SWOOSH: Practical Lattice-Based Non-Interactive Key Exchange

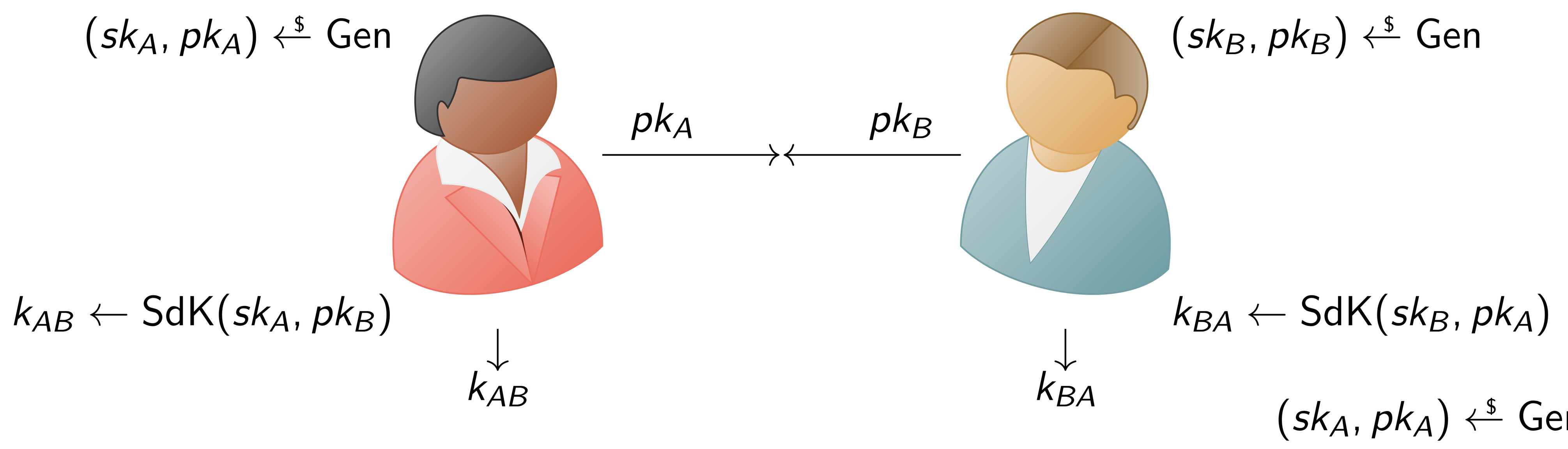
Phillip Gajland[1, 2], Bor de Kock[3], Miguel Quaresma[1], Giulio Malavolta[1], Peter Schwabe[1, 4]

[1] Max Planck Institute for Security and Privacy, Bochum, Germany 🇩🇪
[2] Ruhr University Bochum, Bochum, Germany 🇩🇪
[3] NTNU – Norwegian University of Science and Technology, Trondheim, Norway 🇳🇴
[4] Radboud University, Nijmegen, The Netherlands 🇳🇱

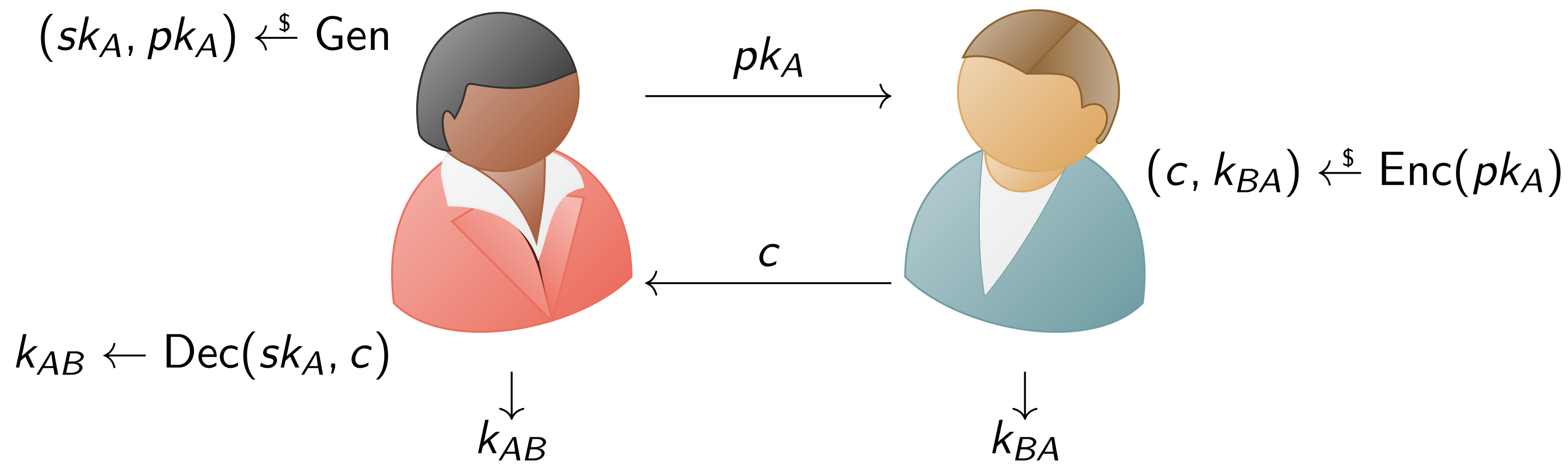
https://ia.cr/2023/271

Accepted at *USENIX 2024*

Non-Interactive Key Exchange (NIKE) vs. Key-Encapsulation Mechanisms (KEMs)



- Efficient post-quantum key exchange protocols differ from standard Diffie-Hellman, needing extra rounds of communication.
- These protocols can replace Diffie-Hellman in some scenarios. However others require a post-quantum secure non-interactive protocol.



- Our work aims to show the practical feasibility of lattice-based NIKE, which has proven challenging for the past decades, and answer the question:

Is lattice-based non-interactive key exchange feasible in practice?

Results: Our lattice-based NIKE SWOOSH

Scheme (variant)	Assumption	Non-interactive	Post-quantum	Size (bytes)		Cycles	
				c	pk	Gen	Enc + Dec **or** SdK
CRYSTALS-Kyber (Kyber-768 [1])	M-LWE	✗	✓	1 088	1 184	200 302	539 108 (251 384 + 287 724)
Classic McEliece (mceliece348864 [2])	Binary Goppa Codes	✗	✓	96	261 120	46 715 060	143 178 (31 000 + 112 178)
ECDH (X25519 [3])	CDH	✓	✗	—	32	28 187	87 942
CTIDH (CTIDH-1024 [4])	CSIDH	✓	✓	—	128	469 520 000	511 190 000
This work (Passive-SWOOSH)	M-LWE	✓	✓	—	221 184	146 920 890	10 612 666

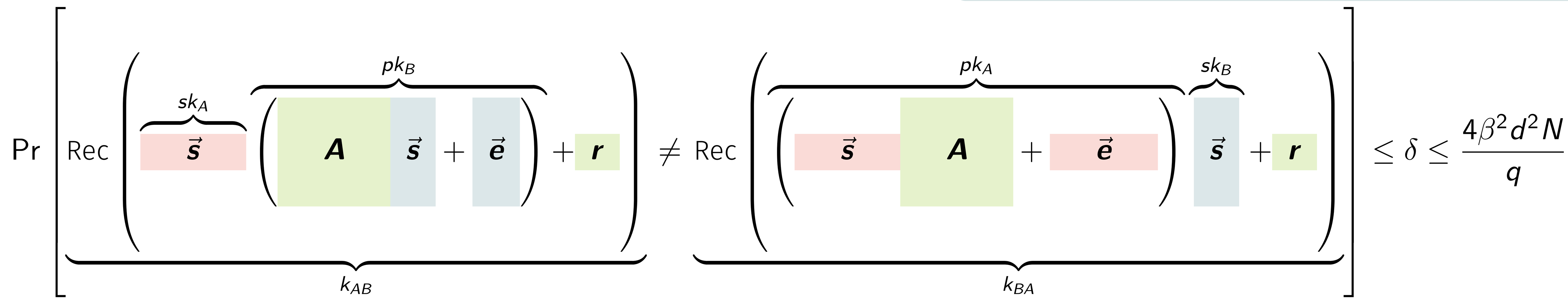
M-LWE based NIKE with strong correctness ⇒ **Passive to active security transformation using NIZKs** ⇓ **Parameter selection for 120 bits of security** ⇐ **Highly optimised implementation written in Rust**

Theorem 1: Passive-SWOOSH satisfies semi-malicious correctness in the quantum random oracle model (QROM).

Observation:

- Our use of the random oracle differs from the Fiat-Shamir and the Fujisaki-Okamoto transformations, and may be of independent interest.

Theorem 2: Passive-SWOOSH + NIZKs $\Longrightarrow$ SWOOSH.



The shared keys k_{AB} and k_{BA} are identical except for the small error terms $\vec{s}\,\vec{e}$ and $\vec{e}\,\vec{s}$. To correct these errors we run a non-interactive reconciliation function Rec resulting in a correctness error δ. Adding a random offset r gives semi-malicious correctness.

Parameters

Parameter	Description	Value
β	upper bound on $\|\vec{s}\|_\infty = \|\vec{e}\|_\infty$	1
q	prime modulus	$2^{214} - 255$
d	dim of $\mathcal{R}_q := \mathbb{Z}_q[X]/(X^d + 1)$	256
l	# factors $X^d + 1$ splits into $\bmod q$	128
N	height of the A matrix	32
n	lattice dimension	8192
χ	secret / noise distribution	$p(-1) = 25\%$, $p(0) = 50\%$, $p(1) = 25\%$

Select References

[1] P. Schwabe, R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, G. Seiler, D. Stehlé, and J. Ding. *CRYSTALS-KYBER*. Technical report, National Institute of Standards and Technology, 2022.

[2] M. R. Albrecht, D. J. Bernstein, T. Chou, C. Cid, J. Gilcher, T. Lange, V. Maram, I. von Maurich, R. Misoczki, R. Niederhagen, K. G. Paterson, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, C. Jung Tjhai, M. Tomlinson, and W. Wang. *Classic McEliece*. Technical report, National Institute of Standards and Technology, 2022.

[3] D. J. Bernstein *Curve25519: New Diffie-Hellman speed records*. PKC, 2023.

[4] G. Banegas, D. J. Bernstein, F. Campos, T. Chou, T. Lange, M. Meyer, B. Smith, and J. Sotáková. *CTIDH: faster constant- time CSIDH*. TCHES, 2021.