168 Selected Journal Papers (since 1985)

1. Zhen Liu, Zhenfu Cao, and Duncan S. Wong. Traceable CP-ABE: How to Trace Decryption Devices Found in the Wild. **IEEE Transactions on Information Forensics and Security**, 10(1): 55-68 (2015).
2. Jun Zhou, Xiaodong Lin, Xiaolei Dong, and Zhenfu Cao. PSMPA: Patient Self-controllable and Multi-level Privacy-preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System. **IEEE Transactions on Parallel and Distributed Systems**. DOI: 10.1109/TPDS.2014.2314119, to appear.
3. J. Zhou, Z. Cao, Xiaolei Dong, N. Xiong, A. V. Vasilakos. 4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks, **Information Sciences**, DOI:10.1016/j.ins.2014.09.003, to appear.
4. Le Chen, Rongxing Lu, Khalid AlHarbi, Xiaodong Lin, and Zhenfu Cao. ReDD: Recommendation-based Data Dissemination in Privacy-preserving Mobile Social Networks. **Security and Communication Networks**, DOI: 10.1002/sec.1082, to appear.
5. Weiwei Jia, Haojin Zhu, Suguo Du, Xiaolei Dong, and Zhenfu Cao. CPPA: Cloud Based Privacy Preserving Aggregation Architecture in Multi-Domain Wireless Networks. **Security and Communication Networks**. DOI: 10.1002/sec.950, to appear.
6. Le Chen, Rongxing Lu, Zhenfu Cao, Khalid AlHarbi, and Xiaodong Lin. MuDA: Multifunctional Data Aggregation in Privacy-preserving Smart Grid Communications, **Peer-to-Peer Networking and Applications**, DOI: 10.1007/s12083-014-0292-0, to appear.
7. Le Chen, Rongxing Lu, and Zhenfu Cao, PDAFT: A Privacy-preserving Data Aggregation Scheme with Fault Tolerance for Smart Grid Communications, **Peer-to-Peer Networking and Applications**, DOI: 10.1007/s12083-014-0255-5, to appear.
8. Yu Chen, Zongyang Zhang, Dongdai Lin, Zhenfu Cao: CCA-Secure IB-KEM from Identity-Based Extractable Hash Proof System. **The Computer Journal**, 57(10): 1537-1556 (2014)
9. Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Weiwei Jia, Yunlu Chen, Athanasios V. Vasilakos: Security and privacy for storage and computation in cloud computing. **Information Sciences** 258: 371-386 (2014)
10. Zongyang Zhang, Zhenfu Cao, Haojin Zhu: Constant-round adaptive zero-knowledge proofs for NP. **Information Sciences** 261: 219-236 (2014)
11. Hongbing Wang, Zhenfu Cao, Lifei Wei: A scalable certificateless architecture for multicast wireless mesh network using proxy re-encryption. **Security and Communication Networks** 7(1): 14-32 (2014)
12. Weiwei Jia, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Chengxin Xiao: Human-Factor-Aware Privacy-Preserving Aggregation in Smart Grid. **IEEE Systems Journal** 8(2): 598-607 (2014)
13. Haojin Zhu, Suguo Du, Zhaoyu Gao, Mianxiong Dong, Zhenfu Cao: A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks. **IEEE Trans. Parallel Distrib. Syst.** 25(1): 22-32 (2014)
14. Zhenfu Cao, Keqiu Li, Xu Li, Patrick McDaniel, Radha Poovendran, Guojun Wang, Yang Xiang: Guest Editors' Introduction: Special Issue on Trust, Security, and Privacy in Parallel and Distributed Systems. **IEEE Trans. Parallel Distrib. Syst.** 25(2): 279-282 (2014)
15. Lifei Wei, Haojin Zhu, Zhenfu Cao, Xuemin (Sherman) Shen: SUCCESS: A Secure User-centric and Social-aware Reputation Based Incentive Scheme for DTNs. **Ad Hoc & Sensor Wireless Networks** 19(1-2): 95-118 (2013)
16. Dazhi Sun and Zhenfu Cao. On the Privacy of Khan et al.'s Dynamic ID-Based Remote Authentication Scheme with User Anonymity. **Cryptologia**, 37(4), 345-355, 2013.
17. Lihua Wang, Jun Shao, Zhenfu Cao, Masahiro Mambo, Akihiro Yamamura, Licheng Wang: Certificate-based proxy decryption systems with revocability in the standard model. **Information Sciences** 247: 188-201 (2013)
18. Dazhi Sun, Jinpeng Huai, and Zhenfu Cao. A comment on ' ' An efficient common-multiplicand-multiplication method to the Montgomery algorithm for speeding up exponentiation". **Information Sciences**, 223, 331-334, 2013.
19. Haiyong Bao, Zhenfu Cao: Group-Proxy Signature Scheme: A Novel Solution to Electronic Cash. **J. Intelligent Systems** 22(2): 95-110 (2013)
20. Huang Lin, Xiaoyan Zhu, Y. Fang, Dongsheng Xing, Chi Zhang, and Zhenfu Cao. Efficient Trust Based Information Sharing Schemes over Distributed Collaborative Network. **IEEE Journal on Selected Areas in Communications**, 31(9), 279-290, 2013.
21. Dazhi Sun, Jianxin Li, Zhiyong Feng, Zhenfu Cao, and Guangquan Xu. On the security and improvement of a two-factor user authentication scheme in wireless sensor networks. **Personal and Ubiquitous Computing**, 17(5), 895-905, 2013.
22. Hongbing Wang, Zhenfu Cao: More efficient CCA-secure unidirectional proxy re-encryption schemes without random oracles. **Security and Communication Networks** 6(2): 173-181 (2013)
23. Lifei Wei, Zhenfu Cao, Xiaolei Dong: Secure identity-based multisignature schemes under quadratic residue assumptions. **Security and Communication Networks** 6(6): 689-701 (2013)
24. Lize Gu, Licheng Wang, Kaoru Ota, Mianxiong Dong, Zhenfu Cao, Yixian Yang: New public key cryptosystems based on non-Abelian factorization problems. **Security and Communication Networks** 6(7): 912-922 (2013)
25. Zhen Liu, Zhenfu Cao, Duncan S. Wong: White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Any Monotone Access Structures. **IEEE Transactions on Information Forensics and Security** 8(1): 76-88 (2013)
26. Jun Zhou, Zhenfu Cao, Xiaolei Dong, Xiaodong Lin, Athanasios V. Vasilakos: Securing m-healthcare social networks: challenges, countermeasures and future directions. **IEEE Wireless Commun.** 20(4) , 12-21, 2013.
27. Haiyong Bao, Mande Xie, Zhenfu Cao, and Shanshan Hong. Signature-Encryption Scheme: A Novel Solution to Mobile Computation. **Advanced Materials Research**. 546, 1415-1420, 2012.
28. Zongyang Zhang, Zhenfu Cao: Concurrent non-malleable statistically hiding commitment. **Information Processing Letters** 112(11): 443-448 (2012)
29. Jun Shao, Zhenfu Cao: Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption. **Information Sciences** 206: 83-95 (2012)
30. Zongyang Zhang, Zhenfu Cao, Haifeng Qian: Chosen-ciphertext attack secure public key encryption with auxiliary inputs. **Security and Communication Networks** 5(12): 1404-1411 (2012)
31. Peng Zeng, Zhenfu Cao, Kim-Kwang Raymond Choo: An ID-based digital watermarking protocol for copyright protection. **Computers & Electrical Engineering** 37(4): 526-531 (2011)
32. Piyi Yang, Zhenfu Cao, Xiaolei Dong: Fuzzy identity based signature with applications to biometric authentication. **Computers & Electrical Engineering** 37(4): 532-540 (2011)
33. Hai Huang, Zhenfu Cao: Blake-Wilson, Johnson & Menezes protocol revisited. **SCIENCE CHINA Information Sciences** 54(7): 1365-1374 (2011)
34. Dongsheng Xing, Zhenfu Cao, Xiaolei Dong: Identity based signature scheme based on cubic residues. **SCIENCE CHINA Information Sciences** 54(10): 2001-2012 (2011)
35. Piyi Yang, Zhenfu Cao, Xiaolei Dong, Tanveer A. Zia: An Efficient Privacy Preserving Data Aggregation Scheme with Constant Communication Overheads for Wireless Sensor Networks. **IEEE Communications Letters** 15(11): 1205-1207 (2011)
36. Zhenfu Cao, Ivan Visconti, Zongyang Zhang: On constant-round concurrent non-malleable proof systems. **Information Processing Letters** 111(18): 883-890 (2011)
37. Piyi Yang, Zhenfu Cao, Xiaolei Dong: Threshold proxy re-signature. **J. Systems Science & Complexity** 24(4): 816-824 (2011)
38. Jun Shao, Zhenfu Cao, Peng Liu: SCCR: a generic approach to simultaneously achieve CCA security and collusion-resistance in proxy re-encryption. **Security and Communication Networks** 4(2): 122-135 (2011)

39. Hai Huang, Zhenfu Cao: Authenticated key exchange protocol with enhanced freshness properties. **Security and Communication Networks** 4(10): 1130-1136 (2011)
40. Hai Huang, Zhenfu Cao: IDOAKE: strongly secure ID-based one-pass authenticated key exchange protocol. **Security and Communication Networks** 4(10): 1153-1161 (2011)
41. Xiaolei Dong, Lifei Wei, Haojin Zhu, Zhenfu Cao, Licheng Wang: : An Efficient Privacy-Preserving Data-Forwarding Scheme for Service-Oriented Vehicular Ad Hoc Networks. **IEEE T. Vehicular Technology 60**(2): 580-591 (2011)
42. Renwang Su, Zhenfu Cao: An efficient anonymous authentication mechanism for delay tolerant networks. **Computers & Electrical Engineering** 36(3): 435-441 (2010)
43. Licheng Wang, Lihua Wang, Zhenfu Cao, Yixian Yang, Xinxin Niu: Conjugate adjoining problem in braid groups and new design of braid-based signatures. **SCIENCE CHINA Information Sciences** 53(3): 524-536 (2010)
44. Huang Lin, Zhenfu Cao: On the security of metering scheme. **Computers & Mathematics with Applications** 60(2): 272-275 (2010)
45. Jun Shao, Zhenfu Cao, Xiaohui Liang, Huang Lin: Proxy re-encryption with keyword search. **Information Sciences** 180(13): 2576-2587 (2010)
46. Huang Lin, Zhenfu Cao, Xiaohui Liang, Jun Shao: Secure threshold multi authority attribute based encryption without a central authority. **Information Sciences** 180(13): 2618-2632 (2010)
47. Hongbing Wang, Zhenfu Cao, Licheng Wang: Multi-use and unidirectional identity-based proxy re-encryption schemes. **Information Sciences** 180(20): 4042-4059 (2010)
48. Huang Lin and Zhenfu Cao. Metering scheme with fine grained pricing. **Journal of Internet Technology**, 11(6), 837-846, 2010.
49. Piyi Yang, Zhenfu Cao, Xiaolei Dong: Efficient certificateless threshold signatures without random oracles. **J. Systems Science & Complexity** 23(6): 1167-1182 (2010)
50. Zhenfu Cao. Universal encrypted deniable authentication protocol. **International Journal of Network Security**, 8(2), 151-158, 2009.
51. Xiaolei Dong, Haifeng Qian, and Zhenfu Cao. Provably secure RSA-type signature based on conic curve. **Wireless Communications and Mobile Computing**, 9(2), 217-225, 2009.
52. Shengbao Wang, Zhenfu Cao, Zhaohui Cheng, and Kim-Kwang Raymond Choo. Perfect forward secure identity-based authenticated key agreement protocol in the escrow mode, **Science in China Series F**, 52(8), 1358-1370, 2009.
53. Peng Zeng, Zhenfu Cao, Kim-Kwang Raymond Choo, and Shengbao Wang. On the Anonymity of Some Authentication Schemes for Wireless Communications, **IEEE Communications Letters**, 13(3), 170-171, 2009.
54. Hai Huang and Zhenfu Cao. A Novel and Efficient Unlinkable Secret Handshakes Scheme, **IEEE Communications Letters**, 13(5), 363-365, 2009.
55. Peng Zeng, Zhenfu Cao, Kim-Kwang Raymond Choo, and Shengbao Wang. Security Weakness in a Dynamic Program Update Protocol for Wireless Sensor Networks, **IEEE Communications Letters**, 13(6), 426-428, 2009.
56. Feng Cao and Zhenfu Cao. A secure identity-based proxy multi-signature scheme, **Information Sciences**, 179(3), 292-302, 2009.
57. Shengbao Wang, Zhenfu Cao, Kim-Kwang Raymond Choo, and Lihua Wang. An improved identity-based key agreement protocol and its security proof, **Information Sciences**, 179(3), 307-318, 2009.
58. Feng Cao and Zhenfu Cao. An identity based universal designated verifier signature scheme secure in the standard model, **Journal of Systems and Software**, 82(4), 643-649, 2009.
59. Feng Cao and Zhenfu Cao. A secure identity-based multi-proxy signature scheme, **Computers & Electrical Engineering**, 35(1), 86-95, 2009.
60. Zhenfu Cao, Chuan I Chu, and Wai Chee Shiu. The exponontial Diophantine equation $AX^2 + BY^2 = \lambda K^Z$ and its applications, **Taiwanese Journal of Mathematics**, 12(5), 1015-1034, 2008.
61. Xiaolei Dong, Zhenfu Cao, and Licheng Wang. New designing of cryptosystems based on quadratic fields, **Science in China Series F**, 51(8), 1106-1116, 2008.
62. Rongxing Lu, Xiaolei Dong, and Zhenfu Cao. Designing efficient proxy signature schemes for mobile communication, **Science in China Series F**, 51 (2), 183-195, 2008.
63. Shengbao Wang, Zhenfu Cao, Maurizio Adriano Strangio, and Lihua Wang. Cryptanalysis and improvement of an elliptic curve Diffie-Hellman key agreement protocol, **IEEE Communications Letters**, 12(2), 149-151, 2008.
64. Xiaodong Lin, Rongxing Lu, Pin-Han Ho, Xuemin(Sherman) Shen, and Zhenfu Cao. TUA: A novel compromise-resilient authentication architecture for wireless mesh networks, **IEEE Transactions on Wireless Communications**, 7(4), 1389-1399, 2008.
65. Rongxing Lu, Xiaodong Lin, Zhenfu Cao, Jun Shao, and Xiaohui Liang. New (t, n) threshold directed signature scheme with provable security, **Information Sciences**, 178 (3), 756-765, 2008.
66. Xiaohui Liang, Zhenfu Cao, Rongxing Lu, and Liuquan Qin. Efficient and secure protocol in fair document exchange, **Computer Standards & Interfaces**, 30 (3), 167-176, MAR 2008.
67. Licheng Wang, Zhenfu Cao, Feng Cao. Haifeng Qian and Haiyong Bao. Biased bit commitment and applications, **Journal of Information Science and Engineering**, 24(2), 441-452, 2008.
68. Rongxing Lu, Xiaodong Lin, Zhenfu Cao, Liuquan Qin, and Xiaohui Liang. A simple deniable authentication protocol based on the Diffie-Hellman algorithm, **International Journal of Computer Mathematics**, 85(9), 1315-1323, 2008.
69. Dazhi Sun and Zhenfu Cao. New cryptanalysis paradigm on a nonce-based mutual authentication scheme, **International Journal of Network Security**, 6(1), 116-120, 2008.
70. Shengbao Wang, Zhenfu Cao, and Feng Cao. Efficient identity-based authenticated key agreement with PKG forward secrecy, **International Journal of Network Security**, 7(2), 181-186, 2008.
71. Rongxing Lu, Zhenfu Cao, Zhenchuan Chai, and Xiaohui Liang. A simple user authentication scheme for grid computing, **International Journal of Network Security**, 7(2), 202-206, 2008.
72. Shengbao Wang, Zhenfu Cao, and Haiyong Bao. Efficient certificateless authentication and key agreement (CL-AK) for grid computing, **International Journal of Network Security**, 7(3), 342-347, 2008.
73. Xiaolei Dong, W. C. Shiu, C. I. Chu, and Zhenfu Cao. The simultaneous Pell equations $y^2 - Dz^2 = 1$ and $x^2 - 2Dz^2 = 1$, **Acta Arithmetica**, 126(2), 115-123, 2007.
74. Rongxing Lu, Zhenfu Cao, and Xiaolei Dong. A new practical limited identity-based encryption scheme, **Fundamenta Informaticae**, 80(4), 461-474, 2007.
75. Dazhi Sun, Jinpeng Huai, Jizhou Sun, Zhenfu Cao. An efficient modular exponentiation algorithm against simple power analysis attacks, **IEEE Transactions on Consumer Electronics**, 53 (4): 1718-1723, 2007.
76. Licheng Wang, Zhenfu Cao, Xiangxue Li and Haifeng Qian. Simulatability and security of certificateless threshold signatures, **Information Sciences**, 177(6), 1382-1394, 2007.
77. Yuan Zhou, Binxing Fang, Zhenfu Cao, Xiaochun Yun and Xiaoming Cheng. How to construct secure proxy cryptosystem, **Information Sciences**, 177(19), 4095-4108, 2007.
78. Zhenchuan Chai, Zhenfu Cao, and Xiaolei Dong. Efficient ID-based multi-receiver threshold decryption, **International Journal of Foundations of Computer Science**, 18(5), 987-1004, 2007.
79. Jun Shao, Zhenfu Cao, and Rongxing Lu. Improvement of Yang et al.'s threshold proxy signature scheme, **Journal of Systems and Software**, 80(2), 172-177, 2007.
80. Qin Wang and Zhenfu Cao. Identity-based proxy multi-signature, **Journal of Systems and Software**, 80(7), 1023-1029, 2007.
81. Rongxing Lu and Zhenfu Cao. Simple three-party key exchange protocol, **Computers & Security**, 26(1), 94-97, 2007.
82. Zhenchuan Chai, Zhenfu Cao, and Rongxing Lu. Threshold password authentication against guessing attacks in Ad hoc networks, **Ad Hoc Networks**, 5(7), 1046–1054, 2007.

83. Rongxing Lu, Zhenfu Cao, Licheng Wang, Congkai Sun. A secure anonymous routing protocol with authenticated key exchange for Ad hoc networks, **Computer Standards & Interfaces**, 29(5), 521-527, 2007.
84. Rongxing Lu, Zhenfu Cao, and Haojin Zhu. An enhanced authenticated key agreement protocol for wireless mobile communication, **Computer Standards & Interfaces**, 29 (6), 647-652, 2007.
85. Rongxing Lu and Zhenfu Cao. Erratum to "Non-interactive deniable authentication protocol based on factoring", **Computer Standards & Interfaces**, 29(2), Page 275, 2007.
86. Rongxing Lu, Zhenfu Cao, Shengbao Wang, Haiyong Bao. A new ID-based deniable authentication protocol, **Informatica**, 18(1), 67-78, 2007.
87. Zhenchuan Chai, Zhenfu Cao, and Xiaolei Dong. Identity-based signature scheme based on quadratic residues, **Science in China Series F**, 50(3), 373-380, 2007.
88. Changxiang Shen, Huangguo Zhang, Dengguo Feng, Zhenfu Cao, Jiwu Huang. Survey of information security, **Science in China Series F**, 50 (3): 273-298, 2007.
89. Zhenchuan Chai, Zhenfu Cao, and Yuan Zhou. Efficient ID-based multi-decrypter encryption with short ciphertexts, **Journal of Computer Science and Technology**, 22(1), 103-108, 2007.
90. Rongxing Lu and Zhenfu Cao. Group oriented identity-based deniable authentication protocol from the bilinear pairings, **International Journal of Network Security**, 5(3), 283 - 287, 2007.
91. Rongxing Lu Zhenfu Cao, and Jun Shao. On security of two nonrepudiable threshold multi-proxy multi-signature schemes with shared verification, **International Journal of Network Security**, 4(3), 248-253, 2007.
92. Shengbao Wang, Zhenfu Cao and Feng Cao. More efficient identity-based authenticated key agreement with perfect forward secrecy, **Journal of Information and Computational Science**, 4(1), 317-323, 2007.
93. Xuemin (Sherman) Shen, Chuang Lin, Yan (Lindsay) Sun, Jianping Pan, Peter Langendoerfer, Zhenfu Cao. Wireless network security, **Wireless Communications and Mobile Computing**, 6(3), 269-271, 2006.
94. Zhenfu Cao, Gennian Ge and Ying Miao. Combinatorial Characterizations of One-Coincidence Frequency-Hopping Sequences, **Designs Codes and Cryptography**, 41(2), 177-184, 2006.
95. Zhenfu Cao, Haojin Zhu, and Rongxing Lu. Provably Secure Robust Threshold Partial Blind Signature, **Science in China Series F**, 49(5), 604 - 615, 2006.
96. Jun Shao, Zhenfu Cao, and Rongxing Lu. An Improved Deniable Authentication Protocol, **Networks**, 48(4), 179-181, 2006.
97. Qingshui Xue and Zhenfu Cao. Factoring based proxy signature schemes, **Journal of Computational and Applied Mathematics**, 195(1-2), pp. 229 - 241, 2006.
98. Rongxing Lu, Zhenfu Cao and Xiaolei Dong. Authenticated encryption protocol with perfect forward secrecy for mobile communication, **Wireless Communications and Mobile Computing**, 6 (3), 273-280, 2006.
99. Jun Shao, Zhenfu Cao. A traceable threshold signature scheme with multiple signing policies, **Computers & Security**, 25(3), 201-206, 2006.
100. Dazhi Sun, Zhenfu Cao and Yu Sun. How to compute modular exponentiation with large operators based on the right-to-left binary algorithm, **Applied Mathematics and Computation**, 176(1), 280-292, 2006.
101. Lihua Wang, Zhenfu Cao, Takeshi Okamoto, Ying Miao, and Eiji Okamoto. Authorization-Limited Transformation-Free Proxy Cryptosystems and Their Security Analyses, **IEICE Transactions on Fundamentals**, E89-A, 106 -114, 2006.
102. Rongxing Lu and Zhenfu Cao. Off-line Password Guessing Attack on An Efficient Key Agreement Protocol for Secure Authentication, **International Journal of Network Security**, 3 (1), 35-38, 2006
103. Rongxing Lu and Zhenfu Cao. A Directed Signature Scheme Based on RSA Assumption, **International Journal of Network Security**, 2(3), 182-186, 2006.
104. Zhenchuan Chai, Zhenfu Cao, and Rongxing Lu. A forward secure remote authentication based on factoring, **Journal of Information and Computational Science**, 3(3), 373-384, 2006.
105. Qin Wang, Zhenfu Cao. A Secure Proxy Signcryption Scheme Based on Discrete Logarithm Problem, **Journal of Information and Computational Science**, 3(3), 567-574, 2006.
106. Shengbao Wang, Zhenfu Cao and Xiaolei Dong. Certificateless Authenticated Key Agreement Based on the MTI/C0 Protocol, **Journal of Information and Computational Science**, 3(3), 575-582, 2006.
107. Rongxing Lu and Zhenfu Cao. Efficient remote user authentication scheme using smart card, **Computer Networks**, 49 (4), 535-540, 2005.
108. Haiyong Bao, Zhenfu Cao and Shengbao Wang. Remarks on Wu -Hsu's threshold signature scheme using self-certified public keys, **Journal of Systems and Software**, 78(1), 56-59, 2005.
109. Rongxing Lu and Zhenfu Cao. Non-interactive deniable authentication protocol based on factoring, **Computer Standards & Interfaces**, 27 (4), 401-405, 2005.
110. Kejun Chen, Zhenfu Cao and Ruizhong Wei. Super-simple balanced incomplete block designs with block size 4 and index 6, **Journal of Statistical Planning and Inference**, 133(2), 537-554, 2005.
111. Rongxing Lu, Zhenfu Cao and Yuan Zhou. Threshold undeniable signature scheme based on conic, **Applied Mathematics and Computation**, 162 (1), 165-177, 2005.
112. Yuan Zhou, Zhenfu Cao and Rongxing Lu. Provably secure proxy-protected signature schemes based on factoring, **Applied Mathematics and Computation**, 164(1), 83-98, 2005.
113. Rongxing Lu, Zhenfu Cao and Yuan Zhou. Proxy blind multi-signature scheme without a secure channel, **Applied Mathematics and Computation**, 164 (1), 179 -187, 2005.
114. Dazhi Sun, Zhenfu Cao, Yu Sun. Comment: cryptanalysis of Lee-Hwang-Li's key authentication scheme, **Applied Mathematics and Computation**, 164(3), 675-678, 2005.
115. Rongxing Lu, Zhenfu Cao and Haojin Zhu. A robust (k, n) + 1 threshold proxy signature scheme based on factoring, **Applied Mathematics and Computation**, 166 (1), 35-45, 2005.
116. Haifeng Qian, Zhenfu Cao and Haiyong Bao. Cryptanalysis of Li-Tzeng-Hwang's improved signature schemes based on factoring and discrete logarithms, **Applied Mathematics and Computation**, 166(3), 501-505, 2005.
117. Dazhi Sun, Zhenfu Cao, Yu Sun. Remarks on a new key authentication scheme based on discrete logarithms, **Applied Mathematics and Computation**, 167(1), 572-575, 2005.
118. Jun Shao and Zhenfu Cao. A new efficient (t, n) verifiable multi-secret sharing (VMSS) based on YCH scheme, **Applied Mathematics and Computation**, 168(1), 135 -140, 2005.
119. Dazhi Sun, Zhenfu Cao. Improved public key authentication scheme for non-repudiation, **Applied Mathematics and Computation**, 168(2), 527 - 532, 2005.
120. Rongxing Lu and Zhenfu Cao, A new deniable authentication protocol from bilinear pairings, **Applied Mathematics and Computation**, 168(2), 954 - 961, 2005.
121. Rongxing Lu and Zhenfu Cao. Designated verifier proxy signature scheme with message recovery, **Applied Mathematics and Computation**, 169 (2), 1237-1246, 2005.
122. Haiyong Bao, Zhenfu Cao and Rongxing Lu. Proxy signature scheme using self-certified public key, **Applied Mathematics and Computation**, 169(2), 1380 -1389, 2005.
123. Haiyong Bao, Zhenfu Cao and Shengbao Wang. Improvement on Tzeng et al.'s nonrepudiable threshold multi-proxy multi-signature scheme with shared verification, **Applied Mathematics and Computation**, 169(2), 1419 -1430, 2005.
124. Haifeng Qian, Zhenfu Cao and Haiyong Bao. Security of Pon-Lu-Jeng's Meta-He digital signature schemes, **Applied Mathematics and Computation**, 170(1), 724 - 730, 2005.
125. Yu Long, Zhenfu Cao, Kefei Chen. A dynamic threshold commercial key escrow scheme based on conic, **Applied Mathematics and Computation**, 171 (2), 972 - 982, 2005.
126. Qian Haifeng, Cao Zhenfu and Xue Qingshui. Efficient pairing-based threshold proxy signature scheme with known signers, **Informatica**, 16(2), 261 - 274, 2005.

127. Dazhi Sun and Zhenfu Cao. Novel forgery method based on some password authentication schemes, **Journal of Computational Information Systems**, 1(3), 471 - 475, 2005.
128. Kejun Chen, Zhenfu Cao and R Wei. Elementary Abelian Difference Families with Block Size <= 6, **Bulletin of ICA**, Vol. 43, 80 - 84, 2005.
129. Kejun Chen, Zhenfu Cao and Ruizhong Wei. Existence of V(9, t) vectors, **Journal of Combinatorial Mathematics and Combinatorial Computing**, Vol. 55, 209 - 221, 2005.
130. Kejun Chen, Zhenfu Cao and Dianhua Wu. Existence of APAV(q, k) with q a prime power = 5 mod 8, **Discrete Mathematics**, 279(1-3), 153 - 161, 2004.
131. Haifeng Qian, Zhenfu Cao, Qingshui Xue. A new threshold proxy signature scheme from bilinear pairings, **Science in China Series F**, 47(5), 612 - 622, 2004.
132. Zhenfu Cao and Xiaolei Dong. An application of a lower bound for linear forms in two logarithms to the Terai-Jesmanowicz conjecture, **Acta Arithmetica**, 110 (2), 153 - 164, 2003.
133. Jiguo Li, Zhenfu Cao and Yichen Zhang, Nonrepudiable proxy multi - signature schemes, **Journal of Computer Science and Technology**, 18(3), 399 - 402, 2003.
134. Jiguo Li, Jianzhong Li, Zhenfu Cao and Yichen Zhang. Nonrepudiable threshold proxy signcryption scheme with known signers, **Journal of Software**, 14(12), 2029 - 2035, 2003.
135. Zhenfu Cao, Xiaolei Dong and Zhong Li, A new conjecture concerning the Diophantine equation $x^2+b^y=c^z$, **Proceedings of the Japan Academy Series A**, 78A (10), 202 - 205, 2002.
136. Zhenfu Cao, Xiaolei Dong, On the Terai-Jesmanowicz conjecture, **Publicationes Mathematicae-Debrecen**, 22, 1 - 13, 2002.
137. Zhenfu Cao. A threshold key escrow scheme based on public key cryptosystem, **Science in China (Series E)**, 44(4), 441-448, 2001.
138. Xiaolei Dong and Zhenfu Cao. Diophantine equations and class number of real quadratic fields, **Acta Arithmetica**, 97(4), 313-328, 2001.
139. Zhenfu Cao and Xiaolei Dong. The Diophantine equation $x^2 + b^y = c^z$, **Proceedings of the Japan Academy Series A**, 77A(1),1-4, 2001.
140. Zhenfu Cao. On Whiteman's and Storer's difference sets, **Journal of Statistical Planning and Inference**, 94(2), 147-154, 2001.
141. Y. Bugeaud, Zhenfu Cao and M. Mignotte. On simple K_4-groups, **Journal of Algebra**, 241(2), 658-668, 2001.
142. Zhenfu Cao, Jozsef Sandor. On the diophantine equation $4^x + 18^y = 22^z$, **Octogon Mathematical Magazine**, 9(2), 937-938, 2001.
143. Zhenfu Cao. On the Diophantine equation $x^p+2^{2m}=py^2$, **Proceedings of the American Mathematical Society**, 128(7), 1927-1931, 2000.
144. Zhenfu Cao S. Mu and Xiaolei Dong. A new proof of a conjecture of Antoniadis, **Journal of Number Theory**, 83(2), 185-193, 2000.
145. Zhenfu Cao. The multi-dimension RSA and its low exponent security, **Science in China (Series E)**, 43(4), 349-354, 2000.
146. Zhenfu Cao. A kind of Diophantine equations in finite simple groups, **Northeast Math. J.**, 16(4), 391-397, 2000.
147. Zhenfu Cao and Aleksander Grytczuk. Some remarks on Fermat's equation in the set of matrices, **Acta Academiae Paedagogicae Agriensis**, 27, 39-46, 2000.
148. Zhenfu Cao and A. Grytczuk. Some classes of Diophantine equations connected with McFarland's and Ma's conjectures, **Discuss. Math.-General Algebra and Applications**, 20(2), 193-198, 2000.
149. Zhenfu Cao and Xiaolei Dong. Diophantine equations and class number of imaginary quadratic fields, **Discuss. Math.- General Algebra and Applications**, 20(2), 199 -206, 2000.
150. Zhenfu Cao. A note on the Diophantine equation $a^x+b^y=c^z$, **Acta Arithmetica**, 91(1), 85-93, 1999.
151. Zhenfu Cao. The Diophantine equations $x^4 - y^4 = z^p$ and $x^4 - 1 = dy^q$, **C. R. Math. Rep. Acad. Sci. Canada**, 21(1), 23-27, 1999.
152. Zhenfu Cao and Xiaolei Dong. Diophantine equation $Ax^2 + B = y^n$, **Chinese Science Bulletin**, 43(13), 1141-1142, 1998.
153. Zhenfu Cao and Xiaolei Dong. On Terai's conjecture, **Proceedings of the Japan Academy Series A**, 74A(8), 127-129, 1998.
154. Zhenfu Cao and A. Grytczuk. Fermat's type equation in the set of 2x2 integral matrices, **Tsukuba Journal of Mathematics**, 22 (3), 637-643, 1998.
155. Zhenfu Cao. Corrigendum to ' ' On the Diophantine equation $x^4 - py^2 = z^p$'', **C. R. Math. Rep. Acad. Sci. Canada**, 18(5), 233-234, 1996.
156. Zhenfu Cao. Finite set theory and its application to cryptology, **Journal of Statistical Planning and Inference**, 51(2), 129-136, 1996.
157. Zhenfu Cao. On the Diophantine equation $x^4 - py^2 = z^p$, **C. R. Math. Rep. Acad. Sci. Canada**, 17(2), 61-66, 1995.
158. Zhenfu Cao. The Diophantine equation $cx^4 + dy^4 = z^p$, **C. R. Math. Rep. Acad. Sci. Canada**, 14(5), 231-234, 1992.
159. Zhenfu Cao. On the Diophantine equation $\frac{ax^m - 1} {abx - 1} = by^2$, **Chinese Science Bulletin**, 36(4), 275-278, 1991.
160. Zhenfu Cao. On the Diophantine equation $ax^m - by^n = 2$, **Chinese Science Bulletin**, 35(14), 1227-1228, 1990.
161. Zhenfu Cao, R. Liu and L. Zhang. On the Diophantine equation $\sum_{j=1}^s \frac1{x_j}+\frac1{x_1 \cdots x_s}=1$ and Znam's problem, **Journal of Number Theory**, 27(2), 206-211, 1987.
162. Zhenfu Cao. On the Diophantine equation $a^x + b^y = c^z$, I, **Chinese Science Bulletin**, 32(22), 1519-1521, 1987.
163. Zhenfu Cao. On the Diophantine equation $x^{2n} - \mathcal{D}y^2 = 1$, **Proceedings of the American Mathematical Society**, 98(1), 11-16, 1986.
164. Q. Sun and Zhenfu Cao. On the equation $\sum_{j=1}^s \frac1{x_j} + \frac1{x_1 \cdots x_s} = n$ and the number of solutions of Znam's problem, **Advances in Mathematics (China)**, 15(3), 329-330, 1986.
165. Zhenfu Cao. The equation $a^x - b^y = (2p^s)^z$ and Hugh Edgar's problem, **Chinese Science Bulletin**, 31(8), 572-573, 1986.
166. Zhenfu Cao. The equation $x^2 + 2^m = y^n$ and Hugh Edgar's problem, **Chinese Science Bulletin**, 31(22), 1578-1579, 1986.
167. Z. Xu and Zhenfu Cao. On a problem of Mordell, **Chinese Science Bulletin**, 31(13), 932, 1986.
168. Q. Sun and Zhenfu Cao. On the equation $\frac1{x_1} + \cdots + \frac1{x_s} - \frac1{x_1 \cdots x_s} = 1$ and its applications, **Chinese Science Bulletin**, 30(5), 700-701, 1985.