

Phong Q. Nguyen · Jianying Zhou (Eds.)

# Information Security

20th International Conference, ISC 2017

Ho Chi Minh City, Vietnam, November 22–24, 2017

Proceedings

# Contents

## Symmetric Cryptography

Rate-One AE with Security Under RUP. . . . .	3
<i>Shoichi Hirose, Yu Sasaki, and Kan Yasuda</i>	
An Improved SAT-Based Guess-and-Determine Attack on the Alternating Step Generator . . . . .	21
<i>Oleg Zaikin and Stepan Kochemazov</i>	
Efficient Masking of ARX-Based Block Ciphers Using Carry-Save Addition on Boolean Shares . . . . .	39
<i>Daniel Dinu, Johann Großschädl, and Yann Le Corre</i>	
Improved Automatic Search Tool for Related-Key Differential Characteristics on Byte-Oriented Block Ciphers . . . . .	58
<i>Li Lin, Wenling Wu, and Yafei Zheng</i>	

## Post-quantum Cryptography

Choosing Parameters for the Subfield Lattice Attack Against Overstretched NTRU . . . . .	79
<i>Dung Hoang Duong, Masaya Yasuda, and Tsuyoshi Takagi</i>	
Zero-Knowledge Password Policy Check from Lattices . . . . .	92
<i>Khoa Nguyen, Benjamin Hong Meng Tan, and Huaxiong Wang</i>	
Generic Forward-Secure Key Agreement Without Signatures . . . . .	114
<i>Cyprien de Saint Guilhem, Nigel P. Smart, and Bogdan Warinschi</i>	

## Public-Key Cryptography

A Constant-Size Signature Scheme with Tighter Reduction from CDH Assumption . . . . .	137
<i>Kaisei Kajita, Kazuto Ogawa, and Eiichiro Fujisaki</i>	
Homomorphic-Policy Attribute-Based Key Encapsulation Mechanisms . . . . .	155
<i>Jérémy Chotard, Duong Hieu Phan, and David Pointcheval</i>	
Watermarking Public-Key Cryptographic Functionalities and Implementations . . . . .	173
<i>Foteini Baldimtsi, Aggelos Kiayias, and Katerina Samari</i>	

**Authentication**

Contactless Access Control Based on Distance Bounding . . . . . 195  
*Handan Kılınç and Serge Vaudenay*

Improving Gait Cryptosystem Security Using Gray Code Quantization  
and Linear Discriminant Analysis . . . . . 214  
*Lam Tran, Thang Hoang, Thuc Nguyen, and Deokjai Choi*

**Attacks**

Low-Level Attacks in Bitcoin Wallets . . . . . 233  
*Andriana Gkaniatsou, Myrto Arapinis, and Aggelos Kiayias*

Improving Password Guessing Using Byte Pair Encoding . . . . . 254  
*Xingxing Wang, Dakui Wang, Xiaojun Chen, Rui Xu, Jinqiao Shi,  
and Li Guo*

How to Make Information-Flow Analysis Based Defense Ineffective:  
An ART Behavior-Mask Attack . . . . . 269  
*Xueyi Yang, Limin Liu, Lingchen Zhang, Weiyu Jiang, and Shiran Pan*

**Privacy**

Harvesting Smartphone Privacy Through Enhanced Juice Filming  
Charging Attacks . . . . . 291  
*Weizhi Meng, Fei Fei, Wenjuan Li, and Man Ho Au*

A Differentially Private Encryption Scheme . . . . . 309  
*Carlo Brunetta, Christos Dimitrakakis, Bei Liang,  
and Aikaterini Mitrokotsa*

**Mobile Security**

Droid Mood Swing (DMS): Automatic Security Modes Based on Contexts . . . 329  
*Md Shahrear Iqbal and Mohammad Zulkernine*

T-MAC: Protecting Mandatory Access Control System Integrity from  
Malicious Execution Environment on ARM-Based Mobile Devices . . . . . 348  
*Diming Zhang, Liangqiang Chen, Fei Xue, Hao Wu, and Hao Huang*

Enforcing ACL Access Control on Android Platform. . . . . 366  
*Xiaohai Cai, Xiaozhuo Gu, Yuewu Wang, Quan Zhou,  
and Zhenhuan Cao*

**Software Security**

Nightingale: Translating Embedded VM Code in x86 Binary Executables . . .	387
<i>Xie Haijiang, Zhang Yuanyuan, Li Juanru, and Gu Dawu</i>	
Run-Time Verification for Observational Determinism Using Dynamic Program Slicing . . . . .	405
<i>Mohammad Ghorbani and Mehran S. Fallah</i>	
Automated Analysis of Accountability . . . . .	417
<i>Alessandro Bruni, Rosario Giustolisi, and Carsten Schuermann</i>	

**Network and System Security**

Visualization of Intrusion Detection Alarms Collected from Multiple Networks . . . . .	437
<i>Boyeon Song, Sang-Soo Choi, Jangwon Choi, and Jungsuk Song</i>	
Curtain: Keep Your Hosts Away from USB Attacks . . . . .	455
<i>Jianming Fu, Jianwei Huang, and Lanxin Zhang</i>	
<b>Author Index</b> . . . . .	473