Faster Zero-Knowledge Protocols for General Circuits and Applications
(Invited Talk Abstract)

Claudio Orlandi

Aarhus University, Aarhus, Denmark

Zero-knowledge protocols (ZKP) [GMR85] are one of the cornerstones of modern cryptography. In a nutshell, a ZKP allows a prover P (with a secret input x) to persuade a verifier V that $f(x) = 1$ for some public function f, without the V learning any other information about x.

A large body of literature has investigated the efficiency of ZKP for statements with a rich algebraic structure, starting from Schnorr's classic ZKP for discrete logarithm [Sch89]. However, the lack of efficient ZKP for interesting, non-algebraic statements (such as "*I know* x *such that SHA-256*$(x) = y$" for a public y), has arguably prevented the application of ZKPs to real-world applications.

In this talk I will describe two recent ZKPs for arbitrary circuits, ZKGC [JKO13] and ZKBoo [GMO16], together with their applications.

The first protocol (ZKGC), leveraging on the impressive advances in the field of practically efficient secure two-party computation (2PC), proposes to perform *zero-knowledge from garbled Boolean circuits*. As opposed to general 2PC (where many copies of the circuit must be garbled to achieve active security), when constructing ZKP it is enough to garble and evaluate *a single circuit*. Moreover, due to the nature of the application (since the verifier has no secret input), more efficient special purpose *privacy-free garbling schemes* [FNO15] can be used instead.

The second protocol instead (ZKBoo) follows a more classic "commit-challenge-response" structure (i.e., is a Σ-protocol). In ZKBoo the prover decomposes the computation of the function f in such a way that subsets of the computation can be checked by the verifier without revealing any information about the input to the computation, following the approach proposed by [IKOS07].

ZKGC and ZKBoo both have interesting properties: ZKGC leads to *smaller proof sizes* and, since it is based on garbled circuits, it can be combined very naturally with pre-existing secure computation tools towards building interesting applications such as: enforcing input validity in secure two-party computation [Bau16, KMW16], attributed-based key exchange with general policies [KKL$^+$16], privacy-preserving credentials [CGM16], ZKPs for RAM programs [HMR15], etc.

ZKBoo on the other hand is *faster* and can be used for both Boolean and arithmetic circuits. Perhaps most importantly, ZKBoo can be made *non-interactive* using the Fiat-Shamir [FS86] heuristic. This qualitative advantage allows to use ZKBoo in applications such as (post-quantum) signature schemes from symmetric-key primitives [DOR$^+$16], blind certificate authorities [WPaR16], etc.

It is exciting to see the growing number of applications which are enabled (or benefit) by the advances in the realm of ZKPs, and it seems likely that future research will make use of these tools in designing cryptographic solutions to interesting problems.

From a technical point of view, the main bottleneck in ZKGC and ZKBoo is their communication complexity, which in both cases is proportional to the number of non-linear gates in f times the security parameter (resulting in proof sizes in the order of hundreds of kylobytes for functions like SHA-1/256). Whether and how we can overcome this is a major and very exciting research question.

Acknowledgements Research supported by: the Danish National Research Foundation and The National Science Foundation of China (grant 61361136003) for the Sino-Danish Center for the Theory of Interactive Computation; the European Union Seventh Framework Programme ([FP7/2007-2013]) under grant agreement number ICT-609611 (PRACTICE).

References

Bau16. Carsten Baum. On garbling schemes with and without privacy. In *Security and Cryptography for Networks - 10th International Conference, SCN 2016, Amalfi, Italy, August 31 - September 2, 2016, Proceedings*, pages 468–485, 2016.

CGM16. Melissa Chase, Chaya Ganesh, and Payman Mohassel. Efficient zero-knowledge proof of algebraic and non-algebraic statements with applications to privacy preserving credentials. In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part III*, pages 499–530, 2016.

DOR+16. David Derler, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, and Daniel Slamanig. Digital signatures from symmetric-key primitives. In *Manuscript*, 2016.

FNO15. Tore Kasper Frederiksen, Jesper Buus Nielsen, and Claudio Orlandi. Privacy-free garbled circuits with applications to efficient zero-knowledge. In *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II*, pages 191–219, 2015.

FS86. Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Advances in Cryptology—CRYPTO'86*, pages 186–194. Springer, 1986.

GMO16. Irene Giacomelli, Jesper Madsen, and Claudio Orlandi. Zkboo: Faster zero-knowledge for boolean circuits. In *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016.*, pages 1069–1083, 2016.

GMR85. Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof-systems (extended abstract). In *Proceedings of the 17th Annual ACM Symposium on Theory of Computing, May 6-8, 1985, Providence, Rhode Island, USA*, pages 291–304, 1985.

HMR15. Zhangxiang Hu, Payman Mohassel, and Mike Rosulek. Efficient zero-knowledge proofs of non-algebraic statements with sublinear amortized cost. In *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*, pages 150–169, 2015.

IKOS07. Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Zero-knowledge from secure multiparty computation. In *Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing*, STOC '07, pages 21–30. ACM, 2007.

JKO13. Marek Jawurek, Florian Kerschbaum, and Claudio Orlandi. Zero-knowledge using garbled circuits: how to prove non-algebraic statements efficiently. In *2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013*, pages 955–966, 2013.

KKL+16. Vladimir Kolesnikov, Hugo Krawczyk, Yehuda Lindell, Alex J. Malozemoff, and Tal Rabin. Attribute-based key exchange with general policies. CCS 2016, 2016. `http://eprint.iacr.org/2016/518`.

KMW16. Jonathan Katz, Alex J. Malozemoff, and Xiao Wang. Efficiently enforcing input validity in secure two-party computation. Cryptology ePrint Archive, Report 2016/184, 2016. `http://eprint.iacr.org/2016/184`.

Sch89. Claus-Peter Schnorr. Efficient identification and signatures for smart cards. In *CRYPTO*, pages 239–252, 1989.

WPaR16. Liang Wang, Rafael Pass, abhi shelat, and Thomas Ristenpart. Secure channel injection and anonymous proofs of account ownership. Cryptology ePrint Archive, Report 2016/925, 2016. `http://eprint.iacr.org/2016/925`.