AFRICACRYPT 2008

Casablanca, Morocco, June 11-14, 2008

http://www.africacrypt.org/index_en.htm

Invited Speakers :

T. El Gamal, J. Stern, B. Schneier, A. Dent

Accepted papers

1. Yet Another Attack on Vest Pascal, Delaunay, Antoine Joux
2. An Attribute-Based Broadcast Encryption Scheme, David Lubicz, Thomas Sirvent
3. Lower Bounds for Subset Cover Based Broadcast Encryption, Per Austrin, Gunnar Kreitz
4. Robust Threshold Schemes Based on the Chinese Remainder Theorem, Kamer Kaya, Ali Aydin Selcuk
5. An (Almost) Constant-Effort Solution-Verification Proof-of-Work Protocol based on Merkle Trees, Fabien Coelho
6. Improving integral attacks against Rijndael-256 up to 9 rounds, Samuel Galice, Marine Minier
7. Efficient Multiplication in F_{3^m}, Murat Cenk, Ferruh Ozbudak
8. Chosen IV Statistical Analysis for Key Recovery Attacks on Stream Ciphers, Simon Fischer, Shahram Khazaei, Willi Meier
9. An Authentication Protocol with Encrypted Biometric Data, Julien Bringer, Hervé Chabanne
10. Weaknesses in a Recent Ultralightweight RFID Authentication Protocol, Paolo D'Arco, Alfredo De Santis
11. A Proof of Security in $O(2^n)$ for the Benes Scheme, Jacques Patarin
12. Correlated Keystreams in MOUSTIQUE Tor, E. Bjorstad, Emilia Kasper, Christian Rechberger, Vincent Rijmen, Matt Robshaw, Gautham Sekar
13. Differential Cryptanalysis of PRESENT, Meiqin Wang
14. New Definition of Density on Knapsack Cryptosystems, Noboru Kunihiro
15. Cryptanalysis of the TRMS Cryptosystem of PKC'05 Luk Bettale, Jean-Charles Faugère, Ludovic Perret
16. Another generalization of Wiener's attack on RSA, Abderrahmane Nitaj
17. Stream Ciphers using a Random Update Function : Study of the Entropy of the Inner State, Andrea Röck
18. On compressible pairings and their computation, Michael Naehrig, Paulo S. L. M. Barreto, Peter Schwabe
19. Password Recovery on Challenge and Response : Impossible Differential Attack on Hash Function, Yu Sasaki, Lei Wang, Kazuo Ohta, Noboru Kunihiro
20. An Adaptation of the NICE Cryptosystem to Real Quadratic Orders, M. J. Jacobson, Jr, R. Scheidler, D. Weimer
21. Implementation of the AES-128 on Virtex-5 FPGAs P. Bulens, F.-X. Standaert, J.-J. Quisquater, P. Pellegrin, G. Rouvroy
22. Analysis of Grain's Initialization Algorithm, Christophe De Canniere, Özgül Küçük, Bart Preneel
23. Twisted Edwards Curves Daniel, J. Bernstein, Peter Birkner, Tanja Lange, Christiane Peters
24. Authenticated Encryption Mode for Beyond the Birthday Bound Security, Tetsu Iwata
25. How (Not) to Efficiently Dither Blockcipher-Based Hash Functions ?, Jean-Philippe Aumasson and Raphael C.-W. Phan