

Journal or Formally Refereed Conference Articles

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

1. D. J. Bernstein, N. Duif, T. Lange, *P. Schwabe, and B.-Y. YANG, High-speed high-security signatures, CHES 2011 (13th Workshop on Cryptographic Hardware and Embedded Systems, September 28 – October 1, Nara, Japan), LNCS 6917, pp. 124–142. Full version at ePrint 2011/368 and to appear in the Journal of Cryptographic Engineering.
2. 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.
3. 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.
4. 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.
5. 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.
6. *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 #10 as invited paper of IEEE Trans. TMC.]
7. 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.
8. 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).
9. 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.
10. 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**).
11. D. J. Bernstein, T.-R. Chen, *C.-M. Cheng, T. Lange, and B.-Y. YANG, *ECM on Video Cards*, Eurocrypt 2009 (April 25–29, Köln, Germany) LNCS 5479, pp. 483–501.
12. 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.

13. A. I.-T. Chen, C.-H. O. Chen, M.-S. Chen, C.-M. Cheng and *B.-Y. YANG, *Practical-Sized Instances of Multivariate PKCs: Rainbow, and ℓ IC-derivatives*, PQCrypto 2008 (Second Post-Quantum Cryptography Workshop, Oct. 17–19, Cincinnati, USA) and LNCS 5299, pp. 95–106.
14. F.-H. Liu, C.-J. Lu, and *B.-Y. YANG, *Secure PRNGs from Specialized Polynomial Maps over Any F_q* , PQCrypto'08 and LNCS 5299 (*ibid.*), pp. 181–202.
15. C.-H. O. 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.
16. J. Ding, V. Dubois, *B.-Y. YANG, C.-H. O. 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.
17. J. Ding, *B.-Y. YANG, C.-H. O. 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.
18. J. Ding and *B.-Y. YANG, *Multivariate Polynomials for Hashing*, Inscrypt 2007, Aug. 31–Sep. 5, Xining, China, LNCS 4990, pp. 358–371.
19. *B.-Y. YANG, C.-H. O. 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.
20. 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.]
21. *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.
22. 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.
23. *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.
24. 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.
25. 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 .

26. *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.
27. *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.
28. *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.
29. *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.
30. *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.
31. *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.
32. *B.-Y. YANG and Y. Yeh, *Wiener Polynomials of some Chemically Interesting Graphs*, International J. of Quantum Chem. **99**:2(2004), pp. 80–91.
33. *B.-Y. YANG and Y. Yeh, *A Crowning Moment for Wiener Indices*, Studies in Applied Mathematics, **112**(2004), pp. 333–340.
34. *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.
35. *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.
36. 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)
37. 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.
38. *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. 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.

2. L. Goubin, J. Patarin, and B.-Y. YANG, *Multivariate Cryptosystems*, section in *Encyclopedia of Cryptography and Security*, H. van Tillborg and S. Jajodia, eds., Springer 2011, ISBN 978-1-4419-5905-8.
3. 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).
4. J. Ding, *B.-Y. YANG, F. Werner, C.-H. O. Chen, M.-S. Chen, *Odd-Field Multivariate Hidden Field Equations*, poster at Eurocrypt 2009, ePrint 2008/543.
5. J. Ding and *B.-Y. YANG, *On Multivariate Cryptosystems*, 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.
6. C.-H. O. 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.
7. 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).
8. *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.
9. *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.
10. *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.
11. 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.
12. *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.
13. *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.

Submitted articles and works in progress

1. F.-H. Liu and B.-Y. YANG, *Public-Key Cryptography from New Multivariate Quadratic Assumptions*, submitted to PKC 2012.
2. C.-H. Yu and B.-Y. YANG, *Randomized Secure Two-Party Computation for Modular Reduction, Zero Test, Comparison, MOD and Exponentiation*, submitted to Eurocrypt 2012.

3. M.-S. Chen, T.-R. Chen, C.-M. Cheng, C.-H. Hsiao, R. Niederhagen, and *B.-Y. YANG, *What Price a Provably Secure Cipher?*
4. D. J. Bernstein, H.-C. Chen, M.-S. Chen, C.-M. Cheng, C.-H. Hsiao, T. Lange, and *B.-Y. YANG, *Batch NFS*