Books


3. **Multivariate public key cryptography** (with Bo-yin Yang), a Chapter in *Post-Quantum Cryptography* by Daniel J. Bernstein (Editor), Johannes Buchmann (Editor), Erik Dahmen (Editor), Springer, 2009.

US patents

1. Cryptographic systems using pairing with errors
   Patent number: 9246675
   This patent covers the new post-quantum key exchange invention.
   Type: Grant
   Filed: April 11, 2013
   Date of Patent: January 26, 2016
   Inventor: Jintai Ding

2. Method to produce new multivariate public key cryptosystems
   This patent covers Rainbow signature scheme
   Patent number: 7961876
   Type: Grant
   Filed: December 30, 2005
   Date of Patent: June 14, 2011
   Inventor: Jintai Ding

3. Multivariable cryptosystem
   Patent number: 7158636
   Type: Grant
   Filed: April 11, 2003
   Date of Patent: January 2, 2007
   Inventor: Jintai Ding

Papers


10. HMFEv - An Efficient Multivariate Signature Scheme, (Anonymously Refereed) with Albrecht Petzoldt, Ming-Shing Chen, Bo-Yin Yang, PQCrypto 2017: 205-223


13. Cryptanalysis of a Public Key Cryptosystem Based on Diophantine Equations via Weighted LLL Reduction. (Anonymously Refereed) with Momonari Kudo, Shinya Okumura, Tsuyoshi Takagi, Chengdong Tao, IWSEC 2016: 305-315


16. Design Principles for HFEv- based Multivariate Signature Schemes, (Anonymously Refereed), (with Albrecht Petzoldt, Ming-Shing Chen, Bo-Yin Yang, Chengdong Tao), ASIACRYPT 2015: 311-334


18. Authenticated Key Exchange from Ideal Lattices, (Anonymously Refereed), (with Jiang Zhang; Zhenfeng Zhang; Michael Snook; Ozgur Dagdelen,) EUROCRYPT (2) 2015: 719-751


24. Inverting Square systems algebraically is exponential, with Crystal Clough; Roberto Araujo. Finite Fields and Applications. V. 26, P. 32-48 (2014)


26. Solving Degree and Degree of Regularity for Polynomial Systems over a Finite Fields ( with Dieter Schmidt). Number Theory and Cryptography 2013: 34-49


35. Linear Algebra to Compute Syzygies and Grobner Bases with Daniel Cabarcas, (refereed), accepted for the 36th International Symposium on Symbolic and Algebraic Computation (ISSAC11), June 2011, San Jose, USA

36. On Kipnis-Shamir Attack on Unbalanced Oil-Vinegar Scheme with Weiwei Cao, Lei Hu, Zhijun Yin, accepted for the 7th Information Security Practice and Experience Conference (ISPEC 2011 ), May 2011, Guangzhou, China, (Anonymously refereed), to be published in LNCS.


61. High order linearization equation (HOLE) attack on multivariate public key cryptosystems (Anonymously Refereed), with Lei Hu, Xuyun Nie, Jianyu Li, John Wagner. PKC-2007, LNCS 4450, 233-245, Springer 2007


74. Cryptanalysis of TTS and Tame-Like Multivariable Signature Schemes (with Zhijun Yin) (Anonymousely Refereed) presented and published in the Third International Workshop in Applied Public-key Infrastructure, Page 14-25, 2004 (IWAP’04)


82. On the universal R-matrix of quantum affine superalgebra $U_q(\hat{o}sp(1,2))$, CZECHOSLOVAK Journal of Physics 51 (2001), No, 12, 1291-1298


90. A Remark On the FRTS realization and Drinfeld Realization of quantum affine superalgebra $osp(1,2)$, Letters in Mathematical Physics, Vol. 49, No. 2, 161-171.


94. Spinor Representations of quantum affine $gl(n)$ and quantum Boson-Fermion correspondence, Communications in Mathematical Physics, Vol. 200, No. 2, 399-420.

95. On the FRTS approach to quantized current algebras, with S. Khoroshkin, Letters in Mathematical Physics, Vol. 45, No. 4, 331-352.


100. Spinor representations of quantum affine $o(N)$, Letters in Mathematical Physics, Vol. 39, No. 1, 81-94.


102. The center of a quantum affine algebra at the critical level, with P. Etingof, Mathematical Research Letters, Vol. 1, No. 4, 469-480.
103. *Spinor and oscillator representations of quantum groups*, in Lie theory and geometry, with I. Frenkel, Progress in Mathematics 123, Birkhaeuser Boston, Boston, MA, 127-165. (Refereed)


105. *Isomorphism of two realizations of quantum affine $gl(n)$*, with I. Frenkel, Communications in Mathematical Physics, Vol. 156, No. 2, 277-300.

**Publicity**

