Journal or Formally Refereed Conference Articles


38. 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.


44. 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.

45. 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.


63. 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.]


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


