Post-quantum security of cryptographic transformations in the random oracle model

Huang, Y.

Post-Quantum Security of Cryptographic Transformations in the Random Oracle Model

Proefschrift

ter verkrijging van
de graad van doctor aan de Universiteit Leiden,
op gezag van rector magnificus prof.dr. S. de Rijcke,
volgens besluit van het college voor promoties
te verdedigen op woensdag 1 april 2026
klokke 10:00 uur

door

Yu-Hsuan Huang
geboren te Kaohsiung, Taiwan
in 1996

Promotores:
Prof.dr. S.O. Fehr
Prof.dr. R.J.F. Cramer

Promotiecommissie:
Prof.dr. S. Agrawal (Indian Institute of Technology)
Dr. C. Majenz (Technical University Denmark)
Prof.dr. S. Vaudenay (École Polytechnique Fédérale de Lausanne)
Prof.dr.ir. G.L.A. Derks
Prof.dr. R.M. van Luijk

The author of this thesis carried out his PhD research at the Cryptology Group of Centrum Wiskunde & Informatica (CWI) in The Netherlands, and is supported by the Dutch Research Agenda (NWA) project HAPKIDO (Project No. NWA.1215.18.002), which is financed by the Dutch Research Council (NWO).

CWI
Centrum Wiskunde & Informatica

Universiteit Leiden

Post-Quantum Security of Cryptographic Transformations in the Random Oracle Model

Yu-Hsuan Huang

If you reveal your secrets to the wind
you should not blame the wind for revealing them to the trees.

— Kahlil Gibran, Sand and Foam

Illustrations on the front and back covers are designed and drawn by the author.

Contents

List of Publications

The content of this thesis is based on the following articles, with all (co)authors, throughout this section except [HC18, HYC20, FHA23], listed alphabetically.

[FFH25] Pouria Fallahpour, Serge Fehr, and Yu-Hsuan Huang. Tighter quantum security for Fiat-Shamir-with-aborts and hash-and-sign-with-retry signatures. Cryptology ePrint Archive, Paper 2025/985, 2025

[FHK25] Serge Fehr, Yu-Hsuan Huang, and Julia Kastner. Sandwich BUFF: Achieving non-resignability using iterative hash functions. In Benny Applebaum and Huijia (Rachel) Lin, editors, *TCC 2025, Part III*, volume 16270 of *LNCS*, pages 235–265. Springer, Cham, December 2025

[DFH+24] Jelle Don, Serge Fehr, Yu-Hsuan Huang, Jyun-Jie Liao, and Patrick Struck. Hide-and-seek and the non-resignability of the BUFF transform. In Elette Boyle and Mohammad Mahmoody, editors, *TCC 2024, Part III*, volume 15366 of *LNCS*, pages 347–370. Springer, Cham, December 2024

[DFHS24] Jelle Don, Serge Fehr, Yu-Hsuan Huang, and Patrick Struck. On the (in)security of the BUFF transform. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part I*, volume 14920 of *LNCS*, pages 246–275. Springer, Cham, August 2024

[BBD+23] Manuel Barbosa, Gilles Barthe, Christian Doczkal, Jelle Don, Serge Fehr, Benjamin Grégoire, Yu-Hsuan Huang, Andreas Hülsing, Yi Lee, and Xiaodi Wu. Fixing and mechanizing the security proof of Fiat-Shamir with aborts and Dilithium. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part V*, volume 14085 of *LNCS*, pages 358–389. Springer, Cham, August 2023

[DFH22] Jelle Don, Serge Fehr, and Yu-Hsuan Huang. Adaptive versus static multi-oracle algorithms, and quantum security of a split-key PRF. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part I*, volume 13747 of *LNCS*, pages 33–51. Springer, Cham, November 2022

During his Ph.D. study and before, the author also (co)authored the following works, which are not included in this thesis.

[FH23] Serge Fehr and Yu-Hsuan Huang. On the quantum security of HAWK. In Thomas Johansson and Daniel Smith-Tone, editors, *Post-Quantum Cryptography - 14th International Workshop, PQCrypto 2023*, pages 405–416. Springer, Cham, August 2023

[CHH+21] Kai-Min Chung, Yao-Ching Hsieh, Mi-Ying Huang, Yu-Hsuan Huang, Tanja Lange, and Bo-Yin Yang. Isogeny-based group signatures and accountable ring signatures in QROM. Cryptology ePrint Archive, Paper 2021/1368, 2021

[CFHL21] Kai-Min Chung, Serge Fehr, Yu-Hsuan Huang, and Tai-Ning Liao. On the compressed-oracle technique, and post-quantum security of proofs of sequential work. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 598–629. Springer, Cham, October 2021

[HYC20] Yu-Hsuan Huang, Chih-Kai Yang, and Rong-Jaye Chen. Quadrangle inequality improvement for CSIDH strategy. In *Cryptology and Information Security Conference*, 2020

[HC18] Yu-Hsuan Huang and Rong-Jaye Chen. Simulating quantum algorithm by using singular value decomposition. In *Cryptology and Information Security Conference*, 2018

In addition to the above research articles, the author has contributed to the following technical documents.

[FHA23] Serge Fehr, Yu-Hsuan Huang, and Alessandro Amadori. Literature review - (quantum-safe) cryptographic combiners and hybrid security. Technical report, 2023. available at `https://hapkido.tno.nl/deliverables/literature-review-quantum-safe/`

[BBD+24] Joppe W. Bos, Olivier Bronchain, Léo Ducas, Serge Fehr, Yu-Hsuan Huang, Thomas Pornin, Eamonn W. Postlethwaite, Thomas Prest, Ludo N. Pulles, and Wessel van Woerden. HAWK. Technical report, National Institute of Standards and Technology, 2024. available at `https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures`