

Table of Contents

Bits and Booleans

| | |
|---|---|
| Semi-bent Functions from Oval Polynomials | 1 |
| <i>Sihem Mesnager</i> | |

| | |
|--|----|
| Efficient Generation of Elementary Sequences | 16 |
| <i>David Gardner, Ana Sălăgean, and Raphael C.-W. Phan</i> | |

Homomorphic Encryption

| | |
|---|----|
| On the Homomorphic Computation of Symmetric Cryptographic Primitives | 28 |
| <i>Silvia Mella and Ruggero Susella</i> | |

| | |
|---|----|
| Improved Security for a Ring-Based Fully Homomorphic Encryption Scheme | 45 |
| <i>Joppe W. Bos, Kristin Lauter, Jake Loftus, and Michael Naehrig</i> | |

| | |
|--|----|
| On the Relationship between Functional Encryption, Obfuscation, and Fully Homomorphic Encryption | 65 |
| <i>Joël Alwen, Manuel Barbosa, Pooya Farshim, Rosario Gennaro, S. Dov Gordon, Stefano Tessaro, and David A. Wilson</i> | |

Codes and Applications

| | |
|---|----|
| On Minimal and Quasi-minimal Linear Codes | 85 |
| <i>G rard D. Cohen, Sihem Mesnager, and Alain Patey</i> | |
| A Code-Based Undeniable Signature Scheme | 99 |
| <i>Carlos Aguilar-Melchor, Slim Bettaieb, Philippe Gaborit, and Julien Schrek</i> | |

Cryptanalysis

| | |
|--|-----|
| Filtered Nonlinear Cryptanalysis of Reduced-Round Serpent, and the Wrong-Key Randomization Hypothesis | 120 |
| <i>James McLaughlin and John A. Clark</i> | |

| | |
|---|-----|
| Differential Cryptanalysis of Keccak Variants | 141 |
| <i>Stefan Kölbl, Florian Mendel, Tomislav Nad, and Martin Schläffer</i> | |

| | |
|--|-----|
| Recovering Private Keys Generated with Weak PRNGs | 158 |
| <i>Pierre-Alain Fouque, Mehdi Tibouchi, and Jean-Christophe Zapalowicz</i> | |

Protecting against Leakage

| | |
|---|-----|
| A Leakage-Resilient Pairing-Based Variant of the Schnorr Signature Scheme | 173 |
| <i>David Galindo and Srinivas Vivek</i> | |

| | |
|--|-----|
| High-Order Masking by Using Coding Theory and Its Application to AES | 193 |
| <i>Guilhem Castagnos, Soline Renner, and Gilles Zémor</i> | |

Hash Functions

| | |
|--|-----|
| Hashing Mode Using a Lightweight Blockcipher | 213 |
| <i>Hidekazu Kuwakado and Shoichi Hirose</i> | |

| | |
|--|-----|
| Indifferentiability of Double Length Compression Functions | 232 |
| <i>Bart Mennink</i> | |

| | |
|---|-----|
| Security Amplification against Meet-in-the-Middle Attacks Using Whitening | 252 |
| <i>Pierre-Alain Fouque and Pierre Karpman</i> | |

Key Issues

| | |
|---|-----|
| Secure Key Management in the Cloud | 270 |
| <i>Ivan Damgård, Thomas P. Jakobsen, Jesper Buus Nielsen, and Jakob I. Pagter</i> | |

| | |
|---|-----|
| Estimating Key Sizes for High Dimensional Lattice-Based Systems | 290 |
| <i>Joop van de Pol and Nigel P. Smart</i> | |

Public Key Primitives

| | |
|---|-----|
| Sub-linear Blind Ring Signatures without Random Oracles | 304 |
| <i>Essam M. Ghadafi</i> | |

| | |
|---|-----|
| Constructions of Signcryption in the Multi-user Setting from Identity-Based Encryption | 324 |
| <i>Rintaro Nakano and Junji Shikata</i> | |
| Anonymous Constant-Size Ciphertext HIBE from Asymmetric Pairings | 344 |
| <i>Somindu C. Ramanna and Palash Sarkar</i> | |
| Author Index | 365 |