Electronic Colloquium on Computational Complexity - Reports Series 1996 - available via:

Comment 01 on ECCC TR96-065

FTP: ftp.eccc.uni-trier.de:/pub/eccc/

WWW: http://www.eccc.uni-trier.de/eccc/

Email: ftpmail@ftp.eccc.uni-trier.de with subject 'help eccc'

Correction. Shai Halevi, has pointed out the following error in the original proof of Lemma 3.1, (pp. 40-42 in the first version of the paper). We have assumed in the proof, that the distribution of the vectors $v_{\frac{m}{2}+1}, \ldots, v_m$ is uniform on the parallelepiped $\mathcal{P}$. This assumption is not justified, since the vectors were taken with uniform distribution from another set, namely the cube $\mathcal{Q}$. In the new (second) version of the paper we correct the proof (with some additional steps). The statements of the theorems and lemmata of the first version remain correct, only the choices for the constants $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{D}_3$ change.

There is another, in some sense simpler, way to correct the mentioned mistake, namely to modify the cryptosystem in the way as suggested in Remark 1, (on page 39 in both versions). This however requires more extensive (although technically much easier) changes in other parts of the proof and in the statement of the results, as indicated in the Remark.

Acknowledgement. We are grateful to Shai Halevi for pointing out this mistake and for other valuable comments.