A Solutions to Type V and VI MQ Challenge

Type V - (n, m) = (24, 16) - Seed 1
(46, 0C, 42, 10, 26, 4F, 43, 31, C4, 9D, 34, 55, 3A, C9, 39, 3F, D4, 3A, 88, E5, 05, 17, 2D, 4B)

Type V - (n, m) = (25, 17) - Seed 0
(49, BB, 5E, C9, E, BF, 1B, FE, 9E, F6, C8, DC, 4C, 3, C9, AA, 53, 20, 34, 1A, 16, 62, 94, 45, 8C)

Type V - (n, m) = (27, 18) - Seed 0
(21, 21, 9E, 93, 6A, 19, 3E, CE, A2, 1A, 5D, 19, D3, D7, 16, 5, 9F, E1, 0, DA, 92, 55, EB, 19, 89, F0, 1)

Type V - (n, m) = (28, 19) - Seed 0
(F0, E2, 62, D7, 7F, A7, B3, 72, 51, 91, AD, 89, 57, F3, E6, 42, 4C, 63, C2, 16, FA, 6B, 54, 9B, 10, 62, C3, 34)

Type VI - (n, m) = (24, 16) - Seed 1
(30, 9, 25, 25, 23, 22, 25, 18, 4, 25, 23, 30, 26, 13, 19, 14, 30, 29, 6, 0, 3, 14, 23, 23)

Type VI - (n, m) = (25, 17) - Seed 0
(8, 1, 4, 15, 3, 14, 18, 16, 28, 2, 29, 24, 11, 17, 18, 8, 26, 27, 12, 23, 26, 18, 11, 26, 6)

Type VI - (n, m) = (27, 18) - Seed 0
(19, 19, 20, 30, 13, 12, 6, 11, 3, 16, 12, 14, 29, 29, 26, 0, 13, 11, 20, 17, 1, 11, 30, 11, 14, 2, 24)

Type VI - (n, m) = (28, 19) - Seed 0
(12, 26, 6, 4, 9, 24, 21, 8, 0, 19, 23, 28, 11, 24, 22, 5, 9, 24, 24, 13, 0, 19, 25, 25, 26, 10, 27, 16)

Type VI - (n, m) = (30, 20) - Seed 0
(11, 4, 28, 8, 10, 20, 26, 20, 30, 28, 0, 13, 26, 2, 22, 9, 8, 26, 7, 6, 9, 26, 24, 15, 22, 18, 12, 3, 11, 13)

B CPU Time and Memory usage of M4GB

$\mathbb{F}_{2^8}$, $m-n=1$			
n	m	CPU time	Memory
15	16	2121.83 s	1149 MB
16	17	18454.55 s	4557 MB
17	18	96000.30 s	14935 MB
18	19	840535.63 s	57000 MB

$\mathbb{F}_{2^8}$, $m-n=2$			
n	m	CPU time	Memory
14	16	81.73 s	108 MB
15	17	489.34 s	395 MB
16	18	2593.36 s	1169 MB
17	19	21461.78 s	4696 MB
18	20	106369.83 s	14880 MB
19	21	930243.86 s	55410 MB

$\mathbb{F}_{2^8}$, $m-n=3$			
n	m	CPU time	Memory
13	16	5.85 s	21 MB
14	17	35.56 s	66 MB
15	18	132.68 s	167 MB
16	19	1148.80 s	576 MB
17	20	4929.98 s	1723 MB
18	21	26096.75 s	5334 MB
19	22	207408.54 s	19835 MB
20	23	1115986.42 s	74004 MB

Table 24: *The CPU time and memory usage of* M4GB *to solve system of polynomials over* $\mathbb{F}_{2^8}$*.*

$\mathbb{F}_{31}, m-n=1$			
n	m	CPU time	Memory
15	16	2157.01 s	1149 MB
16	17	18592.99 s	4559 MB
17	18	119299.90 s	14868 MB
18	19	847613.39 s	57011 MB

$\mathbb{F}_{31}$, $m-n=2$			
n	m	CPU time	Memory
14	16	81.47 s	109 MB
15	17	491.49 s	398 MB
16	18	2620.79 s	1168 MB
17	19	21632.05 s	4657 MB
18	20	107099.96 s	14868 MB
19	21	941960.45 s	55516 MB

$\mathbb{F}_{31}$, $m-n=3$			
n	m	CPU time	Memory
13	16	6.29 s	21 MB
14	17	36.69 s	66 MB
15	18	134.21 s	164 MB
16	19	1157.86 s	580 MB
17	20	4961.64 s	1733 MB
18	21	26277.35 s	5343 MB
19	22	208961.14 s	19842 MB
20	23	1124110.35 s	74265 MB
21	24	1729007.02 s	126538 MB

$\mathbb{F}_{31}$, $m-n=4$			
n	m	CPU Time	Memory
12	16	0.83 s	10 MB
13	17	4.47 s	18 MB
14	18	10.13 s	31 MB
15	19	80.41 s	100 MB
16	20	284.43 s	275 MB
17	21	1640.92 s	796 MB
18	22	11400.29s	2749 MB
19	23	51281.00 s	8438 MB
20	24	323866.14 s	28865 MB
21	25	2114895.49 s	99646 MB

$\mathbb{F}_{31}$, $m-n=5$			
n	m	CPU Time	Memory
11	16	0.44 s	10 MB
12	17	0.80 s	10 MB
13	18	1.55 s	10 MB
14	19	7.54 s	25 MB
15	20	30.13 s	52 MB
16	21	181.32 s	154 MB
17	22	719.10 s	460 MB
18	23	3538.91 s	1368 MB
19	24	25530.18 s	4240 MB
20	25	111324.47 s	14035 MB
21	26	678252.18 s	46196 MB

$\mathbb{F}_{31}$, $m-n=6$			
n	m	CPU Time	Memory
10	16	0.12 s	9 MB
11	17	0.39 s	10 MB
12	18	0.77 s	10 MB
13	19	1.61 s	10 MB
14	20	6.40 s	20 MB
15	21	14.16 s	37 MB
16	22	72.64 s	83 MB
17	23	417.50 s	268 MB
18	24	1604.10 s	733 MB
19	25	8600.97 s	2468 MB
20	26	59280.30 s	7332 MB
21	27	262183.34 s	24526 MB
22	28	1465417.71 s	78768 MB

$\mathbb{F}_{31}$, $m-n=7$			
n	m	CPU Time	Memory
9	16	0.07 s	8 MB
10	17	0.12 s	9 MB
11	18	0.16 s	9 MB
12	19	0.66 s	9 MB
13	20	1.27 s	10 MB
14	21	2.29 s	11 MB
15	22	12.90 s	30 MB
16	23	42.25 s	64 MB
17	24	173.77 s	164 MB
18	25	1016.54 s	468 MB
19	26	3641.07 s	1301 MB
20	27	21341.13 s	4274 MB
21	28	139796.22 s	12595 MB
22	29	578488.31 s	40602 MB

$\mathbb{F}_{31}$, $m-n=8$			
n	m	CPU Time	Memory
8	16	0.05 s	7 MB
9	17	0.10 s	8 MB
10	18	0.13 s	9 MB
11	19	0.18 s	9 MB
12	20	0.28 s	8 MB
13	21	1.07 s	9 MB
14	22	1.97 s	11 MB
15	23	7.44 s	17 MB
16	24	25.80 s	47 MB
17	25	100.40 s	108 MB
18	26	440.25 s	288 MB
19	27	2414.14 s	807 MB
20	28	9464.87 s	2311 MB
21	29	52474.98 s	7678 MB
22	30	320730.95 s	22185 MB
23	31	1345880.83 s	70750 MB

Table 25: *The CPU time and memory usage of* M4GB *to solve system of polynomials over* $\mathbb{F}_{31}$.

References

[AC09] Martin R. Albrecht and Carlos Cid, *Algebraic Techniques in Differential Cryptanalysis*, Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, February 22-25, 2009, Revised Selected Papers (Orr Dunkelman, ed.), Lecture Notes in Computer Science, vol. 5665, Springer, 2009, pp. 193–208.

[ACF+15] Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, Robert Fitzpatrick, and Ludovic Perret, *Algebraic algorithms for LWE problems*, ACM Commun. Comput. Algebra **49** (2015), no. 2, 62.

[ACFP12] Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, and Ludovic Perret, *On the relation between the MXL family of algorithms and Gröbner basis algorithms*, J. Symb. Comput. **47** (2012), no. 8, 926–941.

[ADH+19] Martin R. Albrecht, Lèo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn W. Postlethwaite, and Marc Stevens, *The General Sieve Kernel (G6K)*, Available at `https://github.com/fplll/g6k`, 2019.

[AFI+04] Gwénolé Ars, Jean-Charles Faugère, Hideki Imai, Mitsuru Kawazoe, and Makoto Sugita, *Comparison Between XL and Gröbner Basis Algorithms*, Advances in Cryptology - ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings (Pil Joong Lee, ed.), Lecture Notes in Computer Science, vol. 3329, Springer, 2004, pp. 338–353.

[AG11] Sanjeev Arora and Rong Ge, *New Algorithms for Learning in Presence of Errors*, Automata, Languages and Programming - 38th International Colloquium, ICALP 2011, Zurich, Switzerland, July 4-8, 2011, Proceedings, Part I (Luca Aceto, Monika Henzinger, and Jirí Sgall, eds.), Lecture Notes in Computer Science, vol. 6755, Springer, 2011, pp. 403–415.

[AIK+00] Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, and Toshio Tokita, *Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms - Design and Analysis*, in Stinson and Tavares [ST01], pp. 39–56.

[AK03] Frederik Armknecht and Matthias Krause, *Algebraic Attacks on Combiners with Memory*, in Boneh [Bon03], pp. 162–175.

[AL94] William W. Adams and Philippe Loustaunau, *An Introduction to Grobner Bases*, American Mathematical Society (AMS), 1994.

[Alb07] Martin Albrecht, *Algebraic Attacks on the Courtois Toy Cipher*, Master's thesis, Universität Bremen, 2007.

[AP10] Martin Albrecht and John Perry, *F4/5*, 2010.

[AST24] Thomas Aulbach, Simona Samardjiska, and Monika Trimoska, *Practical Key-Recovery Attack on MQ-Sign and More*, Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Oxford, UK, June 12-14, 2024, Proceedings, Part II (Markku-Juhani O. Saarinen and Daniel Smith-Tone, eds.), Lecture Notes in Computer Science, vol. 14772, Springer, 2024, pp. 168–185.

[BAK98] Eli Biham, Ross J. Anderson, and Lars R. Knudsen, *Serpent: A New Block Cipher Proposal*, Fast Software Encryption, 5th International Workshop, FSE '98, Paris, France, March 23-25, 1998, Proceedings (Serge Vaudenay, ed.), Lecture Notes in Computer Science, vol. 1372, Springer, 1998, pp. 222–238.

[Bar04] Magali Bardet, *Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie*, Theses, Université Pierre et Marie Curie - Paris VI, December 2004.

[Bar07] Gregory Bard, *Algorithms for Solving Linear and Polynomial Systems of Equations over Finite Fields with Applications to Cryptanalysis*, Ph.D. thesis, Department of Mathematics, University of Maryland, 2007.

[Bar09] Gregory Bard, *Algebraic Cryptanalysis*, Springer, 2009.

[Bay82] David Allen Bayer, *The Division Algorithm and the Hilbert Scheme*, Ph.D. thesis, Harvard University, Cambridge, MA, USA, 1982, AAI8222588.

[BBB+20] Magali Bardet, Pierre Briaud, Maxime Bros, Philippe Gaborit, Vincent Neiger, Olivier Ruatta, and Jean-Pierre Tillich, *An Algebraic Attack on Rank Metric Code-Based Cryptosystems*, Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part III (Anne Canteaut and Yuval Ishai, eds.), Lecture Notes in Computer Science, vol. 12107, Springer, 2020, pp. 64–93.

[BBD09] Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen (eds.), *Post-Quantum Cryptography*, Springer Berlin, Heidelberg, 2009.

[BBM23] Stefano Barbero, Emanuele Bellini, and Rusydi H. Makarim, *Rotational analysis of ChaCha permutation*, Adv. Math. Commun. **17** (2023), no. 6, 1422–1439.

[BBS99] Eli Biham, Alex Biryukov, and Adi Shamir, *Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials*, in Stern [Ste99], pp. 12–23.

[BC03] Alex Biryukov and Christophe De Cannière, *Block Ciphers and Systems of Quadratic Equations*, Fast Software Encryption, 10th International Workshop, FSE 2003, Lund, Sweden, February 24-26, 2003, Revised Papers (Thomas Johansson, ed.), Lecture Notes in Computer Science, vol. 2887, Springer, 2003, pp. 274–289.

[BCC+10] Charles Bouillaguet, Hsieh-Chung Chen, Chen-Mou Cheng, Tung Chou, Ruben Niederhagen, Adi Shamir, and Bo-Yin Yang, *Fast Exhaustive Search for Polynomial Systems in* $\mathbb{F}_2$, Cryptographic Hardware and Embedded Systems, CHES 2010, 12th International Workshop, Santa Barbara, CA, USA, August 17-20, 2010. Proceedings (Stefan Mangard and François-Xavier Standaert, eds.), Lecture Notes in Computer Science, vol. 6225, Springer, 2010, pp. 203–218.

[BCC+13] Charles Bouillaguet, Chen-Mou Cheng, Tung Chou, Ruben Niederhagen, and Bo-Yin Yang, *Fast Exhaustive Search for Quadratic Systems in $$\mathbb {F}_{2}$$ on FPGAs*, Selected Areas in Cryptography - SAC 2013 - 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers (Tanja Lange, Kristin E. Lauter, and Petr Lisonek, eds.), Lecture Notes in Computer Science, vol. 8282, Springer, 2013, pp. 205–222.

[BCC+23] Ward Beullens, Fabio Campos, Sofía Celi, Basil Hess, and Matthias J. Kannwischer, *MAYO Specification*, Tech. report, National Institute for Standards and Technology (NIST), 2023.

[BCD+23] Ward Beullens, Ming-Shing Chen, Jintai Ding, Boru Gong, Matthias J. Kannwischer, Jacques Patarin, Bo-Yuan Peng, Dieter Schmidt, Cheng-Jhih Shih, Chengdong Tao, and Bo-Yin Yang, *UOV: Unbalanced Oil and Vinegar*, Tech. report, National Institute for Standards and Technology (NIST), 2023.

[BCJ07] Gregory V. Bard, Nicolas Courtois, and Chris Jefferson, *Efficient Methods for Conversion and Solution of Sparse Systems of Low-Degree Multivariate Polynomials over GF(2) via SAT-Solvers*, IACR Cryptology ePrint Archive **2007** (2007), 24.

[BCM+19] Emanuele Bellini, Florian Caullery, Rusydi H. Makarim, Marc Manzano, Chiara Marcolla, and Víctor Mateu, *Advances and Challenges of Rank Metric Cryptography Implementations*, 37th IEEE International Conference on Computer Design, ICCD 2019, Abu Dhabi, United Arab Emirates, November 17-20, 2019, IEEE, 2019, pp. 325–328.

[BCP97] Wieb Bosma, John J. Cannon, and Catherine Playoust, *The Magma Algebra System I: The User Language*, J. Symb. Comput. **24** (1997), no. 3/4, 235–265.

[BD07] Eli Biham and Orr Dunkelman, *Differential Cryptanalysis in Stream Ciphers*, IACR Cryptology ePrint Archive **2007** (2007), 218.

[BD09a] Michael Brickenstein and Alexander Dreyer, *PolyBoRi: A framework for Gröbner-basis computations with Boolean polynomials*, J. Symb. Comput. **44** (2009), no. 9, 1326–1345.

[BD09b] Michael Brickenstein and Alexander Dreyer, *PolyBoRi: A framework for Gröbner-basis computations with Boolean polynomials*, Journal of Symbolic Computation **44** (2009), no. 9, 1326 – 1345, Effective Methods in Algebraic Geometry.

[BDDL16] Xavier Bultel, Jannik Dreier, Jean-Guillaume Dumas, and Pascal Lafourcade, *Physical Zero-Knowledge Proofs for Akari, Takuzu, Kakuro and KenKen*, 8th International Conference on Fun with Algorithms, FUN 2016, June 8-10, 2016, La Maddalena, Italy (Erik D. Demaine and Fabrizio Grandoni, eds.), LIPIcs, vol. 49, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016, pp. 8:1–8:20.

[BDK+18] Joppe W. Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé, *CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM*, 2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018, London, United Kingdom, April 24-26, 2018, IEEE, 2018, pp. 353–367.

[BDKW19] Achiya Bar-On, Orr Dunkelman, Nathan Keller, and Ariel Weizman, *DLCT: A New Tool for Differential-Linear Cryptanalysis*, Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part I (Yuval Ishai and Vincent Rijmen, eds.), Lecture Notes in Computer Science, vol. 11476, Springer, 2019, pp. 313–342.

[BDZ04] Feng Bao, Robert H. Deng, and Jianying Zhou (eds.), *Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004*, Lecture Notes in Computer Science, vol. 2947, Springer, 2004.

[BERW08] Andrey Bogdanov, Thomas Eisenbarth, Andy Rupp, and Christopher Wolf, *Time-Area Optimized Public-Key Engines: MQ-Cryptosystems as Replacement for Elliptic Curves?*, Cryptographic Hardware and Embedded Systems - CHES 2008, 10th International Workshop, Washington, D.C., USA, August 10-13, 2008. Proceedings (Elisabeth Oswald and Pankaj Rohatgi, eds.), Lecture Notes in Computer Science, vol. 5154, Springer, 2008, pp. 45–61.

[Beu22] Ward Beullens, *Breaking Rainbow Takes a Weekend on a Laptop*, Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II (Yevgeniy Dodis and Thomas Shrimpton, eds.), Lecture Notes in Computer Science, vol. 13508, Springer, 2022, pp. 464–479.

[Beu24] Ward Beullens, *Improved Cryptanalysis of SNOVA*, IACR Cryptol. ePrint Arch. (2024), 1297.

[BFP09] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret, *Hybrid approach for solving multivariate systems over finite fields*, J. Mathematical Cryptology **3** (2009), no. 3, 177–197.

[BFP12] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret, *Solving polynomial systems over finite fields: improved analysis of the hybrid approach*, in van der Hoeven and van Hoeij [vdHvH12], pp. 67–74.

[BFS04] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy, *On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equation*, Proceedings of the International Conference on Polynomial System Solving, 2004, pp. 71–75.

[BFSS13] Magali Bardet, Jean-Charles Faugère, Bruno Salvy, and Pierre-Jean Spaenlehauer, *On the complexity of solving quadratic Boolean systems*, J. Complex. **29** (2013), no. 1, 53–75.

[BFSY05] Magali Bardet, Jean-Charles Faugère, Bruno Salvy, and Bo-Yin Yang, *Asymptotic Behaviour of the Degree of Regularity of Semi-Regular Polynomial Systems*, Eighth International Symposium on Effective Methods in Algebraic Geometry, Porto Conte Alghero, Sardinia (Italy), 2005, pp. 1–14.

[BGG+23a] Emanuele Bellini, David Gérault, Juan Grados, Yun Ju Huang, Rusydi H. Makarim, Mohamed Rachidi, and Sharwan K. Tiwari, *CLAASP: A Cryptographic Library for the Automated Analysis of Symmetric Primitives*, Selected Areas in Cryptography - SAC 2023 - 30th International Conference, Fredericton, Canada, August 14-18, 2023, Revised Selected Papers (Claude Carlet, Kalikinkar Mandal, and Vincent Rijmen, eds.), Lecture Notes in Computer Science, vol. 14201, Springer, 2023, pp. 387–408.

[BGG+23b] Emanuele Bellini, David Gérault, Juan Grados, Rusydi H. Makarim, and Thomas Peyrin, *Boosting Differential-Linear Cryptanalysis of ChaCha7 with MILP*, IACR Trans. Symmetric Cryptol. **2023** (2023), no. 2, 189–223.

[BGG+23c] Emanuele Bellini, David Gérault, Juan Grados, Rusydi H. Makarim, and Thomas Peyrin, *Fully Automated Differential-Linear Attacks Against ARX Ciphers*, Topics in Cryptology - CT-RSA 2023 - Cryptographers' Track at the RSA Conference 2023, San Francisco, CA, USA, April 24-27, 2023, Proceedings (Mike Rosulek, ed.), Lecture Notes in Computer Science, vol. 13871, Springer, 2023, pp. 252–276.

[BGMS24] Emanuele Bellini, Juan Grados, Rusydi H. Makarim, and Carlo Sanna, *Finding differential trails on ChaCha by means of state functions*, Int. J. Appl. Cryptogr. **4** (2024), no. 3/4, 156–175.

[Bie17] Armin Biere, *CaDiCaL, Lingeling, Plingeling, Treengeling, YalSAT Entering the SAT Competition 2017*, Proc. of SAT Competition 2017 – Solver and Benchmark Descriptions (Tomáš Balyo, Marijn Heule, and Matti Järvisalo, eds.), Department of Computer Science Series of Publications B, vol. B-2017-1, University of Helsinki, 2017, pp. 14–15.

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe, *PRESENT: An Ultra-Lightweight Block Cipher*, Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings (Pascal Paillier and Ingrid Verbauwhede, eds.), Lecture Notes in Computer Science, vol. 4727, Springer, 2007, pp. 450–466.

[BKPV23] Luk Bettale, Delaram Kahrobaei, Ludovic Perret, and Javier Verbel, *Biscuit: Shorter MPC-based Signature from PoSSo*, Tech. report, National Institute for Standards and Technology (NIST), 2023.

[BKS09] Julia Borghoff, Lars R. Knudsen, and Mathias Stolpe, *Bivium as a Mixed-Integer Linear Programming Problem*, Cryptography and Coding, 12th IMA International Conference, Cryptography and Coding 2009, Cirencester, UK, December 15-17, 2009. Proceedings (Matthew G. Parker, ed.), Lecture Notes in Computer Science, vol. 5921, Springer, 2009, pp. 133–152.

[BKW19] Andreas Björklund, Petteri Kaski, and Ryan Williams, *Solving Systems of Polynomial Equations over GF(2) by a Parity-Counting Self-Reduction*, 46th International Colloquium on Automata, Languages, and Programming, ICALP 2019, July 9-12, 2019, Patras, Greece (Christel Baier, Ioannis Chatzigiannakis, Paola Flocchini, and Stefano Leonardi, eds.), LIPIcs, vol. 132, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019, pp. 26:1–26:13.

[Blu01] BluetoothSIG, *Specification of the Bluetooth System*, 1.1 ed., February 2001.

[BM22] Emanuele Bellini and Rusydi H. Makarim, *Functional Cryptanalysis: Application to reduced-round Xoodoo*, IACR Cryptol. ePrint Arch. (2022), 134.

[BMS16] Emanuele Bellini, Teo Mora, and Massimiliano Sala, *An algorithmic approach using multivariate polynomials for the nonlinearity of Boolean functions*, CoRR **abs/1610.05932** (2016).

[BMSV22] Emanuele Bellini, Rusydi H. Makarim, Carlo Sanna, and Javier A. Verbel, *An Estimator for the Hardness of the MQ Problem*, Progress in Cryptology - AFRICACRYPT 2022: 13th International Conference on Cryptology in Africa, AFRICACRYPT 2022, Fes, Morocco, July 18-20, 2022, Proceedings (Lejla Batina and Joan Daemen, eds.), Lecture Notes in Computer Science, vol. 13503, Springer Nature Switzerland, 2022, pp. 323–347.

[Bon03] Dan Boneh (ed.), *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, Lecture Notes in Computer Science, vol. 2729, Springer, 2003.

[BP09] Stanislav Bulygin and Ruud Pellikaan, *Bounded distance decoding of linear error-correcting codes with Gröbner bases*, J. Symb. Comput. **44** (2009), no. 12, 1626–1643.

[BP17] Ward Beullens and Bart Preneel, *Field Lifting for Smaller UOV Public Keys*, Progress in Cryptology - INDOCRYPT 2017 - 18th International Conference on Cryptology in India, Chennai, India, December 10-13, 2017, Proceedings (Arpita Patra and Nigel P. Smart, eds.), Lecture Notes in Computer Science, vol. 10698, Springer, 2017, pp. 227–246.

[BPM+21] Emanuele Bellini, Alessandro De Piccoli, Rusydi H. Makarim, Sergio Polese, Lorenzo Riva, and Andrea Visconti, *New Records of Preimage Search of Reduced SHA-1 Using SAT Solvers*, Proceedings of the Seventh International Conference on Mathematics and Computing - ICMC 2021, Shibpur, India, (Debasis Giri, Kim-Kwang Raymond Choo, Saminathan Ponnusamy, Weizhi Meng, Sedat Akleylek, and Santi Prasad Maity, eds.), Advances in Intelligent Systems and Computing, vol. 1412, Springer, 2021, pp. 141–151.

[BPSV17] Ward Beullens, Bart Preenel, Alan Szepieniec, and Frederik Vercauteren, *LUOV, Signature Scheme Proposal for NIST PQC Project*, Tech. report, National Institute for Standards and Technology (NIST), 2017.

[BR00] Paulo Barreto and Vincent Rijmen, *The Khazad Legacy-Level Block Cipher*, Submission to the NESSIE Project, 2000.

[Bri10] Michael Brickenstein, *Boolean Gröbner bases - Theory, Algorithms, and Applications*, Ph.D. thesis, Technische Universität Kaiserslautern, 2010.

[BS90] Eli Biham and Adi Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings (Alfred Menezes and Scott A. Vanstone, eds.), Lecture Notes in Computer Science, vol. 537, Springer, 1990, pp. 2–21.

[BS23] Charles Bouillaguet and Julia Sauvage, *High-Performance Xbred*, September 2023.

[BSS14] Emanuele Bellini, I. Simonetti, and Massimiliano Sala, *Nonlinearity of Boolean functions: an algorithmic approach based on multivariate polynomials*, CoRR **abs/1404.2741** (2014).

[Buc65] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Ph.D. thesis, University of Innsbruck, 1965.

[Buc79] Bruno Buchberger, *A criterion for detecting unnecessary reductions in the construction of Groebner bases*, Symbolic and Algebraic Computation, EUROSAM '79, An International Symposiumon Symbolic and Algebraic Computation, Marseille, France, June 1979, Proceedings (Edward W. Ng, ed.), Lecture Notes in Computer Science, vol. 72, Springer, 1979, pp. 3–21.

[Buc06] Bruno Buchberger, *Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal*, Journal of Symbolic Computation **41** (2006), no. 3, 475 – 511.

[BW93] Thomas Becker and Volker Weispfenning, *Gröbner Bases - A Computational Approach to Commutative Algebra*, Graduate Texts in Mathematics, vol. 141, Springer New York, 1993.

[Can06] Christophe De Cannière, *Trivium: A Stream Cipher Construction Inspired by Block Cipher Design Principles*, Information Security, 9th International Conference, ISC 2006, Samos Island, Greece, August 30 - September 2, 2006, Proceedings (Sokratis K. Katsikas, Javier Lopez, Michael Backes, Stefanos Gritzalis, and Bart Preneel, eds.), Lecture Notes in Computer Science, vol. 4176, Springer, 2006, pp. 171–186.

[Car10] Claude Carlet, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, ch. Boolean Functions for Cryptography and Error Correcting Codes, pp. 257–397, Cambridge University Press, 2010.

[CB07] Nicolas Courtois and Gregory V. Bard, *Algebraic Cryptanalysis of the Data Encryption Standard*, Cryptography and Coding, 11th IMA International Conference, Cirencester, UK, December 18-20, 2007, Proceedings (Steven D. Galbraith, ed.), Lecture Notes in Computer Science, vol. 4887, Springer, 2007, pp. 152–169.

[CBD+09] Crystal Clough, John Baena, Jintai Ding, Bo-Yin Yang, and Ming-Shing Chen, *Square, a New Multivariate Encryption Scheme*, Topics in Cryptology - CT-RSA 2009, The Cryptographers' Track at the RSA Conference 2009, San Francisco, CA, USA, April 20-24, 2009. Proceedings (Marc Fischlin, ed.), Lecture Notes in Computer Science, vol. 5473, Springer, 2009, pp. 252–264.

[CCNY12] Chen-Mou Cheng, Tung Chou, Ruben Niederhagen, and Bo-Yin Yang, *Solving Quadratic Equations with XL on Parallel Architectures*, Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings (Emmanuel Prouff and Patrick Schaumont, eds.), Lecture Notes in Computer Science, vol. 7428, Springer, 2012, pp. 356–373.

[CGMT02] Nicolas T. Courtois, Louis Goubin, Willi Meier, and Jean-Daniel Tacier, *Solving Underdefined Systems of Multivariate Quadratic Equations*, Public Key Cryptography, 5th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2002, Paris, France, February 12-14, 2002, Proceedings (David Naccache and Pascal Paillier, eds.), Lecture Notes in Computer Science, vol. 2274, Springer, 2002, pp. 211–227.

[Che16] Chen-Mou Cheng, *Solving the "CS" Challenge with MiniGB*, Seminar Abstract, March 2016.

[CHR+17] Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe, *MQDSS Specifications*, Tech. report, National Institute for Standards and Technology (NIST), 2017.

[CKL+19] Anne Canteaut, Lukas Kölsch, Chao Li, Chunlei Li, Kangquan Li, Longjiang Qu, and Friedrich Wiemer, *On the Differential-Linear Connectivity Table of Vectorial Boolean Functions*, CoRR **abs/1908.07445** (2019).

[CKM97] Stéphane Collart, Michael Kalkbrener, and Daniel Mall, *Converting Bases with the Gröbner Walk*, J. Symb. Comput. **24** (1997), no. 3/4, 465–469.

[CKPS00] Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir, *Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations*, Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding (Bart Preneel, ed.), Lecture Notes in Computer Science, vol. 1807, Springer, 2000, pp. 392–407.

[CLO15] David A. Cox, John Little, and Donal O'Shea, *Ideals, Varieties, and Algorithms - An Introduction to Computational Algebraic Geometry and Commutative Algebra*, 4th ed., Undergraduate Texts in Mathematics, Springer International Publishing, 2015.

[CM03] Nicolas Courtois and Willi Meier, *Algebraic Attacks on Stream Ciphers with Linear Feedback*, Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings (Eli Biham, ed.), Lecture Notes in Computer Science, vol. 2656, Springer, 2003, pp. 345–359.

[CMR05] Carlos Cid, Sean Murphy, and Matthew J. B. Robshaw, *Small Scale Variants of the AES*, Fast Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers (Henri Gilbert and Helena Handschuh, eds.), Lecture Notes in Computer Science, vol. 3557, Springer, 2005, pp. 145–162.

[CMR06] Carlos Cid, Sean Murphy, and Matthew Robshaw, *Algebraic Aspects of the Advanced Encryption Standard*, Springer, 2006.

[Coo71] Stephen A. Cook, *The Complexity of Theorem-Proving Procedures*, Proceedings of the 3rd Annual ACM Symposium on Theory of Computing, May 3-5, 1971, Shaker Heights, Ohio, USA (Michael A. Harrison, Ranan B. Banerji, and Jeffrey D. Ullman, eds.), ACM, 1971, pp. 151–158.

[Cop94] Don Coppersmith, *Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm*, Mathematics of Computation **62** (1994), 333–350.

[Cou03] Nicolas Courtois, *Fast Algebraic Attacks on Stream Ciphers with Linear Feedback*, in Boneh [Bon03], pp. 176–194.

[Cou04] Nicolas Courtois, *Algebraic Attacks over GF(2^k), Application to HFE Challenge 2 and Sflash-v2*, in Bao et al. [BDZ04], pp. 201–217.

[CP02] Nicolas Courtois and Josef Pieprzyk, *Cryptanalysis of Block Ciphers with Overdefined Systems of Equations*, Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings (Yuliang Zheng, ed.), Lecture Notes in Computer Science, vol. 2501, Springer, 2002, pp. 267–287.

[CP03] Nicolas Courtois and Jacques Patarin, *About the XL Algorithm over GF(2)*, Topics in Cryptology - CT-RSA 2003, The Cryptographers' Track at the RSA Conference 2003, San Francisco, CA, USA, April 13-17, 2003, Proceedings (Marc Joye, ed.), Lecture Notes in Computer Science, vol. 2612, Springer, 2003, pp. 141–157.

[CS09] Thomas W. Cusick and Pantelimon Stănică, *Cryptographic Boolean Functions and Applications*, Elsevier Inc, 2009.

[CV05] Anne Canteaut and Marion Videau, *Symmetric Boolean functions*, IEEE Trans. Information Theory **51** (2005), no. 8, 2791–2811.

[CVJ] Titouan Coladon, Vanessa Vitse, and Antoine Joux, *OpenF4 implementation*, `https://github.com/nauotit/openf4`.

[Dav87] James H. Davenport, *Looking at a Set of Equations*, Tech. report, School of Mathematical Sciences, University of Bath, 1987.

[dB12] Marzio de Biasi, *Binary Puzzle is NP-Complete*, July 2012.

[DCG+01] Ed Dawson, Andrew Clark, Helen Gustafson, Bill Millan, and Leonie Sipmson, *Evaluation of TOYOCRYPT-HS1*, Tech. report, Information Security Research Centre, Queensland University of Technology, 2001.

[DCP+17] Jintai Ding, Ming-Shing Chen, Albrecht Petzoldt, Dieter Schmidt, and Bo-Yin Yang, *Gui - Algorithm Specification and Documentation*, Tech. report, National Institute for Standards and Technology (NIST), 2017.

[DGG+23] Jintai Ding, Boru Gong, Hao Guo, Xiaoou He, Yi Jin, Yuansheng Pan, Dieter Schmidt, Chengdong Tao, Danli Xie, Bo-Yin Yang, and Ziyu Zhao, *TUOV: Triangular Unbalanced Oil and Vinegar*, Tech. report, National Institute for Standards and Technology (NIST), 2023.

[DGPS18] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann, SINGULAR *4-1-1 — A computer algebra system for polynomial computations*, `http://www.singular.uni-kl.de`, 2018.

[DH76] Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Trans. Information Theory **22** (1976), no. 6, 644–654.

[Din04] Jintai Ding, *A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation*, in Bao et al. [BDZ04], pp. 305–318.

[DKL$^+$18] Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé, *CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme*, IACR Trans. Cryptogr. Hardw. Embed. Syst. **2018** (2018), no. 1, 238–268.

[DPW14] Jintai Ding, Albrecht Petzoldt, and Lih-chung Wang, *The Cubic Simple Matrix Encryption Scheme*, in Mosca [Mos14], pp. 76–87.

[DS05] Jintai Ding and Dieter Schmidt, *Rainbow, a New Multivariable Polynomial Signature Scheme*, Applied Cryptography and Network Security, Third International Conference, ACNS 2005, New York, NY, USA, June 7-10, 2005, Proceedings (John Ioannidis, Angelos D. Keromytis, and Moti Yung, eds.), Lecture Notes in Computer Science, vol. 3531, 2005, pp. 164–175.

[dt16] The FPLLL development team, *fplll, a lattice reduction library*, Available at `https://github.com/fplll/fplll`, 2016.

[DY07] Jintai Ding and Bo-Yin Yang, *Multivariates Polynomials for Hashing*, Information Security and Cryptology, Third SKLOIS Conference, Inscrypt 2007, Xining, China, August 31 - September 5, 2007, Revised Selected Papers (Dingyi Pei, Moti Yung, Dongdai Lin, and Chuankun Wu, eds.), Lecture Notes in Computer Science, vol. 4990, Springer, 2007, pp. 358–371.

[ECC97] *The Certicom ECC Challenge*, `https://www.certicom.com/index.php/the-certicom-ecc-challenge`, 1997.

[EF17] Christian Eder and Jean-Charles Faugère, *A survey on signature-based algorithms for computing Gröbner bases*, J. Symb. Comput. **80** (2017), 719–784.

[EP10] Christian Eder and John Edward Perry, *F5C: A variant of Faugère's F5 algorithm with reduced Gröbner bases*, J. Symb. Comput. **45** (2010), no. 12, 1442–1458.

[EP11] Christian Eder and John Edward Perry, *Signature-based algorithms to compute Gröbner bases*, Symbolic and Algebraic Computation, International Symposium, ISSAC 2011 (co-located with FCRC 2011), San Jose, CA, USA, June 7-11, 2011, Proceedings (Éric Schost and Ioannis Z. Emiris, eds.), ACM, 2011, pp. 99–106.

[ES03] Niklas Eén and Niklas Sörensson, *An Extensible SAT-solver*, Theory and Applications of Satisfiability Testing, 6th International Conference, SAT 2003. Santa Margherita Ligure, Italy, May 5-8, 2003 Selected Revised Papers (Enrico Giunchiglia and Armando Tacchella, eds.), Lecture Notes in Computer Science, vol. 2919, Springer, 2003, pp. 502–518.

[Eve87] Jan-Hendrik Evertse, *Linear Structures in Blockciphers*, Advances in Cryptology - EUROCRYPT '87, Workshop on the Theory and Application of of Cryptographic Techniques, Amsterdam, The Netherlands, April 13-15, 1987, Proceedings (David Chaum and Wyn L. Price, eds.), Lecture Notes in Computer Science, vol. 304, Springer, 1987, pp. 249–266.

[Fau99] Jean-Charles Faugère, *A new efficient algorithm for computing Gröbner bases (F4).*, Journal of Pure and Applied Algebra **139** (1999), no. 1–3, 61–88.

[Fau02] Jean Charles Faugère, *A New Efficient Algorithm for Computing GrÖBner Bases Without Reduction to Zero (F5)*, Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ISSAC '02, ACM, 2002, pp. 75–83.

[Fau10] Jean-Charles Faugère, *FGb: A Library for Computing Gröbner Bases*, Mathematical Software - ICMS 2010, Third International Congress on Mathematical Software, Kobe, Japan, September 13-17, 2010. Proceedings (Komei Fukuda, Joris van der Hoeven, Michael Joswig, and Nobuki Takayama, eds.), Lecture Notes in Computer Science, vol. 6327, Springer, 2010, pp. 84–87.

[FB09] Giordano Fusco and Eric Bach, *Phase transition of multivariate polynomial systems*, Mathematical Structures in Computer Science **19** (2009), 9–23.

[Feo17] Luca De Feo, *Mathematics of Isogeny Based Cryptography*, CoRR **abs/1711.04062** (2017).

[FGLM93] Jean-Charles Faugère, Patrizia M. Gianni, Daniel Lazard, and Teo Mora, *Efficient Computation of Zero-Dimensional Gröbner Bases by Change of Ordering*, J. Symb. Comput. **16** (1993), no. 4, 329–344.

[FGP+15] Jean-Charles Faugère, Danilo Gligoroski, Ludovic Perret, Simona Samardjiska, and Enrico Thomae, *A Polynomial-Time Key-Recovery Attack on MQQ Cryptosystems*, Public-Key Cryptography - PKC 2015 - 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, March 30 - April 1, 2015, Proceedings (Jonathan Katz, ed.), Lecture Notes in Computer Science, vol. 9020, Springer, 2015, pp. 150–174.

[FIH+23] Hiroki Furue, Yasuhiko Ikematsu, Fumitaka Hoshino, Tsuyoshi Takagi, Kan Yasuda, Toshiyuki Miyazawa, Tsunekazu Saito, and Akira Nagai, *QR-UOV Specification*, Tech. report, National Institute for Standards and Technology (NIST), 2023.

[FJ03] Jean-Charles Faugère and Antoine Joux, *Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases*, in Boneh [Bon03], pp. 44–60.

[FLP08] Jean-Charles Faugère, Françoise Levy-dit-Vehel, and Ludovic Perret, *Cryptanalysis of MinRank*, Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings (David A. Wagner, ed.), Lecture Notes in Computer Science, vol. 5157, Springer, 2008, pp. 280–296.

[FOPT10] Jean-Charles Faugère, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich, *Algebraic Cryptanalysis of McEliece Variants with Compact Keys*, Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings (Henri Gilbert, ed.), Lecture Notes in Computer Science, vol. 6110, Springer, 2010, pp. 279–298.

[FPR17a] Jean-Charles Faugère, Ludovic Perret, and Jocelyn Ryckeghem, *DualModeMS : A Dual Mode for Multivariate-based Signature*, Tech. report, National Institute for Standards and Technology (NIST), 2017.

[FPR+17b] Jean-Charles Faugère, Ludovic Perret, Jocelyn Ryckeghem, A. Casanova, Jacques Patarin, and Gilles Macario-Rat, *GeMSS : A Great Multivariate Short Signature*, Tech. report, National Institute for Standards and Technology (NIST), 2017.

[FR23] Thibauld Feneuil and Matthieu Rivain, *MQOM: MQ on my Mind*, Tech. report, National Institute for Standards and Technology (NIST), 2023.

[Gam84] Taher El Gamal, *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*, Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings (G. R. Blakley and David Chaum, eds.), Lecture Notes in Computer Science, vol. 196, Springer, 1984, pp. 10–18.

[GCF+23] Louis Goubin, Benoît Cogliati, Jean-Charles Faugère, Pierre-Alain Fouque, Robin Larrieu, Gilles Macario-Rat, Brice Minaud, and Jacques Patarin, *PROV: PRovable unbalanced Oil and Vinegar*, Tech. report, National Institute for Standards and Technology (NIST), 2023.

[GEG+17] Ambros Gleixner, Leon Eifler, Tristan Gally, Gerald Gamrath, Patrick Gemander, Robert Lion Gottwald, Gregor Hendel, Christopher Hojny, Thorsten Koch, Matthias Miltenberger, Benjamin Müller, Marc E. Pfetsch, Christian Puchert, Daniel Rehfeldt, Franziska Schlösser, Felipe Serrano, Yuji Shinano, Jan Merlin Viernickel, Stefan Vigerske, Dieter Weninger, Jonas T. Witt, and Jakob Witzig, *The SCIP Optimization Suite 5.0*, Tech. Report 17-61, ZIB, Takustr. 7, 14195 Berlin, 2017.

[GGV10] Shuhong Gao, Yinhua Guan, and Frank Volny, IV, *A New Incremental Algorithm for Computing Groebner Bases*, Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ISSAC '10, ACM, 2010, pp. 13–19.

[GIW16] Shuhong Gao, Frank Volny IV, and Mingsheng Wang, *A new framework for computing Gröbner bases*, Math. Comput. **85** (2016), no. 297, 449–465.

[GM88] Rüdiger Gebauer and H. Michael Möller, *On an Installation of Buchberger's Algorithm*, J. Symb. Comput. **6** (1988), no. 2/3, 275–286.

[Gol94] Jovan Dj. Golic, *Linear Cryptanalysis of Stream Ciphers*, in Preneel [Pre95], pp. 154–169.

[Gur16] Gurobi Optimization, Inc., *Gurobi Optimizer Reference Manual*, 2016.

[HA10] Amir Hashemi and Gwénolé Ars, *Extended F_5 criteria*, J. Symb. Comput. **45** (2010), no. 12, 1330–1340.

[HB13] Heliang Huang and Wansu Bao, *Middle-Solving F4 to Compute Grobner bases for Cryptanalysis over GF(2)*, CoRR **abs/1310.2332** (2013).

[HCN19] Miia Hermelin, Joo Yeon Cho, and Kaisa Nyberg, *Multidimensional Linear Cryptanalysis*, J. Cryptology **32** (2019), no. 1, 1–34.

[HDRM23] Solane El Hirch, Joan Daemen, Raghvendra Rohit, and Rusydi H. Makarim, *Twin Column Parity Mixers and Gaston - A New Mixing Layer and Permutation*, Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part III (Helena Handschuh and Anna Lysyanskaya, eds.), Lecture Notes in Computer Science, vol. 14083, Springer, 2023, pp. 475–506.

[Hel94] Tor Helleseth (ed.), *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, Lecture Notes in Computer Science, vol. 765, Springer, 1994.

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, *NTRU: A Ring-Based Public Key Cryptosystem*, Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings (Joe Buhler, ed.), Lecture Notes in Computer Science, vol. 1423, Springer, 1998, pp. 267–288.

[IM85] Hideki Imai and Tsutomu Matsumoto, *Algebraic Methods for Constructing Asymmetric Cryptosystems*, Algebraic Algorithms and Error-Correcting Codes, 3rd International Conference, AAECC-3, Grenoble, France, July 15-19, 1985, Proceedings (Jacques Calmet, ed.), Lecture Notes in Computer Science, vol. 229, Springer, 1985, pp. 108–119.

[JDF11] David Jao and Luca De Feo, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, Post-Quantum Cryptography (PQCrypto 2011), Springer, 2011, pp. 19–34.

[JJGvD13] Christopher Jefferson, Peter Jeavons, Martin James Green, and Marc R. C. van Dongen, *Representing and solving finite-domain constraint problems using systems of polynomials*, Ann. Math. Artif. Intell. **67** (2013), no. 3-4, 359–382.

[JV11] Antoine Joux and Vanessa Vitse, *A Variant of the F4 Algorithm*, Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings (Aggelos Kiayias, ed.), Lecture Notes in Computer Science, vol. 6558, Springer, 2011, pp. 356–375.

[JV17] Antoine Joux and Vanessa Vitse, *A Crossbred Algorithm for Solving Boolean Polynomial Systems*, Number-Theoretic Methods in Cryptology - First International Conference, NuTMiC 2017, Warsaw, Poland, September 11-13, 2017, Revised Selected Papers (Jerzy Kaczorowski, Josef Pieprzyk, and Jacek Pomykala, eds.), Lecture Notes in Computer Science, vol. 10737, Springer, 2017, pp. 3–21.

[Ker83] Auguste Kerckhoffs, *La Cryptographie Militaire*, Journal des Sciences Militaires **IX** (1883), 5–83.

[Knu94] Lars R. Knudsen, *Truncated and Higher Order Differentials*, in Preneel [Pre95], pp. 196–211.

[KPG99] Aviad Kipnis, Jacques Patarin, and Louis Goubin, *Unbalanced Oil and Vinegar Signature Schemes*, in Stern [Ste99], pp. 206–222.

[KR96] Lars R. Knudsen and Matthew J. B. Robshaw, *Non-Linear Approximations in Linear Cryptanalysis*, in Maurer [Mau96], pp. 224–236.

[KR00] Martin Kreuzer and Lorenzo Robbiano, *Computational Commutative Algebra 1*, Springer Berlin Heidelberg, 2000.

[Kra93] David Kravitz, *Digital Signature Algorithm*, U.S. Patent #5,231,668, 1993.

[KS99] Aviad Kipnis and Adi Shamir, *Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization*, Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings (Michael J. Wiener, ed.), Lecture Notes in Computer Science, vol. 1666, Springer, 1999, pp. 19–30.

[Lai94] Xuejia Lai, *Additive and Linear Structures of Cryptographic Functions*, in Preneel [Pre95], pp. 75–85.

[Lev73] L. A. Levin, *Universal enumeration problems*, Problemy Peredači Informacii **9** (1973), no. 3, 115–116. MR 0340042

[LH94] Susan K. Langford and Martin E. Hellman, *Differential-Linear Cryptanalysis*, Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings (Yvo Desmedt, ed.), Lecture Notes in Computer Science, vol. 839, Springer, 1994, pp. 17–25.

[Ln23] Ignacio Luengo and Martín Avenda no, *DME: MULTIVARIATE SIGNATURE PUBLIC KEY SCHEME*, Tech. report, National Institute for Standards and Technology (NIST), 2023.

[LPT+17] Daniel Lokshtanov, Ramamohan Paturi, Suguru Tamaki, R. Ryan Williams, and Huacheng Yu, *Beating Brute Force for Systems of Polynomial Equations over Finite Fields*, Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2017, Barcelona, Spain, Hotel Porta Fira, January 16-19 (Philip N. Klein, ed.), SIAM, 2017, pp. 2190–2202.

[Luc78] Edouard Lucas, *Théorie des Fonctions Numériques Simplement Périodiques*, American Journal of Mathematics **1** (1878), no. 2, 184–196.

[Lue17] Ignacio Luengo, *DME : A Public Key, Signature, and KEM System Based on Double Exponentiation with Matrix Exponents*, Tech. report, ICMAT and Department of Algebra, Geometry, and Topology, Complutense University of Madrid, Plaza de Las Ciencias S/N, CIUDAD Universitaria 28040 Madrid, Spain, 2017.

[MAAT02] Mohammed Mrayati, Yahya Meer Alam, and M. Hassan At-Tayyan, *Al-Kindi's Treatise on Cryptanalysis*, Series on Arabic Origins of Cryptology, vol. one, KFCRIS & KACST, 2002.

[MAB+21] Carlos Aguilar Melchor, Nicolas Aragon, Emanuele Bellini, Florian Caullery, Rusydi H. Makarim, and Chiara Marcolla, *Constant Time Algorithms for ROLLO-I-128*, SN Comput. Sci. **2** (2021), no. 5, 382.

[Mak18] Andrew O. Makhorin, *GNU Linear Programming Kit*, 2018.

[Map18] Maplesoft, a division of Waterloo Maple Inc., Waterloo, Ontario, *Maple 2018*, `https://www.maplesoft.com/`, 2018.

[Mat93] Mitsuru Matsui, *Linear Cryptanalysis Method for DES Cipher*, in Helleseth [Hel94], pp. 386–397.

[Mat97] Mitsuru Matsui, *New Block Encryption Algorithm MISTY*, Fast Software Encryption, 4th International Workshop, FSE '97, Haifa, Israel, January 20-22, 1997, Proceedings (Eli Biham, ed.), Lecture Notes in Computer Science, vol. 1267, Springer, 1997, pp. 54–68.

[Mau96] Ueli M. Maurer (ed.), *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding*, Lecture Notes in Computer Science, vol. 1070, Springer, 1996.

[MCD$^+$09] Mohamed Saied Emam Mohamed, Daniel Cabarcas, Jintai Ding, Johannes A. Buchmann, and Stanislav Bulygin, *MXL_3: An Efficient Algorithm for Computing Gröbner Bases of Zero-Dimensional Ideals*, Information, Security and Cryptology - ICISC 2009, 12th International Conference, Seoul, Korea, December 2-4, 2009, Revised Selected Papers (Dong Hoon Lee and Seokhie Hong, eds.), Lecture Notes in Computer Science, vol. 5984, Springer, 2009, pp. 87–100.

[MDBW09] Mohamed Saied Emam Mohamed, Jintai Ding, Johannes A. Buchmann, and Fabian Werner, *Algebraic Attack on the MQQ Public Key Cryptosystem*, Cryptology and Network Security, 8th International Conference, CANS 2009, Kanazawa, Japan, December 12-14, 2009. Proceedings (Juan A. Garay, Atsuko Miyaji, and Akira Otsuka, eds.), Lecture Notes in Computer Science, vol. 5888, Springer, 2009, pp. 392–401.

[Mer78] Ralph C. Merkle, *Secure Communications Over Insecure Channels*, Commun. ACM **21** (1978), no. 4, 294–299.

[MH78] Ralph C. Merkle and Martin E. Hellman, *Hiding information and signatures in trapdoor knapsacks*, IEEE Trans. Information Theory **24** (1978), no. 5, 525–530.

[MHT13] Hiroyuki Miura, Yasufumi Hashimoto, and Tsuyoshi Takagi, *Extended Algorithm for Solving Underdefined Multivariate Quadratic Equations*, Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013. Proceedings (Philippe Gaborit, ed.), Lecture Notes in Computer Science, vol. 7932, Springer, 2013, pp. 118–135.

[Min95] S. Minato, *Implicit manipulation of polynomials using zero-suppressed BDDs*, Proceedings the European Design and Test Conference. ED TC 1995, Mar 1995, pp. 449–454.

[MMDB08] Mohamed Saied Emam Mohamed, Wael Said Abd Elmageed Mohamed, Jintai Ding, and Johannes A. Buchmann, *MXL2: Solving Polynomial Equations over GF(2) Using an Improved Mutant Strategy*, Post-Quantum Cryptography, Second International Workshop, PQCrypto 2008, Cincinnati, OH, USA, October 17-19, 2008, Proceedings (Johannes A. Buchmann and Jintai Ding, eds.), Lecture Notes in Computer Science, vol. 5299, Springer, 2008, pp. 203–215.

[MMR91] Harold F. Mattson, Teo Mora, and T. R. N. Rao (eds.), *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 9th International Symposium, AAECC-9, New Orleans, LA, USA, October 7-11, 1991, Proceedings*, Lecture Notes in Computer Science, vol. 539, Springer, 1991.

[Mon16] David Monniaux, *A Survey of Satisfiability Modulo Theory*, CoRR **abs/1606.04786** (2016).

[Mos14] Michele Mosca (ed.), *Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October*

1-3, 2014. Proceedings, Lecture Notes in Computer Science, vol. 8772, Springer, 2014.

[MP08] Sean Murphy and Maura B. Paterson, *A geometric view of cryptographic equation solving*, J. Mathematical Cryptology **2** (2008), no. 1, 63–107.

[MP15] Michael Monagan and Roman Pearce, *A Compact Parallel Implementation of F4*, Proceedings of the 2015 International Workshop on Parallel Symbolic Computation (New York, NY, USA), PASCO '15, ACM, 2015, pp. 95–100.

[MR22] Rusydi H. Makarim and Raghvendra Rohit, *Towards Tight Differential Bounds of Ascon A Hybrid Usage of SMT and MILP*, IACR Trans. Symmetric Cryptol. **2022** (2022), no. 3, 303–340.

[MS89a] Willi Meier and Othmar Staffelbach, *Fast Correlation Attacks on Certain Stream Ciphers*, J. Cryptology **1** (1989), no. 3, 159–176.

[MS89b] Willi Meier and Othmar Staffelbach, *Nonlinearity Criteria for Cryptographic Functions*, Advances in Cryptology - EUROCRYPT '89, Workshop on the Theory and Application of of Cryptographic Techniques, Houthalen, Belgium, April 10-13, 1989, Proceedings (Jean-Jacques Quisquater and Joos Vandewalle, eds.), Lecture Notes in Computer Science, vol. 434, Springer, 1989, pp. 549–562.

[MS17] Rusydi H. Makarim and Marc Stevens, *M4GB: An Efficient Gröbner-Basis Algorithm*, Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2017, Kaiserslautern, Germany, July 25-28, 2017 (Michael A. Burr, Chee K. Yap, and Mohab Safey El Din, eds.), ACM, 2017, pp. 293–300.

[MT14] 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 2014, Istanbul, Turkey, September 1-2, 2014, Revised Selected Papers (Thomas Eisenbarth and Erdinç Öztürk, eds.), Lecture Notes in Computer Science, vol. 8898, Springer, 2014, pp. 109–125.

[MvOV96] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[Nat77] National Bureau of Standards (NBS), *Data Encryption Standard*, U.S. Department of Commerce, Washington DC, publication 46 ed., 1977.

[Neu13] Severin Neumann, *A modified parallel F4 algorithm for shared and distributed memory architectures*, 5th International Symposium on Symbolic Computation in Software Science, SCSS 2013, Castle of Hagenberg, Austria (Laura Kovács and Temur Kutsia, eds.), EPiC Series in Computing, vol. 15, EasyChair, 2013, pp. 70–80.

[Nin17] Kai-Chun Ning, *An Adaptation of the Crossbred Algorithm for Solving Multivariate Quadratic Systems over $\mathbb{F}_2$ on GPUs*, November 2017, Available at `https://pure.tue.nl/ws/portalfiles/portal/91105984/NING.K_parallel_cb_v103.pdf`.

[NIS01] NIST, *FIPS 197 - Advanced Encryption Standard (AES)*, November 2001.

[NIS20] NIST, *Post-Quantum Cryptography, Round 3 Submissions*, July 2020.

[NIS22] NIST, *Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process*, October 2022.

[NNY18] Ruben Niederhagen, Kai-Chun Ning, and Bo-Yin Yang, *Implementing Joux-Vitse's Crossbred Algorithm for Solving $${\mathcal M\mathcal Q}$$ Systems over* $\mathbf{F}_2$ *on GPUs*, Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings (Tanja Lange and Rainer Steinwandt, eds.), Lecture Notes in Computer Science, vol. 10786, Springer, 2018, pp. 121–141.

[Nyb92] Kaisa Nyberg, *On the Construction of Highly Nonlinear Permutations*, Advances in Cryptology - EUROCRYPT '92, Workshop on the Theory and Application of of Cryptographic Techniques, Balatonfüred, Hungary, May 24-28, 1992, Proceedings (Rainer A. Rueppel, ed.), Lecture Notes in Computer Science, vol. 658, Springer, 1992, pp. 92–98.

[Nyb93] Kaisa Nyberg, *Differentially Uniform Mappings for Cryptography*, in Helleseth [Hel94], pp. 55–64.

[Pat96] Jacques Patarin, *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms*, in Maurer [Mau96], pp. 33–48.

[PBD14] Jaiberth Porras, John Baena, and Jintai Ding, *ZHFE, a New Multivariate Public Key Encryption Scheme*, in Mosca [Mos14], pp. 229–245.

[PCDY17] Albrecht Petzoldt, Ming-Shing Chen, Jintai Ding, and Bo-Yin Yang, *HMFEv - An Efficient Multivariate Signature Scheme*, Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26-28, 2017, Proceedings (Tanja Lange and Tsuyoshi Takagi, eds.), Lecture Notes in Computer Science, vol. 10346, Springer, 2017, pp. 205–223.

[PCF+23] Jacques Patarin, Benoît Cogliati, Jean-Charles Faugère, Pierre-Alain Fouque, Louis Goubin, Robin Larrieu, Gilles Macario-Rat, and Brice Minaud, *Vox Specification*, Tech. report, National Institute for Standards and Technology (NIST), 2023.

[PFH$^+$] Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang, *FALCON: Fast-Fourier Lattice-based Compact Signatures over NTRU.*

[Pre95] Bart Preneel (ed.), *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, Lecture Notes in Computer Science, vol. 1008, Springer, 1995.

[Pre11] Bart Preneel, *Modes of Operation of a Block Cipher*, Encyclopedia of Cryptography and Security, 2nd Ed. (Henk C. A. van Tilborg and Sushil Jajodia, eds.), Springer, 2011, pp. 789–794.

[Pro99] Third Generation Partnership Project, *KASUMI Specification*, Tech. Report version 1.0, Security Algorithms Group of Experts (SAGE), 1999.

[Rad06] Håvard Raddum, *Cryptanalytic Results on Trivium*, Tech. report, eSTREAM Report 2006/039, 2006.

[RN10] Stuart Russell and Peter Norvig, *Artifical Intelligence, a Modern Approach*, third ed., Series in Artificial Intelligence, Prentice Hall, 2010.

[Rod23a] Borja Gómez Rodríguez, *3WISE: Cubic Element-Wise trapdoor based MPKC cryptosystem*, Tech. report, National Institute for Standards and Technology (NIST), 2023.

[Rod23b] Borja Gómez Rodríguez, *HPPC: Hidden Product of Polynomial Composition*, Tech. report, National Institute for Standards and Technology (NIST), 2023.

[RS06] Håvard Raddum and Igor A. Semaev, *New Technique for Solving Sparse Equation Systems*, IACR Cryptology ePrint Archive **2006** (2006), 475.

[RS08] Håvard Raddum and Igor A. Semaev, *Solving Multiple Right Hand Sides linear equations*, Des. Codes Cryptography **49** (2008), no. 1-3, 147–160.

[RS12] Bjarke Hammersholt Roune and Michael Stillman, *Practical Gröbner basis computation*, in van der Hoeven and van Hoeij [vdHvH12], pp. 203–210.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Commun. ACM **21** (1978), no. 2, 120–126.

[RSA91] *The RSA Factoring Challenge*, `http://www.emc.com/emc-plus/rsa-labs/historical/the-rsa-factoring-challenge.htm`, 1991.

[Sak98] Shojiro Sakata, *Gröbner Bases and Coding Theory*, London Mathematical Society Lecture Note Series, p. 205–220, Cambridge University Press, 1998.

[SDGM00] Leonie Ruth Simpson, Ed Dawson, Jovan Dj. Golic, and William Millan, *LILI Keystream Generator*, in Stinson and Tavares [ST01], pp. 248–261.

[SG14] Simona Samardjiska and Danilo Gligoroski, *Linearity Measures for Multivariate Cryptography*, SECURWARE 2014, The Eighth International Conference on Emerging Security Information, Systems and Technologies, International Academy, Research and Industry Association (IARIA), 2014, pp. 157–166.

[Sha49] Claude E. Shannon, *Communication theory of secrecy systems*, Bell Labs Technical Journal **28** (1949), no. 4, 656–715.

[Sho97] Peter W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J. Comput. **26** (1997), no. 5, 1484–1509.

[Sho08] Victor Shoup, *A Computational Introduction to Number Theory and Algebra*, vol. 2, Cambridge University Press, 2008.

[Sie85] Thomas Siegenthaler, *Decrypting a Class of Stream Ciphers Using Ciphertext Only*, IEEE Trans. Computers **34** (1985), no. 1, 81–85.

[Sin00] Simon Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor Books, 2000.

[SNC09] Mate Soos, Karsten Nohl, and Claude Castelluccia, *Extending SAT Solvers to Cryptographic Problems*, Theory and Applications of Satisfiability Testing - SAT 2009, 12th International Conference, SAT 2009, Swansea, UK, June 30 - July 3, 2009. Proceedings (Oliver Kullmann, ed.), Lecture Notes in Computer Science, vol. 5584, Springer, 2009, pp. 244–257.

[Soo16] Mate Soos, *The CryptoMiniSat 5 set of solvers at SAT Competition 2016*, Proceedings of SAT Competition 2016: Solver and Benchmark Descriptions - SAT Competition 2016, 2016, Available at `https://github.com/msoos/cryptominisat`, p. 28.

[SPK17] Kyung-Ah Shim, Cheol-Min Park, and Aeyoung Kim, *HiMQ-3 : A High Speed Signature Scheme based on Multivariate Quadratic Equations*, Tech. report, National Institute for Standards and Technology (NIST), 2017.

[SSM$^+$09] Massimiliano Sala, Shojiro Sakata, Teo Mora, Carlo Traverso, and Ludovic Perret (eds.), *Gröbner Bases, Coding, and Cryptography*, Springer Berlin Heidelberg, 2009.

[ST01] Douglas R. Stinson and Stafford E. Tavares (eds.), *Selected Areas in Cryptography, 7th Annual International Workshop, SAC 2000, Waterloo, Ontario, Canada, August 14-15, 2000, Proceedings*, Lecture Notes in Computer Science, vol. 2012, Springer, 2001.

[ST23] Kosuke Sakata and Tsuyoshi Takagi, *An Efficient Algorithm for Solving the MQ Problem using Hilbert Series*, Cryptology ePrint Archive, Paper 2023/1650, 2023, `https://eprint.iacr.org/2023/1650`.

[Ste99] Jacques Stern (ed.), *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding*, Lecture Notes in Computer Science, vol. 1592, Springer, 1999.

[Ste24] Matthias Johann Steiner, *The Complexity of Algebraic Algorithms for LWE*, Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part III (Marc Joye and Gregor Leander, eds.), Lecture Notes in Computer Science, vol. 14653, Springer, 2024, pp. 375–403.

[SVP10] *The Lattice Challenge*, `http://www.latticechallenge.org/`, 2010.

[TDTD13] Chengdong Tao, Adama Diene, Shaohua Tang, and Jintai Ding, *Simple Matrix Scheme for Encryption*, Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013. Proceedings (Philippe Gaborit, ed.), Lecture Notes in Computer Science, vol. 7932, Springer, 2013, pp. 231–242.

[The18] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 8.3.0)*, 2018, `http://www.sagemath.org`.

[UM17] Putranto H. Utomo and Rusydi H. Makarim, *Solving a Binary Puzzle*, Mathematics in Computer Science **11** (2017), no. 3-4, 515–526.

[UP15] Putranto H. Utomo and Ruud Pellikaan, *Binary Puzzles as an Erasure Decoding Problem*, Proceedings of the 36th Symposium on Information Theory in the Benelux and the 5th Joint WIC/IEEE Symposium on Information Theory and Signal Processing in the Benelux (Jérémie Roland and François Horlin, eds.), 2015.

[UP17] Putranto H. Utomo and Ruud Pellikaan, *Binary Puzzles as a SAT Problem*, Proceedings of the 2017 Symposium on Information Theory and Signal Processing in the Benelux (Richard Heusdens and Jos Weber, eds.), 2017.

[Uto17] Putranto Utomo, *Satisfiability modulo theory and binary puzzle*, Journal of Physics: Conference Series **855** (2017), no. 1, 012057.

[vdHvH12] Joris van der Hoeven and Mark van Hoeij (eds.), *International Symposium on Symbolic and Algebraic Computation, ISSAC'12, Grenoble, France - July 22 - 25, 2012*, ACM, 2012.

[VDI24] Damien Vidal, Claire Delaplace, and Sorina Ionica, *An analysis of the Crossbred Algorithm for the MQ Problem*, IACR Commun. Cryptol. **1** (2024), no. 3, 36.

[vzG15] Joachim von zur Gathen, *CryptoSchool*, Springer, 2015.

[Wan98] Dongming Wang, *Gröbner Bases Applied to Geometric Theorem Proving and Discovering*, London Mathematical Society Lecture Note Series, p. 281–302, Cambridge University Press, 1998.

[WCD+23] Lih-Chung Wang, Chun-Yen Chou, Jintai Ding, Yen-Liang Kuan, Ming-Siou Li, Bo-Shu Tseng, Po-En Tseng, and Chia-Chun Wang, *SNOVA Proposal for NISTPQC: Digital Signature Schemes project*, Tech. report, National Institute for Standards and Technology (NIST), 2023.

[WHL+05] Lih-Chung Wang, Yuh-Hua Hu, Feipei Lai, Chun-yen Chou, and Bo-Yin Yang, *Tractable Rational Map Signature*, Public Key Cryptography - PKC 2005, 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, 2005, Proceedings (Serge Vaudenay, ed.), Lecture Notes in Computer Science, vol. 3386, Springer, 2005, pp. 244–257.

[Wie86] Douglas H. Wiedemann, *Solving sparse linear equations over finite fields*, IEEE Trans. Inf. Theory **32** (1986), no. 1, 54–62.

[Wol05] Christopher Wolf, *Multivariate Quadratic Polynomials in Public-Key Cryptography*, Ph.D. thesis, Katholieke Universiteit Leuven, November 2005.

[YCC04] Bo-Yin Yang, Jiun-Ming Chen, and Nicolas Courtois, *On Asymptotic Security Estimates in XL and Gröbner Bases-Related Algebraic Cryptanalysis*, Information and Communications Security, 6th International Conference, ICICS 2004, Malaga, Spain, October 27-29, 2004, Proceedings (Javier López, Sihan Qing, and Eiji Okamoto, eds.), Lecture Notes in Computer Science, vol. 3269, Springer, 2004, pp. 401–413.

[YDH+15a] Takanori Yasuda, Xavier Dahan, Yun-Ju Huang, Tsuyoshi Takagi, and Kouichi Sakurai, *MQ Challenge: Hardness Evaluation of Solving Multivariate Quadratic Problems*, IACR Cryptology ePrint Archive **2015** (2015), 275.

[YDH+15b] Takanori Yasuda, Xavier Dahan, Yun-Ju Huang, Tsuyoshi Takagi, and Kouichi Sakurai, *A multivariate quadratic challenge toward post-quantum generation cryptography*, ACM Comm. Computer Algebra **49** (2015), no. 3, 105–107.

Notations

$\mathbb{Z}$	Ring of integers	49
$\mathbb{Z}_{\geq 0}$	The set of non-negative integers	49
$\mathbb{F}$	A field	49
$\mathbb{F}_q$	Finite field of order q	49
$\deg(f)$	The degree of the polynomial f	51
$\mathbb{F}[x_1,\ldots,x_n]$	An n-variable polynomial ring over the field $\mathbb{F}$	50
$\mathcal{R}$	The ring $\mathbb{F}[x_1,\ldots,x_n]$ unless explicitly stated otherwise	50
$\langle f_1,\ldots,f_m\rangle$	Ideal generated by $f_1,\ldots,f_m \in \mathbb{F}[x_1,\ldots,x_n]$	51
$x^\alpha \mid x^\beta$	Monomial x^α divides x^β	49
$\mathsf{M}(f)$	The set of monomials of $f \in \mathbb{F}[x_1,\ldots,x_n]$	50
$\mathsf{T}(f)$	The set of terms of $f \in \mathbb{F}[x_1,\ldots,x_n]$	50
$\mathsf{M}(F)$	The set of monomials of $F \subseteq \mathbb{F}[x_1,\ldots,x_n]$	50
$\mathsf{T}(F)$	The set of terms of $F \subseteq \mathbb{F}[x_1,\ldots,x_n]$	50
$\mathsf{LC}(f)$	The leading coefficient of a polynomial $f \neq 0$	53
$\mathsf{LM}(f)$	The leading monomial of a polynomial $f \neq 0$	53
$\mathsf{LT}(f)$	The leading term of a polynomial $f \neq 0$	53
$\mathsf{Tail}(f)$	The tail of a polynomial $f \neq 0$	53
$\overline{f}^G$	The remainder after division of f by an ordered set G	55
$\mathbf{V}(f_1,\ldots,f_m)$	The affine variety defined by the polynomials $f_1,\ldots,f_m$	59
$\mathbf{I}(V)$	The ideal of affine variety V	60
I_ℓ	The ℓ-th elimination ideal	60
$\mathsf{Spoly}(f,g)$	S-polynomial of $f \neq 0$ and $g \neq 0$	65
$\mathsf{LCM}(a,b)$	The least common multiple of a and b	65
$f \underset{G}{\longrightarrow} r$	f reduces to r modulo G	67
$\widetilde{F}$	(reduced) row echelon form of $F \subseteq \mathcal{R}$	72
$\mathrm{wt}(u)$	The Hamming weight of $u \in \mathbb{F}_2^n$	120
$v \preceq w$	The vector v is covered by w	120
φ_f	The pseudo Boolean function of f	121
$v(f)$	The simplified value vector of a symmetric Boolean function f	121
$\sigma_{i,n}$	The i-th elementary symmetric polynomial in n variables	122
$\mathsf{FP}(\mathcal{R})$	The set of field polynomials of $\mathcal{R} = \mathbb{F}_q[x_1,\ldots,x_n]$	133
$\boldsymbol{v} \parallel \boldsymbol{w}$	Concatenation of vector $\boldsymbol{v} \in \mathbb{F}_2^n$ and $\boldsymbol{w} \in \mathbb{F}_2^m$	133
$\boldsymbol{v} \cdot \boldsymbol{w}$	The dot product of $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{F}_2^n$	133
$S_{\boldsymbol{b}}$	The function $\boldsymbol{b} \cdot S(x)$ where $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$	133
$\mathcal{F}_f, \mathcal{W}_f$	The Fourier and Walsh transform of $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ respectively	134
$\lambda_S(\boldsymbol{a},\boldsymbol{b})$	The linear approximation table of S	135
$\lambda I_S(\boldsymbol{a},\boldsymbol{b})$	The linear ideal of S	135
$\delta_S(\boldsymbol{\alpha},\boldsymbol{\beta})$	The difference distribution table of S	138
$\delta I_S(\boldsymbol{\alpha},\boldsymbol{\beta})$	The differential ideal of S	139

Index

List of Algorithms

List of Figures

List of Tables