

Table of Contents

Invited Papers

Abstract Models of Computation in Cryptography <i>U. Maurer</i>	1
Pairing-Based Cryptography at High Security Levels <i>N. Kobitz, A. Menezes</i>	13
Improved Decoding of Interleaved AG Codes <i>A. Brown, L. Minder, A. Shokrollahi</i>	37

Coding Theory

Performance Improvement of Turbo Code Based on the Extrinsic Information Transition Characteristics <i>W.T. Kim, S.H. Kang, E.K. Joo</i>	47
A Trellis-Based Bound on $(2, 1)$ -Separating Codes <i>H.G. Schaathun, G.D. Cohen</i>	59
Tessellation Based Multiple Description Coding <i>C. Cai, J. Chen</i>	68
Exploiting Coding Theory for Collision Attacks on SHA-1 <i>N. Pramstaller, C. Rechberger, V. Rijmen</i>	78

Signatures and Signcryption

Hash Based Digital Signature Schemes <i>C. Dods, N.P. Smart, M. Stam</i>	96
A General Construction for Simultaneous Signing and Encrypting <i>J. Malone-Lee</i>	116
Non-interactive Designated Verifier Proofs and Undeniable Signatures <i>C. Kudla, K.G. Paterson</i>	136

Symmetric Cryptography

Partial Key Recovery Attacks on XCBC, TMAC and OMAC

C.J. Mitchell 155

Domain Expansion of MACs: Alternative Uses of the FIL-MAC

U. Maurer, J. Sjödin 168

Normality of Vectorial Functions

A. Braeken, C. Wolf, B. Preneel 186

Related-Key Differential Attacks on Cobra-H64 and Cobra-H128

C. Lee, J. Kim, J. Sung, S. Hong, S. Lee, D. Moon 201

Side Channels

The Physically Observable Security of Signature Schemes

A.W. Dent, J. Malone-Lee 220

On the Automatic Construction of Indistinguishable Operations

M. Barbosa, D. Page 233

Efficient Countermeasures for Thwarting the SCA Attacks on the Frobenius Based Methods

M. Hedabou 248

Algebraic Cryptanalysis

Complexity Estimates for the F_4 Attack on the Perturbed Matsumoto-Imai Cryptosystem

J. Ding, J.E. Gower, D. Schmidt, C. Wolf, Z. Yin 262

An Algebraic Framework for Cipher Embeddings

C. Cid, S. Murphy, M.J.B. Robshaw 278

Probabilistic Algebraic Attacks

A. Braeken, B. Preneel 290

Information Theoretic Applications

Unconditionally Secure Information Authentication in Presence of Erasures <i>G. Jakimoski</i>	304
Generalized Strong Extractors and Deterministic Privacy Amplification <i>R. König, U. Maurer</i>	322
On Threshold Self-healing Key Distribution Schemes <i>G. Sáez</i>	340

Number Theoretic Foundations

Concrete Security of the Blum-Blum-Shub Pseudorandom Generator <i>A. Sidorenko, B. Schoenmakers</i>	355
The Equivalence Between the DHP and DLP for Elliptic Curves Used in Practical Applications, Revisited <i>K. Bentahar</i>	376
Pairings on Elliptic Curves over Finite Commutative Rings <i>S.D. Galbraith, J.F. McKee</i>	392

Public Key and ID-Based Encryption Schemes

A Key Encapsulation Mechanism for NTRU <i>M. Stam</i>	410
Efficient Identity-Based Key Encapsulation to Multiple Parties <i>M. Barbosa, P. Farshim</i>	428
Security Proof of Sakai-Kasahara's Identity-Based Encryption Scheme <i>L. Chen, Z. Cheng</i>	442
Author Index	461