Cascudo, Ignacio; **Damgård, Ivan**; **David, Bernardo**; **Giacomelli, Irene**; **Nielsen, Jesper Buus**; **Trifiletti, Roberto**

Additively homomorphic UC commitments with optimal amortized overhead. (English)

Zbl 1345.94047

Katz, Jonathan (ed.), Public-key cryptography – PKC 2015. 18th IACR international conference on practice and theory in public-key cryptography, Gaithersburg, MD, USA, March 30 – April 1, 2015. Proceedings. Berlin: Springer (ISBN 978-3-662-46446-5/pbk; 978-3-662-46447-2/ebook). Lecture Notes in Computer Science 9020, 495-515 (2015).

Summary: We propose the first UC secure commitment scheme with (amortized) computational complexity linear in the size of the string committed to. After a preprocessing phase based on oblivious transfer, that only needs to be done once and for all, our scheme only requires a pseudorandom generator and a linear code with efficient encoding. We also construct an additively homomorphic version of our basic scheme using VSS. Furthermore we evaluate the concrete efficiency of our schemes and show that the amortized computational overhead is significantly lower than in the previous best constructions. In fact, our basic scheme has amortised concrete efficiency comparable with previous protocols in the random oracle model even though it is constructed in the plain model.

For the entire collection see [Zbl 1318.94002].

MSC:

94A60 Cryptography

Full Text: DOI