K-Waay: Fast and Deniable Post-Quantum X3DH without Ring Signatures

Daniel Collins[1], Loïs Huguenin-Dumittan[1], Ngoc Khanh Nguyen[1], Nicolas Rolin[2], Serge Vaudenay[1]

[1]EPFL, [2]Spuerkeess

[Paper under submission]

Background: X3DH-Like Key Exchange

- Used for authenticated key exchange (AKE) in Signal, WhatsApp, etc. alongside the Double Ratchet.
- Deniable [VGIK20] but not post-quantum (PQ).
- [HKKP21, HKKP22] and [BFGJS22] propose deniable and PQ X3DH-like algorithms.

  - Each rely on ring/designated verifier signatures.
- Split-KEM [BFGJS20]: KEM, but Encaps and Decaps take as input caller’s secret key and counterpart’s public key.

Results (1/5): LWE-based Split-KEM

- Revisit split-KEM: its original security notions are *insufficient* to build X3DH-like DAKE.
- Define appropriate authenticity and deniability notions.
- Propose plain LWE-based instantiation.
- Technically:
  - Reduction to LWE from extended LWE-like assumption [AP12].
  - Proofs in the QROM (unlike many existing ring signatures).

Results (2/5): K-Waay

- **Propose K-Waay: deniable PQ X3DH based on split-KEM.**
- **Deniability strengthens [BFGJS22]'s notion.**
- **Key indistinguishability (AKE security): stronger than weak forward security.**
- **Uses split-KEM with ephemeral-ephemeral keys, ephemeral KEM, long-term KEM and signatures for prekeys.**

Results (3/5): Relationships Between Primitives

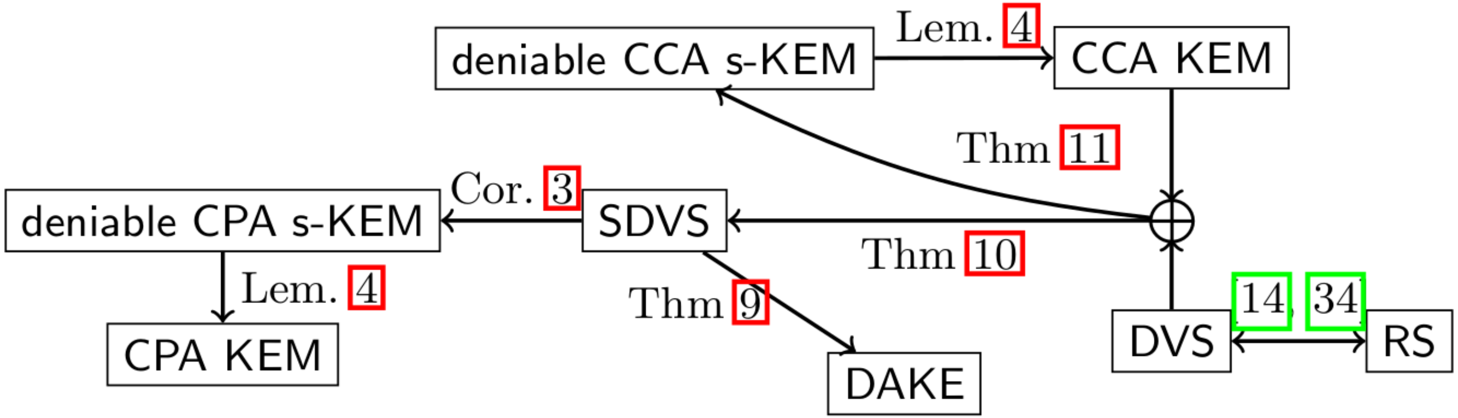
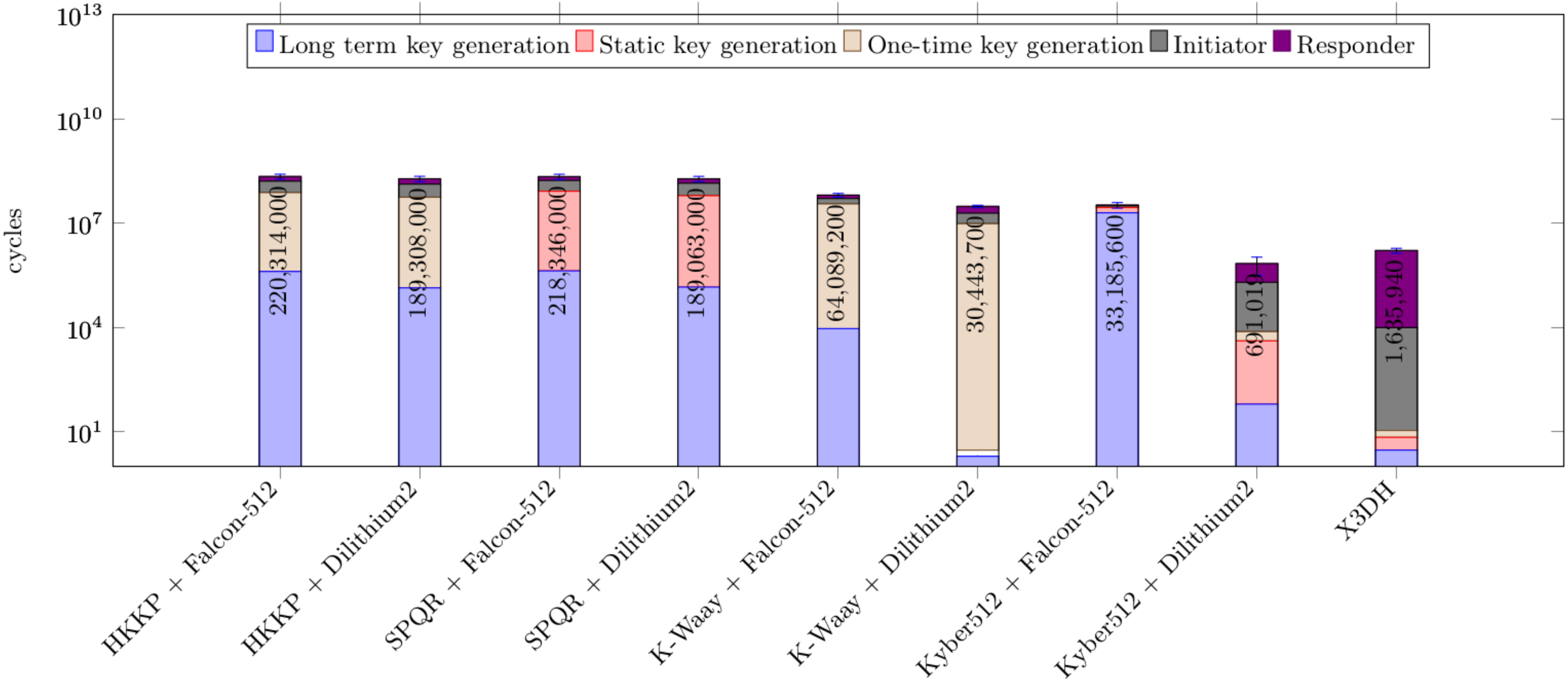
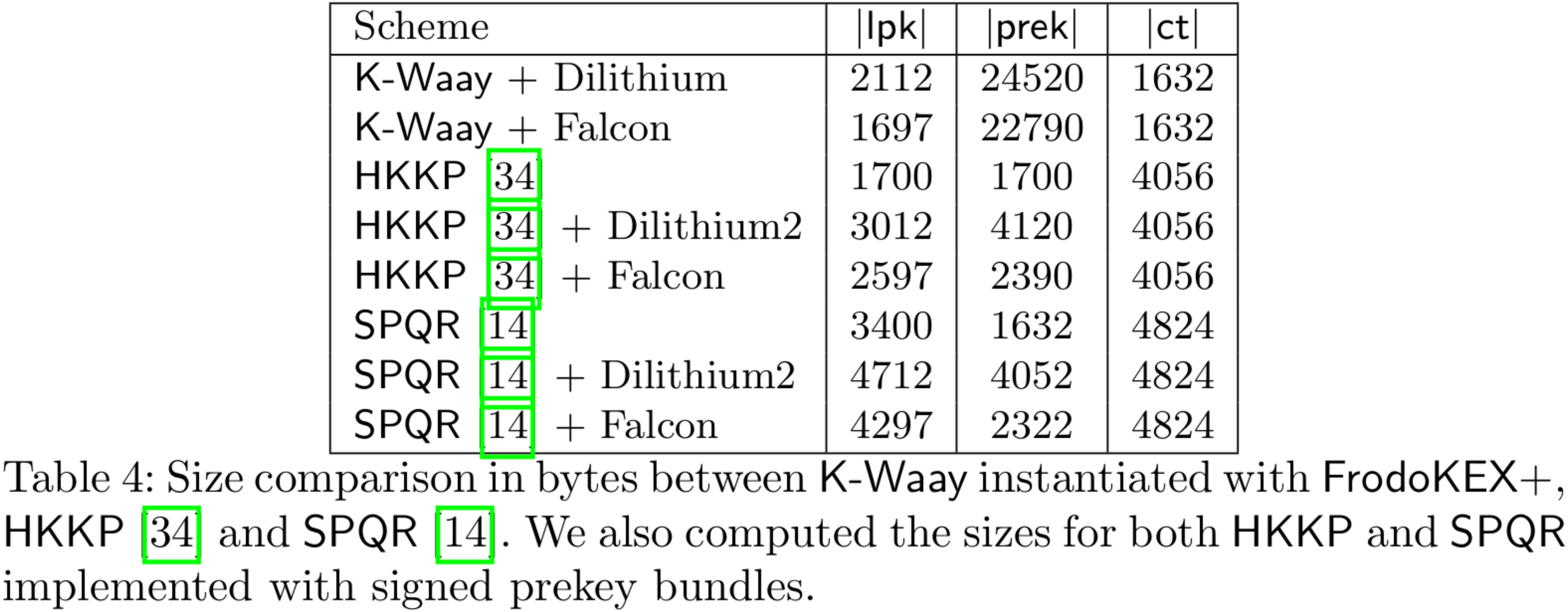


Fig. 1: Relations between primitives related to X3DH-like AKE. RS stands for ring signatures, s-KEM for split-KEM, and (S)DVS for (strong) designated verifier signature. CPA (resp. CCA) stands for IND-CPA (resp. IND-CCA) when it is linked to a KEM and to UNF-1KMA/IND-CPA (resp. UNF-CCA/IND-CCA) when it is linked to a split-KEM.

Results (4/5): Speed Benchmarks



Results (5/5): Space Benchmarks (SPQR = [BFGJS22])



Scheme	|lpk|	|prek|	|ct|
K-Waay + Dilithium	2112	24520	1632
K-Waay + Falcon	1697	22790	1632
HKKP [34]	1700	1700	4056
HKKP [34] + Dilithium2	3012	4120	4056
HKKP [34] + Falcon	2597	2390	4056
SPQR [14]	3400	1632	4824
SPQR [14] + Dilithium2	4712	4052	4824
SPQR [14] + Falcon	4297	2322	4824

Table 4: Size comparison in bytes between K-Waay instantiated with FrodoKEX+, HKKP [34] and SPQR [14]. We also computed the sizes for both HKKP and SPQR implemented with signed prekey bundles.

Conclusion

- Propose K-Waay: deniable PQ X3DH based on split-KEM.
- Future work: split-KEM from structured lattices, more efficient one-time ring signatures…
- Paper in submission: watch this space!

References

- [AP12]: Alperin-Sheriff, Peikert: *Circular and KDM Security for Identity-Based Encryption*, PKC 2012
- [BFGJS20]: Brendel, Fischlin, Günther, Janson, Stebila: *Towards post-quantum security for signal’s X3DH handshake*, SAC 2020
- [VGIK20]: Vatandas, Gennaro, Ithurburn, Krawczyk: *On the Cryptographic Deniability of the Signal Protocol*, ACNS 2020
- [HKKP21/22]: Hashimoto, Katsumata, Kwiatkowski, Prest: *An Efficient and Generic Construction for Signal's Handshake (X3DH): Post-Quantum, State Leakage Secure, and Deniable*, PKC 2021/JoC 2022
- [BFGJS22]: Brendel, Fiedler, Günther, Janson, Stebila: *Post-quantum Asynchronous Deniable Key Exchange and the Signal Handshake*, PKC 2022