Editorial Board

David Hutchison
    Lancaster University, Lancaster, UK
Takeo Kanade
    Carnegie Mellon University, Pittsburgh, PA, USA
Josef Kittler
    University of Surrey, Guildford, UK
Jon M. Kleinberg
    Cornell University, Ithaca, NY, USA
Friedemann Mattern
    ETH Zurich, Zürich, Switzerland
John C. Mitchell
    Stanford University, Stanford, CA, USA
Moni Naor
    Weizmann Institute of Science, Rehovot, Israel
C. Pandu Rangan
    Indian Institute of Technology, Madras, India
Bernhard Steffen
    TU Dortmund University, Dortmund, Germany
Demetri Terzopoulos
    University of California, Los Angeles, CA, USA
Doug Tygar
    University of California, Berkeley, CA, USA
Gerhard Weikum
    Max Planck Institute for Informatics, Saarbrücken, Germany
More information about this series at http://www.springer.com/series/7410
Preface

Eurocrypt 2016, the 35th annual International Conference on the Theory and Applications of Cryptographic Techniques, was held in Vienna, Austria, during May 8–12, 2016. The conference was sponsored by the International Association for Cryptologic Research (IACR). Krzysztof Pietrzak (IST Austria), together with Joël Alwen, Georg Fuchsbauer, Peter Gaži (all IST Austria), and Eike Kiltz (Ruhr-Universität Bochum), were responsible for the local organization. They were supported by a local organizing team consisting of Hamza Abusalah, Chethan Kamath, and Michal Rybár (all IST Austria). We are indebted to them for their support and smooth collaboration.

The conference program followed the now established parallel track system where the works of the authors were presented in two concurrently running tracks. As in the previous edition of Eurocrypt, one track was labeled $R$ (for real) and the other one was labeled $I$ (for ideal). Only the invited talks, the tutorial, the best paper, papers with honorable mentions, and the final session of the conference spanned over both tracks.

The proceedings of Eurocrypt contain 62 papers selected from 274 submissions, which corresponds to a record number of submissions in the history of Eurocrypt. Each submission was anonymized for the reviewing process and was assigned to at least three of the 55 Program Committee members. Submissions co-authored by committee members were assigned to at least four members. Committee members were allowed to submit at most one paper, or two if both were co-authored. The reviewing process included a first-round notification followed by a rebuttal for papers that made it to the second round. After extensive deliberations the Program Committee accepted 62 papers. The revised versions of these papers are included in these two-volume proceedings.

The committee decided to give the Best Paper Award to “Tightly Secure CCA-Secure Encryption Without Pairings” by Romain Gay, Dennis Hofheinz, Eike Kiltz, and Hoeteck Wee. The two runners-up to the award, “Indistinguishability Obfuscation from Constant-Degree Graded Encoding Schemes” by Huijia Lin and “Essentially Optimal Robust Secret Sharing with Maximal Corruptions” by Allison Bishop, Valerio Pastro, Rajmohan Rajaraman, Daniel and Wichs, received honorable mentions. All three papers received invitations for the Journal of Cryptology.

The program also included invited talks by Karthikeyan Bhargavan, entitled “Protecting Transport Layer Security from Legacy Vulnerabilities”, Bart Preneel, entitled “The Future of Cryptography” (IACR distinguished lecture), and Christian Collberg, entitled “Engineering Code Obfuscation.” In addition, Emmanuel Prouff gave a tutorial about “Securing Cryptography Implementations in Embedded Systems.” All the speakers were so kind as to also provide a short abstract for the proceedings.

We would like to thank all the authors who submitted papers. We know that the Program Committee’s decisions, especially rejections of very good papers that did not find a slot among the sparse number of accepted papers, can be very disappointing. We sincerely hope that the rejected works eventually get the attention they deserve.
We are also indebted to the Program Committee members and all external reviewers for their voluntary work, especially since the newly established and unified page limits and the increasing number of submissions induce quite a workload. It has been an honor to work with everyone. The committee’s work was tremendously simplified by Shai Halevi’s submission software and his support, including running the service on IACR servers.

Finally, we thank everyone else—speakers, session chairs, and rump session chairs—for their contribution to the program of Eurocrypt 2016.

May 2016

Marc Fischlin
Jean-Sébastien Coron
Eurocrypt 2016

The 35th Annual International Conference on
the Theory and Applications of Cryptographic
Techniques

Vienna, Austria
May 8–12, 2016

Track $\mathcal{R}$

General Chair
Krzysztof Pietrzak IST Austria

Program Chairs
Marc Fischlin Technische Universität Darmstadt, Germany
Jean-Sébastien Coron University of Luxembourg, Luxembourg

Program Committee
Michel Abdalla Ecole Normale Superieure and CNRS, France
Shweta Agrawal IIT Delhi, India
Elette Boyle IDC Herzliya, Israel
Christina Brzuska TU Hamburg-Harburg, Germany
Ran Canetti Tel Aviv University, Israel, and Boston University, USA
David Cash Rutgers University, USA
Dario Catalano University of Catania, Italy
Jean-Sébastien Coron University of Luxembourg, Luxembourg
Cas Cremers University of Oxford, UK
Yevgeniy Dodis New York University, USA
Nico Döttling Aarhus University, Denmark
Pooya Farshim Queen’s University Belfast, UK
Jean-Charles Faugère Inria Paris-Rocquencourt, France
Sebastian Faust Ruhr University Bochum, Germany
Dario Fiore IMDEA Software Institute, Spain
Marc Fischlin TU Darmstadt, Germany
Georg Fuchsbauer IST, Austria
Juan A. Garay Yahoo Labs, USA
Vipul Goyal Microsoft Research, India
Tim Güneysu University of Bremen, Germany
Shai Halevi IBM, USA
Goichiro Hanaoka AIST, Japan
Martin Hirt ETH Zurich, Switzerland
Dennis Hofheinz Karlsruhe KIT, Germany
Tibor Jager Ruhr University Bochum, Germany
Abhishek Jain Johns Hopkins University, USA
Aniket Kate Purdue University, USA
Dmitry Khovratovich University of Luxembourg, Luxembourg
Vadim Lyubashevsky Ecole Normale Superieure, France
Sarah Meiklejohn University College London, UK
Mridul Nandi Indian Statistical Institute, Kolkata, India
Maria Naya-Plasencia Inria, France
Svetla Nikova KU Leuven, Belgium
Adam O’Neill Georgetown University, USA
Claudio Orlandi Aarhus University, Denmark
Josef Pieprzyk Queensland University of Technology, Australia
Mariana Raykova Yale University, USA
Thomas Ristenpart Cornell Tech, USA
Matthieu Rivain CryptoExperts, France
Arnab Roy Fujitsu Laboratories of America, USA
Benedikt Schmidt IMDEA Software Institute, Spain
Thomas Schneider TU Darmstadt, Germany
Berry Schoenmakers TU Eindhoven, The Netherlands
Peter Schwabe Radboud University, The Netherlands
Yannick Seurin ANSSI, France
Thomas Shrimpton University of Florida, USA
Nigel P. Smart University of Bristol, UK
John P. Steinberger Tsinghua University, China
Ron Steinfeld Monash University, Australia
Emmanuel Thomé Inria Nancy, France
Yosuke Todo NTT, Japan
Dominique Unruh University of Tartu, Estonia
Daniele Venturi Sapienza University of Rome, Italy
Ivan Visconti University of Salerno, Italy
Stefan Wolf USI Lugano, Switzerland

External Reviewers

Divesh Aggarwal Kazumaro Aoki Subhadeep Banik
Shashank Agrawal Afonso Arriaga Harry Bartlett
Adi Akavia Gilad Asharov Lejla Batina
Martin Albrecht Gilles Van Assche Carsten Baum
Joël Alwen Nuttapong Attrapadung Aemin Baumeler
Prabhanjan Ananth Christian Badertscher Christof Beierle
Ewerton Rodrigues Thomas Baignères Sonia Belaïd
Andrade Josep Balasch Fabrice Benhamouda
Elena Andreeva Foteini Baldimtsi David Bernhard
<table>
<thead>
<tr>
<th>Name</th>
<th>Name</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bogdan Warinschi</td>
<td>Jürg Wullschleger</td>
<td>Ching-Hua Yu</td>
</tr>
<tr>
<td>Hoeteck Wee</td>
<td>Masahiro Yagisawa</td>
<td>Samee Zahur</td>
</tr>
<tr>
<td>Carolyn Whitnall</td>
<td>Shota Yamada</td>
<td>Mark Zhandry</td>
</tr>
<tr>
<td>Daniel Wichs</td>
<td>Kan Yasuda</td>
<td>Zongyang Zhang</td>
</tr>
<tr>
<td>Alexander Wild</td>
<td>Scott Yilek</td>
<td>Vassilis Zikas</td>
</tr>
<tr>
<td>David Wu</td>
<td>Kazuki Yoneyama</td>
<td>Michael Zohner</td>
</tr>
</tbody>
</table>
Invited Talks and Tutorial Papers
Protecting Transport Layer Security from Legacy Vulnerabilities

Karthikeyan Bhargavan
INRIA

Abstract. The Transport Layer Security protocol (TLS) is the most widely-used secure channel protocol on the Web. After 20 years of evolution, TLS has grown to include five protocol versions, dozens of extensions, and hundreds of ciphersuites. The success of TLS as an open standard is at least partially due its protocol agility: clients and servers can implement different subsets of protocol features and still interoperate, as long as they can negotiate a common version and ciphersuite. Hence, software vendors can seamlessly deploy newer cryptographic mechanisms while still supporting older algorithms for backwards compatibility.

An undesirable consequence of this agility is that obsolete and broken ciphers can stay enabled in TLS clients and servers for years after cryptographers have explicitly warned against their use. Practitioners consider this relatively safe for two reasons. First, the TLS key exchange protocol incorporates downgrade protection, so if a client and server both support a strong ciphersuite, they should never negotiate a weaker ciphersuite even if it is enabled. Second, even if a connection uses a cryptographic algorithm with known weaknesses, it is typically hard to exploit the theoretical vulnerability to attack the protocol.

In this talk, we will see that both these assumptions are false. Leaving legacy crypto unattended within TLS configurations has serious consequences, as shown by a recent series of downgrade attacks including Logjam [1] and SLOTH [3]. We will show how these attacks expose protocol-level weaknesses in TLS that can be exploited with practical cryptanalysis. We will propose a new notion of downgrade resilience for key exchange protocols [2] and use this definition to evaluate the downgrade protections mechanisms built into the upcoming TLS 1.3 protocol.

References

The Future of Cryptography

Bart Preneel

KU Leuven and iMinds
Department of Electrical Engineering-ESAT/COSIC
Kasteelpark Arenberg 10 Bus 2452, B-3001 Leuven, Belgium
bart.preneel@esat.kuleuven.be

Abstract. We reflect on the historic role of cryptography. We develop the contrast between its success as an academic discipline and the serious shortcomings of current cryptographic deployments in protecting users against mass surveillance and overreach by corporations. We discuss how the cryptographic research community can contribute towards addressing these challenges.

Since its early days, the goal of cryptography is to protect confidentiality of information, which means that it is used to control who has access to information. A second goal of cryptography is to protect authenticity of data and entities: this allows to protect payment information, transaction records but also configuration files and software. Cryptography also plays a central role in the protection of meta data: in many settings it is important to hide the identities and locations of the communicating parties. In modern cryptography much more complex goals can be achieved beyond protection communications and stored data: cryptographic techniques are used to guarantee the correctness of the execution of a program or to obfuscate programs. Multi-party computation allows parties to compute on data while each one can keep its input private and all can check the correctness of the results, even if some of the parties are malicious. Sophisticated techniques are being developed to compute on encrypted data and to search in the data. Even in a domain as challenging as e-voting progress is being made.

Until the late 1980s, cryptographic devices were expensive, which means that the use of cryptography was limited to military, government, and diplomatic applications as well as a few business contexts such as financial transactions. In the early 1990s the cost of cryptography dropped quickly as the increased power of CPUs made it feasible to implement crypto in software. This resulted in the crypto wars, in which government key escrow schemes were proposed and defeated. One decade later commodity cryptographic hardware started to appear, resulting in a cryptography everywhere. The fast dropping cost of cryptography combined with a rich cryptographic literature leads to the conclusion that today cryptography is widespread.

A quick count shows that there are about 30 billion devices with cryptography. The largest volumes are for mobile communications, the web ecosystem, access cards, bank cards, DRM for media protection, hard disk encryption, and applications such as WhatsApp and Skype. It is remarkable that very few of those mass applications offer end-to-end confidentiality protection; moreover, those that do typically have some key
management or governance issue: the specifications or the source code are not public, or the ecosystem is brittle as it relies on trust in hundreds of CAs.

The threat models considered in cryptographic papers can be very strong: we assume powerful opponents who can intercept all communications, corrupt some parties, and perform expensive computations. Since the mid-1990s we take into account opponents who use physics to eavesdrop on signals (side channel attacks) or inject faults in computations. However, the Snowden revelations have shown that our threat models are not sufficiently strong to model intelligence agencies: they undermine the standardization process by injecting stealthily schemes with backdoors, they increase complexity of standards, break supply-chain integrity, undermine end systems using malware, obtain keys using security letters or via malware, and exploit implementation weaknesses, to name just a few.

By combining massive interception with sophisticated search techniques, intelligence agencies have developed mass surveillance systems that are a threat to our values and democracy. In response academic cryptographers have started to publish articles that consider some of these more advanced threat models. Industry has expanded its deployment of cryptography and increased the strength of deployments, e.g., by switching to solutions that offer forward secrecy. However, their efforts are sometimes limited because of the business models that monetize user data and business plans to exploit Big Data at an ever larger scale.

In terms of protection of users, progress is still very slow. The cryptographic literature has plenty of schemes to increase robustness of cryptographic implementations, but few are implemented. The reasons are cost, the lack of open source implementations, and the misalignment with business objectives that are driven by the Big Data gold rush. Moreover, in response to the modest advances made by industry, law enforcement is reviving the early 1990s crypto wars.

Overall, this complex context brings new opportunities for cryptographers: we have the responsibility to help restoring the balance of power between citizens on the one hand, and governments and corporations on the other hand. We can invent new architectures that give users more control and visibility and that avoid single points of failure. We can propose new protocols that are more robust against local compromises by malware, backdoors or security letters. And we can contribute towards developing or analyzing open implementations of these protocols to facilitate their deployment.
In the Man-at-the-end (MATE) security scenario [2] a user (and potential adversary) has physical access to a device and can gain some advantage by extracting or tampering with an asset within that device. Assets can be data (cryptographic keys and media streams) as well as code (security checks and intellectual property). As defenders, our goal is to protect the confidentiality and integrity of these assets.

MATE scenarios are ubiquitous. Consider, for example, the Advanced Metering Infrastructure where smart meters are installed at house-holds to allow utility companies to connect and disconnect users and to monitor usage. A malicious consumer can tamper with their meter to avoid payment and may even be able to send disconnect commands to other meters [5]. In the mobile Snapchat application pictures exchanged between teenagers must be deleted a few seconds after reaching a friend’s device. A malicious user can tamper with the application code to save the pictures and use them later for cyber bullying. Finally, in a massive multiplayer online game a malicious player can tamper with the game client to get an unfair advantage over other players [3].

Adversarial Model. In a realistic MATE scenario we must assume that, since the adversary has physical control over his device, in time all assets will be compromised, and, at best, any defenses will be time-limited [4]. Even protection techniques based on tamper-resistant hardware have shown themselves susceptible to attack [1]. In particular, in analogy with Kerckhoff’s principles, we must assume an adversary who has complete understanding of our system, including its source code, and who can achieve in-depth understanding of the system through static and dynamic analyses using advanced reverse engineering tools.

Protection Mechanisms and Strategies. MATE protection mechanisms are typically based on the application of obfuscating code transformations that add complexity (for confidentiality) and/or the insertion of tamper-detecting guards (for integrity). Given that individual mechanisms provide limited protection, strategies have to be put in place to extend the in-the-wild survival time.

An important such strategy is diversity. Spatial diversity (or defense-in-depth) means compounding multiple layers of interchangeable primitive protective transformations. Temporal diversity (or renewability) means to deliver, over time, an infinite and non-repeating sequence of code variants to the user. The basic principle is that every program should be protected with a different combination of transformations, that every user/potential adversary should get a uniquely protected program, and that we
will provide an ever-changing attack target to the adversary. In other words, we hope to provide long-term security by overwhelming the adversary’s analytical abilities with randomized, unique, and varying code variants.

**Evaluation and Benchmarking.** MATE protection systems are evaluated on their resilience to attack and their performance, i.e. the increase in size and speed of a protected program over the original. Many real-world applications are interactive (such as the Snapchat and game examples above), and many are running on highly constrained devices (smart meters); performance is thus always of paramount concern.

Finding the combination of primitive transformations and spatial and temporal diversity strategies that achieve the highest level of protection while staying within strict performance bounds is an unsolved engineering problem. Part of the problem is a lack of behavioral models that express the capabilities and limitations of a human adversary, and part of the problem is a lack of universally accepted benchmarks.

**Summary.** We present an overview of the engineering challenges in providing long-term protection of applications that run under complete control of an adversary. In particular, we discuss the principle of diversity and the need for adversarial modeling and benchmarking.

**Acknowledgments.** This work was funded in part by NSF grants CNF-1145913 and CNS-1525820 and BSF grant 2008362.

**References**

Securing Cryptography Implementations in Embedded Systems

Emmanuel Prouff$^{1,2}$

$^1$ANSSI, France
emmanuel.prouff@ssi.gouv.fr
$^2$POLSYS, UMR 7606, LIP6
Sorbonne Universities, UPMC University Paris VI

Abstract. Side Channel Analysis is a class of attacks which exploit leakages of information from a cryptographic implementation during execution. To defeat them, various techniques have been introduced during the two last decades, among which masking (aka implementation sharing) is a common countermeasure. The principle is to randomly split every sensitive intermediate variable occurring in the computation into several shares and the number of shares, called the order, plays the role of a security parameter. The main issue while applying masking to protect cryptographic implementations is to specify efficient schemes to secure the non-linear steps during the processing. Several solutions, applicable for arbitrary orders, have been recently published. Most of them start from the original concept of Private Circuits originally introduced by Ishai, Sahai and Wagner at Crypto 2003. In parallel, and in order to formally prove the security of the proposed masking schemes, the community has also made important efforts to define leakage models that accurately capture the leakage complexity and simultaneously enable to build accurate security arguments. It is worth noting that there is a tight link between masking/sharing techniques, secure Multi Party Computation, Coding Theory and also Threshold Implementations. During a two hours tutorial, the main classes of countermeasures will be presented, together with models which have been introduced to prove their security. The link with other areas such as secure multi-party computation, error correcting codes and information theory will also be discussed.
Contents – Part I

Best Paper and Honorable Mentions

Tightly CCA-Secure Encryption Without Pairings . . . . . . . . . . . . . . . . . . . . 1
   Romain Gay, Dennis Hofheinz, Eike Kiltz, and Hoeteck Wee

Indistinguishability Obfuscation from Constant-Degree Graded
   Encoding Schemes . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 28
   Huijia Lin

Essentially Optimal Robust Secret Sharing with Maximal Corruptions . . . . . . . 58
   Allison Bishop, Valerio Pastro, Rajmohan Rajaraman,
   and Daniel Wichs

(Pseudo) Randomness

Provably Robust Sponge-Based PRNGs and KDFs . . . . . . . . . . . . . . . . . . . . 87
   Peter Gaži and Stefano Tessaro

Reusable Fuzzy Extractors for Low-Entropy Distributions . . . . . . . . . . . . . . . . 117
   Ran Canetti, Benjamin Fuller, Omer Paneth, Leonid Reyzin,
   and Adam Smith

LPN/LWE

Provably Weak Instances of Ring-LWE Revisited . . . . . . . . . . . . . . . . . . . . 147
   Wouter Castryck, Ilia Iliashenko, and Frederik Vercauteren

Faster Algorithms for Solving LPN . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 168
   Bin Zhang, Lin Jiao, and Mingsheng Wang

Cryptanalysis I

Provable Security Evaluation of Structures Against Impossible
   Differential and Zero Correlation Linear Cryptanalysis . . . . . . . . . . . . . . . . 196
   Bing Sun, Meicheng Liu, Jian Guo, Vincent Rijmen, and Ruilin Li

Polytopic Cryptanalysis . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 214
   Tyge Tiessen
XXII  Contents – Part I

Masking

From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces ................................................................. 240
  François Durvaux and François-Xavier Standaert

Improved Masking for Tweakable Blockciphers with Applications to Authenticated Encryption ......................................................... 263
  Robert Granger, Philipp Jovanovic, Bart Mennink, and Samuel Neves

Fully Homomorphic Encryption

Sanitization of FHE Ciphertexts .......................................................... 294
  Léo Ducas and Damien Stehlé

Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts ................................................................. 311
  Pierrick Méaux, Anthony Journault, François-Xavier Standaert, and Claude Carlet

Cryptanalysis II

Improved Differential-Linear Cryptanalysis of 7-Round Chaskey with Partitioning ................................................................. 344
  Gaëtan Leurent

Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1 ................................................................. 372
  Alex Biryukov, Léo Perrin, and Aleksei Udovenko

Number Theory

Complete Addition Formulas for Prime Order Elliptic Curves .................. 403
  Joost Renes, Craig Costello, and Lejla Batina

New Complexity Trade-Offs for the (Multiple) Number Field Sieve Algorithm in Non-Prime Fields ......................................................... 429
  Palash Sarkar and Shashank Singh

Hash Functions

Freestart Collision for Full SHA-1 ......................................................... 459
  Marc Stevens, Pierre Karpman, and Thomas Peyrin

New Attacks on the Concatenation and XOR Hash Combiners ................ 484
  Itai Dinur
# Multilinear Maps

Cryptanalysis of the New CLT Multilinear Map over the Integers

Jung Hee Cheon, Pierre-Alain Fouque, Changmin Lee, Brice Minaud, and Hansol Ryu

Cryptanalysis of GGH Map

Yupu Hu and Huiwen Jia

# Message Authentication Codes

Hash-Function Based PRFs: AMAC and Its Multi-User Security

Mihir Bellare, Daniel J. Bernstein, and Stefano Tessaro

On the Influence of Message Length in PMAC’s Security Bounds

Atul Luykx, Bart Preneel, Alan Szepieniec, and Kan Yasuda

# Attacks on SSL/TLS

Lucky Microseconds: A Timing Attack on Amazon’s s2n Implementation of TLS

Martin R. Albrecht and Kenneth G. Paterson

An Analysis of OpenSSL’s Random Number Generator

Falko Strenzke

# Real-World Protocols

Safely Exporting Keys from Secure Channels: On the Security of EAP-TLS and TLS Key Exporters

Christina Brzuska, Håkon Jacobsen, and Douglas Stebila

Valiant’s Universal Circuit is Practical

Ágnes Kiss and Thomas Schneider

# Robust Designs

Nonce-Based Cryptography: Retaining Security When Randomness Fails

Mihir Bellare and Björn Tackmann

Honey Encryption Beyond Message Recovery Security

Joseph Jaeger, Thomas Ristenpart, and Qiang Tang
**Lattice Reduction**

Improved Progressive BKZ Algorithms and Their Precise Cost Estimation by Sharp Simulator .................................................. 789

*Yoshinori Aono, Yuntao Wang, Takuya Hayashi, and Tsuyoshi Takagi*

Practical, Predictable Lattice Basis Reduction .......................... 820

*Daniele Micciancio and Michael Walter*

**Author Index** .............................................................. 851
Contents – Part II

Lattice-Based Schemes

Zero-Knowledge Arguments for Lattice-Based Accumulators:
Logarithmic-Size Ring Signatures and Group Signatures Without Trapdoors ................................................................. 1
Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang

Adaptively Secure Identity-Based Encryption from Lattices with Asymptotically Shorter Public Parameters .......................... 32
Shota Yamada

Zero-Knowledge I

Online/Offline OR Composition of Sigma Protocols ......................... 63
Michele Ciampi, Giuseppe Persiano, Alessandra Scafuro, Luisa Siniscalchi, and Ivan Visconti

Constant-Round Leakage-Resilient Zero-Knowledge from Collision Resistance .......................................................... 93
Susumu Kiyoshima

Pseudorandom Functions

Constrained Pseudorandom Functions for Unconstrained Inputs ........... 124
Apoorvaa Deshpande, Venkata Koppula, and Brent Waters

Pseudorandom Functions in Almost Constant Depth from Low-Noise LPN . . . 154
Yu Yu and John Steinberger

Multi-Party Computation I

Secure Computation from Elastic Noisy Channels ............................ 184
Dakshita Khurana, Hemanta K. Maji, and Amit Sahai

All Complete Functionalities are Reversible .................................... 213
Dakshita Khurana, Daniel Kraschewski, Hemanta K. Maji, Manoj Prabhakaran, and Amit Sahai
Separations

On the Power of Hierarchical Identity-Based Encryption .......................... 243
Mohammad Mahmoody and Ameer Mohammed

On the Impossibility of Tight Cryptographic Reductions ....................... 273
Christoph Bader, Tibor Jager, Yong Li, and Sven Schäge

Zero-Knowledge II

On the Size of Pairing-Based Non-interactive Arguments ....................... 305
Jens Groth

Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the
Discrete Log Setting ......................................................... 327
Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Jens Groth,
and Christophe Petit

Protocols

On the Complexity of Scrypt and Proofs of Space in the Parallel Random
Oracle Model ................................................................. 358
Joël Alwen, Binyi Chen, Chethan Kamath, Vladimir Kolmogorov,
Krzysztof Pietrzak, and Stefano Tessaro

Anonymous Traitor Tracing: How to Embed Arbitrary Information
in a Key ........................................................................... 388
Ryo Nishimaki, Daniel Wichs, and Mark Zhandry

Round Complexity

Unconditionally Secure Computation with Reduced Interaction ............... 420
Ivan Damgård, Jesper Buus Nielsen, Rafail Ostrovsky, and Adi Rosén

The Exact Round Complexity of Secure Computation ......................... 448
Sanjam Garg, Pratyay Mukherjee, Omkant Pandey,
and Antigoni Polychroniadou

Commitments

On the Composition of Two-Prover Commitments, and Applications
to Multi-round Relativistic Commitments ........................................... 477
Serge Fehr and Max Fillinger

Computationally Binding Quantum Commitments .............................. 497
Dominique Unruh
Lattices

Structural Lattice Reduction: Generalized Worst-Case to Average-Case Reductions and Homomorphic Cryptosystems. ................................. 528
Nicolas Gama, Malika Izabachène, Phong Q. Nguyen, and Xiang Xie

Recovering Short Generators of Principal Ideals in Cyclotomic Rings ........ 559
Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev

Leakage

Circuit Compilers with $O(1/\log(n))$ Leakage Rate ............................... 586
Marcin Andrychowicz, Stefan Dziembowski, and Sebastian Faust

Randomness Complexity of Private Circuits for Multiplication ................. 616
Sonia Belaid, Fabrice Benhamouda, Alain Passelègue,
Emmanuel Prouff, Adrian Thillard, and Damien Vergnaud

Indifferentiability

10-Round Feistel is Indifferentiable from an Ideal Cipher ...................... 649
Dana Dachman-Soled, Jonathan Katz, and Aishwarya Thiruvengadam

Indifferentiability of Confusion-Diffusion Networks .............................. 679
Yevgeniy Dodis, Martijn Stam, John Steinberger, and Tianren Liu

Multi-Party Computation II

Fair and Robust Multi-party Computation Using a Global Transaction Ledger ........................................... 705
Aggelos Kiayias, Hong-Sheng Zhou, and Vassilis Zikas

Two Round Multiparty Computation via Multi-key FHE ......................... 735
Pratyay Mukherjee and Daniel Wichs

Obfuscation

Post-zeroizing Obfuscation: New Mathematical Tools, and the Case
of Evasive Circuits ........................................................................... 764
Saikrishna Badrinarayanan, Eric Miles, Amit Sahai, and Mark Zhandry

New Negative Results on Differing-Inputs Obfuscation .......................... 792
Mihir Bellare, Igors Stepanovs, and Brent Waters
Automated Analysis, Functional Encryption, and Non-malleable Codes

Automated Unbounded Analysis of Cryptographic Constructions in the Generic Group Model. .................................................. 822
   Miguel Ambrona, Gilles Barthe, and Benedikt Schmidt

Multi-input Functional Encryption in the Private-Key Setting: Stronger Security from Weaker Assumptions. .......................... 852
   Zvika Brakerski, Ilan Komargodski, and Gil Segev

Non-malleable Codes for Bounded Depth, Bounded Fan-In Circuits ................................. 881
   Marshall Ball, Dana Dachman-Soled, Mukul Kulkarni, and Tal Malkin

Author Index ........................................................................... 909