Cryptology ePrint Archive: Report 2013/123

Analysis and Improvement of Lindell's UC-Secure Commitment Schemes

Olivier Blazy and Céline Chevalier and David Pointcheval and Damien Vergnaud

Abstract: In 2011, Lindell proposed an efficient commitment scheme, with a non-interactive opening algorithm, in the Universal Composability (UC) framework. He recently acknowledged a bug in its security analysis for the adaptive case. We analyze the proof of the original paper and propose a simple patch of the scheme.

More interestingly, we then modify it and present a more efficient commitment scheme secure in the UC framework, with the same level of security as Lindell's protocol: adaptive corruptions, with erasures. The security is proven in the standard model (with a Common Reference String) under the classical Decisional Diffie-Hellman assumption. Our proposal is the most efficient UC-secure commitment proposed to date (in terms of computational workload and communication complexity).

Category / Keywords: cryptographic protocols / UC Commitment

Date: received 28 Feb 2013

Contact author: olivier blazy at rub de

Available formats: PDF | BibTeX Citation

Version: 20130305:124739 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]