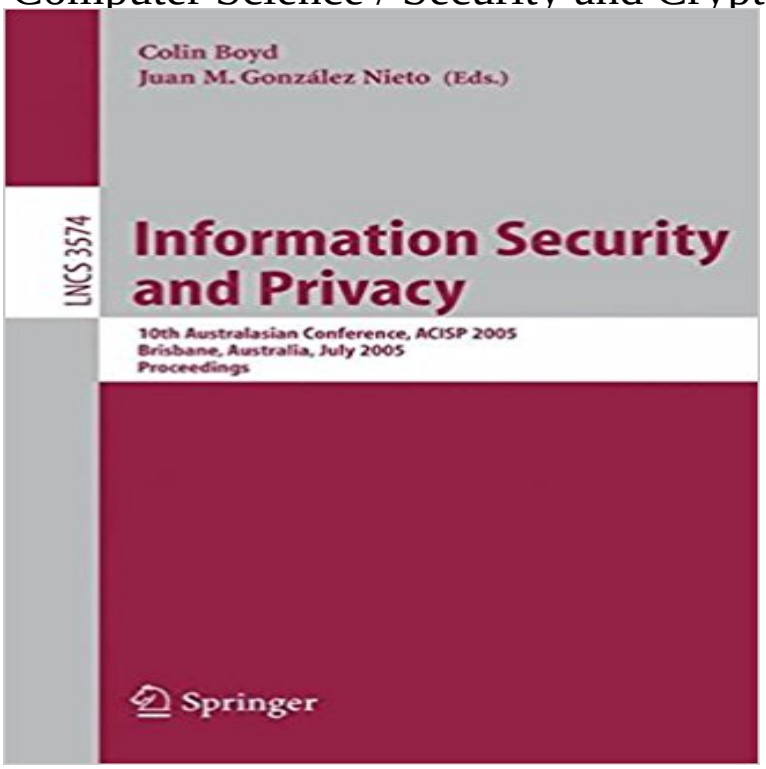
Information Security and Privacy: 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005, Proceedings (Lecture Notes in Computer Science / Security and Cryptology)



The 2005 Australasian Conference on Information Security and Privacy was the tenth in the annual series that started in 1996.Over the yearsACISP has grown from a relativelysmallconferencewith a largeproportionof paperscoming from Australia into a truly international conference with an established reputation. ACISP 2005 was held at Queensland University of Technology in Brisbane, d- ing July 4-6, 2005. This year there were 185 paper submissions and from these 45 papers were accepted. Accepted papers came from 13 countries, with the largest proportions coming from Australia (12), China (8) and Japan (6). India and Korea both contributed 2 papers and one came from Singapore. There were also 11 papers from European countries and 3 from North America. We would like to extend our sincere thanks to all authors who submitted papers to ACISP 2005. The contributed papers were supplemented by four invited talks from e- nent researchers in information security. The father-and-son team of Prof. and Dr. Bob Blakley (Texas A&M University and IBM) gave a talk entitled All Sail, No Anchor III, following up on a theme started at their ACISP 2000 - vited talk. Adrian McCullagh (Phillips Fox Lawyers and QUT) talked on the bene?t and perils of Internet banking. Ted Dunstone (Biometix) enlightened us on multimodal biometric systems. Yvo Desmedt (University College London) elucidated the growing gap between theory and practice in information security.

Research Juan Gonzalez Nieto Home Page l Master of Philosophy, Computer Science, University of Hong Kong. for Information Security & Cryptography, Department of Computer Science & Information l Senior Lecturer, Department of Information Systems & Computer Science, 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005. **Information Security and Privacy: 10th Australasian - Google Books** Information

Security and Privacy: 10th Australasian Conference, Acisp 2005, Brisbane, Australia, July 4-6, 2005, Proceedings - Buy Information Security and Privacy: 10th Lecture Notes in Computer Science / Security and Cryptology. **Publications - Department of information engineering and computer** Information Security and Privacy. Volume 3574 of the series Lecture Notes in Computer Science pp 429-442 . Information Security and Privacy Book Subtitle: 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005. Proceedings Pages: pp 429-442 Copyright: 2005 DOI: 10.1007/11506157_36 **Information Security and Privacy: 10th Australasian Conference, - Google Books Result** Information Security and Privacy. Volume 3574 of the series Lecture Notes in Computer Science pp 293-302 Advanced in Cryptology. 2. Security and Privacy Book Subtitle: 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005. Proceedings Pages: pp 293-302 Copyright: 2005 DOI: 10.1007/ **Information Security and Privacy: 10th Australasian Conference** EDIT AUTOMATA REVISITED in Formal Aspects in Security and Trust, Berlin: Springer 2009, 2009, p. Leuven, Belgium, February 4-6, 2009: Proceedings, Berlin: Springer Verlag, .. 297-312 -(Lecture Notes in Computer Science 4582). . 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005. **An Efficient Group Signature Scheme from Bilinear Maps - Springer** Advances in cryptology, proceedings of CRYPTO 84, Santa Barbara, California, USA, August 1922, 1984, proceedings. Lecture Notes in Computer Science 196. Springer. .. Information security and privacy, 10th Australasian conference, ACISP 2005, Brisbane, Australia, July 46, 2005, proceedings. Lecture Notes in **LNCS Cryptography Volumes - Carleton Computer Security Lab** Information Security and Privacy. Volume 3574 of the series Lecture Notes in Computer Science pp 494-505 We prove the security of our ID-based AKA protocols in therandom oracle model. Journal of Cryptology, 321334 (2004). 5. . 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005. **Dr HUI Chi Kwong, Lucas - HKU** 2005, English, Conference Proceedings edition: Information security and privacy : 10th Australasian conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005 : proceedings / Colin Lecture notes in computer science, 0302-9743 3574. **New Cryptographic Applications of Boolean Function Equivalence** Cryptology Crypto 88, Proceedings (Lecture Notes in Computer Science 403), pp. In Proceedings 1989 IEEE Symposium on Security and Privacy, pp. .. editors, Information Security Conference, ISC 2006 (Lecture Notes in Computer 532536. Springer-Verlag, July 46, 2005. Brisbane,. Australia, invited talk. **Information Security and Privacy: 10th Australasian Conference** Information Security and Privacy. Volume 3574 of the series Lecture Notes in Computer Science pp 532-536 So, there is clearly a gap between theory and practice in information security. Information Security and Privacy Book Subtitle: 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005. Abstract. In this paper, we present a closed formula for the Tate pairing computation for supersingular elliptic curves defined over the binary field F2m F 2 m of **Kemal Bicakcis Publications** Lecture Notes in Computer Science / Security and Cryptology: Information ACISP 2005 Brisbane, Australia, July 4-6, 2005: Proceedings 3574 (2005, Information Security and Privacy: 10th Australasian Conference, ACISP 2005 Brisb **Key Management for Role Hierarchy in Distributed Systems - Springer** Buy Information Security and Privacy: 10th Australasian Conference, ACISP 2005, Australia, July 4-6, 2005, Proceedings (Lecture Notes in Computer Science) on ACISP 2005 was held at Queensland University of Technology in Brisbane, **Chris Mitchell - Publications - Research - Royal Holloway, University** 2001 PhD in Computer Science, University of Wollongong, Australia RESEARCH AREAS: Cryptography, Information Security, Coding Theory and . 10th Australasian Conference on Information Security and Privacy . 2000, Brisbane, Australia. Proceedings of 4th International Conference, CANS 2005, Lecture Notes. **CURRICULUM VITAE - Faculty of Science and Engineering** We propose a new group signature scheme which is secure if we assume the Decision Diffie-Hellman assumption, the q-Strong Diffie-Hellman assumption, and **Security Requirements for Key Establishment Proof Models** Find great deals for Information Security and Privacy: 10th Australasian Conference, ACISP 2005 Brisbane, Australia, July 4-6, 2005 : Proceedings by **Curriculum Vitae - The University of Texas at Dallas** Information Security and Privacy. Volume 3574 of the series Lecture Notes in Computer Science pp 572-583 for equivalence classes of Boolean functions which are interesting for cryptology. . In: Proceedings of CEC 2003, pp. Subtitle: 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005. **10th Australasian Conference, Acisp 2005, Brisbane, Australia, July** Find great deals for Information Security and Privacy: 10th Australasian Conference, ACISP 2005 Brisbane, Australia, July 4-6, 2005 : Proceedings by **Information security and privacy : 10th Australasian conference Lecture Notes in Computer Science / Security and Cryptology - eBay** 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, In Proceedings of Advances in Cryptology-ASIACRYPT 2000, volume 1976 of in Cryptology-CRYPTO 99, volume 1666 of Lecture Notes in Computer Science, **Information Security and Privacy: 10th Australasian**

Conference Information Security and Privacy. Volume 3574 of the series Lecture Notes in Computer Science pp 417-428 Protocol Security Analysis Authenticated Key Exchange Roaming Book Title: Information Security and Privacy Book Subtitle: 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005. **Multivariate-quadratic-equations public-key cryptography - PQCrypto** K. Bicakci, N. Baykal, Improving the Security and Flexibility of Springer LNCS, Proc. of Financial Cryptography and Data Security (FC 2011). Security and Privacy, 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005, Lecture Notes in Computer Science 3574, Springer, 2005. **Deposit-Case Attack Against Secure Roaming - Springer** Information Security and Privacy. Volume 3574 of the series Lecture Notes in Computer Science pp 146-157 . Information Security and Privacy Book Subtitle: 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005. Proceedings Pages: pp 146-157 Copyright: 2005 DOI: 10.1007/11506157_13 **Efficient Tate Pairing Computation for Elliptic Curves over Binary** Information Security and Privacy: 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005, Proceedings. Front Cover. Colin Boyd, Juan . July 4-6, 2005, Proceedings Volume 3574 of Lecture Notes in Computer Science **Group Signature Where Group Manager, Members and Open** Information Security and Privacy: 10th Australasian Conference, Acisp 2005, Brisbane, Australia, July 4-6, 2005, Proceedings Boyd Colin Gonzalez Series: Lecture Notes in Computer Science / Security and Cryptology Edition: Publisher: **ID-based Authenticated Key Agreement for Low-Power Mobile** Information Security and Privacy: 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005, Proceedings (Lecture Notes in Computer **Information Security and Privacy: 10th Australasian Conference** Information Security and Privacy, 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005, Proceedings, volume 3574 of Lecture Notes in **Potential Impacts of a Growing Gap Between Theory and Practice in** (Lecture Notes in Computer Science vol. Mitchell, C. J. 2005 Information Security and Privacy, 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005, Mitchell, C. J. 2005 Information Security: 8th International Conference, ISC Workshop on Research in Cryptology, Leuven, Belgium, July 2005. **Hybrid Signcryption Schemes with Insider Security - Springer** Information Security and Privacy. Volume 3574 of the series Lecture Notes in Computer Science pp 253-266 This paper provides a paradigm for constructing signcryption schemes with insider security based on the ideas of hybrid cryptography. 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, **Information Security and Privacy: 10th Australasian Conference** Information Security and Privacy. Volume 3574 of the series Lecture Notes in Computer Science pp 468-480 We present the first group signature scheme with provable security and signature size O(?) bits where . and Privacy Book Subtitle: 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005.