Journal or Formally Refereed Conference Articles

LNCS is the series of Lecture Notes in Computer Science by Springer-Verlag, EI.

1. J. Almeida, M. Barbosa, G. Barthe, L. Blatter, G. Delerue, J. Duarte, B. Gregoire, T. Oliveira, M. Quaresma, P. Strub, M. Tsai, B. Wang, and B.-Y. YANG, *Jazzline: Composable CryptoLine functional correctness proofs for Jasmin programs*, ACM CCS 2025(a) **to appear**.

2. C.-M. Chiu, J. Liu, X. Shi, M.-H. Tsai, B.-Y. Wang and B.-Y. YANG, *Algebraic Linear Analysis for Number Theoretic Transform in Lattice-Based Cryptography*, IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), **2025(3)**, **to appear**.

3. Z. Zhao, J. Ding, and B.-Y. YANG. Sieving with Streaming Memory Access. IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), **2025(2)**, pp. 362-384. https://doi.org/10.46586/tches.v2025.i2.362-384

4. D. J. Bernstein, T. Lange, J. Levin, and B.-Y. YANG, *PQConnect: Automated Post-Quantum End-to-End Tunnels*, NDSS 2025 (Network and Distributed Systems Security, February 25-27, San Diego). https://www.ndss-symposium.org/ndss-paper/pqconnect-automated-post-quantum-end

5. L.-J. Jian, T.-Y. Wang, B.-Y. YANG *, and M.-S. Chen, *Jumping for Bernstein-Yang Inversion*, ACISP 2024, LNCS 14896, pp. 1-21.

6. L.-C. Lai, J. Liu, X. Shi, M.-H. Tsai, B.-Y. Wang and B.-Y. YANG, *Automatic Verification of Cryptographic Block Function Implementations with Logical Equivalence Checking* https://eprint.iacr.org/2023/1861, ESORICS 2024, LNCS 14985, pp. 377–395.

7. V. Hwang, C.-T. Liu, and B.-Y. YANG, *Algorithmic Views of Vectorized Polynomial Multipliers - NTRU Prime*, ACNS 2024 (22nd International Conference on Applied Cryptography and Network Security, Abu Dhabi, UAE, 5-8 March), LNCS 14584, pp. 1–23. https://doi.org/10.1007/978-3-031-54773-7_2.

8. R. Chen, J. Liu, X. Shi, M.-H. Tsai, B.-Y. Wang, B.-Y. YANG, llvm2CryptoLine, *Verifying Arithmetic in Cryptographic C Programs*, Proc. ACM ESEC/SIGSOFT FSE 2023 (22nd ESEC/31st SIGSOFT FSE, San Francisco, December 3–9), pp. 2167-2171. https://doi.org/10.1145/3611643.3613096.

9. H.-T. Chen, Y.-H. Chung, V. Hwang, and B.-Y. YANG, *Algorithmic Views of Vectorized Polynomial Multipliers - NTRU*, Indocrypt (24th International Conference on Cryptology in India 2023, December 10–13), LNCS 14460, pp. 177-196. https://eprint.iacr.org/2023/1637.

10. M.-H. Tsai, Y.-F. Fu, J. Liu, X. Shi, B.-Y. Wang, and B.-Y. YANG, *Certified Verification for Algebraic Abstraction*, CAV 2023 (35th International Conference on Computer Aided Verification), LNCS 13966, pp. 329–343. https://doi.org/10.1007/978-3-031-37709-9_16.

11. M.-H. Tsai, Y.-F. Fu, J. Liu, X. Shi, B.-Y. Wang, and B.-Y. YANG, CoqCryptoLine*: A Verified Model Checker with Certified Results*, CAV 2023 (ibid.). https://doi.org/10.1007/978-3-031-37703-7_11, LNCS 13966, pp. 329–343.

12. W. Beullens, M.-S. Chen, S.-H. Hung, Matthias J. Kannwischer, B.-Y. Peng, C.-J. Shih, B.-Y. YANG, *Oil and Vinegar: Modern Parameters and Implementation*, IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), **2023(3)**, pp. 321–365. https://doi.org/10.46586/tches.v2023.i3.321-365.

13. J. Ding, S. Kim, T. Takagi, Y. Wang and B.-Y. YANG, *A physical study of the LLL algorithm*, J. of Number Theory **244**(Mar. 2023), pp. 339-368, https://doi.org/10.1016/j.jnt.2022.09.013.

14. B.-Y. Peng, A. Marotzke, M.-H. Tsai, B.-Y. YANG, and H.-L. Chen, *Streamlined NTRU Prime on FPGA*, Journal of Cryptographic Engineering **13(2)**, pp. 167–186 (2023), https://doi.org/10.1007/s13389-022-00303-z.

15. E. Alkim, V. Hwang, and B.-Y. YANG, Multi-Parameter Support with NTTs for NTRU and NTRU Prime on Cortex-M4, IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), **2022(4)**, pp. 349-371. https://doi.org/10.46586/tches.v2022.i4.349-371

16. V. Hwang, J. Liu, G. Seiler, X. Shi, M.-H. Tsai, B.-Y. Wang, and B.-Y. YANG, Verified NTT Multiplications for NISTPQC KEM Lattice Finalists: Kyber, SABER, and NTRU, IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), **2022(4)**, pp. 718-750. https://doi.org/10.46586/tches.v2022.i4.718-750

17. T.-H. Chang, Y.-T. Kuo, J.-P. Chen, and B.-Y. YANG, Secure Boolean Masking of Gimli - Optimization and Evaluation on the Cortex-M4, ICICS 2022 (24th International Conference on Information and Communications Security, Sept. 5–8, U. of Kent, Canterbury), LNCS 13407, pp. 376-393.

18. H. Becker, V. Hwang, M. J. Kannwischer, L. Panny, and B.-Y. YANG, Efficient Multiplication of Somewhat Small Integers Using Number-Theoretic Transforms. IWSEC 2022 (17th International Workshop on Security, IWSEC 2022, Tokyo, Japan, August 31 – September 2): LNCS 13504, 3-23, ***best paper***.

19. H. Becker, V. Hwang, M. J. Kannwischer, B.-Y. YANG, and S.-Y. Yang, *Neon NTT: Faster Dilithium, Kyber, and Saber on Cortex-A72 and Apple M1*, IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), **2022(1)**, pp. 221–244. https://doi.org/10.46586/tches.v2022.i1.221-244, IACR e-Print 2021/986.

20. A. Abdulrahman, J.-P. Chen, Y.-J. Chen, V. Hwang, M. J. Kannwischer, and B.-Y. YANG, *Multi-moduli NTTs for Saber on Cortex-M3 and Cortex-M4*, IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), **2022(1)**, pp. 127–151. https://doi.org/10.46586/tches.v2022.i1.127-151, IACR e-Print 2021/995.

21. X. Shi, Y.-F. Fu, J. Liu, M.-H. Tsai, B.-Y. Wang, and B.-Y. YANG, *CoqQFBV: A Scalable Certified SMT Quantifier-Free Bit-Vector Solver*, CAV 2021 (Virtual Conference, July 18–24), LNCS 12760, pp. 149–171.

22. P.-C. Kuo, Y.-W. Chen, Y.-C. Hsu, C.-M. Cheng, W.-D. Li, and B.-Y. YANG, *High Performance Post-Quantum Key Exchange on FPGAs*, J. of Information Science and Engineering 37(5), pp. 1211–1229.

23. P.-C. Kuo, C.-M. Cheng, W.-D. Li, and B.-Y. YANG, *Parallelization on Gauss Sieve Algorithm over Ideal Lattice*, J. of Information Science and Engineering 37(5), pp. 1187–1209.

24. T. Chou, M. J. Kannwischer, and B.-Y. YANG, *Rainbow on Cortex-M4*, IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), **2021(4)**, pp.650–675. https://doi.org/10.46586/tches.v2021.i4.650-675, IACR e-Print 2021/532.

25. R. Gonzalez, A. Hülsing, M. J. Kannwischer, J. Krämer, T. Lange, M. Stöttinger, E. Waitz, T. Wiggers, and B.-Y. YANG, *Verifying Post-Quantum Signatures in 8 kB of RAM*. PQCrypto 2021 (virtual conference, July 20–22): LNCS 12841, pp. 215-233.

26. J. Ding, J. Deaton, Vishakha, and B.-Y. YANG, *The Nested Subset Differential Attack — A Practical Direct Attack Against LUOV Which Forges a Signature Within 210 Minutes*, Eurocrypt 2021 (Hybrid: Online and Zagreb, Croatia, October 17–21), LNCS 12696, pp. 329–347.

27. C.-M. M. Chung, V. Hwang, M. J. Kannwischer, G. Seiler, C.-J. Shih and B.-Y. YANG, *NTT Multiplication for NTT-unfriendly Rings, New Speed Records for Saber and NTRU on Cortex-M4 and AVX2*, IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), **2021(2)**, pp. 159–188. https://doi.org/10.46586/tches.v2021.i2.159-188, IACR e-Print 2020/1397.

28. E. Alkim, D. Y.-L. Cheng, C.-M. M. Chung, H. Evkan, L. W.-L. Huang, V. Hwang, C.-L. T. Li, R. Niederhagen, C.J. Shih, J. Wälde, and B.-Y. YANG, *Polynomial Multiplication in NTRU Prime, Comparison of Optimization Strategies on Cortex-M4*, IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), **2021(1),** pp. 217-238. https://doi.org/10.46586/tches.v2021.i1.217-238. *Full version*: IACR e-Print 2020/1216.

29. W.-L. Huang, J.-P. Chen, and B.-Y. YANG, *Power Analysis on NTRU Prime*, IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), 2020(1), pp. 123–151. https://doi.org/10.13154/tches.v2020.i1.123-151.

30. Y.-F. Fu, J. Liu, X. Shi, M.-H. Tsai, B.-Y. Wang, and B.-Y. YANG, *Signed Cryptographic Program Verification with Typed CryptoLine*, ACM CCS 2019 (26th ACM Conference on Computer and Communications Security, November 11–15, London, UK), pp. 1591-1606.

31. J. Liu, X. Shi, M.-H. Tsai, B.-Y. Wang, and B.-Y. YANG, *Verifying Arithmetic in Cryptographic C Programs*, ASE 2019 (34th IEEE/ACM Conference on Automated Software Engineering, November 11–15, San Diego, CA, USA), pp. 552-564.

32. D. J. Bernstein and B.-Y. YANG, *Fast constant-time gcd computation and modular inversion*. IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), **2019(3)**, pp. 340-398. https://doi.org/10.13154/tches.v2019.i3.340-398

33. A. Polyakov, M.-H. Tsai, B.-Y. Wang, and B.-Y. YANG, *Verifying Arithmetic Assembly Programs in Cryptographic Primitives*, Invited Talk and Paper, CONCUR 2018 (September 4–7, Beijing, China): Leibniz International Proceedings in Informatics 118, pp. 4:1–4:16.

34. W.-D. Li, M.-S. Chen, P.-C. Kuo, C.-M. Cheng, and B.-Y. YANG, *Frobenius Additive Fast Fourier Transform*, Proc. ACM ISSAC 2018 (July 15–18, New York City) pp. 1973–1987.

35. D. J. Bernstein and B.-Y. YANG, *Asymptotically faster quantum algorithms to solve multivariate quadratic equations*, PQCrypto 2018 (April 9–11, Fort Lauderdale, Florida, USA), LNCS 10786, pp. 487–506.

36. R. Niederhagen, K.-C. Ning and B.-Y. YANG, *Implementing Joux-Vitse's Crossbred Algorithm for Solving MQ Systems on GPUs*, PQCrypto 2018, *ibid.* pp. 121–141.

37. M.-S. Chen, W.-D. Li, B.-Y. Peng, B.-Y. YANG, and C.-M. Cheng, *Implementing 128-bit Secure MPKC Signatures*, IEICE Transactions vol. E101-A(2018) No. 3, pp. 553–569.

38. M.-H. Tsai, B.-Y. Wang, and B.-Y. YANG *Certified Verification of Algebraic Properties on Low-Level Mathematical Constructs in Cryptographic Programs*, proc. ACM CCS 2017 (24th ACM Conference on Computer and Communications Security, Dallas, TX, USA, Oct. 30-Nov. 3), pp. 1973–1987.

39. A. Petzoldt, M.-S. Chen, J. Ding, and B.-Y. YANG, *HMFEv - An Efficient Multivariate Signature Scheme*, PQCrypto 2017 (Utrecht, the Netherlands, Jun. 26-28), LNCS 10346, pp. 205–223.

40. S.-Y. Yang, P.-C. Kuo, C.-M. Cheng, and B.-Y. YANG, *Gauss Sieve Algorithm on GPUs*, CT-RSA 2017 (San Francisco, Feb. 14–17), LNCS 10159, pp. 39–57.

41. B.-Y. Peng, Y.-C. Hsu, Y.-J. Chen, D.-C. Chueh, C.-M. Cheng, and B.-Y. YANG, *Multi-core FPGA Implementation of ECC with Homogeneous Co-Z Coordinate Representation*, CANS 2016, (Milan, Italy, Nov. 14-16), LNCS 10052, pp. 637–647.

42. A. Petzoldt, M.-S. Chen, B.-Y. YANG, C. Tao, J. Ding: *Design Principles for HFEv- Based Multivariate Signature Schemes*, Asiacrypt 2015 (Auckland, New Zealand, Nov. 29-Dec. 3), LNCS 9452, pp. 311-334.

43. Y.-A. Chang, M.-S. Chen, J.-S. Wu and B.-Y. YANG, *Postquantum SSL/TLS for Embedded Systems*, IoTS workshop at IEEE SOCA 2014 (Matsue, Japan, Nov. 17-19).

44. Y.-F. Chen, C.-H. Hsu, H.-H. Lin, P. Schwabe, M.-H. Tsai, B.-Y. Wang, B.-Y. YANG, and S.-Y. Yang, *Verifying Curve25519 Software*, presented at ACM CCS 2014 (21st ACM Conference on Computer and Communications Security, Scottsdale, Arizona, USA, Nov. 3-7, 2014).

45. Y-J. Huang, W.-C. Hong, C.-M. Cheng, J.-M. Chen, and B.-Y. YANG, *Memory Efficient Variant of an Implementation of the* $\mathbf{F_4}$ *Algorithm for Computing Gröbner Bases*. INTRUST 2014 (6th Trusted Systems Conference, Dec. 16–17, Beijing, China), LNCS 9473, pp. 374-393.

46. R. Fitzpatrick, C. Bischof, J. Buchmann, Ö. Dagdelen, F. Göpfert, A. Mariano, B.-Y. Yang, *Tuning Gauss Sieve for Speed*, Latincrypt 2014 (3rd Latin American Conference on Cryptography and Information Security, Florianopolis, Brazil, Sept. 17-19), LNCS 8895, pp. 288-305.

47. Y.-A. Chang, W.-C. Hong, M.-C. Hsiao, B.-Y. YANG, A.-Y. Wu and C.-M. Cheng, *Hydra: An energy-efficient programmable cryptographic coprocessor supporting elliptic-curve pairings over fields of large characteristics*, IWSEC 2014 (The 9th International Workshop on Security, Hirosaki, Japan, Aug. 27-29, 2014), LNCS 8639, pp. 174–186.

48. J. Y.-C. Yeh, C.-M. Cheng, B.-Y. YANG, *Operating Degrees for XL vs.* $\mathbf{F_4}$/$\mathbf{F_5}$ *for Generic* $\mathcal{MQ}$ *with Number of Equations Linear in That of Variables*, Number Theory and Cryptography Workshop 2013 (November 21-22, TU Darmstadt, Germany), LNCS 8260, pp. 19–33.

49. Y.-H. Chiu, W.-C. Hong, L.-P. Chou, J. Ding, B.-Y. YANG, C.-M. Cheng, *A Practical Attack on Patched MIFARE Classic*. Inscrypt 2013 (Guangzhou, China, November 27-30), Revised Selected Papers. LNCS 8567, pp. 150-164.

50. C. Bouillaguet, C.-M. Cheng, T. Chou, R. Niederhagen and B.-Y. YANG, *Fast Exhaustive Search for Quadratic Systems in* $\mathbf{F_2}$ *on FPGAs*, SAC 2013 (20th workshop on Selected Areas in Cryptography, Aug. 14–16, Simon Fraser University, Burnaby, BC, Canada); LNCS 8282, pp. 205–222. Current version at ePrint 2014/436.

51. M.-S. Chen, C.-M. Cheng, B.-Y. YANG, *RAIDq: A software-friendly, multiple-parity RAID*, USENIX HotStorage 2013 (USENIX Federated Workshops, June 27-28, San Jose, CA, USA).

52. J. Ding, B.-Y. YANG, *Degree of Regularity for HFEv and HFEv-*, PQCrypto 2013 (5th Post-Quantum Cryptography Workshop, June 4–6, Limoges, France), LNCS 7932, pp. 52–66.

53. J.-R. Shih, Y. Hu, M.-C. Hsiao, M.-S. Chen, W.-T. Shen, B.-Y. YANG, and C.-M. Cheng, *Securing M2M with Post-Quantum Public-Key Cryptography*, IEEE Journal on Emerging and Selected Topics in Circuits and Systems, **3:1**(2013), pp. 106–116.

54. T. Chou, C.-M. Cheng, R. Niederhagen, and B.-Y. YANG, *Solving Quadratic Equations with XL on Parallel Architectures*, CHES 2012 (14th workshop on Cryptographic Hardware and Embedded Systems, September 9–12, Leuven, Belgium), LNCS 7428, pp. 356–373.

55. C.-H. Yu and B.-Y. YANG, *Probabilistically Correct Secure Arithmetic Computation for Modular Conversion, Zero Test, Comparison, MOD and Exponentiation*, to appear at SCN 2012 (8th Conference on Security and Cryptography for Networks, September 5-7, Amalfi, Italy), LNCS 7485, pp. 426–444.

56. S. Tanaka, T. Chou, B.-Y. YANG, C.-M. Cheng, K. Sakurai: *Efficient Parallel Evaluation of Multivariate Quadratic Polynomials on GPUs*, WISA 2012 (13th Workshop on Information Security Applications, August 16–18, Jeju Island, Korea), LNCS 7690, pp. 28–42.

57. D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B.-Y. YANG, *High-speed high-security signatures*, Journal of Cryptographic Engineering **2:2**(2012), pp. 77–89. Earlier version presented at CHES 2011 (13th Workshop on Cryptographic Hardware and Embedded Systems, September 28 – October 1, Nara, Japan), LNCS 6917, pp. 124–142. Also ePrint 2011/368.

58. P. Schwabe, S.-Y. Yang, and B.-Y. YANG, *SHA-3 on ARM11 processors*, Africacrypt 2012 (July 10-12, Ifrane, Morocco), LNCS 7374, pp. 324–341.

59. F.-H. Liu, Y.-J. Huang, and B.-Y. YANG, *Public-Key Cryptography from New Multivariate Quadratic Assumptions*, PKC 2012 (15th International Workshop for Public Key Cryptography, IACR, May 21–23, Darmstadt, Germany), and LNCS 7293, pp. 190–205.

60. P.-C. Kuo, M. Schneider, Ö. Dagdelen, J. Reichelt, J. Buchmann, C.-M. Cheng, and B.-Y. YANG, *Extreme Enumeration on GPU and in Clouds*, CHES 2011 *(ibid.)*, pp. 176–191.

61. D. J. Bernstein, H.-C. Chen, C.-M. Cheng, T. Lange, R. Niederhagen, P. Schwabe, and B.-Y. YANG, *ECC2K-130 on NVIDIA GPUs*, Indocrypt 2010 (December 13-15, Hyperabad, India) LNCS 6498, pp. 328–344.

62. K.-M. Chung, F.-H. Liu, C.-J. Lu, and B.-Y. YANG, *Efficient String-Commitment from Weak Bit-Commitment*, Asiacrypt 2010 (December 5-9, Singapore), LNCS 6477, pp. 268–282.

63. C. Bouillaguet, H.-C. K. Chen, C.-M. Cheng, T. Chou, R. Niederhagen, A. Shamir, and B.-Y. YANG, *Fast Exhaustive Search for Polynomial Systems in* $\mathbf{F_2}$, CHES 2010 (12th Workshop on Cryptographic Hardware and Embedded Systems, August 17-20, UC Santa Barbara), LNCS 6225, pp. 203–218.

64. Y.-H. Lin, A. Studer, Y.-H. Chen, H.-C. Hsiao, E. L.-H. Kuo, J. Lee, J. McCune, K.-H. Wang, M. Krohn, A. Perrig, B.-Y. YANG, H.-M. Sun, and P.-L. Lin, *SPATE: Small-group PKI-less Authenticated Trust Establishment*, IEEE Trans on Mobile Computing **9:12**(2010), pp. 1666-1681 (SCI). [Note: IEEE Trans. TMC. invited this paper as best paper of MobiSys 2009 (7th Int'l Conference on Mobile Systems, Applications, and Services, June 22–25, Wroclaw, Poland), ACM proceedings pp. 1–14 *SPATE: Small-group PKI-less Authenticated Trust Establishment*.]

65. C.-I Lee, T.-C. Wu, B.-Y. YANG and W.-G. Tzeng, *New Secure Broadcasting Scheme Realizing Information Granularity*, J. of Info. Sci. and Eng., **26:4**(2010) pp. 1509–1523.

66. H.-C. Hsiao, Y.-H. Lin, A. Studer, C. Studer, K.-H. Wang, H. Kikuchi, A. Perrig, H.-M. Sun, B.-Y. YANG, *A Study of User-Friendly Hash Comparison Schemes*, pp. 105-114, Proc. ACSAC 2009 (December 7–11, Honolulu).

67. A. I.-T. Chen, M.-S. Chen, T.-R. Chen, C.-M. Cheng, J. Ding, E. L.-H. Kuo, F. Y.-S. Lee, and B.-Y. YANG, *SSE Implementation of Multivariate PKCs on Modern x86 CPUs*, CHES 2009 (11th Workshop on Cryptographic Hardware and Embedded Systems, Sept. 6–9, Lausanne, Switzerland), pp. 33–48, LNCS 5747.

68. D. J. Bernstein, T.-R. Chen, C.-M. Cheng, T. Lange, and B.-Y. YANG, *ECM on Graphics Cards*, Eurocrypt 2009 (April 25–29, Köln, Germany) LNCS 5479, pp. 483–501.

69. J. Baena, M.-S. Chen, C. Clough, J. Ding, and B.-Y. YANG, *Square, a New Multivariate Encryption Scheme*, CT-RSA 2009 (10th Cryptographer's Track RSA Conference, April 20–24, San Francisco), LNCS 5473, pp. 252–264.

70. A. I.-T. Chen, C.-H. Chen, M.-S. Chen, C.-M. Cheng and B.-Y. YANG, *Practical-Sized Instances of Multivariate PKCs: Rainbow, and ℓIC-derivatives*, PQCrypto 2008 (Second Post-Quantum Cryptography Workshop, Oct. 17–19, Cincinnati, USA) and LNCS 5299, pp. 95–106.

71. F.-H. Liu, C.-J. Lu, and B.-Y. YANG, *Secure PRNGs from Specialized Polynomial Maps over Any* $\mathbf{F_q}$, PQCrypto'08 and LNCS 5299 (*ibid.*), pp. 181–202.

72. C.-H. Chen, C.-W. Chen, C. Kuo, Y.-H. Lai, J. McCune, A. Perrig, A. Studer, and B.-Y. YANG, *GAnGS: Gather, Authenticate 'n Group Securely*, Proc. MobiCom 2008 (14th Annual International Conference on Mobile Computing and Networking, ACM SigMobile, September 14–19, San Francisco), pp. 92–103.

73. J. Ding, V. Dubois, B.-Y. YANG, C.-H. Chen, and C.-M. Cheng. *Can SFLASH be Repaired?*, ICALP 2008 (35th International Colloquium on Automata, Languages and Programming, July 6–13, Reykjavik, Iceland), LNCS 5126, pp. 691–701.

74. J. Ding, B.-Y. YANG, C.-H. Chen, M.-S. Chen, and C.-M. Cheng, *New Differential-Algebraic Attacks and Reparametrization of Rainbow*, ACNS 2008 (6th Applied Cryptography and Network Security Conference, June 3–6, New York, USA), LNCS 5037, pp. 242–257. Updates at ePrint 2008/108.

75. J. Ding and B.-Y. YANG, *Multivariate Polynomials for Hashing*, Inscrypt 2007, Aug. 31–Sep. 5, Xining, China, LNCS 4990, pp. 358–371.

76. B.-Y. YANG, C.-H. Chen, D. J. Bernstein, and J.-M. Chen, *Analysis of QUAD*, FSE 2007 (14th International Workshop for Fast Software Encryption, IACR, Mar. 26–28, Luxemberg City, Luxemberg), LNCS 4593, pp. 290–307.

77. J. Ding, C. Wolf, and B.-Y. YANG, *ℓ-Invertible Cycles for Multivariate Quadratic Public Key Cryptography*, PKC 2007 (10th International Workshop for Public Key Cryptography, IACR, Apr. 21–24, Beijing, China), LNCS 4450, pp. 266–281. [Prior version at Post-Quantum Crypto Workshop '06, KU Leuven, Belgium.]

78. W. Yan, B.-Y. YANG, and Y.-N. Yeh, *The Behavior of Wiener Indices and Polynomials of Graphs under Five Graph Operators*, Appl. Math. Lett. **20**(2007) pp. 290–295.

79. I. Gutman, W. Yan, B.-Y. YANG, and Y.-N. Yeh, *Generalized Wiener Indices of Zigzagging Pentachains*, J. Math. Chem. **42:2**(2007) pp. 103–117.

80. B.-Y. YANG, C.-M. Cheng, B.-R. Chen, and J.-M. Chen, *Implementing Minimized Multivariate Public-Key Cryptosystems on Low-Resource Embedded Systems*, SPC 2006 (3rd Security of Pervasive Computing Conference, Apr. 18–21, York, UK) LNCS 3934, pp. 73-88.

81. L.-C. Wang, B.-Y. YANG, Y.-H. Hu, and F.-P. Lai, *A "Medium-Field" Multivariate Public-Key Encryption Scheme*, CT-RSA 2006 (7th Cryptographer's Track RSA Conference, Feb. 13–17, San Jose CA), LNCS 3860, pp. 132–149.

82. S.-P. Eu, B.-Y. YANG, and Y. Yeh, *Computing the Generalized Wiener Indices of Hex Chains*, Int'l J. of Quant. Chem. **106**(2006), pp. 426–435 .

83. B.-Y. YANG and J.-M. Chen, *Building Secure Tame-Like Multivariate Public-Key Cryptosystems: the New TTS*, ACISP 2005 (10th Australasian Conference on Info. Sec. and Privacy, July 4–6, Brisbane), LNCS 3574, pp. 518–531.

84. B.-Y. YANG and J.-M. Chen, *All in the XL Family: Theory and Practice*, ICISC 2004 (7th International Conference on Information Security and Cryptology, Dec. 2–3, Seoul, Korea), LNCS 3506, pp. 67–86.

85. L.-C. Wang, Y.-H. Hu, F.-P. Lai, C.-Y. Chou, and B.-Y. YANG, *Tractable Rational Map Signature*, PKC 2005 (8th Int'l Workshop for Public-Key Cryptography, IACR, Jan. 26–28, Diablerets, Switzerland), LNCS 3386, pp. 244–257.

86. B.-Y. YANG, J.-M. Chen, and N. Courtois, *On Asymptotic Security Estimates in XL and Gröbner Bases-Related Algebraic Cryptanalysis*, ICICS 2004 (6th International Conference on Information and Communications Security, Oct. 27–29, Malaga, Spain), LNCS 3269, pp. 401–413.

87. B.-Y. YANG, J.-M. Chen, and Y.-H. Chen, *TTS: High-Speed Signatures on a Low-Cost Smart Card*, CHES 2004 (6th Workshop on Cryptographic Hardware and Embedded Systems, IACR, Aug. 11–13, Boston MA); LNCS 3156, pp. 371-385.

88. B.-Y. YANG and J.-M. Chen, *Theoretical Analysis of XL over Small Fields*, ACISP 2004 (9th Australasian Conference on Info. Sec. and Privacy, July 13-15, Sydney); LNCS 3108, pp. 277-288.

89. B.-Y. YANG and Y. Yeh, *Wiener Polynomials of some Chemically Interesting Graphs*, International J. of Quantum Chem. **99:2**(2004), pp. 80-91.

90. B.-Y. YANG and Y. Yeh, *A Crowning Moment for Wiener Indices*, Studies in Applied Mathematics, **112**(2004), pp. 333-340.

91. J.-M. Chen and B.-Y. YANG, *A More Secure and Efficacious TTS Signature Scheme*, ICISC 2003 (6th Int'l Conference on Info. Sec. & Cryptology, Nov. 27–28, Seoul, Korea), LNCS 2971, pp. 320–338.

92. H.-K. Hwang, B.-Y. YANG, and Y. Yeh, *Presorting algorithms: an average-case point of view*, Theo. Comp. Sci. **242**(2000), no. 1-2, pp. 29–40.

93. W.-C. Huang, B.-Y. YANG, and Y. Yeh, *From Ternary Strings to Wiener indices of Benzenoid Chains*, Discrete Appl. Math. **73**(1997), pp. 113–131. (SCI)

94. I-W. Huang, B.-Y. YANG, and Y. Yeh, *Wiener Indices of Hex Carpets— from Hexagon Models to Square Grids*, SE Asia Bull. of Math. **20**(1996), pp. 81-102.

95. B.-Y. YANG, and Y. Yeh, *Zigging and Zagging in Pentachains*, Adv. in Appl. Math. **16**(1995) pp. 72-94. (SCI)

Conference Articles without Journal Proceedings, Books/Book Chapters, Tech Reports

1. W. Beullens, M.-S. Chen, J. Ding, B. Gong, M. J. Kannwischer, J. Patarin, B.-Y. Peng, D. Schmidt, C.-J. Shih, C. Tao, B.-Y. YANG, *UOV: Unbalanced Oil and Vinegar*, technical report and specifications, 2023.05.31. `https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-f`

2. M.-S. Chen, J. Ding, M. J. Kannwischer, J. Patarin, D. Schmidt, B.-Y. YANG, *Response to Ward Bellens's new Rainbow Attacks*, technical report, 2020.12.01.

3. D. J. Bernstein, B. B. Brumley, M.-S. Chen, C. Chuengsatiansup, T. Lange, A. Marotzke, B.-Y. Peng, N. Tuveri, C. van Vredendaal, and B.-Y. YANG, *NTRU Prime 3rd Round Submission* `http://ntruprime.cr.yp.to/nist/ntruprime-20201007.pdf`, NIST submission document, 2020.10.07. Also available at: `https://csrc.nist.gov/CSRC/media/Projects/post-quantum-cryptography/documents/` (warning: large file).

4. J. Ding, M.-S. Chen, M. J.Kannwischer, A. Petzoldt, J. Patarin, D. Schmidt, B.-Y. YANG, *Rainbow 3rd Round Submission* `troll.iis.sinica.edu.tw://by-publ/recent/Rainbow3round.pdf`, NIST submission document, 2020.10.01. Also available at: https://csrc.nist.gov/CSRC/media/Projects/post-quantum-cryptography/documents/round-3/submissions/Rainbow-Round3.zip (warning: large file).

5. R. C.-W. Phan, M. Abe, L. Batten, J. H. Cheon, E. Dawson, S. D. Galbraith, J. Guo, L. C. K. Hui, K. Kim, X. Lai, D. H. Lee, M. Matsui, T. Matsumoto, S. Moriai, P. Q. Nguyen, D. Pei, D. H. Phan, J. Pieprzyk, H. Wang, H. Wolfe, D. S. Wong, T.-C. Wu, B.-Y. Yang, S.-M. Yiu, Y. Yu, J. Zhou: *Advances in security research in the Asiacrypt region*. Commun. ACM **63:4**(2020), pp. 76-81.

6. M.-S. Chen, J. Ding, M. Kannwischer, J. Patarin, A. Petzoldt, D. Schmidt, B.-Y. YANG, *Modified Parameters of Rainbow in Response to a Refined Analysis of the Rainbow Band Separation Attack by the NIST Team and the Recent New MinRank attacks* , technical report.

7. M.-S. Chen, J. Ding, A. Petzoldt, D. Schmidt, B.-Y. YANG, *Rainbow 2nd Round Submission*, NIST submission document and technical report, 2018.04.30.

8. B.-Y. YANG, W.-J. Wang, S.-Y. Yang, C.-S. Miou, C.-M. Cheng, *Fast Exhaustive Search for Polynomial Systems over* $\mathbf{F_3}$, updated version of *Masters Thesis by Wei-Jeng Wang, National Taiwan University, 2016*.

9. M.-S. Chen, B.-Y. YANG, and D. Smith-Tone, *PFLASH - secure asymmetric signatures on smart cards*. NIST Lightweight Cryptography Workshop 2015 csrc.nist.gov/groups/ST/lwc-workshop2015/papers/session3-smith-tone-paper.pdf.

10. D. J. Bernstein, S. Josefsson, T. Lange, P. Schwabe and B.-Y. YANG, EdDSA for more curves, IACR e-Print Archive, http://eprint.iacr.org/2015/677.

11. B.-Y. YANG, ed., *Post-Quantum Cryptography*, Proc. 4th Post-Quantum Cryptography Workshop, Nov. 29–Dec. 2, 2011, Taipei, Taiwan, LNCS 7071, Springer, ISBN 978-3-642-25404-8.

12. L. Goubin, J. Patarin, and B.-Y. YANG, *Multivariate Cryptosystems*, pp. 824–828, in *Encyclopedia of Cryptography and Security*, H. van Tillborg and S. Jajodia, eds., Springer 2011, ISBN 978-1-4419-5905-8.

13. D. J. Bernstein, H.-C. Chen, M.-S. Chen, C.-M. Cheng, C.-H. Hsiao, Z.-C. Lin, T. Lange, and B.-Y. YANG, *The 1 Billion-Mulmod Personal Computer*, Presented at SHARCS 2009 (Sept. 9–10, Lausanne, Switzerland).

14. J. Ding, B.-Y. YANG, F. Werner, C.-H. Chen, M.-S. Chen, *Odd-Field Multivariate Hidden Field Equations*, poster at Eurocrypt 2009, ePrint 2008/543.

15. J. Ding and B.-Y. YANG, *Multivariate Public-Key Cryptography*, chapter in *Post-Quantum Cryptography*, pp. 193–241, D. J. Bernstein, J. Buchmann and E. Dahmen, eds., Springer 2009, ISBN: 978-3-540-88701-0.

16. C.-H. Chen, B.-Y. YANG, and J.-M. Chen, *Exploring the Limits of Lazard-Faugère Gröbner Bases Methods*, PQCrypto'06 (First Post-Quantum Crypto Workshop), KU Leuven, Belgium.

17. S.-Y. Wang, C.-S. Laih, and B.-Y. YANG, *Partially Ordered Signature Schemes*, TFIT'06 (third Taiwan-France Info Tech Conference, Mar. 28–30, Nancy, France).

18. M. Bardet, J.-C. Faugère, B. Salvy, and B.-Y. YANG, *Asymptotic Expansion of the Degree of Regularity for Semi-Regular Systems of Equations*, MEGA '05 (8th Conférence des Méthodes Effectives en Géométrie Algebrique, May 27– June 1, Porto Conte, Sardinia, Italy); being re-edited for journal submission.

19. B.-Y. YANG and J.-M. Chen, *Cryptanalysis Today*, Chap. 6 in Book 19 of the third Information and Communications Security Series, W.-G. Tzeng, ed., C-S. Laih, series editor, published by the National Science of Council of Taiwan, 2004.

20. B.-Y. YANG and J.-M. Chen, *XL: A Brief on the State of the Art*, **Best Paper Award**, Chinese (Taipei) Cryptology and Info. Sec. Assoc. (CCISA) 2004 conference.

21. J.-M. Chen, B.-Y. YANG, and B.-Y. Peng, *Tame Transformation Signatures and Topsy-Turvy Hashes* IWAP '02 (11/29–12/01, Taipei), pp. 93-100.

22. B.-Y. YANG, and Y. Yeh, *About Wiener Numbers and Polynomials*, Sec. 5 in *Lie Algebras, Rings and Related Topics: Proc. of Second International Tainan-Moscow Algebra Workshop (Tainan, 1997)*, pp. 203–226, Y. Fong, A. Mikhalev, and E. Zelmanov, eds., Springer-Verlag (Berlin) 2000.

23. B.-Y. YANG, and Y. Yeh, *Chains of Motley Gems and their Wiener Indices,* in Proc. of *First International Tainan-Moscow Algebra Workshop (Tainan, 1994)*, pp. 329–349, de Gruyter (Berlin), Y. Fong *et al* ed., De Gruyter (Berlin) 1996.