J Cryptol (2023)36:5
https://doi.org/10.1007/s00145-023-09443-9

Journal of CRYPTOLOGY

Correction

Correction: Locally Computable UOWHF with Linear Shrinkage

Benny Applebaum
School of Electrical Engineering, Tel-Aviv University, Tel Aviv, Israel
bennyap@post.tau.ac.il

Yoni Moses
School of Computer Science, Tel-Aviv University, Tel Aviv, Israel
ymoses@gmail.com

Online publication 14 February 2023

Correction to: J Cryptol (2017) 30:672–698
https://doi.org/10.1007/s00145-016-9232-x

This is an errata for our Journal of Cryptology paper, "Locally Computable UOWHF with Linear Shrinkage" [2]. There is a gap in the proof of Theorem 4.1 that asserts that the collection $\mathcal{F}_{P,n,m}$ is δ-secure β-random target collision resistant assuming the one-wayness and the pseudorandomness of the collection for related parameters. We currently do not know whether Theorem 4.1 (as stated in Section 4) holds.

The source of trouble is a miscalculation in the proof of Claim 4.4. Indeed, it is essentially claimed that for a random graph G and random input $x \in \{0,1\}^n$, any string $z \in \{0,1\}^n$ whose output $f_{G,P}(z) \in \{0,1\}^{2m}$ agrees with $f_{G,P}(x) \in \{0,1\}^{2m}$ on about $(1+\gamma)m$ locations, must be correlated with x. Unfortunately, this level of "output correlation" is not significant enough to guarantee the desired input correlation.

We note that Theorem 5.1 that transforms any δ-secure β-random target collision-resistant collection to a target collision-resistant collection while preserving constant locality and linear shrinkage remains intact. Thus, one can construct a locally computable UOWHF with linear shrinkage based on the hypothesis that random local functions are δ-secure β-random target collision resistant. Specifically, the main result of the paper can be based (via Theorem 5.1) on the following hypothesis.

Assumption 1. For every constants $\varepsilon, \beta > 0$, there exists an integer d and a d-local predicate $P : \{0,1\}^d \to \{0,1\}$ such that the ensemble $\mathcal{F}_{P,n,(1-\varepsilon)n}$ is $o(1)$-secure β-random target collision resistance. That is, every polynomial-time adversary $\mathcal{A}$ that is given a random local function $f \xleftarrow{R} \mathcal{F}_{P,n,(1-\varepsilon)n}$ and a random target $x \xleftarrow{R} \{0,1\}^n$, outputs $x' \in f^{-1}(f(x))$ which is βn-far from x with probability at most $o(1)$.

The original article can be found online at https://doi.org/10.1007/s00145-016-9232-x.

We also mention that locally-computable functions with linear-shrinkage that achieve a stronger form of *collision resistance* were constructed in [1] based on incomparable assumptions.

Acknowledgements

We are grateful to Colin Sandon for pointing out the gap in Claim 4.4.

References

[1] B. Applebaum, N. Haramaty, Y. Ishai, E. Kushilevitz, and V. Vaikuntanathan. Low-complexity cryptographic hash functions. In C. H. Papadimitriou, editor, *8th Innovations in Theoretical Computer Science Conference, ITCS 2017, January 9-11, 2017, Berkeley, CA, USA*, volume 67 of *LIPIcs*, pages 7:1–7:31. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017.

[2] B. Applebaum and Y. Moses. Locally computable UOWHF with linear shrinkage. *J. Cryptol.*, 30(3):672–698, 2017.