Compressed Σ-protocol theory

Attema, T.

ACKNOWLEDGMENTS

Acknowledgments

With writing these acknowledgments I realize how many have contributed, directly or indirectly, to this dissertation. I am finishing a project that would not have been possible without the support of family, friends and colleagues. Therefore, a sincere thanks to everyone. Also, or perhaps especially, to the ones I do not address explicitly below.

First, I would like to thank Ronald Cramer, my promotor and daily supervisor. In our collaboration, he taught me to create my own "map of the cryptographic landscape" and aim to position novel ideas and techniques within this map. We have had many interesting discussions resulting in new research directions, not rarely in one of Amsterdam's pubs enjoying a "Kopstootje." Ronald, thanks for everything!

Also to Thijs Veugen I owe my gratitude. Thijs has helped me arrange this part-time PhD construction with CWI and TNO. He helped me acquire support from both organizations and find a supervisor. As such Thijs has been involved from the very start. I could always rely on his incredibly careful reviews, allowing me to apply the much needed finishing touches. Thijs, I hope our collaborations to continue far beyond this PhD.

Further, I would like to thank Serge Fehr. Working with Serge has been extremely educational. His ability to spot even the most subtle mistakes and ambiguities forced me to be very careful and precise. Often enough he sent me back to the drawing board, after I had incorrectly convinced myself that a problem had been solved.

Moreover, I had the pleasure to collaborate with some fantastic co-authors. Especially, I would like to thank Lisa Kohl, Michael Klooß and Matthieu Rambaud, who directly contributed to the results presented in this dissertation. I very much enjoyed the discussions that carried us away.

Next, this PhD project would not have been possible without the support from my employer TNO. In particular, I am extremely grateful for the many research managers that have helped me along the way: Christophe Hoegaerts, Paul de Jager, Daniëlle Keus, Milena Kooij-Janic, Annemieke Kips, Adri Krabbendam and Dick van Smirren. Annemieke put a lot of effort into the contract negotiations prior to the start of this PhD. During the PhD, Daniëlle gave me the freedom to work on topics with yet to be proven practical relevance. And Dick, even after leaving his position as my manager, was always available for a cup of coffee, ready to reflect on my ambitions and personal development.

I would also like to thank my other TNO colleagues. Vincent Dunning, Maran van Heesch, Michiel Marcus, Niels Neumann, Frank Phillipson, Alex Sangers, Ward van der Schoot, Gabriele Spini, Carolien van der Vliet-Hameeteman, Daniël Worm and many others kept inspiring me with new research directions motivated

by all sorts of practical applications. They acquired and led new projects, allowing me to focus on the content. Altogether they have made this PhD a joyful experience.

Moreover, the Cryptology Group of CWI has given me a very warm welcome. Their deep understanding of cryptology was occasionally intimidating, but the doors were always open, for answering my questions and sharing their knowledge.

Further, I could not have finished this dissertation without the everlasting patience of my wife Fieke. All those evenings that I was occupied trying to solve open problems, she was there to support me in the best way imaginable.

Finally, I would like to thank my family and friends. Throughout the years, my parents Jelle and José have supported and encouraged me to pursue my dreams, whatever these might be. My sister Maud has always had my back; she seems to be available day-and-night to help me with anything I need. Also my friends, Stefan, Mark, Norbert, Rick, Jordy and Leon, have been incredibly supportive. I am urged to write that they appreciated all my monologues about cryptology, but often enough they would kindly ask me to change the topic. Their friendship offered me indispensable distractions allowing me to completely recharge whenever I needed to.

Thanks for everything!

ABOUT THE AUTHOR

About the Author

Thomas Attema was born in Amersfoort, the Netherlands, on July 27, 1990. In 2008, he completed his secondary education at Het Nieuwe Eemland College in Amersfoort. He then continued to study Mathematical Sciences at Utrecht University, receiving a bachelor's degree in 2011 and a master's degree in 2013. Under the supervision of professor Frits Beukers, he wrote the master's thesis titled Super Congruences.

Subsequently, in 2013, Thomas started as a researcher at the Netherlands Organisation for Applied Scientific Research (TNO), where he applied mathematical techniques to solve network related problems in a variety of application domains. In 2016, his research interests started to shift towards (applied) cryptography. In 2018, Thomas obtained a part-time PhD position in the Cryptology Group of Centrum Wiskunde & Informatica (CWI), under the supervision of professor Ronald Cramer (CWI & Leiden University) and professor Serge Fehr (CWI & Leiden University).

Thomas currently holds a position as a senior researcher in the Applied Cryptography and Quantum Algorithms department of TNO, combined with a part-time deployment as a senior staff member in the Cryptology Group of CWI.

THE MATHEMATICIAN'S PATTERNS, LIKE THE PAINTER'S OR THE POET'S MUST BE BEAUTIFUL; THE IDEAS, LIKE THE COLOURS OR THE WORDS MUST FIT TOGETHER IN A HARMONIOUS WAY. BEAUTY IS THE FIRST TEST: THERE IS NO PERMANENT PLACE IN THIS WORLD FOR UGLY MATHEMATICS.

— **G.H. Hardy,** *A Mathematician's Apology (1940)*