

Table of Contents

Software and System Security

Secure Log Transfer by Replacing a Library in a Virtual Machine	1
<i>Masaya Sato and Toshihiro Yamauchi</i>	
Static Integer Overflow Vulnerability Detection in Windows Binary	19
<i>Yi Deng, Yang Zhang, Liang Cheng, and Xiaoshan Sun</i>	
Solving Google's Continuous Audio CAPTCHA with HMM-Based Automatic Speech Recognition	36
<i>Shotaro Sano, Takuma Otsuka, and Hiroshi G. Okuno</i>	
Constructions of Almost Secure Frameproof Codes Based on Small-Bias Probability Spaces	53
<i>José Moreira, Marcel Fernández, and Grigory Kabatiansky</i>	

Cryptanalysis

Differential Power Analysis of MAC-Keccak at Any Key-Length	68
<i>Mostafa Taha and Patrick Schaumont</i>	
Generic State-Recovery and Forgery Attacks on ChopMD-MAC and on NMAC/HMAC	83
<i>Yusuke Naito, Yu Sasaki, Lei Wang, and Kan Yasuda</i>	
New Property of Diffusion Switching Mechanism on CLEFIA and Its Application to DFA	99
<i>Yosuke Todo and Yu Sasaki</i>	
Improvement of Faugère <i>et al.</i> 's Method to Solve ECDLP	115
<i>Yun-Ju Huang, Christophe Petit, Naoyuki Shinohara, and Tsuyoshi Takagi</i>	

Privacy and Cloud Computing

Statistics on Encrypted Cloud Data	133
<i>Fu-Kuo Tseng, Yung-Hsiang Liu, Rong-Jaye Chen, and Bao-Shuh Paul Lin</i>	
Toward Practical Searchable Symmetric Encryption	151
<i>Wakaha Ogata, Keita Koiwa, Akira Kanaoka, and Shin'ichiro Matsuo</i>	

Unconditionally Secure Oblivious Transfer from Real Network Behavior	168
<i>Paolo Palmieri and Olivier Pereira</i>	
Cryptographically-Secure and Efficient Remote Cancelable Biometrics Based on Public-Key Homomorphic Encryption	183
<i>Takato Hirano, Mitsuhiro Hattori, Takashi Ito, and Nori Matsuda</i>	
Public Key Cryptosystems	
Efficient Algorithm for Tate Pairing of Composite Order	201
<i>Yutaro Kiyomura and Tsuyoshi Takagi</i>	
How to Factor N_1 and N_2 When $p_1 = p_2 \bmod 2^t$	217
<i>Kaoru Kurosawa and Takuma Ueda</i>	
Achieving Chosen Ciphertext Security from Detectable Public Key Encryption Efficiently via Hybrid Encryption	226
<i>Takahiro Matsuda and Goichiro Hanaoka</i>	
Cryptanalysis of the Quaternion Rainbow	244
<i>Yasufumi Hashimoto</i>	
Security Protocols	
On Cheater Identifiable Secret Sharing Schemes Secure against Rushing Adversary	258
<i>Rui Xu, Kirill Morozov, and Tsuyoshi Takagi</i>	
One-Round Authenticated Key Exchange without Implementation Trick	272
<i>Kazuki Yoneyama</i>	
Attacks to the Proxy Re-Encryption Schemes from IWSEC2011	290
<i>Toshiyuki Isshiki, Manh Ha Nguyen, and Keisuke Tanaka</i>	
Game-Theoretic Security for Bit Commitment	303
<i>Haruna Higo, Keisuke Tanaka, and Kenji Yasunaga</i>	
Author Index	319