

Table of Contents

Symmetric Cryptosystems

An Enciphering Scheme Based on a Card Shuffle	1
<i>Viet Tung Hoang, Ben Morris, and Phillip Rogaway</i>	
Tweakable Blockciphers with Beyond Birthday-Bound Security	14
<i>Will Landecker, Thomas Shrimpton, and R. Seth Terashima</i>	
Breaking and Repairing GCM Security Proofs	31
<i>Tetsu Iwata, Keisuke Ohashi, and Kazuhiko Minematsu</i>	
On the Distribution of Linear Biases: Three Instructive Examples	50
<i>Mohamed Ahmed Abdelraheem, Martin Ågren, Peter Beelen, and Gregor Leander</i>	
Substitution-Permutation Networks, Pseudorandom Functions, and Natural Proofs	68
<i>Eric Miles and Emanuele Viola</i>	

Invited Talk

The End of Crypto	86
<i>Jonathan Zittrain</i>	

Secure Computation I

Must You Know the Code of f to Securely Compute f ?	87
<i>Mike Rosulek</i>	
Adaptively Secure Multi-Party Computation with Dishonest Majority	105
<i>Sanjam Garg and Amit Sahai</i>	
Collusion-Preserving Computation	124
<i>Joël Alwen, Jonathan Katz, Ueli Maurer, and Vassilis Zikas</i>	
Secret Sharing Schemes for Very Dense Graphs	144
<i>Amos Beimel, Oriol Farràs, and Yuval Mintz</i>	

Attribute-Based and Functional Encryption

Functional Encryption with Bounded Collusions via Multi-party Computation	162
<i>Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee</i>	
New Proof Methods for Attribute-Based Encryption: Achieving Full Security through Selective Techniques	180
<i>Allison Lewko and Brent Waters</i>	
Dynamic Credentials and Ciphertext Delegation for Attribute-Based Encryption	199
<i>Amit Sahai, Hakan Seyalioglu, and Brent Waters</i>	
Functional Encryption for Regular Languages	218
<i>Brent Waters</i>	

Proof Systems

Secure Database Commitments and Universal Arguments of Quasi Knowledge	236
<i>Melissa Chase and Ivan Visconti</i>	
Succinct Arguments from Multi-prover Interactive Proofs and Their Efficiency Benefits	255
<i>Nir Bitansky and Alessandro Chiesa</i>	

Protocols

On the Security of TLS-DHE in the Standard Model	273
<i>Tibor Jager, Florian Kohlar, Sven Schäge, and Jörg Schwenk</i>	
Semantic Security for the Wiretap Channel	294
<i>Mihir Bellare, Stefano Tessaro, and Alexander Vardy</i>	
Multi-instance Security and Its Application to Password-Based Cryptography	312
<i>Mihir Bellare, Thomas Ristenpart, and Stefano Tessaro</i>	

Hash Functions

Hash Functions Based on Three Permutations: A Generic Security Analysis	330
<i>Bart Mennink and Bart Preneel</i>	

To Hash or Not to Hash Again? (In)Differentiability Results for H^2 and HMAC	348
<i>Yevgeniy Dodis, Thomas Ristenpart, John Steinberger, and Stefano Tessaro</i>	
New Preimage Attacks against Reduced SHA-1	367
<i>Simon Knellwolf and Dmitry Khovratovich</i>	
Stam's Conjecture and Threshold Phenomena in Collision Resistance ...	384
<i>John Steinberger, Xiaoming Sun, and Zhe Yang</i>	

Composable Security

Universal Composability from Essentially Any Trusted Setup	406
<i>Mike Rosulek</i>	
Impossibility Results for Static Input Secure Computation	424
<i>Sanjam Garg, Abishek Kumarasubramanian, Rafail Ostrovsky, and Ivan Visconti</i>	
New Impossibility Results for Concurrent Composition and a Non-interactive Completeness Theorem for Secure Computation	443
<i>Shweta Agrawal, Vipul Goyal, Abhishek Jain, Manoj Prabhakaran, and Amit Sahai</i>	
Black-Box Constructions of Composable Protocols without Set-Up	461
<i>Huijia Lin and Rafael Pass</i>	

Privacy

Crowd-Blending Privacy	479
<i>Johannes Gehrke, Michael Hay, Edward Lui, and Rafael Pass</i>	
Differential Privacy with Imperfect Randomness	497
<i>Yevgeniy Dodis, Adriana López-Alt, Ilya Mironov, and Salil Vadhan</i>	

Leakage and Side-Channels

Tamper and Leakage Resilience in the Split-State Model	517
<i>Feng-Hao Liu and Anna Lysyanskaya</i>	
Securing Circuits against Constant-Rate Tampering	533
<i>Dana Dachman-Soled and Yael Tauman Kalai</i>	
How to Compute under \mathcal{AC}^0 Leakage without Secure Hardware	552
<i>Guy N. Rothblum</i>	

Invited Talk

Recent Advances and Existing Research Questions in Platform
Security 570
Ernie Brickell

Signatures

Group Signatures with Almost-for-Free Revocation 571
Benoît Libert, Thomas Peters, and Moti Yung

Tightly Secure Signatures and Public-Key Encryption 590
Dennis Hofheinz and Tibor Jager

Implementation Analysis

Efficient Padding Oracle Attacks on Cryptographic Hardware..... 608
*Romain Bardou, Riccardo Focardi, Yusuke Kawamoto,
Lorenzo Simionato, Graham Steel, and Joe-Kai Tsay*

Public Keys 626
*Arjen K. Lenstra, James P. Hughes, Maxime Augier,
Joppe W. Bos, Thorsten Kleinjung, and Christophe Wachter*

Secure Computation II

Multiparty Computation from Somewhat Homomorphic Encryption 643
Ivan Damgård, Valerio Pastro, Nigel P. Smart, and Sarah Zakarias

Near-Linear Unconditionally-Secure Multiparty Computation
with a Dishonest Minority 663
Eli Ben-Sasson, Serge Fehr, and Rafail Ostrovsky

A New Approach to Practical Active-Secure Two-Party Computation... 681
*Jesper Buus Nielsen, Peter Sebastian Nordholt,
Claudio Orlandi, and Sai Sheshank Burra*

Black-Box Separation

The Curious Case of Non-Interactive Commitments – On the Power
of Black-Box vs. Non-Black-Box Use of Primitives..... 701
Mohammad Mahmoody and Rafael Pass

Cryptanalysis

Efficient Dissection of Composite Problems, with Applications to Cryptanalysis, Knapsacks, and Combinatorial Search Problems	719
<i>Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir</i>	

Resistance against Iterated Attacks by Decorrelation Revisited	741
<i>Ash Bay, Atefeh Mashatan, and Serge Vaudenay</i>	

Quantum Cryptography

Secure Identity-Based Encryption in the Quantum Random Oracle Model	758
<i>Mark Zhandry</i>	

Quantum to Classical Randomness Extractors	776
<i>Mario Berta, Omar Fawzi, and Stephanie Wehner</i>	

Actively Secure Two-Party Evaluation of Any Quantum Operation	794
<i>Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail</i>	

Key Encapsulation and One-Way functions

On the Impossibility of Constructing Efficient Key Encapsulation and Programmable Hash Functions in Prime Order Groups	812
<i>Goichiro Hanaoka, Takahiro Matsuda, and Jacob C.N. Schuldt</i>	

Hardness of Computing Individual Bits for One-Way Functions on Elliptic Curves	832
<i>Alexandre Duc and Dimitar Jetchev</i>	

Homomorphic Evaluation of the AES Circuit	850
<i>Craig Gentry, Shai Halevi, and Nigel P. Smart</i>	

Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP	868
<i>Zvika Brakerski</i>	

Author Index	887
------------------------	-----