

Table of Contents

Algorithms for Pairing Computation

On Efficient Pairings on Elliptic Curves over Extension Fields	1
<i>Xusheng Zhang, Kunpeng Wang, and Dongdai Lin</i>	
Factor-4 and 6 (De)Compression for Values of Pairings Using Trace Maps	19
<i>Tomoko Yonemura, Taichi Isogai, Hirofumi Muratani, and Yoshikazu Hanatani</i>	
An Improved Twisted Ate Pairing over KSS Curves with $k = 18$	35
<i>Shan Chen, Kunpeng Wang, and Dongdai Lin</i>	

Security Models for Encryption

Controlled Joining on Encrypted Relational Database	46
<i>Jun Furukawa and Toshiyuki Isshiki</i>	
Stronger Security Model for Public-Key Encryption with Equality Test	65
<i>Yao Lu, Rui Zhang, and Dongdai Lin</i>	

Functional Encryption

Forward-Secure Hierarchical Predicate Encryption	83
<i>Juan Manuel González Nieto, Mark Manulis, and Dongdong Sun</i>	
Fully Secure Hidden Vector Encryption	102
<i>Angelo De Caro, Vincenzo Iovino, and Giuseppe Persiano</i>	
Shorter IBE and Signatures via Asymmetric Pairings	122
<i>Jie Chen, Hoon Wei Lim, San Ling, Huaxiong Wang, and Hoeteck Wee</i>	

Implementations in Hardware and Software

Core Based Architecture to Speed Up Optimal Ate Pairing on FPGA Platform	141
<i>Santosh Ghosh, Ingrid Verbauwhede, and Dipanwita Roychowdhury</i>	
Faster Pairing Coprocessor Architecture	160
<i>Gavin Xiaozu Yao, Junfeng Fan, Ray C.C. Cheung, and Ingrid Verbauwhede</i>	

Implementing Pairings at the 192-Bit Security Level	177
<i>Diego F. Aranha, Laura Fuentes-Castañeda, Edward Knapp, Alfred Menezes, and Francisco Rodríguez-Henríquez</i>	
Industry Track	
Improved Broadcast Encryption Scheme with Constant-Size Ciphertext	196
<i>Renaud Dubois, Aurore Guillevic, and Marine Sengelin Le Breton</i>	
Affine Pairings on ARM	203
<i>Tolga Acar, Kristin Lauter, Michael Naehrig, and Daniel Shumow</i>	
On the Implementation of a Pairing-Based Cryptographic Protocol in a Constrained Device	210
<i>Sébastien Canard, Nicolas Desmoulins, Julien Devigne, and Jacques Traoré</i>	
Properties of Pairings	
The Tate-Lichtenbaum Pairing on a Hyperelliptic Curve via Hyperelliptic Nets	218
<i>Yukihiro Uchida and Shigenori Uchiyama</i>	
Genus 2 Hyperelliptic Curve Families with Explicit Jacobian Order Evaluation and Pairing-Friendly Constructions	234
<i>Aurore Guillevic and Damien Vergnaud</i>	
Tate Pairing Computation on Jacobi's Elliptic Curves	254
<i>Sylvain Duquesne and Emmanuel Fouotsa</i>	
Signature Schemes and Applications	
Group Signatures with Message-Dependent Opening	270
<i>Yusuke Sakai, Keita Emura, Goichiro Hanaoka, Yutaka Kawai, Takahiro Matsuda, and Kazumasa Omote</i>	
Short Pairing-Efficient Threshold-Attribute-Based Signature	295
<i>Martin Gagné, Shivaramakrishnan Narayan, and Reihaneh Safavi-Naini</i>	
Divisible E-Cash in the Standard Model	314
<i>Malika Izabachène and Benoît Libert</i>	
Author Index	333