comput. complex. **25** (2016), 563 – 565

1016-3328/16/030563-3
published online April 11, 2016
DOI 10.1007/s00037-016-0119-2

SPECIAL ISSUE ON THE 10TH THEORY OF CRYPTOGRAPHY CONFERENCE: EDITOR'S FOREWORD

Oded Goldreich

This special issue celebrates the 10th anniversary of the *Theory of Cryptography Conference* (TCC). The *10th TCC* took place in March 2013, in Tokyo, following prior venues in MIT (2004 and 2005), NYC (2006), Amsterdam (2007), NYC (2008), San Francisco (2009), Zurich (2010), Brown (2011), and Sicily (2012).

The connection between complexity theory and the foundations of cryptography is well known. It is also known that this connection goes both ways: Research done in Cryptography often uses complexity theoretic assumptions (e.g., average-case hardness), and it also distills concepts that inspires complexity theoretic research (e.g., computational indistinguishability and probabilistic proof systems). More direct technical interaction is also quite common. In fact, at times, it is hard to tell whether a specific work should be categorized under cryptography or under complexity theory. Indeed, for a wide class of works, the question seems odd, and they can be claimed to belong to both areas. In other words, these two areas have a significant intersection, although it is also clear that their symmetric difference is much larger.

The intersection between cryptography and complexity theory is most visible in venues devoted to one area, which often feature works that also belong to the other area. A typical case is that of the annual *Theory of Cryptography Conference* (TCC), which took for the 10th time in March 2013, in Tokyo. As usual in TCC, the program included several works that may be of interest to complexity theorists, and three of these works are included in this

special issue. (These works were solicited by us, but underwent the normal review process.)

The first work is *a counterexample to the chain rule for conditional HILL entropy* (by Stephan Krenn, Krzysztof Pietrzak, and Akshay Wadia). This refers to the notion of pseudo-entropy (PE) as defined by Hastad, Impagliazzo, Levin, and Luby (*SICOMP*, 1999). Specifically, the conditional PE of X given Z is at least k if there exists a joint distribution (Y, Z) that is computationally indistinguishable from the joint distribution (X, Z) such that the conditional min-entropy of Y given Z is at least k, where the latter holds if and only if $\mathrm{E}_{z \leftarrow Z}(\max_x\{\Pr[X=x|Z=z]\}) \leq 2^{-k}$. Assuming the existence of one-way function, the authors present a joint distribution (b, X, Y) such that $\mathrm{PE}[X|Y] \geq 2^t$ (where $|(b, x, Y)| = \mathrm{poly}(t)$) while $\mathrm{PE}[X|Y, b] = 0$ with b being a random bit. This constitutes a strong violation of the natural chain rule for conditional PE.

The second work discusses the *unprovable security of perfect NIZK and non-interactive non-malleable commitments* (by Rafael Pass). The author advocates viewing both simple intractability assumptions and complex cryptographic primitives as elements in a hierarchy (or rather a lattice) of intractability assumptions, where different assumptions are captured by different challenger games and the "complexity of the assumption" is reflected by the complexity of the game. (Typical results of the form "Assumption A implies Primitive P" capture the derivation of a complex assumption from a simpler one.) He presents a taxonomy of assumptions and separates the two primitives in the title from the set of *refutable assumptions*, where separation is with respect to black-box proofs of security. This result also provides an appealing example of natural primitives that are security implemented in the Random Oracle Model but cannot be proved secure (via a black-box reduction) in the standard model.

The third work is a survey of *cryptographic hardness of random local functions* (by Benny Applebaum). The author touched on a variety of issues regarding the hardness of random (or rather quasi-random) local functions, while only mentioning the alternative structured construction of hard local functions by generically

compiling hard log-space functions. One concrete motivation for avoiding the latter transformation is its effect on the input/output lengths. The author indicates that in the context of local computation there are implications that are not valid in the standard setting (e.g., robustness to linear tests implies robustness to stronger tests). I would also stress that things we take for granted in the standard setting may not hold in the context of local computation (or may be hard to establish in it): One such example is the amplification of the stretch of pseudo-random generators.

Manuscript received 13 August 2015

Oded Goldreich
Department of Computer Science
Weizmann Institute of Science
Rehovot, Israel
oded.goldreich@weizmann.ac.il