Algorithmic techniques in algebraic cryptanalysis and their applications

Makarim, R.H.

Acknowledgments

I would like to thank my supervisor Ronald Cramer and my co-supervisor Marc Stevens. The opportunity to pursue a PhD degree in the Netherlands has opened up a whole new world in my educational, professional, and personal experience. The thought of doing a PhD in Mathematics was something that never crossed my mind, let alone doing it in the Netherlands. I especially want to thank Marc for multiple discussions and feedbacks that improved my research ability as well as my technical knowledge on the modern C++ features.

I would like to thank the financial support from the Mathematical Institute, University Leiden under the ALGANT (Algebra, Geometry and Number Theory) PhD program. A special thanks to Peter Stevenhagen for coordinating and arranging the funding.

I want to thank my fellow PhD students at the CWI Cryptology Group for the enjoyable discussions over coffee break and table-tennis game. A special thanks to Wessel van Woerden for proofreading part of this thesis and providing useful feedbacks.

I want to thank Putranto Hadi Utomo as one of my collaborator. Our brief meeting in Utrecht turned into a collaborative work after I realized that the problem of solving a binary puzzle can be reduced to the problem of solving a system of polynomial equations. On this part I would also like to thank Ruud Pellikaan for his feedbacks on the simplification of some polynomials that represent the constraints.

I want to express my gratitude also to Ami Muhammad Djuned and family (Ameh Fatma, Hana, Maryam) and Torik Djuned and family (Hafida, Rayyan, Adam, Sofia). Thank you for helping me to settle down in the Netherlands and for always being there whenever I needed help.

My PhD life in the Netherlands would be completely different without the presence of Om Tezar Saputra and family (Teh Intan, Aiden, and Alisha). There is no way I could thank all of you enough for accepting me as part of your family. Thank you for the patience, for the help, for the discussion over dinner, for the food, for the jokes, for the trip together, for the lessons on life and most importantly for the Pro Evolution Soccer game night. The warmth of your family is an antidote for me to fight against homesickness and gloomy cold winter in the Netherlands.

My special thanks also goes to Ahmed Abd-El-Haliem and family, Fuat Özman, Furkan Özman, Abdulaziz Balbaid and family, Said Badjuber, Ibrahim, Adam Belloum, Haryadi and Aya, Damar and Mauril, Mas Fajran and family, the Indonesian students in Leiden (Albert and Dwi) and in Amsterdam (Pram, Hana, Bowo, Widi). I also want to thank Bas Edixhoven for many conversations we had over mathematics, culture, education, and your wish to visit Indonesia again to try to ride a motorcycle. You will be missed greatly.

I want to thank my parents and my brothers Nabiel and Zacky for their support while I was thousands of kilometres away from home.

Finally, for Sarah, Ilyas, and Janan: thank you for your patience and for constantly reminding me that there is a beauty in life outside the realm of rationality and logic.

Curriculum Vitae

Rusydi Hasan Makarim was born in Cilacap, Indonesia, on June 7, 1989. He grew up in the same city, where he attended public high school 1 (Sekolah Menengah Atas Negeri 1) and learned computer programming for the very first time.

In 2007 he enrolled in the undergraduate program in computer science at the International Islamic University (Universiti Islam Antarabangsa) in Kuala Lumpur, Malaysia. During his undergraduate studies, he participated in multiple ACM-ICPC programming contests at the national, regional, and international level. After his graduation in December 2011, he worked briefly as HTML5 Developer Support in ServiceRocket Sdn. Bhd. (formerly CustomWare Sdn. Bhd.) until June 2012.

In September 2012 he started the master programme in cryptography at the Institute of Applied Mathematics (Uygulamalı Matematik Enstitüsü), Middle East Technical University (Orta Doğu Teknik Üniversitesi) in Ankara, Türkiye. He wrote his master thesis with the title "Relating Undisturbed Bits to Other Properties of Substitution Boxes" under the supervision of Assoc. Prof. Dr. Ali Doğanaksoy and graduated in July 2014.

In October 2014, he started the PhD program at the Mathematical Institute, University Leiden and was also affiliated with the Cryptology Group, Centrum Wiskunde en Informatica (CWI) Amsterdam, the Netherlands. His PhD thesis is completed under the supervision of Prof.dr. Ronald Cramer and dr. Marc Stevens.

From May 2019 until March 2023, Rusydi worked as a Lead Cryptography Analyst at the Technology Innovation Institute (TII) in Abu Dhabi, United Arab Emirates. His current research work focuses primarily on the design and the cryptanalysis of symmetric-key primitives, particularly using automated tools such as Mixed-Integer Linear Program (MILP), Satisfiability Modulo Theory (SMT), and SAT solvers.

Publications

1. Emanuele Bellini, Juan Grados, Rusydi H. Makarim, Carlo Sanna. *Finding Differential Trails on ChaCha by Means of State Functions*. International Journal of Applied Cryptography, Volume 4, No. 3/4, 2024, pp. 156-175.

2. Solane El Hirch, Joan Daemen, Raghvendra Rohit, Rusydi H. Makarim. *Twin Column Parity Mixers and Gaston - A New Mixing Layer and Permutation*. 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20–24, 2023, Proceedings, Part III, pp. 475-506.

3. Emanuele Bellini, David Gérault, Juan Grados, Rusydi H. Makarim, Thomas Peyrin. *Boosting Differential-Linear Cryptanalysis of ChaCha7 with MILP*. (2023). IACR Transactions on Symmetric Cryptology, Volume 2023, Issue 2, pp. 189-223.

4. Emanuele Bellini, David Gérault, Juan Grados, Yun Ju Huang, Rusydi H. Makarim, Mohamed Rachidi, Sharwan K. Tiwari. *CLAASP: a Crypto-*

graphic Library for the Automated Analysis of Symmetric Primitives. Selected Areas in Cryptography (SAC), Fredericton, New Brunswick, Canada, 2023, pp. 387-408.

5. Emanuele Bellini, David Gérault, Juan Grados, Rusydi H. Makarim, Thomas Peyrin. *Fully Automated Differential-Linear Attacks Against ARX Ciphers*. Cryptographers' Track at the RSA Conference (CT-RSA), San Francisco, USA, 2023, pp 252–276.

6. Stefano Barbero, Emanuele Bellini, Rusydi H. Makarim. *Rotational Analysis of ChaCha Permutation*. Advances in Mathematics of Communications, Volume 17, Issue 6, 2023, pp. 1422-1439.

7. Rusydi H. Makarim and Raghvendra Rohit. *Towards Tight Differential Bounds of Ascon: A Hybrid Usage of SMT and MILP*. (2022). IACR Transactions on Symmetric Cryptology, Volume 2022, Issue 3, pp. 303-340.

8. Emanuele Bellini, Rusydi H. Makarim, Carlo Sanna, Javier A. Verbel. *An Estimator for the Hardness of the MQ Problem*. 13th International Conference on Cryptology in Africa (AFRICACRYPT), Fez, Morocco, 2022, pp. 323-347.

9. Carlos Aguilar Melchor, Nicolas Aragon, Emanuele Bellini, Florian Caullery, Rusydi H. Makarim, Chiara Marcolla. *Constant Time Algorithms for ROLLO-I-128*. SN Computer Science, Volume 2, Number 5, September 2021, article number 382.

10. Emanuele Bellini, Alessandro De Piccoli, Rusydi H. Makarim, Sergio Polese, Lorenzo Riva, Andrea Visconti. *New Records of Pre-image Search of Reduced SHA-1 Using SAT Solvers*. Proceedings of the Seventh International Conference on Mathematics and Computing (ICMC), Shibpur, India, 2021, pp. 141-151.

11. Emanuele Bellini, Florian Caullery, Rusydi H. Makarim, Marc Manzano, Chiara Marcolla, Victor Mateu. *Advances and Challenges of Rank Metric Cryptography Implementations*. IEEE 37th International Conference on Computer Design (ICCD), Abu Dhabi, United Arab Emirates, 2019, pp. 325-328.

12. Putranto H. Utomo and Rusydi H. Makarim. *Solving a Binary Puzzle*. Mathematics in Computer Science, Volume 11, 2017, pp. 515-526.

13. Rusydi H. Makarim and Marc Stevens. *M4GB: An Efficient Gröbner Basis Algorithm*. Proceedings of the 2017 ACM International Symposium on Symbolic and Algebraic Computation (ISSAC), Kaiserslautern, Germany, 2017, pp. 293-300.

14. Rusydi H. Makarim and Cihangir Tezcan. *Relating Undisturbed Bits to Other Properties of Substitution Boxes*. Lightweight Cryptography for Security and Privacy - Third International Workshop (LightSec), Istanbul, Türkiye, 2014, pp. 109-125.

Courses and Summer Schools

1. Parallel Algorithms (Mastermath). Utrecht University, Utrecht, the Netherlands. Fall 2015.
2. Presentation Skills. Centrum Wiskunde en Informatica, Amsterdam, the Netherlands. Fall 2015.
3. UbiCrypt Spring School on Symmetric Cryptography. Ruhr University, Bochum, Germany. 17-19 March 2016.
4. Scientific Conduct for PhDs (Science). Leiden University (Online). 30 May 2024.

Presentations

1. *M4GB: A new Gröbner-basis Algorithm.* The 42nd International Symposium on Symbolic and Algebraic Computation (ISSAC), Technical University of Kaiserslautern, Germany. 25-28 July 2017
2. *M4GB: A new Gröbner-basis Algorithm.* ALGANT-DOC Students Meeting. Leiden University. 15 May 2017
3. *Introduction to Cryptography.* ALGANT-DOC Weekend Seminar. University of Duisburg-Essen, Germany. 27-28 February 2016.

Conferences, Seminars, and Workshops

1. Special RISC Seminar/CWI Lectures on Privacy and Security, Centrum Wiskunde en Informatica, 15 November 2018
2. RISC Seminar on Secure Multi-Party Computation and Code-Based Cryptography, Centrum Wiskunde en Informatica, 7 December 2017
3. The 8th International Workshop on Parallel Symbolic Computation (PASCO), Technical University of Kaiserslautern, 23-24 July 2017
4. The 42nd International Symposium on Symbolic and Algebraic Computation (ISSAC), Technical University of Kaiserslautern, Germany, 25-28 July 2017
5. ALGANT-DOC Students Meeting, Leiden University, 15 May 2017.
6. Mathematical Structures for Cryptography, Lorentz Center, Leiden, 22-26 August 2016
7. Directions in Symmetric Cryptography (DISC) 2016 Workshop. Bochum, Germany, 23-24 March 2016
8. The 23rd International Conference on Fast Software Encryption (FSE), Bochum, Germany, 20-23 March 2016
9. ALGANT-DOC Weekend Seminar, University of Duisburg-Essen, 27-28 February 2016
10. DIAMANT Symposium Fall 2015, Lunteren, 26-27 November 2015

11. ALGANT-DOC Students Meeting, University of Regensburg, Germany, February 2015
12. Security in Times of Surveillance, Technical University Eindhoven, 8 May 2015
13. RISC Seminar on Secret Sharing and Multiparty Computation, Centrum Wiskunde en Informatica, 24 April 2015
14. Special LACAL@RISC Seminar on Cryptologic Algorithms, Centrum Wiskunde en Informatica, 6 February 2015

Teaching Assistant

1. Cryptology (Mastermath) - Fall 2015