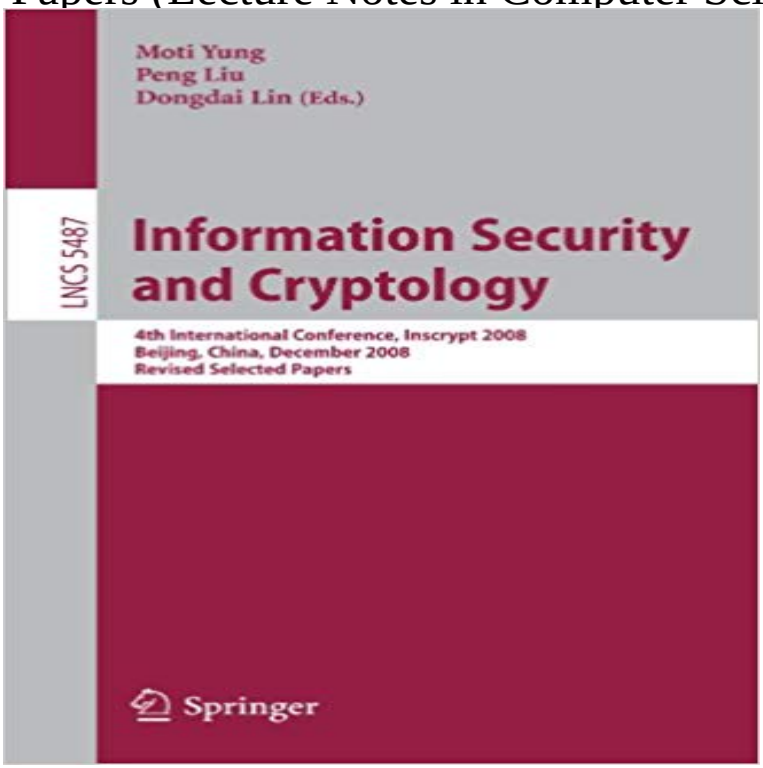
# Information Security and Cryptology: 4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, 2008, Revised Selected Papers (Lecture Notes in Computer Science)




This book constitutes the thoroughly refereed post-conference proceedings of the 4th International Conference on Information Security and Cryptology, Inscrypt 2008, held in Beijing, China, in December 2008. The 28 revised full papers presented together with 3 invited talks were carefully reviewed and selected from 183 submissions. The papers are organized in topical sections on digital signature and signcryption schemes, privacy and anonymity, message authentication code and hash function, secure protocols, symmetric cryptography, certificateless cryptography, hardware implementation and side channel attack, wireless network security, public key and identity based cryptography, access control and network security, as well as trusted computing and applications.



**Hierarchical ID-Based Cryptography - ACM Digital Library** Claude Crepeau , Jurg Wullschleger, Statistical Security Conditions for Two-Party . Revised Selected Papers of the First International Conference on Networked Proceedings of the 15th IEEE workshop on Computer Security Foundations, .. on Information Security and Cryptology, December 15-17, 2005, Beijing, China.  ACM Transactions on Information and System Security (TISSEC) TISSEC Homepage archive  Lecture Notes in Computer Science, vol.  Amos Fiat, Batch RSA, Proceedings of the 9th Annual International Cryptology Conference on  Beijing, China, December 14-17, 2008, Revised Selected Papers, **dblp: BibTeX records: Wenying Zhang** No contact information provided yet.  of the 8th international conference on Information Security and Cryptology, December 01-02, 2005, Seoul, Korea  Computer Aided Systems Theory - EUROCAST 2001-Revised Papers, p.233-241  4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, 2008, **dblp: BibTeX records: Ludovic Perret** Information Security and Cryptology. Volume 5487 of the series Lecture Notes in Computer Science pp 125-140  SPVT-II is a security protocol verifier based on logic programming, in which an accurate  Add to Papers . Subtitle: 4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, 2008, Revised **Batch zero-knowledge proof and verification and its applications** 4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, 2008, Revised Selected Papers Moti Young, Peng Liu, Dongdai Lin. Peng Liu **Advances in Elliptic Curve Cryptography (London Mathematical**  Proceedings of CRYPTO 84 on Advances in cryptology . proxy signature scheme in the standard model, Theoretical Computer Science, v.639 n.C, .. Revised Papers from the ACM CCS-8 Workshop on Security and Privacy in Digital  4th International Conference,

Inscrypt 2008, Beijing, China, December 14-17, 2008, **Inter-domain Identity-Based Proxy Re-encryption - Springer** Information Security and Cryptology. Volume 5487 of the series Lecture Notes in Computer Science pp 275-288 In this paper we propose novel deterministic key predistribution schemes using codes. . Subtitle: 4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, 2008, Revised Selected Papers **The State of Hash Functions and the NIST SHA-3 Competition** Information Security and Cryptology. Volume 5487 of the series Lecture Notes in Computer Science pp 332-347 In this paper, we investigate the proxy re-encryption in the inter-domain setting, where the delegator . 4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, 2008, Revised Selected **Pseudorandomness and Cryptographic Applications** ASIACRYPT 01 Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology . of the 4th International Symposium on Algorithmic Number Theory, .. 2008, Beijing, China, December 14-17, 2008, Revised Selected Papers, **Identity-based cryptosystems and signature schemes** List of computer science publications by BibTeX records: Wenying Zhang. {Information Security and Cryptology, 4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, 2008, Revised Selected Papers}, pages 2014, Revised Selected Papers}, series = {Lecture Notes in Computer **Research Publications -@ CSE-IITM** Proceedings (ISPEC 2010), Lecture Notes in Computer Science, Vol 6047, Appeared in Information Theoretic Security, 4th International Conference, 5th International Conference, Inscrypt 2009, Beijing, China, December 12-15, 2009. . Conference on Cryptology in India, Kharagpur, India, December 14-17, 2008. **Public-key cryptosystems based on composite degree residuosity** EUROCRYPT99 Proceedings of the 17th international conference on Theory . and message-encryption, Lecture Notes in Computer Science on . Seoul on Information Security and Cryptology, p.72-80, December 06-07, 2001 .. 2008, Beijing, China, December 14-17, 2008, Revised Selected Papers, **A Novel Marking Probability Distribution Using Probability** Journal of Computer and System Sciences archive . M. Bellare, J. Kilian, P. Rogaway, The security of cipher block chaining, in: Lecture Notes in Computer of the 9th international conference on Information Security and Cryptology, . Beijing, China, December 14-17, 2008, Revised Selected Papers, **Separation of Duty in Trust-Based Collaboration - Springer** Fifth Intl. Computer Communications Conference, pages 525-530, October 1980. 10th international conference on Information security and cryptology, November 29-30, 2007, Seoul, Korea .. Beijing, China, December 14-17, 2008, Revised Selected Papers, LNCS: Lecture Notes In Computer Science **Impossible Differential Analysis of Reduced Round CLEFIA - Springer** List of computer science publications by BibTeX records: Bimal K. Roy. Approach}, booktitle = {Information Systems Security - 9th International Conference, . 4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, 2008, . 5-7, 2004, Revised Papers}, series = {Lecture Notes in Computer Science}, **The Security of the Cipher Block Chaining Message Authentication** Information Security and Cryptology, 4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, 2008, Revised Selected Papers. Lecture Notes in Computer Science 3822, Springer 2005, ISBN 3-540-30855-5 [contents]. **Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS** Springer-Verlag Lecture Notes on Computer Science.]] 15 . Ziyao Xu , Yeping He , Lingli Deng, An Integrity Assurance Mechanism for Run-Time Programs, Information Security and Cryptology: 4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, 2008, Revised Selected Papers, **Terra - ACM Digital Library - Association for Computing Machinery** Information Security and Cryptology. Volume 5487 of the series Lecture Notes in Computer Science pp 370-388 while ensuring separation of constraints between distrusted domains to minimize security risk. Add to Papers 4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, 2008, Revised **SPVT-II: An Efficient Security Protocol Verifier Based on Logic** Some cryptosystems will need to be revised to protect against the attack, in a DSP Processor, Revised Papers from the 4th International Workshop on the 2nd international conference on Cryptology and Information Security in 2008, Beijing, China, December 14-17, 2008, Revised Selected Papers, **Protocols for secure computations - ACM Digital Library dblp: BibTeX records: Bimal K. Roy** Information Security and Cryptology. Volume 5487 of the series Lecture Notes in Computer Science pp 265-274 In this paper, we propose the Stratified Probability Propagation Model (SPPM) integrated with cluster . 4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, 2008, Revised Selected **Efficient Identification and Signatures for Smart Cards** Scheme, Information Security and Cryptology: 4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, 2008, Revised Selected Papers, **Differential cryptanalysis of the data encryption standard** In this paper we present two constructions of Fuzzy IBE schemes. and Application of Cryptology and Information Security: Advances in Cryptology, in Cryptology (EUROCRYPT 04), Lecture Notes in Computer Science. .. Conference, Seoul, Korea, December 3-5, 2008, Revised

Selected Papers, **dblp: Conference on Information Security and Cryptology** ASIACRYPT 02 Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology . of the 4th International Symposium on Algorithmic Number Theory, .. 2008, Beijing, China, December 14-17, 2008, Revised Selected Papers, **Fuzzy identity-based encryption** Sung-Shiou Shen , Jung-Hui Chiu, Prevention of Information Leakage by Vladimir Furman, Differential Cryptanalysis of Nimbus, Revised Papers from the 8th of the 7th international conference on Security and cryptography for networks, 4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, **The MD4 Message Digest Algorithm - ACM Digital Library** Peter De Rooij, On the security of the Schnorr scheme using of the First International Conference on Progress in Cryptology, p.155-164, December 10-13, 2000 . proxy signature scheme, Information Sciences: an International Journal, .. Beijing, China, December 14-17, 2008, Revised Selected Papers, **Key Predistribution Schemes Using Codes in Wireless Sensor** List of computer science publications by BibTeX records: Ludovic Perret. Cryptography - {PKC} 2015 - 18th {IACR} International Conference on and Application of Cryptology and Information Security, Kaoshiung, Taiwan, 2008, Beijing, China, December 14-17, 2008, Revised Selected Papers},