Designs, Codes and Cryptography (2023) 91:3331–3332
https://doi.org/10.1007/s10623-023-01260-2

Guest editorial: Special issue on Mathematics of Zero-Knowledge

Steven Galbraith[1] · Rosario Gennaro[2] · Carla Ràfols[3] · Ron Steinfeld[4]

Accepted: 1 June 2023 / Published online: 7 July 2023

This special issue of Designs, Codes and Cryptography on the topic Mathematics of Zero-Knowledge aims at encouraging mathematicians and computer scientists with a strong interest in Mathematics to contribute to the burgeoning topic of zero-knowledge proofs. The last few years have seen a spectacular development in research in both the foundations and the practical applications of this primitive. Advances in this area touch on many different areas of mathematics.

The paper by Diego F. Aranha, Youssef El Housni and Aurore Guillevic takes a deep dive into the new challenges and new uses of elliptic curves that are brought about by recent developments in Zero-Knowledge arguments. Different proof systems require elliptic curves with different properties: for example, it would be ideal to have 2-cycles of pairing-friendly curves for recursive proof composition. The paper explicitly describes many open problems, related to the existence of more efficient cycles of pairing friendly curves or about the efficiency of 2-chains of elliptic curves at different security levels. The paper by Steven Galbraith, Ward Beullens, Luca De Feo and Christophe Petit presents a survey of the latest developments of isogenies, covering also the recent attacks against this post quantum primitive presented just before this special issue was finalized.The paper points out that proof systems based on isogenies need further research, and probably one of the most important open questions is to find more proof systems with low soundness error. Scott Ames, Carmit Hazay, Yuval Ishai and Muthuramakrishnan Venkitasubramaniam present Ligero, a very important and efficient proof system that was among the first to be post quantum secure and have sublinear proof size.The version included in this special issue presents several efficiency improvements with respect to the original scheme backed up with experimental results that shed light on the different performance of proof systems with similar characteristics for

Rosario Gennaro, Work done while on leave at Protocol Labs.

✉ Carla Ràfols
carla.rafols@upf.edu

1 Mathematics Department, Cyber Security Foundry, University of Auckland, Private Bag 92019, Auckland 1142, New Zealand

2 The City College of New York, 160 Convent Ave, New York, NY 10031, USA

3 Departament de les Tecnologies de la Informació i les Comunicacions, Universitat Pompeu Fabra, C/Roc Boronat, 138, 08018 Barcelona, Spain

4 Department of Software Systems and Cybersecurity, Faculty of Information Technology, Monash University, Clayton, VIC 3800, Australia

different proof sizes. The paper also presents a list of very interesting open problems in proof systems design and coding theory with a description of recent progress. For example, fundamental questions include whether it is possible to construct proof systems with linear prover time and with negligible soundness error for circuits over small fields, or the existence of complexity preserving proof systems. The paper of Carsten Baum, Samuel Dittmer, Peter Scholl and Xiao Wang gives a comprehensive view on zero knowledge from a different primitive, oblivious vector evaluation, a tool from secure two-party computation. The paper lists the main open questions left in the area both theoretically and practically, mainly related with the inherent tension between communication efficiency and quality of assumptions in proof systems. Daniel Benarroch, Matteo Campanelli, Dario Fiore, Kobi Gurkan and Dimitris Kolonelos focus on set membership and non-membership proofs. These are an important subclass of statements that appear naturally in many applications. The modular approach developed in the paper is an important method for describing these proofs systematically. The paper achieves different properties from commitment schemes based on RSA and based on the discrete logarithm. Important open questions are whether these differences are inherent, and how efficient modular composition of these commitment schemes with SNARKs can be.

Collectively, these five papers illustrate the diverse range of approaches and techniques that are being investigated with the motivation of constructing zero-knowledge proofs, and leaves a body of open questions that we are confident will be of interest to the readers of this special issue.