CEIoT-CFP: Cryptographic Engineering for Internet of Things: Security Foundations, Lightweight Solutions, and Attacks

Interconnected embedded systems, within the Internet of Things (IoT), enable everyday objects around us to collect, exchange, and process information. They unlock new applications and are gradually transforming our lives. In general, useful and personalized features we enjoy often stem from the collection of sensitive information. When this information determines the action of cyber-physical systems (CPS), any attack might not only compromise user privacy but it can also be a life-or-death matter. New cryptographic techniques are needed to secure these systems, not only because of the constraints of embedded systems but also due to the often conflicting requirements appearing in new application scenarios.

With the increasing popularity of IoT and CPS, and the advances in energy-efficient, high-speed, and leakage-resilient cryptographic libraries, we believe it is now a prime time to solicit original, cutting-edge research on the topic of cryptographic engineering for embedded systems. Topics of interest include but are not limited to:

- Formal security definitions and rigorous security analysis on CPS and IoT applications

- Security issues on interactions of IoT/CPS with cloud computing and big data analytics

- Lightweight cryptographic solutions and privacy-enhancing technologies

- Lightweight software and hardware cryptographic implementations

- Energy/computation/memory-saving implementation of cryptographic protocols

- System security issues related to IoT/CPS

- Side-channel attacks and low-cost countermeasure

- Countermeasures against tampering and reverse engineering

- User-centric issues: authentication, identity management, user-controlled data privacy, etc.

- Physical layer security of IoT communication

- Fault injection analysis and countermeasures

High-quality survey and position papers on the above topics are also welcome.

Instructions for Authors:
The manuscript must not be under consideration for publication elsewhere. Conference papers may only be submitted if the paper was completely re-written or substantially extended (at least 30%). Authors should submit their journal version at the ACM TECS Manuscript Central website (https://mc.manuscriptcentral.com/tecs) strictly adhering to the formatting instructions on the TECS website, and indicate that you are submitting to the Special Issue on Cryptographic Engineering for IoTs on the first page and in the field "Author's Cover Letter:" in Manuscript Central. The page count limit is 25. For additional questions please contact the guest editors.

Note: If a submitted paper is recommended by the guest editors for “major revision”, the paper will be put through the reviewing process when revised, but not guaranteed to be included in the special issue for which it was submitted. However, if the paper is accepted at the conclusion of the review process, it will then be included in a regular issue of the journal.

Submission Deadline:	February 15th 2018
Result of First round of Reviews:	May 31st 2018
Submission of Revised Manuscripts:	June 30th 2018
Results of Second Round of Reviews:	August 15th 2018
Camera-Ready Due:	September 15th 2018
Tentative publication date:	Late 2018 / Early 2019