Final Call for Papers - IEEE Transactions on Dependable & Secure Computing

Special Issue on **Paradigm Shifts in Cryptographic Engineering**

Background
Research on cryptologic approaches to solving real-world security problems has been conducted in the public domain for decades, and well established paradigms and techniques now exist that can solve numerous security problems in our lives. Since then, substantial breakthroughs have been made in cryptographic engineering especially in the recent years. To be more precise, by cryptographic engineering, we mean the security techniques researched with cryptographic rigour aimed at solving real-life problems in our current world; these involve systems, components, practical methods and algorithms, implementations as well as human elements.

Indeed, our society is constantly influenced by different lifestyle shifts driven by diverse technological advances: to name a few recent technological revolutions beyond the more established trends of cloud computing and big data; notably internet of things (IoT), cyber-physical systems (CPS), cyber-physical social lifestyles augmented by social media, smart clothing, and more recently nanosensors and flexible electronics.

Meanwhile, the security research community has now matured to a level where cryptographic engineering techniques with additional features beyond the basic security requirements are increasingly being proposed, due largely to real-world constraints, changing needs or socio-technological revolutions. Recent ones include fully homomorphic cryptography, functional cryptography and *-preserving cryptography, where we use * as a wildcard to denote different features that can be preserved, e.g. format, order, structure, privacy, property. In response to recent news of security systems being subverted, attention has also been devoted to the notions of malicious security and adversarial security, i.e. where security is no longer just against bad guys but where good guys who are conventionally viewed as mostly defensive can equally be adversarial. Meanwhile, the way that humans interact with each other has drastically changed since the days when cryptographic engineering research first commenced that modelled the security problems essentially as multi-party communications. From conventional terminal-based communications, our world now is one where people interact on the go, with others virtually in social media, aided by a myriad of personal networked gadgets and smart things.

Therefore, it is time to revisit the existing cryptographic engineering paradigms and underlying assumptions on which current techniques are built. This special issue will solicit original papers of substantial technical contribution with particular focus on paradigm-shifting cryptographic engineering research & thinking outside the current box. These will include the following indicative topic categories:

- *paradigm-shifting*, *unconventional* cryptographic engineering techniques and/or frameworks, influenced by recent and/or future socio-technological revolutions including cyber-physical systems (CPS), Internet of Everything (IoE), nano-sensors, flexible electronics; in addition to the cloud and big data
  (e.g. malicious security, adversarial security, unconventional formulations of underlying problems, or new hard problems to suit such revolutions)
- *position* papers on *breakthrough* cryptographic engineering research
- *revisits*/critiques/analysis of long-standing cryptographic engineering paradigms / approaches / models / formulations
  (in fact, we also encourage paired submissions by security factions of opposing views, where each paper in the pair argues for/against a well-established paradigm)
- approaches/solutions to *long-standing open problems*; or formulations of long-standing/thus-far adhoc security approaches
- new paradigms for *cryptofications of the real world*
  (e.g. new types of *adversarial models* and/or *formal security notions* inspired by real world incidents/problems, such as accountability, dependability, provenance, verifiability, chain-of-custody, admissibility, compromisability; formally modelling humans-in-the-security-loop)
- cryptographic engineering & beyond: cryptologic techniques in union with techniques from other disciplines

The gist is that we welcome all things non-conventional, paradigm-shifting & out of the box.

Instructions for Authors
Submissions must be at most 14 pages (double column IEEE format); and be in 10pt fonts using the IEEE Trans format with the specified margins.

The main part of the paper should be intelligible as reviewers are not required to read the appendices. The

introduction should summarize the main contributions of the paper so that it is understandable to a non-expert in cryptography.

Submissions must not substantially duplicate work that any of the authors has published in a journal or a conference/workshop with proceedings, or has submitted/is planning to submit before the author notification deadline to a journal or other conferences/workshops that have proceedings. Significantly extended versions of preliminary conference versions may be submitted provided authors can justify clearly where the distinctions lie. Accepted submissions may not appear in any other conference or workshop that has proceedings. The Guest Editors reserve the right to share information about submissions with other program committees or editors to detect parallel submissions and the IEEE policy on irregular submissions will be strictly enforced.

Submissions not meeting these guidelines will be rejected without consideration of their merits.

Submitted papers must be in PDF format and should be submitted electronically via the submission server.

The reviewing process will involve two stages. Some papers will be rejected after stage 1, others will proceed to stage 2 and rebuttals will be requested from these authors. The rebuttals will be taken into consideration during the stage 2 of the reviewers discussion.

Note that this is a final call for submissions. We have received a batch of submissions from the initial call, but decided to give a final call to capture more recent paradigm-shifting breakthroughs.

Important dates

Final Call submission deadline	March 31, 2017 (23:59 UTC)
First round of comments	May 31, 2017
Rebuttals due	June 15, 2017
Notification of acceptance	July 15, 2017
Camera ready version due	August 15, 2017
Publication date	Q4, 2017

Guest Editors

1. Professor Raphael C.-W. Phan
Multimedia University (MMU), Malaysia

2. Professor Moti Yung
Google & Columbia University, USA