MARSHAL: Messaging with Asynchronous Ratchets and Signatures for faster HeALing

Olivier Blazy[1] Pierre-Alain Fouque[2] Thibaut Jacques[2,3,4] Pascal Lafourcade[5]
Cristina Onete[4] Léo Robert[5]

[1]LIX, CNRS, INRIA, École Polytechnique, Institut Polytechnique de Paris, France

[2]IRISA, Université Rennes 1, France

[3]Orange Labs, Rennes, France

[4]XLIM, Université de Limoges, France

[5]Université Clermont-Auvergne, CNRS, Mines de Saint-Étienne, LIMOS

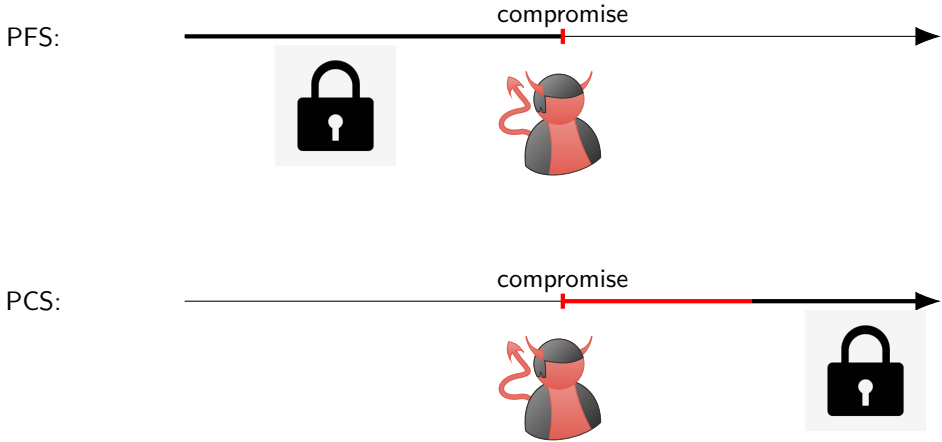
April 25 - April 29, 2022

SAC2022

Asynchronous Messaging Protocols

- Asynchronicity
- Mutual authentication
- Perfect Forward Secrecy (PFS)
- **Post-Compromise Security** (PCS)
- ...

PFS [1] and PCS [2]



[1] Christoph G Günther (1990). "An Identity-Based Key-Exchange Protocol". In: *Advances in Cryptology — EUROCRYPT '89*

[2] Katriel Cohn-Gordon, Cas J. F. Cremers, and Luke Garratt (2016). "On Post-compromise Security". In: *CSF*

Outline

Stage Definition

Chain 1
1. Hello
2. How are you?

⋮

Chain 2
1. Good, and you?

⋮

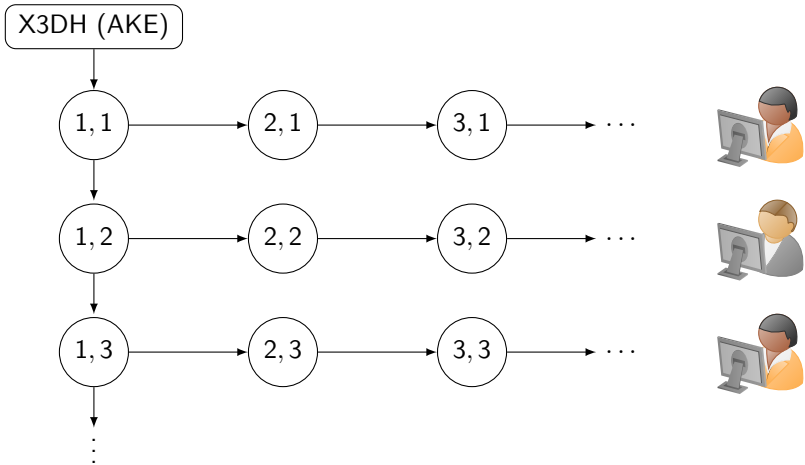
Chain 3
1. Great!

⋮

Stage $(1,1)$: "Hello"
Stage $(2,1)$: "How are you? "
Stage $(1,2)$: "Good, and you? "

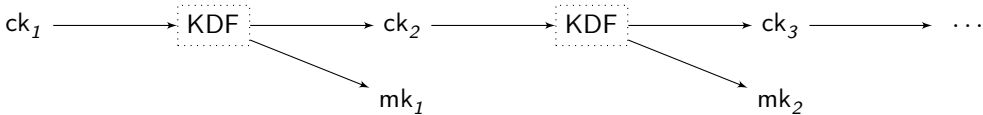
Stage (x,y): x^{th} message of chain y

Stage flow in Signal

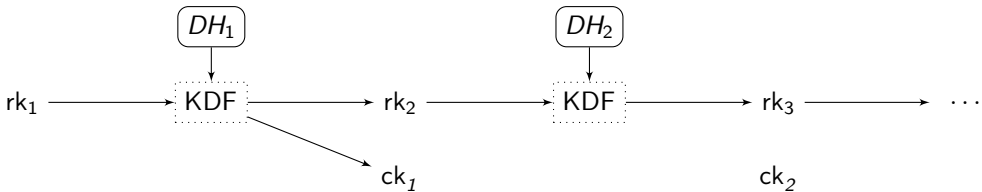


Ratchet Algorithms

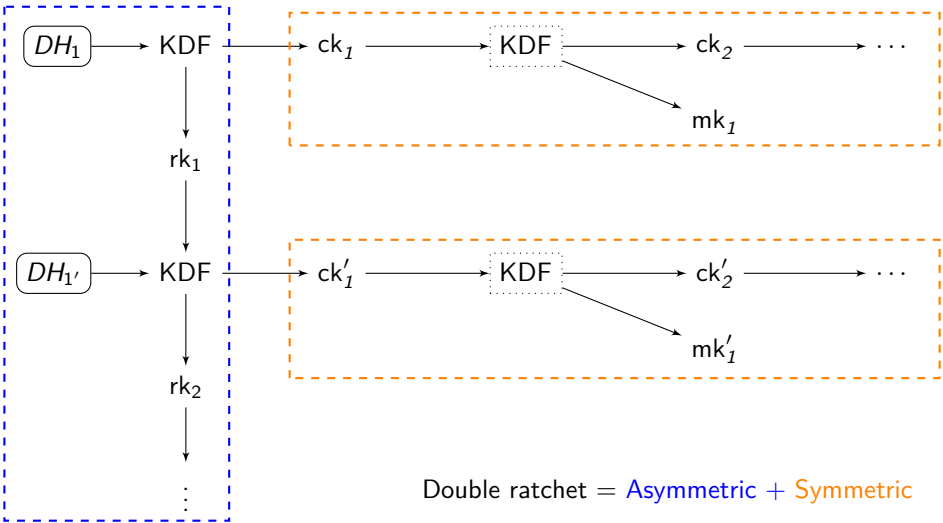
Symmetric ratchet: PFS



Asymmetric ratchet: PCS

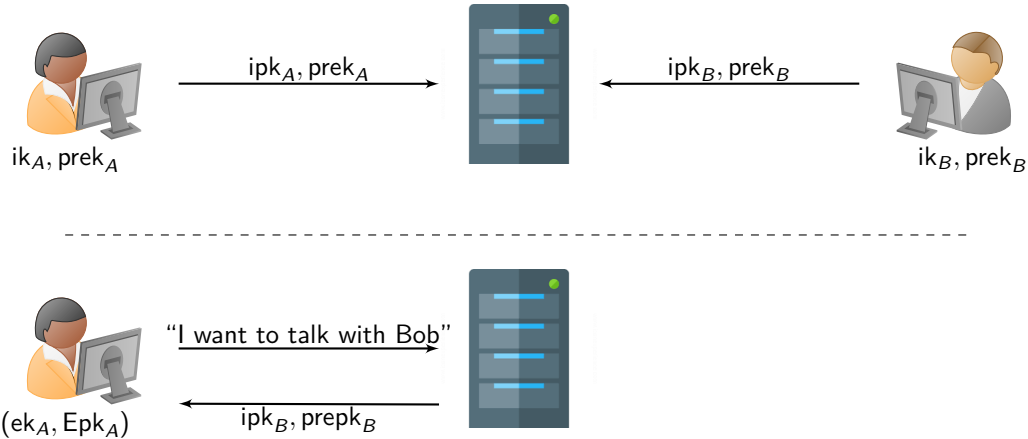


Double ratchet algorithm



Double ratchet = Asymmetric + Symmetric

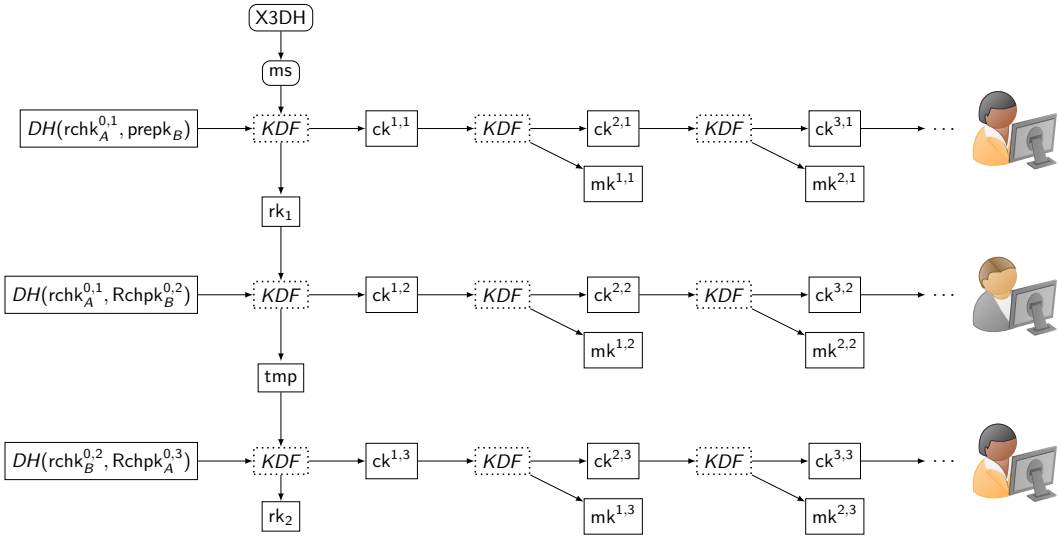
Registration - Setup



X3DH:

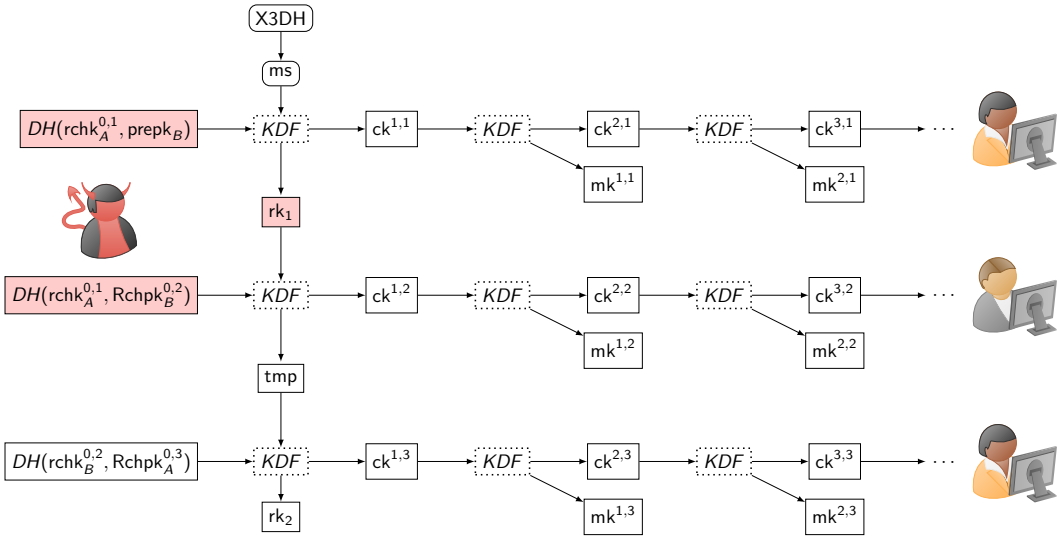
$$\mathsf{ms} := (\mathsf{prepk}_B)^{\mathsf{ik}_A} || (\mathsf{ipk}_B)^{\mathsf{ek}_A} || (\mathsf{prepk}_B)^{\mathsf{ek}_A}$$

Key Schedule of Signal



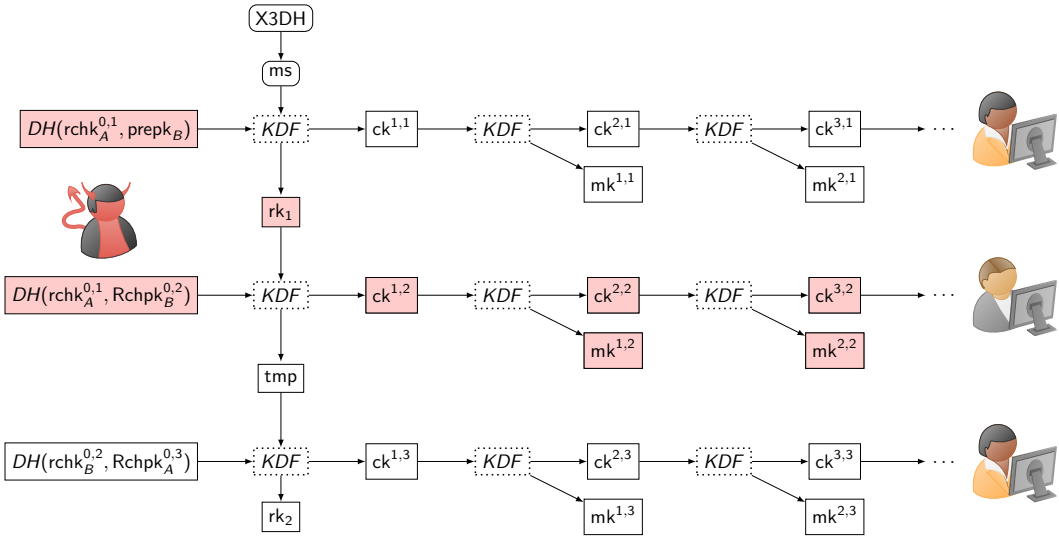
Passive attack

Keys revealed: $\mathrm{rchk}_A^{0,1}$ and rk_1



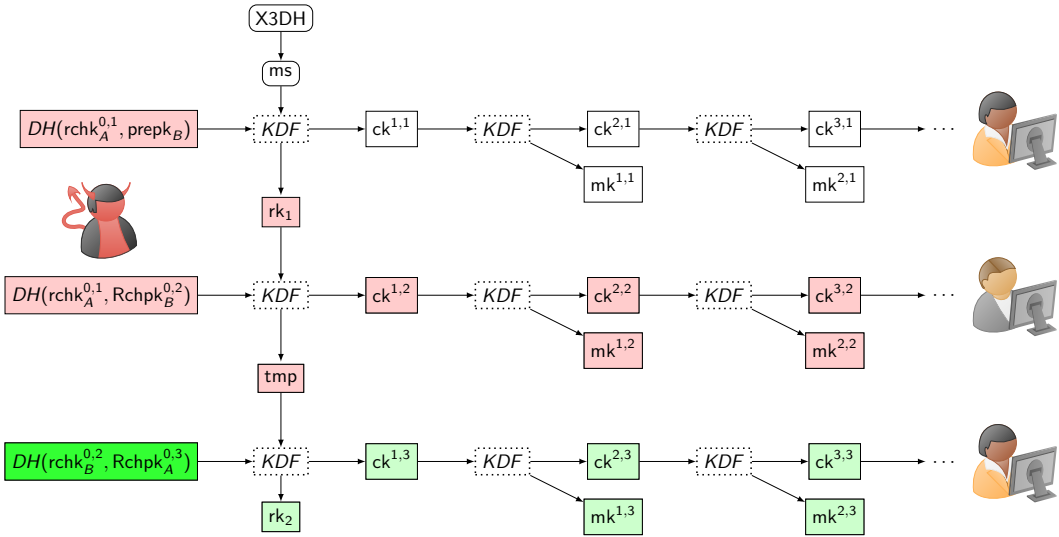
Passive attack

Keys revealed: $\mathrm{rchk}_A^{0,1}$ and rk_1



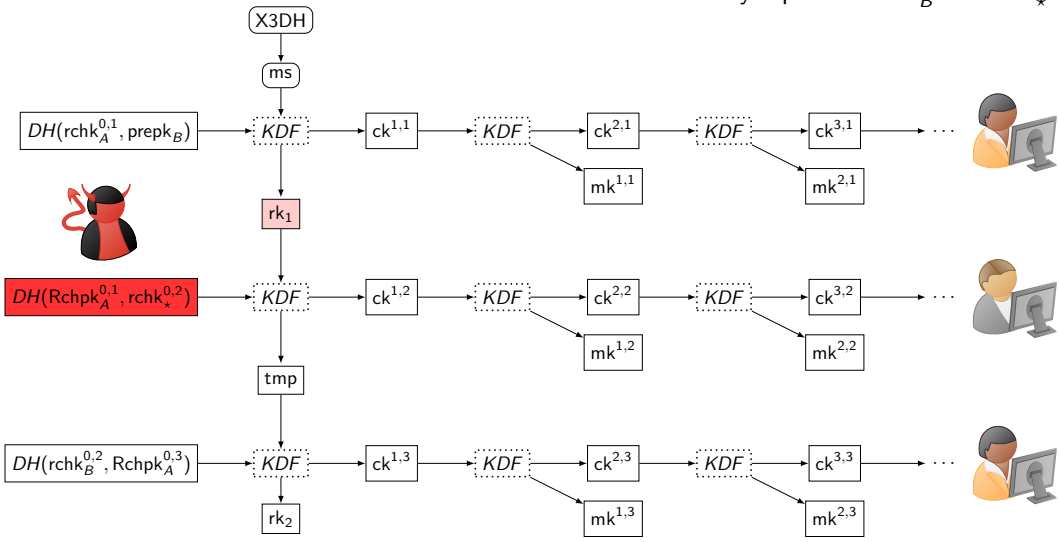
Passive attack

Keys revealed: $\mathrm{rchk}_A^{0,1}$ and rk_1

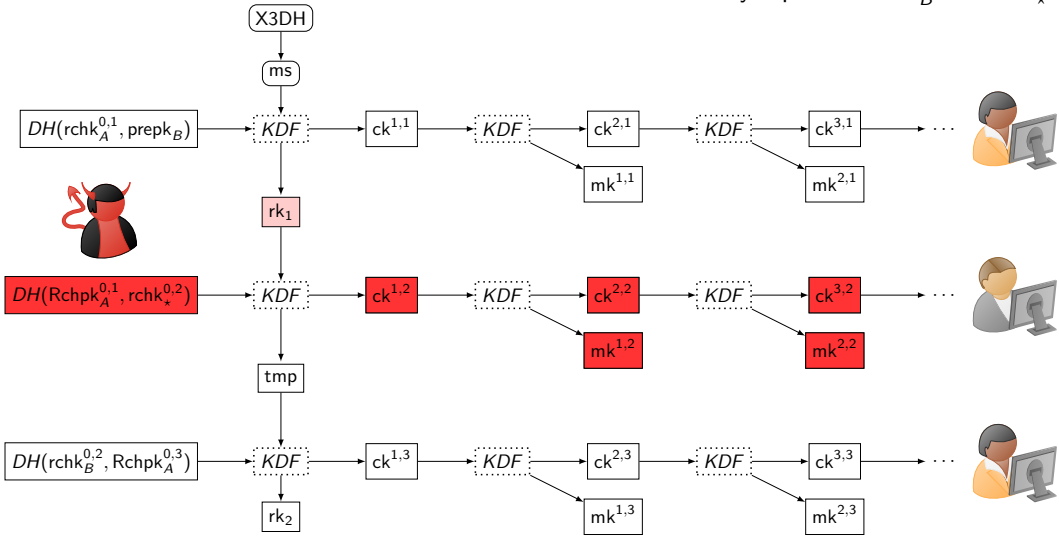


Active attack

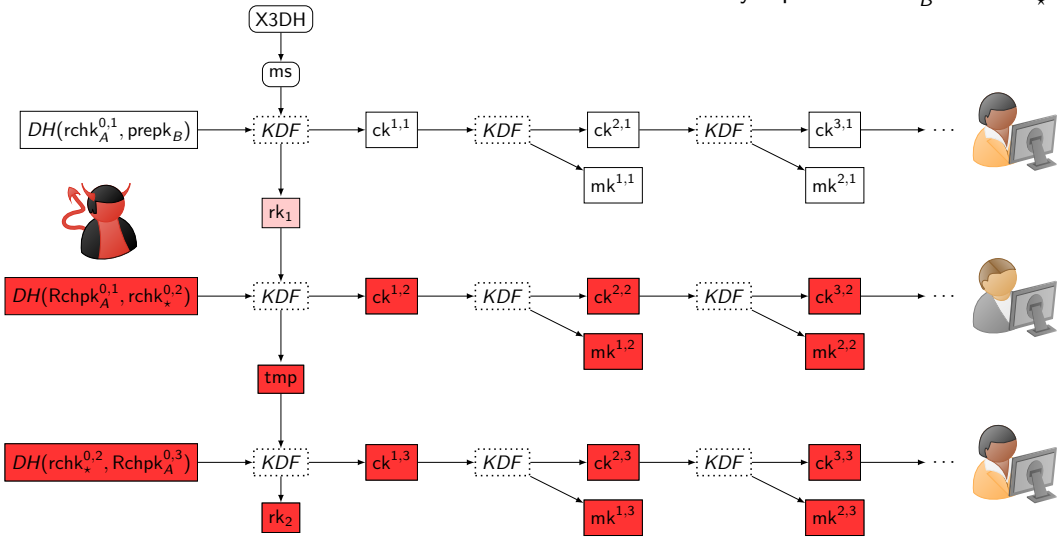
Key revealed: rk_1
Key replaced: $\mathrm{rchk}_B^{0,2} \rightarrow \mathrm{rchk}_\star^{0,2}$



Active attack



Active attack



Description of Signal

Example of attacks

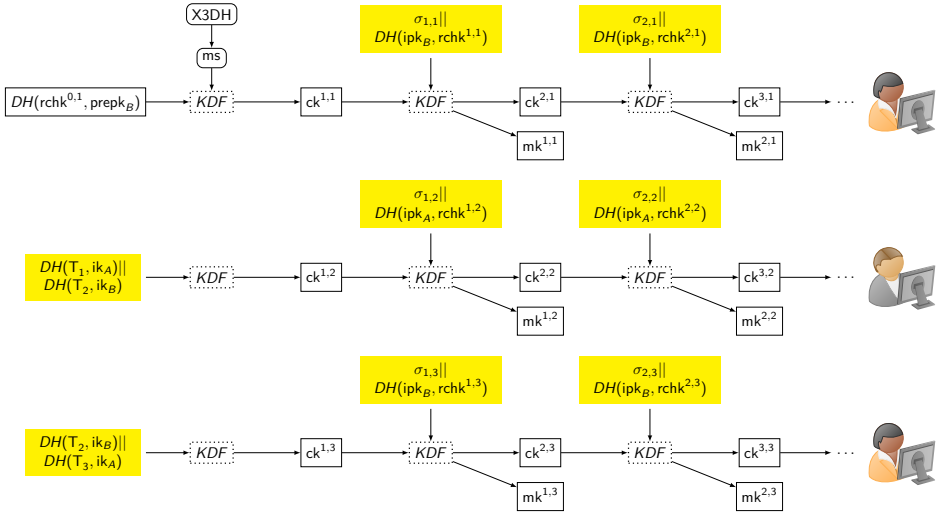
MARSHAL **protocol**

Security Analysis

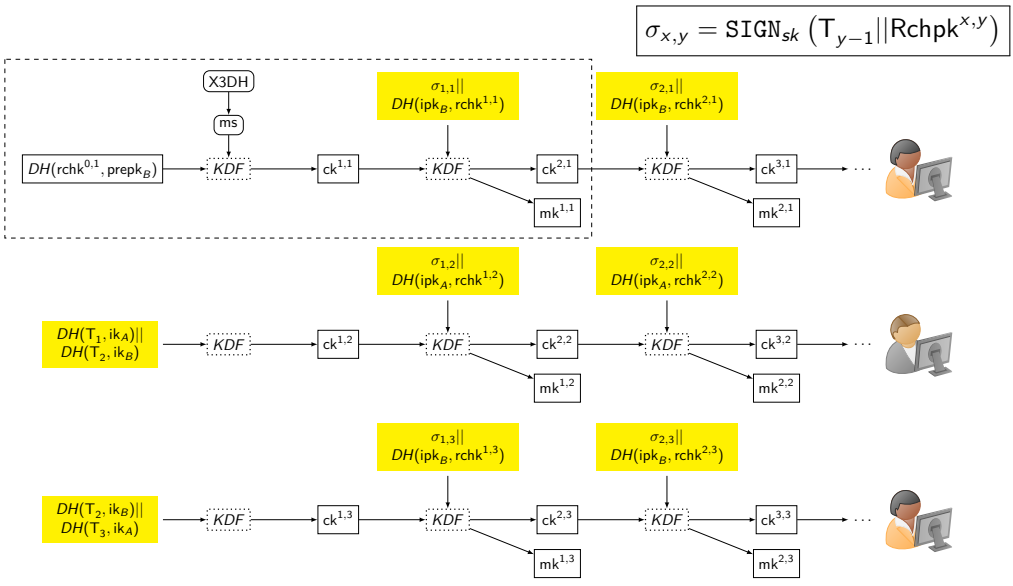
Implementation

MARSHAL key schedule

$$\sigma_{x,y} = \mathtt{SIGN}_{sk}\left(\mathsf{T}_{y-1} || \mathsf{Rchpk}^{x,y}\right)$$



MARSHAL key schedule



MARSHAL Registration and 1st message

Alice $(\mathsf{ik}_A, \mathsf{ipk}_B, \mathsf{prepk}_B, \mathsf{ephpk}_B, \mathsf{T}_0)$ | **Bob** $(\mathsf{ik}_B, \mathsf{ipk}_A, \mathsf{prek}_B, \mathsf{ephk}_B, \mathsf{T}_0)$

Session initialization: initiator Alice, responder Bob.

$\mathsf{ek}_A, \mathsf{rchk}^{0,1}, \mathsf{t}_1, \mathsf{rchk}^{1,1} \xleftarrow{\$} \mathbb{Z}_q$;

$\mathsf{T}_1 = g^{t_1}$; $\mathsf{Epk}_A = g^{\mathsf{ek}_A}$;

$\mathsf{Rchpk}^{0,1} = g^{\mathsf{rchk}^{0,1}}$; $\mathsf{Rchpk}^{1,1} = g^{\mathsf{rchk}^{1,1}}$

$ms = \mathsf{prepk}_B^{\mathsf{ik}_A} || \mathsf{ipk}_B^{\mathsf{ek}_A} || \mathsf{prepk}_B^{\mathsf{ek}_A} || \mathsf{ephpk}_B{}^{\mathsf{ek}_A}$

$\mathsf{ck}^{1,1} = \mathsf{HKDF}(\mathsf{prepk}_B^{\mathsf{rchk}^{0,1}} || ms)$

$(\mathsf{ck}^{2,1}, \mathsf{mk}^{1,1}) = \mathsf{HKDF}(\mathsf{ck}^{1,1}, \sigma_{1,1} || (\mathsf{ipk}_B)^{\mathsf{rchk}^{1,1}})$

First message: stage $(1,1)$, Alice is the sender, Bob, the receiver.

$AD_{y=1} = \mathsf{Epk}_A || \mathsf{ipk}_A || \mathsf{ipk}_B || \mathsf{prepk}_B || \mathsf{ephpk}_B || \mathsf{T}_0 || \mathsf{Rchpk}^{0,1} || \mathsf{T}_1$

$AD_{1,1} = (1,1) || \mathsf{Rchpk}^{1,1} || \sigma_{1,1}$

$c_{1,1} = \mathtt{AEAD.Enc}_{\mathsf{mk}^{1,1}}(M_{1,1}; AD_1 || AD_{1,1})$

$\xrightarrow{c_{1,1}, \mathtt{SIGN}_{sk_A}(c_{1,1}), pk_A, \mathtt{SIGN}_{\mathsf{ik}_A}(pk_A)}$

Verify signature on pk_A and $\sigma_{1,1}$

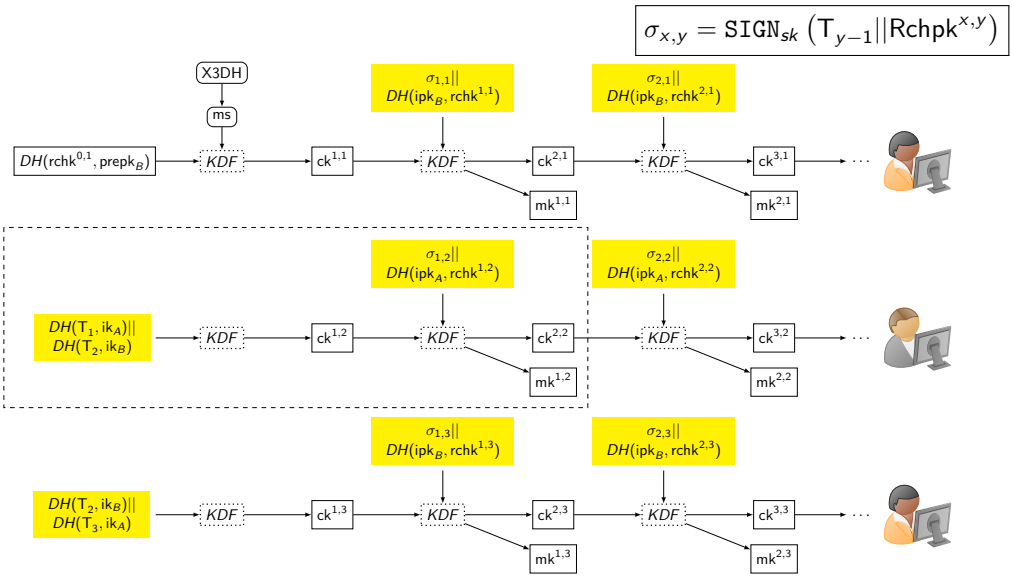
$ms = \mathsf{ipk}_A^{\mathsf{prek}_B} || \mathsf{Epk}_A^{\mathsf{ik}_B} || \mathsf{Epk}_A^{\mathsf{prek}_B} || \mathsf{Epk}_A^{\mathsf{ephk}_B}$

$\mathsf{ck}^{1,1} = \mathsf{HKDF}((\mathsf{Rchpk}^{0,1})^{\mathsf{prek}_B} || ms)$

$(\mathsf{ck}^{2,1}, \mathsf{mk}^{1,1}) = \mathsf{HKDF}(\mathsf{ck}^{1,1}, \sigma_{1,1} || (\mathsf{Rchpk}^{1,1})^{\mathsf{ik}_B})$

$M_{1,1} = \mathtt{AEAD.Dec}_{\mathsf{mk}^{1,1}}(c_{1,1})$.

MARSHAL Communication



MARSHAL Communication

ℓ^{th} message: stage $(\ell, 1)$, Alice is the sender, Bob, the receiver.

$\text{rchk}^{\ell,1} \xleftarrow{\$} \mathbb{Z}_q$, set $\text{Rchpk}^{\ell,1} = g^{\text{rchk}^{\ell,1}}$

$(\text{ck}^{\ell+1,1}, \text{mk}^{\ell,1}) = \text{HKDF}(\text{ck}^{\ell,1}, \sigma_{\ell,1} || \text{ipk}_B^{\text{rchk}^{\ell,1}})$

$AD_{\ell,1} = (\ell, 1) || \{\text{Rchpk}^{x,1}\}_{1 \le x \le \ell} || \sigma_{\ell,1}$

$c_{\ell,1} = \text{AEAD.Enc}_{\text{mk}^{\ell,1}}(M_{\ell,1}; AD_1 || AD_{\ell,1})$

$c_{\ell,1}, \text{SIGN}_{pk_A}(c_{\ell,1}), pk_A, \text{SIGN}_{\text{ik}_A}(pk_A)$ →

Verify leftover signatures

$(\text{ck}^{\ell+1,1}, \text{mk}^{\ell,1}) = \text{HKDF}(\text{ck}^{\ell,1}, \sigma_{\ell,1} || (\text{Rchpk}^{\ell,1})^{\text{ik}_B})$

$M_{\ell,1} = \text{AEAD.Dec}_{\text{mk}^{\ell,1}}(c_{\ell,1})$.

Switching speakers: Bob comes online and begins a new ratcheting chain.

$\text{t}_2, \text{rchk}^{1,2} \xleftarrow{\$} \mathbb{Z}_q$; $\text{T}_2 = g^{\text{t}_2}$, $\text{Rchpk}^{1,2} = g^{\text{rchk}^{1,2}}$

$\text{ck}^{1,2} = \text{HKDF}(\text{T}_1^{\text{ik}_B} || \text{ipk}_A^{\text{t}_2})$

$(\text{ck}^{2,2}, \text{mk}^{1,2}) = \text{HKDF}(\text{ck}^{1,2}, \sigma_{1,2} || (\text{ipk}_A)^{\text{rchk}^{1,2}})$

Bob's message, stage $(1, 2)$: Bob is the sender, Alice is the receiver.

$AD_{y=2} = \text{T}_2$

$AD_{1,2} = (1, 2) || \text{Rchpk}^{1,2} || \sigma_{1,2}$

$c_{1,2} = \text{AEAD.Enc}_{\text{mk}^{1,2}}(M_{1,2}; AD_2 || AD_{1,2})$

← $c_{1,2}, \text{SIGN}_{pk_B}(c_{1,2}), pk_B, \text{SIGN}_{\text{ik}_B}(pk_B)$

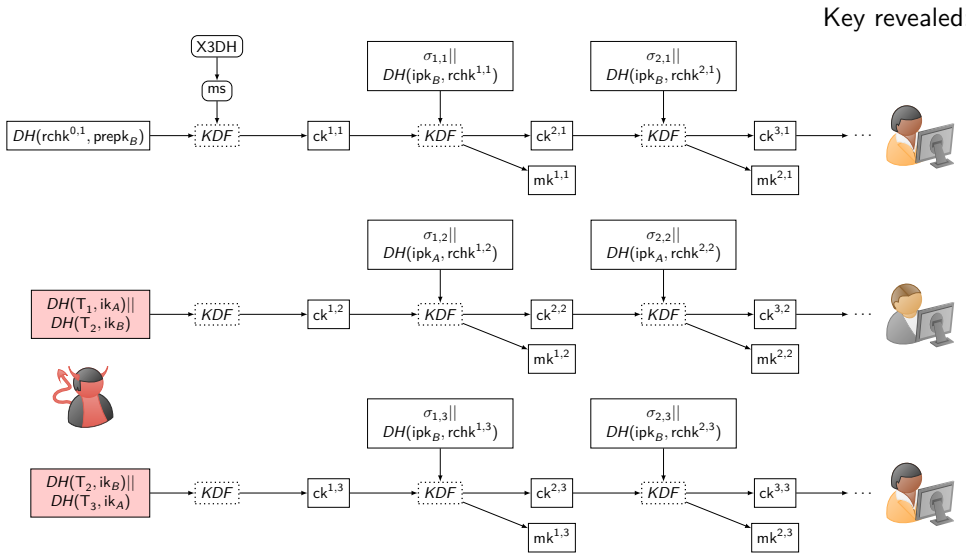
Verify signature on pk_B and $\sigma_{1,2}$

$\text{ck}^{1,2} = \text{HKDF}((\text{ipk}_B)^{\text{t}_1} || (\text{T}_2)^{\text{ik}_A})$

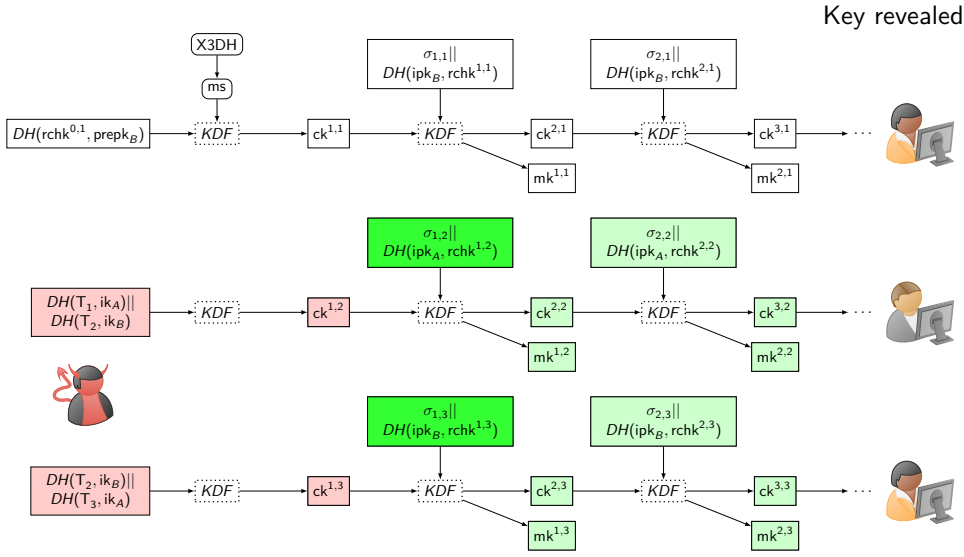
$(\text{ck}^{2,2}, \text{mk}^{1,2}) = \text{HKDF}(\text{ck}^{1,2}, \sigma_{1,2} || (\text{Rchpk}^{1,2})^{\text{ik}_A})$

$M_{1,2} = \text{AEAD.Dec}_{\text{mk}^{1,2}}(c_{1,2})$

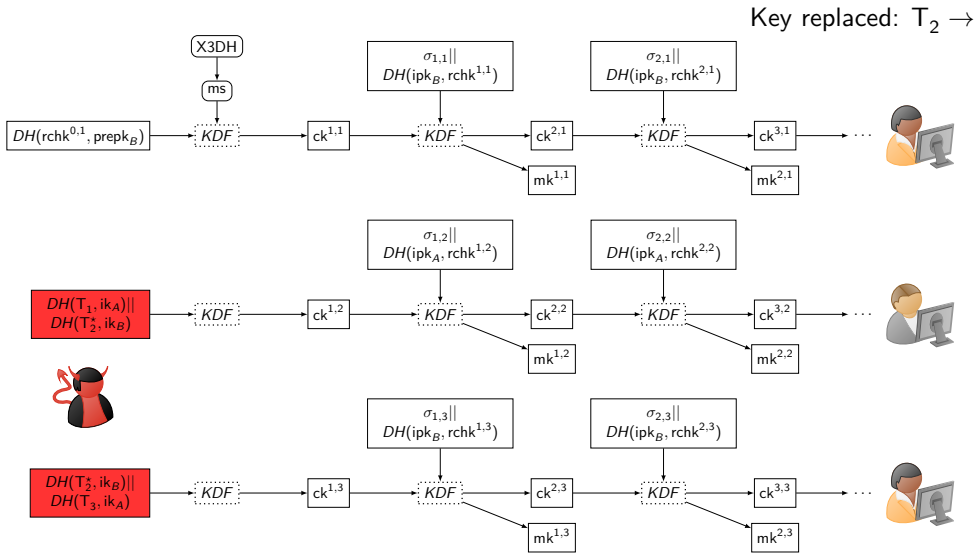
Passive attack



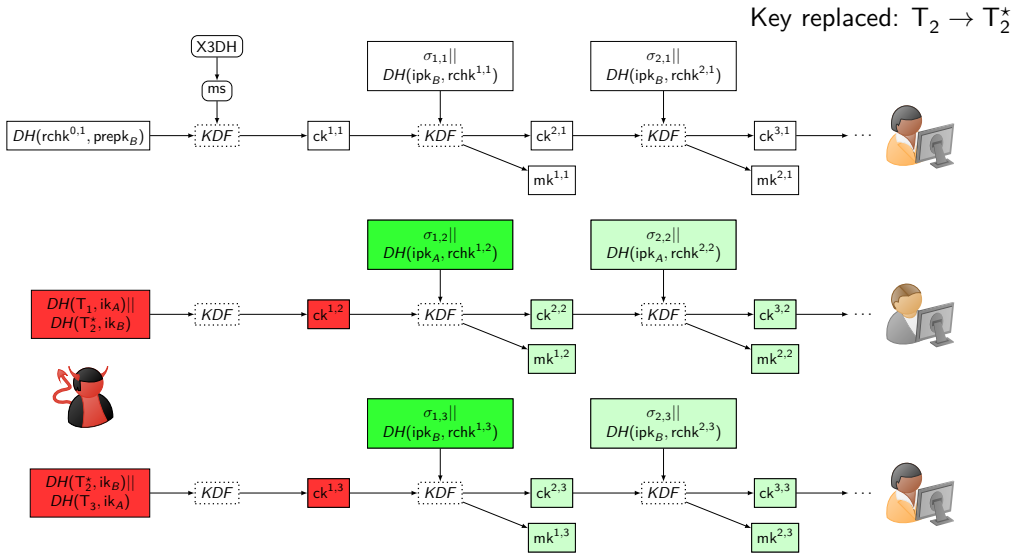
Passive attack



Active attack



Active attack



Description of Signal

Example of attacks

MARSHAL protocol

Security Analysis

Implementation

Model

Our model is close to Cohn-Gordon et al. 2017 and Blazy et al. 2019 but stronger:

- PCS is explicit: we design a indistinguishability game between $\mathcal{A}$ and $\mathcal{C}$;
- Trivial attacks are ruled out: MARSHAL is secure but not Signal;
- We add Message-Loss-Resilience (MLR) notion;

Security Proof

Theorem

If the GDH assumption holds, if the signature scheme is EUF-CMA-secure, then MARSHAL is PCS-AKE secure in the random oracle model (we model the two KDFs as $\mathcal{RO}_1, \mathcal{RO}_2$). In addition, MARSHAL is MLR-secure.

- The proof is not tight;
- No technical problem but trivial attacks are ruled out;
- Active adversary is handled.

Description of Signal

Example of attacks

MARSHAL protocol

Security Analysis

Implementation

Proof-of-concept

Implementation of MARSHAL in Java.
Results are the mean result (in ms) over 1000 executions:

Test	Signal	MARSHAL
Session Setup	3.856	6.924
Message $(1, y)$	1.284	5.082
Message (ℓ, y)	0.06	1.512

- Session setup: registration and encryption/decryption of first message;
- Message $(1, y)$: first message of a new chain;
- Message (ℓ, y): same speaker adding a new message.

Conclusion

We propose an improved Signal protocol toward PCS:

1. Asymmetric ratchet for each stage (passive $\mathcal{A}$);
2. Persistent authentication for each stage (active $\mathcal{A}$).
3. Overhead larger but the global evalutation remains practical.

Future works

- Improving the memory management;
- Design a multi-party MARSHAL;
- Propose a unified model to compare PCS protocols.

Thank you for your attention, questions ?


Blazy, Olivier et al. (2019). “SAID: Reshaping Signal into an Identity-Based Asynchronous Messaging Protocol with Authenticated Ratcheting”. In:


Cohn-Gordon, Katriel, Cas J. F. Cremers, and Luke Garratt (2016). “On Post-compromise Security”. In: *CSF*.


Cohn-Gordon, Katriel et al. (2017). “A Formal Security Analysis of the Signal Messaging Protocol”. In: *EuroS&P*.


Günther, Christoph G (1990). “An Identity-Based Key-Exchange Protocol”. In: *Advances in Cryptology — EUROCRYPT '89*. Ed. by Jean-Jacques Quisquater and Joos Vandewalle. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 29–37.