J. Cryptology (1996) 9: 127–128

Journal of
CRYPTOLOGY

Guest Editor's Introduction

One of the great inventions of the 1980s is the concept of *Zero-Knowledge Proofs* introduced by Shafi Goldwasser, Silvio Micali, and Charles Rackoff. Designed for cryptographic purposes, this notion has also played a major role in the theory of complexity. An extraordinarily large literature on the topic has flourished since then.

In the fall of 1992, authors were encouraged to submit papers about zero-knowledge for a special issue of the *Journal of Cryptology.* One objective of this special issue was to put together a set of very-high-quality papers ranging over the different aspects of this field. Seven papers were submitted, from which only two have reached the final round: "The Power of Preprocessing in Zero-Knowledge Proofs of Knowledge" by Alfredo De Santis and Guiseppe Persiano, and "Certifying Permutations: Noninteractive Zero-Knowledge Based on Any Trapdoor Permutation" by Mihir Bellare and Moti Yung. In the process of preparing this special issue, a regular submission to the *Journal of Cryptology* was also invited to join in because of its scope and very high quality: "How To Construct Constant-Round Zero-Knowledge Proof Systems for NP" by Oded Goldreich and Ariel Kahan.

This special issue also seemed a great occasion to invite a *famous unpublished* paper to appear in print. The paper "A Secure Protocol for the Oblivious Transfer (Extended Abstract)" by Michael J. Fischer, Silvio Micali, and Charles Rackoff was thus invited. The paper appears in its original form, it has not been refereed nor revised. It is included in this special issue for historical purposes: this Eurocrypt 84 paper has been referenced by many authors as one of the first instances of zero-knowledge proofs. Unfortunately the paper did not appear in the proceedings of that conference as explained by Silvio Micali:

> This type-written article (that so eloquently talks about theory funding) is the authors' original submission to Eurocrypt 84. The paper being accepted, the second author gave its corresponding talk in Paris in April 84. Endless debates on how to write it properly made so that no written version of it ever appeared in the conference proceedings. (Perfection is the enemy of the good.)
>
> The article constitutes the first *Zero-Knowledge Proof of Knowledge.* By then, zero-knowledge proofs had already been invented, but, still systematically rejected by all conferences, had not yet been published either. (Apparently, the most successful approach to zero-knowledge in the early eighties consisted in not publishing anything about it.)

> We thank oral tradition for making it still possible for our article to be quite influential. But even more we thank the editor of this issue for creating such a wonderful opportunity of having our article enter the written record: prehistory is fun and exciting, but dangerous too!
>
> Silvio Micali

As a final note, I thank the authors for their hard work and submission of their papers for this issue, and the referees for their invaluable help in selecting and reviewing the papers. I hope you enjoy reading this great set of articles.

CLAUDE CRÉPEAU

Département IRO
Université de Montréal
C.P. 6128, succ. "Centre-Ville"
Montréal (Québec)
Canada H3C 3J7