References I

[Ban+15] Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. "Midori: A Block Cipher for Low Energy". In: *Advances in Cryptology – ASIACRYPT 2015*. 2015, pp. 411–436.

[Ban+17] Subhadeep Banik, Sumit Kumar Pandey, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, and Yosuke Todo. "GIFT: A Small Present". In: *Cryptographic Hardware and Embedded Systems – CHES 2017*. 2017, pp. 321–345.

[BBS99] Eli Biham, Alex Biryukov, and Adi Shamir. "Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials". In: *Advances in Cryptology – EUROCRYPT 1999*. 1999, pp. 12–23.

[BC20] Christina Boura and Daniel Coggia. "Efficient MILP Modelings for Sboxes and Linear Layers of SPN ciphers". In: *IACR Transactions on Symmetric Cryptology* (2020), pp. 327–361.

[Bei+16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. "The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS". In: *Advances in Cryptology – CRYPTO 2016*. 2016, pp. 123–153.

[Ber+16] Thierry P. Berger, Julien Francq, Marine Minier, and Gaël Thomas. "Extended Generalized Feistel Networks Using Matrix Representation to Propose a New Lightweight Block Cipher: Lilliput". In: *IEEE Transactions on Computers* 65.7 (2016), pp. 2074–2089.

[BJ72] Egon Balas and Robert Jeroslow. "Canonical Cuts on the Unit Hypercube". In: *SIAM Journal on Applied Mathematics* 23.1 (1972), pp. 61–69.

[BS91] Eli Biham and Adi Shamir. "Differential Cryptanalysis of DES-like Cryptosystems". In: *Journal of Cryptology* 4.1 (1991), pp. 3–72.

[GNL12] Zheng Gong, Svetla Nikova, and Yee Wei Law. "KLEIN: A New Family of Lightweight Block Ciphers". In: *RFID. Security and Privacy*. 2012, pp. 1–18.

[Gur23] Gurobi Optimization, LLC. *Gurobi Optimizer Reference Manual (Version 10.0.1)*. Available: `https://www.gurobi.com`. 2023.

References II

[IS21] Murat Burhan Ilter and Ali Aydin Selçuk. "A New MILP Model for Matrix Multiplications with Applications to KLEIN and PRINCE". In: *Proceedings of the 18th International Conference on Security and Cryptography, SECRYPT 2021*. 2021, pp. 420–427.

[Ker83] Auguste Kerckhoffs. "La Cryptographie Militaire". In: *Journal des Sciences Militaires* 9 (1883), pp. 5–83.

[Kim+03] Jongsung Kim, Seokhie Hong, Jaechul Sung, Sangjin Lee, Jongin Lim, and Soohak Sung. "Impossible Differential Cryptanalysis for Block Cipher Structures". In: *Progress in Cryptology – INDOCRYPT 2003*. 2003, pp. 82–96.

[KL07] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman and Hall/CRC, 2007.

[Luo+09] Yiyuan Luo, Zhongming Wu, Xuejia Lai, and Guang Gong. *A Unified Method for Finding Impossible Differentials of Block Cipher Structures*. Cryptology ePrint Archive, Paper 2009/627. 2009.

[Mou+12] Nicky Mouha, Qingju Wang, Dawu Gu, and Bart Preneel. "Differential and Linear Cryptanalysis Using Mixed-Integer Linear Programming". In: *Information Security and Cryptology*. 2012, pp. 57–76.

[ST17a] Yu Sasaki and Yosuke Todo. "New Algorithm for Modeling S-box in MILP Based Differential and Division Trail Search". In: *Innovative Security Solutions for Information Technology and Communications*. 2017, pp. 150–165.

[ST17b] Yu Sasaki and Yosuke Todo. "New Impossible Differential Search Tool from Design and Cryptanalysis Aspects". In: *Advances in Cryptology – EUROCRYPT 2017*. 2017, pp. 185–215.

[ST18] Yu Sasaki and Yosuke Todo. "Tight Bounds of Differentially and Linearly Active S-Boxes and Division Property of Lilliput". In: *IEEE Transactions on Computers* 67.5 (2018), pp. 717–732.

References III

[Sun+14a] Siwei Sun, Lei Hu, Meiqin Wang, Pengpian Wang, Kexin Qiao, Xiaoshuang Ma, Danping Shi, and Ling Song. "Towards Finding the Best Characteristics of Some Bit-oriented Block Ciphers and Automatic Enumeration of (Related-key) Differential and Linear Characteristics with Predefined Properties". In: *IACR Cryptology ePrint Archive* 2014 (2014), pp. 747–777.

[Sun+14b] Siwei Sun, Lei Hu, Peng Wang, Kexin Qiao, Xiaoshuang Ma, and Ling Song. "Automatic Security Evaluation and (Related-key) Differential Characteristic Search: Application to SIMON, PRESENT, LBlock, DES(L) and Other Bit-Oriented Block Ciphers". In: *Advances in Cryptology – ASIACRYPT 2014*. 2014, pp. 158–178.

[The20] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)*. Available: `https://www.sagemath.org`. 2020.

[Udo21] Aleksei Udovenko. "MILP Modeling of Boolean Functions by Minimum Number of Inequalities". In: *IACR Cryptology ePrint Archive* 2021 (2021), p. 1099.

[WW12] Shengbao Wu and Mingsheng Wang. "Automatic Search of Truncated Impossible Differentials for Word-Oriented Block Ciphers". In: *Progress in Cryptology – INDOCRYPT 2012*. 2012, pp. 283–302.

[Yin+18] Jun Yin, Chuyan Ma, Lijun Lyu, Jian Song, Guang Zeng, Chuangui Ma, and Fushan Wei. "Improved Cryptanalysis of an ISO Standard Lightweight Block Cipher with Refined MILP Modelling". In: *Information Security and Cryptology*. 2018, pp. 404–426.