Paradigm Shifts in Cryptographic Engineering

Raphaël Phan and Moti Yung

MODERN cryptography is almost five decades old, and we have seen some interesting breakthroughs throughout its relatively young history. These include the engineering foundations of symmetric key cryptography and block ciphers in particular (like the DES and the AES), the discovery of public-key cryptography, protocols for secure computations for general and specific tasks using interactions among parties and tools like homomorphic encryption (this line of work has been enhancing the use of cryptography beyond secure messaging into secure computing).

Cryptography is currently embedded in our computational infrastructure based on the world wide web and mobile networks, and the recent trend triggered by cryptography-enabled currencies (starting with Bitcoin) has rejuvenated widespread public interest in cryptography. Also, information security best practices and privacy laws, in fact, implicitly or explicitly, mandate the use of cryptography in many applications and systems.

Cryptography has to be thought about from many directions. As with any technology, and as was predicted over 20 years ago by cryptographers, cryptography is a double-edged sword that has been used by both the good guys to get security, but also by others to get insecurity, as well as by the dark side. For instance, Bitcoin is a popular payment mechanism for ransomware, which additionally uses highly secure encryption techniques as part of this prevalent cybersecurity attack, as would the most advanced self-encrypting malware.

While researchers continue to improve upon the latest schemes, to achieve better performance, and better proofs, or to demonstrate that the security of schemes can be preserved while relaxing underlying security assumptions, essentially it is invigorating to go beyond these to revisit long-standing paradigms, critique previously proven results, and question well-accepted assumptions. Such ongoing activities assure that the field will persist to be a source of new conceptual ideas, have new applications, and perhaps will move in new unexpected directions in the future.

Indeed, the field is far from being in a state of stagnation: Substantial breakthroughs have been made in cryptography and security in the past decade that were beyond the norm of natural linear progress, or provided new twists, including notions pertaining to homomorphic encryption, obfuscation, and new protocols and models, on the one hand, and notions that reverse the trust model like questionable encryption and malicious security, i.e., where security is no longer simply against bad guys but where good guys who are conventionally viewed as mostly defensive can equally be adversarial. These align well with recent trends wherein trusted parties need no longer be trustworthy, or where insiders can potentially be malicious, or where different organizations have differing goals and engage in what is known as "crypto wars."

This special issue of *IEEE Transactions on Dependable and Secure Computing* (*TDSC*) on the Paradigm Shifts in Cryptographic Engineering places particular focus on unconventional cryptographic research and thinking outside the current box, with focus on applied constructions.

Privacy is a key public concern these days. Such that major internet giants, especially in recent years, champion this as their top priority. While privacy has many flavors, foremost in people's privacy concerns is the issue of anonymity. Appropriately, the first paper in our special issue: "Another Look at Anonymous Communication" revisits the anonymous communication problem and formalizes the first-known simple indistinguishability-style notions of anonymity.

Privacy of data should not be compromised despite the current trend of outsourcing both computations and storage to third party servers (say, in the cloud). The second paper "Private Compound Wildcard Queries Using Fully Homomorphic Encryption" proposes the first-known privacy-preserving protocol for compound wildcarded queries to encrypted databases, underpinned by the fully homomorphic encryption primitive.

Note that the human is at the heart of the security problem. Attacks, be they via bots, machines, networks or software, are initiated by malicious humans. Weaknesses in security systems due to design flaws, implementation bugs, or careless usage, are equally due to human errors. Passwords are one of the top security issues related to human users. The paper "Generation of Secure and Reliable Honeywords, Preventing False Detection" focuses on advancing on existing techniques of generating secure honeywords, which are decoy passwords injected among the real passwords in databases to enable detection of compromises. The strategies for ensuring indistinguishability between passwords and honeywords is to maintain similar distributions, while ensuring that users have a low chance of mistyping passwords into honeywords by enforcing a minimal distance between them.

- *R. Phan is with the Monash University, Malaysia. E-mail: raphael.phan@monash.edu.*
- *M. Yung is with Google and Columbia University. E-mail: motiyung@gmail.com.*

For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TDSC.2019.2934527

The other paper dedicated to passwords, "Building & Studying a Password Store that Perfectly Hides Passwords from Itself" focuses on ensuring that even when the device storing password-relevant information is compromised, yet the password cannot be recovered. The gist is to input the human-provided low-entropy password in encrypted form to the device, which then transforms it to a random password; and this is stored on the device. Therefore, even if the device is subsequently compromised, the human-provided password remains secure because the stored random password would not enable the extraction of any information about the human-provided password as they are theoretically independent of each other.

With humans being a central theme in diverse security situations, the paper "Robust Fuzzy Extractors and Helper Data Manipulation Attacks Revisited: Theory vs Practice" revisits the context of robust fuzzy extractors. These are methods to generate keys from random sources of nature e.g., from human biometrics. In particular, it shows why a robust fuzzy extractor based on BCH codes cannot be built in practice, and proposes a new attack strategy that attacks the integrity of the key rather than its secrecy.

The paper "It is All in the System's Parameters: Privacy & Security Issues in Transforming Biometric Raw Data into Binary Strings" provides a new perspective into how privacy leakages could occur in various stages of the biometric processing due to system parameters, including from feature extraction and quantization.

Aligned with this special issue's theme of revisiting convention, the final paper "Strong Stationary Times & Its Use in Cryptography" proposes a different approach to constructing pseudo-random permutation generators (PRPGs), contrary to well known approaches. Notably, such generators do not run for a predefined number of steps but rather they are designed to stop upon some stopping rules being observed, e.g., distribution of generator outputs resembling that of a uniform distribution.

To recap, this special issue focuses on beyond-norm, paradigm-shifting, unconventional cryptography, and it corresponds to our firm belief that a field can only advance if its research community revisits conventional paradigms, rocks the crypto boat, questions the status quo, and raises controversial issues. Since attackers adapt and try new things in their attempt to break systems, so must do cryptographers! Since malicious players think in devious ways so must researchers! We hope that the readers, those interested in protection and those interested in understanding malicious attempts and attacks, will benefit from such a special issue that is designed to maximize the impact of its frontier-stretching theme.

Raphaël Phan
Moti Yung
Guest Editors

Raphaël Phan received the BEng, MEngSc, and PhD degrees from MMU, in 1999, 2001 and 2005, respectively. He is currently a professor with the Monash University. He was general chair for Mycrypt 2005 & Asiacrypt 2007, Technical Program chair for Mycrypt 2016; and is regularly invited to serve in the technical program committees of security conferences. He is co-designer of the hash function BLAKE, one of the five finalists in the U.S. NIST SHA-3 Hash Competition. He has Erdős number 2. His recent research interests are notably on dark side technologies: fake fingers, hidden emotions, invisible motions and stealth.

Moti Yung received the PhD degree from Columbia University, in 1988. He is a Security and Privacy Research Scientist with Google and an Adjunct Research faculty with the Computer Science Department, Columbia University. Previously, he was with IBM Research, Certco/ Bankers Trust, RSA Laboratories (EMC), and Snap. He is a fellow of the IEEE, the Association for Computing Machinery (ACM), the International Association for Cryptologic Research (IACR), and the European Association for Theoretical Computer Science (EATCS). In 2018 he received the IEEE Computer Society W.W. McDowell award for innovative contributions to computer and network security, predicting, both attack scenarios and design needs in this important evolving area. In 2010 he gave the IACR Distinguished Lecture. He is also the recipient of the 2014 ACM's SIGSAC Outstanding Innovation award, the 2014 ESORICS (European Symposium on Research in Computer Security) Outstanding Research award, an IBM Outstanding Innovation award, a Google OC award, and a Google founders' award. His main professional interests are in security, privacy, and cryptography. His contributions to research and development treat science and technology holistically: from the theoretical mathematical foundations, via conceptual mechanisms which typify computer science, to participation in the design and development of industrial products. His published work (articles, patents, a book, and edited books) includes collaborations with more than 300 highly appreciated co-authors. Yung's work has been predicting future needs of secure systems, and analyzing coming threats. These led to basic theoretical and applied notions, like: ransomware attacks, cryptosystems subversion, concurrent sessions in authentication protocols, strong (chosen ciphertext) secure encryption, and digital signatures from simplified cryptography. His industrial work gave rise to new diversified mechanisms, some of which are in extensive use. These include: public-key based second factor (resulting in U2F); new factors for user identification; distributed signing methods; secure large scale distributed computation protocol for privacy preserving data analytics; and various very large scale encryption systems, such as Google encryption within the Advertisement Exchange system and Snap's secure end-to-end encryption.