Algorithmica (2017) 79:985–986
DOI 10.1007/s00453-017-0368-3

Special Issue: Algorithmic Tools in Cryptography

Juan A. Garay[1] · **Rafail Ostrovsky**[2]

Published online: 24 August 2017

The wide availability of computer networks, and in particular of the global Internet, offers the opportunity to perform electronically and in a distributed way a wide range of transactions. As such, cryptology assumes an increasingly important role, not just as the traditional warrantor of the mechanisms' soundness and safety against the potential misbehavior of some of their participants, but also as a critical enabler of new functionalities and ways of interaction that preserve the privacy of participants' data. As the premier annual conference in the field, *Crypto* embodies the most significant advances and trends in all of its areas. This special issue presents a selection of ten highly ranked papers that were accepted for publication at *Crypto 2014*, which was co-chaired by Juan Garay. The papers have been expanded and reviewed according to rigorous journal standards.

Cryptology consists of many areas, with algorithmic notions and techniques underlying all of them—from its foundational aspects and security proofs, to the number theory and relevant hardness assumptions on which it is based, to the design aspects of functions and protocols (understood as collections of algorithms, one for each participant), to the "destructive" ventures of cryptoanalysis, drawing from combinatorics and probability theory to render futile the security purpose of commonly used cryptographic tools. Even though our main inclusion criterion was quality (as deemed by the conference's Program Committee members and expert sub-reviewers), as opposed to breadth, all the above areas are represented in this special issue, albeit with a natural bias towards the current flurry of research on the broader applicability of cryptogra-

✉ Juan A. Garay
juan.a.garay@gmail.com

[1] Department of Computer Science and Engineering, Texas A&M University, H. R. Bright Building, 710 Ross St., College Station, TX 77843, USA

[2] UCLA, Los Angeles, CA 90095, USA

phy based on stronger assumptions. Also represented in this issue are studies on the fundamental notions to cryptography of pseudo-randomness and entropy; hardness of number-theoretic problems (lattices, eliptic curves) and applications; advances in the cryptoanalysis of hash-based message-authentication codes (HMAC); and—last but not least—further understanding of a version ("non-perfect") of the core building block of information-theoretic cryptographic protocols known as *secret sharing*.

We are indebted to the reviewers who significantly contributed to the comprehensive evaluation and improvement of the articles, and hope the reader enjoys the reach and depth of these representative works of the exciting field of cryptology.

Juan A. Garay
Rafail Ostrovsky