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

Huang, Y.

Acknowledgement

Being able to do scientific research for the last four years has been a life-long dream come true. Like many others, my PhD journey has consisted of both ebbs and flows, and I owe my sincerest gratitude to the many people who have supported me along the way.

First and foremost, I would like to thank my first advisor, Serge Fehr, who has provided me with guidance on a day-to-day basis. Serge and I shared a common interest in a research style that is theoretical and foundational, which made our collaboration very natural and rewarding. Working with Serge has been a pleasant and unique experience. I often notice his persistence in stripping down complicated arguments and ideas to their simplest forms. At first, this pursuit of simplicity almost felt too restrictive. Over time, however, it has led to better scientific papers and understandings. Even today, I can still vividly recall his voice, urging me to simplify my manuscripts further. Beyond research itself, I also learned from him how to interact with others, kindly and respectfully. My thesis would not have been the same without these lessons, which will surely continue to shape how I do research in the future.

Ronald Cramer, my second advisor, is also the head of Cryptology Group. As a scholar who has witnessed and shaped much of the history of cryptology himself, Ronald often shared with us stories of modern cryptographic methods from the perspective of their historical origins. Located at a hub of cryptology for more than two decades, the group has nurtured so many leading figures in the field. Having been a member for the last four years, I thank him for founding such a wonderful group, and for his down-to-earth friendliness that has bonded the group members more firmly together.

Julia Kastner, my office mate, collaborator, and paranymph, I will never forget your enthusiasm for squirrels, nor all the German language support you provided during the last year of my PhD. Thank you for always having my back — not only in research, when I stumbled over security proofs, but also in the bouldering gym and in everyday life.

Jelle Don, the days that we spent countless hours in front of a whiteboard, trying to tackle a single problem, are truly unforgettable. I also enjoyed hearing your life stories and anecdotes outside of research, whether about an advanture deep in nature, a special choir event, or your fundraising experiences. Thank

you for all the fruitful conversations and for being such an inspiration.

This thesis would literally not exist without its funding source — the HAPKIDO project. My sincere thanks go to everyone who contributed to this project. Additionally, I would also like to thank the reading committee — Prof.dr. Shewta Agrawal, Dr. Christian Majenz, and Prof.dr. Serge Vaudenay — for carefully reading through this thesis, and providing their useful feedbacks.

CWI has been an incredible place to be, largely because of the people at the institute. Special thanks to Simona Etinski, Michael Yonli, Junqiao (Randy) Lin, Shane Gibbons, and the activity committee for putting together engaging activities every once in a while; to Eamonn Postlethwaite, André Schrottenloher, long-term visitors Patrick Struck, Pouria Fallahpour, and Dominik Hartmann for many fruitful research discussions; to Pedro Capitão for co-organizing weekly seminars with me for an entire year; and to Minnie Middelberg, Susanne van Dam, Emil Gorter, and all other supporting staff for their extensive assistance with non-research matters.

The four-year study at CWI is not an easy journey, but even getting to the starting line would not have been possible without Kai-Min Chung. The summer after finishing my undergraduate study, I visited Kai-Min as a summer intern. There, I had my first chance to work with him on the topic of the quantum random oracle model (QROM), an experience without which I might have pursued a PhD elsewhere, or might not have pursued a PhD at all. For a similar reason, I also thank Rong-Jaye Chen, the advisor of my Bachelor's and Master's research, who introduced me into the fascinating world of cryptography.

My fellow ICPC nerds — Jarik Karsten, Wouter Koolen-Wijkstra, Ludo Pulles (who is also my paranymph), and Michelle Sweering — thank you for all the enjoyable moments that we spent on solving a wide range of puzzles, often unrelated to research, whether in front of a computer or around a dinner table. These fast-paced problem-solving sessions, like games of blitz chess, have always refreshed my mind alongside the slower pace of long-term research.

My Taiwanese friends, including but not limited to Yi Lee, Yao-Ting Lin, Miryam Huang, Er-Cheng Tang, Po-Yao (Cosmos) Wang, Alfon Hwu, Po-Kai Yang, David Lin, and Yong-Xuan Wang, thank you for the check-ins (even just occasionally). Knowing everyone is doing well has given me a sense of reassurance, when living on the opposite side of the globe from my hometown.

Finally, my deepest gratitude goes to my family, for their unwavering support, even when it is difficult to understand what I am doing. I was lucky to be raised in a family that values education, without drowning my curiosity in too much coursework. Having my younger brother by my side in childhood, our friendly rivalry has also pushed us to learn and grow together. Today, as lives have taken us to different corners of the world, the bonds we have built will continue to keep our hearts inseparable.

Curriculum Vitae

Yu-Hsuan Huang was born in Kaohsiung, Taiwan, on April 21, 1996. He graduated from Kaohsiung Senior High School in 2014. After spending one more year preparing for the annual Taiwanese Advanced Subject Test, he continued to study at National Chiao-Tung University, and obtained his Bachelor's and Master's degree in Computer Science, in 2019 and 2020 respectively.

During the undergraduate study, Yu-Hsuan was an active member of Programming Challenging Contest Association, where he participated in International Collegiate Programming Contest (ICPC) on behalf of the university. In the spring of 2019, he visited University of Illinois Urbana-Champaign (UIUC) as an exchange student for one semester.

Yu-Hsuan grew his interest in cryptology already since he was an undergraduate student, where he was supervised by Prof. Rong-Jaye Chen for both his Bachelor's and Master's research, the focus of which eventually shifted to elliptic-curve isogenies in the context of post-quantum cryptography. In 2019, he also worked as a summer intern at Academia Sinica in the research group of Dr. Kai-Min Chung, where he first had the chance to work on a research topic about quantum random oracle model (QROM).

In 2021, Yu-Hsuan started working at Centrum Wiskunde & Informatica (CWI) as a PhD student, on the topic of post-quantum cryptography, under the supervision of Prof.dr. Serge Fehr. His PhD research is mainly focused on provable security, with QROM playing a significant role. During his PhD study, Yu-Hsuan also contributed[4] to the proposal of HAWK, a lattice-based signature scheme that is also a candidate in the NIST PQC competition.

[4]More specifically, he contributed to the QROM security proof of HAWK, which is also included in the proposal.