Electronic Colloquium on Computational Complexity, Comment 1 on Report No. 46 (2006)

A Comment to ECCC Technical Report 06-046

Dima Grigoriev* Edward A. Hirsch† Konstantin Pervyshev‡

November 8, 2006

Abstract

After we published our ECCC report, we were made aware about a recent work of Harnik et al. [1] that predates ours. Although the construction in our report is very similar to the construction sketched in [1], there is a subtle difference in the definitions: while we declare that the constructed cryptosystem C is *complete* in a common complexity-theoretical sense (that is, the break of any cryptosystem efficiently *reduces* to the break of C), Harnik et al. only state the fact that C is secure if and only if there exists a secure cryptosystem, in particular, the construction of the reduction is missing.

This difference in the definitions, however, does not affect the construction of the cryptosystem.

References

[1] Danny Harnik, Joe Kilian, Moni Naor, Omer Reingold, Alon Rosen. On Robust Combiners for Oblivious Transfer and Other Primitives. EUROCRYPT 2005: 96-113.

*IRMAR, Université de Rennes, Campus de Beaulieu, 35042 Rennes, cedex France, Web: `http://name.math.univ-rennes1.fr/dimitri.grigoriev/`.

†Steklov Institute of Mathematics at St.Petersburg, 27 Fontanka, 191023 St.Petersburg, Russia, Web: `http://logic.pdmi.ras.ru/~hirsch/`.

‡St.Petersburg State University, Russia, Mathematics and Mechanics Department, Web: `http://logic.pdmi.ras.ru/~pervyshev/`.

ISSN 1433-8092