Introduction to the Issue on Signal and Information Processing for Privacy

AS we enter an era of ever-abundant data collection and distribution, it is natural to be focused on the benefits associated with such data ubiquity. New cloud-based applications will assimilate data from many sources to make recommendations, help us drive our vehicles, and even live healthier and longer lives. All of these new advantages do not come without risks—the data being collected and shared is intimately tied to our daily activities, to who we are, to things we value. Unfortunately, the rate of technological advancement associated with building applications that produce and use such data typically outpaces the development of mechanisms that ensure the privacy of such data and the systems that process it. As a society we are currently witnessing many privacy-related concerns that have resulted from these technologies—there are now grave concerns about our communications being wiretapped, about our SSL/TLS connections being compromised, about our transactions being captured by cyber-exploits, about our personal data being shared with entities we have no relationship with, etc. It is therefore essential that safeguards are developed that can protect the sharing and collection of information and, in particular, the explicit and implicit values associated with that information.

Traditionally electronic data has been protected via cryptographic techniques, but unfortunately these security mechanisms fail to protect the privacy of the data producers and consumers as this data often leaves the protection of encrypted channels/storage, or the data is subjected to analysis through queries, as occurs in a database. Hence, privacy is an important problem that needs a large toolbox of technological solutions, ranging from traditional cryptographic methods to complementary techniques that are built through signal and information-theoretic principles. In particular, information exchange, interaction, and access problems lend themselves to fundamental information processing abstractions and theoretical analysis. The tools and techniques of rate distortion, distributed compression algorithms, machine learning for feature identification and suppression, and compressive sensing are fundamental and can be applied to precisely formulate and quantify the tradeoff between utility and privacy in a variety of domains.

The purpose behind the JSTSP Special Issue on Signal and Information Processing for Privacy is to provide a venue for state-of-the-art research being doing in how signal and information processing is advancing the field of information privacy. The special issue received 55 high-quality submissions and through an extensive peer-review process, the final version of the special issue settled on 15 articles that span a variety of different aspects related to privacy, ranging from supporting anonymous communication to private information retrieval from databases to evaluating different primitives intended for encrypted search.

Digital Object Identifier 10.1109/JSTSP.2015.2462391

At a high-level, the articles in the special issue can be categorized as being focused on:

- Fundamental contributions to the theory of privacy;
- Methods for supporting private communications;
- Cryptographic protocols for privacy;
- Supporting privacy in various applications.

This last category covers the majority of the accepted papers, as supporting privacy for specific applications tends to require specialized solutions that focus on the details underpinning each application area.

We begin the special issue with an invited paper "The Staircase Mechanism for Differential Privacy." Differential privacy is a strong formal model for providing worst-case privacy guarantees for statistical databases. In practice, differential privacy is often achieved by adding noise to the data prior to publishing where the noise added is chosen as Laplace distributed. In the first invited paper, the authors show that the universal optimal differentially private additive noise mechanism is a "staircase mechanism" involving a geometric mixture of uniform random variables, and in particular highlight the power of this mechanism in the low-privacy regime (a regime of much practical importance). The article also sets the stage for the special issue by contributing new, important results in the fundamental theory behind privacy.

We next move into a collection of three articles that focus on supporting private communications. The second article in the special issue, "Optical Signal Processing and Stealth Transmission for Privacy" is the second invited article and provides a survey of different techniques that have been developed in the optical communications community for supporting stealthy communications. These optical signal processing techniques are characterized by the ultra-fast processing and wide bandwidths associated with optical systems. Interestingly, though, the methods are analogous to classical signal processing techniques used for low probability of detection and for steganography. As editors, we believe that these similarities might allow for future cross-pollination between optical communications and the signal processing community. The next article, "Achieving Undetectable Communication" examines the fundamentals of stealthy communication by examining what rate of error free communications is possible without being detected by a detection device. The third paper on private communication, "Distributed Secret Dissemination Across a Network" examines the problem of secret sharing when the dealer does not have direct communication links with all participants, but instead is only connected to the participants through a general network graph.

The article, "Secure Comparison Protocols in the Semi-Honest Model" examines a collection of comparison protocols that operate in the encrypted domain and that serve as the basis for privacy-preserving protocols. This article ex-

amines different approaches and, for the first time, places these disparate approaches on a common footing by providing fair comparison of their performance.

The next section of the special issue examines the popular area of databases and Big Data, where privacy has received significant attention. "Efficient Private Information Retrieval over Unsynchronized Databases" examines an efficient form of private information retrieval when the associated databases lack synchronization, which is a fundamental hurdle that has been left unaddressed by the classical PIR community. The article "Managing your Private and Public Data: Bringing Down Inference Attacks Against Your Privacy" is a unique article that attempts to bridge theory and practice by providing a methodology for tuning the public release of private data through a privacy-preserving probabilistic mapping. In the course of their work, the authors explore pragmatic issues associated with applying their methodology to real-world data. In the same vein of privacy-versus-utility, the next paper, "Privacy or Utility in Data Collection? A Contract Theoretic Approach," provides fundamentally new models associated with how to view the tradeoff between privacy and utility by formulating the tradeoff using contract theory.

The special issue next proceeds to cover a series of papers that focus on different application areas for privacy. The paper "A Study of Online Social Network Privacy via the TAPE Framework" examines the problem of designing tools that support user privacy over social networks. The paper "Enabling Data Exchange in Two-Agent Interactive Systems under Privacy Constraints" focuses on how privacy-guaranteed data sharing can be enabled in distributed systems such as the electric power system using powerful game-theoretic tools. In the same game-theoretic vein, the paper "A Secure Radio Environment Map Database to Share Spectrum" examines the basic problem of obscuring spectrum usage information being shared between primary users and secondary users who might use that information to improperly interfere with primary usage of the spectrum. The next two articles, "A Belief Propagation Approach to Privacy Preserving Item-Based Collaborative Filtering" and "The Price of Privacy in Untrusted Recommender Systems" both examine the challenges associated with achieving privacy in recommendation systems. The last two articles of the special issue focus on aspects related to privacy in health care and the Internet of Things. The paper "PPDM: A Privacy-preserving Protocol for Cloud-Assisted e-Healthcare Systems" examines the design of practical issues of computation and communication overhead associated with privacy-preserving data aggregation for medical applications. The article "Privacy-Aware Distributed Bayesian Detection" examines the problem of data sharing and aggregation for Internet of Things applications where application decisions are being made based on detections associated with the data being collected. In this work, the authors are concerned with eavesdropping adversary that might witness a fraction of the communications involved, and then examine the fundamental question of how distributed detection can be formulated with privacy guarantees against such an eavesdropper.

WADE TRAPPE, *Lead Guest Editor*
Electrical and Computer Engineering Department
Rutgers University
New Brunswick, NJ 08902 USA

LALITHA SANKAR, *Guest Editor*
Department of Electrical, Computer, and Energy Engineering,
Arizona State University
Tempe, AZ 85287 USA

RADHA POOVENDRAN, *Guest Editor*
Department of Electrical Engineering
University of Washington
Seattle, WA USA

HEEJO LEE, *Guest Editor*
Department of Computer Science and Engineering
Korea University
Seoul 136-713, Korea

SRDJAN CAPKUN, *Guest Editor*
Department of Computer Science
ETH Zurich
8092 Zurich, Switzerland

Wade Trappe (S'98–A'02–M'03–SM'13–F'14) is a Professor in the Electrical and Computer Engineering Department at Rutgers University, and Associate Director of the Wireless Information Network Laboratory (WINLAB), where he directs WINLAB's research in wireless security. He has published over 150 papers, including five best papers awards (two in media security, one in Internet design, one in cognitive radio systems and one in mobile computing). His papers have appeared in numerous IEEE/ACM journals and premier conferences, spanning the areas of signal processing and security. His experience in network security and wireless spans over 15 years, and he has co-authored a popular textbook in security, *Introduction to Cryptography with Coding Theory*, as well as several notable monographs on wireless security, including *Securing Wireless Communications at the Physical Layer* and *Securing Emerging Wireless Systems: Lower-layer Approaches*. Professor Trappe has served as an editor for IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY (TIFS), *IEEE Signal Processing Magazine* (SPM), and IEEE TRANSACTIONS ON MOBILE COMPUTING (TMC). He served as the lead guest editor for September 2011 special issue of the TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY on "Using the Physical Layer for Securing the Next Generation of Communication Systems" and also served IEEE Signal Processing Society as the SPS representative to the governing board of IEEE TMC.

Lalitha Sankar is an Assistant Professor in electrical, computer, and energy engineering at Arizona State University. Her research interests include information privacy as viewed through the lens of information theory and statistics as well as cyber-security of cyber-physical systems, in particular the electric power grid. Dr. Sankar received the NSF CAREER award in 2014. She was also a recipient of a three year Science and Technology Teaching Postdoctoral Fellowship from Princeton University. For her doctoral work, she received the 2007 Electrical Engineering Academic Achievement Award from Rutgers University. She received the IEEE Globecom 2011 Best Paper Award.

Radha Poovendran is a Professor and chair of the Department of Electrical Engineering at the University of Washington, Seattle. He is the founding director of the Network Security Lab (NSL) in the Electrical Engineering (EE) Dept. at the University of Washington (UW). His research interests are in the areas of wireless and sensor network security, adversarial modeling, security in cyber-physical systems, privacy and anonymity in public wireless networks, control-security, games-security and information theoretic-security in the context of wireless mobile networks. He has co-chaired multiple conferences and workshops including the first ACM Conference on Wireless Network Security (WiSec) in 2008, NITRD-NSF National workshop on high-confidence transportation cyber-physical systems in 2009, trustworthy aviation information systems at the 2010, 2011 AIAA Infotech@Aerospace, 2011 IEEE Aerospace, 2014 IEEE CNS, 2014 GameSec. He was chief editor for the PROCEEDINGS OF THE IEEE special issue on cyber-physical systems (2012), an editor of IEEE TMC and ACM TOSN, co-guest editor for two special issues on security and privacy (IEEE Networks 2013; IEEE TPDS 2013). He is a co-inventor of four recently issued patents in the area of wireless security. He is a fellow of the IEEE.

Heejo Lee is a Professor at the Department of Computer Science and Engineering, Korea University, Seoul, Korea. Before joining Korea University, he was at AhnLab, Inc. as a CTO from 2001 to 2003. From 2000 to 2001, he was a Postdoctorate Researcher at the Department of Computer Science and CERIAS at Purdue University. In 2010, he was a Visiting Professor at CyLab/CMU. Dr. Lee received his B.S., M.S., and Ph.D. degrees in computer science and engineering from POSTECH, Pohang, Korea. Dr. Lee serves as an editor of the *Journal of Communications and Networks*, and the *International Journal of Network Management*.

Srdjan Capkun (M'01) is an Associate Professor in the Department of Computer Science, ETH Zurich and Director of the Zurich Information Security and Privacy Center (ZISC). He was born in Split, Croatia, and received his Dipl.Ing. degree in electrical engineering/computer science from the University of Split, Croatia (1998), and his Ph.D. degree in communication systems from EPFL in 2004. Prior to joining ETH Zurich in 2006 he was a Postdoctoral Researcher in the Networked & Embedded Systems Laboratory, University of California Los Angeles and an Assistant Professor in the Informatics and Mathematical Modeling Department, Technical University of Denmark. Professor Capkun is well known in the security community and has contributed numerous papers in a diverse range of topics, including security for wireless networks, security and privacy for smart vehicular systems, anti-jamming mechanisms for wireless communications, secure neighbor discovery, and security based on distance bounding protocols.