Cascudo, Ignacio; **Damgård, Ivan**; **David, Bernardo**; **Döttling, Nico**; **Dowsley, Rafael**; **Giacomelli, Irene**

Efficient UC commitment extension with homomorphism for free (and applications). (English) Zbl 07196576

Galbraith, Steven D. (ed.) et al., Advances in cryptology – ASIACRYPT 2019. 25th international conference on the theory and application of cryptology and information security, Kobe, Japan, December 8–12, 2019. Proceedings. Part II. Cham: Springer (ISBN 978-3-030-34620-1/pbk; 978-3-030-34621-8/ebook). Lecture Notes in Computer Science 11922, 606-635 (2019).

Summary: Homomorphic universally composable (UC) commitments allow for the sender to reveal the result of additions and multiplications of values contained in commitments without revealing the values themselves while assuring the receiver of the correctness of such computation on committed values. In this work, we construct essentially optimal additively homomorphic UC commitments from any (not necessarily UC or homomorphic) extractable commitment, while the previous best constructions require oblivious transfer. We obtain amortized linear computational complexity in the length of the input messages and rate 1. Next, we show how to extend our scheme to also obtain multiplicative homomorphism at the cost of asymptotic optimality but retaining low concrete complexity for practical parameters. Moreover, our techniques yield public coin protocols, which are compatible with the Fiat-Shamir heuristic. These results come at the cost of realizing a restricted version of the homomorphic commitment functionality where the sender is allowed to perform any number of commitments and operations on committed messages but is only allowed to perform a single batch opening of a number of commitments. Although this functionality seems restrictive, we show that it can be used as a building block for more efficient instantiations of recent protocols for secure multiparty computation and zero knowledge non-interactive arguments of knowledge.

For the entire collection see [Zbl 1428.94009].

MSC:

94A60 Cryptography
68M12 Network protocols

Keywords:

homomorphic universally composable commitments; Fiat-Shamir heuristic

Full Text: DOI