

Table of Contents

Invited Talks

How to Steal a Botnet and What Can Happen When You Do.....	1
<i>Richard A. Kemmerer</i>	

A User-Mode-Kernel-Mode Co-operative Architecture for Trustable Computing.....	2
<i>Wenbo Mao</i>	

Cryptanalysis

Security Evaluation of a DPA-Resistant S-Box Based on the Fourier Transform	3
<i>Yang Li, Kazuo Sakiyama, Shinichi Kawamura, Yuichi Komano, and Kazuo Ohta</i>	

Security Analysis of the GF-NLFSR Structure and Four-Cell Block Cipher.....	17
<i>Wenling Wu, Lei Zhang, Liting Zhang, and Wentao Zhang</i>	

Algorithms and Implementations

The RAKAPOSHI Stream Cipher	32
<i>Carlos Cid, Shinsaku Kiyomoto, and Jun Kurihara</i>	

Design of Reliable and Secure Multipliers by Multilinear Arithmetic Codes	47
<i>Zhen Wang, Mark Karpovsky, Berk Sunar, and Ajay Joshi</i>	

Hardware/Software Co-design of Public-Key Cryptography for SSL Protocol Execution in Embedded Systems.....	63
<i>Manuel Koschuch, Johann Großschädl, Dan Page, Philipp Grabher, Matthias Hudler, and Michael Krüger</i>	

Public Key Cryptography

Online/Offline Ring Signature Scheme	80
<i>Joseph K. Liu, Man Ho Au, Willy Susilo, and Jianying Zhou</i>	

Policy-Controlled Signatures.....	91
<i>Pairat Thorncharoensri, Willy Susilo, and Yi Mu</i>	

Public Key Encryption without Random Oracle Made Truly Practical	107
<i>Puwen Wei, Xiaoyun Wang, and Yuliang Zheng</i>	

A Public-Key Traitor Tracing Scheme with an Optimal Transmission Rate	121
<i>Yi-Ruei Chen and Wen-Guey Tzeng</i>	

Security Applications

Computationally Secure Hierarchical Self-healing Key Distribution for Heterogeneous Wireless Sensor Networks	135
<i>Yanjiang Yang, Jianying Zhou, Robert H. Deng, and Feng Bao</i>	

Enabling Secure Secret Updating for Unidirectional Key Distribution in RFID-Enabled Supply Chains	150
<i>Shaoying Cai, Tieyan Li, Changshe Ma, Yingjiu Li, and Robert H. Deng</i>	

Biometric-Based Non-transferable Anonymous Credentials	165
<i>Marina Blanton and William M.P. Hudelson</i>	

Software Security

Secure Remote Execution of Sequential Computations	181
<i>Ghassan O. Karame, Mario Strasser, and Srdjan Čapkun</i>	

Architecture- and OS-Independent Binary-Level Dynamic Test Generation	198
<i>Gen Li, Kai Lu, Ying Zhang, Xicheng Lu, and Wei Zhang</i>	

System Security

Measuring Information Flow in Reactive Processes	211
<i>Chunyan Mu</i>	

Trusted Isolation Environment: An Attestation Architecture with Usage Control Model	226
<i>Anbang Ruan, Qingni Shen, Liang Gu, Li Wang, Lei Shi, Yahui Yang, and Zhong Chen</i>	

Denial-of-Service Attacks on Host-Based Generic Unpackers	241
<i>Limin Liu, Jiang Ming, Zhi Wang, Debin Gao, and Chunfu Jia</i>	

Network Security

Predictive Pattern Matching for Scalable Network Intrusion Detection	254
<i>Lucas Vespa, Mini Mathew, and Ning Weng</i>	

Deterministic Finite Automata Characterization for Memory-Based Pattern Matching	268
<i>Lucas Vespa and Ning Weng</i>	
A LoSS Based On-line Detection of Abnormal Traffic Using Dynamic Detection Threshold	283
<i>Zhengmin Xia, Songnian Lu, Jianhua Li, and Aixin Zhang</i>	
User-Assisted Host-Based Detection of Outbound Malware Traffic	293
<i>Huijun Xiong, Prateek Malhotra, Deian Stefan, Chehai Wu, and Danfeng Yao</i>	
Assessing Security Risk to a Network Using a Statistical Model of Attacker Community Competence	308
<i>Tomas Olsson</i>	

Short Papers I

Using the (Open) Solaris Service Management Facility as a Building Block for System Security	325
<i>Christoph Schuba</i>	
IntFinder: Automatically Detecting Integer Bugs in x86 Binary Program	336
<i>Ping Chen, Hao Han, Yi Wang, Xiaobin Shen, Xinchun Yin, Bing Mao, and Li Xie</i>	
A Comparative Study of Privacy Mechanisms and a Novel Privacy Mechanism	346
<i>Gunmeet Singh and Sarbjeet Singh</i>	

Database Security

Collusion-Resistant Protocol for Privacy-Preserving Distributed Association Rules Mining	359
<i>Xin-Jing Ge and Jian-Ming Zhu</i>	
GUC-Secure Join Operator in Distributed Relational Database	370
<i>Yuan Tian and Hao Zhang</i>	

Trust Management

TSM-Trust: A Time-Cognition Based Computational Model for Trust Dynamics	385
<i>Guangquan Xu, Zhiyong Feng, Xiaohong Li, Hutong Wu, Yongxin Yu, Shizhan Chen, and Guozheng Rao</i>	

Bring Efficient Connotation Expressible Policies to Trust Management	396
<i>Yan Zhang, Zhengde Zhai, and Dengguo Feng</i>	
A User Trust-Based Collaborative Filtering Recommendation Algorithm.....	411
<i>Fuzhi Zhang, Long Bai, and Feng Gao</i>	
 Applied Cryptography	
Fingerprinting Attack on the Tor Anonymity System	425
<i>Yi Shi and Kanta Matsuura</i>	
Proactive Verifiable Linear Integer Secret Sharing Scheme	439
<i>Chuangui Ma and Xiaofei Ding</i>	
A Multi-stage Secret Sharing Scheme Using All-or-Nothing Transform Approach	449
<i>Mitra Fatemi, Taraneh Eghlidos, and Mohammadreza Aref</i>	
Digital Audio Watermarking Technique Using Pseudo-Zernike Moments	459
<i>Xiangyang Wang, Tianxiao Ma, and Panpan Niu</i>	
 Short Papers II	
An Image Sanitizing Scheme Using Digital Watermarking	474
<i>Masatoshi Noguchi, Manabu Inuma, Rie Shigetomi, and Hideki Imai</i>	
Adaptive and Composable Oblivious Transfer Protocols	483
<i>Huafei Zhu and Feng Bao</i>	
Discrete-Log-Based Additively Homomorphic Encryption and Secure WSN Data Aggregation.....	493
<i>Licheng Wang, Lihua Wang, Yun Pan, Zonghua Zhang, and Yixian Yang</i>	
 Author Index	 503