

Contents

Keynotes

The Case For Human Primacy in Cryptography (Summary from the Keynote Lecture)	3
<i>X. Boyen</i>	
Time for a Paradigm Shift in Our Disciplinary Culture?	11
<i>Neal Koblitz</i>	

Revisiting Tradition

Another Look at Tightness II: Practical Issues in Cryptography	21
<i>Sanjit Chatterjee, Neal Koblitz, Alfred Menezes, and Palash Sarkar</i>	
Another Look at Anonymous Communication: Security and Modular Constructions	56
<i>Russell W.F. Lai, Henry K.F. Cheung, Sherman S.M. Chow, and Anthony Man-Cho So</i>	
Challenges with Assessing the Impact of NFS Advances on the Security of Pairing-Based Cryptography	83
<i>Alfred Menezes, Palash Sarkar, and Shashank Singh</i>	

Different Paradigms

Key Recovery: Inert and Public	111
<i>Colin Boyd, Xavier Boyen, Christopher Carr, and Thomas Haines</i>	
Honey Encryption for Language: Robbing Shannon to Pay Turing?	127
<i>Marc Beunardeau, Houda Ferradi, Rémi Géraud, and David Naccache</i>	
Randomized Stopping Times and Provably Secure Pseudorandom Permutation Generators	145
<i>Michal Kulis, Pawel Lorek, and Filip Zagorski</i>	

Cryptofication

A Virtual Wiretap Channel for Secure Message Transmission.	171
<i>Setareh Sharifian, Reihaneh Safavi-Naini, and Fuchun Lin</i>	

Necessary and Sufficient Numbers of Cards for Securely Computing Two-Bit Output Functions	193
<i>Danny Francis, Syarifah Ruqayyah Aljumid, Takuya Nishida, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone</i>	

Malicious Cryptography

Controlled Randomness – A Defense Against Backdoors in Cryptographic Devices	215
<i>Lucjan Hanzlik, Kamil Kluczniak, and Mirosław Kutylowski</i>	
Malware, Encryption, and Rerandomization – Everything Is Under Attack . . .	233
<i>Herman Galteland and Kristian Gjosteen</i>	
Protecting Electronic Signatures in Case of Key Leakage	252
<i>Mirosław Kutylowski, Jacek Cichoń, Lucjan Hanzlik, Kamil Kluczniak, Xiaofeng Chen, and Jianfeng Wang</i>	

Advances in Cryptanalysis

A New Test Statistic for Key Recovery Attacks Using Multiple Linear Approximations	277
<i>Subhabrata Samajder and Palash Sarkar</i>	
Tuple Cryptanalysis: Slicing and Fusing Multisets	294
<i>Marine Minier and Raphaël C.-W. Phan</i>	
Improvements of Attacks on Various Feistel Schemes	321
<i>Emmanuel Volte, Valérie Nachev, and Nicolas Marrière</i>	

Primitives and Features

Updatable Functional Encryption.	347
<i>Afonso Arriaga, Vincenzo Iovino, and Qiang Tang</i>	
Linking-Based Revocation for Group Signatures: A Pragmatic Approach for Efficient Revocation Checks	364
<i>Daniel Slamanig, Raphael Spreitzer, and Thomas Unterluggauer</i>	
CARIBE: Cascaded IBE for Maximum Flexibility and User-Side Control . . .	389
<i>Britta Hale, Christopher Carr, and Danilo Gligoroski</i>	
Multi-authority Distributed Attribute-Based Encryption with Application to Searchable Encryption on Lattices	409
<i>Veronika Kuchta and Olivier Markowitch</i>	

One-Round Exposure-Resilient Identity-Based Authenticated Key Agreement with Multiple Private Key Generators	436
<i>Atsushi Fujioka</i>	

Cryptanalysis Correspondence

Attacks on the Basic cMix Design: On the Necessity of Commitments and Randomized Partial Checking.	463
<i>Herman Galteland, Stig F. Mjølsnes, and Ruxandra F. Olimid</i>	

Cryptanalysis of an Identity-Based Convertible Undeniable Signature Scheme	474
<i>Rouzbeh Behnia, Syh-Yuan Tan, and Swee-Huay Heng</i>	

Invited and Insight Papers

Towards User-Friendly Cryptography	481
<i>Goichiro Hanaoka</i>	

Multi-prover Interactive Proofs: Unsound Foundations.	485
<i>Claude Crépeau and Nan Yang</i>	

Human Public-Key Encryption	494
<i>Houda Ferradi, Rémi Géraud, and David Naccache</i>	

Two Philosophies for Solving Non-linear Equations in Algebraic Cryptanalysis	506
<i>Nicolas T. Courtois</i>	

Watermarking Cryptographic Programs	521
<i>Ryo Nishimaki</i>	

From Higher-Order Differentials to Polytopic Cryptanalysis	544
<i>Tyge Tiessen</i>	

Division Property: Efficient Method to Estimate Upper Bound of Algebraic Degree	553
<i>Yosuke Todo</i>	

Author Index	573
-------------------------------	-----

Paradigms in Cryptology – Mycrypt 2016. Malicious and
Exploratory Cryptology

Second International Conference, Mycrypt 2016, Kuala
Lumpur, Malaysia, December 1-2, 2016, Revised
Selected Papers

Pham, R.C.-W.; Moti, Y. (Eds.)

2017, XI, 573 p. 84 illus., Softcover

ISBN: 978-3-319-61272-0