Making Signal Post-quantum Secure:
Post-quantum Asynchronous Deniable Key Exchange from Key Encapsulation and Designated Verifier Signatures

Jacqueline Brendel[1]

Rune Fiedler[1]

Felix Günther[2]

Christian Janson[1]

Douglas Stebila[3]

[1]TU Darmstadt, Germany
{jacqueline.brendel, rune.fiedler, christian.janson}@cryptoplexity.de

[2]ETH Zürich, Switzerland
mail@felixguenther.info

[3]University of Waterloo, Canada
dstebila@uwaterloo.ca

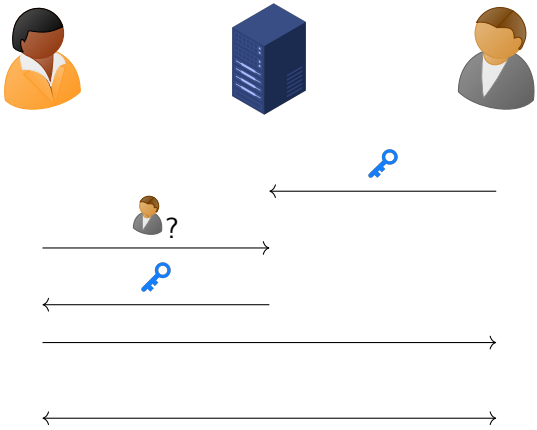
RWC 2022

Instant Messaging

Instant Messaging

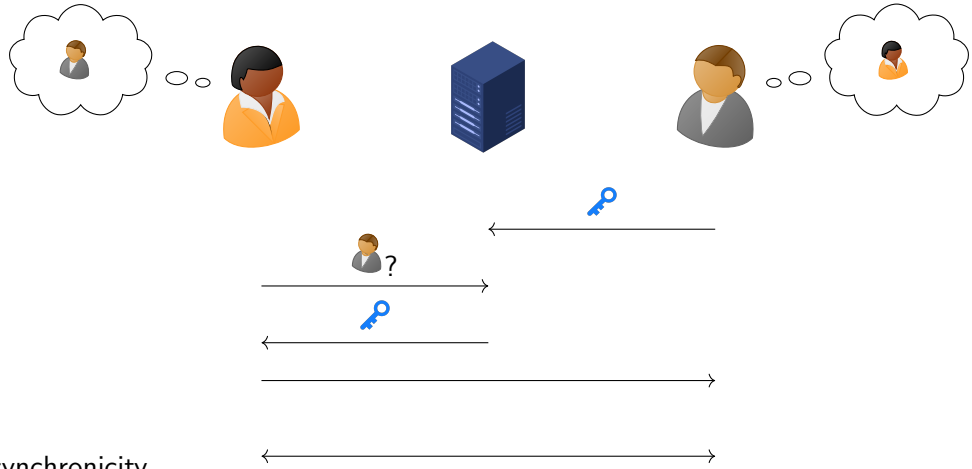
?

Instant Messaging



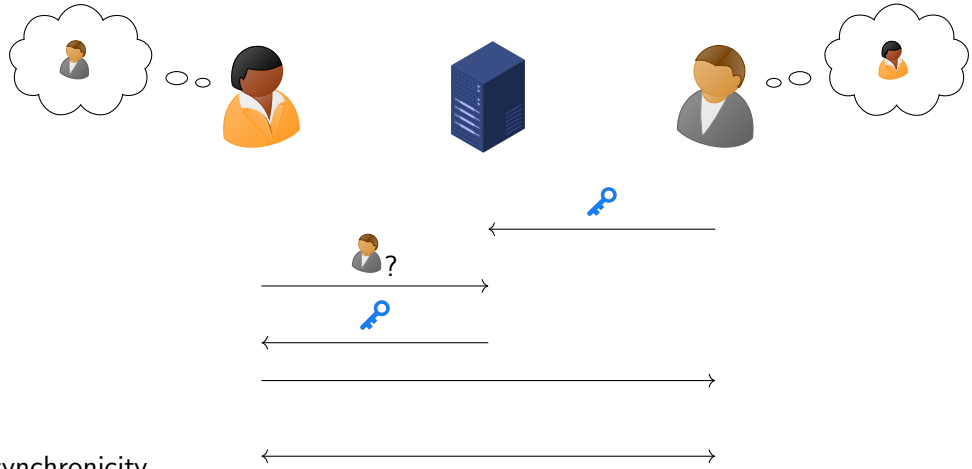
- Asynchronicity

Instant Messaging



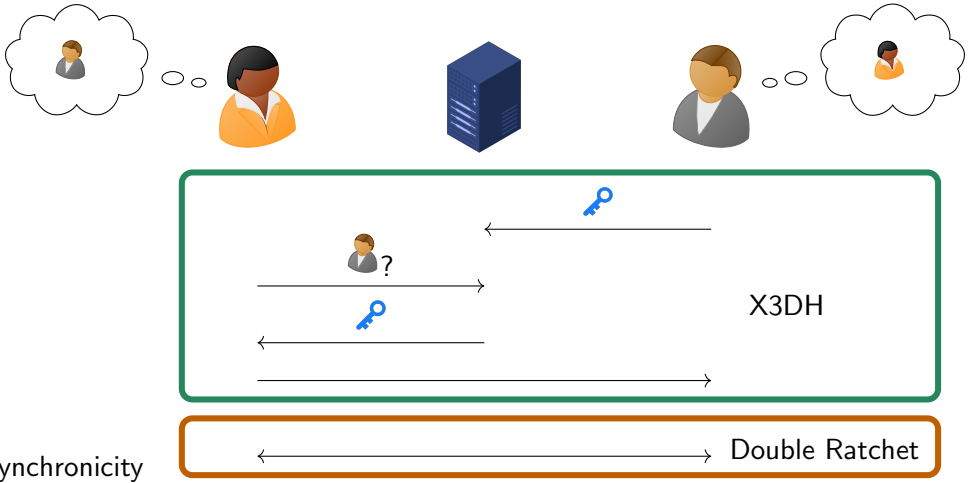
- Asynchronicity
- Mutual authentication

Instant Messaging



- Asynchronicity
- Mutual authentication
- Offline deniability **Signal**

Instant Messaging



- Asynchronicity
- Mutual authentication
- Offline deniability **Signal**

Signal initial handshake: X3DH

pre-key bundle

long-term

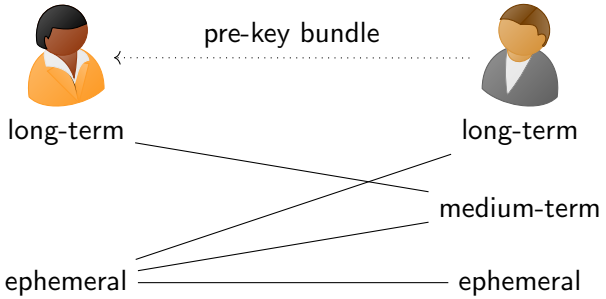
long-term

medium-term

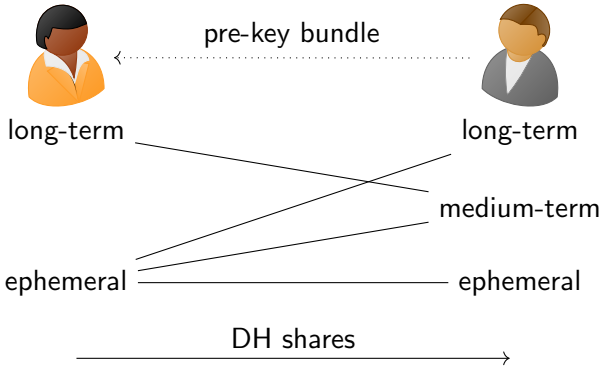
ephemeral

ephemeral

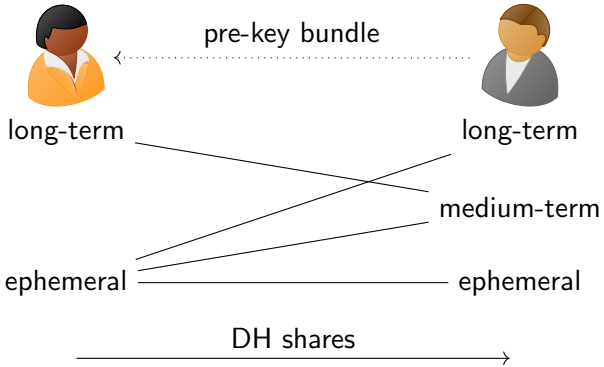
Signal initial handshake: X3DH



Signal initial handshake: X3DH



Signal initial handshake: X3DH



- ⚠ *not* post-quantum

Initial Handshake: X3DH

⚠ not post-quantum

Double Ratchet

post-quantum from e.g. Key Encapsulation [ACD19]

[ACD19] Alwen, Coretti, Dodis, EUROCRYPT 2019, `https://ia.cr/2018/1037`

Initial Handshake: X3DH

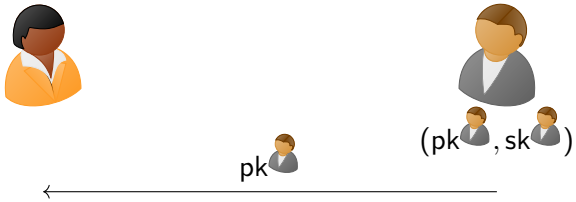
⚠ not post-quantum

Double Ratchet

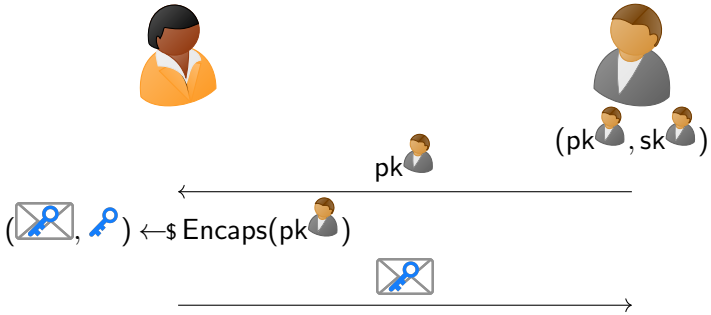
post-quantum from e.g. Key Encapsulation [ACD19]

[ACD19] Alwen, Coretti, Dodis, EUROCRYPT 2019, https://ia.cr/2018/1037

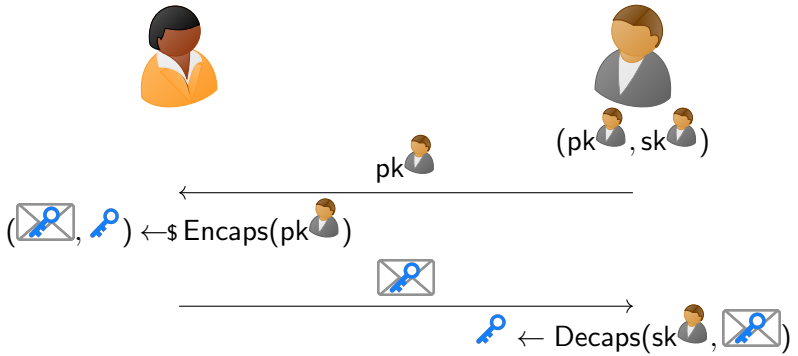
Key Encapsulation Mechanisms (KEMs)



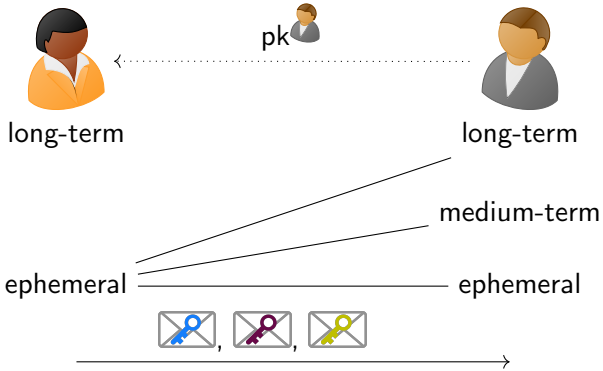
Key Encapsulation Mechanisms (KEMs)



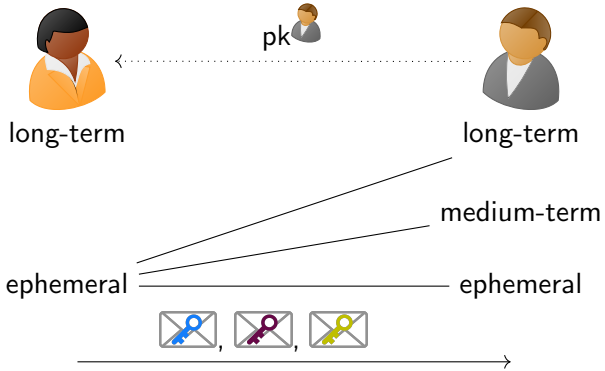
Key Encapsulation Mechanisms (KEMs)



PQSignal from KEMs?

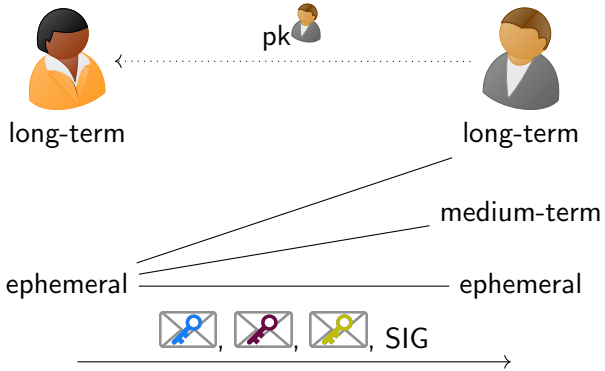


PQSignal from KEMs?



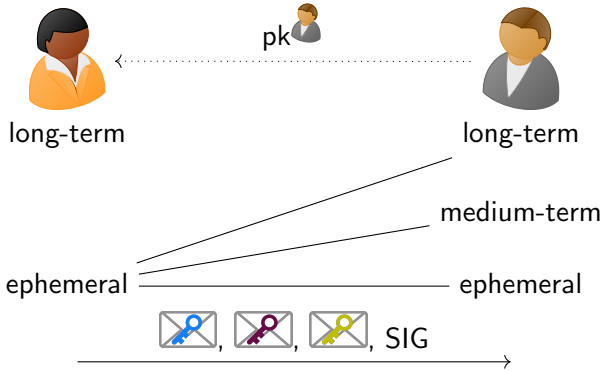
⚠ Alice-to-Bob authentication

PQSignal from KEMs?



⚠ Alice-to-Bob authentication

PQSignal from KEMs?



⚠ Alice-to-Bob authentication

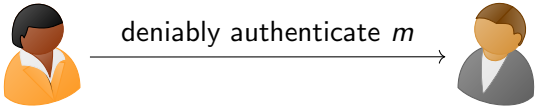
⚠ SIG breaks deniability for Alice

KEMs for PQSignal

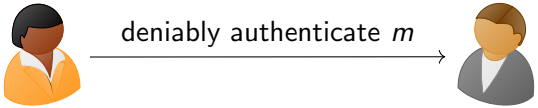
- [BFG+20] proposed initial handshake with *split KEMs* but not instantiable
- Design idea: KEMs + deniable authentication
  - Designated Verifier Signatures [BFG+22]
  - Ring Signatures [HKKP21]

[BFG+20] Brendel, Fischlin, Günther, Janson, Stebila, SAC 2020, https://ia.cr/2019/1356
[BFG+22] Brendel, Fiedler, Günther, Janson, Stebila, PKC 2022, https://ia.cr/2021/769
[HKKP21] Hashimoto, Katsumata, Kwiatkowski, Prest, PKC 2021, https://ia.cr/2021/616

Deniable Authentication: Designated Verifier Signatures (DVS)

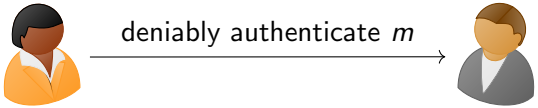


Deniable Authentication: Designated Verifier Signatures (DVS)



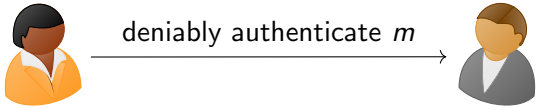
- Sign $\left(\text{sk}, \text{pk}, m\right) \rightarrow$

Deniable Authentication: Designated Verifier Signatures (DVS)



- Sign $\left(\text{sk}, \text{pk}, m\right) \rightarrow$
- Sim $\left(\text{pk}, \text{sk}, m\right) \rightarrow$

Deniable Authentication: Designated Verifier Signatures (DVS)



- Sign $\left(\text{sk}, \text{pk}, m\right) \to$
- Sim $\left(\text{pk}, \text{sk}, m\right) \to$
- source hiding: $\approx$

Core idea of [HKKP21, BFG+22]

DVS

long-term

long-term

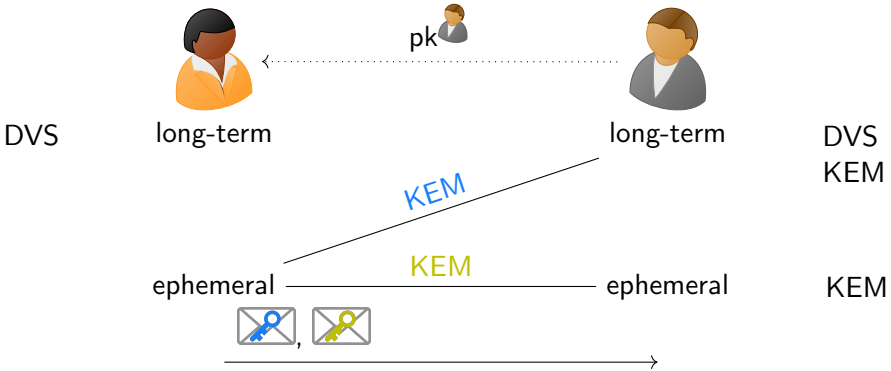
DVS
KEM

ephemeral

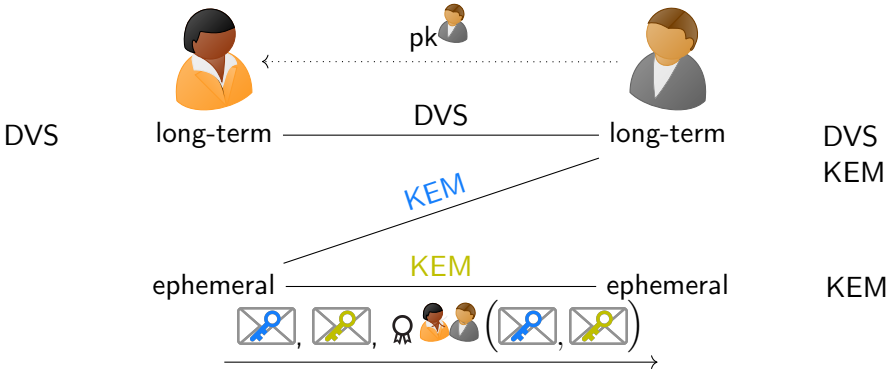
ephemeral

KEM

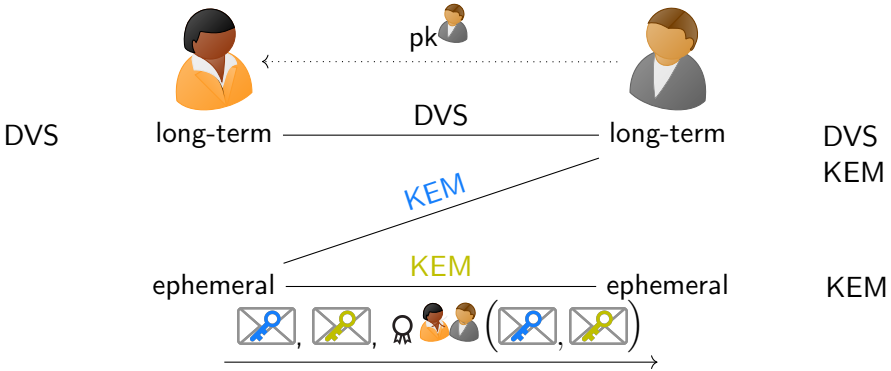
Core idea of [HKKP21, BFG+22]



Core idea of [HKKP21, BFG+22]



Core idea of [HKKP21, BFG+22]



- [HKKP21] uses ring signatures instead of DVS (equivalence shown for 2-user rings)

What is Deniability for Asynchronous DAKE? [BFG+22]

A **third party that has compromised legitimate private keys** *from Alice or Bob could be* **provided a communication transcript** *that appears to be between Alice and Bob and that can* **only** *have been* **created by** *some other party that also has access to* **legitimate private keys** *from Alice or Bob. [MP16]*

[MP16] Marlinspike, Perrin, Signal specification, `https://signal.org/docs/specifications/x3dh/`

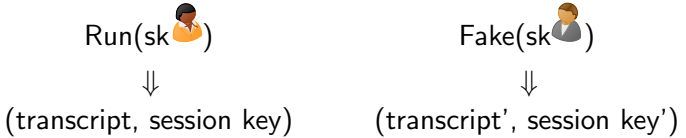
What is Deniability for Asynchronous DAKE? [BFG+22]

A **third party that has compromised legitimate private keys** *from Alice or Bob could be* **provided a communication transcript** *that appears to be between Alice and Bob and that can* **only** *have been* **created by** *some other party that also has access to* **legitimate private keys** *from Alice or Bob. [MP16]*

[MP16] Marlinspike, Perrin, Signal specification, `https://signal.org/docs/specifications/x3dh/`

What is Deniability for Asynchronous DAKE? [BFG+22]

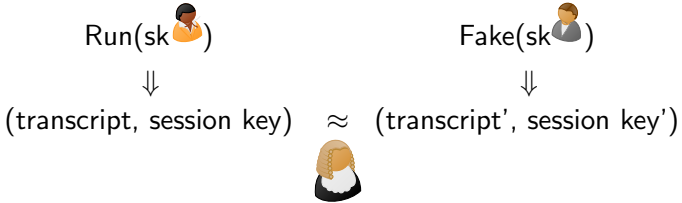
A **third party that has compromised legitimate private keys** *from Alice or Bob could be* **provided a communication transcript** *that appears to be between Alice and Bob and that can* **only** *have been* **created by** *some other party that also has access to* **legitimate private keys** *from Alice or Bob. [MP16]*



[MP16] Marlinspike, Perrin, Signal specification, `https://signal.org/docs/specifications/x3dh/`

What is Deniability for Asynchronous DAKE? [BFG+22]

A **third party that has compromised legitimate private keys** *from Alice or Bob could be* **provided a communication transcript** *that appears to be between Alice and Bob and that can* **only** *have been* **created by** *some other party that also has access to* **legitimate private keys** *from Alice or Bob. [MP16]*



[MP16] Marlinspike, Perrin, Signal specification, `https://signal.org/docs/specifications/x3dh/`

Difference to Prior Deniability Definition [DGK06]

- Our Fake requires sk 

[DGK06] Di Raimondo, Gennaro, Krawczyk, CCS 2006, https://ia.cr/2006/280

Difference to Prior Deniability Definition [DGK06]

- Our Fake requires sk 
- Our  gets all secret keys

[DGK06] Di Raimondo, Gennaro, Krawczyk, CCS 2006, https://ia.cr/2006/280

Difference to Prior Deniability Definition [DGK06]

- Our Fake requires sk 
- Our  gets all secret keys
- Our definition does not need strong knowledge-type assumptions

[DGK06] Di Raimondo, Gennaro, Krawczyk, CCS 2006, https://ia.cr/2006/280

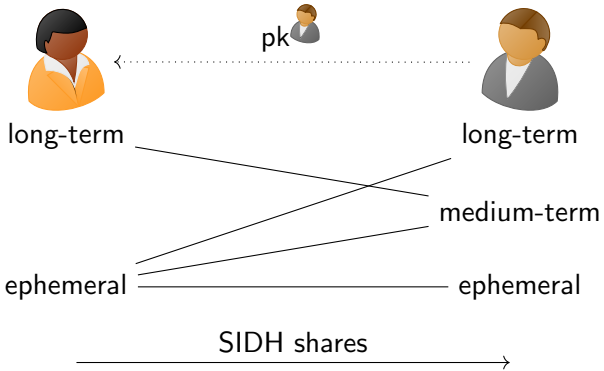
Our full construction: SPQR [BFG+21]

- Signal in a Post-Quantum Regime (SPQR)
- full scope:
  - Includes medium-term keys
  - Security against randomness exposure via twisted PRF
- Security model analogous to original Signal analysis [CCD+17] & deniability

[BFG+21] Brendel, Fiedler, Günther, Janson, Stebila, full version, https://ia.cr/2021/769

[CCD+17] Cohn-Gordon, Cremers, Dowling, Garratt, Stebila, EuroS&P, https://ia.cr/2016/1013

Concurrent work: [DG21]



- Adapts DH to supsersingular isogenies $\Rightarrow$ SI-X3DH
- Asynchronous, mutual authentication, offline deniability, post-quantum

[DG21] Dobson, Galbraith, ePrint, `https://ia.cr/2021/1187`

Comparison of initial handshake protocols

		PQ	deniability		full scope
			strong judge	public sim.	
X3DH	DH	✗	•	✓	✓
SC-DAKE [HKKP21]	KEM + RingSIG	✓	•	✗	✗
SC-DAKE′ [HKKP21]	SC-DAKE + NIZK	✓	•	✓	✗
SPQR [BFG+22]	KEM + DVS	✓	✓	✗	✓
SI-X3DH [DG21]	SIDH	✓	•	✓	✓

✓ proven ✗ not satisfied • needs to be verified

full scope: real-world setting with medium-term keys and maximal-exposure security

Signal goes post-quantum?

Initial Handshake

post-quantum with [HKKP21], SPQR [BFG+21], or [DG21]

Double Ratchet

post-quantum from e.g. Key Encapsulation [ACD19]

- Which deniability notion do we want?
- How to efficiently instantiate?

rune.fiedler@cryptoplexity.de

Full paper: `https://eprint.iacr.org/2021/769` published at PKC 2022

References I

[ACD19] Joël Alwen, Sandro Coretti, and Yevgeniy Dodis.
The double ratchet: Security notions, proofs, and modularization for the Signal protocol.
In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019, Part I*, volume 11476 of *Lecture Notes in Computer Science*, pages 129–158, Darmstadt, Germany, May 19–23, 2019. Springer, Heidelberg, Germany.

[BFG+20] Jacqueline Brendel, Marc Fischlin, Felix Günther, Christian Janson, and Douglas Stebila.
Towards post-quantum security for Signal's X3DH handshake.
In *27th Conference on Selected Areas in Cryptography (SAC)*. Springer, October 2020.

[BFG+21] Jacqueline Brendel, Rune Fiedler, Felix Günther, Christian Janson, and Douglas Stebila.
Post-quantum asynchronous deniable key exchange and the Signal handshake.
Cryptology ePrint Archive, Report 2021/769, 2021.
`https://eprint.iacr.org/2021/769`.

[BFG+22] Jacqueline Brendel, Rune Fiedler, Felix Günther, Christian Janson, and Douglas Stebila.
Post-quantum asynchronous deniable key exchange and the Signal handshake.
In *Public-Key Cryptography - PKC 2022 - 25th IACR International Conference on Practice and Theory of Public Key Cryptography, Yokohama, Japan May 7-11, 2022 (to be released)*, 2022.

References II

[CCD+17] Katriel Cohn-Gordon, Cas J. F. Cremers, Benjamin Dowling, Luke Garratt, and Douglas Stebila.
A formal security analysis of the Signal messaging protocol.
In *IEEE European Symposium on Security and Privacy, EuroS&P 2017*, pages 451–466, 2017.

[DG21] Samuel Dobson and Steven D. Galbraith.
Post-quantum signal key agreement with SIDH.
Cryptology ePrint Archive, Report 2021/1187, 2021.
https://eprint.iacr.org/2021/1187.

[DGK06] Mario Di Raimondo, Rosario Gennaro, and Hugo Krawczyk.
Deniable authentication and key exchange.
In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *ACM CCS 2006: 13th Conference on Computer and Communications Security*, pages 400–409, Alexandria, Virginia, USA, October 30 – November 3, 2006. ACM Press.

[HKKP21] Keitaro Hashimoto, Shuichi Katsumata, Kris Kwiatkowski, and Thomas Prest.
An efficient and generic construction for signal's handshake (X3DH): Post-quantum, state leakage secure, and deniable.
In Juan Garay, editor, *PKC 2021: 24th International Conference on Theory and Practice of Public Key Cryptography, Part II*, volume 12711 of *Lecture Notes in Computer Science*, pages 410–440, Virtual Event, May 10–13, 2021. Springer, Heidelberg, Germany.

References III

[LLY18] BaoHong Li, YanZhi Liu, and Sai Yang.
Lattice-based universal designated verifier signatures.
In *2018 IEEE 15th International Conference on e-Business Engineering (ICEBE)*, pages 329–334. IEEE, 2018.

[MP16] Moxie Marlinspike and Trevor Perrin.
The X3DH key agreement protocol, November 2016.

[VGIK20] Nihal Vatandas, Rosario Gennaro, Bertrand Ithurburn, and Hugo Krawczyk.
On the cryptographic deniability of the Signal protocol.
In Mauro Conti, Jianying Zhou, Emiliano Casalicchio, and Angelo Spognardi, editors, *ACNS 20: 18th International Conference on Applied Cryptography and Network Security, Part II*, volume 12147 of *Lecture Notes in Computer Science*, pages 188–209, Rome, Italy, October 19–22, 2020. Springer, Heidelberg, Germany.

[ZLTT15] Yongqiang Zhang, Qiang Liu, Chengpei Tang, and Haibo Tian.
A lattice-based designated verifier signature for cloud computing.
International Journal of High Performance Computing and Networking, 8:135–143, June 2015.

Picture references

- server icon by Alexiuz AS
- key icon by Yannick Lung
- envelope icon by Yannick Lung
- signature icon by PINPOINT.WORLD

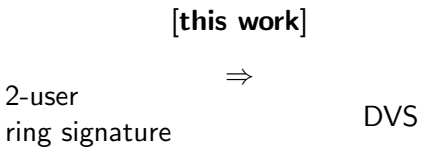
Post-Quantum DVS

- Direct constructions in need of more scrutiny [LLY18, ZLTT15]

[LLY18] Li, Liu, Yang, ICEBE 2018, https://doi.org/10.1109/ICEBE.2018.00062
[ZLTT15] Zhang, Liu, Tang, Tian, IJHPCN 2019, https://doi.org/10.1504/IJHPCN.2015.070013

Post-Quantum DVS

- Direct constructions in need of more scrutiny [LLY18, ZLTT15]

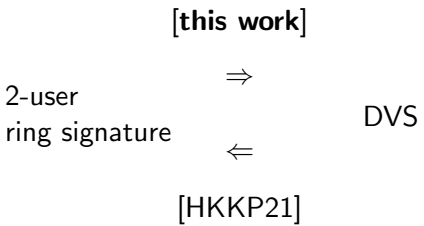


- More literature on post-quantum ring signature than DVS

[LLY18] Li, Liu, Yang, ICEBE 2018, https://doi.org/10.1109/ICEBE.2018.00062
[ZLTT15] Zhang, Liu, Tang, Tian, IJHPCN 2019, https://doi.org/10.1504/IJHPCN.2015.070013

Post-Quantum DVS

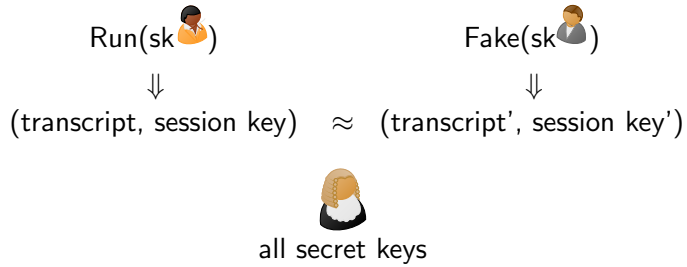
- Direct constructions in need of more scrutiny [LLY18, ZLTT15]



- More literature on post-quantum ring signature than DVS

[LLY18] Li, Liu, Yang, ICEBE 2018, https://doi.org/10.1109/ICEBE.2018.00062
[ZLTT15] Zhang, Liu, Tang, Tian, IJHPCN 2019, https://doi.org/10.1504/IJHPCN.2015.070013

Variants of Deniability



- Does Fake get sk?
- Does get all secret keys?
- Does the judge interact during the protocol execution?