132 Selected Conference Papers (since 2002)

1. Jun Zhou, Zhenfu Cao, Xiaolei Dong, Xiaodong Lin. TR-MABE: White-Box Traceable and Revocable Multi-authority Attribute-based Encryption and Its Applications to Multi-level Privacy-preserving e-Healthcare Cloud Computing Systems, **IEEE INFOCOM 2015**.
2. Jianting Ning, Zhenfu Cao, Xiaolei Dong, Lifei Wei, Xiaodong Lin: Large Universe Ciphertext-Policy Attribute-Based Encryption with White-Box Traceability. **ESORICS 2014 (2)**: 55-72, 2014.
3. Xiaolei Dong, J. Zhou, K. Alharbi, X. Lin and Zhenfu Cao, An ElGamal-based efficient and privacy-preserving data aggregation scheme for smart grid, **IEEE Globecom 2014**.
4. Yabin Ping, Zhenfu Cao, Haojin Zhu, Sybil-aware Least Cost Rumor Blocking in Social Networks, **IEEE Globecom 2014.**
5. Hong Zhang, Zhenfu Cao, Xiaolei Dong and Jiachen Shen. 4P_VES: a Collusion-Resistant Accountable Virtual Economy System. **ICICS 2014**.
6. Zongyang Zhang, Yu Chen, Sherman S. M. Chow, Goichiro Hanaoka, Zhenfu Cao, Yunlei Zhao: All-but-One Dual Projective Hashing and Its Applications. **ACNS 2014**: 181-198, 2014.
7. Qingshui Xue, Fengying Li and Zhenfu Cao： Proxy Multi-Signature Binding Positioning Protocol. **IEEE/CIC ICCC 2014**, October 13-15, Shanghai, China, pp. 166-170 (2014).
8. Qingshui Xue, Fengying Li and Zhenfu Cao: Threshold proxy signature based on position. **SECURWARE 2014**, November 16-20, Lisbon, Portugal. pp.151-156 (2014) .
9. Qingshui Xue, Fengying Li, and Zhenfu Cao: Secure-positioning-protocol-based symmetric cryptography. **MobiHealth 2014**, November 3-5, Athens, Greece (2014) .
10. Qingshui Xue, Fengying Li, and Zhenfu Cao: positioning-protocol-based digital signature. **WICON 2014**, November 13-14, Lisbon, Portugal (2014) .
11. Danyang He, Zhenfu Cao, Xiaolei Dong, Jiachen Shen. User Self-controllable Profile Matching for Privacy-preserving Mobile Social Networks, **ICCS 2014**.
12. Zhe Li, Xiaolei Dong, Zhenfu Cao. Generalized Cipolla-Lehmer Root Computation in Finite Fields, **ICINS 2014**.
13. Siqiong Fan, Zhenfu Cao, Xiaolei Dong. Cryptanalysis and improvement of a smart card-based identity authentication scheme, **ICINS 2014**.
14. Zhenfu Cao, Fangguo Zhang (Eds.): **Pairing-Based Cryptography - Pairing 2013** - 6th International Conference, Beijing, China, November 22-24, 2013, Revised Selected Papers. Lecture Notes in Computer Science 8365, Springer 2014, ISBN 978-3-319-04872-7.
15. Zhen Liu, Zhenfu Cao, Duncan S. Wong: Blackbox traceable CP-ABE: how to catch people leaking their keys by selling decryption devices on ebay. **ACM CCS 2013**: 475-486, 2013.
16. Zhaoyu Gao, Haojin Zhu, Yao Liu, Muyuan Li, Zhenfu Cao: Location privacy in database-driven Cognitive Radio Networks: Attacks and countermeasures. **INFOCOM 2013**: 2751-2759, 2013.
17. Jun Zhou, Zhenfu Cao, and Xiaolei Dong. BDK: Secure and Efficient Biometric based Deterministic Key Agreement in Wireless Body Area Networks. **BODYNETS 2013**, Boston, Massachusetts, United States, September 30–October 2, 2013.
18. Yu Chen, Zongyang Zhang, Dongdai Lin, Zhenfu Cao: Identity-Based Extractable Hash Proofs and Their Applications. **ACNS 2012**: 153-170, 2012.
19. Zhaoyu Gao, Haojin Zhu, Yao Liu, Muyuan Li, Zhenfu Cao: Location privacy leaking from spectrum utilization information in database-driven cognitive radio network. **ACM CCS 2012**: 1025-1027
20. Jun Zhou, Zhenfu Cao: TIS: A threshold incentive scheme for secure and reliable data forwarding in vehicular Delay Tolerant Networks. **GLOBECOM 2012**: 985-990
21. Yu Chen, Zongyang Zhang, Dongdai Lin, Zhenfu Cao: Anonymous Identity-Based Hash Proof System and Its Applications. **ProvSec 2012**: 143-160
22. Chengxin Xiao, Weiwei Jia, Haojin Zhu, Suguo Du, Zhenfu Cao: Leveraging Cloud Computing for Privacy Preserving Aggregation in Multi-domain Wireless Networks. **WASA 2012**: 733-744
23. Lifei Wei, Haojin Zhu, Zhenfu Cao, Xuemin (Sherman) Shen: MobiID: A User-Centric and Social-Aware Reputation Based Incentive Scheme for Delay/Disruption Tolerant Networks. **ADHOC-NOW 2011**: 177-190
24. Huang Lin, Zhenfu Cao, Yuguang Fang, Muxin Zhou, Haojin Zhu: How to design space efficient revocable IBE from non-monotonic ABE. **ASIACCS 2011**: 381-385
25. Zhen Liu, Zhenfu Cao, Qiong Huang, Duncan S. Wong, Tsz Hon Yuen: Fully Secure Multi-authority Ciphertext-Policy Attribute-Based Encryption without Random Oracles. **ESORICS 2011**: 278-297
26. Haiyong Bao, Guiyi Wei, Jun Shao, Zhenfu Cao: Efficient and secure electronic resume using smart cards. **FSKD 2011**: 2271-2274
27. Haiyong Bao, Guiyi Wei, Jun Shao, Zhenfu Cao: Novel conic-based group signature scheme with revocation. **FSKD 2011**: 2623-2627
28. Le Chen, Zhenfu Cao, Rongxing Lu, Xiaohui Liang, Xuemin Shen: EPF: An Event-Aided Packet Forwarding Protocol for Privacy-Preserving Mobile Healthcare Social Networks. **GLOBECOM 2011**: 1-5
29. Lifei Wei, Zhenfu Cao, Haojin Zhu: MobiGame: A User-Centric Reputation Based Incentive Protocol for Delay/Disruption Tolerant Networks. **GLOBECOM 2011**: 1-5
30. Jun Shao, Peng Liu, Zhenfu Cao, Guiyi Wei: Multi-Use Unidirectional Proxy Re-Encryption. **ICC 2011**: 1-5
31. Jun Shao, Min Feng, Bin B. Zhu, Zhenfu Cao, Peng Liu: The Security Model of Unidirectional Proxy Re-Signature with Private Re-Signature Key. **ACISP 2010**: 216-232
32. Huang Lin, Zhenfu Cao, Xiaohui Liang, Muxin Zhou, Haojin Zhu, Dongsheng Xing: How to Construct Interval Encryption from Binary Tree Encryption. **ACNS 2010**: 19-34
33. Lihua Wang, Licheng Wang, Zhenfu Cao, Eiji Okamoto, Jun Shao: New Constructions of Public-Key Encryption Schemes from Conjugacy Search Problems. **Inscrypt 2010**: 1-17
34. Fengying Li, Qingshui Xue, Zhenfu Cao: Some basic principles for proxy signature schemes based on ECDLP. **CollaborateCom 2010**: 1-5
35. Feng Cao, Zhenfu Cao: An Identity Based Proxy Signature Scheme Secure in the Standard Model. **GrC 2010**: 67-72
36. Lifei Wei, Haojin Zhu, Zhenfu Cao, Weiwei Jia, Athanasios V. Vasilakos: SecCloud: Bridging Secure Storage and Computation in Cloud. **ICDCS Workshops 2010**: 52-61
37. Haojin Zhu, Xiaodong Lin, Rongxing Lu, Xuemin Shen, Dongsheng Xing, Zhenfu Cao: An Opportunistic Batch Bundle Authentication Scheme for Energy Constrained DTNs. **INFOCOM 2010**: 605-613
38. Zhenfu Cao, Ivan Visconti, Zongyang Zhang: Constant-Round Concurrent Non-Malleable Statistically Binding Commitments and Decommitments. **PKC 2010**: 193-208
39. Xiaohui Liang, Zhenfu Cao, Huang Lin, and Jun Shao. Attribute Based Proxy Re-encryption with Delegating Capabilities. **ASIACCS 2009**, Sydney, Australia, 10-12 March 2009. ACM, 276-286, 2009.
40. Xiaohui Liang, Zhenfu Cao, Huang Lin, and Dongsheng Xing. Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption. **ASIACCS 2009**, Sydney, Australia, 10-12 March 2009. ACM, 343-352, 2009.
41. Hai Huang and Zhenfu Cao. An ID-based Authenticated Key Exchange Protocol Based on Bilinear Diffie-Hellman Problem. **ASIACCS 2009**, Sydney, Australia, 10-12 March 2009. ACM, 333-342, 2009.
42. Zongyang Zhang, Zhenfu Cao, Ning Ding, and Rong Ma. Non-malleable Statistically Hiding Commitment from Any One-way Function. **ASIACRYPT 2009**, Tokyo, Japan, December 6-10, 2009.
43. Jun Shao and Zhenfu Cao. CCA-Secure Proxy Re-Encryption without Pairings. **PKC 2009**, California, USA, March 18-20, 2009. Lecture Notes in Computer Science, Springer, 5443: 357-376, 2009.
44. Hai Huang and Zhenfu Cao. An Insider-Resistant Group Key Exchange Protocol without Signatures. **IEEE ICC'09**, Dresden, Germany, June 14-18, 2009.

45. Zongyang Zhang, Zhenfu Cao, and Rong Ma. An Observation on Non-Malleable Witness-Indistinguishability and Non-Malleable Zero-Knowledge. **TAMC 2009**, Changsha, P. R. China, May 18-22, 2009. Lecture Notes in Computer Science, Springer, 5532: 470-479, 2009.
46. Muxin Zhou and Zhenfu Cao. Spatial Encryption under Simpler Assumption. **ProvSec 2009**, Guangzhou, China, November 11-13, 2009.
47. Yinan Shan and Zhefu Cao. Extended attribute based encryption for private information retrieval. **MASS 2009**: 702-707, October 12-14, 2009.
48. Piyi Yang, Zhenfu Cao, and Xiaolei Dong. A Dependable Threshold Broadcast Encryption System for Key Distribution in Mobile Ad Hoc Network. The Second (IEEE) International Conference on Dependability (**DEPEND 2009**), Athens/Glyfada, Greece, June 18-23, 2009.
49. Piyi Yang, Zhenfu Cao, and Xiaolei Dong. Certificateless Threshold Signature for Data Report Authentication in Mobile Ad-Hoc Network. 3rd International Conference on Network & System Security (**NSS 2009**), Gold Coast, Australia, October 19-21, 2009.
50. Qingshui Xue, Fengying Li, Yuan Zhou, Jiping Zhang, Zhenfu Cao, Haifeng Qian: Bilinear-pairings Based Designated-verifier Threshold Proxy Signature Scheme. **Security and Management 2009**: 323-327
51. Qingshui Xue, Fengying Li, Yuan Zhou, Jiping Zhang, Zhenfu Cao, Haifeng Qian: An ECDLP-Based Threshold Proxy Signature Scheme Using Self-Certified Public Key System. **MobiSec 2009**: 58-70
52. Liuquan Qin, Zhenfu Cao, and Xiaolei Dong. Multi-receiver identity-based encryption in multiple PKG environment, Proc. **IEEE Globecom'08**, New Orleans, LA, USA, Nov. 30-Dec. 4, 2008. IEEE, 1862-1866, 2008.
53. Rongxing Lu, Xiaodong Lin, Haojin Zhu, Pin-Han Ho, Xuemin(Sherman) Shen, and Zhenfu Cao. A new dynamic group key management scheme with low rekeying cost, Proc. **IEEE WCNC'08**, Las Vegas, Nevada, USA, March 31 - April 3, 2008. IEEE, 3243-3248, 2008.
54. Huang Lin, Zhenfu Cao, Xiaohui Liang, and Jun Shao. Secure threshold multi-authority attribute based encryption without a central authority, **INDOCRYPT 2008**, Lecture Notes in Computer Science, Springer, 5365: 426-436, 2008.
55. Piyi Yang, Zhenfu Cao, and Xiaolei Dong. Chosen Ciphertext Secure Certificateless Threshold Encryption in the Standard Model, **Inscrypt 2008**, Beijing, December 14-17, 2008. Lecture Notes in Computer Science, Springer, 5487: 201-216, 2009.
56. Congkai Sun, Bin Gao, Zhenfu Cao, and Hang Li. HTM: A topic model for hypertexts, **EMNLP 2008**, Hawaii, USA, October 25-27, 2008. Proceedings of the Conference, 514-522, 2008.
57. Piyi Yang, Zhenfu Cao, and Xiaolei Dong, Threshold Proxy Re-Signature. 27th IEEE International Performance Computing and Communications Conference, **IPCCC 2008**, Dec 7-9 2008, Austin, Texas, USA. Proceedings of the Conference, 450-455, 2008.
58. Fengying Li, Qingshui Xue, Jiping Zhang, and Zhenfu Cao. A Model of Bilinear-Pairings Based Designated-Verifier Proxy Signatue Scheme. **CollaborateCom 2008**, Orlando, FL, USA, November 13-16, 2008, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 10, Springer, 416-424, 2009.
59. Xiaodong Lin, Rongxing Lu, Haojin Zhu, P.H. Ho, Xuemin Shen and Zhenfu Cao. ASRPAKE: An Anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks, Proc. **IEEE ICC'07**, Glasgow, UK, June 24-28, 2007.
60. Xiaodong Lin, Rongxing Lu, P.H. Ho, Xuemin Shen and Zhenfu Cao. A novel compromise-resilient authentication system for wireless mesh networks, Proc. **IEEE WCNC'07**, Hong Kong, March 11-15, 2007.
61. Jun Shao, Zhenfu Cao, Licheng Wang, Rongxing Lu. Efficient password-based authenticated key exchange without public information, **ESORICS 2007**, Lecture Notes in Computer Science, Volume 4734: 299-310, 2007.
62. Jun Shao, Min Feng, Bin Zhu, and Zhenfu Cao. An efficient certified email protocol, **ISC 2007**, Lecture Notes in Computer Science, Volume 4779: 145-157, 2007.
63. Jun Shao, Zhenfu Cao, Licheng Wang, Xiaohui Liang. Proxy re-signature schemes without random oracles, **INDOCRYPT 2007**, Lecture Notes in Computer Science, Volume 4859: 197-209, 2007.
64. Licheng Wang, Zhenfu Cao, Shihui Zheng, Xiaofang Huang, Yixian Yang. Transitive signatures from braid groups, **INDOCRYPT 2007**, Lecture Notes in Computer Science, Volume 4859: 183-196, 2007.
65. Lihua Wang, Jun Shao, Zhenfu Cao, Masahiro Mambo, Akihiro Yamamura. A certificate-based proxy cryptosystem with revocable proxy decryption power, **INDOCRYPT 2007**, Lecture Notes in Computer Science, Volume 4859: 297-311, 2007.
66. Xiaohui Liang, Zhenfu Cao, Jun Shao, Huang Lin. Short group signature without random oracles, **ICICS 2007**, Lecture Notes in Computer Science, Volume 4861: 69-82, 2008.
67. Licheng Wang, Zhenfu Cao, Peng Zeng and Xiangxue Li. One-more matching conjugate problem and security of braid-based signatures, **ASIACCS 2007**, Singapore, ACM Press, pp.295-301, 2007.
68. Fengying Li, Qingshui Xue, Zhenfu Cao. Crypanalysis of Kuo and Chen's threshold proxy signature scheme based on the RSA, **ITNG 2007**, Proceedings, pp. 815-818, 2007.
69. Zhenfu Cao, Dazhi Sun. Cryptanalysis and improvement of user authentication scheme using smart cards for multi-server environments, **ICMLC 2006**, Proceedings, IEEE Computer Society Press, Vol. 5, pp. 2818 - 2822, 2006.
70. Shanshan Duan and Zhenfu Cao. Efficient and provably secure multi-receiver identity-based signcryption, **ACISP 2006**, Lecture Notes in Computer Science, Vol. 4058, 195-206, 2006.
71. Rongxing Lu, Zhenfu Cao, Xiaolei Dong. Efficient ID-based One-time Proxy Signature and Its Application in E-cheque, **CANS 2006**, Lecture Notes in Computer Science, Vol. 4301, 153 -167, 2006.
72. Feng Cao and Zhenfu Cao. Security model of proxy-multi signature schemes, **CANS 2006**, Lecture Notes in Computer Science, Vol. 4301, 144 -152, 2006.
73. Yuan Zhou, Zhenfu Cao, Zhenchuan Chai. Identity Based Key Insulated Signature, **ISPEC 2006**, Lecture Notes in Computer Science, Vol. 3903, 226-234, 2006.
74. Zhenchuan Chai, Zhenfu Cao, Rongxing Lu. Remote Authentication with Forward Security, Remote Authentication with Forward Security, **ATC 2006**, Lecture Notes in Computer Science, Vol. 4158, 418-427, 2006.
75. Zhenchuan Chai, Zhenfu Cao, Rongxing Lu. Efficient Password-based Authentication and Key Exchange Scheme Preserving User Privacy, **WASA 2006**, Lecture Notes in Computer Science, Vol. 4138, 467-477, 2006.
76. Haiyong Bao, Zhenfu Cao, and Shengbao Wang. Identity-based threshold proxy signature scheme with known signers, **TAMC 2006**, Lecture Notes in Computer Science, Vol. 3959, 538-546, 2006.
77. Rongxing Lu, Xiaolei Dong, Zhenfu Cao, Licheng Wang. Design of smart card-based electronic vita using proxy signature technique, **CIS 2006**, pp.1385-1388, 2006.
78. Shengbao Wang and Zhenfu Cao. Cryptanalysis and Improvement of Choie et al.'s Authenticated Key Agreement Protocols, **CIS 2006**, pp.1371-1374, 2006.
79. Licheng Wang, Zhenfu Cao and Feng Cao. Cryptanalysis and Improvement on An ID-Based Key Issuing Protocol, **IMSCCS 06** , IEEE Computer Society Press, Vol. 2, pp. 8 - 12, 2006.
80. Feng Cao, Licheng Wang and Zhenfu Cao. An Improvement of an Identity-Based Key Issuing Protocol, **IMSCCS 2006**, IEEE Computer Society Press, Vol, 2, pp.13 - 18, 2006.
81. Rongxing Lu, Zhenfu Cao, Xiaolei Dong and Renwang Su. Designated Verifier Proxy Signature Scheme from Bilinear Pairings, **IMSCCS 2006**, IEEE Computer Society Press, Vol, 2, pp. 40-47, 2006.
82. Feng Cao and Zhenfu Cao. A proxy-protected signature scheme based on finite automaton, **IMSCCS 2006**, IEEE Computer Society Press, Vol, 2, pp.48 - 55, 2006.
83. Sheng Guo, Zhenfu Cao, Rongxing Lu. An Efficient ID-Based Multi-proxy Multi-signature Scheme, **IMSCCS 2006**, IEEE Computer Society Press, Vol, 2, 81-88, 2006.

84. Rongxing Lu, Zhenfu Cao, Xiaolei Dong and Renwang Su. Group Oriented Deniable Authentication Protocol, **IMSCCS 2006**, IEEE Computer Society Press, Vol, 2, 89 - 92, 2006.
85. Shengbao Wang, Zhenfu Cao and Haiyong Bao. Two-Pass ID-Based Authenticated Key Agreement Protocol with Key Confirmation Using Pairings, **IMSCCS 06**, IEEE Computer Society Press, Vol. 2, pp. 109 - 112, 2006.
86. Haifeng Qian, Zhenfu Cao, Licheng Wang, Sheng Guo. Cryptanalysis of Chang-Lin-Lam's ID-based Multisignature Scheme, **IMSCCS 06**, IEEE Computer Society Press, Vol. 2, pp. 113-116, 2006.
87. Feng Cao and Zhenfu Cao. Cryptanalysis on a proxy multi-signature scheme, **IMSCCS 2006**, IEEE Computer Society Press, Vol, 2, pp.117 - 120, 2006.
88. Zhenchuan Chai, Zhenfu Cao, and Yuan Zhou. Efficient ID-based Broadcast Threshold Decryption in Ad hoc Network, **IMSCCS 06**, IEEE Computer Society Press, Vol. 2, pp.148-154, 2006.
89. Rongxing Lu, Zhenfu Cao, Xiaolei Dong. Efficient and Provably Secure Transformation-free Proxy Cryptosystem, **IWAP2006**, 5th International Workshop on Applied PKC, 2006.
90. Rongxing Lu, Zhenfu Cao, Xiaolei Dong, Licheng Wang. Threshold Short Proxy Signature Scheme with Provable Security, **Inscrypt 2006** (formerly The SKLOIS conference on information security and cryptology) short paper proceedings, pp. 54-68, 2006.
91. Rongxing Lu, Zhenfu Cao, Xiaolei Dong. Pairing-Based Proxy Ring Signature Scheme with Proxy Signer Privacy Protection, **ChinaCrypto'2006**, pp.1-10, 2006.
92. Xiaohui Liang, Zhenfu Cao, Zhenchuan Chai and Rongxing Lu. ID-based Threshold Blind Signature scheme from Bilinear Pair, **ChinaCrypto'2006**, pp.244 - 252, 2006.
93. Licheng Wang, Zhenfu Cao, et al. Certificateless Threshold Signature Schemes, **CIS 2005**, Part II, Lecture Notes in Artificial Intelligence, Vol. 3802, Springer-Verlag, 104-109, 2005.
94. Qin Wang, Zhenfu Cao. Efficient ID-Based Proxy Signature and Proxy Signcryption form Bilinear Pairings, **CIS 2005**, Part II, Lecture Notes in Artificial Intelligence, Vol. 3802, Springer-Verlag, 167-172, 2005.
95. Shanshan Duan, Zhenfu Cao. Secure Delegation-by-Warrant ID-Based Proxy Signcryption Scheme, **CIS 2005**, Part II, Lecture Notes in Artificial Intelligence, Vol. 3802, Springer-Verlag, 445 - 450, 2005.
96. Yuan Zhou, Zhenfu Cao and Rongxing Lu. Constructing Secure Warrant-Based Proxy Signcryption Schemes, **CANS 2005**, Lecture Notes in Computer Science, Vol. 3810, Springer-Verlag, 172 - 185, 2005.
97. Haiyong Bao, Zhenfu Cao, and Haifeng Qian. On the security of a group signcryption scheme from distributed signcryption scheme, **CANS 2005**, Lecture Notes in Computer Science, Vol. 3810, Springer- Verlag, 26 - 34, 2005.
98. Qin Wang, Zhenfu Cao. Two Proxy Signcryption Schemes from Bilinear Pairings, **CANS 2005**, Lecture Notes in Computer Science, 3810, Springer-Verlag, pp.161-171, 2005.
99. Haifeng Qian and Zhenfu Cao. A Novel ID-Based Partial Delegation with Warrant Proxy Signature Scheme, **ISAP2005**, Lecture Notes in Computer Science, Vol. 3759, Springer-Verlag, pp.323 - 331, 2005.
100. Shengbao Wang, Zhenfu Cao, and Haiyong Bao. Security of an Efficient ID-Based Authenticated Key Agreement Protocol from Pairings, **ISAP2005**, Lecture Notes in Computer Science, Vol. 3759, Springer-Verlag, pp. 342-349, 2005.
101. Zhenchuan Chai, Zhenfu Cao, and Yuan Zhou. Encryption Based on Reversible Second-Order Cellular Automata, **ISPA2005**, Lecture Notes in Computer Science, Vol. 3759, Springer-Verlag, pp. 350-358, 2005.
102. Yuan Zhou, Zhenfu Cao and Zhenchuan Chai. An efficient proxy-protected signature scheme based on factoring, **ISPA2005**, Lecture Notes in Computer Science, Vol. 3759, Springer-Verlag, pp. 332 - 341, 2005.
103. Dazhi Sun, Zhenfu Cao. Improvement of Lee-Kim-Yoo's remote user authentication scheme using smart cards, **ICNC'05-FSKD'05**, Lecture Notes in Artificial Intelligence, Vol. 3614, Springer-Verlag, pp.596 - 599, 2005.
104. Yuan Zhou, Zhenfu Cao, Zhenchuan Chai. Construct secure proxy cryptosystem, **CISC 2005**, Lecture Notes in Computer Science, Vol. 3822, Springer-Verlag, pp. 150 - 161, 2005.
105. Qin Wang, Zhenfu Cao and Shengbao Wang. Formailized security model of multi-proxy signature schemes, **CIT 2005**, IEEE CS Press, pp. 668 - 672, 2005.
106. Haifeng Qian, Zhenfu Cao, Lichen Wang and Qingshui Xue. Efficient Non-Interactive Deniable Authentication Protocols, **CIT 2005**, IEEE CS Press, pp. 673 - 679, 2005.
107. Shengbao Wang, Zhenfu Cao, Qin Wang and Mengzi Zhang. Authenticated Key Agreement Protocol using Bilinear Aggregate Signatures, **GMC 2005**, Proceedings of 2005 Global Mobile Congress, Delson Group Inc., pp. 328 - 332, 2005.
108. Qingshui Xue, Zhenfu Cao and Haifeng Qian. A generalized proxy signature scheme based on the RSA cryptosystem, **PDCAT 2004**, Lecture Notes in Computer Science, Vol. 3320, Springer-Verlag, Berlin Heidelberg, pp. 662–665, 2004.
109. Qingshui Xue and Zhenfu Cao. A threshold proxy signature scheme using self-certified public keys, **ISPA 2004**, Lecture Notes in Computer Science, Vol. 3358, Springer-Verlag, Berlin Heidelberg, pp. 715-724, 2004.
110. Zhenchuan Chai and Zhenfu Cao. Factoring-Based Proxy Signature Schemes with Forward-Security, **CIS 2004**, Lecture Notes in Computer Science, Vol. 3314, Springer-Verlag, Berlin Heidelberg, pp. 1034 - 1040, 2004.
111. Qingshui Xue and Zhenfu Cao. Cryptanalysis of new digital nominative proxy signature schemes for mobile communication, **GMC 2004**, Proceedings - 2004 Global Mobile Congress, 302 - 306, 2004.
112. Rongxing Lu and Zhenfu Cao, A proxy-protected twin signature scheme, **GMC 2004**, Proceedings - 2004 Global Mobile Congress, 497 - 502, 2004.
113. Qingshui Xue and Zhenfu Cao, Improvement of Multi-proxy Signature Scheme, **IEEE CIT 2004**, IEEE Computer Society Press, pp. 450 - 455, September 14-16, 2004.
114. Qingshui Xue, Zhenfu Cao and Feilong Tang, An improved threshold proxy signature scheme based on the RSA cryptosystem, **PDPTA 2004**, CSREA Press, Volume 2, pp. 901 - 907, June 21-24, 2004.
115. Qingshui Xue and Zhenfu Cao, A nonrepudiable multi-proxy multi- signature scheme, **IEEE SympoTIC 2004**, Bratislava, Slovakia, pp. 102 - 105, 24-26 October 2004.
116. Qingshui Xue and Zhenfu Cao. A new proxy blind signature scheme with warrant, **IEEE CIS 2004**, Singapore, Volume: 2, 1386-1391, 2004.
117. Rongxing Lu, Zhenfu Cao. A proxy-protected signature scheme based on conic, **ACM Infosecu'04**, ACM press, 22 - 26, 2004.
118. Shanshan Duan, Zhenfu Cao, and Rongxing Lu. Robust ID-based threshold signcryption scheme from pairings, **ACM Infosecu'04**, ACM press, 33 - 37, 2004.
119. Yuan Zhou, Zhenfu Cao, and Rongxing Lu. An efficient digital signature using self-certified public keys, **ACM Infosecu'04**, ACM press, 44 - 47, 2004.
120. Lihua Wang, Zhenhu Cao, Eiji Okamoto, Ying Miao, and Takeshi Okamoto. Transformation-free proxy cryptosystems and their applications to electronic commerce, **ACM Infosecu'04**, ACM press, 92 - 98, 2004.
121. Haiyong Bao, Zhenfu Cao, and Haifeng Qian. Cryptanalysis of group signature scheme from ID-based signature scheme, **ACM Infosecu'04**, ACM press, 115 - 118, 2004.
122. Zhengchuan Chai, Zhenfu Cao, and Rongxing Lu. ID-based Threshold Decryption without Random oracles and its Application in Key Escrow, **ACM Infosecu'04**, ACM press, 119 - 124, 2004.
123. Jun Shao, Rongxing Lu, and Zhenfu Cao. A New Efficient Identification Scheme based on the Strong Diffie-Hellman Assumption, **ISFST 2004**, Published in December 2004 by Software Engineers Association, ISBN 4-916227-17-4.
124. Qingshui Xue and Zhenfu Cao, Security analysis and improvement of some threshold proxy signature schemes, **DCABES 2004**, Wuhan University of Technology Press, Volume 2, pp. 944-949, 2004.
125. Qingshui Xue, Zhenfu Cao, and Haifeng Qian, Bilinear Pairings-based Threshold Proxy Signature Schemes with Known Signers, **DCABES 2004**, Wuhan University of Technology Press, Volume 2, pp. 950 - 955, 2004.
126. Qingshui Xue, Zhenfu Cao and Haifeng Qian, Generalization of Proxy Signature Based on the RSA Cryptosystem, **ISCI 2004**, Volume 2, pp. 913-917, August 15-18, 2004.

127. Qingshui Xue and Zhenfu Cao, Factoring Based Proxy Signature Schemes, **ISCI 2004**, Volume 2, pp. 918-922, August 15-18, 2004.
128. Biao Li, Zhenfu Cao and Shensheng Zhang, ∞-Resilient Robust Key-evolving Scheme, International conference on computer communication, **ICCC 2002**, Indio, 561 - 564, 2002.
129. Zhenfu Cao and Xiaolei Dong. Diophantine equations, quadratic fields and other, **ICM 2002**, Report of International Congress of Mathematicians (15 minutes), Beijing, August 20-28, 2002.
130. Zhenfu Cao. A robust threshold key escrow scheme based on the improved RSA algorithm, **The 5th Northeast Asia Symposium & the 2nd Asian eBusiness Workshop**, Seoul, Korea, August 22-24, 2002.
131. Xiaolei Dong and Zhenfu Cao, $\Bbb Z_N-$trees and its application to public-key cryptosystem, Fourth Shanghai Conference on Combinatorics(**SHC**), May 24-28, 2002.
132. Xiaolei Dong and Zhenfu Cao, Class number problem of some real quadratic fields and quadratic field cryptosystem, Advance in Cryptology-**Chinacrypt'02**, Publishing House of Electronics Industry, 210-219, 2002.