

Table of Contents

Invited Paper

- Can a Program Reverse-Engineer Itself? 1
Antoine Amarilli, David Naccache, Pablo Rauzy, and Emil Simion

Homomorphic Encryption

- Improved Key Generation for Gentry's Fully Homomorphic Encryption Scheme 10
Peter Scholl and Nigel P. Smart
- On Constructing Homomorphic Encryption Schemes from Coding Theory 23
Frederik Armknecht, Daniel Augot, Ludovic Perret, and Ahmad-Reza Sadeghi

Coding Theory I

- Generalised Complementary Arrays 41
Matthew G. Parker and Constanza Riera
- Binary Kloosterman Sums with Value 4 61
Jean-Pierre Flori, Sihem Mesnager, and Gérard Cohen
- On the Triple-Error-Correcting Cyclic Codes with Zero Set $\{1, 2^i + 1, 2^j + 1\}$ 79
Vincent Herbert and Sumanta Sarkar

Knowledge Proof

- A Secure and Efficient Proof of Integer in an Interval Range 97
Kun Peng
- Bit Commitment in the Bounded Storage Model: Tight Bound and Simple Optimal Construction 112
Junji Shikata and Daisuke Yamanaka

Cryptographic Functions

- Self-correctors for Cryptographic Modules 132
Go Yamamoto and Tetsutaro Kobayashi

The Symbiosis between Collision and Preimage Resistance	152
<i>Elena Andreeva and Martijn Stam</i>	

Enhanced Count of Balanced Symmetric Functions and Balanced Alternating Functions	172
<i>Marc Mouffron and Guillaume Vergne</i>	

Public Key Cryptosystem

Ciphertext-Policy Delegatable Hidden Vector Encryption and Its Application to Searchable Encryption in Multi-user Setting.....	190
<i>Mitsuhiro Hattori, Takato Hirano, Takashi Ito, Nori Matsuda, Takumi Mori, Yusuke Sakai, and Kazuo Ohta</i>	

Constructing Secure Hybrid Encryption from Key Encapsulation Mechanism with Authenticity	210
<i>Yuki Shibuya and Junji Shikata</i>	

Coding Theory II

A Note on the Dual Codes of Module Skew Codes.....	230
<i>Delphine Boucher and Felix Ulmer</i>	

Ensuring Message Embedding in Wet Paper Steganography	244
<i>Daniel Augot, Morgan Barbier, and Caroline Fontaine</i>	

On the Stability of m-Sequences	259
<i>Alex J. Burrage, Ana Sălăgean, and Raphael C.-W. Phan</i>	

Pairing and ECC Implementation

Parallelizing the Weil and Tate Pairings	275
<i>Diego F. Aranha, Edward Knapp, Alfred Menezes, and Francisco Rodríguez-Henríquez</i>	

On the Efficient Implementation of Pairing-Based Protocols	296
<i>Michael Scott</i>	

Efficient Pairing Computation on Ordinary Elliptic Curves of Embedding Degree 1 and 2	309
<i>Xusheng Zhang and Dongdai Lin</i>	

Improved Precomputation Scheme for Scalar Multiplication on Elliptic Curves	327
<i>Duc-Phong Le and Chik How Tan</i>	

Security Analysis

Breaking an Identity-Based Encryption Scheme Based on DHIES	344
<i>Martin R. Albrecht and Kenneth G. Paterson</i>	
Analysis of the SSH Key Exchange Protocol	356
<i>Stephen C. Williams</i>	
Cryptanalysis of the Light-Weight Cipher A2U2	375
<i>Mohamed Ahmed Abdelraheem, Julia Borghoff, Erik Zenner, and Mathieu David</i>	

Symmetric Key Cryptosystem

Building Blockcipher from Tweakable Blockcipher: Extending FSE 2009 Proposal	391
<i>Kazuhiko Minematsu and Tetsu Iwata</i>	
Security of Hash-then-CBC Key Wrapping Revisited	413
<i>Yasushi Osaki and Tetsu Iwata</i>	

Cryptographic Protocols

Block-Wise P-Signatures and Non-interactive Anonymous Credentials with Efficient Attributes	431
<i>Malika Izabachène, Benoît Libert, and Damien Vergnaud</i>	
On Forward Secrecy in One-Round Key Exchange	451
<i>Colin Boyd and Juan González Nieto</i>	
Designated Confirmer Signatures with Unified Verification	469
<i>Guilin Wang, Fubiao Xia, and Yunlei Zhao</i>	
Author Index	497