Errata to *(Nearly) Round-Optimal Black-Box Constructions of Commitments Secure against Selective Opening Attacks*

David Xiao

LIAFA
CNRS and Université Paris Diderot - Paris 7
dxiao@liafa.univ-paris-diderot.fr

Abstract. Several proofs initially presented by the author [2] were shown to be incorrect in a recent work of Ostrovsky *et al.* [1]. In this notice we summarize the errors and summarize the current state of the art after taking into account the errors and subsequent work.

In TCC 2011 the author claimed several results about nearly round-optimal black-box constructions of commitments secure against selective opening attacks [2]. It was later shown by Ostrovsky *et al.* [1] (a proceedings version appears in the current volume), that several of the proofs in [2] contained errors. Here we restate the errors discovered by Ostrovsky *et al.* [1], and we summarize what remains true from [2], as well as the current state of the art in light of the revised theorems from [2] and subsequent work including [1].

Errors in [2]: (for details, we refer the reader to [1]

1. The proof of Theorem 1, which claimed several nearly round-optimal black-box constructions, is incorrect as presented there. This is due to problems with the hiding and binding properties of the constructions presented there.
2. Items 1 and 2 of Theorem 2, which claimed to rule out selective-opening secure black-box constructions of 3-round parallel computational binding and hiding commitments and 4-round parallel statistically binding commitments, are incorrect. This is due to an incorrect implicit assumption that the sender sends the last message in the commit phase.

Unaffected results: the proofs of the following theorems from [2] remain valid:

1. Item 3 of Theorem 2, stating that one can build constant-round stand-alone statistically hiding commitments in a black-box way using constant-round statistically binding parallel selective-opening secure commitments.
2. Corollary 1, stating that there is no black-box construction using one-way permutations to build constant-round statistically binding parallel selective-opening secure commitments.
3. Theorem 3, stating there exist no black-box constructions for constant-round receiver public-coin protocols and or perfect binding protocols.

Item 4 of Theorem 2 of [2] regarding fully concurrent selective-opening security also remains valid, but this is superseded by the results of [1] (see below).

A. Sahai (Ed.): TCC 2013, LNCS 7785, pp. 721–722, 2013.

Revised results: The following weakened statement of Theorem 2, Items 1 and 2 of [2] holds, using the original proof except removing the incorrect implicit assumption that the sender sends the last message in the commit phase:

Theorem (Revision of Theorem 2 of [2]). *There exist no black-box constructions of commitments that are parallel selective-opening secure with* 2 *rounds and that are computationally binding and hiding, or with* 3 *rounds and that are statistically binding.*

The author was also able to give a different proof of Item 2 of Theorem 1 of [2], which claimed a black-box construction of $(t + 3)$ statistically-binding parallel selective-opening secure commitments assuming t-round stand-alone statistically hiding commitments, but this is superseded by the results of [4] (see below).

State of the art: For parallel selective opening security, Ostrovsky *et al.* [1] and subsequent work of the author [4] gave the following black-box constructions:

1. 3-round computationally binding and hiding commitments, assuming appropriate stand-alone trapdoor commitment schemes [1] (this is optimal by the revised theorem above).
2. $(t + 2)$-round statistically binding commitments, assuming the existence of stand-alone t-round statistically hiding commitments [4]. (For the case $t = 2$ this is optimal by the above revised theorem.)

Ostrovsky *et al.* [1] also give other constructions with different round complexities under weaker assumptions and/or allowing interactive decommitment.

For concurrent security, it was proved in [1] that *no* secure black-box constructions exist with fully concurrent selective-opening security, although their constructions (including their 3-round construction) are secure in a model they term concurrent-with-barrier. We refer the reader to [1] for details.

Revised Manuscript: a revised (unrefereed) manuscript [3] is available on the Cryptology ePrint archive containing the valid results from [2].

References

[1] Ostrovsky, R., Rao, V., Scafuro, A., Visconti, I.: Revisiting Lower and Upper Bounds for Selective Decommitments. Cryptology ePrint Archive, Report 2011/536 (2011), `http://eprint.iacr.org/`

[2] Xiao, D.: (Nearly) Round-Optimal Black-Box Constructions of Commitments Secure against Selective Opening Attacks. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 541–558. Springer, Heidelberg (2011)

[3] Xiao, D.: On the round complexity of black-box constructions of commitments secure against selective opening attacks. Technical Report 2009/513, Cryptology ePrint Archive (2012)

[4] Xiao, D.: Round-Optimal Black-Box Statistically Binding Selective-Opening Secure Commitments. In: Mitrokotsa, A., Vaudenay, S. (eds.) AFRICACRYPT 2012. LNCS, vol. 7374, pp. 395–411. Springer, Heidelberg (2012)