

Table of Contents

Invited Talk

Cut-&-Paste Attacks with JAVA	1
<i>Serge Lefranc and David Naccache</i>	

Digital Signatures

Provably Secure Encrypt-then-Sign Composition in Hybrid Signcryption ...	16
<i>Ik Rae Jeong, Hee Yun Jeong, Hyun Sook Rhee, Dong Hoon Lee, and Jong In Lim</i>	
New DSA-Verifiable Signcryption Schemes	35
<i>Jun-Bum Shin, Kwangsu Lee, and Kyungah Shim</i>	
Convertible Group Undeniable Signatures	48
<i>Yuh-Dauh Lyuu and Ming-Luen Wu</i>	
An Efficient Fail-Stop Signature Scheme Based on Factorization	62
<i>Willy Susilo and Rei Safavi-Naini</i>	
On the Security of the Li-Hwang-Lee-Tsai Threshold Group Signature Scheme	75
<i>Guilin Wang</i>	

Internet Security

System Specification Based Network Modeling for Survivability Testing Simulation	90
<i>HyungJong Kim</i>	
A Risk-Sensitive Intrusion Detection Model	107
<i>Hai Jin, Jianhua Sun, Hao Chen, and Zongfen Han</i>	
Applet Verification Strategies for RAM-Constrained Devices	118
<i>Nils Maltesson, David Naccache, Elena Trichina, and Christophe Tymen</i>	

Block/Stream Ciphers

Sliding Properties of the DES Key Schedule and Potential Extensions to the Slide Attacks	138
<i>Raphael Chung-Wei Phan and Soichi Furuya</i>	

Consistent Differential Patterns of Rijndael	149
<i>Beomsik Song and Jennifer Seberry</i>	
Hardware Design and Analysis of Block Cipher Components	164
<i>Lu Xiao and Howard M. Heys</i>	
Higher Order Correlation Attacks, XL Algorithm and Cryptanalysis of Toyocrypt	182
<i>Nicolas T. Courtois</i>	

Stream Ciphers & Other Primitives

On the Efficiency of the Clock Control Guessing Attack	200
<i>Erik Zenner</i>	
Balanced Shrinking Generators	213
<i>Se Ah Choi and Kyeongcheol Yang</i>	
On the Universal Hash Functions in Luby-Rackoff Cipher	226
<i>Tetsu Iwata and Kaoru Kurosawa</i>	
Threshold MACs	237
<i>Keith M. Martin, Josef Pieprzyk, Rei Safavi-Naini, Huaxiong Wang, and Peter R. Wild</i>	
Ideal Threshold Schemes from MDS Codes	253
<i>Josef Pieprzyk and Xian-Mo Zhang</i>	

Efficient Implementations

New Frobenius Expansions for Elliptic Curves with Efficient Endomorphisms	264
<i>Tae-Jun Park, Mun-Kyu Lee, and Kunsoo Park</i>	
Efficient Computations of the Tate Pairing for the Large MOV Degrees ...	283
<i>Tetsuya Izu and Tsuyoshi Takagi</i>	
Improved Techniques for Fast Exponentiation	298
<i>Bodo Möller</i>	
Efficient Hardware Multiplicative Inverters	313
<i>Hyun-Gyu Kim and Hyeong-Cheol Oh</i>	

Side-Channel Attacks

Ways to Enhance Differential Power Analysis	327
<i>Régis Bevan and Erik Knudsen</i>	

A Simple Power-Analysis (SPA) Attack on Implementations of the AES Key Expansion	343
<i>Stefan Mangard</i>	
A Reject Timing Attack on an IND-CCA2 Public-Key Cryptosystem	359
<i>Kouichi Sakurai and Tsuyoshi Takagi</i>	
Hardware Fault Attack on RSA with CRT Revisited	374
<i>Sung-Ming Yen, Sangjae Moon, and Jae-Cheol Ha</i>	

Cryptographic Protocols I

Receipt-Free Electronic Voting Scheme with a Tamper-Resistant Randomizer	389
<i>Byoungcheon Lee and Kwangjo Kim</i>	
Non-interactive Auction Scheme with Strong Privacy	407
<i>Kun Peng, Colin Boyd, Ed Dawson, and Kapali Viswanathan</i>	
An Anonymous Buyer-Seller Watermarking Protocol with Anonymity Control	421
<i>Hak Soo Ju, Hyun Jeong Kim, Dong Hoon Lee, and Jong In Lim</i>	
Speeding Up Secure Sessions Establishment on the Internet	433
<i>Yaron Sella</i>	

Cryptographic Protocols II

On Fairness in Exchange Protocols	451
<i>Olivier Markowitch, Dieter Gollmann, and Steve Kremer</i>	
A Model for Embedding and Authorizing Digital Signatures in Printed Documents	465
<i>Jae-il Lee, Taekyoung Kwon, Sanghoon Song, and Jooseok Song</i>	
A Dynamic Group Key Distribution Scheme with Flexible User Join	478
<i>Hartono Kurnio, Luke McAven, Rei Safavi-Naini, and Huaxiong Wang</i>	
Efficient Multicast Key Management for Stateless Receivers	497
<i>Ju Hee Ki, Hyun Jeong Kim, Dong Hoon Lee, and Chang Seop Park</i>	

Biometrics

Fingerprint Verification System Involving Smart Card	510
<i>Younhee Gil, Daesung Moon, Sungbum Pan, and Yongwha Chung</i>	
A Fast Fingerprint Matching Algorithm Using Parzen Density Estimation	525
<i>Choonwoo Ryu and Hakil Kim</i>	

Author Index	535
--------------------	-----