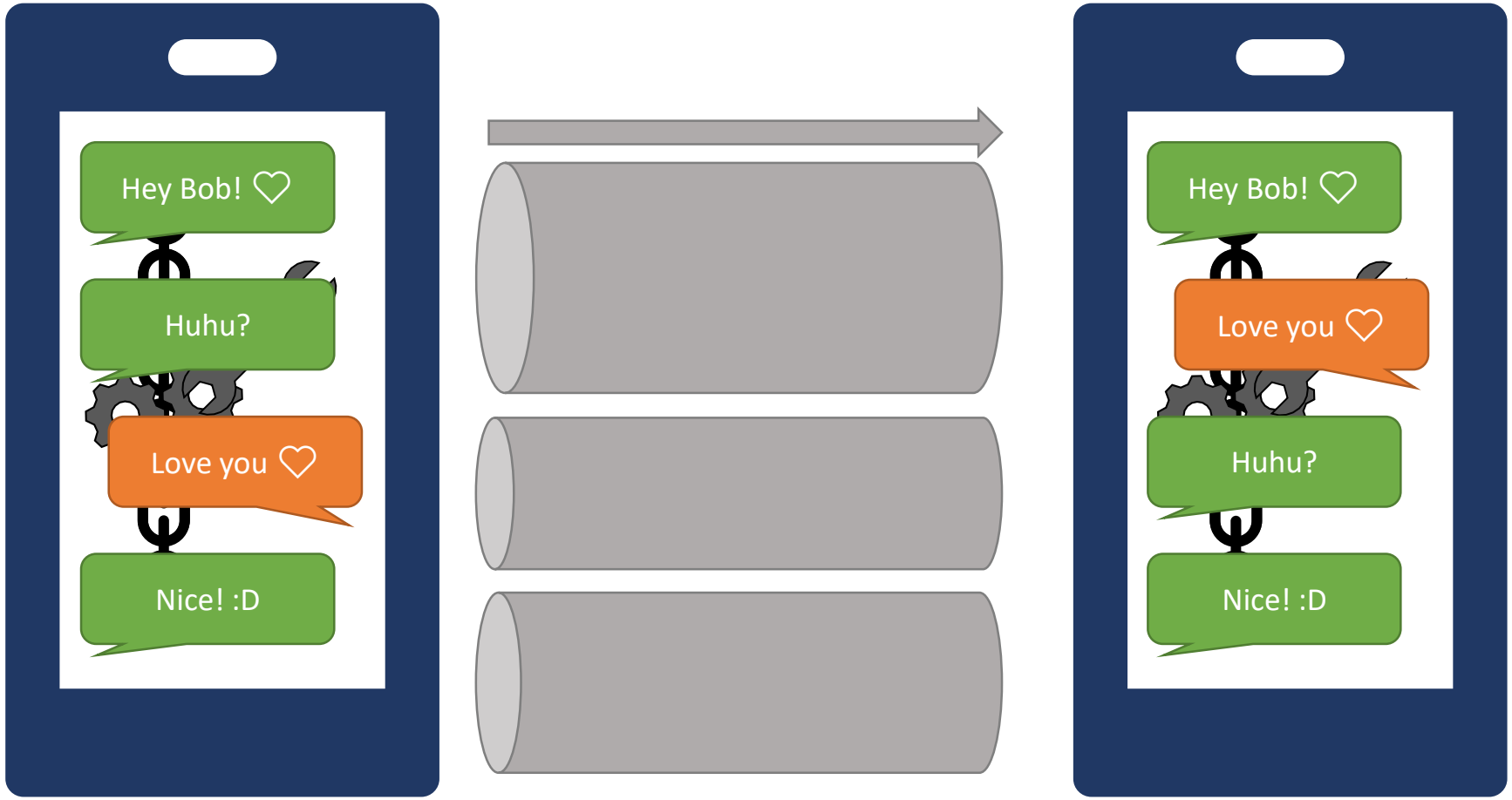
Messaging is complex

- (Asynchronous) session initialization
- “Secure” channel
- Strong security
- Concurrent communication



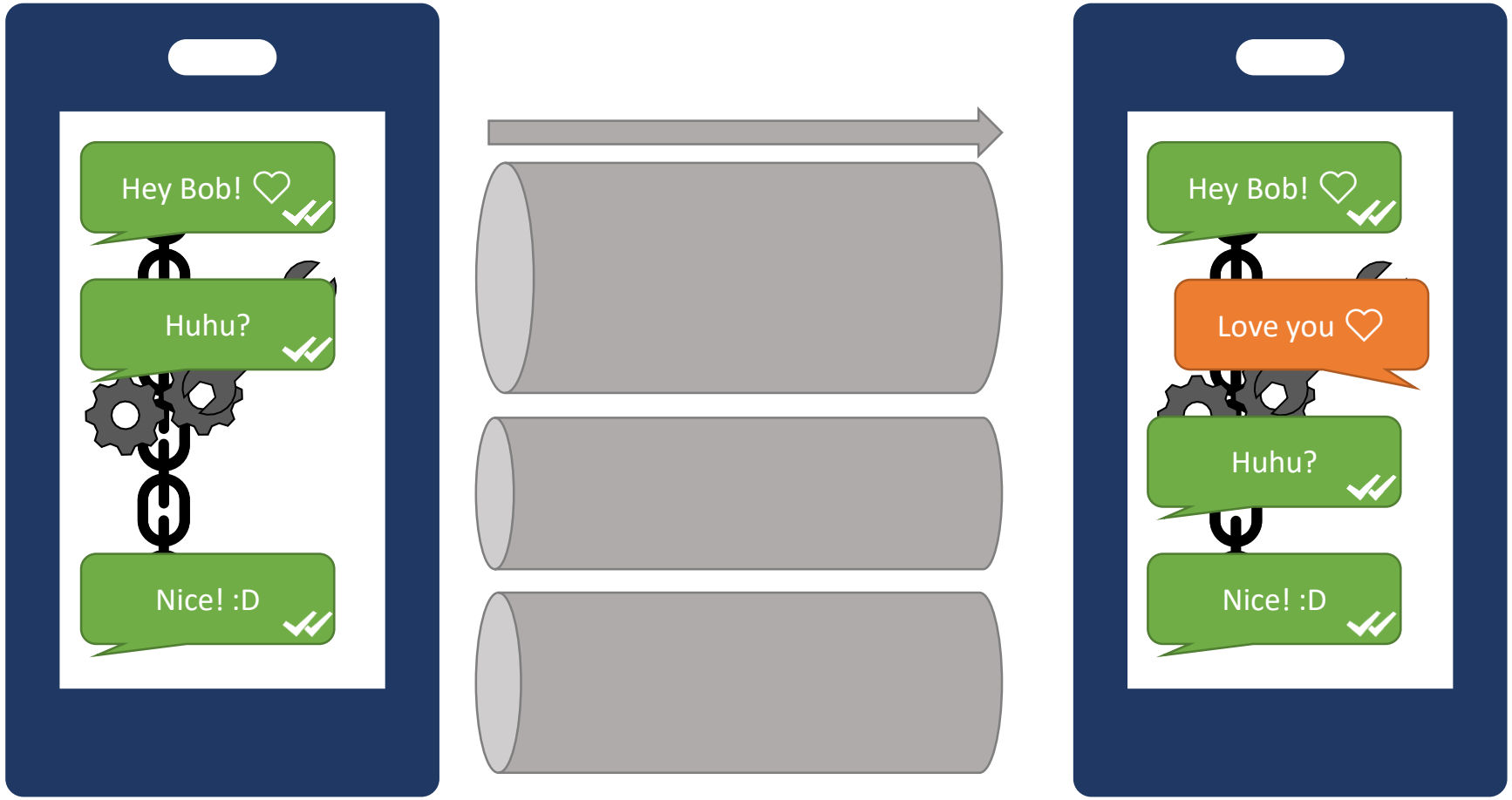
Messaging is complex

- (Asynchronous) session initialization
- “Secure” channel
- Strong security
- Concurrent communication
- Unreliable network



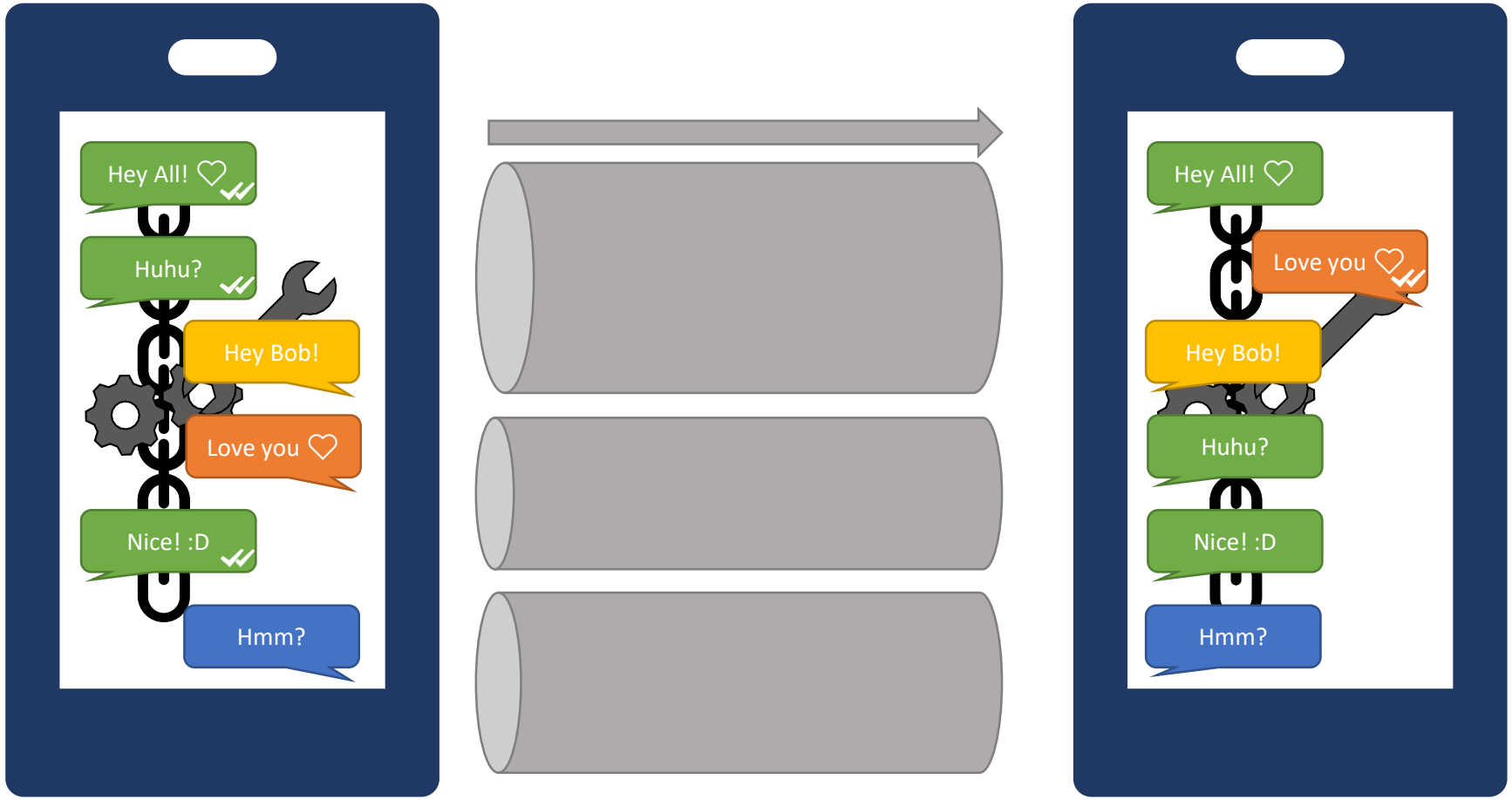
Messaging is complex

- (Asynchronous) session initialization
- “Secure” channel
- Strong security
- Concurrent communication
- Unreliable network
- Explicit reliability



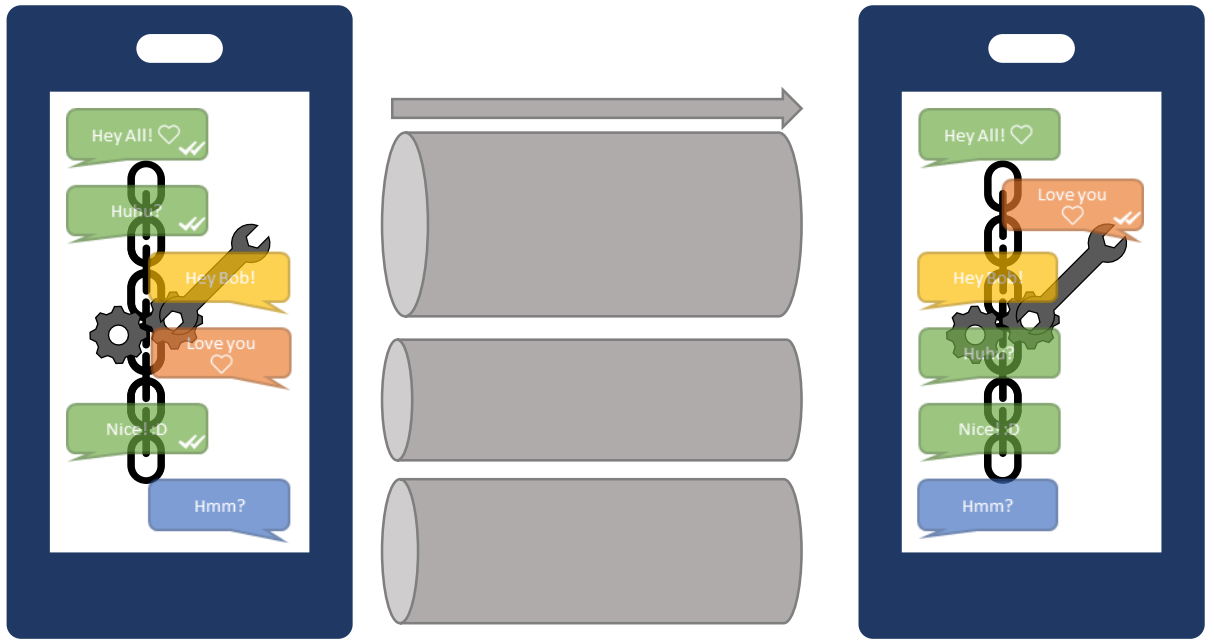
Messaging is complex

- (Asynchronous) session initialization
- “Secure” channel
- Strong security
- Concurrent communication
- Unreliable network
- Explicit reliability
- Group communication



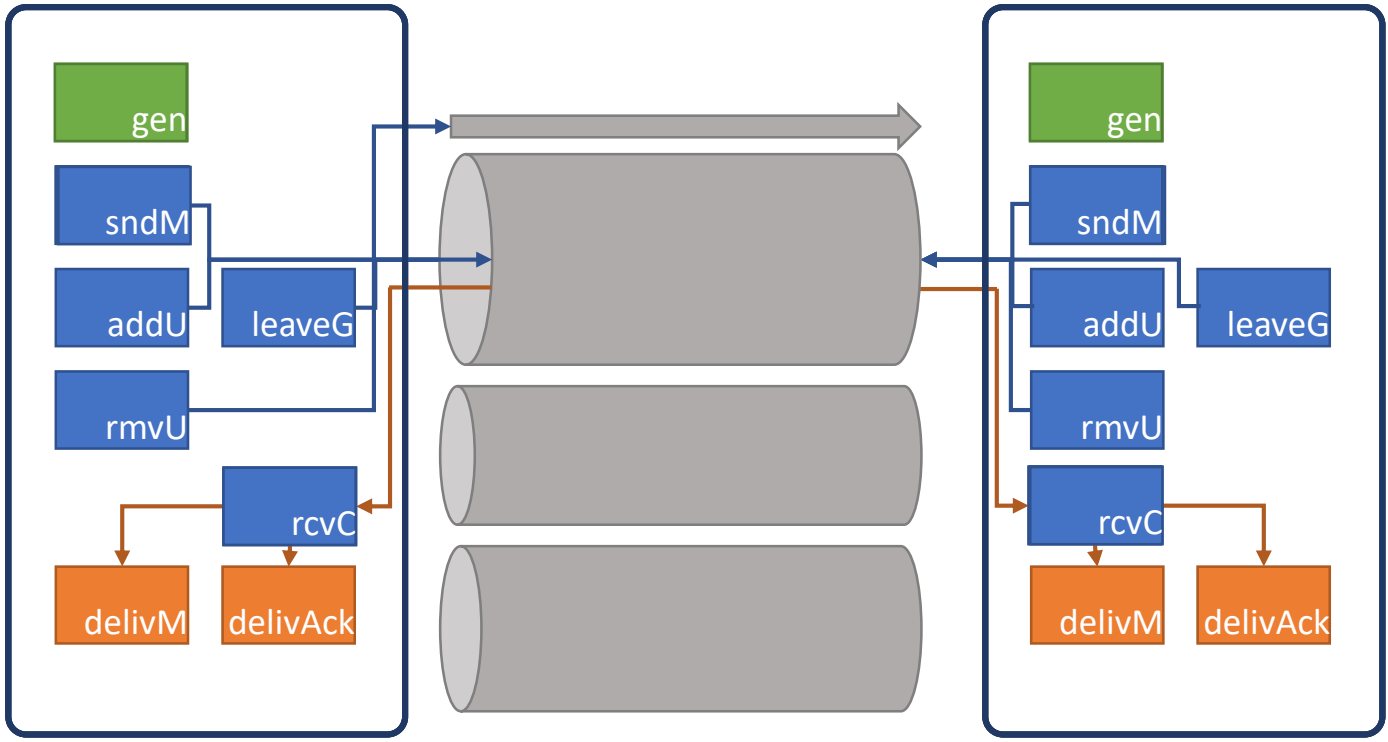
Agenda

- Messaging is complex
- **Finding a Syntax**
- Understanding Attackers
- Defining Security
- Understanding Constructions



Syntax – Taming complexity

- Messenger with
  - Many user interfaces
    - Dynamic groups
    - Explicit reliability
  - Complex functionality
  - Nearly impossible to define security formally
  - Was used to motivate attacks



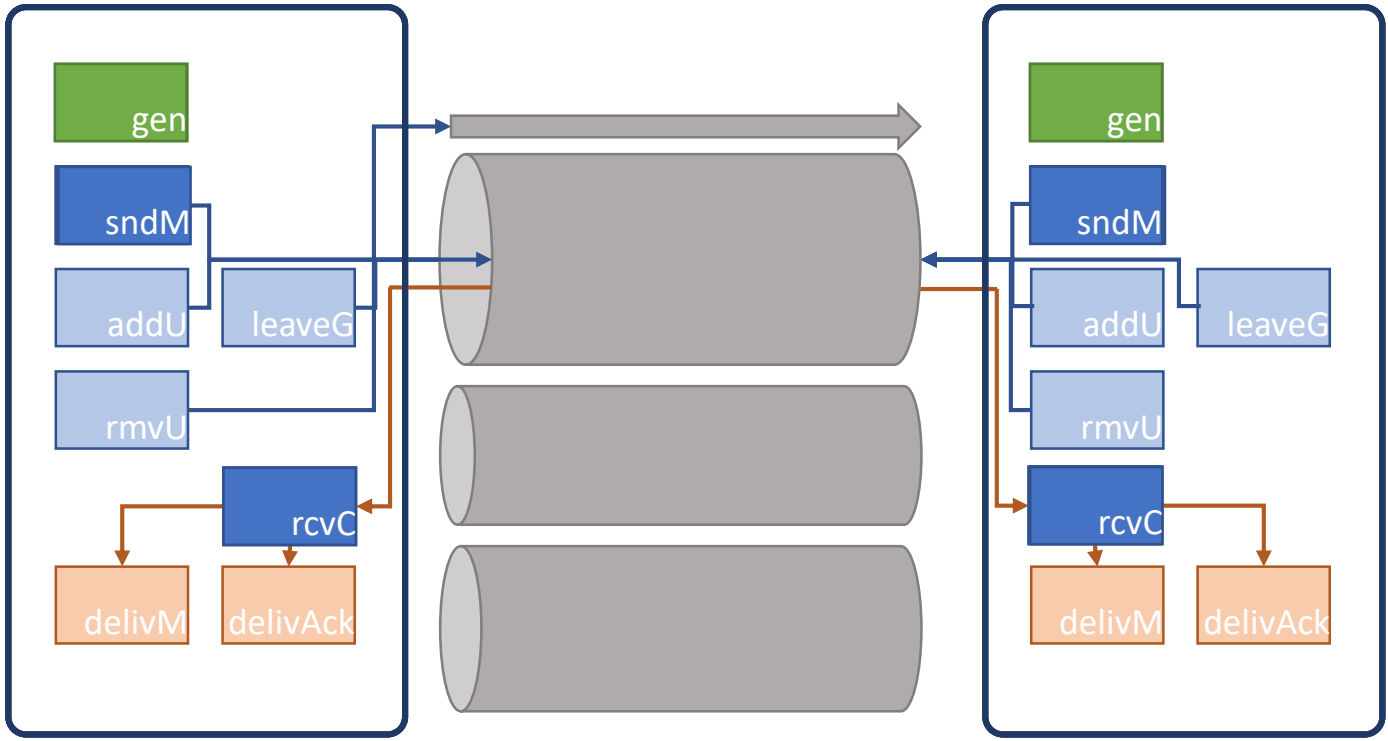
More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema

Paul Rösler, Christian Mainka, Jörg Schwenk
{paul.roesler, christian.mainka, joerg.schwenk}@rub.de
Horst Görtz Institute for IT Security
Chair for Network and Data Security
Ruhr-University Bochum

Messenger

Syntax – Taming complexity

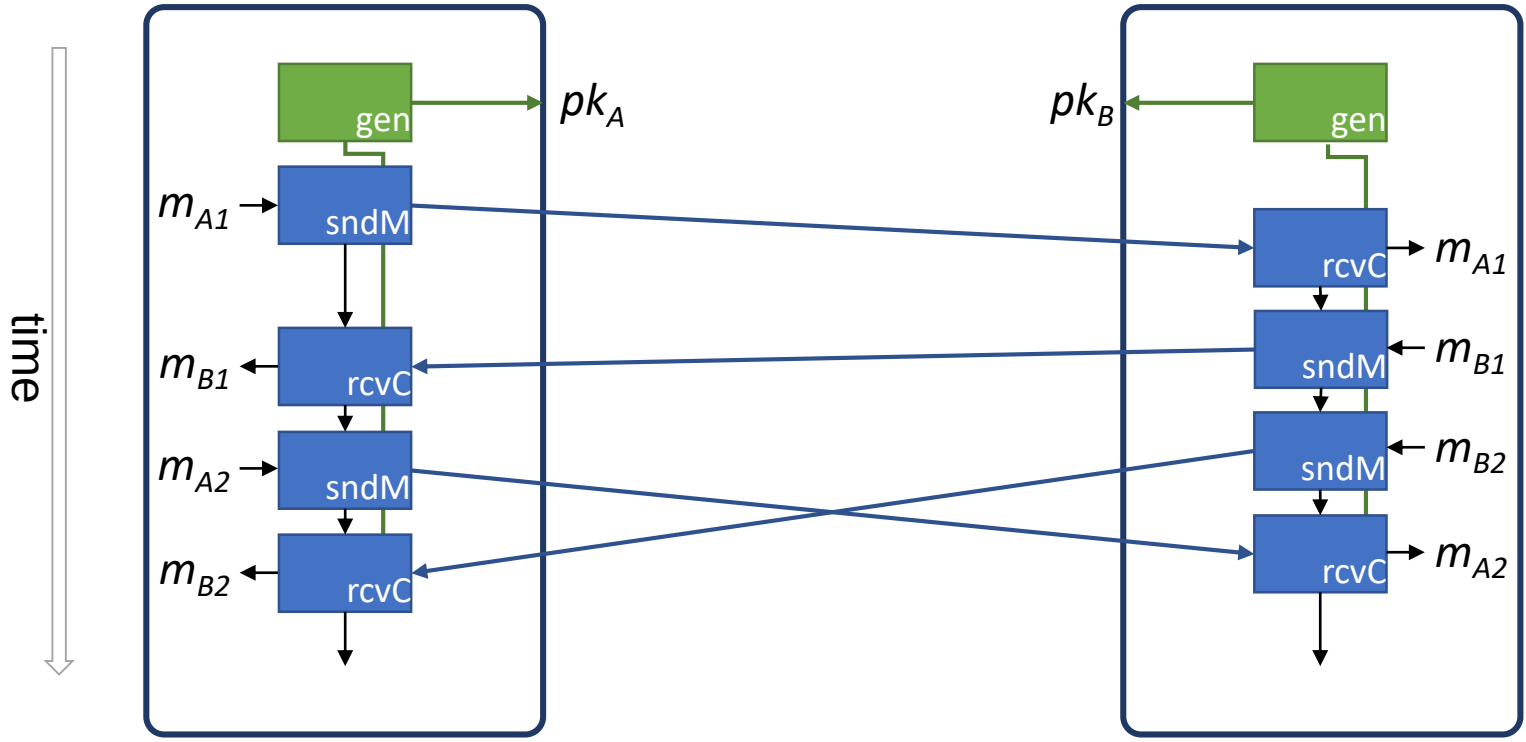
- Remove:
  1. Delivery notifications
  2. Group channels
  3. Group management



Messenger

Syntax – Taming complexity

- Remove:
  1. Delivery notifications
  2. Group channels
  3. Group management



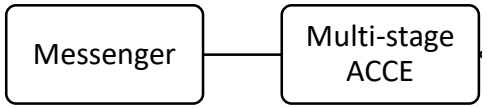
Messenger

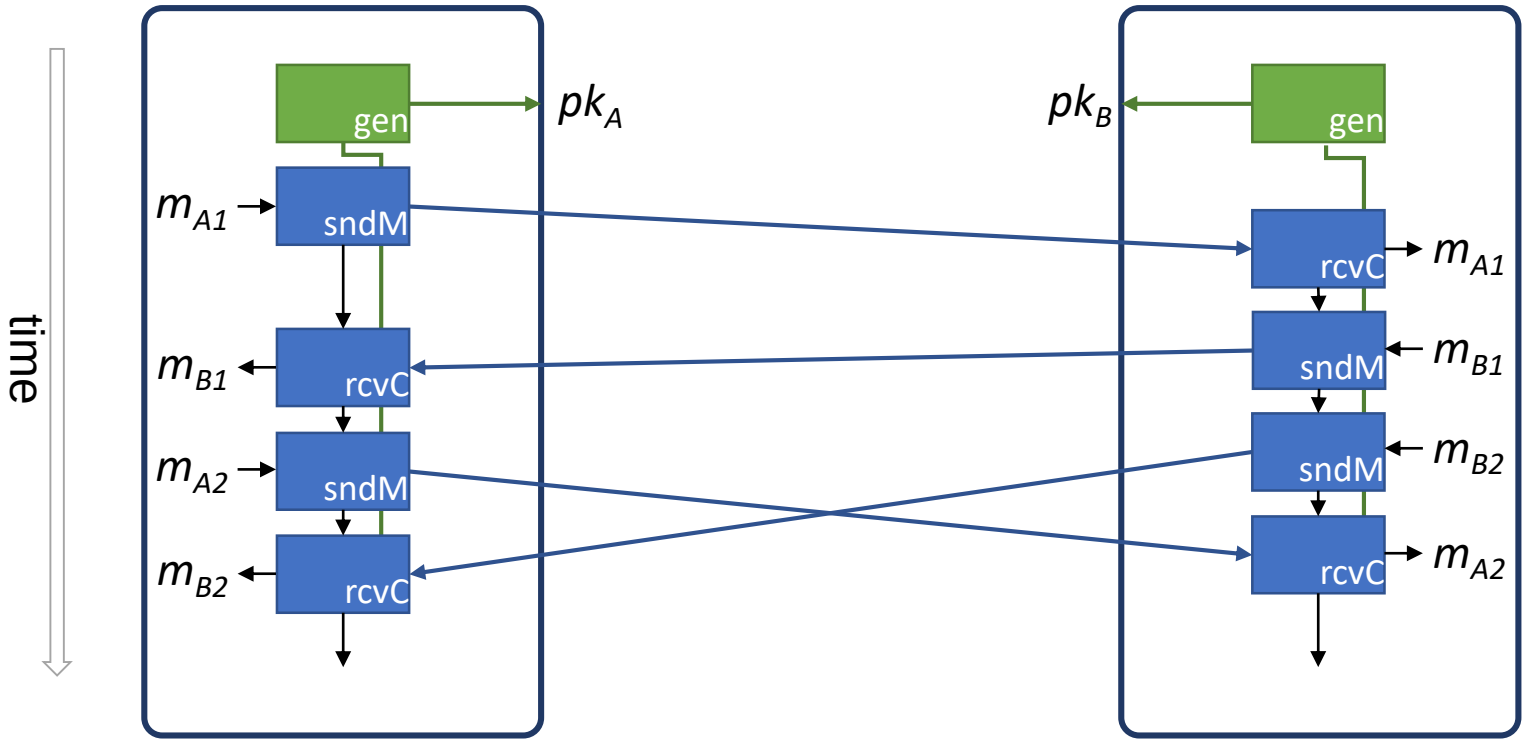
Syntax – Taming complexity

- Remove:
  1. Delivery notifications
  2. Group channels
  3. Group management

  - Still very complex
  - Multiple parties & sessions
  - Establishment & channel

Two party channel (including establishment)





Flexible Authenticated and Confidential Channel Establishment (fACCE): Analyzing the Noise Protocol Framework

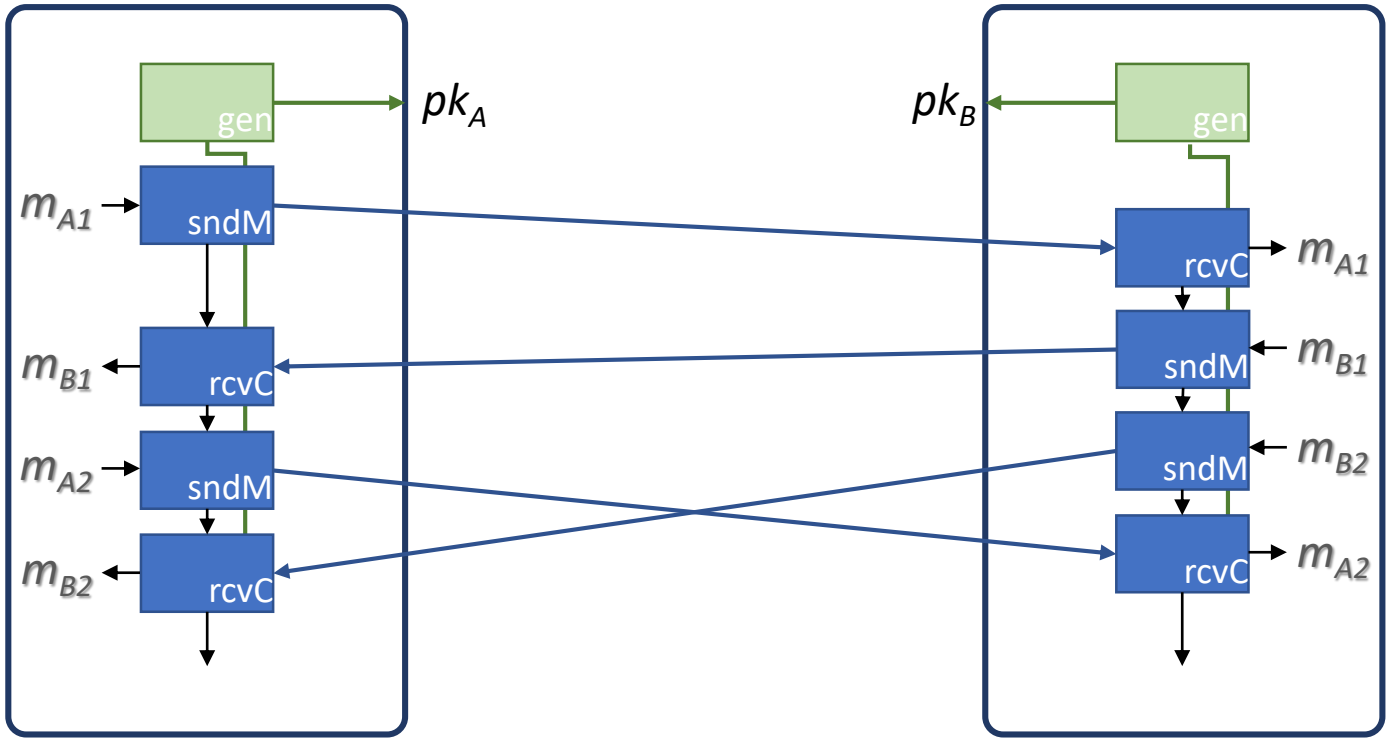
Benjamin Dowling[1], Paul Rösler[2], and Jörg Schwenk[2]

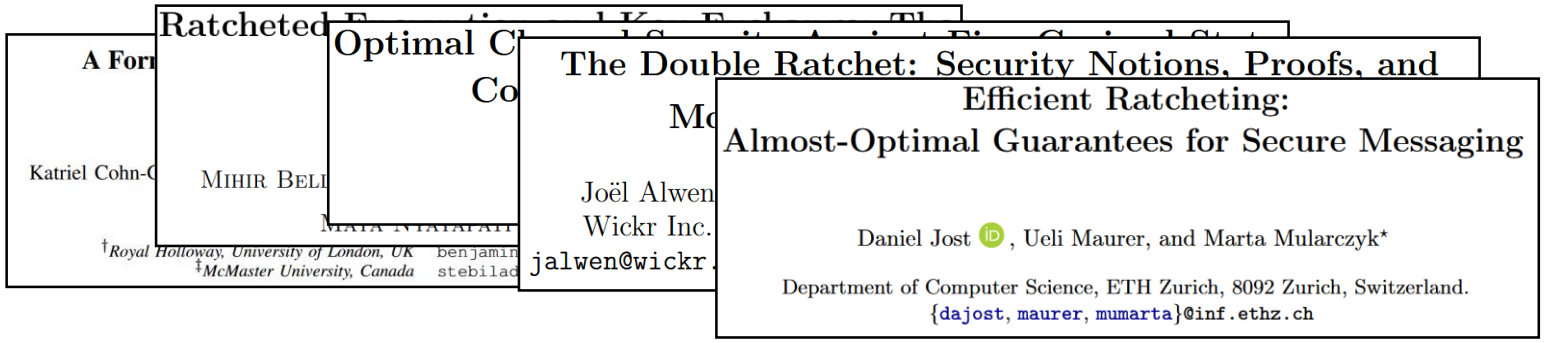
[1] Information Security Group, Royal Holloway, University of London
benjamin.dowling@rhul.ac.uk
[2] Horst-Görtz Institute for IT Security,
Chair for Network and Data Security, Ruhr University Bochum
{paul.roesler,joerg.schwenk}@rub.de

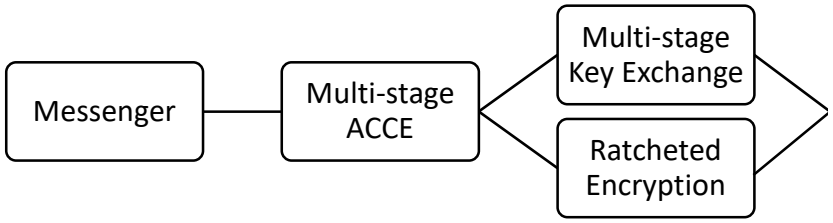
Syntax – Taming complexity

- Remove:
  1. Delivery notifications
  2. Group channels
  3. Group management
  4. Channel establishment
  5. Symmetric encryption

  - Some publications removed (only) one of both:



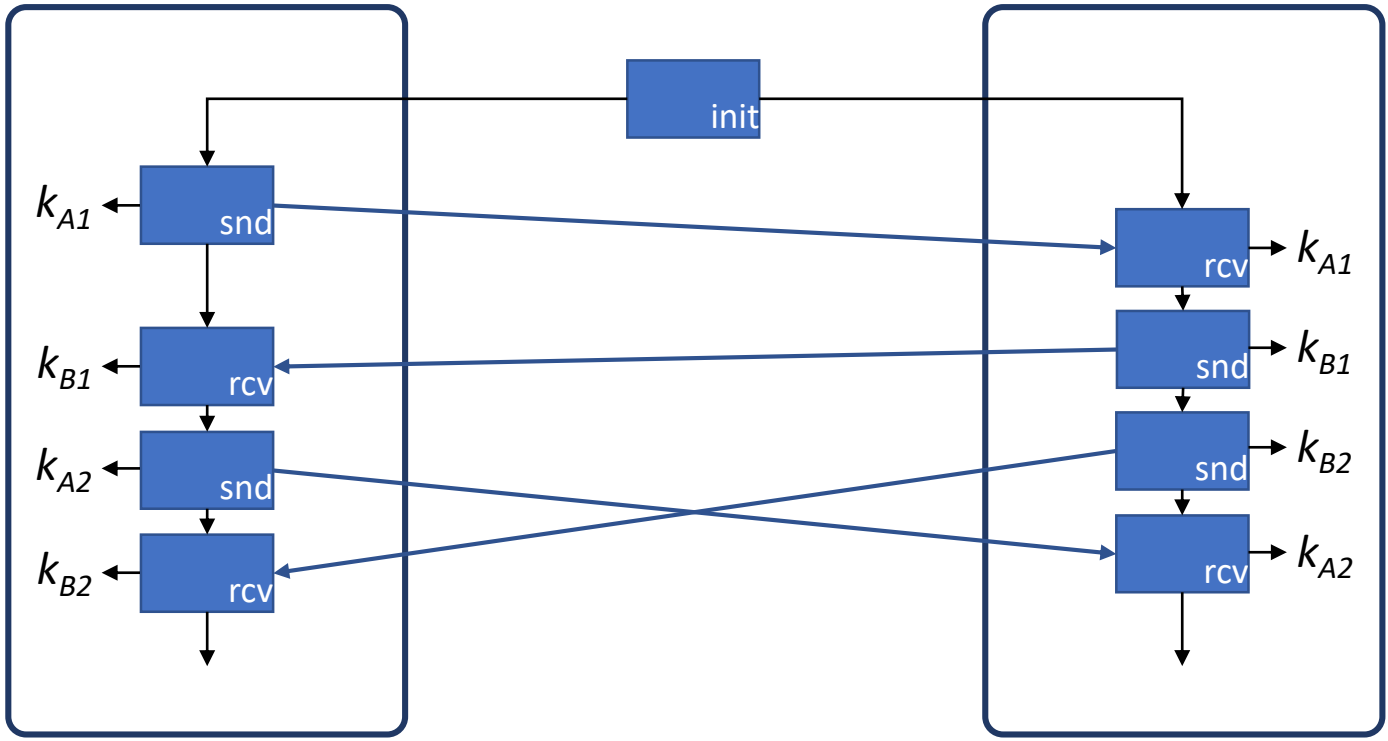




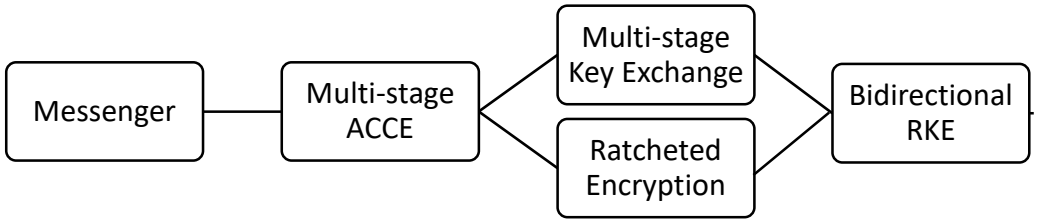
Syntax – Taming complexity

- Remove:
  1. Delivery notifications
  2. Group channels
  3. Group management
  4. Channel establishment
  5. Symmetric encryption

  - Still (*too*) complex to define (and understand) strong security



Ratcheted key exchange



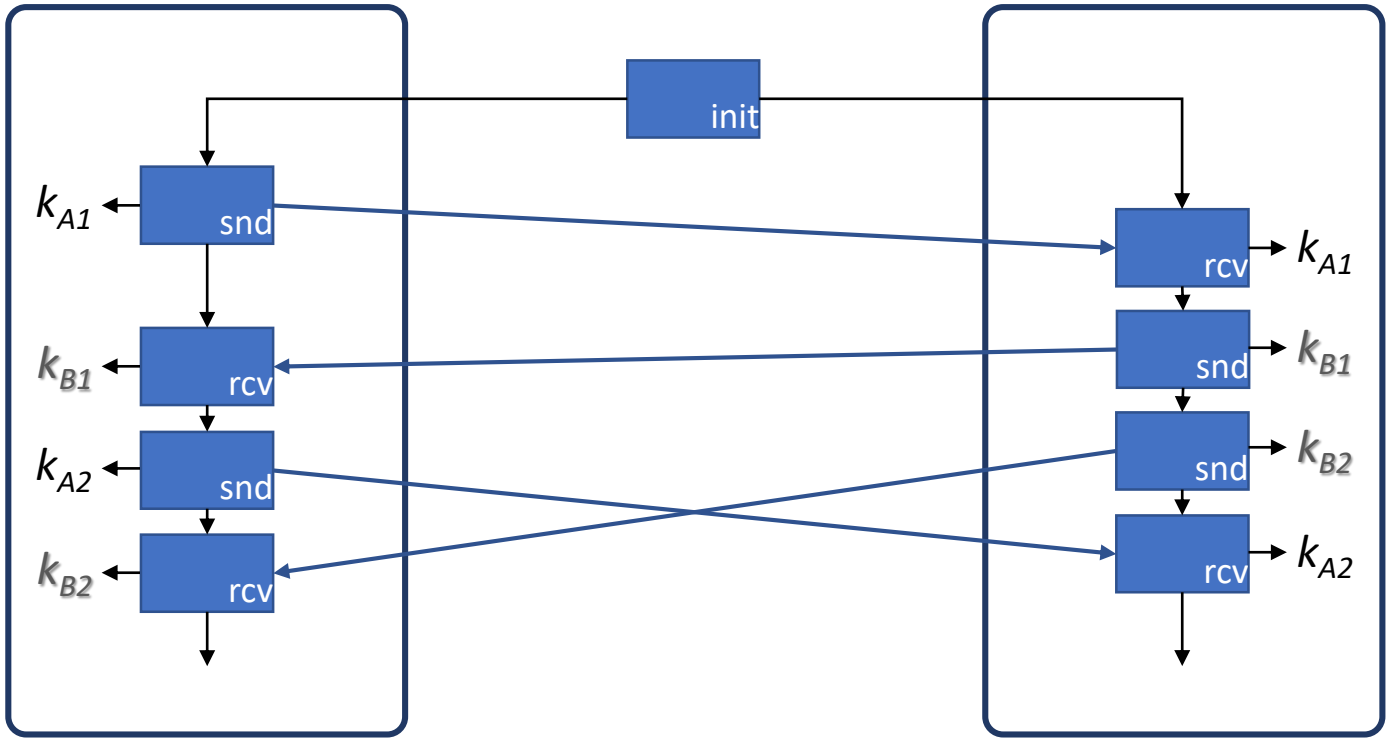
Asynchronous ratcheted key exchange

Bertram Poettering[1] and Paul Rösler[2]

[1] Information Security Group, Royal Holloway, University of London
bertram.poettering@rhul.ac.uk
[2] Horst-Görtz Institute for IT Security,
Chair for Network and Data Security, Ruhr-University Bochum
paul.roesler@rub.de

Syntax – Taming complexity

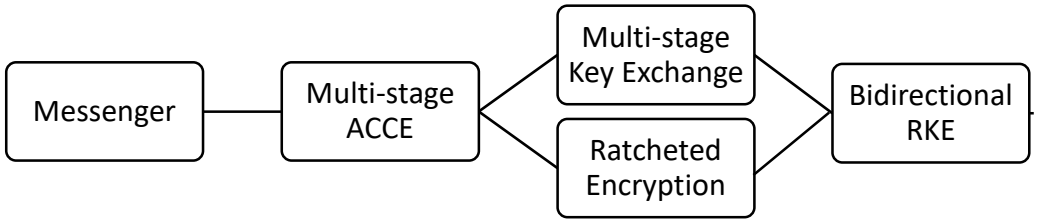
- Remove:
  1. Delivery notifications
  2. Group channels
  3. Group management
  4. Channel establishment
  5. Symmetric encryption
  6. Key establishment B-to-A



Asynchronous ratcheted key exchange

Bertram Poettering[1] and Paul Rösler[2]

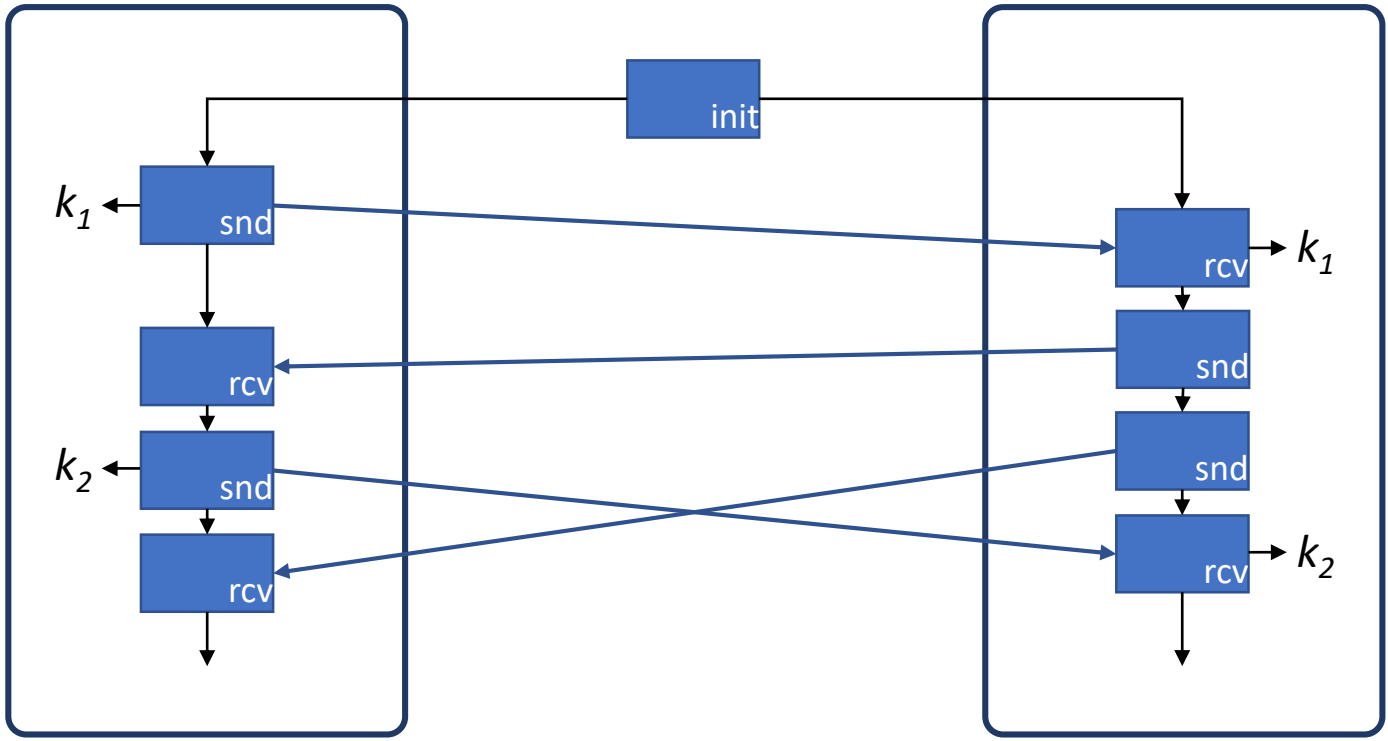
[1] Information Security Group, Royal Holloway, University of London
bertram.poettering@rhul.ac.uk
[2] Horst-Görtz Institute for IT Security,
Chair for Network and Data Security, Ruhr-University Bochum
paul.roesler@rub.de

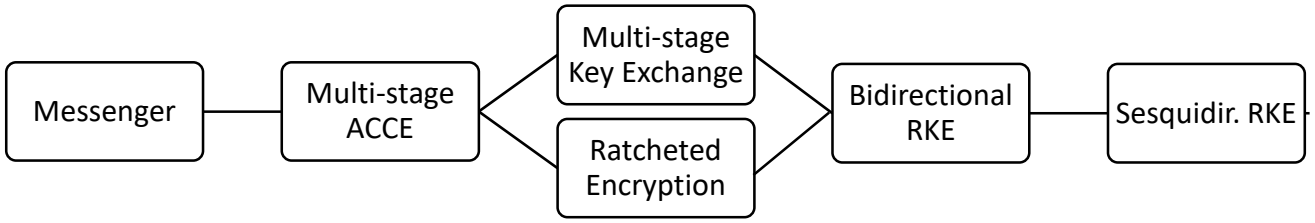


Syntax – Taming complexity

- Remove:
  1. Delivery notifications
  2. Group channels
  3. Group management
  4. Channel establishment
  5. Symmetric encryption
  6. Key establishment B-to-A

  - It can even be simpler ☺





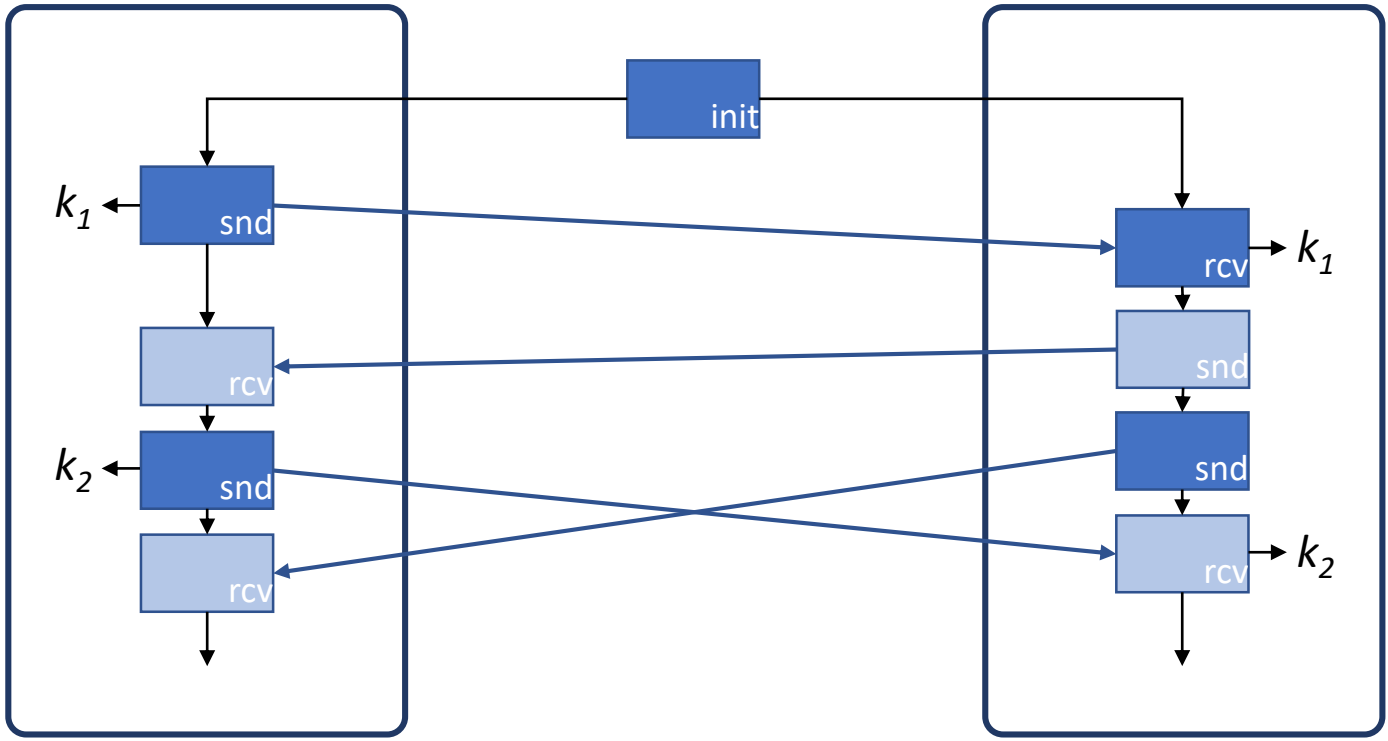
Asynchronous ratcheted key exchange

Bertram Poettering[1] and Paul Rösler[2]

[1] Information Security Group, Royal Holloway, University of London
bertram.poettering@rhul.ac.uk
[2] Horst-Görtz Institute for IT Security,
Chair for Network and Data Security, Ruhr-University Bochum
paul.roesler@rub.de

Syntax – Taming complexity

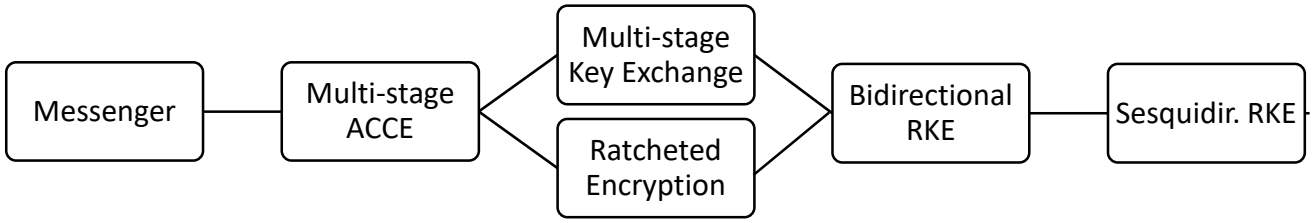
- Remove:
  1. Delivery notifications
  2. Group channels
  3. Group management
  4. Channel establishment
  5. Symmetric encryption
  6. Key establishment B-to-A
  7. B-to-A communication
  - It can even be simpler ☺



Asynchronous ratcheted key exchange

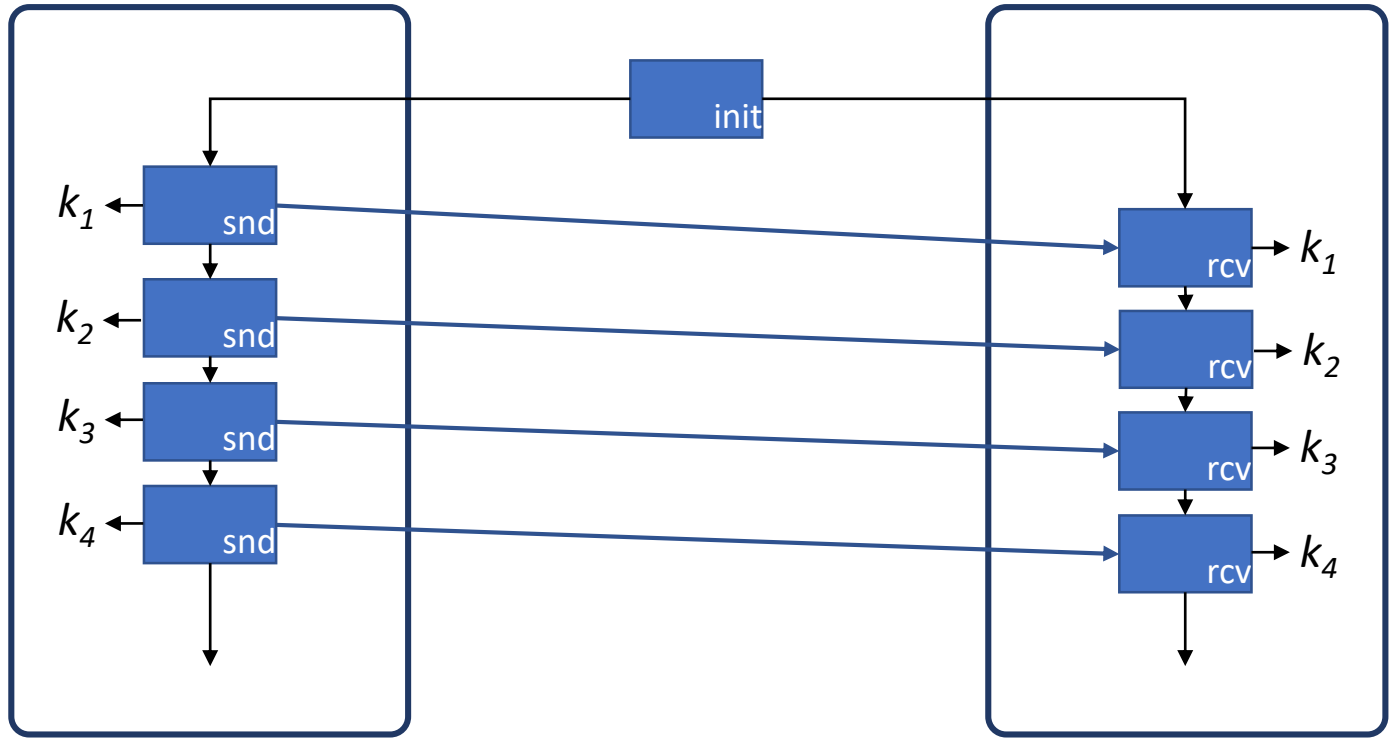
Bertram Poettering[1] and Paul Rösler[2]

[1] Information Security Group, Royal Holloway, University of London
bertram.poettering@rhul.ac.uk
[2] Horst-Görtz Institute for IT Security,
Chair for Network and Data Security, Ruhr-University Bochum
paul.roesler@rub.de

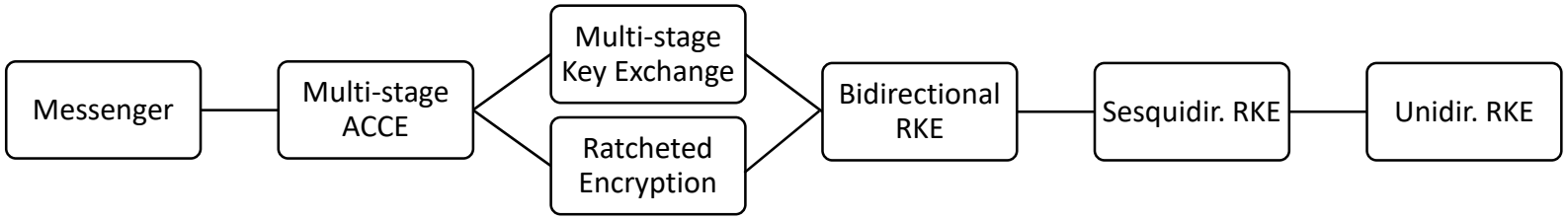


Syntax – Taming complexity

- Remove:
  1. Delivery notifications
  2. Group channels
  3. Group management
  4. Channel establishment
  5. Symmetric encryption
  6. Key establishment B-to-A
  7. B-to-A communication



Unidirectional ratcheted key exchange

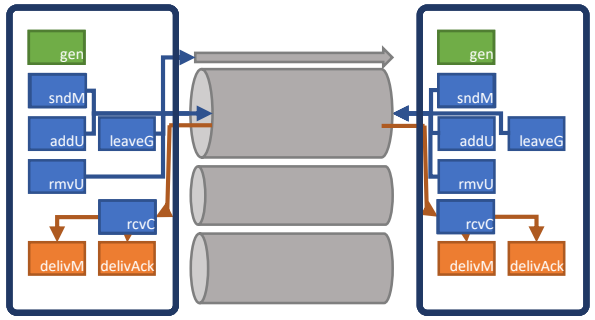


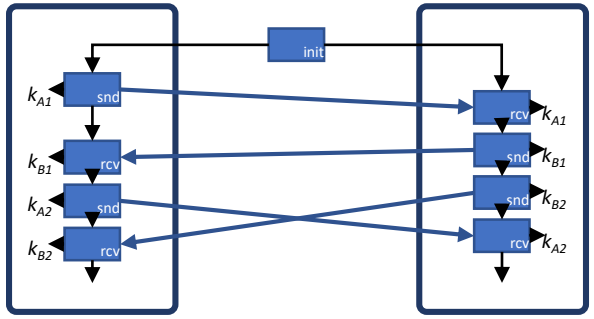
Asynchronous ratcheted key exchange

Bertram Poettering[1] and Paul Rösler[2]

[1] Information Security Group, Royal Holloway, University of London
bertram.poettering@rhul.ac.uk
[2] Horst-Görtz Institute for IT Security,
Chair for Network and Data Security, Ruhr-University Bochum
paul.roesler@rub.de

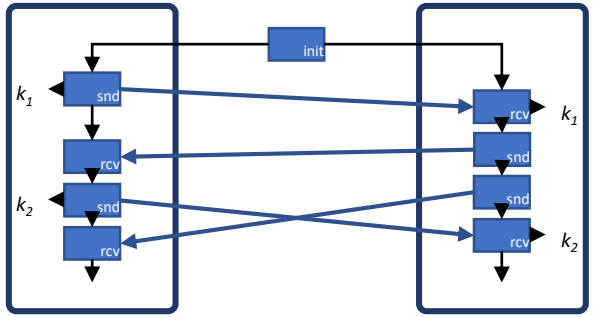
Syntax – Taming complexity



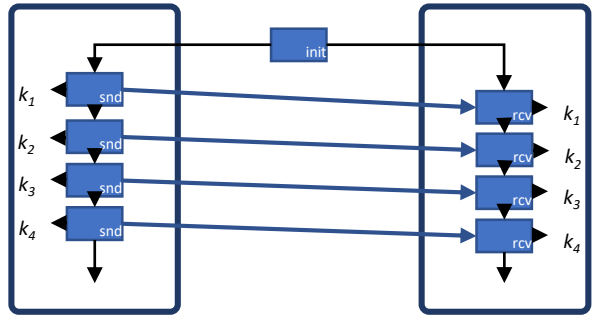


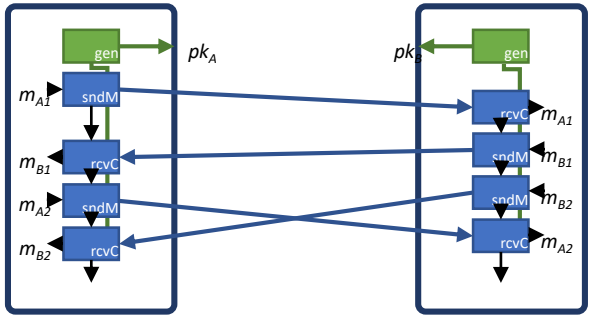
- Abstract initialization
- No symmetric encryption

- No B-to-A key establishment

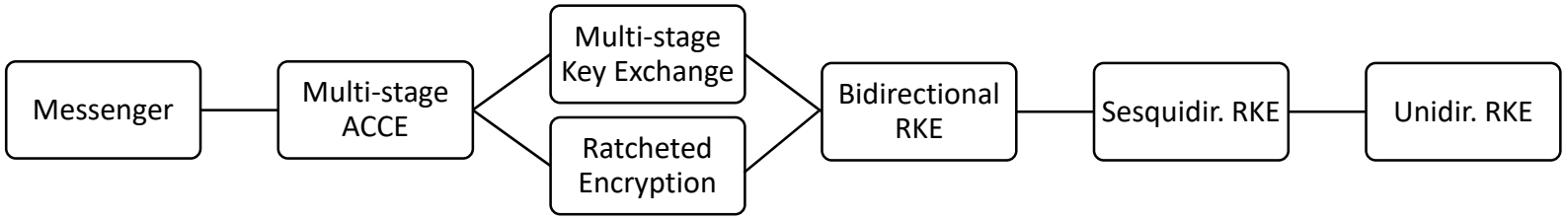


- No B-to-A communication

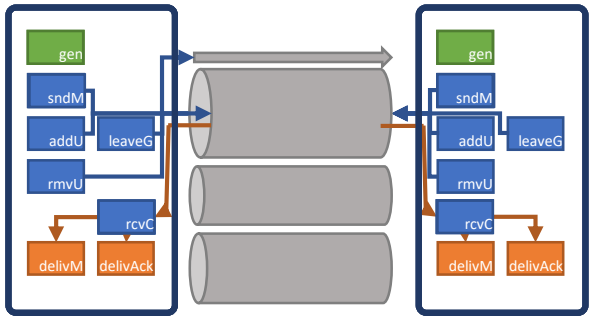


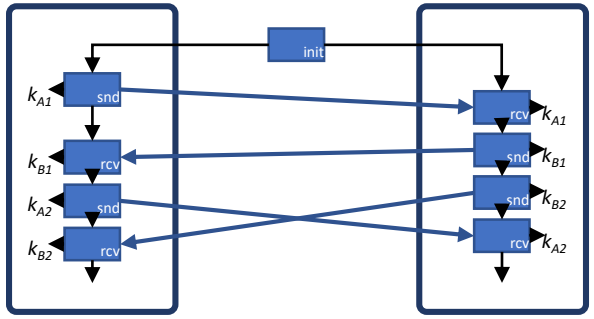


- No groups
- Only pair-wise communication



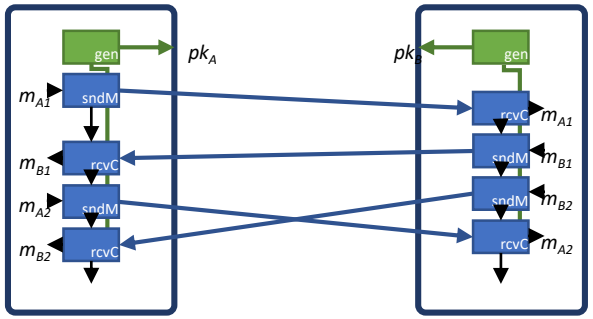
Syntax – Modularity

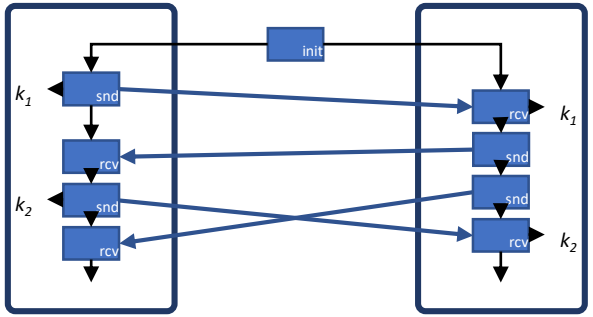




- Copy and merge

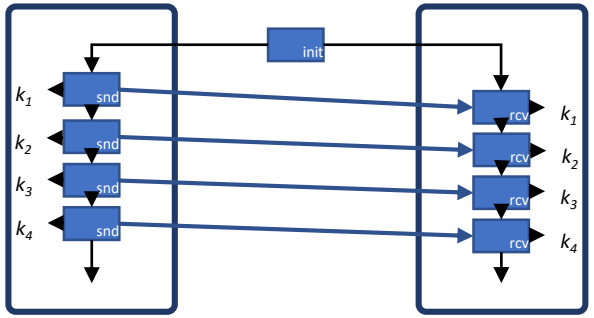
- Initialize with key exchange
- Add authenticated encryption

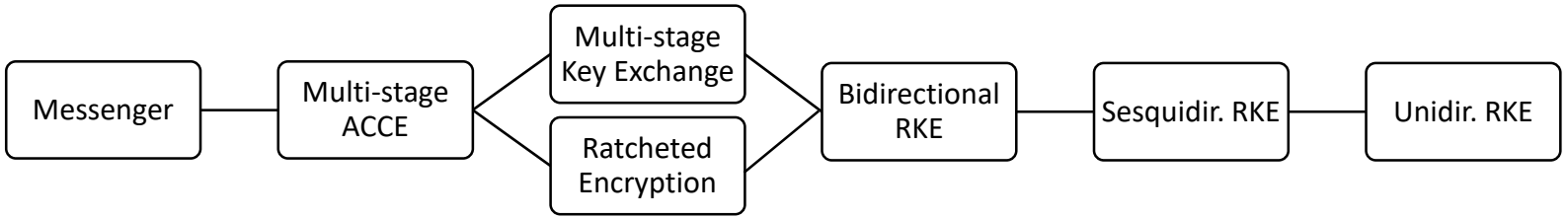




- ???
  We will see…

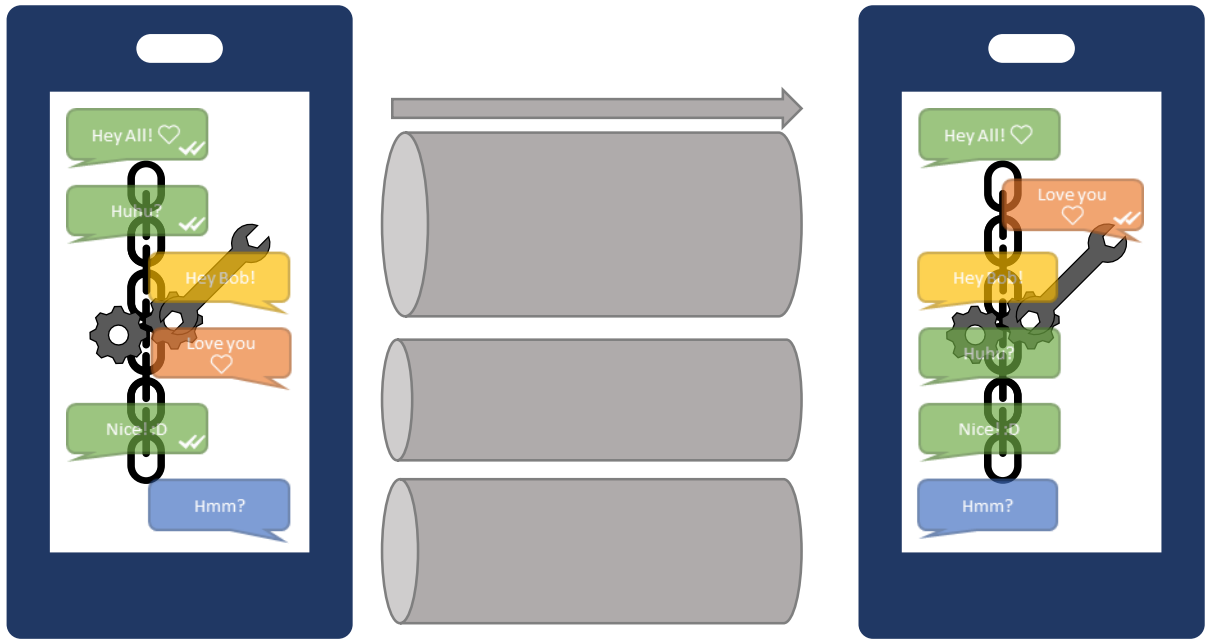
- N pair-wise channels
- Send acks





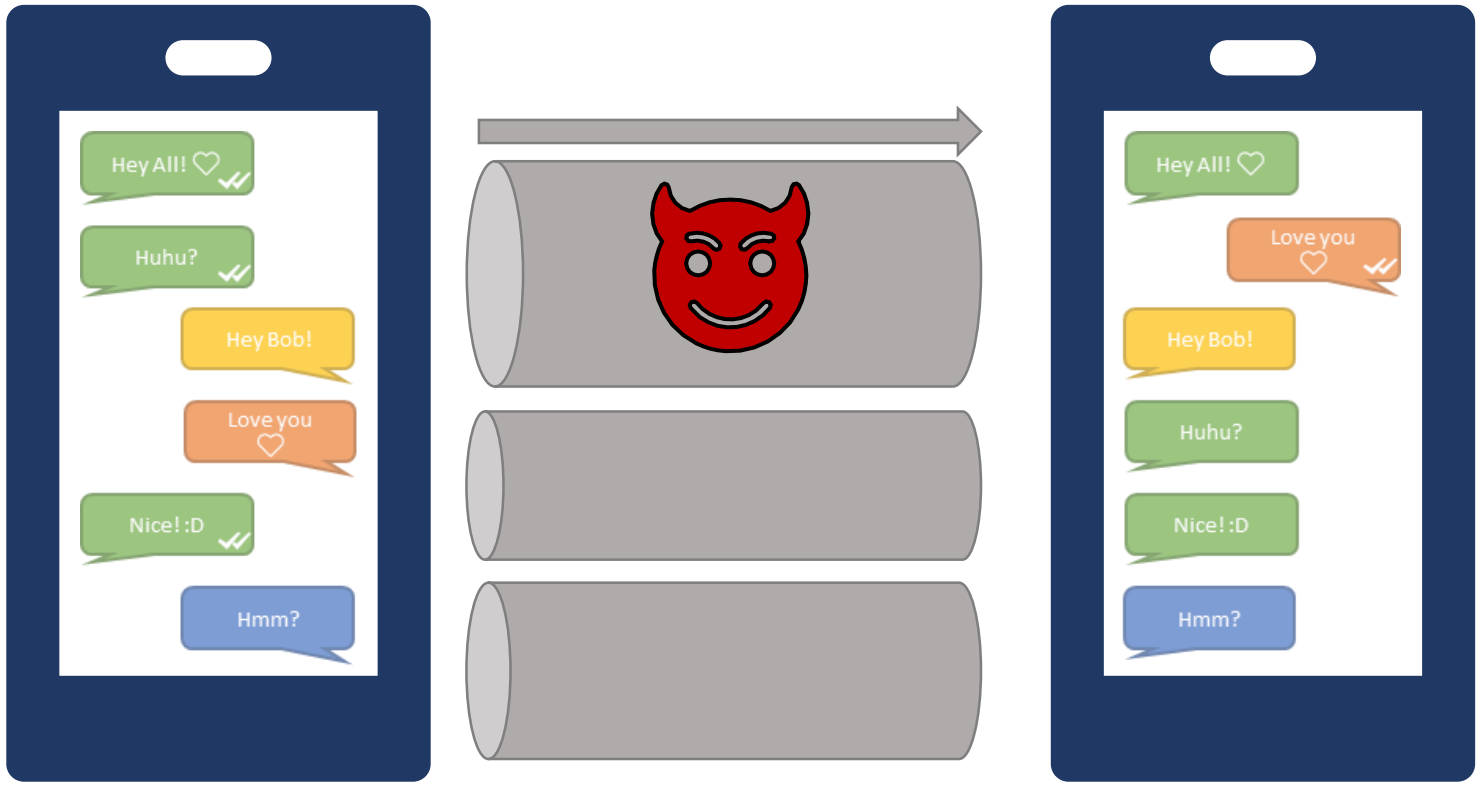
Agenda

- Messaging is complex
- Finding a Syntax
- **Understanding Attackers**
- Defining Security
- Understanding Constructions



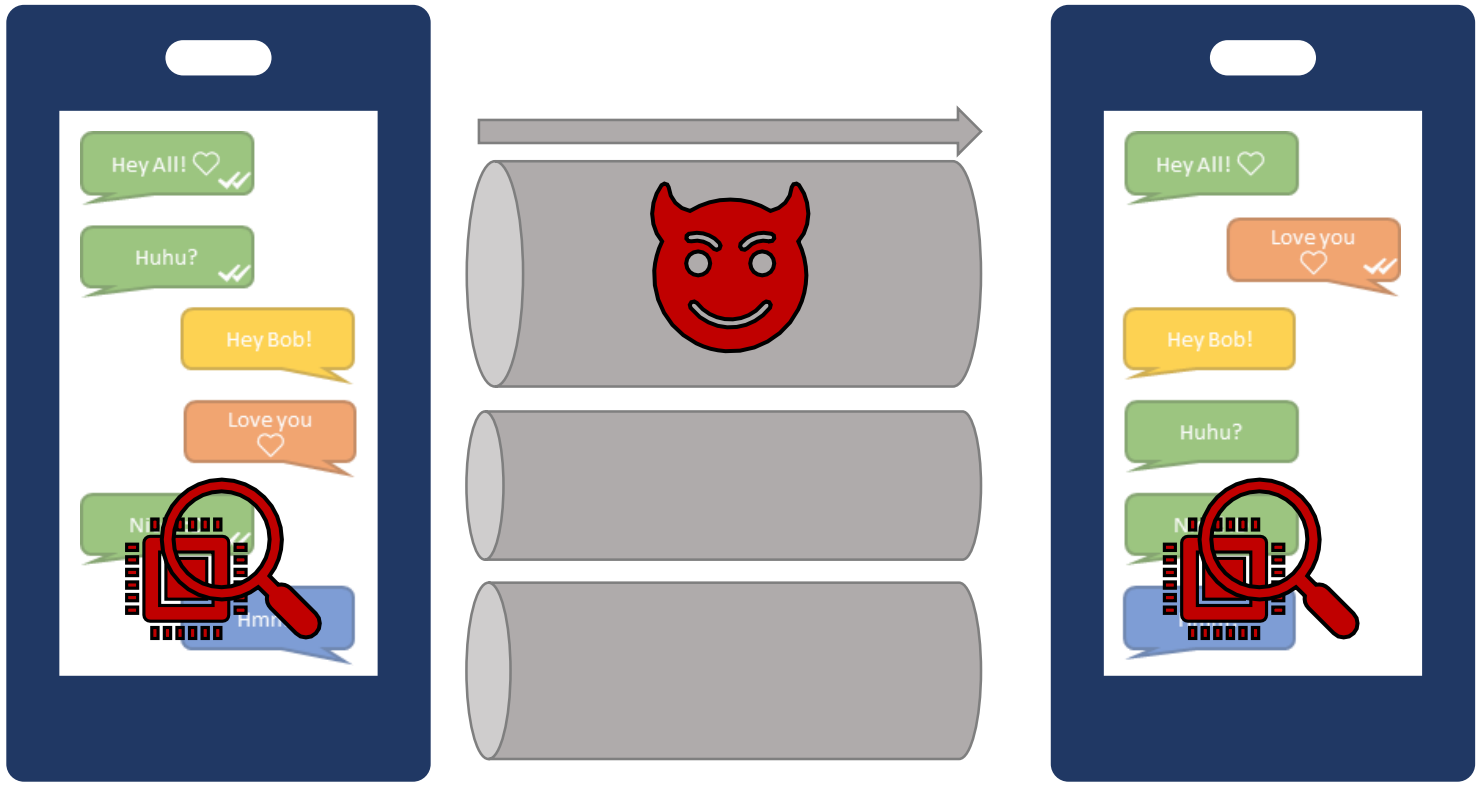
Attacker

- Active attacker on network



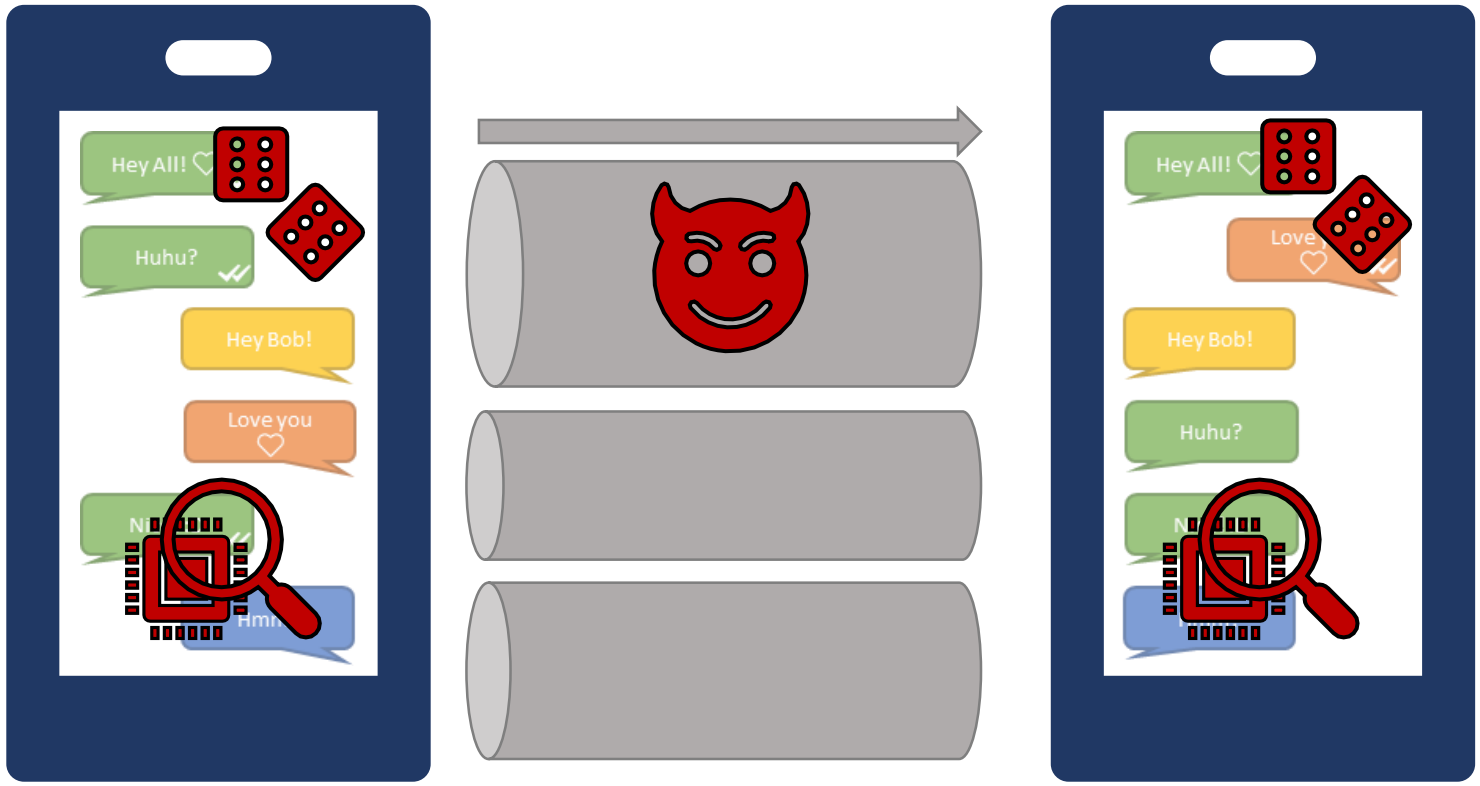
Attacker

- Active attacker on network
- Exposure of secret states
  - Mobile devices are easily accessible
  - Sessions take long time



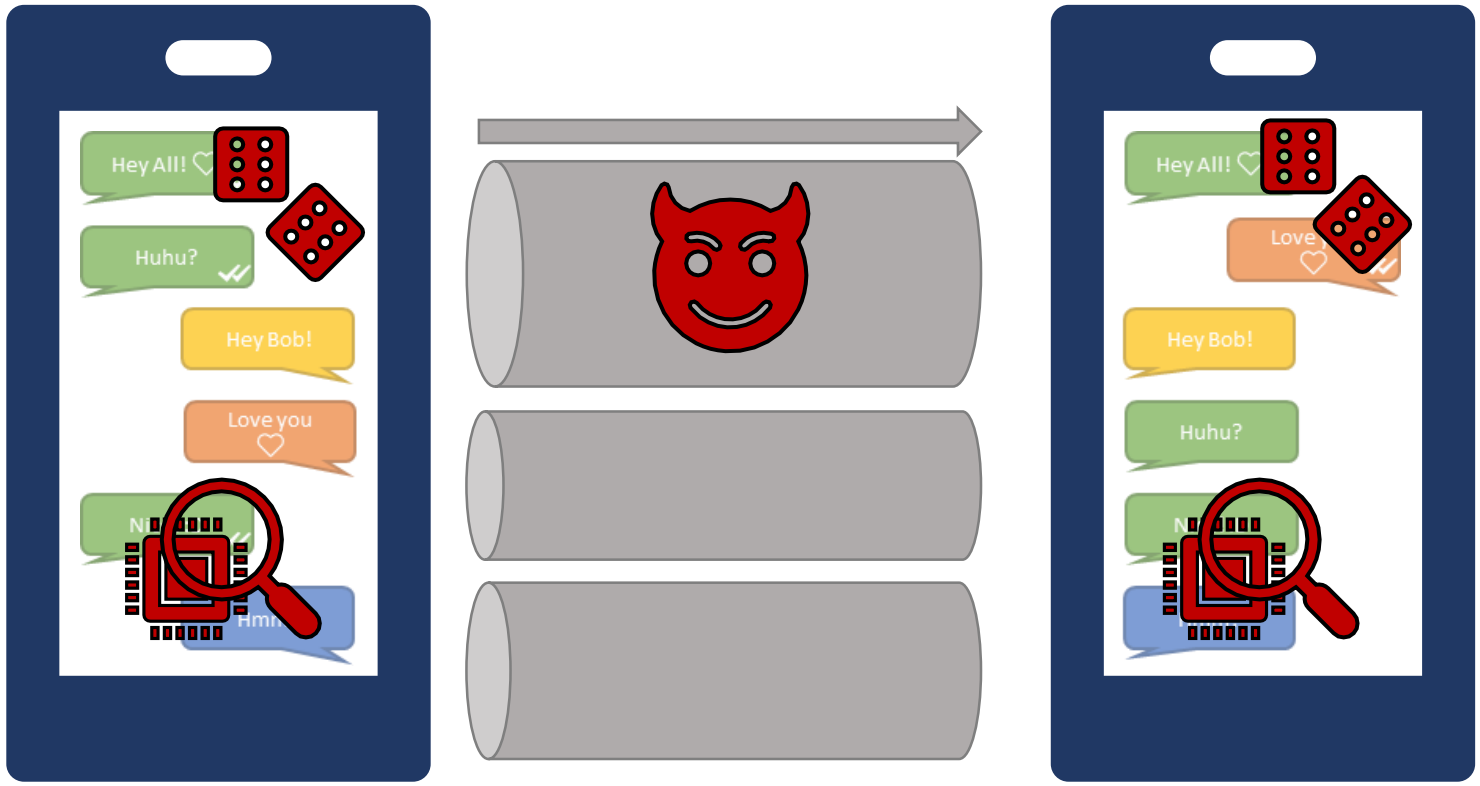
Attacker

- Active attacker on network
- Exposure of secret states
- Attacks against executions' randomness
  - Entropy low
  - Ba(d/ckdoored) randomness generator



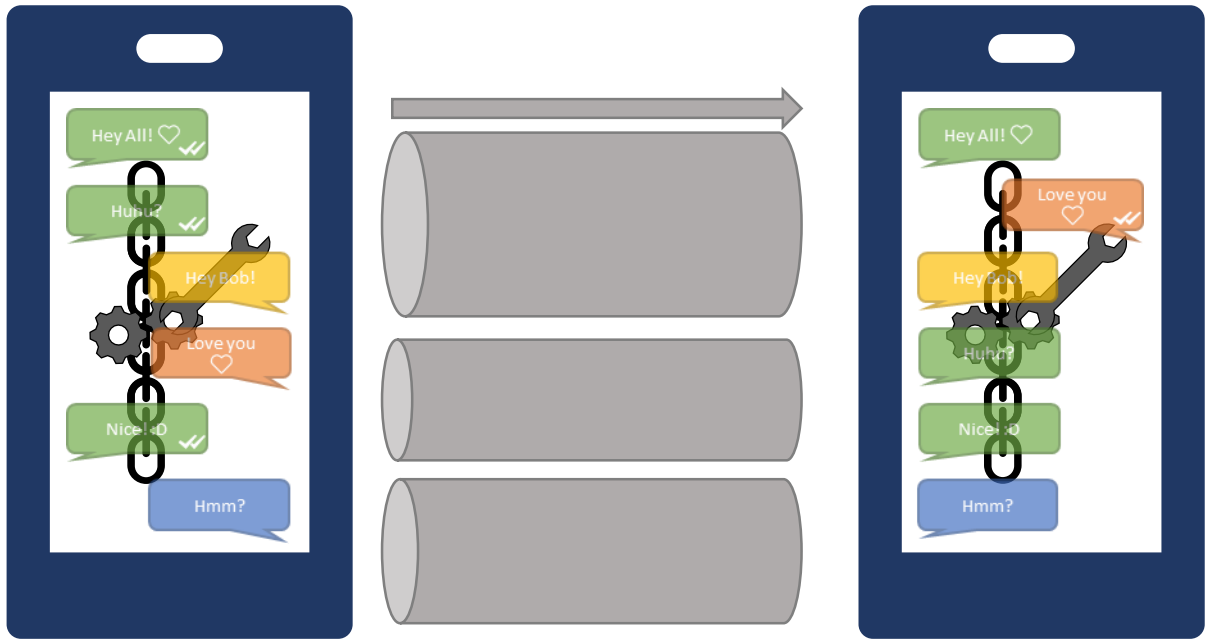
Attacker

- Many more attacker scenarios…
  - Attacker against key distribution
  - Attackers in attacked group
  - Leakage during computation
  - Attacker in implementation



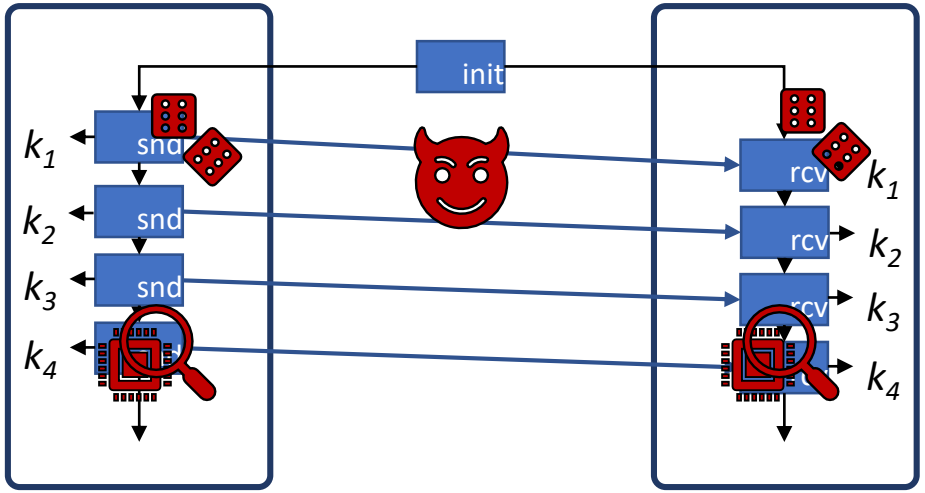
Agenda

- Messaging is complex
- Finding a Syntax
- Understanding Attackers
- **Defining Security**
- Understanding Constructions



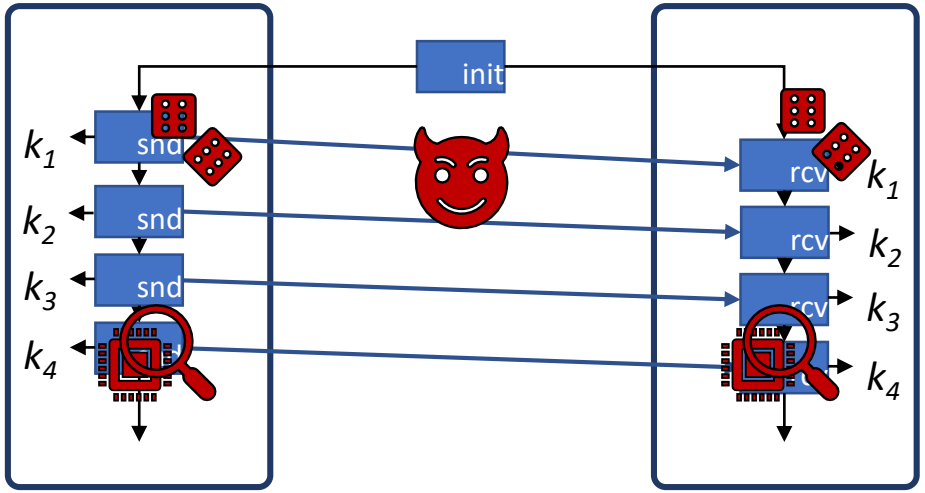
Security definition

- Many security properties, depend on:
  - Syntax
  - Correctness
  - Semantic
- Multiple levels of properties:
  - **Strongest security**
  - Intuitive security (ambiguous)
  - Efficiently instantiable security (ambiguous)



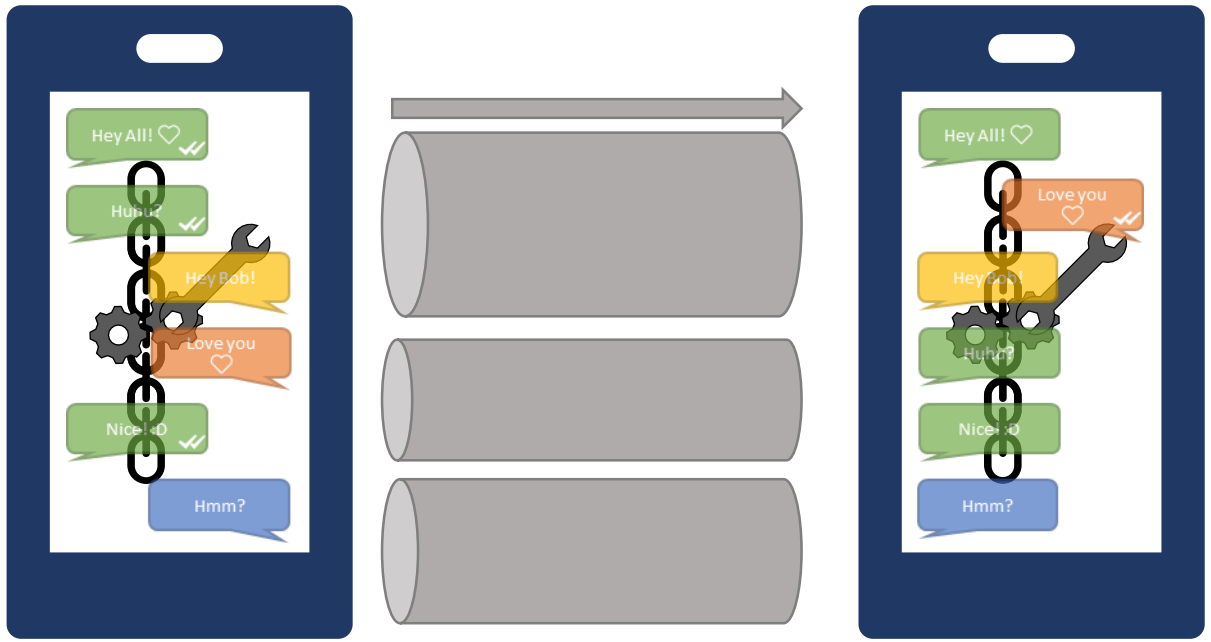
(Strongest) Security definition

- Allow attacker full (defined) power
- Define security property as:
  Event that attacker should not trigger
  Here: attacker guesses exchanged key
- Exclude ways that directly trigger this event (unpreventable attacks)
  - Exposed state of B reveals B's future keys
  - …
- Protocol is insecure if event triggers in remaining cases



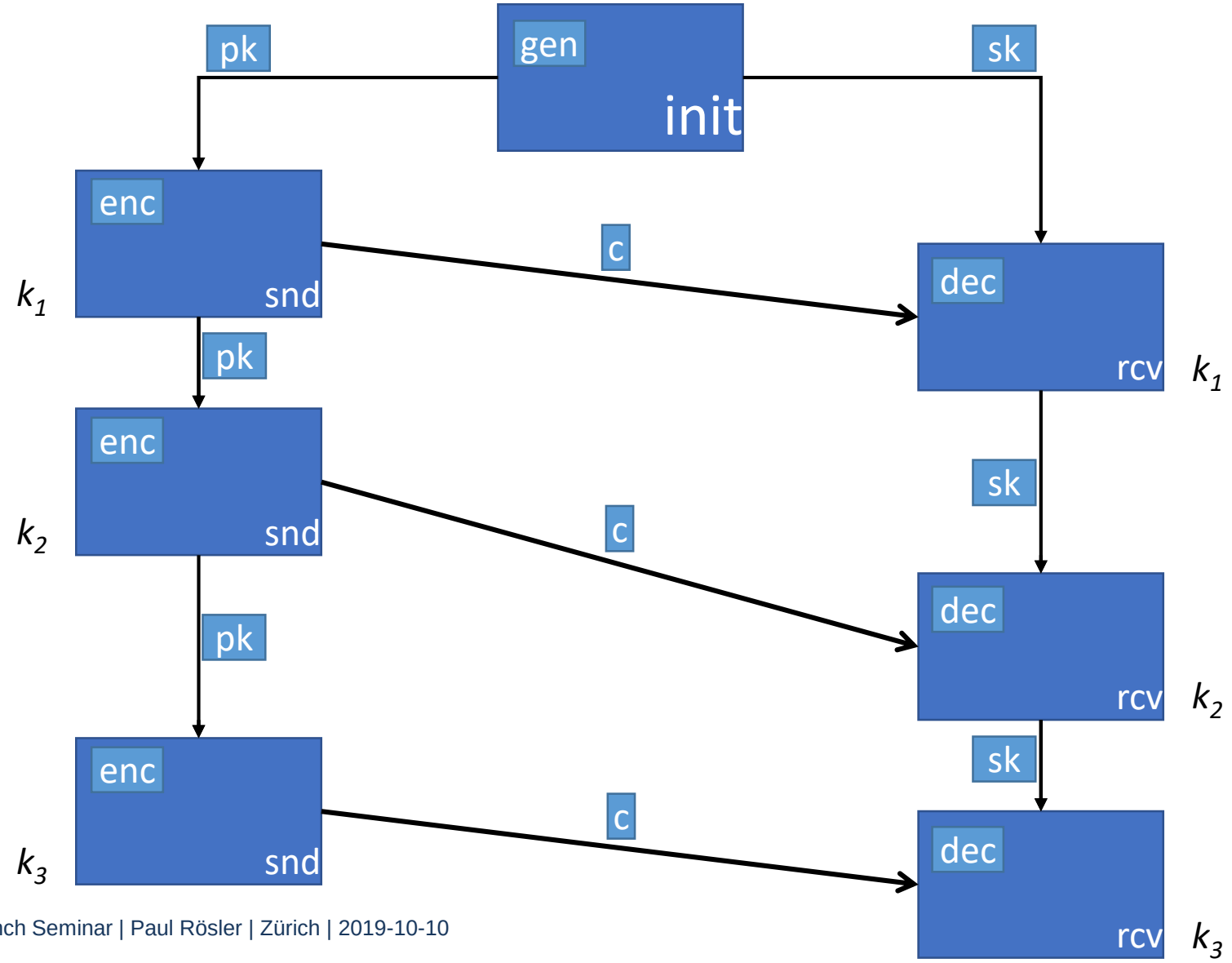
Agenda

- Messaging is complex
- Finding a Syntax
- Understanding Attackers
- Defining Security
- **Understanding Constructions**



Constructing Unidirectional RKE

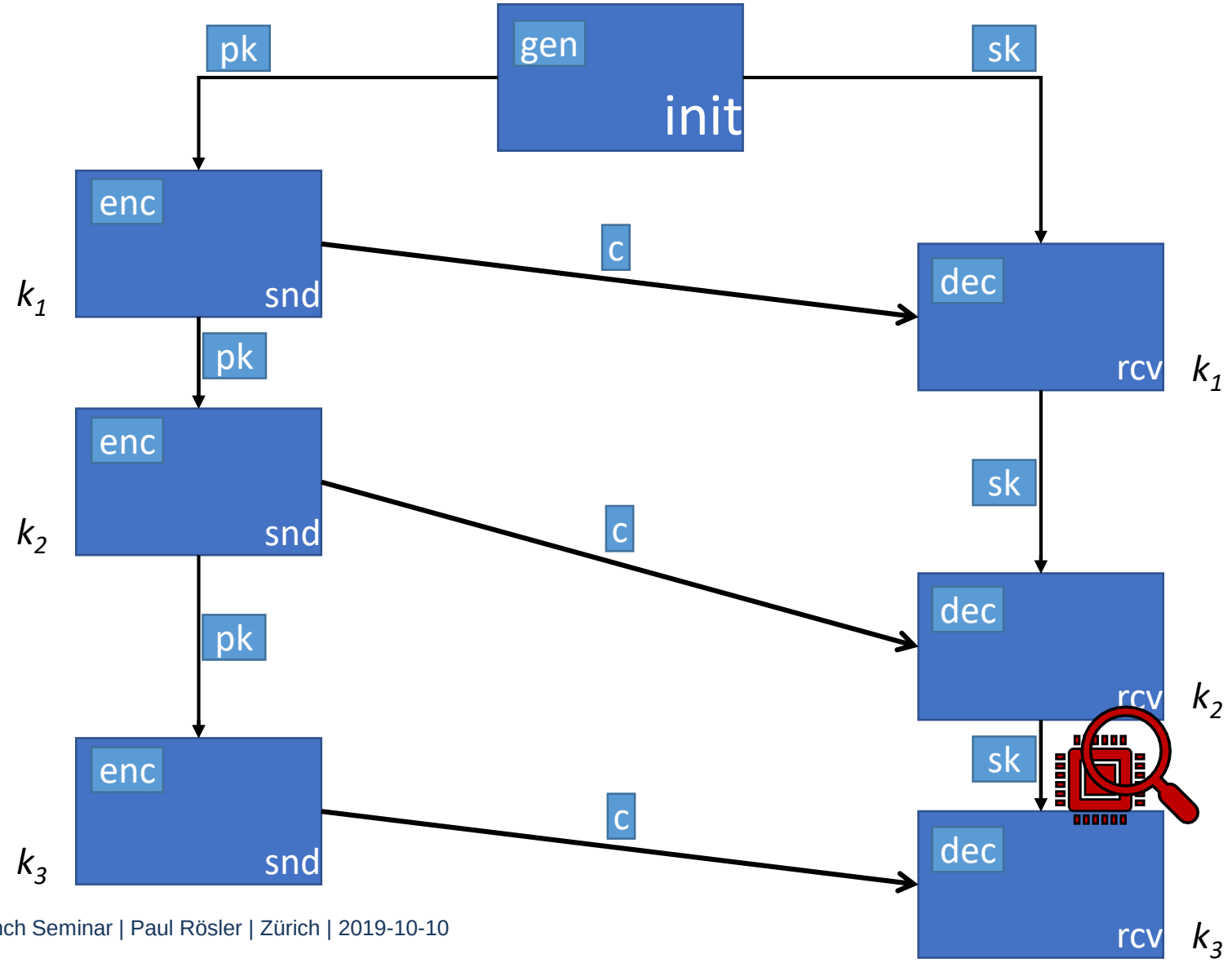
- Alice: enc(pk)→$ c k
- Bob: dec(sk c)→ k



Constructing Unidirectional RKE

- Alice: enc(pk)→$ c k
- Bob: dec(sk c)→ k

- Problem:
  exposure of B's state
  reveals all his keys
- Secret key update!



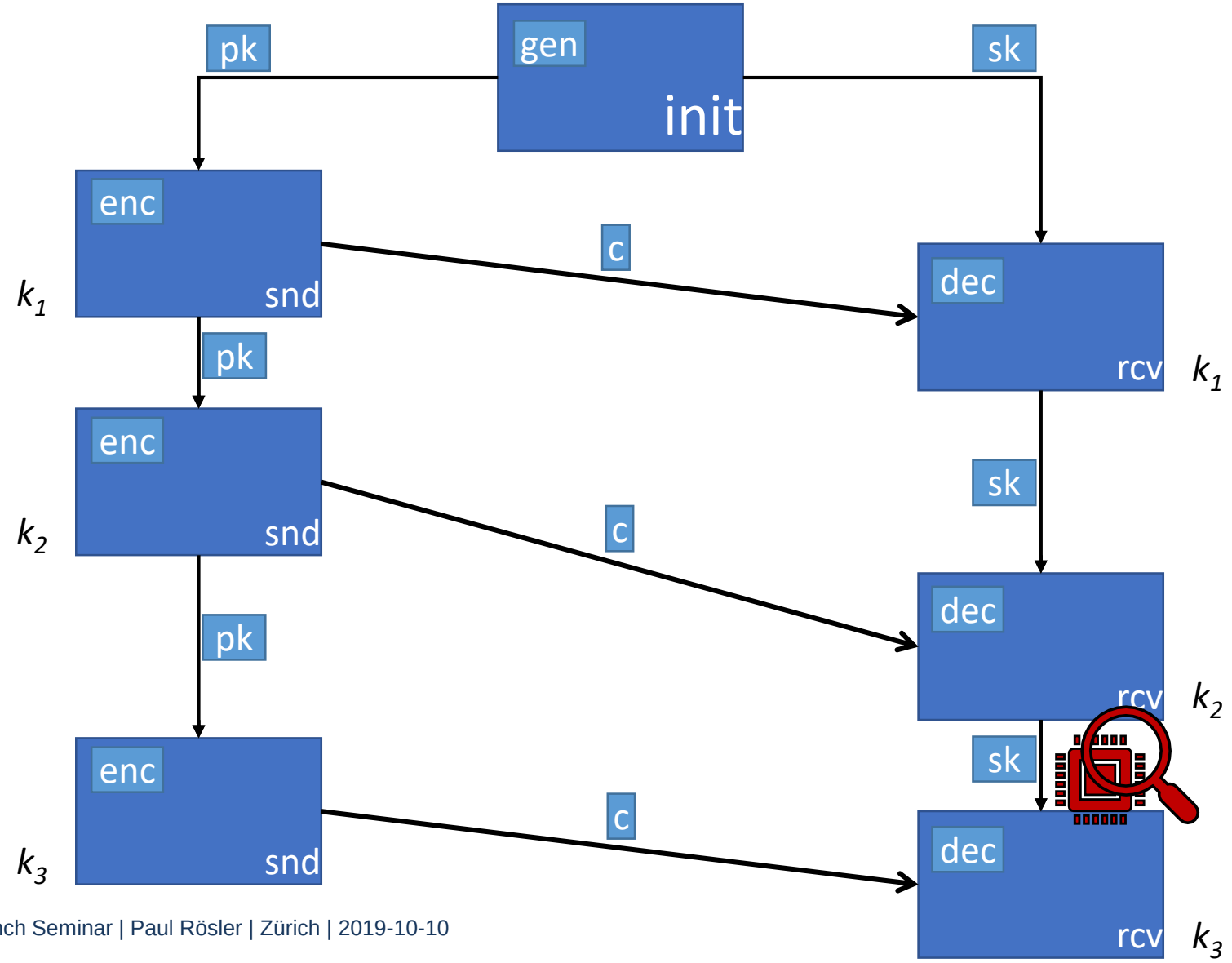
Constructing Unidirectional RKE

- Alice: enc(pk)→$ c k
- Bob: dec(sk c)→ k

- Problem:
  exposure of B's state reveals all his keys
- Secret key update!
- Alice: H(c k)→ k_i sk

  gen(sk)→pk

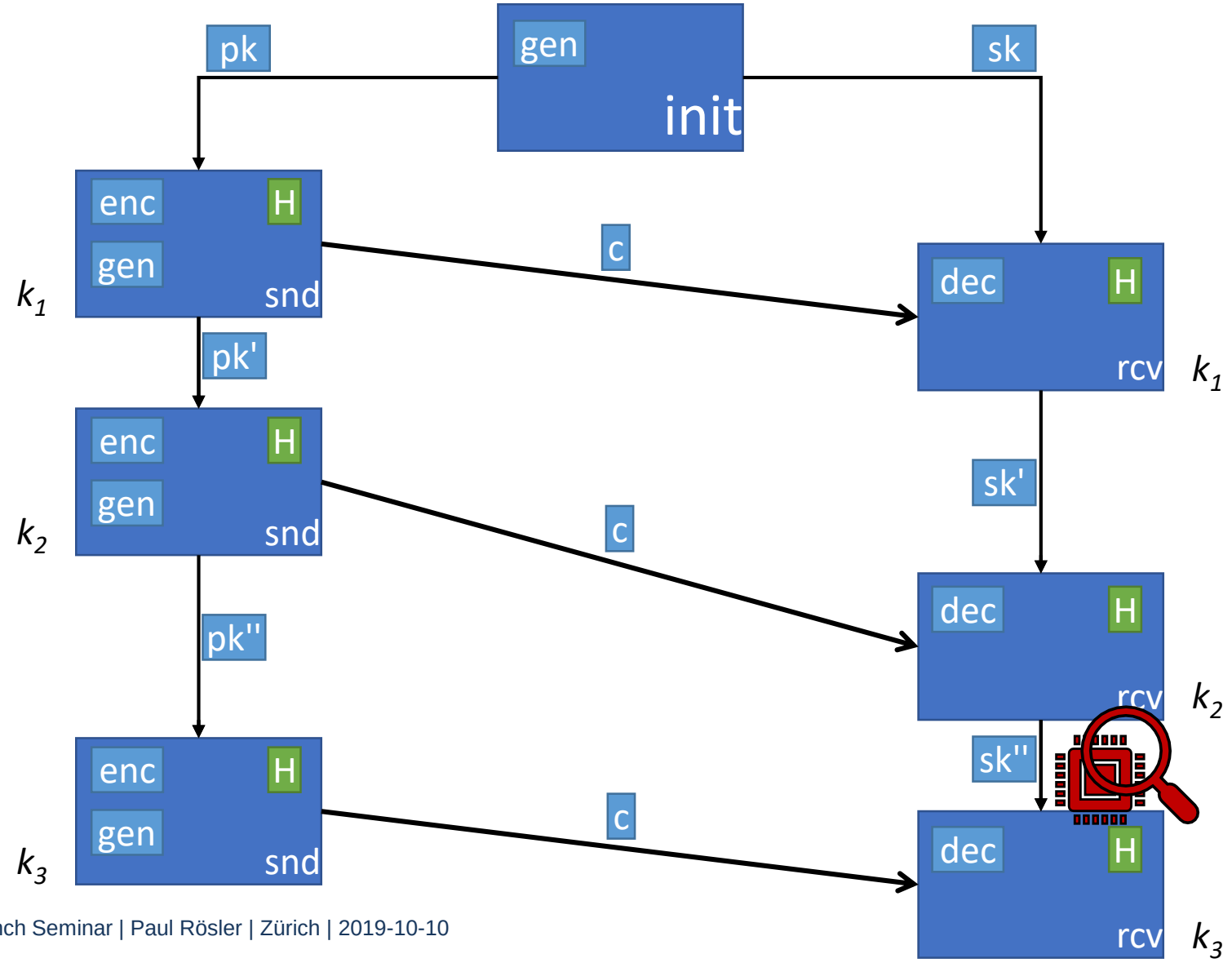
  Forget sk
- Bob: H(c k)→ k_i sk



Constructing Unidirectional RKE

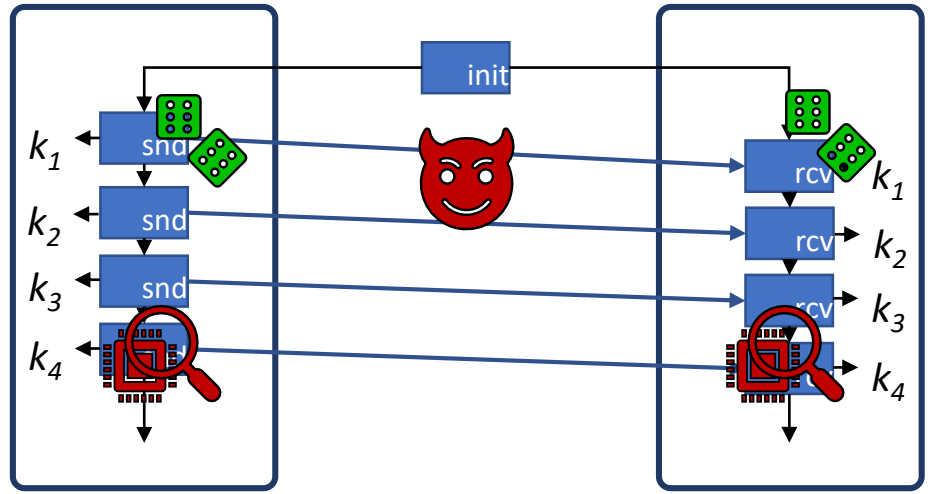
- Alice: enc(pk)→$ c k
- Bob: dec(sk c)→ k

- Problem:
  exposure of B's state reveals all his keys
- Secret key update!
- Alice: H(c k)→ k_i sk
  gen(sk)→pk
  Forget sk
- Bob: H(c k)→ k_i sk



Construction ↔ Security definition

- Bases on pure public key encryption
  - Randomness is good
- *Our* bidirectional RKE uses *heavier* tools
- Many papers with different definitions and different constructions of ratcheting now:



A Formal Security Analysis of the Signal Messaging Protocol
Extended Version, November 2017†

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

Ratcheted Encryption and Key Exchange: The Security of Messaging

Mihir Bellare, Asha Camper Singh, Joseph Jaeger, Maya Nyayapati, Igors Stepanovs

Asynchronous ratcheted key exchange

Bertram Poettering[1] and Paul Rösler[2]

[1] Information Security Group, Royal Holloway, University of London
bertram.poettering@rhul.ac.uk
[2] Horst-Görtz Institute for IT Security,
Chair for Network and Data Security, Ruhr-University Bochum
paul.roesler@rub.de

Optimal Channel Security Against Fine-Grained State Compromise: The Safety of Messaging

Joseph Jaeger, Igors Stepanovs

Bidirectional Asynchronous Ratcheted Key Agreement with Linear Complexity*

F. Betül Durak[1,2] and Serge Vaudenay[1]

[1] Ecole Polytechnique Fédérale de Lausanne (EPFL)
Lausanne, Switzerland
[2] Robert Bosch LLC — Research and Technology Center
Pittsburgh PA, USA

Efficient Ratcheting: Almost-Optimal Guarantees for Secure Messaging

Daniel Jost, Ueli Maurer, and Marta Mularczyk*

Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland.
{dajost, maurer, mumarta}@inf.ethz.ch

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

A Unified and Composable Take on Ratcheting

Daniel Jost, Ueli Maurer, and Marta Mularczyk*

Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland.
{dajost, maurer, mumarta}@inf.ethz.ch

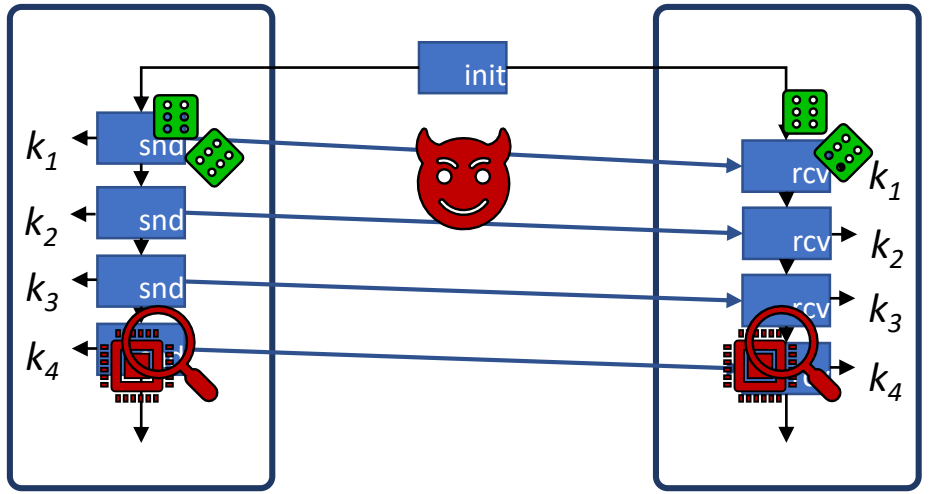
Beyond Security and Efficiency: On-Demand Ratcheting with Security Awareness

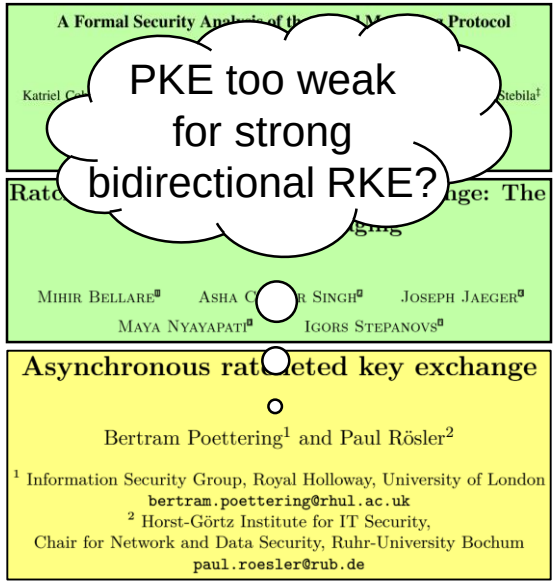
Andrea Caforio[1], F. Betül Durak[2], and Serge Vaudenay[1]

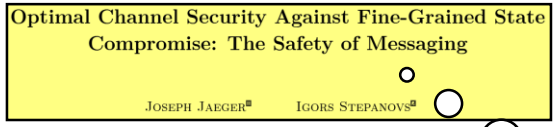
[1] Ecole Polytechnique Fédérale de Lausanne (EPFL)
Lausanne, Switzerland
[2] Robert Bosch LLC - Research and Technology Center
Pittsburgh PA, USA

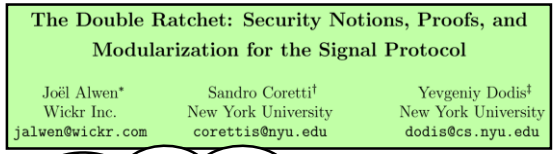
Construction ↔ Security definition

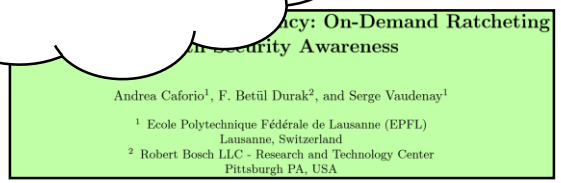
- Bases on pure public key encryption
  - Randomness is good
- *Our* bidirectional RKE uses *heavier* tools
- Many papers with different definitions and different constructions of ratcheting now:
  - Also others with *strongest* security relied on heavier tools
  - "(When) do we need these tools?"
    – Vaudenay, Balli, me











Impact of bad randomness?

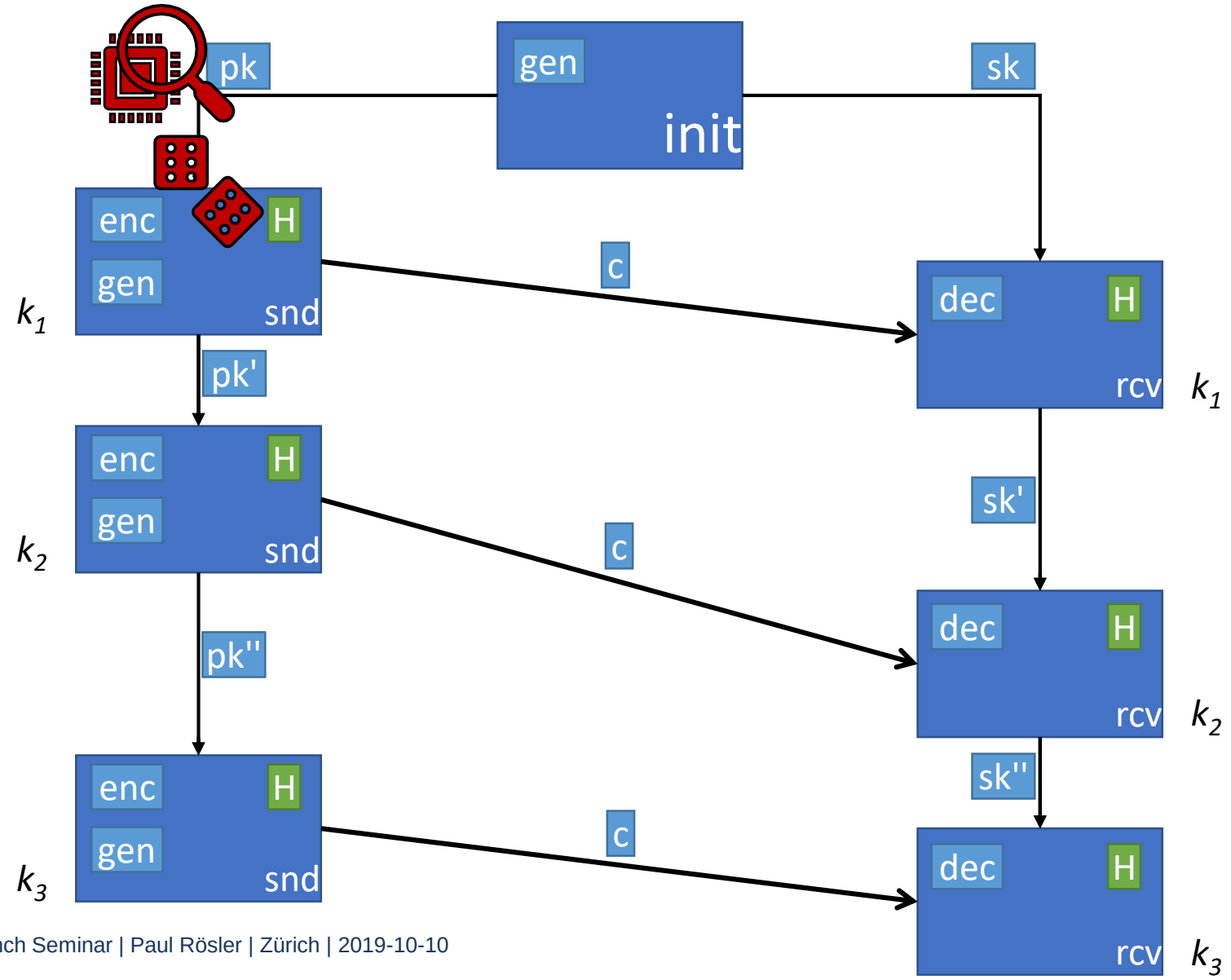
Constructing Unidirectional RKE

- Alice: enc(pk)→$ c k
- Bob: dec(sk c)→ k

- Problem: randomness is revealed (and A's state exposed)
- Secret key update!
- Alice: H(c k)→ k_i sk

  gen(sk)→pk

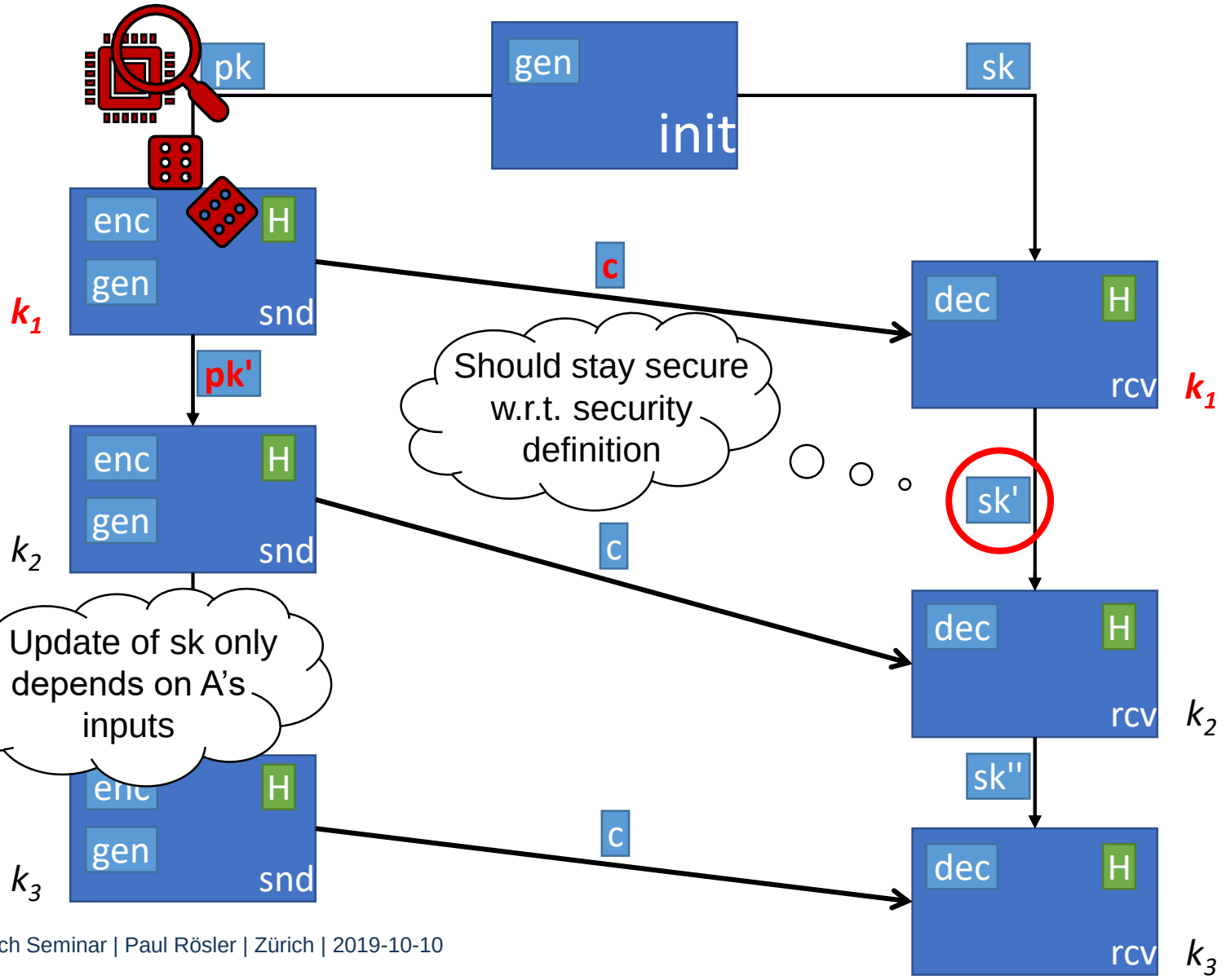
  Forget sk
- Bob: H(c k)→ k_i sk



Constructing Unidirectional RKE

- Alice: enc(pk)→$ c k
- Bob: dec(sk c)→ k

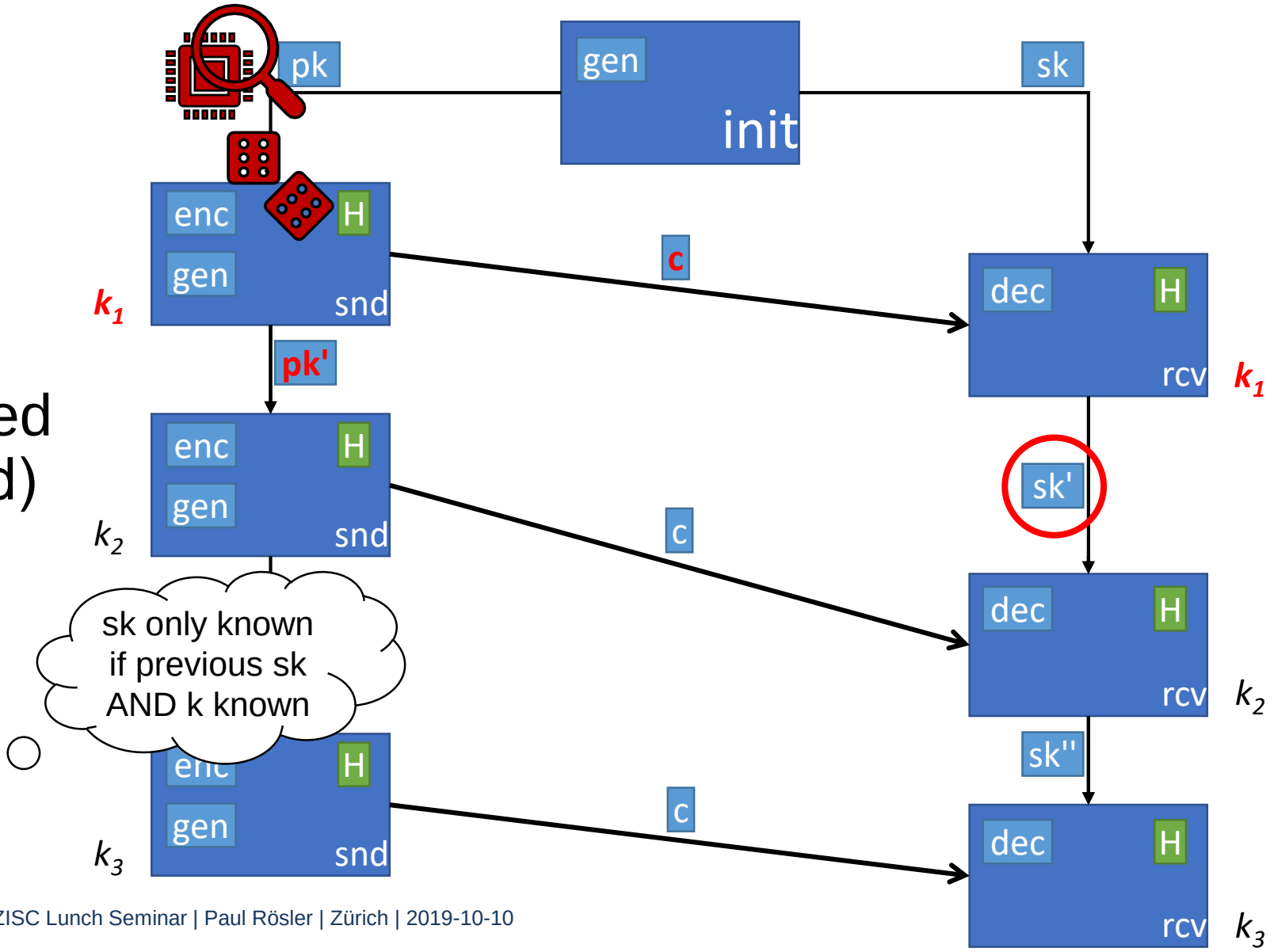
- Problem: randomness exposed (and A's state exposed)
- Secret key update!
- Alice: H(c k)→ k_i sk
  gen(sk)→pk
  Forget sk
- Bob: H(c k)→ k_i sk



Constructing Unidirectional RKE

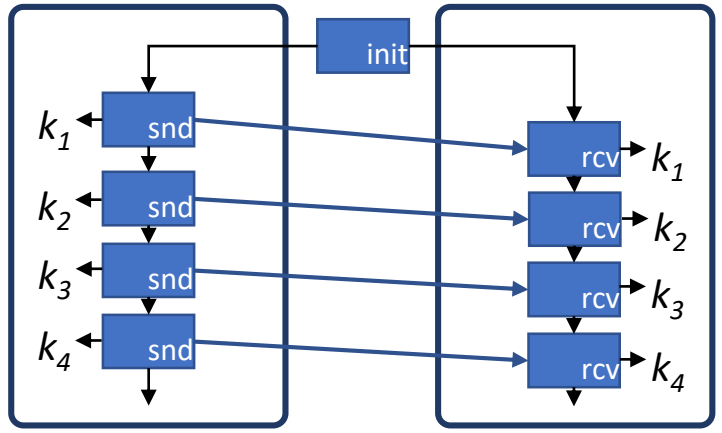
- Alice: enc(pk)→$ c k
- Bob: dec(sk c)→ k

- Problem: randomness is revealed (and A's state exposed)
- Secret key update!
- Alice: H(c k)→ k_i
  up (pk k)→ pk
- Bob: H(c k)→ k_i
  up (sk k)→ sk



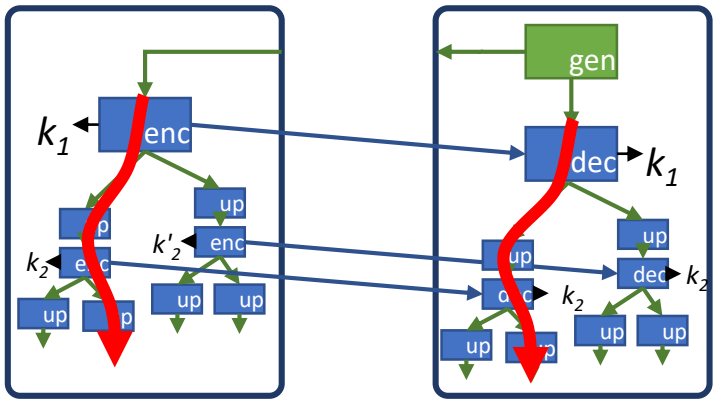
Heavier Tool: key-updatable PKC

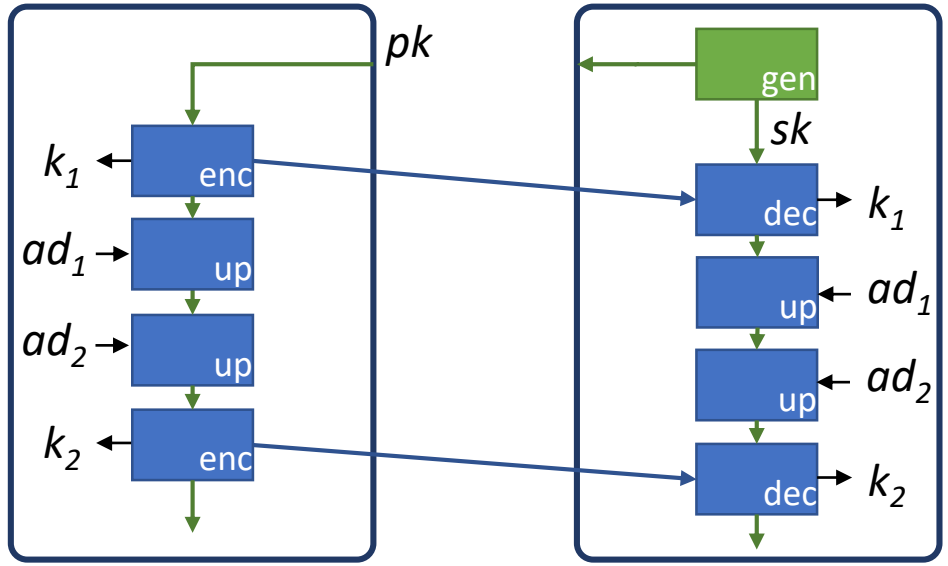
- Idea of key-updatable PKC : update pk and sk independently and forward securely
- Based on (expensive) HIBE
  - Not full HIBE, only path on ‘identity tree’



up (pk k)→ pk

up (sk k)→ sk

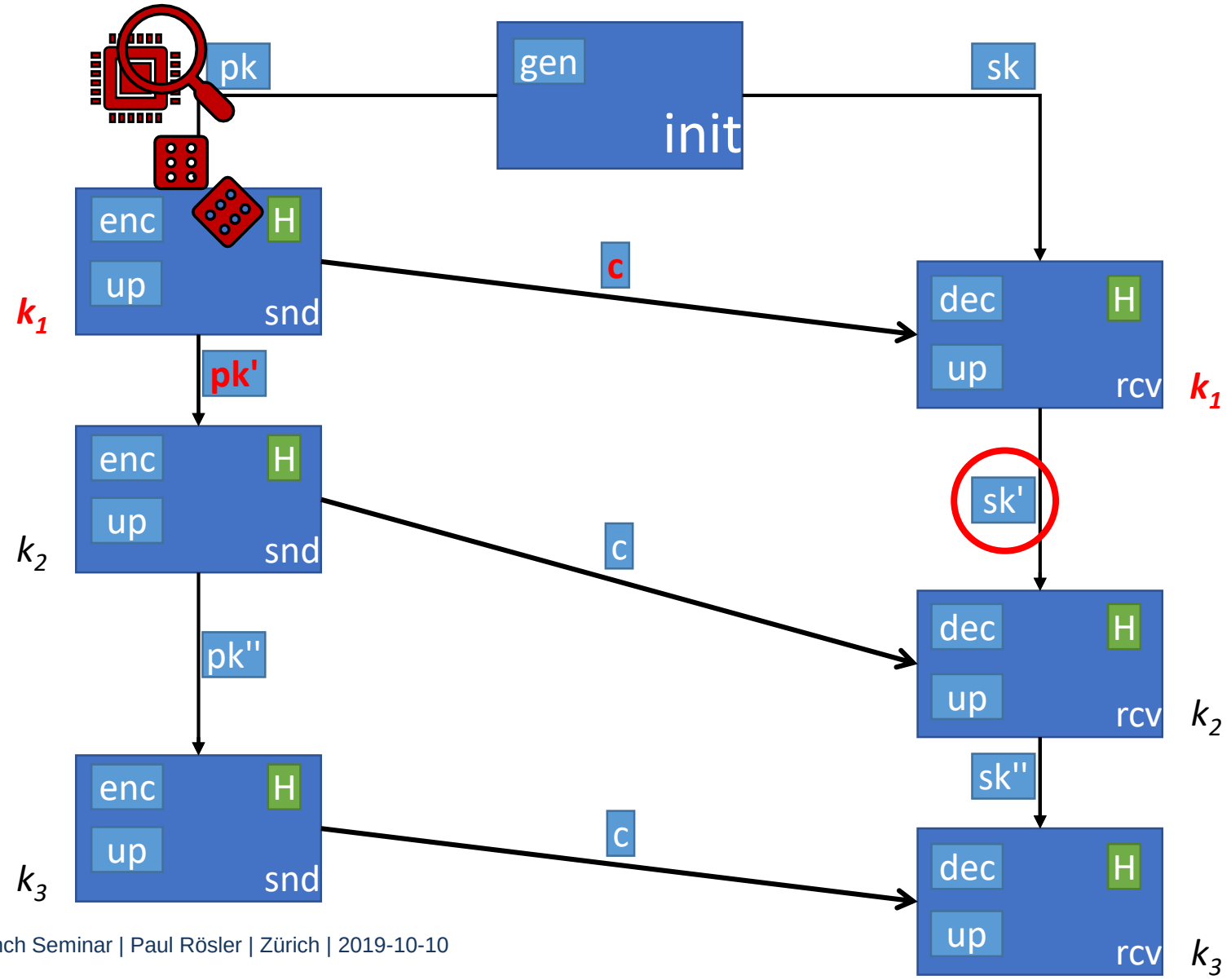




Constructing Unidirectional RKE

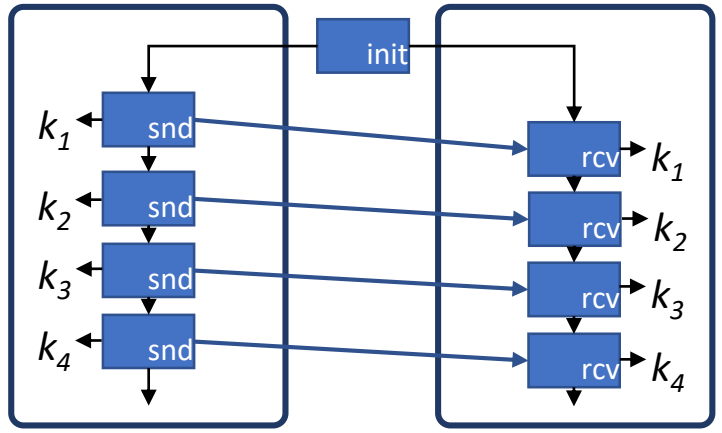
- Alice: enc(pk)→$ c k
- Bob: dec(sk c)→ k

- Problem: randomness is revealed (and A's state exposed)
- Secret key update!
- Alice: H(c k)→ k_i
  up (pk k)→ pk
- Bob: H(c k)→ k_i
  up (sk k)→ sk



Heavier Tool: key-updatable PKC

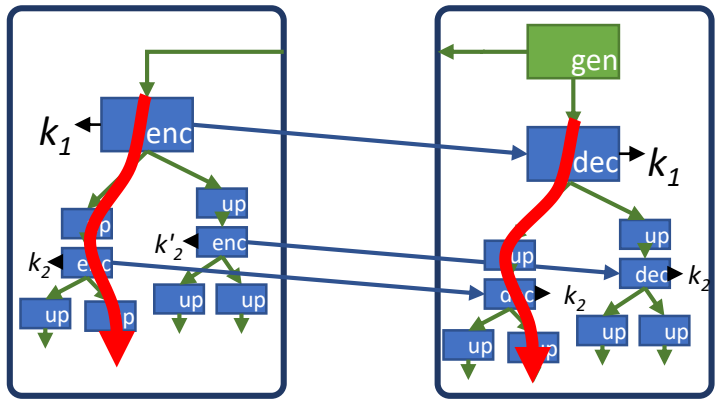
- Idea of key-updatable PKC : update pk and sk independently and forward securely
- Based on (expensive) HIBE
  - Not full HIBE, only path on ‘identity tree’

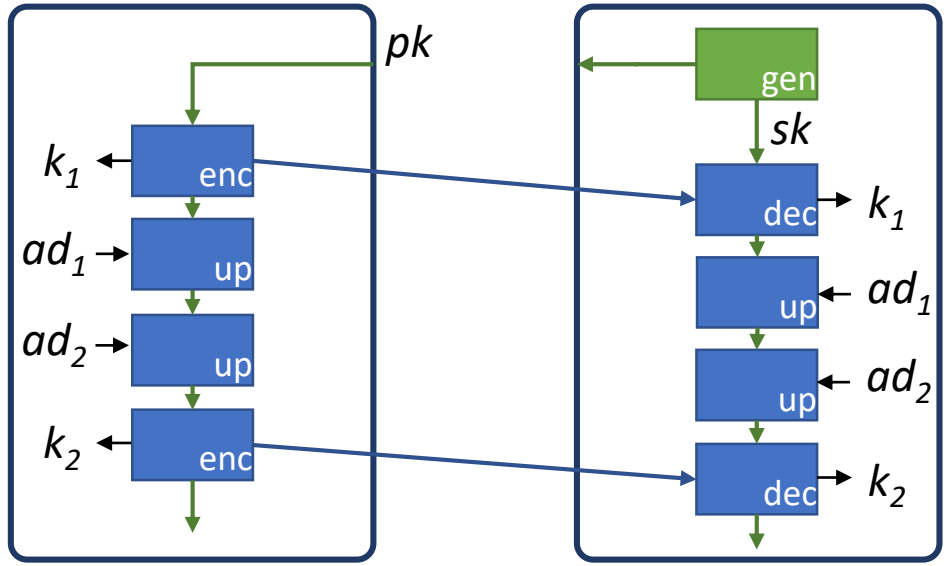


Unpublished work w/ Serge Vaudenay & Fatih Balli

up (pk k)→ pk

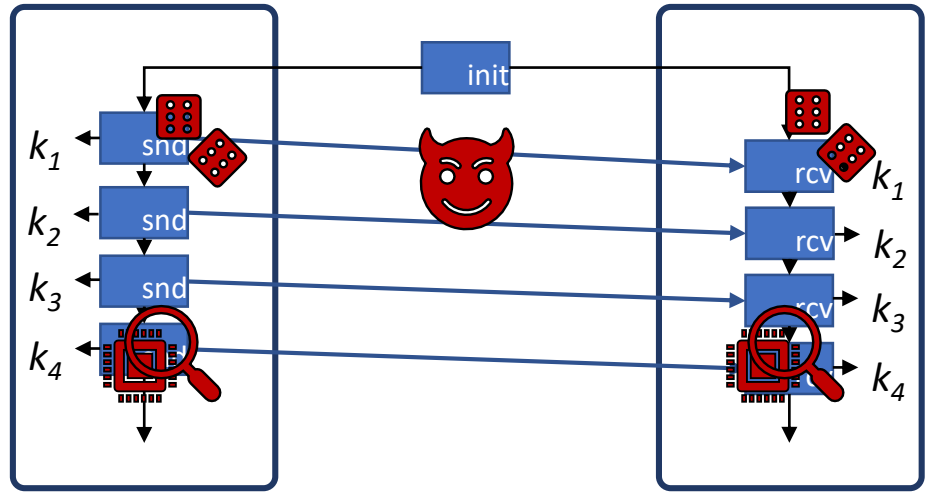
up (sk k)→ sk





Construction ↔ Security definition

- Bases on pure public key encryption
  - Randomness is good
- *Our* bidirectional RKE uses *heavier* tools
- Many papers with different definitions and different constructions of ratcheting now:
  - Also others with *strongest* security relied on heavier tools
  - (When) do we need these tools?



A Formal Security Analysis of the Signal Messaging Protocol
Extended Version, November 2017†

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

Ratcheted Encryption and Key Exchange: The Security of Messaging

Mihir Bellare, Asha Camper Singh, Joseph Jaeger, Maya Nyayapati, Igors Stepanovs

Asynchronous ratcheted key exchange

Bertram Poettering[1] and Paul Rösler[2]
[1] Information Security Group, Royal Holloway, University of London
bertram.poettering@rhul.ac.uk
[2] Horst-Görtz Institute for IT Security,
Chair for Network and Data Security, Ruhr-University Bochum
paul.roesler@rub.de

Optimal Channel Security Against Fine-Grained State Compromise: The Safety of Messaging

Joseph Jaeger, Igors Stepanovs

Bidirectional Asynchronous Ratcheted Key Agreement with Linear Complexity*

F. Betül Durak[1,2] and Serge Vaudenay[1]
[1] Ecole Polytechnique Fédérale de Lausanne (EPFL)
Lausanne, Switzerland
[2] Robert Bosch LLC — Research and Technology Center
Pittsburgh PA, USA

Efficient Ratcheting: Almost-Optimal Guarantees for Secure Messaging

Daniel Jost, Ueli Maurer, and Marta Mularczyk*
Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland.
{dajost, maurer, mumarta}@inf.ethz.ch

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

A Unified and Composable Take on Ratcheting

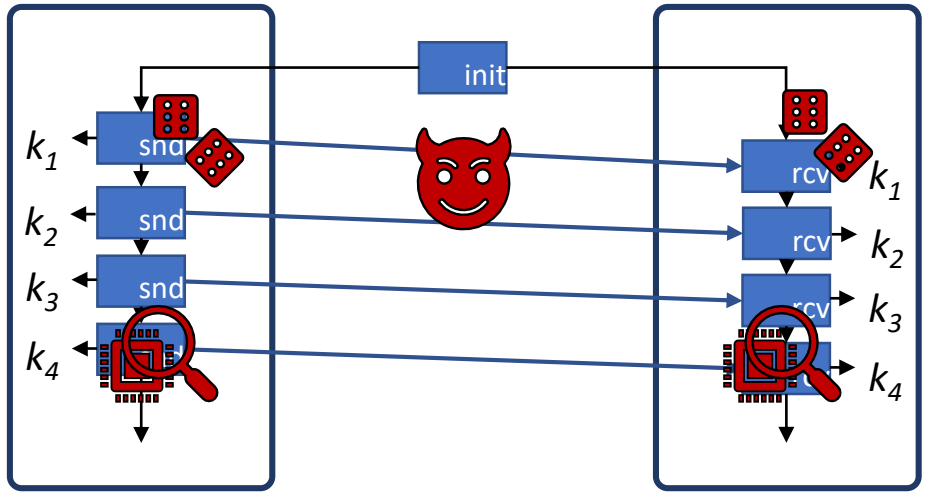
Daniel Jost, Ueli Maurer, and Marta Mularczyk*
Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland.
{dajost, maurer, mumarta}@inf.ethz.ch

Beyond Security and Efficiency: On-Demand Ratcheting with Security Awareness

Andrea Caforio[1], F. Betül Durak[2], and Serge Vaudenay[1]
[1] Ecole Polytechnique Fédérale de Lausanne (EPFL)
Lausanne, Switzerland
[2] Robert Bosch LLC - Research and Technology Center
Pittsburgh PA, USA

Construction ↔ Security definition

- Havier tools are necessary for unidirectional RKE if



A Formal Security Analysis of the Signal Messaging Protocol
Extended Version, November 2017†

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

Ratcheted Encryption and Key Exchange: The Security of Messaging

Mihir Bellare — Asha Camper Singh — Joseph Jaeger
Maya Nyayapati — Igors Stepanovs

Asynchronous ratcheted key exchange

Bertram Poettering[1] and Paul Rösler[2]

[1] Information Security Group, Royal Holloway, University of London
bertram.poettering@rhul.ac.uk
[2] Horst-Görtz Institute for IT Security,
Chair for Network and Data Security, Ruhr-University Bochum
paul.roesler@rub.de

Optimal Channel Security Against Fine-Grained State Compromise: The Safety of Messaging

Joseph Jaeger — Igors Stepanovs

Bidirectional Asynchronous Ratcheted Key Agreement with Linear Complexity*

F. Betül Durak[1,2] and Serge Vaudenay[1]

[1] Ecole Polytechnique Fédérale de Lausanne (EPFL)
Lausanne, Switzerland
[2] Robert Bosch LLC — Research and Technology Center
Pittsburgh PA, USA

Efficient Ratcheting: Almost-Optimal Guarantees for Secure Messaging

Daniel Jost, Ueli Maurer, and Marta Mularczyk*

Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland.
{dajost, maurer, mumarta}@inf.ethz.ch

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

A Unified and Composable Take on Ratcheting

Daniel Jost, Ueli Maurer, and Marta Mularczyk*

Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland.
{dajost, maurer, mumarta}@inf.ethz.ch

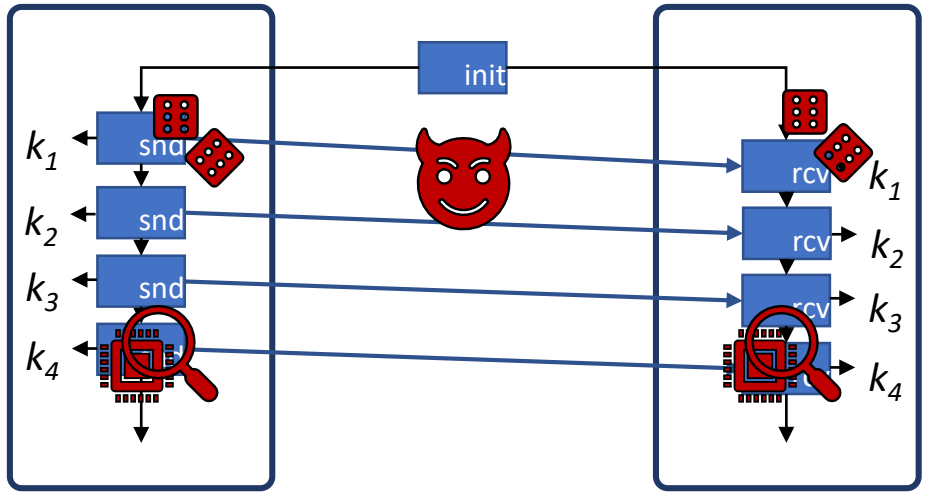
Beyond Security and Efficiency: On-Demand Ratcheting with Security Awareness

Andrea Caforio[1], F. Betül Durak[2], and Serge Vaudenay[1]

[1] Ecole Polytechnique Fédérale de Lausanne (EPFL)
Lausanne, Switzerland
[2] Robert Bosch LLC - Research and Technology Center
Pittsburgh PA, USA

Construction ↔ Security definition

- Havier tools are necessary for unidirectional RKE if
  - State exposures are not unnecessarily restricted



A Formal Security Analysis of the Signal Messaging Protocol
Extended Version, November 2017†

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

Ratcheted Encryption and Key Exchange: The Security of Messaging

Mihir Bellare[1] Asha Camper Singh[2] Joseph Jaeger[3]
Maya Nyayapati[3] Igors Stepanovs[3]

Asynchronous ratcheted key exchange

Bertram Poettering[1] and Paul Rösler[2]

[1] Information Security Group, Royal Holloway, University of London
bertram.poettering@rhul.ac.uk
[2] Horst-Görtz Institute for IT Security,
Chair for Network and Data Security, Ruhr-University Bochum
paul.roesler@rub.de

Optimal Channel Security Against Fine-Grained State Compromise: The Safety of Messaging

Joseph Jaeger[3] Igors Stepanovs[3]

Bidirectional Asynchronous Ratcheted Key Agreement with Linear Complexity*

F. Betül Durak[1,2] and Serge Vaudenay[1]

[1] Ecole Polytechnique Fédérale de Lausanne (EPFL)
Lausanne, Switzerland
[2] Robert Bosch LLC — Research and Technology Center
Pittsburgh PA, USA

Efficient Ratcheting: Almost-Optimal Guarantees for Secure Messaging

Daniel Jost, Ueli Maurer, and Marta Mularczyk*

Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland.
{dajost, maurer, mumarta}@inf.ethz.ch

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

A Unified and Composable Take on Ratcheting

Daniel Jost, Ueli Maurer, and Marta Mularczyk*

Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland.
{dajost, maurer, mumarta}@inf.ethz.ch

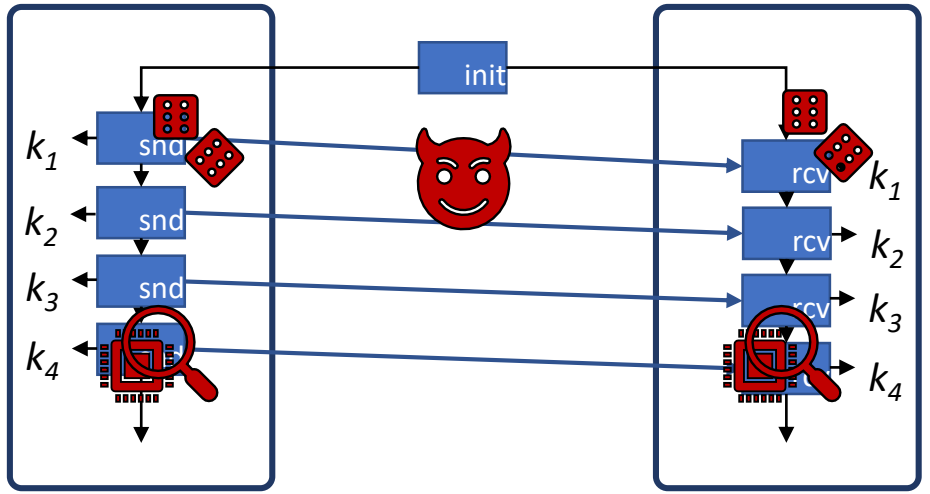
Beyond Security and Efficiency: On-Demand Ratcheting with Security Awareness

Andrea Caforio[1], F. Betül Durak[2], and Serge Vaudenay[1]

[1] Ecole Polytechnique Fédérale de Lausanne (EPFL)
Lausanne, Switzerland
[2] Robert Bosch LLC - Research and Technology Center
Pittsburgh PA, USA

Construction ↔ Security definition

- Havier tools are necessary for unidirectional RKE if
  - State exposures are not unnecessarily restricted
  - Bad randomness is considered



A Formal Security Analysis of the Signal Messaging Protocol
Extended Version, November 2017†

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

Ratcheted Encryption and Key Exchange: The Security of Messaging

Mihir Bellare, Asha Camper Singh, Joseph Jaeger, Maya Nyayapati, Igors Stepanovs

Asynchronous ratcheted key exchange

Bertram Poettering[1] and Paul Rösler[2]
[1] Information Security Group, Royal Holloway, University of London
bertram.poettering@rhul.ac.uk
[2] Horst-Görtz Institute for IT Security,
Chair for Network and Data Security, Ruhr-University Bochum
paul.roesler@rub.de

Optimal Channel Security Against Fine-Grained State Compromise: The Safety of Messaging

Joseph Jaeger, Igors Stepanovs

Bidirectional Asynchronous Ratcheted Key Agreement with Linear Complexity*

F. Betül Durak[1,2] and Serge Vaudenay[1]
[1] Ecole Polytechnique Fédérale de Lausanne (EPFL)
Lausanne, Switzerland
[2] Robert Bosch LLC — Research and Technology Center
Pittsburgh PA, USA

Efficient Ratcheting: Almost-Optimal Guarantees for Secure Messaging

Daniel Jost, Ueli Maurer, and Marta Mularczyk*
Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland.
{dajost, maurer, mumarta}@inf.ethz.ch

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

A Unified and Composable Take on Ratcheting

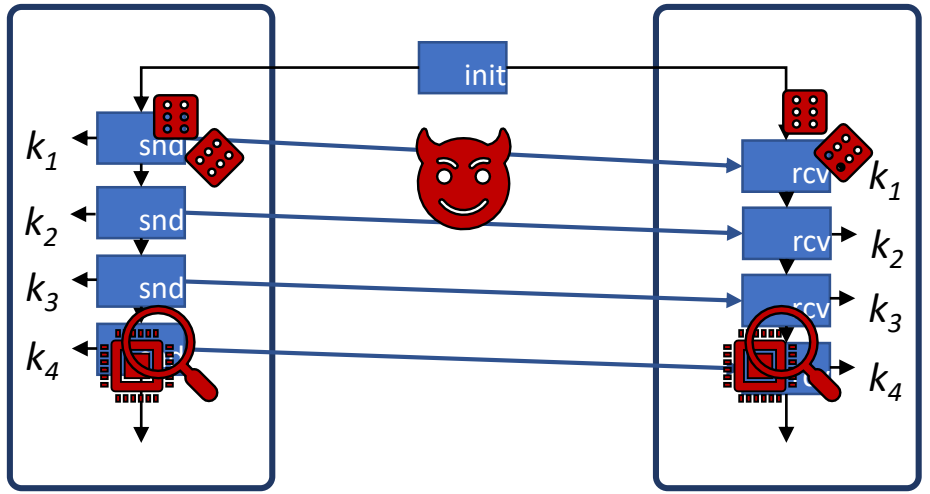
Daniel Jost, Ueli Maurer, and Marta Mularczyk*
Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland.
{dajost, maurer, mumarta}@inf.ethz.ch

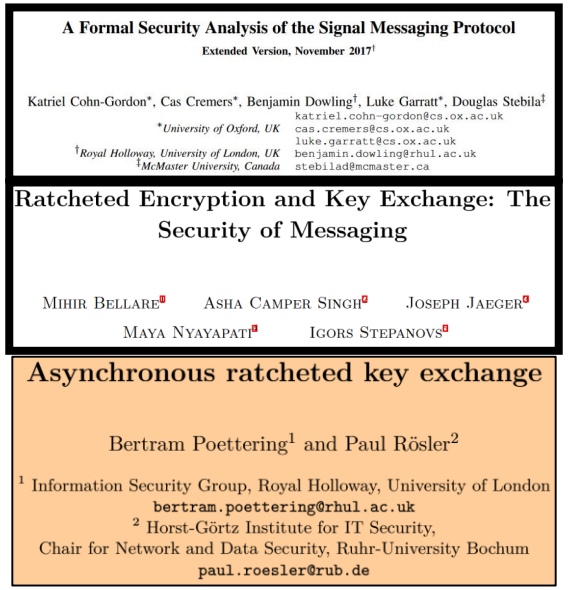
Beyond Security and Efficiency: On-Demand Ratcheting with Security Awareness

Andrea Caforio[1], F. Betül Durak[2], and Serge Vaudenay[1]
[1] Ecole Polytechnique Fédérale de Lausanne (EPFL)
Lausanne, Switzerland
[2] Robert Bosch LLC - Research and Technology Center
Pittsburgh PA, USA

Construction ↔ Security definition

- Havier tools are necessary for unidirectional RKE if
  - State exposures are not unnecessarily restricted
  - Bad randomness is considered
  - Recovery from attacks is required immediately




A Formal Security Analysis of the Signal Messaging Protocol
Extended Version, November 2017†

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

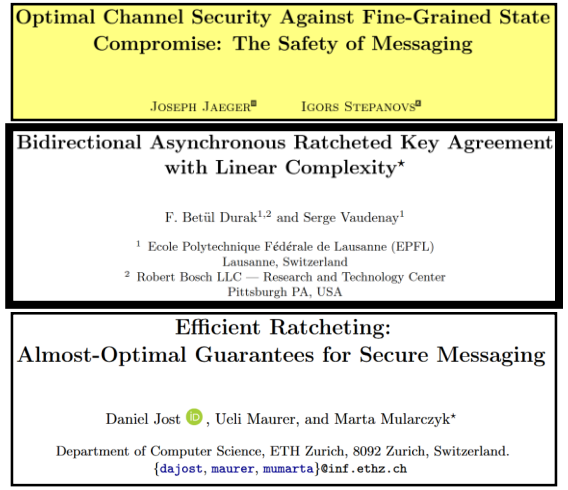
Ratcheted Encryption and Key Exchange: The Security of Messaging

Mihir Bellare — Asha Camper Singh — Joseph Jaeger
Maya Nyayapati — Igors Stepanovs

Asynchronous ratcheted key exchange

Bertram Poettering[1] and Paul Rösler[2]

[1] Information Security Group, Royal Holloway, University of London
bertram.poettering@rhul.ac.uk
[2] Horst-Görtz Institute for IT Security,
Chair for Network and Data Security, Ruhr-University Bochum
paul.roesler@rub.de


Optimal Channel Security Against Fine-Grained State Compromise: The Safety of Messaging

Joseph Jaeger — Igors Stepanovs

Bidirectional Asynchronous Ratcheted Key Agreement with Linear Complexity*

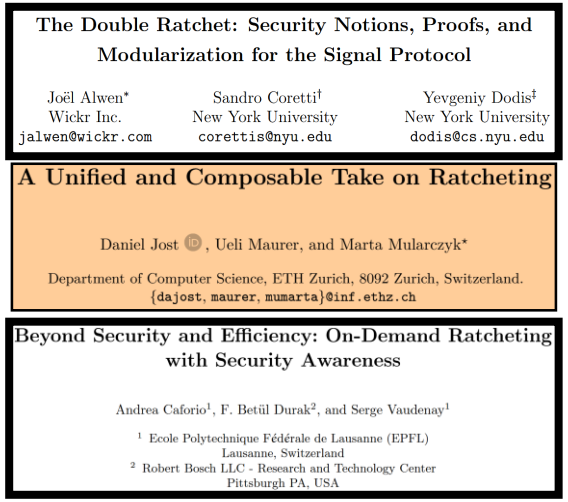
F. Betül Durak[1,2] and Serge Vaudenay[1]

[1] Ecole Polytechnique Fédérale de Lausanne (EPFL)
Lausanne, Switzerland
[2] Robert Bosch LLC — Research and Technology Center
Pittsburgh PA, USA

Efficient Ratcheting:
Almost-Optimal Guarantees for Secure Messaging

Daniel Jost, Ueli Maurer, and Marta Mularczyk*

Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland.
{dajost, maurer, mumarta}@inf.ethz.ch


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

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

A Unified and Composable Take on Ratcheting

Daniel Jost, Ueli Maurer, and Marta Mularczyk*

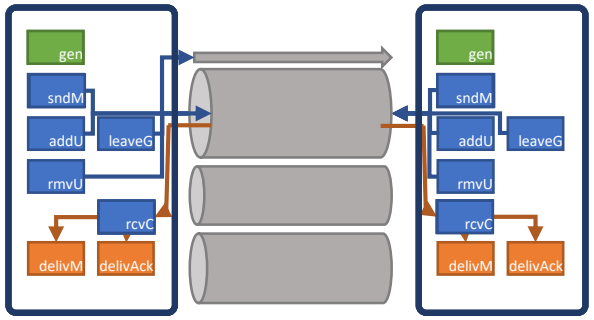
Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland.
{dajost, maurer, mumarta}@inf.ethz.ch

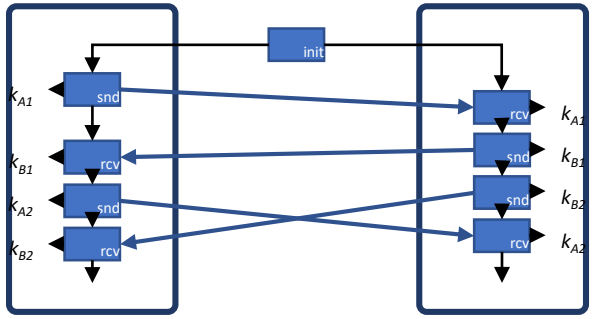
Beyond Security and Efficiency: On-Demand Ratcheting with Security Awareness

Andrea Caforio[1], F. Betül Durak[2], and Serge Vaudenay[1]

[1] Ecole Polytechnique Fédérale de Lausanne (EPFL)
Lausanne, Switzerland
[2] Robert Bosch LLC - Research and Technology Center
Pittsburgh PA, USA

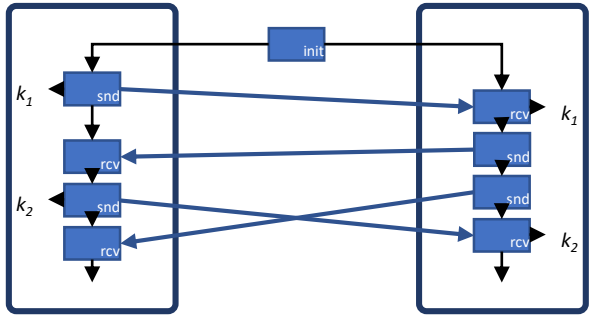
Syntax – Taming complexity



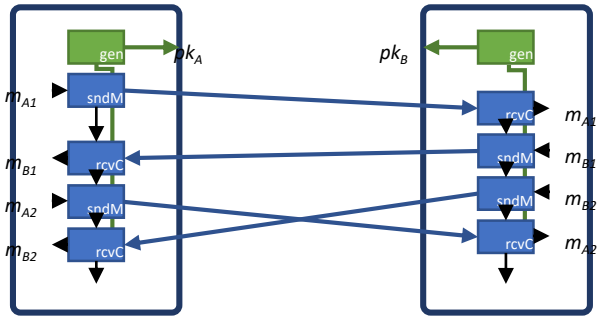


- Copy and merge

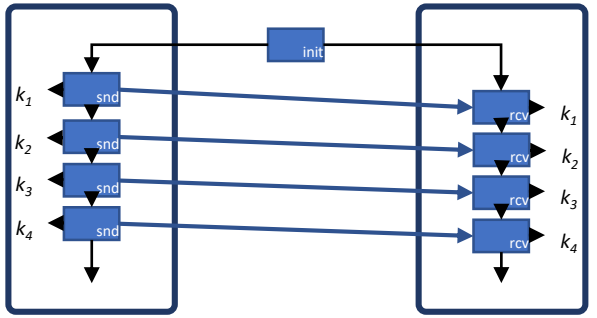
- Initialize with key exchange
- Add authenticated encryption

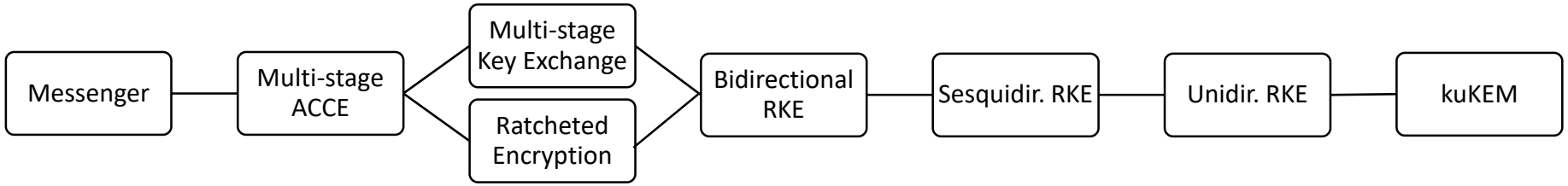


- **N copies and merges (under bad randomness)**



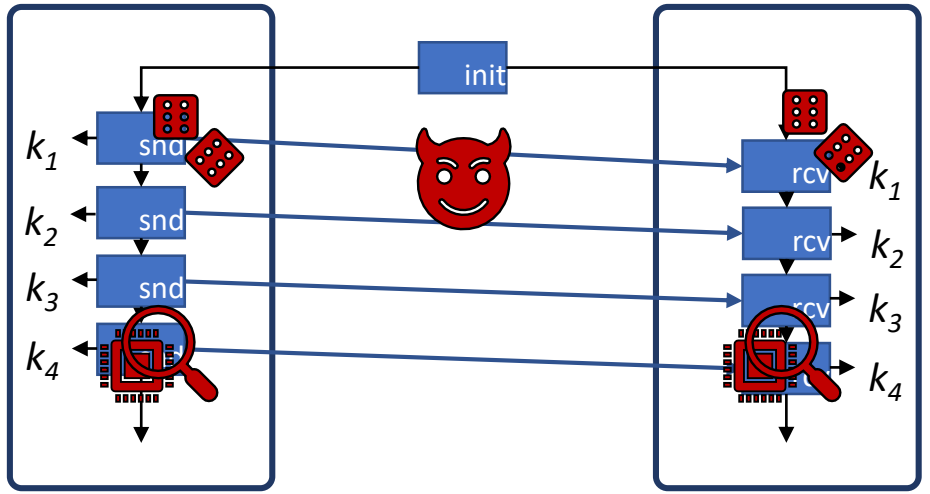
- N pair-wise channels
- Send acks





Construction ↔ Security definition

- Havier tools are necessary for unidirectional RKE if
  - State exposures are not unnecessarily restricted
  - Bad randomness is considered
  - Recovery from attacks is required immediately



- Open question: bad randomness / bidirectional settings?

ia.cr/2018/296

@roeslpa

A Formal Security Analysis of the Signal Messaging Protocol

Extended Version, November 2017

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

Ratcheted Encryption and Key Exchange: The Security of Messaging

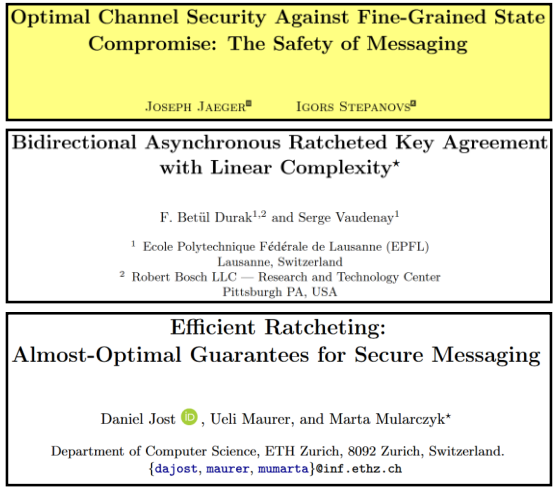
Mihir Bellare, Asha Camper Singh, Joseph Jaeger, Maya Nyayapati, Igors Stepanovs

Asynchronous ratcheted key exchange

Bertram Poettering[1] and Paul Rösler[2]

[1] Information Security Group, Royal Holloway, University of London
bertram.poettering@rhul.ac.uk

[2] Horst-Görtz Institute for IT Security,
Chair for Network and Data Security, Ruhr-University Bochum
paul.roesler@rub.de



Optimal Channel Security Against Fine-Grained State Compromise: The Safety of Messaging

Joseph Jaeger, Igors Stepanovs

Bidirectional Asynchronous Ratcheted Key Agreement with Linear Complexity*

F. Betül Durak[1,2] and Serge Vaudenay[1]

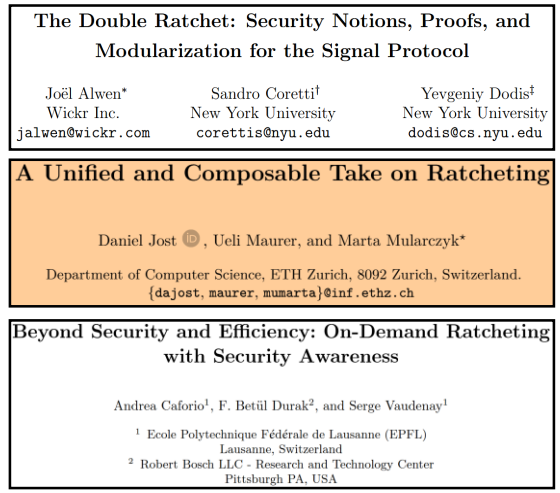
[1] Ecole Polytechnique Fédérale de Lausanne (EPFL)
Lausanne, Switzerland

[2] Robert Bosch LLC — Research and Technology Center
Pittsburgh PA, USA

Efficient Ratcheting:
Almost-Optimal Guarantees for Secure Messaging

Daniel Jost, Ueli Maurer, and Marta Mularczyk*

Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland.
{dajost, maurer, mumarta}@inf.ethz.ch



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

A Unified and Composable Take on Ratcheting

Daniel Jost, Ueli Maurer, and Marta Mularczyk*

Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland.
{dajost, maurer, mumarta}@inf.ethz.ch

Beyond Security and Efficiency: On-Demand Ratcheting with Security Awareness

Andrea Caforio[1], F. Betül Durak[2], and Serge Vaudenay[1]

[1] Ecole Polytechnique Fédérale de Lausanne (EPFL)
Lausanne, Switzerland

[2] Robert Bosch LLC - Research and Technology Center
Pittsburgh PA, USA