

- Professional Visits:**
- **2007.9-2007.12:** Winter'07 Taft Visiting Lecturer, U. of Cincinnati.
  - **2001.8-2002.7:** Visiting Scholar, Department of Mathematics, MIT.

### Jointly Supervised Students

#### with C.-M. Cheng:

- UROPs (Undergraduate Research Opportunities): Michael Feng-Hao Liu (04–05); Chia-Hsin Chen (05–07); Anna Inn-Tung Chen and Frost Yu-Shuang Li (06–08).
- M.S.: Kevin Hsieh-Chung Chen, Ming-Yang Chih and Tung Chou (08–10); Jarron Jie-Ren Shih (09–11); Yun-An Chang, Jong-Shian Wu (11–13); Wen-Ding Li (13–15); Will Wei-Cheng Wang (14—).
- Ph.D.: Ming-Shing Chen (09–), Po-Chun Kuo (10–), Shang-Yi Yang (14–)

with T. Lange: Ruben F. Niederhagen (09–12, Ph.D.).

### Journal or Formally Refereed Conference Articles

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

1. M.-H. Tsai, B.-Y. Wang, B.-Y. Yang, *Certified Verification of Algebraic Properties on Low-Level Mathematical Constructs in Cryptographic Programs*, accepted at ACM CCS 2017 (24th ACM Conference on Computer and Communications Security, Dallas, TX, USA, Oct. 30-Nov. 3).
2. S.-Y. Yang, P.-C. Kuo, B.-Y. Yang and C.-M. Cheng, *Gauss Sieve Algorithm on GPUs*, CT-RSA 2017 (San Francisco, Feb. 14–17), LNCS 10159, pp. 39–57.
3. B.-Y. Peng, Y.-C. Hsu, Y.-J. Chen, D.-C. Chueh, C.-M. Cheng, 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. 637647.
4. 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.
5. Y.-A. Chang, M.-S. Chen, J.-S. Wu and B.-Y. YANG, *Postquantum SSL/TLS for Embedded Systems*, IoTTS workshop at IEEE SOCA 2014 (Matsue, Japan, Nov. 17-19).
6. 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.
7. 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).
8. 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.

9. J. Y.-C. Yeh, C.-M. Cheng, B.-Y. YANG, *Operating Degrees for XL vs.  $\mathbf{F}_4/\mathbf{F}_5$  for Generic 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.
10. 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.
11. 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).
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. 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, Hyderabad, India) LNCS 6498, pp. 328–344.

22. 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.
23. 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  $\mathbb{F}_2$* , CHES 2010 (12th Workshop on Cryptographic Hardware and Embedded Systems, August 17-20, UC Santa Barbara), LNCS 6225, pp. 203–218.
24. 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: Extended from #28 as invited paper of IEEE Trans. TMC.]
25. 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.
26. 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).
27. 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.
28. Y.-H. Lin, A. Studer, H.-C. Hsiao, J. McCune, K.-H. Wang, M. Krohn, P.-L. Lin, A. Perrig, H.-M. Sun, and B.-Y. YANG, *SPATE: Small-group PKI-less Authenticated Trust Establishment*, Proc. MobiSys 2009 (7th Int'l Conference on Mobile Systems, Applications, and Services, June 22–25, Wroclaw, Poland), pp. 1–14 (**best paper**).
29. 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.
30. 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.
31. 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  $\ell$ IC-derivatives*, PQCrypto 2008 (Second Post-Quantum Cryptography Workshop, Oct. 17–19, Cincinnati, USA) and LNCS 5299, pp. 95–106.
32. F.-H. Liu, C.-J. Lu, and B.-Y. YANG, *Secure PRNGs from Specialized Polynomial Maps over Any  $\mathbb{F}_q$* , PQCrypto'08 and LNCS 5299 (*ibid.*), pp. 181–202.
33. 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.
34. 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.

35. 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.
36. J. Ding and B.-Y. YANG, *Multivariate Polynomials for Hashing*, Inscrypt 2007, Aug. 31–Sep. 5, Xining, China, LNCS 4990, pp. 358–371.
37. 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, Luxemburg City, Luxemburg), LNCS 4593, pp. 290–307.
38. J. Ding, C. Wolf, and B.-Y. YANG,  *$\ell$ -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.]
39. 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.
40. 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.
41. 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.
42. 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.
43. 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 .
44. 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.
45. 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.
46. 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.
47. 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.

48. 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.
49. 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.
50. B.-Y. YANG and Y. Yeh, *Wiener Polynomials of some Chemically Interesting Graphs*, International J. of Quantum Chem. **99:2**(2004), pp. 80-91.
51. B.-Y. YANG and Y. Yeh, *A Crowning Moment for Wiener Indices*, Studies in Applied Mathematics, **112**(2004), pp. 333-340.
52. 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.
53. 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.
54. 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)
55. 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.
56. 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. M.-S. Chen, B.-Y. YANG, and D. Smith-Tone, *PFLASH - secure asymmetric signatures on smart cards*. NIST Lightweight Cryptography Workshop 2015  
<http://csrc.nist.gov/groups/ST/lwc-workshop2015/papers/session3-smith-tone-paper.pdf>.
2. 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>.
3. 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.
4. 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.
5. 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).

6. 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.
7. 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.
8. 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.
9. S.-Y. Wang, C.-S. Lai, and B.-Y. YANG, *Partially Ordered Signature Schemes*, TFIT'06 (third Taiwan-France Info Tech Conference, Mar. 28–30, Nancy, France).
10. 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 Algébrique, May 27– June 1, Porto Conte, Sardinia, Italy); being re-edited for journal submission.
11. 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. Lai, series editor, published by the National Science of Council of Taiwan, 2004.
12. 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.
13. 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.
14. 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.
15. 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.