Security Analysis of Signal's PQXDH Handshake

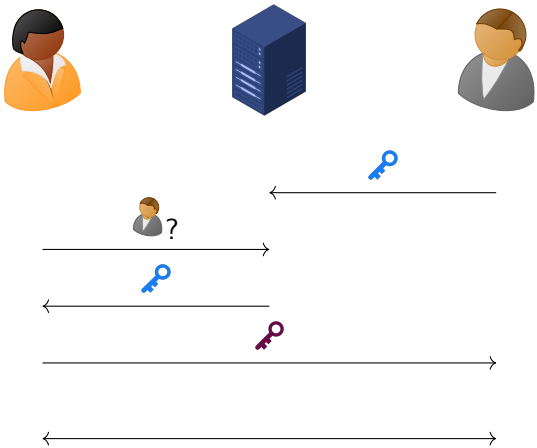
Rune Fiedler[1] Felix Günther[2]

[1]Technische Universität Darmstadt, Germany
rune.fiedler@cryptoplexity.de

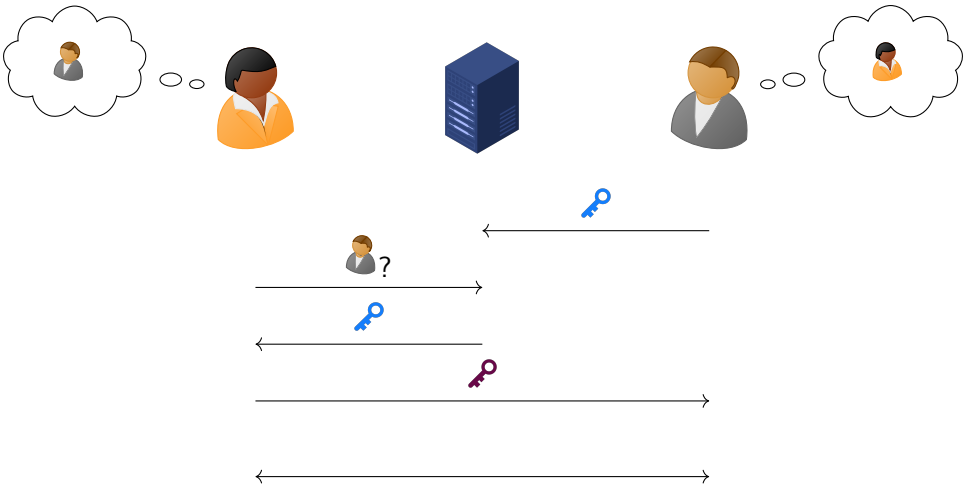
[2]IBM Research Europe – Zurich, Switzerland
mail@felixguenther.info

PKC 2025

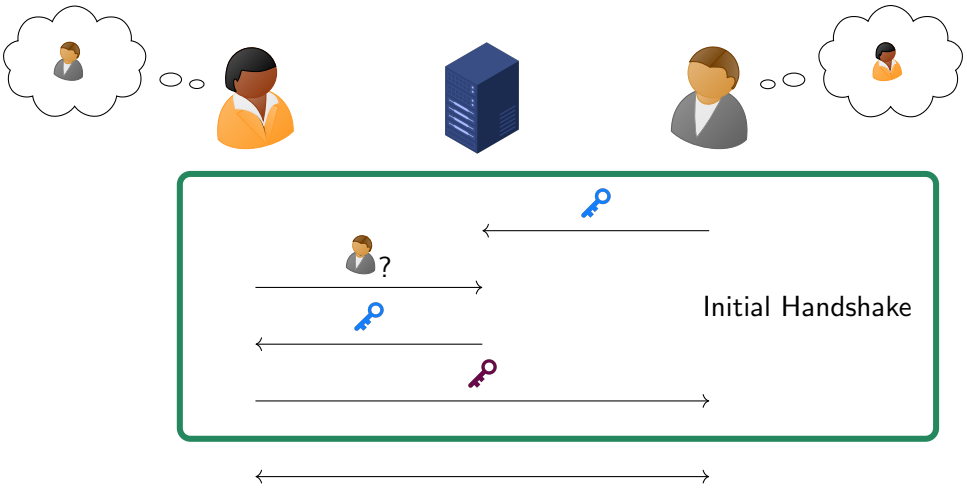
Signal: Asynchronous Authenticated Key Exchange



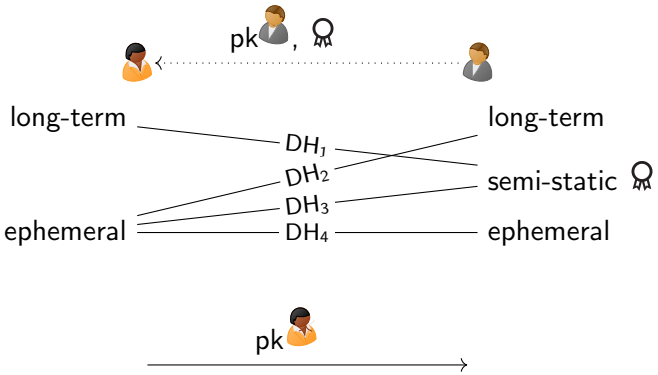
Signal: Asynchronous Authenticated Key Exchange



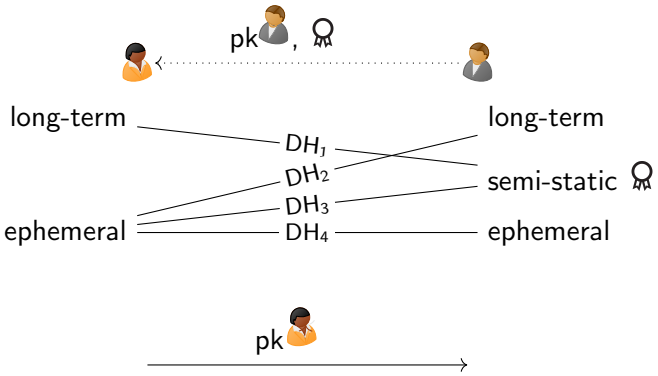
Signal: Asynchronous Authenticated Key Exchange



Signal's Initial Handshake(s): X3DH and PQXDH

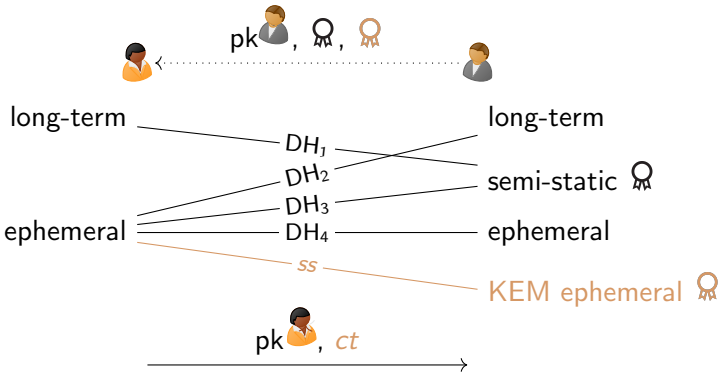


Signal's Initial Handshake(s): X3DH and PQXDH



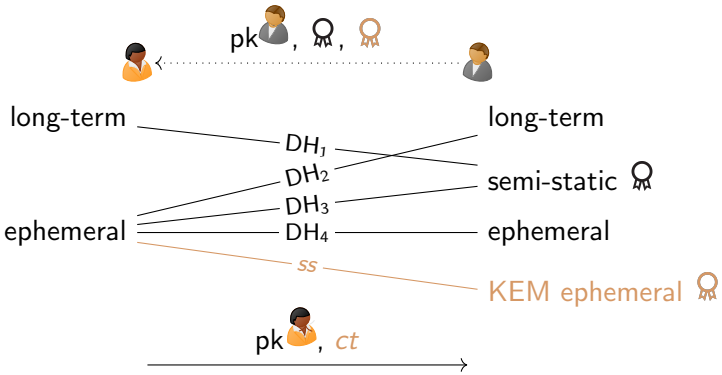
- session key: $\mathrm{KDF}(\mathrm{DH}_1 \| \ldots \| \mathrm{DH}_4 \quad)$

Signal's Initial Handshake(s): X3DH and PQXDH



- session key: $\mathsf{KDF}(\mathsf{DH}_1 \| \ldots \| \mathsf{DH}_4 \| ss)$

Signal's Initial Handshake(s): X3DH and PQXDH



- session key: $\mathrm{KDF}(\mathrm{DH}_1 \| \ldots \| \mathrm{DH}_4 \| ss)$
- reduced session: Bob without ephemeral keys, semi-static KEM

Analyses of Signal's Initial Handshake(s): X3DH and PQXDH

- reductionist analysis of X3DH [CCD+17] with a [BR94] style key-exchange model
- tool-based analysis of PQXDH with ProVerif and CryptoVerif [BJKS24]
  - (re-)discovered (potential) KEM re-encapsulation attack [CDM24]
  - corruption of long-term keys only
  - reduced mode only (without Bob's ephemeral keys)

Analyses of Signal's Initial Handshake(s): X3DH and PQXDH

- reductionist analysis of X3DH [CCD+17] with a [BR94] style key-exchange model
- tool-based analysis of PQXDH with ProVerif and CryptoVerif [BJKS24]
  - (re-)discovered (potential) KEM re-encapsulation attack [CDM24]
  - corruption of long-term keys only
  - reduced mode only (without Bob's ephemeral keys)

- our work
  - follows [CCD+17, BFG+22] but explicitly models signatures (albeit with distinct signing keys)
  - identifies precise requirements of the KEM
  - models maximum-exposure with clean predicates

Concrete Bound for PQXDH against classical adversaries

$$\mathrm{Adv}^{\mathrm{KI}}_{\mathrm{PQXDH}}(\mathcal{A}) \leq \frac{(n_p + n_p \cdot n_{ss} + n_s)^2}{q} + \gamma_{\mathrm{coll}} \cdot (n_p \cdot n_{ss} + n_s) + n_s \cdot \delta_{\mathrm{corr}} + \epsilon_{LEAK^{+r}}$$

$$
\begin{aligned}
&+ \left(n_p \cdot (\epsilon_{\mathrm{SIG}} + n_p \cdot n_{ss} \cdot \epsilon_{\mathrm{GDH}})\right) && /\!/\ \mathrm{clean}_{\text{LT-SS}} \\
&+ \left(n_s \cdot n_p \cdot \epsilon_{\mathrm{GDH}}\right) && /\!/\ \mathrm{clean}_{\text{E-LT}} \\
&+ \left(n_p \cdot (\epsilon_{\mathrm{SIG}} + n_{ss} \cdot n_s \cdot \epsilon_{\mathrm{GDH}})\right) && /\!/\ \mathrm{clean}_{\text{E-SS}} \wedge \mathrm{type} = \mathrm{full} \\
&+ \left(n_p \cdot \left(\epsilon_{\mathrm{SIG}} + n_{ss} \cdot n_s \cdot \min(\epsilon_{\mathrm{GDH}}, \epsilon^{\mathrm{OW}}_{\mathrm{CCA}})\right)\right) && /\!/\ \mathrm{clean}_{\text{E-SS}} \wedge \mathrm{type} = \mathrm{reduced} \\
&+ \left(n_s^2 \cdot \min(\epsilon_{\mathrm{GDH}}, \epsilon^{\mathrm{OW}}_{\mathrm{CCA}})\right) && /\!/\ \mathrm{clean}_{\text{E-E}} \wedge \mathrm{clean}_{\mathrm{peerE}} \\
&+ \left(n_p \cdot \left(\epsilon_{\mathrm{SIG}} + n_s^2 \cdot q_{\mathrm{RO}} \cdot \epsilon^{\mathrm{OW}}_{\mathrm{CCA}}\right)\right) && /\!/\ \mathrm{clean}_{\text{E-E}} \wedge \mathrm{clean}_{\mathrm{sigE}}
\end{aligned}
$$

Concrete Bound for PQXDH against classical adversaries

$$\mathrm{Adv}^{\mathrm{KI}}_{\mathrm{PQXDH}}(\mathcal{A}) \leq \frac{(n_p + n_p \cdot n_{ss} + n_s)^2}{q} + \gamma_{\mathrm{coll}} \cdot (n_p \cdot n_{ss} + n_s) + n_s \cdot \delta_{\mathrm{corr}} + \epsilon_{LEAK^{+r}}$$

$$+ (n_p \cdot (\epsilon_{\mathrm{SIG}} + n_p \cdot n_{ss} \cdot \epsilon_{\mathrm{GDH}})) \quad // \ \mathrm{clean}_{\text{LT-SS}}$$

$$+ (n_s \cdot n_p \cdot \epsilon_{\mathrm{GDH}}) \quad // \ \mathrm{clean}_{\text{E-LT}}$$

$$+ (n_p \cdot (\epsilon_{\mathrm{SIG}} + n_{ss} \cdot n_s \cdot \epsilon_{\mathrm{GDH}})) \quad // \ \mathrm{clean}_{\text{E-SS}} \wedge \mathrm{type} = \mathrm{full}$$

$$+ \left(n_p \cdot \left(\epsilon_{\mathrm{SIG}} + n_{ss} \cdot n_s \cdot \min(\epsilon_{\mathrm{GDH}}, \epsilon^{\mathrm{OW}}_{\mathrm{CCA}})\right)\right) \quad // \ \mathrm{clean}_{\text{E-SS}} \wedge \mathrm{type} = \mathrm{reduced}$$

$$+ \left(n_s^2 \cdot \min(\epsilon_{\mathrm{GDH}}, \epsilon^{\mathrm{OW}}_{\mathrm{CCA}})\right) \quad // \ \mathrm{clean}_{\text{E-E}} \wedge \mathrm{clean}_{\mathrm{peerE}}$$

$$+ \left(n_p \cdot \left(\epsilon_{\mathrm{SIG}} + n_s^2 \cdot q_{\mathrm{RO}} \cdot \epsilon^{\mathrm{OW}}_{\mathrm{CCA}}\right)\right) \quad // \ \mathrm{clean}_{\text{E-E}} \wedge \mathrm{clean}_{\mathrm{sigE}}$$

Concrete Bound for PQXDH against classical adversaries

$$\mathrm{Adv}^{\mathrm{KI}}_{\mathrm{PQXDH}}(\mathcal{A}) \leq \frac{(n_p + n_p \cdot n_{ss} + n_s)^2}{q} + \gamma_{\mathrm{coll}} \cdot (n_p \cdot n_{ss} + n_s) + n_s \cdot \delta_{\mathrm{corr}} + \epsilon_{LEAK^{+r}}$$

$$
\begin{array}{ll}
+ \left(n_p \cdot \left(\epsilon_{\mathrm{SIG}} + n_p \cdot n_{ss} \cdot \epsilon_{\mathrm{GDH}}\right)\right) & /\!/ \ \mathrm{clean}_{\text{LT-SS}} \\
+ \left(n_s \cdot n_p \cdot \epsilon_{\mathrm{GDH}}\right) & /\!/ \ \mathrm{clean}_{\text{E-LT}} \\
+ \left(n_p \cdot \left(\epsilon_{\mathrm{SIG}} + n_{ss} \cdot n_s \cdot \epsilon_{\mathrm{GDH}}\right)\right) & /\!/ \ \mathrm{clean}_{\text{E-SS}} \wedge \mathrm{type} = \mathrm{full} \\
+ \left(n_p \cdot \left(\epsilon_{\mathrm{SIG}} + n_{ss} \cdot n_s \cdot \min(\epsilon_{\mathrm{GDH}}, \epsilon^{\mathrm{OW}}_{\mathrm{CCA}})\right)\right) & /\!/ \ \mathrm{clean}_{\text{E-SS}} \wedge \mathrm{type} = \mathrm{reduced} \\
+ \left(n_s^2 \cdot \min(\epsilon_{\mathrm{GDH}}, \epsilon^{\mathrm{OW}}_{\mathrm{CCA}})\right) & /\!/ \ \mathrm{clean}_{\text{E-E}} \wedge \mathrm{clean}_{\text{peerE}} \\
+ \left(n_p \cdot \left(\epsilon_{\mathrm{SIG}} + n_s^2 \cdot q_{\mathrm{RO}} \cdot \epsilon^{\mathrm{OW}}_{\mathrm{CCA}}\right)\right) & /\!/ \ \mathrm{clean}_{\text{E-E}} \wedge \mathrm{clean}_{\text{sigE}}
\end{array}
$$

Concrete Bound for PQXDH against classical adversaries

$$\mathrm{Adv}^{\mathrm{KI}}_{\mathrm{PQXDH}}(\mathcal{A}) \leq \frac{(n_p + n_p \cdot n_{ss} + n_s)^2}{q} + \gamma_{\mathrm{coll}} \cdot (n_p \cdot n_{ss} + n_s) + n_s \cdot \delta_{\mathrm{corr}} + \epsilon_{LEAK^{+r}}$$

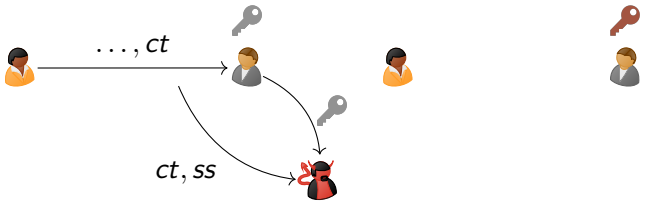
$$\begin{aligned}
&+ (n_p \cdot (\epsilon_{\mathrm{SIG}} + n_p \cdot n_{ss} \cdot \epsilon_{\mathrm{GDH}})) && /\!/\ \mathrm{clean}_{\text{LT-SS}} \\
&+ (n_s \cdot n_p \cdot \epsilon_{\mathrm{GDH}}) && /\!/\ \mathrm{clean}_{\text{E-LT}} \\
&+ (n_p \cdot (\epsilon_{\mathrm{SIG}} + n_{ss} \cdot n_s \cdot \epsilon_{\mathrm{GDH}})) && /\!/\ \mathrm{clean}_{\text{E-SS}} \wedge \mathrm{type} = \mathrm{full} \\
&+ \left(n_p \cdot \left(\epsilon_{\mathrm{SIG}} + n_{ss} \cdot n_s \cdot \min(\epsilon_{\mathrm{GDH}}, \epsilon^{\mathrm{OW}}_{\mathrm{CCA}})\right)\right) && /\!/\ \mathrm{clean}_{\text{E-SS}} \wedge \mathrm{type} = \mathrm{reduced} \\
&+ \left(n_s^2 \cdot \min(\epsilon_{\mathrm{GDH}}, \epsilon^{\mathrm{OW}}_{\mathrm{CCA}})\right) && /\!/\ \mathrm{clean}_{\text{E-E}} \wedge \mathrm{clean}_{\mathrm{peerE}} \\
&+ \left(n_p \cdot \left(\epsilon_{\mathrm{SIG}} + n_s^2 \cdot q_{\mathrm{RO}} \cdot \epsilon^{\mathrm{OW}}_{\mathrm{CCA}}\right)\right) && /\!/\ \mathrm{clean}_{\text{E-E}} \wedge \mathrm{clean}_{\mathrm{sigE}}
\end{aligned}$$

KEM Re-Encapsulation Attack [CDM24, BJKS24]

- two sessions with same DH public keys, distinct KEM keys, both reduced

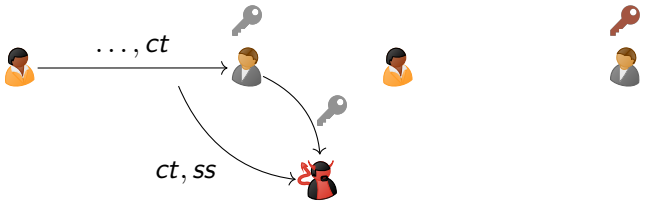
KEM Re-Encapsulation Attack [CDM24, BJKS24]

- two sessions with same DH public keys, distinct KEM keys, both reduced



KEM Re-Encapsulation Attack [CDM24, BJKS24]

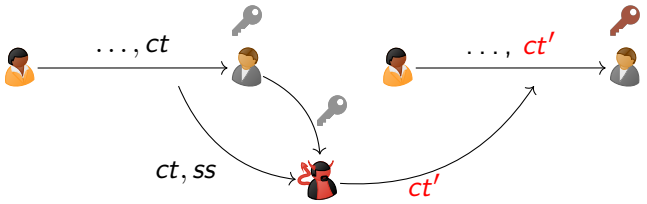
- two sessions with same DH public keys, distinct KEM keys, both reduced



$\underline{KEM.encaps(\mathrm{pk}):}$
$ss \leftarrow \{0,1\}^{256}$
$ct \leftarrow PKE.encrypt(\mathrm{pk}, ss)$
return (ct, ss)

KEM Re-Encapsulation Attack [CDM24, BJKS24]

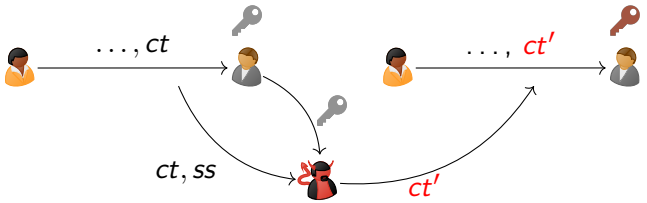
- two sessions with same DH public keys, distinct KEM keys, both reduced



$\underline{KEM.encaps(\mathrm{pk}):}$
$ss \leftarrow \{0,1\}^{256}$
$ct \leftarrow PKE.encrypt(\mathrm{pk}, ss)$
return (ct, ss)

KEM Re-Encapsulation Attack [CDM24, BJKS24]

- two sessions with same DH public keys, distinct KEM keys, both reduced

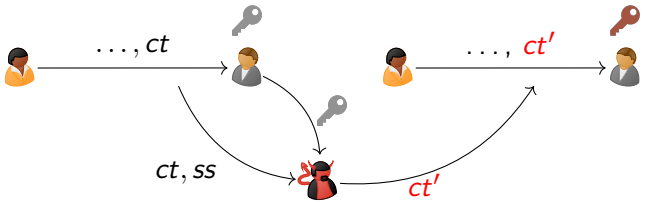


$\underline{KEM.encaps(\mathrm{pk}):}$
$ss \leftarrow \{0,1\}^{256}$
$ct \leftarrow PKE.encrypt(\mathrm{pk}, ss)$
return (ct, ss)

session key: $\mathrm{KDF}(\mathrm{DH}_1 \| \ldots \| \mathrm{DH}_4 \| ss)$

KEM Re-Encapsulation Attack [CDM24, BJKS24]

- two sessions with same DH public keys, distinct KEM keys, both reduced



$\underline{KEM.encaps(\mathrm{pk}):}$
$ss \leftarrow \{0,1\}^{256}$
$ct \leftarrow PKE.encrypt(\mathrm{pk}, ss)$
return (ct, ss)

session key: $\mathrm{KDF}(\mathrm{DH}_1 \| \ldots \| \mathrm{DH}_4 \| ss)$

- $\Rightarrow$ two sessions with same session key: adversary can reveal one and test the other
- proposed protocol fix: session context (KEM public key, ciphertext) in key derivation
- which KEM property needed?

KEM Binding Notion $LEAK^{+r}$-BIND-SS-$\{CT, PK\}$ (extending [CDM24])

$((\mathsf{pk}, \mathsf{sk}, r)_1, \ldots, (\mathsf{pk}, \mathsf{sk}, r)_n)$

KEM Binding Notion $LEAK^{+r}$-BIND-SS-$\{CT, PK\}$ (extending [CDM24])

$((\mathsf{pk}, \mathsf{sk}, r)_1, \ldots, (\mathsf{pk}, \mathsf{sk}, r)_n)$

$(\mathsf{pk}_i, ct_i) \neq (\mathsf{pk}_j, ct_j)$

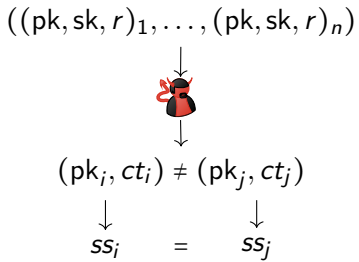
KEM Binding Notion $LEAK^{+r}$-BIND-SS-$\{CT, PK\}$ (extending [CDM24])

$((\mathsf{pk}, \mathsf{sk}, r)_1, \ldots, (\mathsf{pk}, \mathsf{sk}, r)_n)$

$(\mathsf{pk}_i, ct_i) \neq (\mathsf{pk}_j, ct_j)$

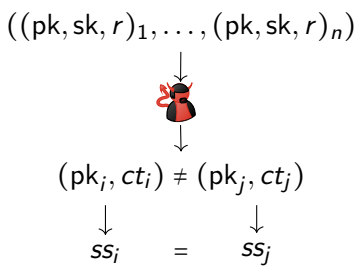
$ss_i \quad = \quad ss_j$

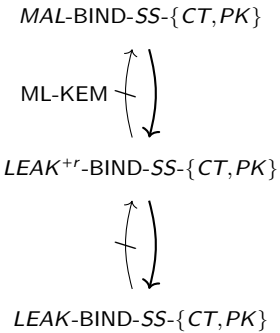
KEM Binding Notion $LEAK^{+r}$-BIND-SS-$\{CT, PK\}$ (extending [CDM24])



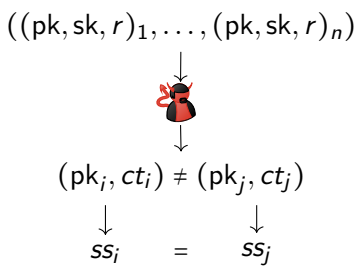
$LEAK^{+r}$-BIND-SS-$\{CT, PK\}$

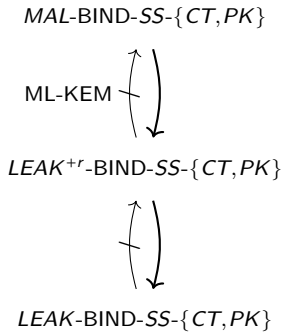
KEM Binding Notion $LEAK^{+r}$-BIND-SS-$\{CT, PK\}$ (extending [CDM24])





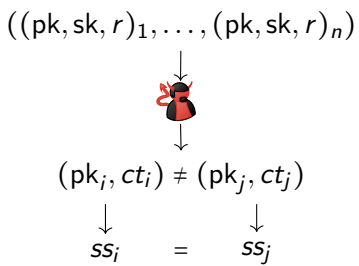
KEM Binding Notion $LEAK^{+r}$-BIND-SS-$\{CT, PK\}$ (extending [CDM24])

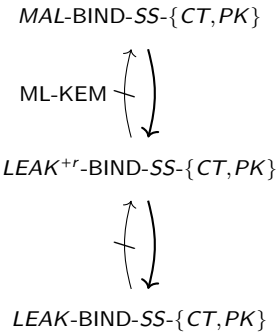




Signal: Kyber ✓
ML-KEM ✓

KEM Binding Notion $LEAK^{+r}$-BIND-SS-$\{CT, PK\}$ (extending [CDM24])





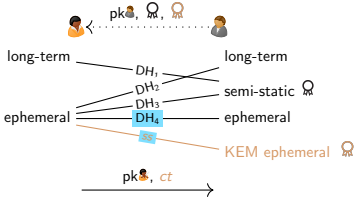
Signal: Kyber ✓
ML-KEM ✓

- related notion: SH-CR [BJKS24] is incomparable

Concrete Hybrid Bound for PQXDH against classical adversaries

$$\mathsf{Adv}^{\mathsf{KI}}_{\mathsf{PQXDH}}(\mathcal{A}) \leq \frac{(n_p + n_p \cdot n_{ss} + n_s)^2}{q} + \gamma_{\mathsf{coll}} \cdot (n_p \cdot n_{ss} + n_s) + n_s \cdot \delta_{\mathsf{corr}} + \epsilon_{LEAK^{+r}}$$

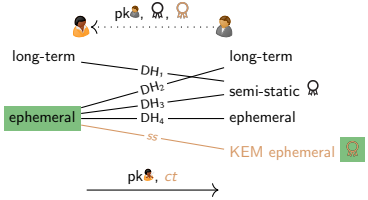
$$+ (n_p \cdot (\epsilon_{\mathsf{SIG}} + n_p \cdot n_{ss} \cdot \epsilon_{\mathsf{GDH}})) \quad // \ \mathsf{clean}_{\text{LT-SS}}$$
$$+ (n_s \cdot n_p \cdot \epsilon_{\mathsf{GDH}}) \quad // \ \mathsf{clean}_{\text{E-LT}}$$
$$+ (n_p \cdot (\epsilon_{\mathsf{SIG}} + n_{ss} \cdot n_s \cdot \epsilon_{\mathsf{GDH}})) \quad // \ \mathsf{clean}_{\text{E-SS}} \wedge \text{type = full}$$
$$+ \left(n_p \cdot \left(\epsilon_{\mathsf{SIG}} + n_{ss} \cdot n_s \cdot \min(\epsilon_{\mathsf{GDH}}, \epsilon^{\mathsf{OW}}_{\mathsf{CCA}})\right)\right) \quad // \ \mathsf{clean}_{\text{E-SS}} \wedge \text{type = reduced}$$
$$+ \left(n_s^2 \cdot \min(\epsilon_{\mathsf{GDH}}, \epsilon^{\mathsf{OW}}_{\mathsf{CCA}})\right) \quad // \ \mathsf{clean}_{\text{E-E}} \wedge \mathsf{clean}_{\text{peerE}}$$
$$+ \left(n_p \cdot \left(\epsilon_{\mathsf{SIG}} + n_s^2 \cdot q_{\mathrm{RO}} \cdot \epsilon^{\mathsf{OW}}_{\mathsf{CCA}}\right)\right) \quad // \ \mathsf{clean}_{\text{E-E}} \wedge \mathsf{clean}_{\text{sigE}}$$



Concrete Bound for PQXDH Against Active-Later-Quantum Adversaries

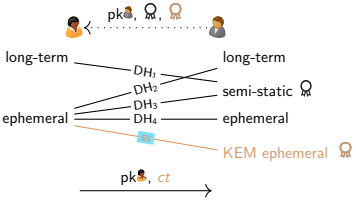
$$\mathsf{Adv}^{\mathsf{KI}}_{\mathsf{PQXDH}}(\mathcal{A}) \leq \frac{(n_p + n_p \cdot n_{ss} + n_s)^2}{q} + \gamma_{\mathsf{coll}} \cdot (n_p \cdot n_{ss} + n_s) + n_s \cdot \delta_{\mathsf{corr}} + \epsilon_{\mathit{LEAK}^{+r}}$$

$$+ (n_p \cdot (\epsilon_{\mathsf{SIG}} + n_p \cdot n_{ss} \cdot \epsilon_{\mathsf{GDH}})) \quad // \ \mathsf{clean}_{\text{LT-SS}}$$
$$+ (n_s \cdot n_p \cdot \epsilon_{\mathsf{GDH}}) \quad // \ \mathsf{clean}_{\text{E-LT}}$$
$$+ (n_p \cdot (\epsilon_{\mathsf{SIG}} + n_{ss} \cdot n_s \cdot \epsilon_{\mathsf{GDH}})) \quad // \ \mathsf{clean}_{\text{E-SS}} \wedge \text{type = full}$$
$$+ \left(n_p \cdot \left(\epsilon_{\mathsf{SIG}} + n_{ss} \cdot n_s \cdot \min(\epsilon_{\mathsf{GDH}}, \epsilon^{\mathsf{OW}}_{\mathsf{CCA}})\right)\right) \quad // \ \mathsf{clean}_{\text{E-SS}} \wedge \text{type = reduced}$$
$$+ \left(n_s^2 \cdot \min(\epsilon_{\mathsf{GDH}}, \epsilon^{\mathsf{OW}}_{\mathsf{CCA}})\right) \quad // \ \mathsf{clean}_{\text{E-E}} \wedge \mathsf{clean}_{\text{peerE}}$$
$$+ \left(n_p \cdot \left(\epsilon_{\mathsf{SIG}} + n_s^2 \cdot q_{\mathrm{RO}} \cdot \epsilon^{\mathsf{OW}}_{\mathsf{CCA}}\right)\right) \quad // \ \mathsf{clean}_{\text{E-E}} \wedge \mathsf{clean}_{\text{sigE}}$$



Concrete Bound for PQXDH Against Quantum Adversaries

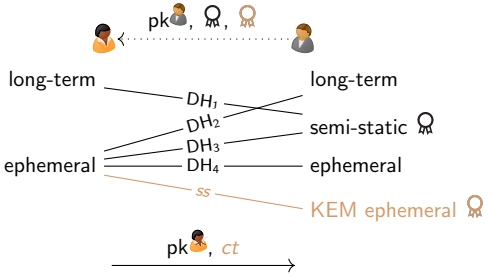
$$\mathsf{Adv}^{\mathsf{KI}}_{\mathsf{PQXDH\text{-}}Q}(\mathcal{A}) \leq \frac{(n_p + n_p \cdot n_{ss} + n_s)^2}{q} + \gamma_{\mathsf{coll}} \cdot (n_p \cdot n_{ss} + n_s) + n_s \cdot \delta_{\mathsf{corr}} + \epsilon_{LEAK^{+r}}$$
$$+ \; n_{ss} \cdot n_s \cdot (\epsilon^{\mathsf{IND}}_{\mathsf{CCA}} + \epsilon_{\mathsf{PRF}}) \qquad // \, \mathsf{clean}^{Q}_{\text{E-SS}}$$
$$+ \; n_s^2 \cdot (\epsilon^{\mathsf{IND}}_{\mathsf{CCA}} + \epsilon_{\mathsf{PRF}}), \qquad // \, \mathsf{clean}^{Q}_{\text{E-E}}$$



Design Discussion of PQXDH

- adding KEM *ss* to the KDF input achieves hybrid security
- secure against active-now-quantum-later due to signature on ephemeral KEM key
- should add context to KDF (especially KEM pk, ct) [BJKS24]
  - forgo binding assumption on KEM
  - tighter proof
- needed: domain separation on signatures against key confusion attacks
  - DH vs KEM [BJKS24]
  - ephemeral vs semi-static KEM

PQXDH Provides Hybrid Key Indistinguishability



$$\mathsf{Adv}^{\mathsf{KI}}_{\mathsf{PQXDH}}(\mathcal{A}) \le \frac{(n_p + n_p \cdot n_{ss} + n_s)^2}{q} + \gamma_{\mathsf{coll}} \cdot (n_p \cdot n_{ss} + n_s) + n_s \cdot \delta_{\mathsf{corr}} + \epsilon_{\mathit{LEAK}^{+r}}$$

$$+ (n_p \cdot (\epsilon_{\mathsf{SIG}} + n_p \cdot n_{ss} \cdot \epsilon_{\mathsf{GDH}})) \quad // \ \mathsf{clean}_{\mathsf{LT\text{-}SS}}$$
$$+ (n_s \cdot n_p \cdot \epsilon_{\mathsf{GDH}}) \quad // \ \mathsf{clean}_{\mathsf{E\text{-}LT}}$$
$$+ (n_p \cdot (\epsilon_{\mathsf{SIG}} + n_{ss} \cdot n_s \cdot \epsilon_{\mathsf{GDH}})) \quad // \ \mathsf{clean}_{\mathsf{E\text{-}SS}} \wedge \mathsf{type} = \mathsf{full}$$
$$+ \left(n_p \cdot (\epsilon_{\mathsf{SIG}} + n_{ss} \cdot n_s \cdot \min(\epsilon_{\mathsf{GDH}}, \epsilon^{\mathsf{OW}}_{\mathsf{CCA}}))\right) \quad // \ \mathsf{clean}_{\mathsf{E\text{-}SS}} \wedge \mathsf{type} = \mathsf{reduced}$$
$$+ \left(n_s^2 \cdot \min(\epsilon_{\mathsf{GDH}}, \epsilon^{\mathsf{OW}}_{\mathsf{CCA}})\right) \quad // \ \mathsf{clean}_{\mathsf{E\text{-}E}} \wedge \mathsf{clean}_{\mathsf{peerE}}$$
$$+ \left(n_p \cdot (\epsilon_{\mathsf{SIG}} + n_s^2 \cdot q_{\mathsf{RO}} \cdot \epsilon^{\mathsf{OW}}_{\mathsf{CCA}})\right) \quad // \ \mathsf{clean}_{\mathsf{E\text{-}E}} \wedge \mathsf{clean}_{\mathsf{sigE}}$$

MAL-BIND-*SS*-{*CT*,*PK*}

ML-KEM

LEAK^{+r}-BIND-*SS*-{*CT*,*PK*}

LEAK-BIND-*SS*-{*CT*,*PK*}

Signal: Kyber ✓
ML-KEM ✓

or include the session context in key derivation

$$\mathsf{Adv}^{\mathsf{KI}}_{\mathsf{PQXDH\text{-}Q}}(\mathcal{A}) \le \frac{(n_p + n_p \cdot n_{ss} + n_s)^2}{q} + \gamma_{\mathsf{coll}} \cdot (n_p \cdot n_{ss} + n_s) + n_s \cdot \delta_{\mathsf{corr}} + \epsilon_{\mathit{LEAK}^{+r}}$$

$$+ n_{ss} \cdot n_s \cdot (\epsilon^{\mathsf{IND}}_{\mathsf{FCCA}} + \epsilon_{\mathsf{PRF}}) \quad // \ \mathsf{clean}^{Q}_{\mathsf{E\text{-}SS}}$$
$$+ n_s^2 \cdot (\epsilon^{\mathsf{IND}}_{\mathsf{CCA}} + \epsilon_{\mathsf{PRF}}), \quad // \ \mathsf{clean}^{Q}_{\mathsf{E\text{-}E}}$$

eprint: 2024/702

rune.fiedler@cryptoplexity.de

References I

[BFG+22] 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.

[BJKS24] Karthikeyan Bhargavan, Charlie Jacomme, Franziskus Kiefer, and Rolfe Schmidt.
Formal verification of the PQXDH post-quantum key agreement protocol for end-to-end secure messaging.
In Davide Balzarotti and Wenyuan Xu, editors, *USENIX Security 2024: 33rd USENIX Security Symposium*, Philadelphia, PA, USA, August 14–16, 2024. USENIX Association.

[BR94] Mihir Bellare and Phillip Rogaway.
Entity authentication and key distribution.
In Douglas R. Stinson, editor, *Advances in Cryptology – CRYPTO'93*, volume 773 of *Lecture Notes in Computer Science*, pages 232–249, Santa Barbara, CA, USA, August 22–26, 1994. Springer Berlin Heidelberg, Germany.

[CCD+17] Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowling, Luke Garratt, and Douglas Stebila.
A formal security analysis of the Signal messaging protocol.
In *2017 IEEE European Symposium on Security and Privacy*, pages 451–466, Paris, France, April 26–28, 2017. IEEE Computer Society Press.

References II

[CDM24] Cas Cremers, Alexander Dax, and Niklas Medinger.
Keeping up with the KEMs: Stronger security notions for KEMs and automated analysis of KEM-based protocols.
In Bo Luo, Xiaojing Liao, Jun Xu, Engin Kirda, and David Lie, editors, *ACM CCS 2024: 31st Conference on Computer and Communications Security*, pages 1046–1060, Salt Lake City, UT, USA, October 14–18, 2024. ACM Press.

Icon References

- server icon by Alexiuz AS
- public key icon by Yannick Lung
- (KEM) secret key icon by Yannick Lung
- Signal, the Signal logo, and all related names, designs, and slogans are registered trademarks of Signal Technology Foundation.

different key lifetimes

long-term

long-term (use forever)

semi-static (use for a week)

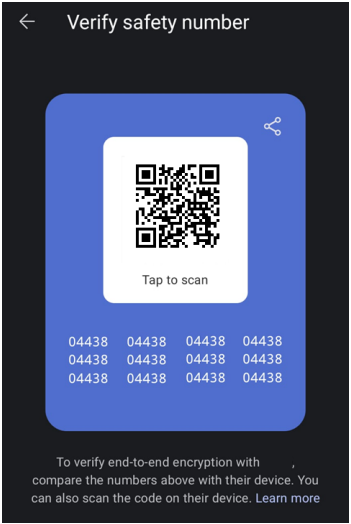
ephemeral

ephemeral (use once)

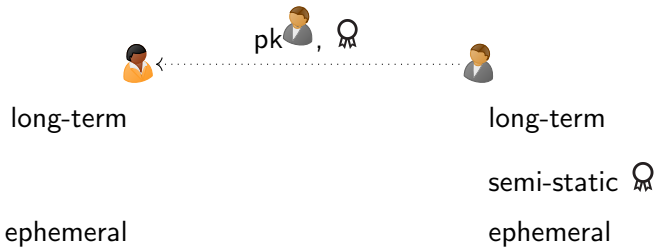
different key lifetimes

long-term	long-term (use forever)
	semi-static (use for a week)
ephemeral	ephemeral (use once)

- authenticate long-term public keys via safety number (hash of both long-term public keys)

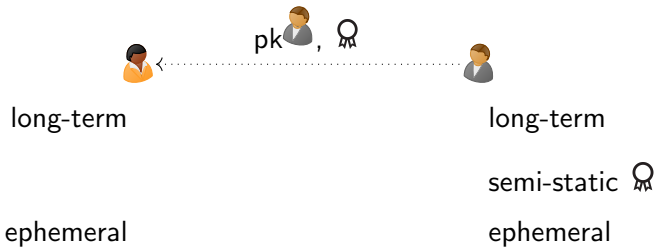


pre-key bundle



- Bob uploads semi-static key, signature, and ephemeral keys to key server

pre-key bundle



- Bob uploads semi-static key, signature, and ephemeral keys to key server
- all key pairs are DH
- long-term keys additionally for a signature scheme