SHADOWFAX: Hybrid Security and Deniability for AKEMs

Phillip Gajland[1], **Vincent Hwang**[2, 3], **Jonas Janneck**[4]

[1] IBM Research – Zurich
[2] Max Planck Institute for Security and Privacy
[3] Radboud University
[4] Ruhr University Bochum

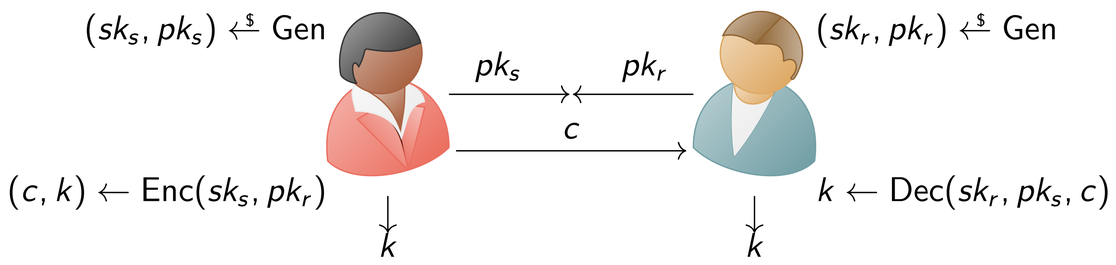
https://ia.cr/2025/154

ARTIFACT EVALUATED USENIX AVAILABLE | ARTIFACT EVALUATED USENIX FUNCTIONAL | ARTIFACT EVALUATED USENIX REPRODUCED

Motivation & Contributions

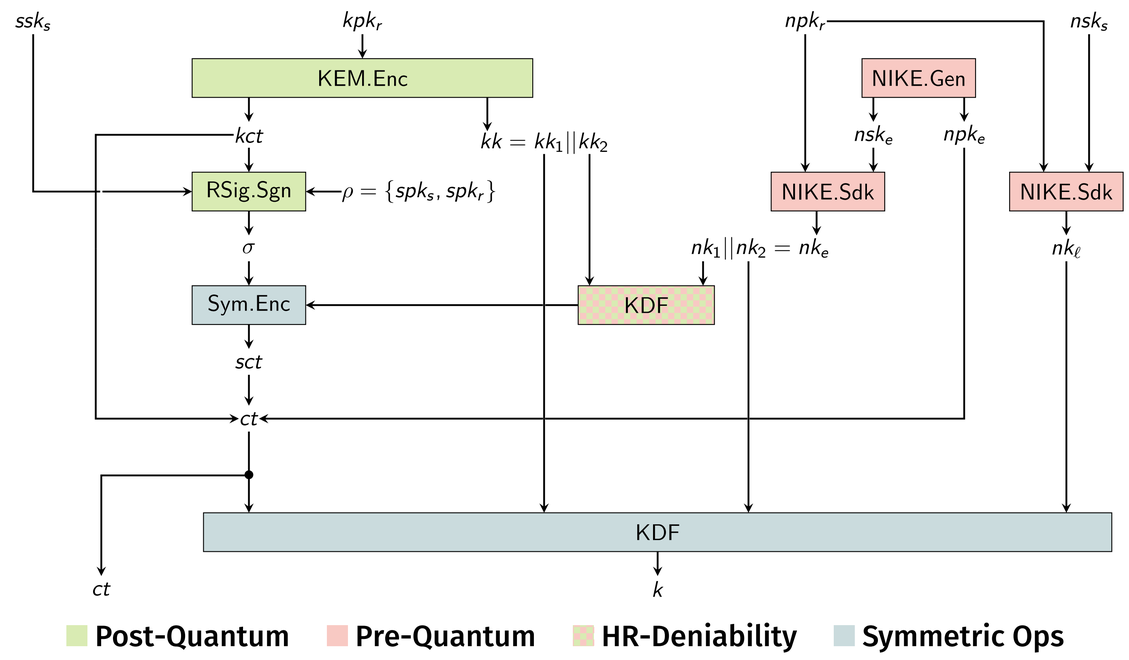
- **Authenticated key encapsulation mechanisms (AKEMs) combine confidentiality and authenticity in one primitive; AKEMs formalise authenticated HPKE.**

What is an AKEM?



- **Pre-quantum AKEMs, such as in HPKE, also had deniability (implicitly); We formalised it [II]. Post-quantum AKEMs using standard signatures and KEMs lose deniability.**
- **Deniability is important for messaging (X3DH).**
- **Hybrid Security: Combines pre-quantum and post-quantum assumptions.**
- **Existing solutions: quantum-vulnerable or no deniability or huge sizes.**

- **Goal: Hybrid AKEM with deniability and efficiency.**
- **Black-box combiner: Preserves deniability when both AKEMs are deniable.**
- **SHADOWFAX : Hybrid AKEM with deniability, confidentiality, and authenticity, assuming at least one pre- or post-quantum assumption holds.**



Shadowfax instantiations: Hybrid AKEM with deniability

- **SHADOWFAX is a generic AKEM construction combining: pre-quantum non-interactive key exchange (NIKE) + post-quantum key encapsulation mechanism (KEM) + post-quantum ring signature scheme RSig (with information-theoretic anonymity).**
- **We instantiate SHADOWFAX with our generic ring signature GANDALF [II], which admits instantiations that either minimize size or rely exclusively on NIST-standardised building blocks.**

Scheme	Instantiation	Confidentiality	Authenticity	Deniability	Assumption		Size (bytes)	
					pre-Q	post-Q	c	pk
DH-AKEM [5]	X25519	✓	✓	**DR***	✓	✗	32	32
ETSTH-AKEM [IV]	bat_257_542 + Antrag			✗	✗	✓	1 119	1 417
	ML-KEM-512 + Falcon-512						1 434	1 697
NIKE-AKEM [IV]	Swoosh [III]			**DR***	✗	✓	> 221 184	> 221 184
FrodoKEX+ [7]	n/a			**DR**	✗	✓	72	21 300
PQ-AKEM [II]	compact = bat_257_542 + GANDALF [Antrag, Mitaka]			**HR & DR**	✗	✓	1 749	1 417
	standardised = ML-KEM-512 + GANDALF [Falcon-512, Falcon-512]						2 044	1 697
SHADOWFAX [I]	compact = X25519 + bat_257_542 + GANDALF [Antrag, Mitaka]			**HR & DR**	✓	✓	1 781	1 449
	standardised = X25519 + ML-KEM-512 + GANDALF [Falcon-512, Falcon-512]						2 076	1 729

Legend: DR = Dishonest Receiver, HR = Honest Receiver, DR* = not formally proven.

Performance

Cycle counts (in kilocycles) and time (in milliseconds) on a Firestorm core of an Apple M1 Pro running at 3GHz.

AKEM	Gen		Encaps		Decaps	
	kcc	ms	kcc	ms	kcc	ms
DH-AKEM [X25519]	227	0.08	679	0.23	457	0.15
PQ-AKEM (compact)	24 851	8.28	1 155	0.39	302	0.10
PQ-AKEM (standardised)	12 462	4.15	1 009	0.34	292	0.10
SHADOWFAX (compact)	25 193	8.40	1 868	0.62	748	0.25
SHADOWFAX (standardised)	12 733	4.24	1 682	0.56	735	0.24
RSig	**Gen**		**Sign**		**Verify**	
	kcc	ms	kcc	ms	kcc	ms
RAPTOR [6]	71 420	23.81	7 980	2.66	505	0.17
GANDALF (compact)	13 009	4.34	1 008	0.34	97	0.03
GANDALF (standardised)	12 295	4.10	838	0.28	97	0.03

Key Takeaways

- **Hybrid AKEM with both post-quantum security and deniability.**
- **Compact: <1.8 KB ciphertexts and <1.5KB public keys.**
- **Practical performance: <1ms encapsulation/decapsulation.**

Select References

[I] P. Gajland, V. Hwang, J. Janneck. *Shadowfax: Hybrid Security and Deniability for AKEMs*. USENIX 2026.

[II] P. Gajland, J. Janneck, E. Kiltz. *Ring Signatures for Deniable AKEM: Gandalf's Fellowship*. CRYPTO 2024.

[III] P. Gajland, B. de Kock, M. Quaresma, G. Malavolta, P. Schwabe. *SWOOSH: Efficient Lattice-Based Non-Interactive Key Exchange*. USENIX Security, 2024.

[IV] J. Alwen, J. Janneck, E. Kiltz, B. Lipp. *The Pre-Shared Key Modes of HPKE*. ASIACRYPT, 2023.

[5] J. Alwen, B. Blanchet, E. Hauck, E. Kiltz, B. Lipp, D. Riepel. *Analysing the HPKE Standard*. EUROCRYPT, 2021.

[6] X. Lu, M. H. Au, Z. Zhang. *Raptor: A Practical Lattice-Based (Linkable) Ring Signature*. ACNS, 2019.

[7] D. Collins, L. Huguenin-Dumittan, N. K. Nguyen, N. Rolin, S. Vaudenay. *K-Waay: Fast and Deniable Post-Quantum X3DH without Ring Signatures*. USENIX, 2024.