

Table of Contents

Optimizing ORAM and Using It Efficiently for Secure Computation	1
<i>Craig Gentry, Kenny A. Goldman, Shai Halevi, Charanjit Julta, Mariana Raykova, and Daniel Wichs</i>	
Anonymity-Preserving Public-Key Encryption: A Constructive Approach	19
<i>Markulf Kohlweiss, Ueli Maurer, Cristina Onete, Björn Tackmann, and Daniele Venturi</i>	
Efficient E-Cash in Practice: NFC-Based Payments for Public Transportation Systems	40
<i>Gesine Hinterwälder, Christian T. Zenger, Foteini Baldimtsi, Anna Lysyanskaya, Christof Paar, and Wayne P. Burleson</i>	
Efficient Privacy-Preserving Stream Aggregation in Mobile Sensing with Low Aggregation Error	60
<i>Qinghua Li and Guohong Cao</i>	
Broadening the Scope of Differential Privacy Using Metrics	82
<i>Konstantinos Chatzikokolakis, Miguel E. Andrés, Nicolás Emilio Bordenabe, and Catuscia Palamidessi</i>	
Turning Off GPS Is Not Enough: Cellular Location Leaks over the Internet	103
<i>Hamed Soroush, Keen Sung, Erik Learned-Miller, Brian Neil Levine, and Marc Liberatore</i>	
How Others Compromise Your Location Privacy: The Case of Shared Public IPs at Hotspots	123
<i>Nevena Vratonjic, Kévin Huguenin, Vincent Bindschaedler, and Jean-Pierre Hubaux</i>	
The Path Less Travelled: Overcoming Tor's Bottlenecks with Traffic Splitting	143
<i>Mashaal AlSabah, Kevin Bauer, Tariq Elahi, and Ian Goldberg</i>	
How Low Can You Go: Balancing Performance with Anonymity in Tor	164
<i>John Geddes, Rob Jansen, and Nicholas Hopper</i>	
OSS: Using Online Scanning Services for Censorship Circumvention	185
<i>David Fifield, Gabi Nakibly, and Dan Boneh</i>	

The Need for Flow Fingerprints to Link Correlated Network Flows 205
 Amir Houmansadr and Nikita Borisov

How Much Is Too Much? Leveraging Ads Audience Estimation to
Evaluate Public Profile Uniqueness 225
 *Terence Chen, Abdelberi Chaabane, Pierre Ugo Tournoux,
 Mohamed-Ali Kaafar, and Roksana Boreli*

On the Acceptance of Privacy-Preserving Authentication Technology:
The Curious Case of National Identity Cards 245
 Marian Harbach, Sascha Fahl, Matthias Rieger, and Matthew Smith

Author Index 265