



Universiteit  
Leiden  
The Netherlands

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

Huang, Y.

### Citation

Huang, Y. (2026, April 1). *Post-quantum security of cryptographic transformations in the random oracle model*. Retrieved from <https://hdl.handle.net/1887/4300382>

Version: Publisher's Version

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/4300382>

**Note:** To cite this publication please use the final published version (if applicable).

*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

Copyright © 2025 *Yu-Hsuan Huang*.

*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).*



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

<b>List of Publications</b>	<b>ix</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Provable Security . . . . .	1
1.2 Cryptographic Transformations . . . . .	6
1.3 Our Contributions . . . . .	12
<b>2 Preliminaries</b>	<b>17</b>
2.1 Notations . . . . .	17
2.2 Oracle Algorithms . . . . .	18
2.2.1 Equivalences of Oracle Algorithms . . . . .	20
2.2.2 Conditioning of Oracle Algorithms . . . . .	21
2.2.3 Simulating the Write Access . . . . .	21
<b>3 Fiat-Shamir and Hash-and-Sign with Aborts</b>	<b>23</b>
3.1 Introduction . . . . .	23
3.1.1 Our Contribution . . . . .	24
3.2 Preliminaries . . . . .	27
3.2.1 Generalized Fiat-Shamir with Aborts Signatures . . . . .	27
3.2.2 A variant of the Adaptive Reprogramming Lemma . . . . .	29
3.3 A Gap in Prior Analyses of FS <sub>WA</sub> . . . . .	30
3.4 A UF-CMA-to-UF-NMA Reduction . . . . .	31
3.4.1 The Statements . . . . .	32
3.4.2 Proof Strategy . . . . .	33
3.4.3 From Sign to Prog . . . . .	35
3.4.4 From Prog to Trans . . . . .	37
3.4.5 Wrapping up the Proof of Theorem 3.5 . . . . .	40
3.4.6 Classical Bounds . . . . .	40
3.5 Tighter Bounds in QROM . . . . .	41
3.5.1 The Statements . . . . .	42
3.5.2 From Prog to Trans . . . . .	42
3.5.3 Wrapping up the Proof of Theorem 3.17 . . . . .	48

3.6	Concrete Analysis of Dilithium . . . . .	49
3.6.1	Controlling the Min-Entropy via the Rank of $\mathbf{A}$ . . . . .	49
3.6.2	Numerically Controlling the Rank of $\mathbf{A}$ . . . . .	50
3.6.3	Plugging in the Numbers . . . . .	53
3.6.4	Analytically Controlling $\epsilon_{\text{sk}}$ . . . . .	54
<b>4</b>	<b>BUFF Transformations</b> . . . . .	<b>59</b>
4.1	Introduction . . . . .	59
4.1.1	Our Contribution . . . . .	60
4.1.2	Related Work . . . . .	64
4.2	Preliminaries . . . . .	65
4.2.1	(HILL) Entropy . . . . .	65
4.2.2	Non-Resignability and $\Phi$ -Non-Malleability . . . . .	66
4.2.3	BUFF Transform . . . . .	68
4.3	On the Impossibility of Non-Resignability . . . . .	69
4.3.1	Non-Resignability and BUFF Transform in the Plain Model . . . . .	70
4.3.2	Non-Resignability and the BUFF Transform in the ROM . . . . .	72
4.3.3	$\Phi$ -Non-Malleability in the ROM . . . . .	74
4.4	Salted BUFF and NR-bot . . . . .	76
4.4.1	Positive Results . . . . .	76
4.4.2	Handling Classical Adversaries . . . . .	78
4.4.3	Handling Quantum Adversaries . . . . .	81
4.4.4	Negative Results with <i>Computational Entropy</i> . . . . .	85
4.5	BUFF and sNR . . . . .	86
4.5.1	Secret-key Non-resignability (sNR) . . . . .	86
4.5.2	The Hide-and-Seek Game . . . . .	88
4.5.3	BUFF via Random Oracles is sNR . . . . .	89
4.5.4	Reducing sNR of BUFF to Hide-and-Seek . . . . .	90
4.5.5	Hide-and-Seek for Random Oracles . . . . .	94
4.5.6	Wrapping up the Proof of Theorem 4.18 . . . . .	98
4.6	BUFF via Iterative Hash Functions . . . . .	99
4.6.1	sNR Relative to (Function-like) Oracles . . . . .	99
4.6.2	Iterative Hash Functions . . . . .	100
4.6.3	BUFF via Iterative Hash Functions is not sNR . . . . .	101
4.7	Sandwich BUFF (sBUFF) Transformation . . . . .	103
4.7.1	Sandwich BUFF via Merkle-Damgård is sNR . . . . .	103
4.7.2	Reducing sNR of Sandwich BUFF to Hide-and-Seek . . . . .	104
4.7.3	Hide-and-Seek for Merkle-Damgård . . . . .	111
4.8	Positive Results with Computational Entropy . . . . .	113
4.8.1	BUFF via RO is sNR, Computationally . . . . .	113
4.8.2	Sandwich BUFF via MD is sNR, Computationally . . . . .	115

<b>5 KEM Combiners via Split-key PRFs</b>	<b>117</b>
5.1 Introduction . . . . .	117
5.1.1 Our Contributions . . . . .	118
5.2 Preliminaries . . . . .	121
5.3 A Generic Adaptive-to-static Compiler . . . . .	122
5.3.1 Our Result . . . . .	122
5.3.2 The Technical Core . . . . .	123
5.3.3 Wrapping up the Proof of Theorem 5.1 . . . . .	126
5.3.4 Applications . . . . .	126
5.4 Quantum Security of a Split-key PRF . . . . .	128
5.4.1 Hybrid Security and skPRFs . . . . .	128
5.4.2 Quantum-security of the skPRF . . . . .	129
5.4.3 Proof of Theorem 5.7 . . . . .	130
<b>Conclusions</b>	<b>137</b>
<b>Appendix</b>	<b>139</b>
A.1 Breaking a Weakened Phi-Non-Malleability . . . . .	139
A.2 A Modified Measure-and-Reprogram Lemma . . . . .	140
A.3 Unsimplified Proof of Lemma 4.32 . . . . .	144
<b>Bibliography</b>	<b>165</b>
<b>Samenvatting</b>	<b>167</b>
<b>Summary</b>	<b>169</b>
<b>Acknowledgement</b>	<b>171</b>
<b>Curriculum Vitae</b>	<b>173</b>



# 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<sup>+</sup>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<sup>+</sup>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<sup>+</sup>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 QRROM. 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<sup>+</sup>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>