Post-quantum Asynchronous Deniable Key Exchange and the Signal Handshake

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

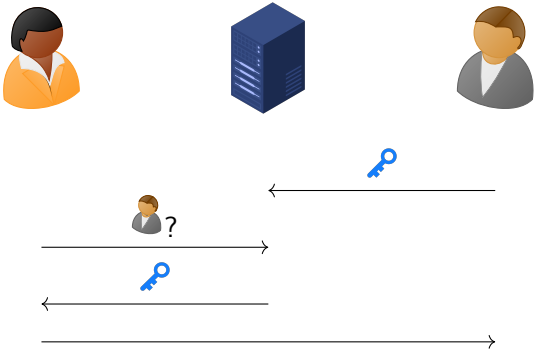
[3]University of Waterloo, Canada
dstebila@uwaterloo.ca

PKC 2022

Instant Messaging

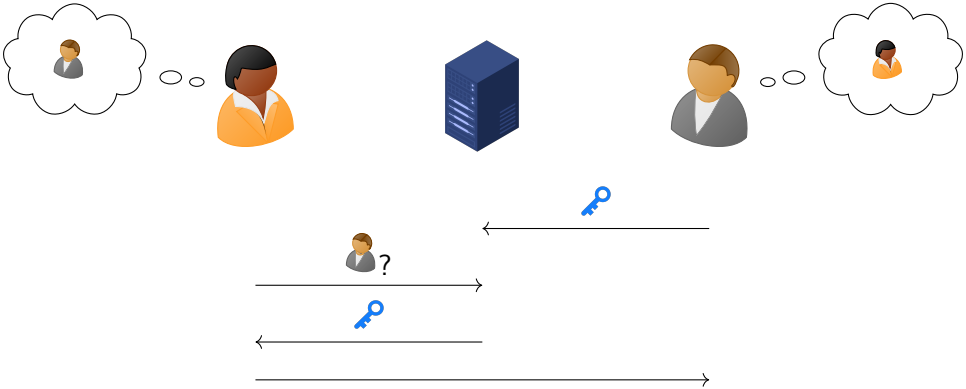
Instant Messaging

Instant Messaging



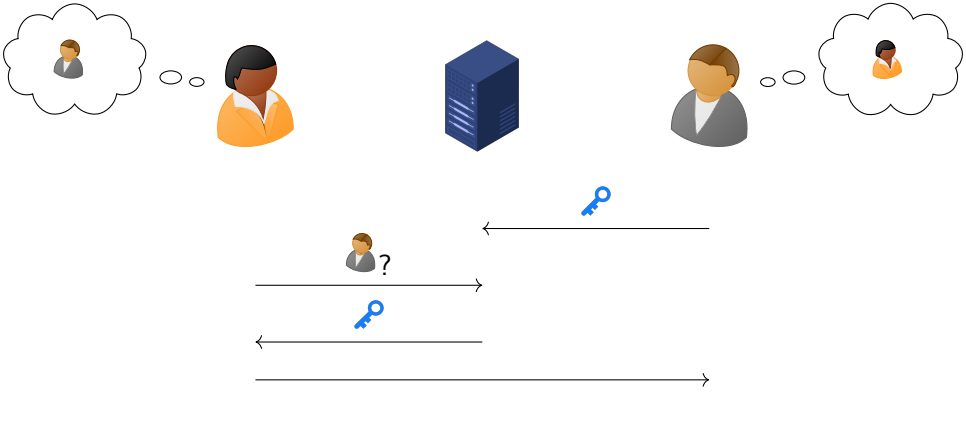
- Asynchronicity

Instant Messaging



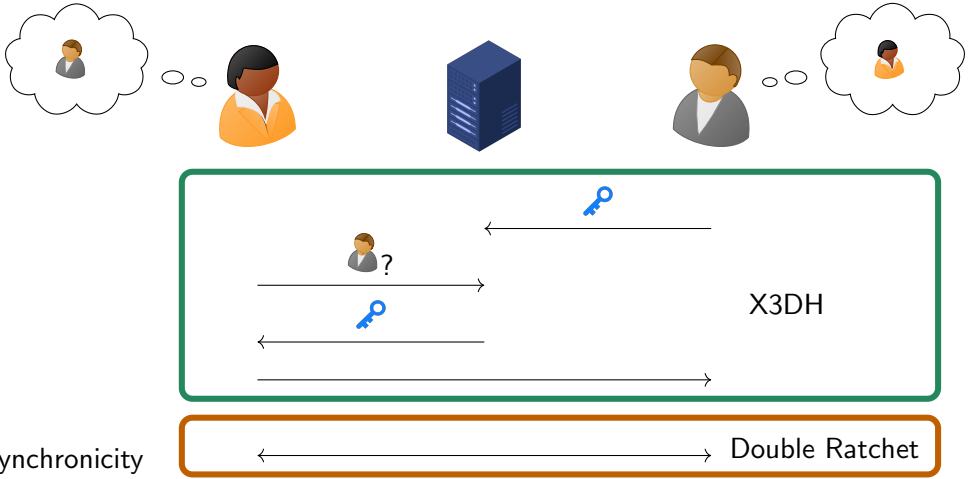
- Asynchronicity
- Mutual authentication

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

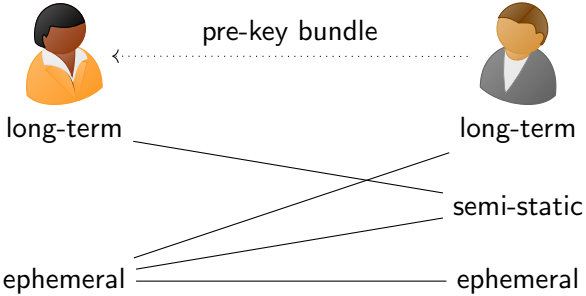
long-term

semi-static

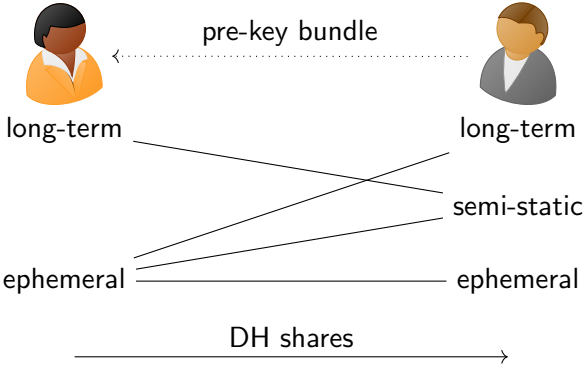
ephemeral

ephemeral

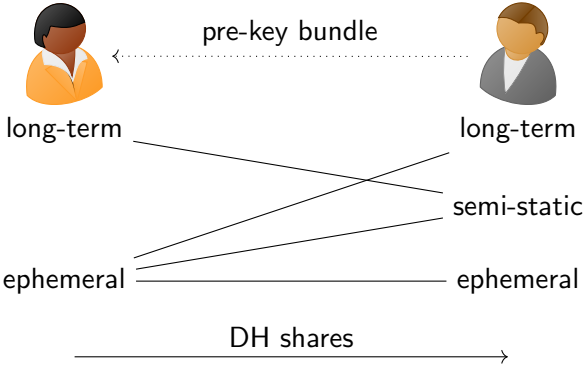
Signal initial handshake: X3DH



Signal initial handshake: X3DH



Signal initial handshake: X3DH



- ⚠ *not* post-quantum

Signal

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`

Signal

Initial Handshake: X3DH

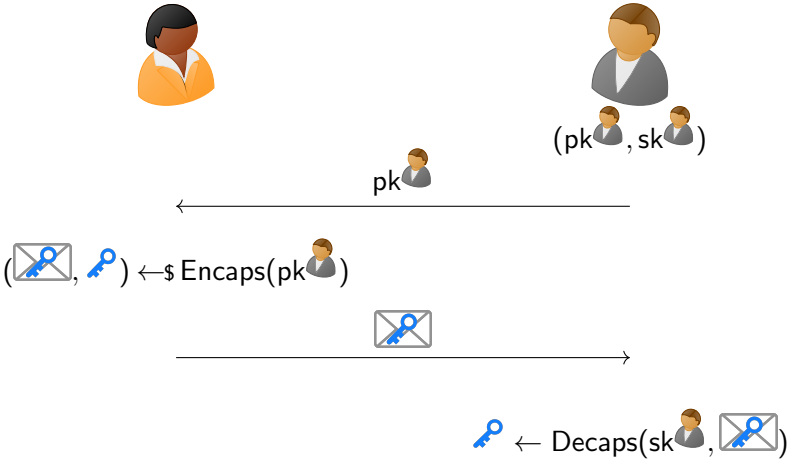
⚠ not post-quantum

Double Ratchet

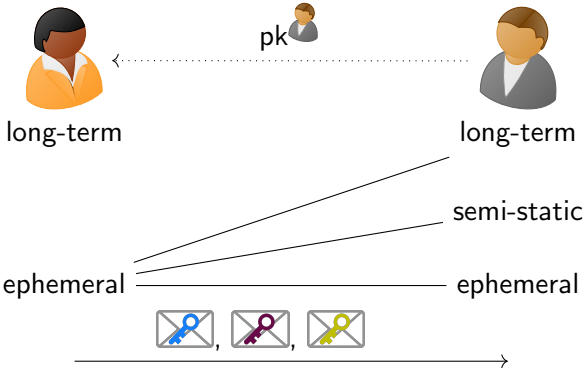
post-quantum from e.g. Key Encapsulation [ACD19]

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

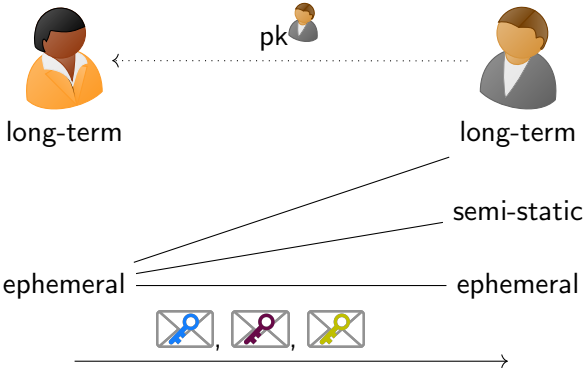
Key Encapsulation Mechanisms (KEMs)



PQSignal from KEMs?

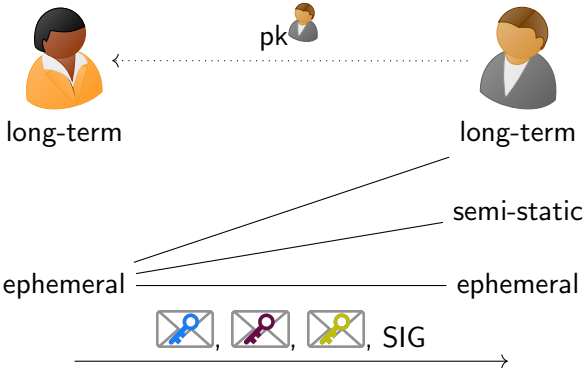


PQSignal from KEMs?



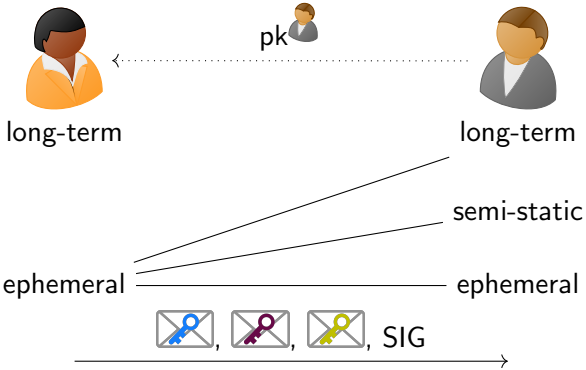
⚠ Alice-to-Bob authentication

PQSignal from KEMs?



⚠ Alice-to-Bob authentication

PQSignal from KEMs?



⚠ Alice-to-Bob authentication

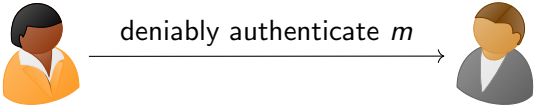
⚠ SIG breaks deniability for Alice

KEMs for PQSignal

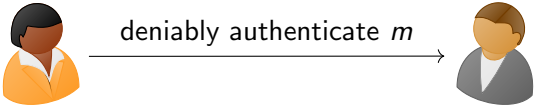
- [BFG+20] proposed initial handshake with *split KEMs* but not instantiable
- Design idea: KEMs + deniable authentication
  - Designated Verifier Signatures **[this work]**
  - Ring Signatures [HKKP21]

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

Deniable Authentication: Designated Verifier Signatures (DVS)

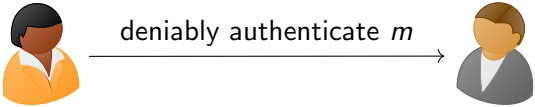


Deniable Authentication: Designated Verifier Signatures (DVS)



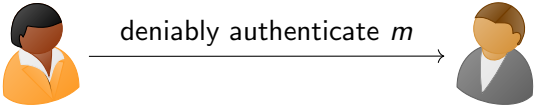
- $\mathsf{Sign}\left(\mathsf{sk}, \mathsf{pk}, m\right) \to$ 

Deniable Authentication: Designated Verifier Signatures (DVS)



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

Deniable Authentication: Designated Verifier Signatures (DVS)



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

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]

[this work]

2-user ring signature $\Rightarrow$ DVS

- 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

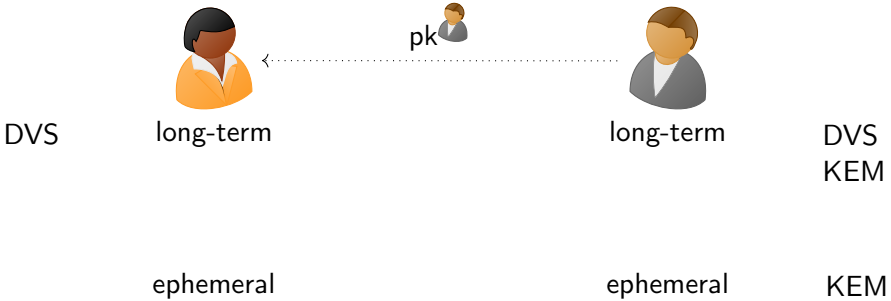
- Direct constructions in need of more scrutiny [LLY18, ZLTT15]

$$\begin{array}{ccc} & [\textbf{this work}] & \\ & \Rightarrow & \\ \text{2-user ring signature} & & \text{DVS} \\ & \Leftarrow & \\ & [\text{HKKP21}] & \end{array}$$

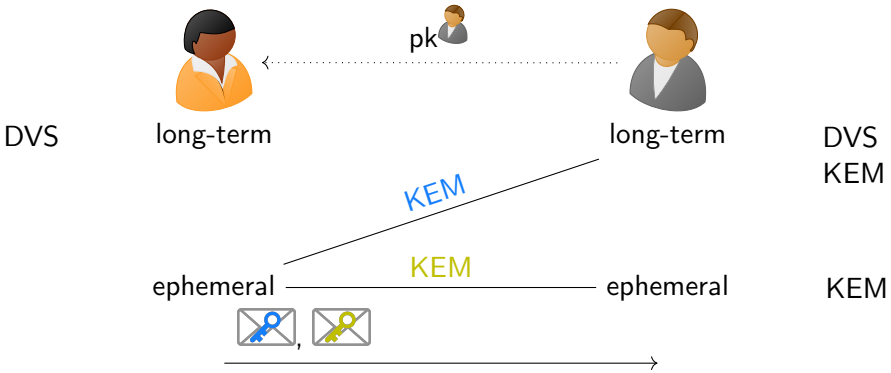
- More literature on post-quantum ring signature than DVS

[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

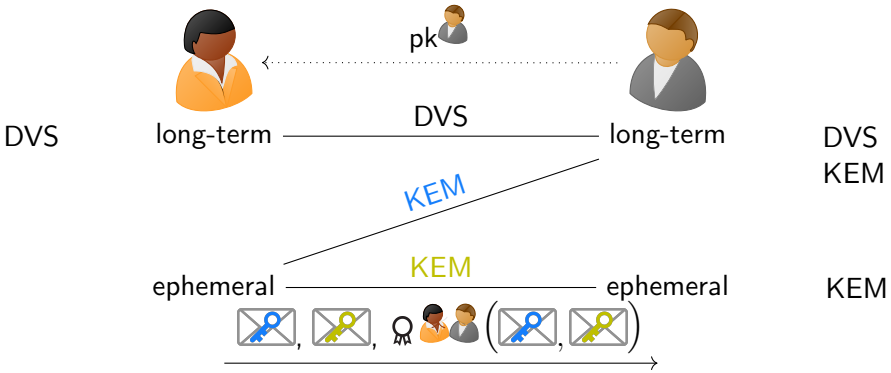
Core idea of our asynchronous DAKE protocol and [HKKP21]



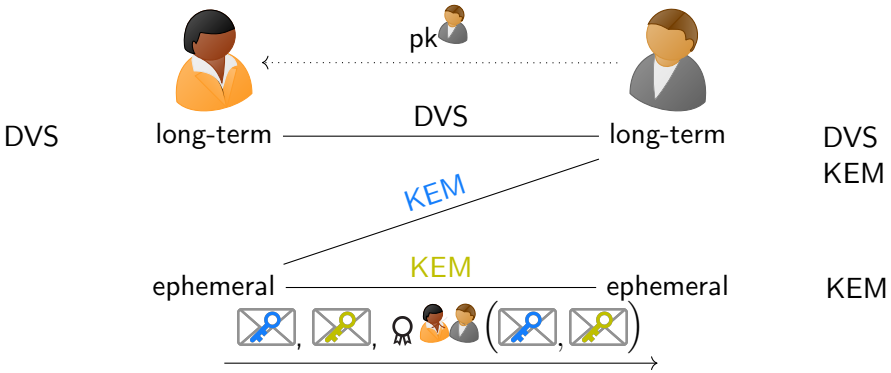
Core idea of our asynchronous DAKE protocol and [HKKP21]



Core idea of our asynchronous DAKE protocol and [HKKP21]



Core idea of our asynchronous DAKE protocol and [HKKP21]



- [HKKP21] uses ring signatures instead of DVS

What is Deniability for Asynchronous DAKE?

X3DH doesn't give either Alice or Bob a publishable cryptographic proof of the contents of their communication or the fact that they communicated.
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?

X3DH doesn't give either Alice or Bob a publishable cryptographic proof of the contents of their communication or the fact that they communicated.
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]

Run(sk )

$\Downarrow$

(transcript, session key)

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

What is Deniability for Asynchronous DAKE?

X3DH doesn't give either Alice or Bob a publishable cryptographic proof of the contents of their communication or the fact that they communicated.
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]

Run(sk )

$\Downarrow$

(transcript, session key)

Fake(sk )

$\Downarrow$

(transcript', session key')

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

What is Deniability for Asynchronous DAKE?

X3DH doesn't give either Alice or Bob a publishable cryptographic proof of the contents of their communication or the fact that they communicated.
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]

Run(sk ) Fake(sk )

$\Downarrow$ $\Downarrow$

(transcript, session key) $\approx$ (transcript', session key')

all secret keys

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

Variants of Deniability

Run(sk ) Fake(sk )

$\Downarrow$ $\Downarrow$

(transcript, session key) $\approx$ (transcript', session key')

all secret keys

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

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

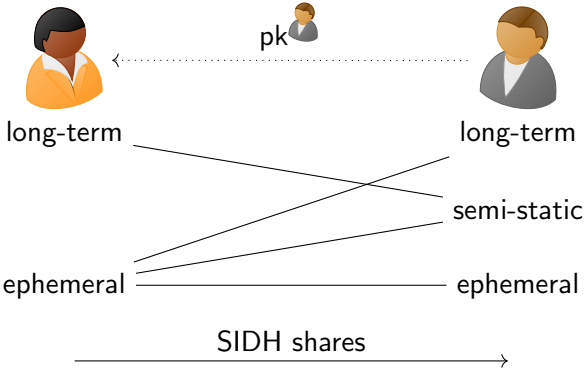
[DGK06] Di Raimondo, Gennaro, Krawczyk, CCS 2006, `https://ia.cr/2006/280`

Difference to Prior Deniability Definition [DGK06]

- Our Fake requires sk 
- Our  gets all secret keys
- Proofs for their definition require knowledge assumptions

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

Concurrent work: [DG21]



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

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

Our full construction: SPQR

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

$\mathsf{KGenLT}()$:
$(pk^{\mathsf{KEM}}, sk^{\mathsf{KEM}}) \leftarrow\$ \mathsf{KEM}_1.\mathsf{KGen}()$
$(pk^{\mathsf{DVS}}, sk^{\mathsf{DVS}}) \leftarrow\$ \mathsf{DVS}.\mathsf{SKGen}()$
$tk \leftarrow \mathsf{tPRF}.\mathsf{KGen}()$
$pk \leftarrow (pk^{\mathsf{KEM}}, pk^{\mathsf{DVS}})$
$sk \leftarrow (sk^{\mathsf{KEM}}, sk^{\mathsf{DVS}}, tk)$
return (pk, sk)

$\mathsf{KGenSS}()$:
$(sspk^{\mathsf{KEM}}, sssk^{\mathsf{KEM}}) \leftarrow\$ \mathsf{KEM}_2.\mathsf{KGen}()$
$(sspk^{\mathsf{DVS}}, sssk^{\mathsf{DVS}}) \leftarrow\$ \mathsf{DVS}.\mathsf{VKGen}()$
$sspk \leftarrow (sspk^{\mathsf{KEM}}, sspk^{\mathsf{DVS}})$
$sssk \leftarrow (sssk^{\mathsf{KEM}}, sssk^{\mathsf{DVS}})$
return $(sspk, sssk)$

$\mathsf{KGenEP}()$:
return $(epk, esk) \leftarrow\$ \mathsf{KEM}_3.\mathsf{KGen}()$

Alice | **Signal Server** | **Bob**

Initiator Registration
$(pk_A, sk_A) \leftarrow\$ \mathsf{KGenLT}()$

Responder Registration
$(\mathsf{pk}_B, sk_B) \leftarrow\$ \mathsf{KGenLT}()$
$(sspk_B, sssk_B) \leftarrow\$ \mathsf{KGenSS}()$

Responder Ephemeral Key Generation
$(epk_B, esk_B) \leftarrow\$ \mathsf{KGenEP}()$

Send Pre-Key Bundle to Initiator

$B, pk_B, sspk_B, epk_B$ ⇠

define: $cid := (B, \mathsf{pk}_B, sspk_B, epk_B)$

define: $sid := (A, B, pk_A, pk_B, sspk_B, epk_B, n, c_1, c_2, c_3)$

Initiator Key Agreement and Protocol Message

$(sk_A^{\mathsf{KEM}}, sk_A^{\mathsf{DVS}}, tk_A) \leftarrow sk_A$

$(pk_B^{\mathsf{KEM}}, pk_B^{\mathsf{DVS}}) \leftarrow pk_B$
$(sspk_B^{\mathsf{KEM}}, sspk_B^{\mathsf{DVS}}) \leftarrow sspk_B$
$(n, r) \leftarrow\$ \{0,1\}^\lambda \times \mathcal{R}_{\mathsf{HHF}}$
$r_1 || r_2 || r_3 || r_4 \leftarrow \mathsf{tPRF}(tk_A, r)$
$(K_1, c_1) \leftarrow \mathsf{KEM}_1.\mathsf{Encaps}(\mathsf{pk}_B^{\mathsf{KEM}}; r_1)$
$(K_2, c_2) \leftarrow \mathsf{KEM}_1.\mathsf{Encaps}(sspk_B^{\mathsf{KEM}}; r_2)$
if $epk_B \neq \perp$
$\quad (K_3, c_3) \leftarrow \mathsf{KEM}_3.\mathsf{Encaps}(epk_B; r_3)$
else $(K_3, c_3) \leftarrow (\varepsilon, \varepsilon)$
$\mathsf{ms} \leftarrow K_1 || K_2 || K_3$
$\sigma \leftarrow \mathsf{DVS.Sign}(sk_A^{\mathsf{DVS}}, sspk_B^{\mathsf{DVS}}, sid; r_4)$
$K \leftarrow \mathsf{KDF}(\mathsf{ms}, sid)$
$m \leftarrow (A, pk_A, n, c_1, c_2, c_3, \sigma)$
return $(K, sid, \mathsf{accepted}, m)$

Responder Key Agreement (on input m)

$(sk_B^{\mathsf{KEM}}, sk_B^{\mathsf{DVS}}, tk_B) \leftarrow sk_B$
$(sssk_B^{\mathsf{KEM}}, sssk_B^{\mathsf{DVS}}) \leftarrow sssk_B$
$(\mathsf{pk}_A^{\mathsf{KEM}}, pk_A^{\mathsf{DVS}}) \leftarrow pk_A$
$(sspk_A^{\mathsf{KEM}}, sspk_A^{\mathsf{DVS}}) \leftarrow sspk_B$
if $\mathsf{DVS.Vrfy}(\mathsf{pk}_A^{\mathsf{DVS}}, sspk_B^{\mathsf{DVS}}, sid, \sigma) = \mathsf{false}$
$\quad$ **return** $(\perp, \perp, \mathsf{rejected}, \perp)$
$K_1 \leftarrow \mathsf{KEM}_1.\mathsf{Decaps}(sk_B^{\mathsf{KEM}}, c_1)$
$K_2 \leftarrow \mathsf{KEM}_2.\mathsf{Decaps}(sssk_B^{\mathsf{KEM}}, c_2)$
if $esk_B \neq \perp$
$\quad K_3 \leftarrow \mathsf{KEM}_3.\mathsf{Decaps}(esk_B, c_3)$
else $(K_3, c_3) \leftarrow (\varepsilon, \varepsilon)$
$\mathsf{ms} \leftarrow K_1 || K_2 || K_3$
$K \leftarrow \mathsf{KDF}(\mathsf{ms}, sid)$
return $(K, sid, \mathsf{accepted}, \varepsilon)$

$m = (A, pk_A, n, c_1, c_2, c_3, \sigma)$ ⇢

Responder Fake transcript
run *Responder Ephemeral Key Generation*, and *Initiator Key Agreement* with a modified randomness sampling and DVS generation:
$(K_1, c_1) \leftarrow\$ \mathsf{KEM}_1.\mathsf{Encaps}(\mathsf{pk}_B^{\mathsf{KEM}})$
$(K_2, c_2) \leftarrow\$ \mathsf{KEM}_2.\mathsf{Encaps}(sspk_B^{\mathsf{KEM}})$
if $epk_B \neq \perp$ $\quad (K_3, c_3) \leftarrow\$ \mathsf{KEM}_3.\mathsf{Encaps}(epk_B)$
else $\quad (K_3, c_3) \leftarrow (\varepsilon, \varepsilon)$
$\sigma \leftarrow\$ \mathsf{DVS.Sim}(sssk_B^{\mathsf{DVS}}, \mathsf{pk}_A^{\mathsf{DVS}}, sid)$
$K \leftarrow \mathsf{KDF}(\mathsf{ms}, sid)$
return $(K, m = (B, pk_B, sspk_B, epk_B, A, pk_A, n, c_1, c_2, c_3, \sigma))$

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

Comparison of initial handshake protocols

			deniability		
		PQ	strong judge	[DGK06]	full scope
X3DH	DH	✗	•	✓ [VGIK20]	✓
SC-DAKE [HKKP21]	KEM + RingSIG	✓	•	✗	✗
SC-DAKE′ [HKKP21]	+ NIZK	✓	•	✓	✗
SPQR [this work]	KEM + DVS	✓	✓	✗	✓
SI-X3DH [DG21]	SIDH	✓	•	✓	✓

✓ proven ✗ broken • conjectured to hold

full scope: real-world setting including semi-static keys

[VGIK20] Vatandas, Gennaro, Ithurburn, Krawczyk, ACNS 2020, `https://ia.cr/2020/642`

Signal goes post-quantum?

Initial Handshake

post-quantum from Key Encapsulation and Designated Verifier Signatures

deniability against strong judges

DVS from ring signatures

Double Ratchet

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

Full paper: `https://eprint.iacr.org/2021/769`

rune.fiedler@cryptoplexity.de

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.

[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.

References II

[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.

[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.

References III

[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