Cryptology ePrint Archive: Report 2011/264

Round Optimal Blind Signatures

Dominique Schröder and Dominique Unruh

Abstract: All known round optimal (i.e., two-move) blind signature schemes either need a common reference string, rely on random oracles, or assume the hardness of some interactive assumption. At Eurocrypt 2010, Fischlin and Schr\"oder showed that a broad class of three-move blind signature scheme cannot be instantiated in the standard model based on any non-interactive assumption. This puts forward the question if round optimal blind signature schemes exist in the standard model. Here, we give a positive answer presenting the first round optimal blind signature scheme that is secure in the standard model without any setup assumptions. Our solution does not need interactive assumptions.

Category / Keywords:

Publication Info: Appears as a merge at CYRPTO 2011

Date: received 25 May 2011

Contact author: schroeder at me com

Available formats: PDF | BibTeX Citation

Note: This paper has been merged with "Round Optimal Blind Signatures in the Standard Model" by Sanjam Garg, Vanishree Rao, and Amit Sahai.

Version: 20110528:041331 (All versions of this report)

Discussion forum: Show discussion | Start new discussion