SHADOWFAX: Hybrid Security and Deniability for AKEMs

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

[1] IBM Research Europe – Zurich

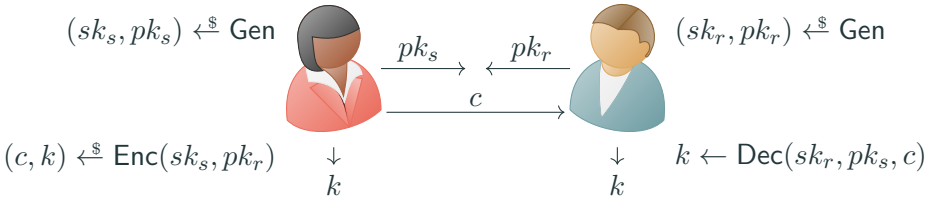
[2] Max Planck Institute for Security and Privacy

[3] Radboud University

[4] Ruhr University Bochum

35th USENIX Security Symposium 2026, Baltimore, MD, USA.

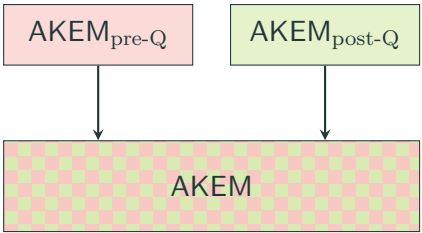
WHAT IS AN AKEM?



- AKEM combines **confidentiality** and **authenticity** into one-shot primitive
- Formalises HPKE standard's `auth` modes
- **Deniability:** Bob knows Alice sent c, but cannot prove it to others
- Many AKEM constructions also have deniability

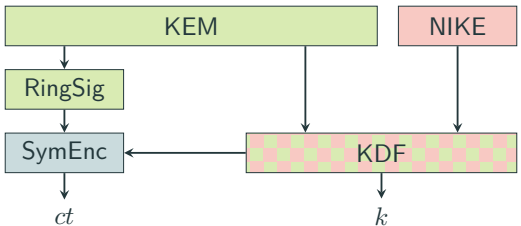
Security Properties:

- **Confidentiality:**
  $\mathsf{AKEM}_{\text{pre-Q}} \vee \mathsf{AKEM}_{\text{post-Q}} \implies \mathsf{AKEM}$ ✓
- **Authenticity:**
  $\mathsf{AKEM}_{\text{pre-Q}} \vee \mathsf{AKEM}_{\text{post-Q}} \implies \mathsf{AKEM}$ ✓
- **Deniability:**
  $\mathsf{AKEM}_{\text{pre-Q}} \wedge \mathsf{AKEM}_{\text{post-Q}} \implies \mathsf{AKEM}$ ✗



Solution: Construct from lower-level primitives, not directly from AKEMs!

SHADOWFAX: HYBRID AKEM CONSTRUCTION (SIMPLIFIED)

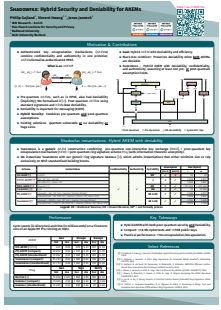


- **Idea:** Encrypt ring signature with KEM key **and** ephemeral NIKE key
- **Deniability:** $\mathsf{NIKE}_{\text{pre-Q}} \vee \mathsf{KEM}_{\text{post-Q}} \implies \mathsf{AKEM}$ ✓

Results & poster invitation

Scheme	Instantiation	Confidentiality	Authenticity	Deniability	Assumption		Size (bytes)	
					pre-Q	post-Q	c	pk
DH-AKEM [ABH+21]	X25519	✓	✓	DR*	✓	✗	32	32
EtStH-AKEM [AJKL23]	bat_257_542 + Antrag			✗	✗	✓	1 119	1 417
	ML-KEM-512 + Falcon-512						1 434	1 697
NIKE-AKEM [AJKL23]	Swoosh [GdKQ+24]			DR*	✗	✓	> 221 184	> 221 184
FrodoKEX+ [CHN+24]	n/a			DR	✗	✓	72	21 300
PQ-AKEM [GJK24]	bat_257_542 + Gandalf [Antrag, Mitaka]			HR & DR	✗	✓	1 749	1 417
	ML-KEM-512 + Gandalf [Falcon-512, Falcon-512]						2 044	1 697
Shadowfax [GHJ25]	X25519 + bat_257_542 + Gandalf [Antrag, Mitaka]			HR & DR	✓	✓	1 781	1 449
	X25519 + ML-KEM-512 + Gandalf [Falcon-512, Falcon-512]						2 076	1 729

- **Compact:** 1.8KB ciphertexts, 1.4KB public keys
- 100× smaller than alternatives (e.g., Swoosh >200KB)
- **Performance:** <1ms encapsulation/decapsulation
- Portable implementations available
- **Visit our poster!**



ARTIFACT EVALUATED USENIX AVAILABLE

ARTIFACT EVALUATED USENIX FUNCTIONAL

ARTIFACT EVALUATED USENIX REPRODUCED

ia.cr/2025/154

[ABH+21] Joël Alwen, Bruno Blanchet, Eduard Hauck, Eike Kiltz, Benjamin Lipp, and Doreen Riepel. Analysing the HPKE standard. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021, Part I*, volume 12696 of *Lecture Notes in Computer Science*, pages 87–116, Zagreb, Croatia, October 17–21, 2021. Springer, Cham, Switzerland.

[AJKL23] Joël Alwen, Jonas Janneck, Eike Kiltz, and Benjamin Lipp. The pre-shared key modes of HPKE. In Jian Guo and Ron Steinfeld, editors, *Advances in Cryptology – ASIACRYPT 2023, Part VI*, volume 14443 of *Lecture Notes in Computer Science*, pages 329–360, Guangzhou, China, December 4–8, 2023. Springer, Singapore, Singapore.

[CHN+24] Daniel Collins, Loïs Huguenin-Dumittan, Ngoc Khanh Nguyen, Nicolas Rolin, and Serge Vaudenay. K-waay: Fast and deniable post-quantum X3DH without ring signatures. In Davide Balzarotti and Wenyuan Xu, editors, *USENIX Security 2024: 33rd USENIX Security Symposium*, Philadelphia, PA, USA, August 14–16, 2024. USENIX Association.

[GdKQ+24] Phillip Gajland, Bor de Kock, Miguel Quaresma, Giulio Malavolta, and Peter Schwabe. SWOOSH: Efficient lattice-based non-interactive key exchange. In Davide Balzarotti and Wenyuan Xu, editors, *USENIX Security 2024: 33rd USENIX Security Symposium*, Philadelphia, PA, USA, August 14–16, 2024. USENIX Association.

[GHJ25] Phillip Gajland, Vincent Hwang, and Jonas Janneck. Shadowfax: Hybrid security and deniability for AKEMs. Cryptology ePrint Archive, Paper 2025/154, 2025.

[GJK24] Phillip Gajland, Jonas Janneck, and Eike Kiltz. Ring signatures for deniable AKEM: Gandalf's fellowship. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology – CRYPTO 2024, Part I*, volume 14920 of *Lecture Notes in Computer Science*, pages 305–338, Santa Barbara, CA, USA, August 18–22, 2024. Springer, Cham, Switzerland.