Call for Papers (ICITS 2017)

10th International Conference on Information Theoretic Security
29 November – 2 December, 2017
Hong Kong, China

http://www.inc.cuhk.edu.hk/icits2017/

Note: ICITS 2017 is held in Cooperation with IACR, and supported by IEEE Hong Kong Information Society Chapter. ICITS 2017 takes place right before Asiacrypt 2017 (3—7 Dec., 2017 in Hong Kong).

Conference Topics: ICITS deals with all aspects of information theoretic security, from relevant mathematical tools to theoretical modeling to implementation. Papers on all technical aspects of these topics are solicited for submission. Areas of interest include, but are not restricted to: *Post-quantum cryptography (e.g. Lattices & cryptography), Quantum cryptography, Quantum information theory, Nonlocality and non-signaling, Physical layer security, Wiretap channels, Adversarial channel models, Cryptography from noisy channels, Bounded storage models, Network coding security, Biometric security, Randomness extraction, Key and message rates, Secret sharing, Authentication codes, Multiparty computations, Information theoretic reductions, Implementation challenges*.

As the goal of ICITS is to bring together researchers on all aspects of information theoretic security, it consists of two tracks, *Conference Track* and *Workshop Track*, with different types of contributed presentations (see below).

- **Instructions for Authors**

(1) Conference Track (with proceedings): Submissions must not substantially duplicate work published elsewhere or submitted in parallel to a journal or any other conference/workshop that has proceedings. The submission must be anonymous, with no author names, affiliations, or obvious references. The length of the submission must be at most 16 pages excluding bibliography and appendices, and at most 30 pages in total. The text must be in a single column format, use at least 11-point fonts, and have reasonable margins. The submission should begin with a title and a short abstract. The introduction should summarize the contributions of the paper at a level appropriate for a non-specialist reader. Committee members are not required to read appendices, and the paper should be intelligible without them. Submissions must be in PDF format. Submissions not meeting the submission guidelines risk rejection without consideration of their merits. Accepted papers will be presented at the conference and will

appear in the conference proceedings. The proceedings will be published by Springer-Verlag in its Lecture Notes in Computer Science (LNCS) Series. At least one author of each accepted paper must register with the conference and present the paper.

(2) Workshop Track (no proceedings): Authors may submit an original manuscript, or a paper published elsewhere as long as it first appeared after May 1, 2016. As with the conference track, submissions should begin with a title and short abstract followed by an introduction that summarizes the contributions at a level appropriate for a non-specialist reader. Information about previous publication, if any, should be indicated on the first page of the submission. Submissions must be in PDF format. Beyond these guidelines no specific format is required. In particular, (a) papers previously published elsewhere may be submitted in their published form provided bibliographic information is clearly indicated; (b) short summaries of works available in other venues or online (on the arXiv or IACR eprint) are acceptable; (c) original submissions may be left anonymous at the discretion of the authors. (Previously published submissions cannot be anonymous.)

There is no restriction on program committee member submissions to either track, though PC-authored papers will be held to a higher standard. Papers should be submitted through EasyChair.

● Important Dates

Submission deadline (both tracks): ~~June 5, 2017 (23:59 UTC)~~ July 31, 2017 (23:59 UTC)
Decision notification: ~~August 14, 2017~~ September 27, 2017
Final version deadline: ~~August 25, 2017~~ October 11, 2017

● Program Committee

Divesh Aggarwal (National University of Singapore, Singapore)
Paulo Barreto (University of Washington, Tacoma, USA)
Mario Berta (Caltech, USA)
Matthieu Bloch (Georgia Institute of Technology, USA)
Ignacio Cascudo (Aalborg University, Denmark)
Paolo D'Arco (University of Salerno, Italy)
Frédéric Dupuis (Masaryk University, Czech Republic)
Benjamin Fuller (University of Connecticut, USA)
Peter Gazi (IOHK Research)
Goichiro Hanaoka (AIST, Japan)
Masahito Hayashi (Nagoya University, Japan)
Mitsugu Iwamoto (The University of Electro-Communications, Japan)

Takeshi Koshiba (Waseda University, Japan)
Yuan Luo (Shanghai Jiao Tong University, China)
Hemanta Maji (Purdue University, USA)
Keith Martin (Royal Holloway, University of London, UK)
Kirill Morozov (Tokyo Institute of Technology, Japan)
Anderson Nacimento (University of Washington, Tacoma, USA)
Frédérique Oggier (Nanyang Technological University, Singapore)
Carles Padró (Universitat Politècnica de Catalunya, Spain)
Vinod M. Prabhakaran (Tata Institute of Fundamental Research, India)
Rei Safavi-Naini (University of Calgary, Canada)
Rafael F. Schaefer (Technische Universität Berlin, Germany)
Junji Shikata (Yokohama National University, Japan), *Chair*
Vincent Y. F. Tan (National University of Singapore, Singapore)
Stefano Tessaro (University of California, Santa Barbara, USA)
Huaxiong Wang (Nanyang Technological University, Singapore)
Shun Watanabe (Tokyo University of Agriculture and Technology, Japan)