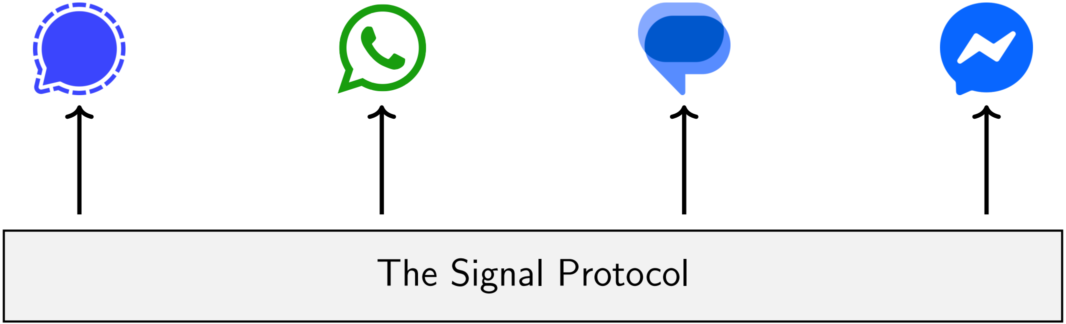
XHMQV: Better Efficiency and Stronger Security for Signal's Initial Handshake based on HMQV

Rune Fiedler[1] Felix Günther[2] Jiaxin Pan[3] Runzhi Zeng[3]

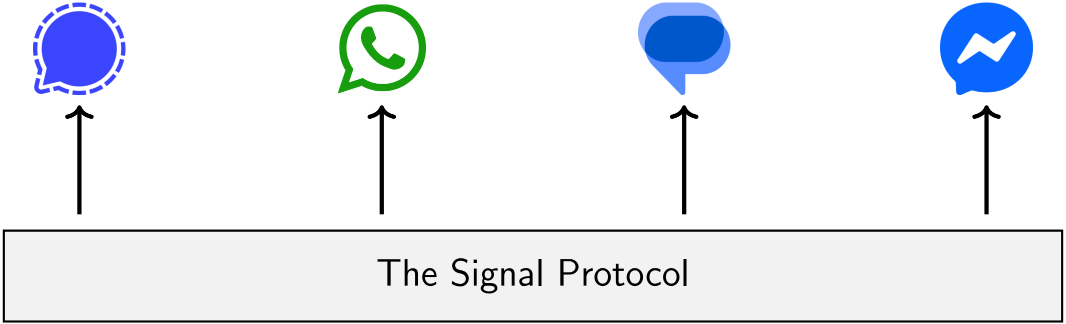
[1] TU Darmstadt, Germany
[2] IBM Research Europe – Zurich, Switzerland
[3] University of Kassel, Germany

The Signal Protocol



The Signal Protocol

The Signal Protocol



The Signal Protocol

Secure messaging – A very active area in the academic community

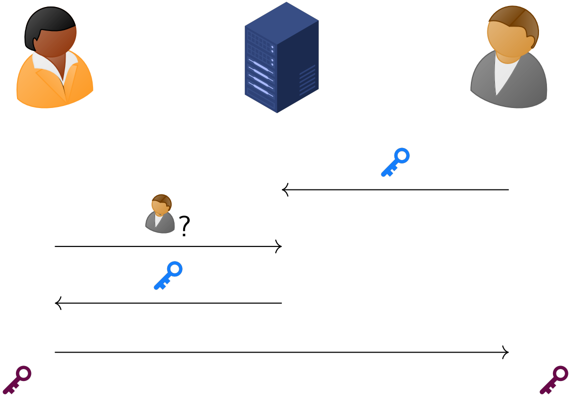
- Formal security analysis, e.g., [CCD$^+$20, CRT24]
- Extension to group messaging, e.g., [CCG$^+$18]
- Post-quantum extension (PQXDH), e.g., [BFG$^+$22, FG25]
- …

Our Contributions

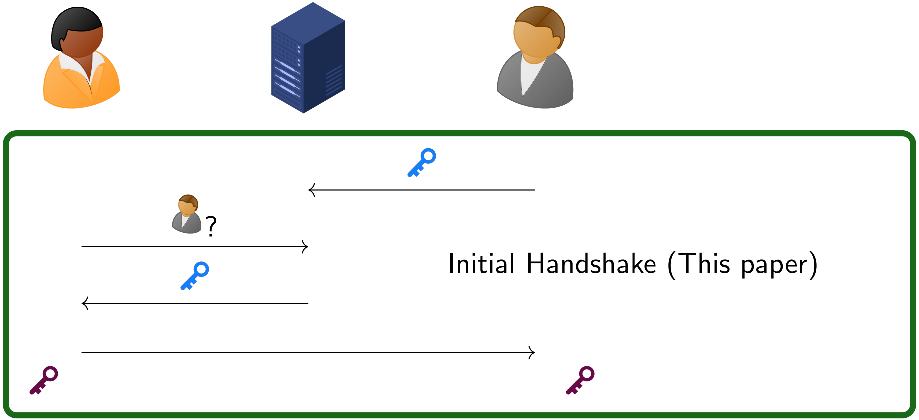
- XHMQV: A new initial handshake protocol that is
  - More efficient
  - Stronger “maximum-exposure” security, and
  - Proven in a more realistic security way (namely, being able to handle the key reuse issue)

  than X3DH (aka. Signal’s classical initial handshake).

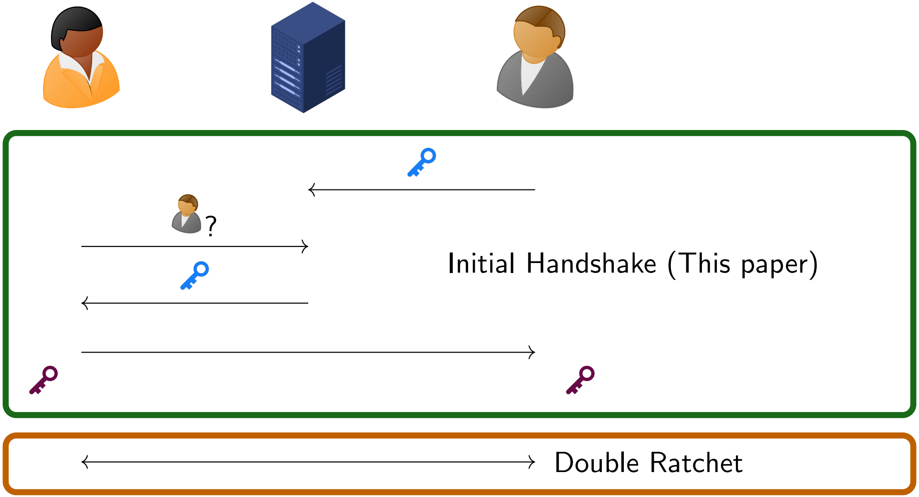
Signal: Asynchronous Authenticated Key Exchange



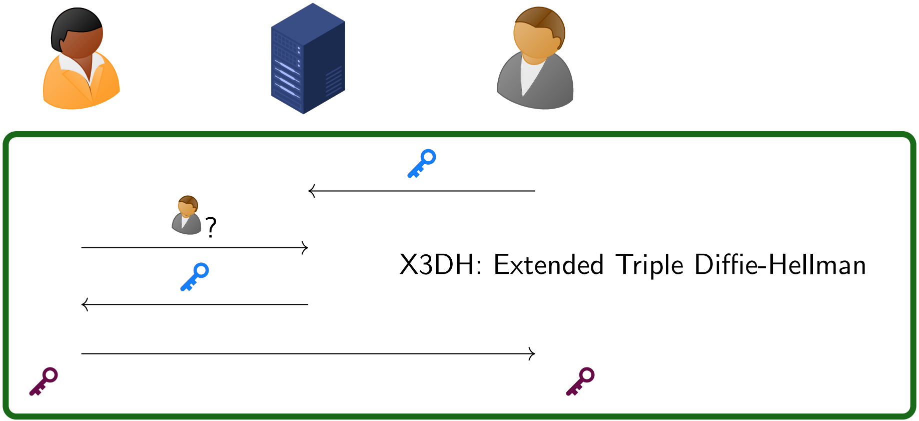
Signal: Asynchronous Authenticated Key Exchange



Signal: Asynchronous Authenticated Key Exchange



Signal: Asynchronous Authenticated Key Exchange



X3DH: Extended Triple Diffie-Hellman

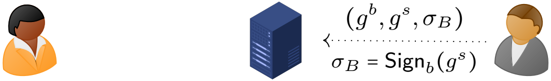
X3DH: Signal's Initial Handshake

long-term (a, g^a)

long-term (b, g^b)

semi-static (s, g^s)

X3DH: Signal's Initial Handshake



(g^b, g^s, σ_B)

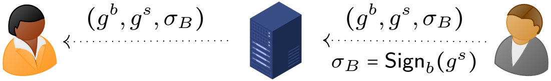
$\sigma_B = \mathsf{Sign}_b(g^s)$

long-term (a, g^a)

long-term (b, g^b)

semi-static (s, g^s)

X3DH: Signal's Initial Handshake

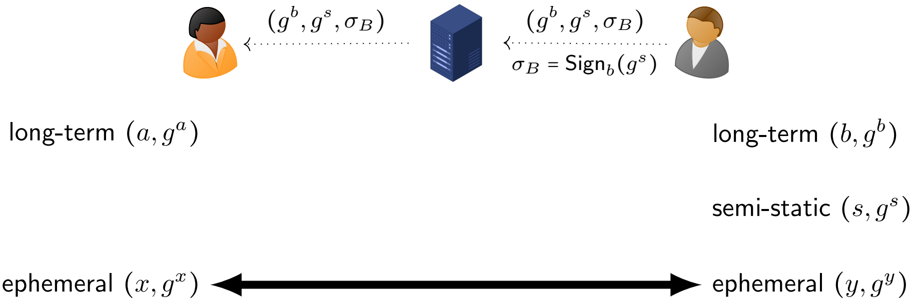


long-term (a, g^a)

long-term (b, g^b)

semi-static (s, g^s)

X3DH: Signal's Initial Handshake



(g^b, g^s, σ_B)

(g^b, g^s, σ_B)

$\sigma_B = \mathrm{Sign}_b(g^s)$

long-term (a, g^a)

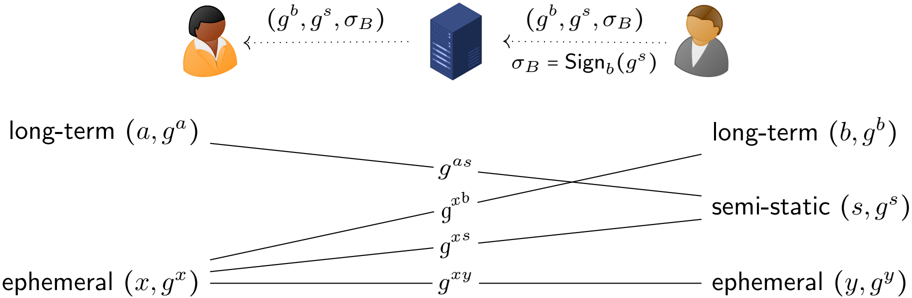
long-term (b, g^b)

semi-static (s, g^s)

ephemeral (x, g^x)

ephemeral (y, g^y)

X3DH: Signal's Initial Handshake



(g^b, g^s, σ_B)

(g^b, g^s, σ_B)

$\sigma_B = \mathsf{Sign}_b(g^s)$

long-term (a, g^a)

ephemeral (x, g^x)

g^{as}

g^{xb}

g^{xs}

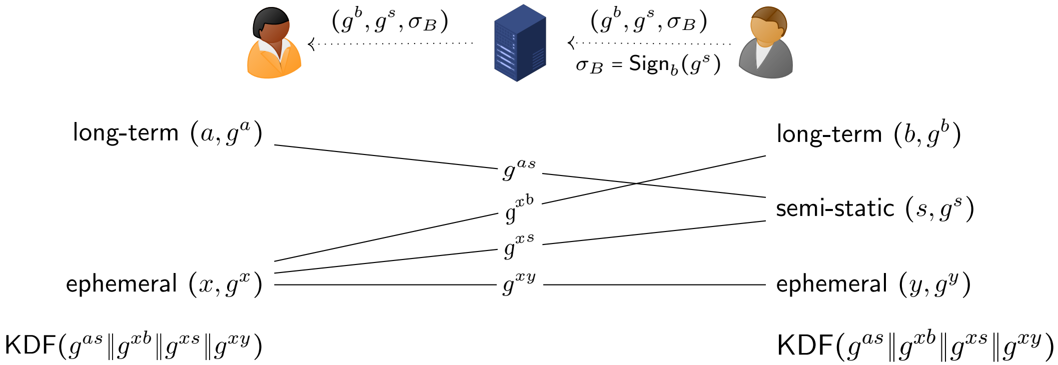
g^{xy}

long-term (b, g^b)

semi-static (s, g^s)

ephemeral (y, g^y)

X3DH: Signal's Initial Handshake



(g^b, g^s, σ_B)

(g^b, g^s, σ_B)

$\sigma_B = \mathsf{Sign}_b(g^s)$

long-term (a, g^a)

ephemeral (x, g^x)

g^{as}

g^{xb}

g^{xs}

g^{xy}

long-term (b, g^b)

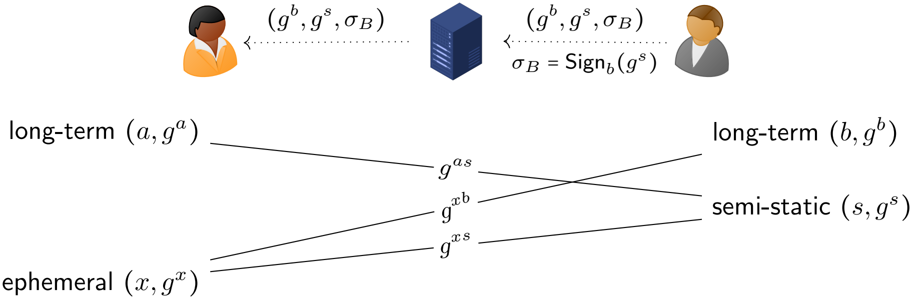
semi-static (s, g^s)

ephemeral (y, g^y)

$\mathsf{KDF}(g^{as} \| g^{xb} \| g^{xs} \| g^{xy})$

$\mathsf{KDF}(g^{as} \| g^{xb} \| g^{xs} \| g^{xy})$

X3DH: Signal's Initial Handshake (Reduced Mode)



(g^b, g^s, σ_B)

(g^b, g^s, σ_B)

$\sigma_B = \mathsf{Sign}_b(g^s)$

long-term (a, g^a)

long-term (b, g^b)

g^{as}

g^{xb}

g^{xs}

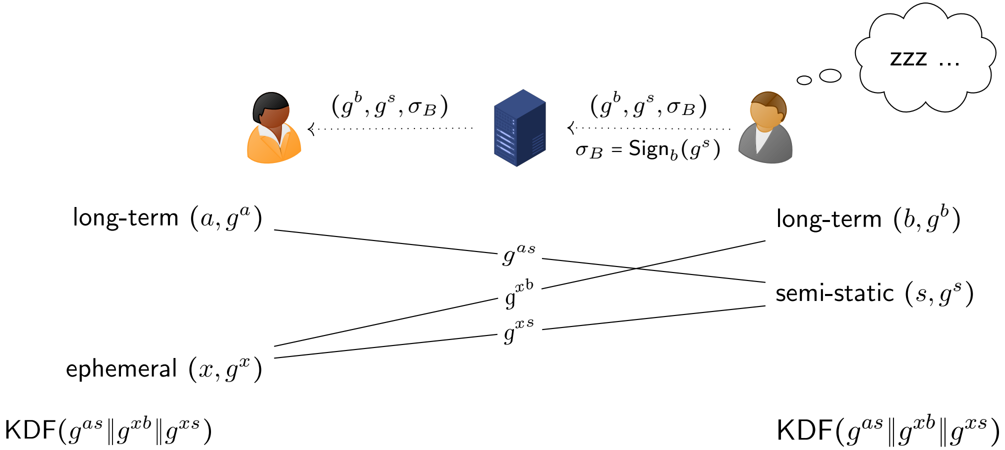
semi-static (s, g^s)

ephemeral (x, g^x)

$\mathsf{KDF}(g^{as} \| g^{xb} \| g^{xs})$

$\mathsf{KDF}(g^{as} \| g^{xb} \| g^{xs})$

X3DH: Signal's Initial Handshake (Reduced Mode)



zzz ...

(g^b, g^s, σ_B)

(g^b, g^s, σ_B)

$\sigma_B = \mathsf{Sign}_b(g^s)$

long-term (a, g^a)

long-term (b, g^b)

g^{as}

g^{xb}

g^{xs}

semi-static (s, g^s)

ephemeral (x, g^x)

$\mathsf{KDF}(g^{as} \| g^{xb} \| g^{xs})$

$\mathsf{KDF}(g^{as} \| g^{xb} \| g^{xs})$

Why X3DH?

- Asynchronous:
  - Bob does not need to be online

Why X3DH?

- Asynchronous:
  - Bob does not need to be online
- “Maximum-exposure” security:
  - Hedge against the maximum leakage of long-term, semi-static, and ephemeral secrets

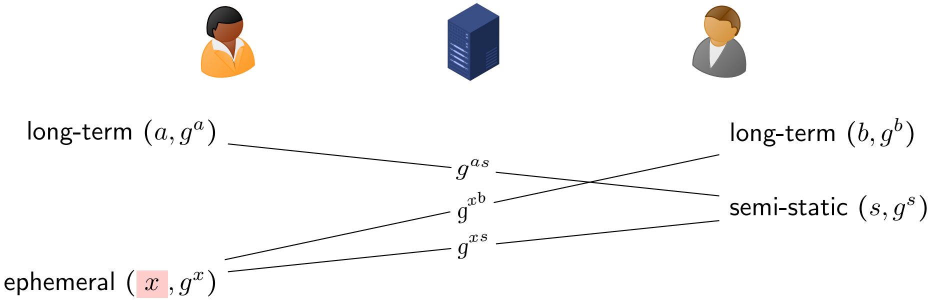
Why X3DH?

- Asynchronous:
  - Bob does not need to be online
- “Maximum-exposure” security:
  - Hedge against the maximum leakage of long-term, semi-static, and ephemeral secrets
- Deniability

Why X3DH?

- Asynchronous:
  - Bob does not need to be online
- **"Maximum-exposure" security:**
  - Hedge against the maximum leakage of long-term, semi-static, and ephemeral secrets
- Deniability

“Maximum-exposure” Security



long-term (a, g^{a})

ephemeral (x, g^{x})

g^{as}

g^{xb}

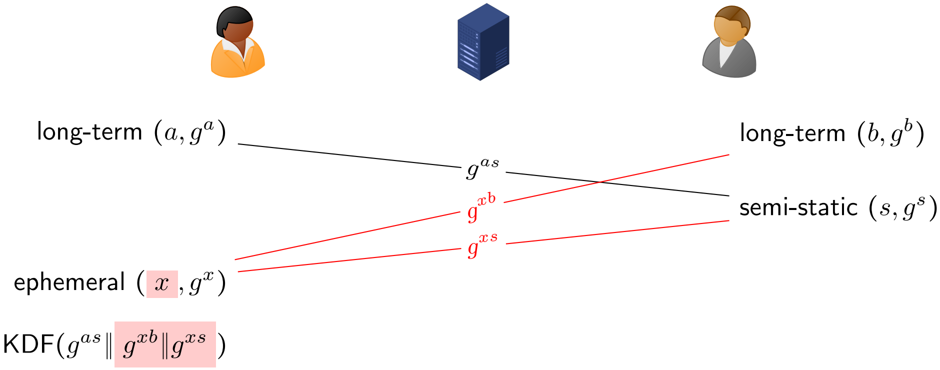
g^{xs}

long-term (b, g^{b})

semi-static (s, g^{s})

$\mathsf{KDF}(g^{as} \| g^{xb} \| g^{xs})$

“Maximum-exposure” Security



long-term (a, g^a)

long-term (b, g^b)

semi-static (s, g^s)

g^{as}

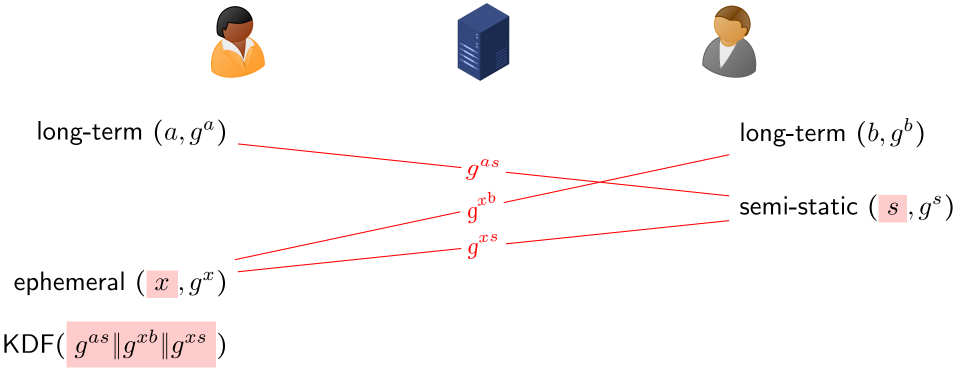
g^{xb}

g^{xs}

ephemeral (x, g^x)

$\mathsf{KDF}(g^{as} \| g^{xb} \| g^{xs})$

“Maximum-exposure” Security



long-term (a, g^a)

ephemeral (x, g^x)

KDF$(g^{as} \| g^{xb} \| g^{xs})$

g^{as}

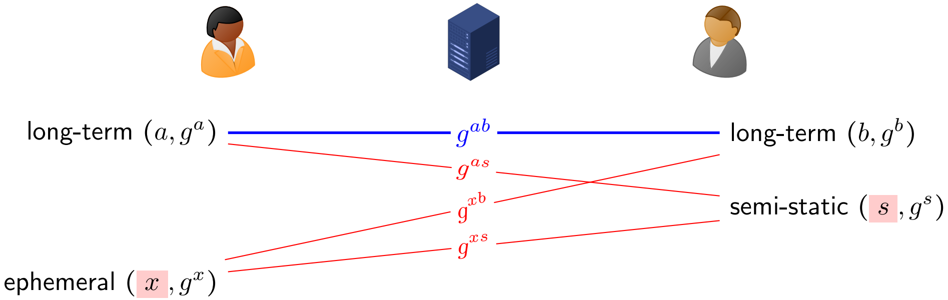
g^{xb}

g^{xs}

long-term (b, g^b)

semi-static (s, g^s)

A Solution



long-term (a, g^a)

g^{ab}

long-term (b, g^b)

g^{as}

semi-static (s, g^s)

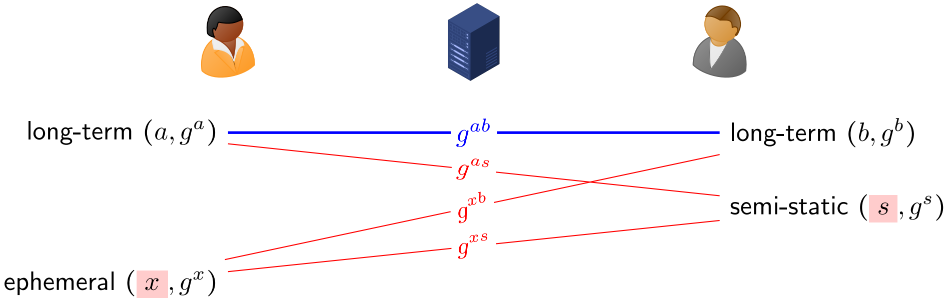
g^{xb}

g^{xs}

ephemeral (x, g^x)

KDF$(g^{as} \| g^{xb} \| g^{xs} \| g^{ab})$

A Solution



long-term (a, g^a)

g^{ab}

long-term (b, g^b)

g^{as}

g^{xb}

semi-static (s, g^s)

g^{xs}

ephemeral (x, g^x)

KDF($g^{as} \| g^{xb} \| g^{xs} \| g^{ab}$)

Already *efficiently* solved by HMQV [Kra05]?

HMQV [Kra05]

long-term (a, g^a)

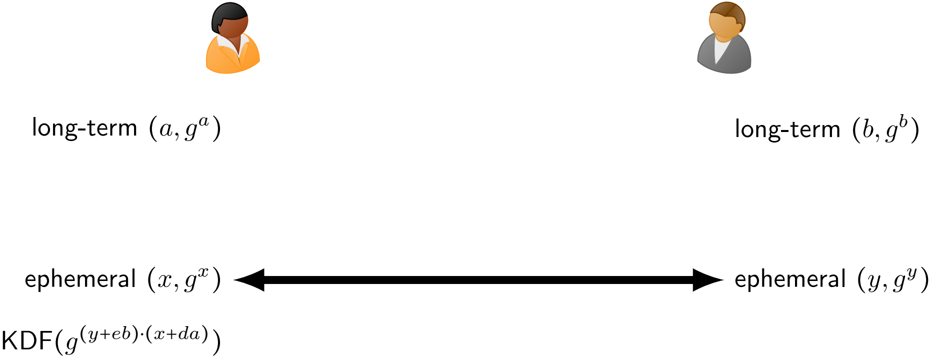
long-term (b, g^b)

ephemeral (x, g^x)

ephemeral (y, g^y)

[*] $e = H(g^y \| \text{Alice})$ and $d = H(g^x \| \text{Bob})$

HMQV [Kra05]



long-term (a, g^a)

long-term (b, g^b)

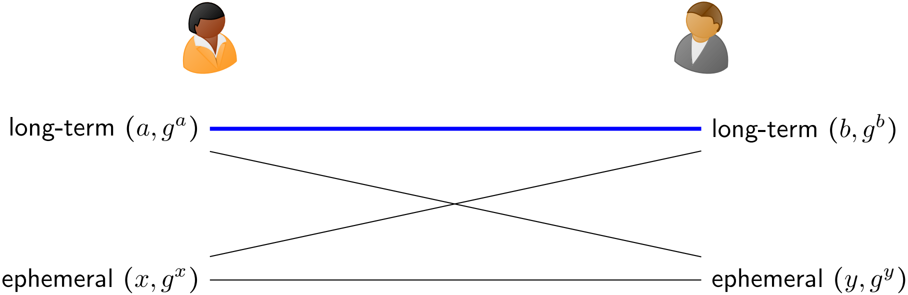
ephemeral (x, g^x)

ephemeral (y, g^y)

$\mathsf{KDF}(g^{(y+eb)\cdot(x+da)})$

*$e = H(g^y \| \mathsf{Alice})$ and $d = H(g^x \| \mathsf{Bob})$

HMQV [Kra05]



long-term (a, g^a)

long-term (b, g^b)

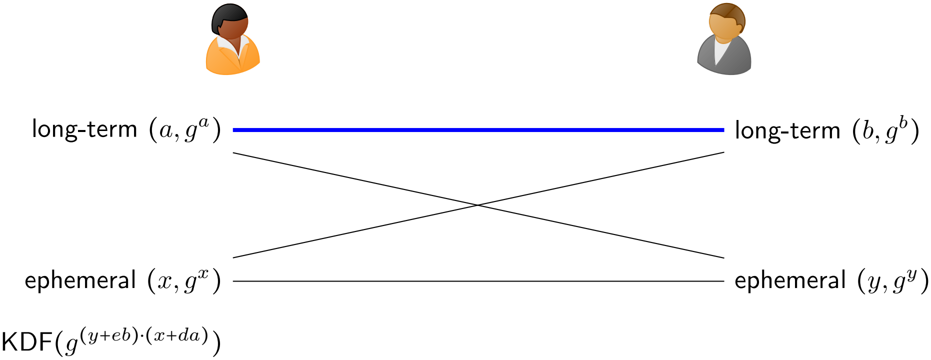
ephemeral (x, g^x)

ephemeral (y, g^y)

$\mathsf{KDF}(g^{(y+eb)\cdot(x+da)})$

[*] $e = H(g^y \| \text{Alice})$ and $d = H(g^x \| \text{Bob})$

HMQV [Kra05]



long-term (a, g^a)

long-term (b, g^b)

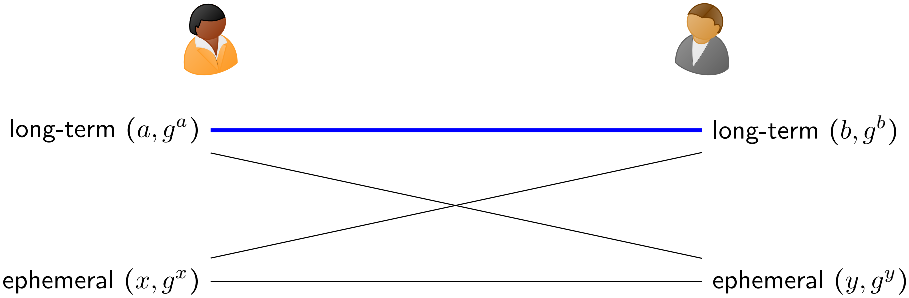
ephemeral (x, g^x)

ephemeral (y, g^y)

KDF$(g^{(y+eb)\cdot(x+da)})$

- More efficient (#Exp $=$ 2 for HMQV and 4 for X3DH) ✓
- Stronger "maximum-exposure" security ✓
- Not asynchronous ✗

HMQV [Kra05]



long-term (a, g^a)

long-term (b, g^b)

ephemeral (x, g^x)

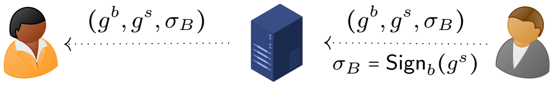
ephemeral (y, g^y)

KDF$(g^{(y+eb)\cdot(x+da)})$

- More efficient (#Exp = 2 for HMQV and 4 for X3DH) ✓
- Stronger “maximum-exposure” security ✓
- Not asynchronous ✗

  $\Rightarrow$ Introducing a semi-static key g^s

Overview of Our XHMQV



(g^b, g^s, σ_B)

(g^b, g^s, σ_B)

$\sigma_B = \mathsf{Sign}_b(g^s)$

long-term (a, g^a)

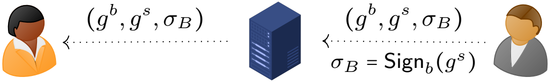
long-term (b, g^b)

semi-static (s, g^s)

ephemeral (x, g^x)

ephemeral (y, g^y)

Overview of Our XHMQV



(g^b, g^s, σ_B)

(g^b, g^s, σ_B)

$\sigma_B = \mathsf{Sign}_b(g^s)$

long-term (a, g^a)

long-term (b, g^b)

semi-static (s, g^s)

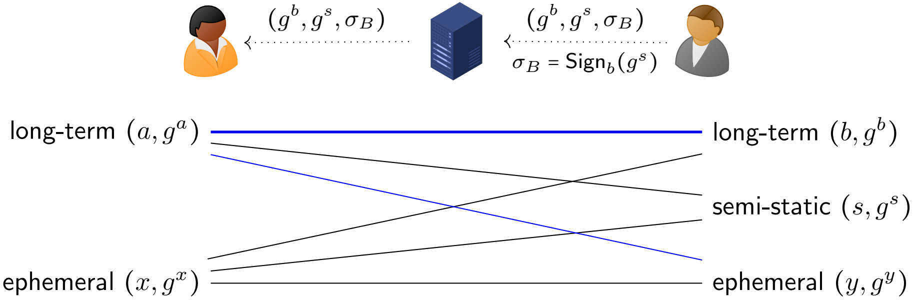
ephemeral (x, g^x)

ephemeral (y, g^y)

Ours: $\mathsf{KDF}(g^{(y+eb+e's)\cdot(x+da)})$

HMQV: $\mathsf{KDF}(g^{(y+eb)\cdot(x+da)})$

Overview of Our XHMQV



(g^b, g^s, σ_B)

(g^b, g^s, σ_B)

$\sigma_B = \mathsf{Sign}_b(g^s)$

long-term (a, g^a)

long-term (b, g^b)

semi-static (s, g^s)

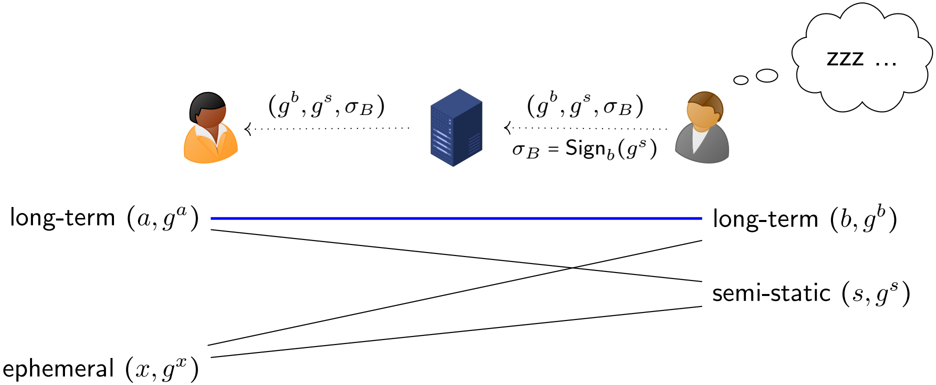
ephemeral (x, g^x)

ephemeral (y, g^y)

Ours: $\mathsf{KDF}(g^{(y+eb+e's)\cdot(x+da)})$

HMQV: $\mathsf{KDF}(g^{(y+eb)\cdot(x+da)})$

Overview of Our XHMQV (Reduced Mode)



zzz ...

(g^b, g^s, σ_B)

(g^b, g^s, σ_B)

$\sigma_B = \mathsf{Sign}_b(g^s)$

long-term (a, g^a)

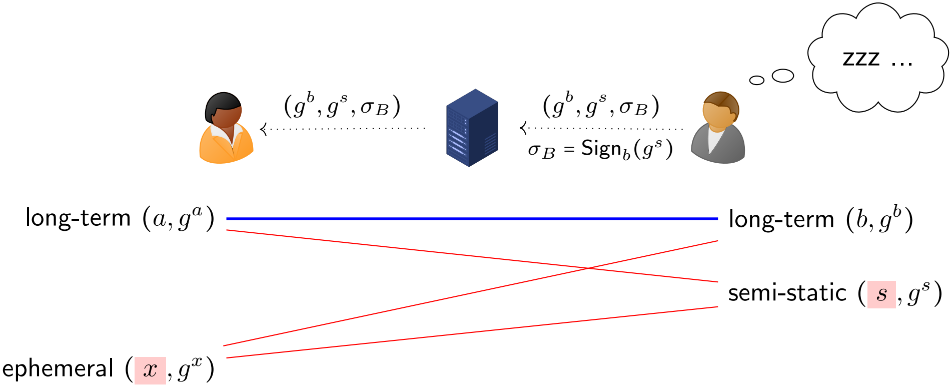
long-term (b, g^b)

semi-static (s, g^s)

ephemeral (x, g^x)

Ours: $\mathsf{KDF}(g^{(eb+e's)\cdot(x+da)})$

Overview of Our XHMQV (Reduced Mode)



zzz ...

(g^b, g^s, σ_B)

(g^b, g^s, σ_B)

$\sigma_B = \mathsf{Sign}_b(g^s)$

long-term (a, g^a)

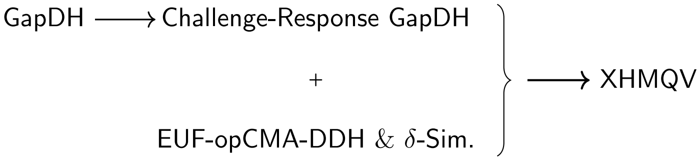
long-term (b, g^b)

semi-static (s, g^s)

ephemeral (x, g^x)

Ours: $\mathsf{KDF}(g^{(eb+e's)\cdot(x+da)})$

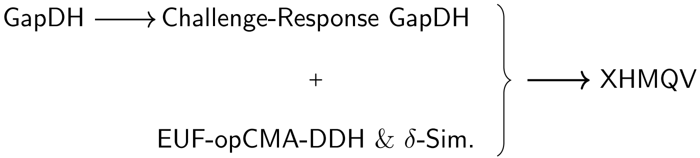
Security of XHMQV



$$\left.\begin{array}{r} \text{GapDH} \longrightarrow \text{Challenge-Response GapDH} \\ + \\ \text{EUF-opCMA-DDH} \ \& \ \delta\text{-Sim.} \end{array}\right\} \longrightarrow \text{XHMQV}$$

- Game-based Model as in [CCD+20, BFG+22, FG25]
- Random Oracles

Security of XHMQV


GapDH ⟶ Challenge-Response GapDH

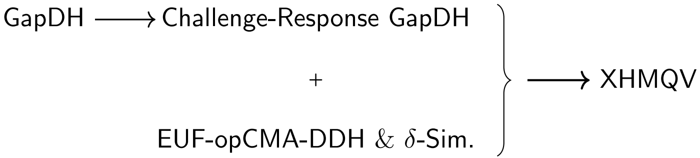
+

EUF-opCMA-DDH & δ-Sim.

⟶ XHMQV

- Game-based Model as in [CCD⁺20, BFG⁺22, FG25]
- Random Oracles
- Challenge-Response GapDH:
  - From the Modular Analysis of HMQV in [KPRR23]

Security of XHMQV



GapDH ⟶ Challenge-Response GapDH

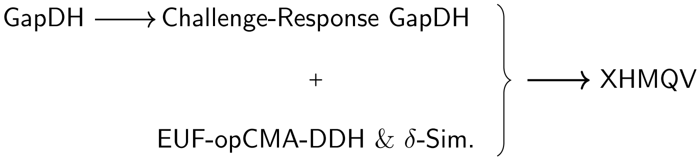
+

EUF-opCMA-DDH & δ-Sim.

⟶ XHMQV

- Game-based Model as in [CCD+20, BFG+22, FG25]
- Random Oracles
- Challenge-Response GapDH:
  - From the Modular Analysis of HMQV in [KPRR23]
- EUF-opCMA-DDH & δ-Simulatability
  - Handle the key reuse issue
  - Can be satisfied by (EC)DSA and Schnorr

Security of XHMQV



GapDH $\longrightarrow$ Challenge-Response GapDH

$+$

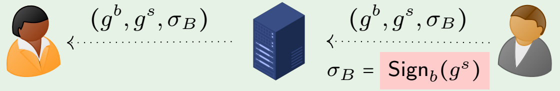
EUF-opCMA-DDH $\&$ δ-Sim.

$\longrightarrow$ XHMQV

- Game-based Model as in [CCD$^+$20, BFG$^+$22, FG25]
- Random Oracles
- Challenge-Response GapDH:
  - From the Modular Analysis of HMQV in [KPRR23]
- EUF-opCMA-DDH $\&$ δ-Simulatability
  - Handle the **key reuse issue**
  - Can be satisfied by (EC)DSA and Schnorr

Key Reuse Issue

In the Real Protocols (X3DH, XHMQV): Signing key = long-term key



(g^b, g^s, σ_B)

(g^b, g^s, σ_B)

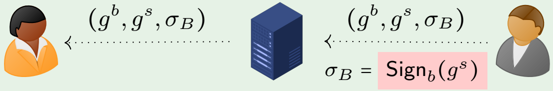
σ_B = $\text{Sign}_b(g^s)$

long-term (a, g^a)

long-term (b, g^b)

Key Reuse Issue

In the Real Protocols (X3DH, XHMQV): Signing key = long-term key



(g^b, g^s, σ_B)

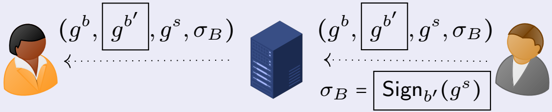
(g^b, g^s, σ_B)

$\sigma_B = \text{Sign}_b(g^s)$

long-term (a, g^a)

long-term (b, g^b)

In the Proofs (e.g. [CCD+20, FG25]): Signing key ≠ long-term key



$(g^b, \boxed{g^{b'}}, g^s, \sigma_B)$

$(g^b, \boxed{g^{b'}}, g^s, \sigma_B)$

$\sigma_B = \boxed{\text{Sign}_{b'}(g^s)}$

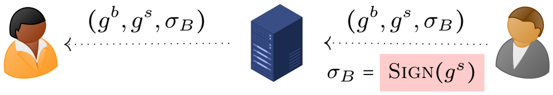
long-term (a, g^a)

long-term (b, g^b)

signing $(\boxed{b'}, g^{b'})$

Key Reuse Issue

In the reduction to the signature security:



(g^b, g^s, σ_B)

(g^b, g^s, σ_B)

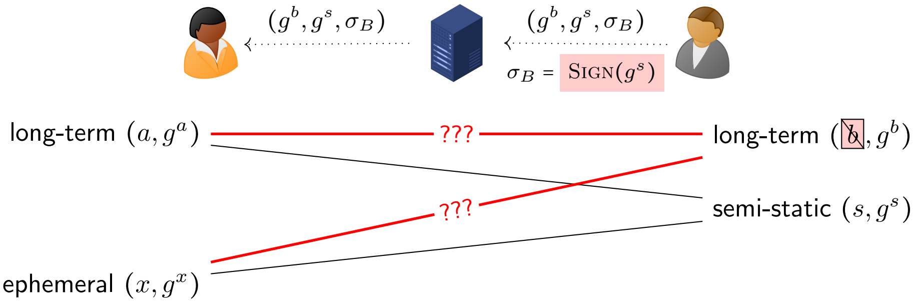
$\sigma_B = \textsc{Sign}(g^s)$

long-term (a, g^a)

long-term $(\boxed{\cancel{b}}, g^b)$

Key Reuse Issue

In the reduction to the signature security:



(g^b, g^s, σ_B)

(g^b, g^s, σ_B)

$\sigma_B = \textsc{Sign}(g^s)$

long-term (a, g^a)

???

long-term $(\boxed{\cancel{b}}, g^b)$

???

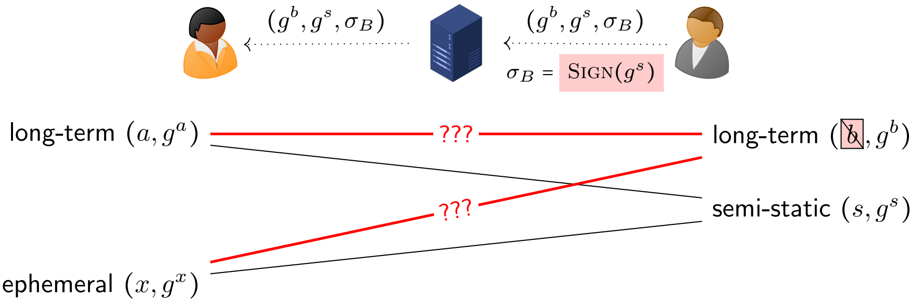
semi-static (s, g^s)

ephemeral (x, g^x)

KDF($g^{(eb+e's)\cdot(x+da)}$)=??

Key Reuse Issue

In the reduction to the signature security:



(g^b, g^s, σ_B)

(g^b, g^s, σ_B)

$\sigma_B = \boxed{\textsc{Sign}(g^s)}$

long-term (a, g^a)

???

long-term $(\boxed{\cancel{b}}, g^b)$

semi-static (s, g^s)

???

ephemeral (x, g^x)

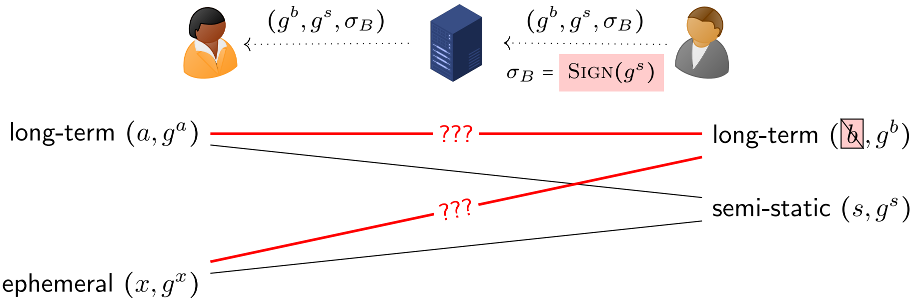
KDF$(g^{(eb+e's)\cdot(x+da)})$=??

Our Solution: EUF-opCMA-DDH ≈ EUF-CMA

- opCMA: One-per message (Weaker than EUF-CMA)

Key Reuse Issue

In the reduction to the signature security:



(g^b, g^s, σ_B)

(g^b, g^s, σ_B)

$\sigma_B = \boxed{\textsc{Sign}(g^s)}$

long-term (a, g^a)

???

long-term $(\boxed{\cancel{b}}, g^b)$

semi-static (s, g^s)

???

ephemeral (x, g^x)

$\mathsf{KDF}(g^{(eb+e's)\cdot(x+da)})$=??

Our Solution: EUF-opCMA-DDH ≈ EUF-CMA

- opCMA: One-per message (Weaker than EUF-CMA)
- DDH Oracle: Allows us to compute $\mathsf{KDF}(g^{(eb+e's)\cdot(x+da)})$ by programming the RO

Security and Efficiency Comparison

Schemes	#Exp	Ephemeral & semi-static leak	Other leak	Security bound	Key reuse?
X3DH	8 (6)	insecure	secure	$O(\sqrt{\varepsilon_{\mathsf{DL}}})^{\dagger}$	✗
XHMQV	5 (4)	secure	secure	$O(\sqrt{\varepsilon_{\mathsf{GapDH}}})^{\ddagger}$	✓

[†] $\sqrt{\varepsilon_{\mathsf{DL}}}$-loss is due to (EC)DSA used in X3DH, where $\varepsilon_{\mathsf{DL}}$ is the probability of breaking DL

[‡] $\sqrt{\varepsilon_{\mathsf{GapDH}}}$-loss comes from GapDH → CRGapDH (cf. [KPRR23])

Conclusion

XHMQV: An initial handshake protocol

- Asynchronous
- More efficient due to fewer exponentiation
- Stronger "maximum-exposure" security
- Similar deniability as X3DH [FL25]
- More realistic security proofs that consider key reuse

[FL25] R. Fiedler and R. Langrehr: On Deniable Authentication against Malicious Verifiers. In CRYPTO'25.

Conclusion

XHMQV: An initial handshake protocol

- Asynchronous
- More efficient due to fewer exponentiation
- Stronger "maximum-exposure" security
- Similar deniability as X3DH [FL25]
- More realistic security proofs that consider key reuse

[FL25] R. Fiedler and R. Langrehr: On Deniable Authentication against Malicious Verifiers. In CRYPTO'25.

Open Problems

- Achieving the same level of "maximum-exposure" security in the post-quantum setting?
- Extending our analysis of key reuse to other protocols?
- Achieving subversion-resilient security using reverse firewall [DMSDT25] ?

[DMSDT25] Y. Dodis, B. Magri, N. Stephens-Davidowitz, and Y. Tselekounis: Guarding the Signal: Secure Messaging with Reverse Firewalls. In CRYPTO'25.

References I

Jacqueline Brendel, Rune Fiedler, Felix Günther, Christian Janson, and Douglas Stebila.
Post-quantum asynchronous deniable key exchange and the Signal handshake.
In Goichiro Hanaoka, Junji Shikata, and Yohei Watanabe, editors, *PKC 2022: 25th International Conference on Theory and Practice of Public Key Cryptography, Part II*, volume 13178 of *Lecture Notes in Computer Science*, pages 3–34, Virtual Event, March 8–11, 2022. Springer, Cham, Switzerland.

Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowling, Luke Garratt, and Douglas Stebila.
A formal security analysis of the Signal messaging protocol.
Journal of Cryptology, 33(4):1914–1983, October 2020.

Katriel Cohn-Gordon, Cas Cremers, Luke Garratt, Jon Millican, and Kevin Milner.
On ends-to-ends encryption: Asynchronous group messaging with strong security guarantees.
In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *ACM CCS 2018: 25th Conference on Computer and Communications Security*, pages 1802–1819, Toronto, ON, Canada, October 15–19, 2018. ACM Press.

Daniel Collins, Doreen Riepel, and Si An Oliver Tran.
On the tight security of the double ratchet.
In Bo Luo, Xiaojing Liao, Jun Xu, Engin Kirda, and David Lie, editors, *ACM CCS 2024: 31st Conference on Computer and Communications Security*, pages 4747–4761, Salt Lake City, UT, USA, October 14–18, 2024. ACM Press.

References II

Rune Fiedler and Felix Günther.
Security analysis of Signal's PQXDH handshake.
In Tibor Jager and Jiaxin Pan, editors, *PKC 2025: 28th International Conference on Theory and Practice of Public Key Cryptography, Part II*, volume 15675 of *Lecture Notes in Computer Science*, pages 137–169, Røros, Norway, May 12–15, 2025. Springer, Cham, Switzerland.

Rune Fiedler, Felix Günther, Jiaxin Pan, and Runzhi Zeng.
XHMQV: Better efficiency and stronger security for Signal's initial handshake based on HMQV.
2025.

Eike Kiltz, Jiaxin Pan, Doreen Riepel, and Magnus Ringerud.
Multi-user CDH problems and the concrete security of NAXOS and HMQV.
In Mike Rosulek, editor, *Topics in Cryptology – CT-RSA 2023*, volume 13871 of *Lecture Notes in Computer Science*, pages 645–671, San Francisco, CA, USA, April 24–27, 2023. Springer, Cham, Switzerland.

Hugo Krawczyk.
HMQV: A high-performance secure Diffie-Hellman protocol.
In Victor Shoup, editor, *Advances in Cryptology – CRYPTO 2005*, volume 3621 of *Lecture Notes in Computer Science*, pages 546–566, Santa Barbara, CA, USA, August 14–18, 2005. Springer Berlin Heidelberg, Germany.

Icon References

- server icon by Alexiuz AS
- public key icon by Yannick Lung
- Secure messaging app icons are by Signal, WhatsApp, Google Messages, Facebook Messenger