Erratum

Erratum to “A Novel Multiple-Bits Collision Attack Based on Double Detection with Error-Tolerant Mechanism”

Ye Yuan ^{1,2}, Liji Wu ^{1,2}, Yijun Yang ^{1,2} and Xiangmin Zhang^{1,2}

¹*Tsinghua National Laboratory for Information Science and Technology, Tsinghua University, Beijing 10084, China*

²*Institute of Microelectronics, Tsinghua University, Beijing 10084, China*

Correspondence should be addressed to Liji Wu; lijiwu@tsinghua.edu.cn

Received 24 December 2018; Accepted 25 December 2018; Published 2 May 2019

Copyright © 2019 Ye Yuan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In the article titled “A Novel Multiple-Bits Collision Attack Based on Double Detection with Error-Tolerant Mechanism” [1], there was a missing reference to a conference article by the same authors, which was intended to have been cited in the Introduction. The text reading “Our Contribution. In this paper, we propose a novel multiple-bits collision attack framework. In particular, double distance voting detection (DDVD) and the error-tolerant and check mechanism are presented to ensure the high accuracy” should be updated to “Our Contribution. In [20], we have already proposed a basic side-channel collision attack strategy. On basis of it, we propose a novel multiple-bits collision attack framework in this paper. In particular, double distance voting detection (DDVD) as well as the error-tolerant and check mechanism are presented to ensure the high accuracy.” Moreover, the reference below [2] should be added to the reference list:

In addition, Figure 8 should be replaced with the figure shown below:

- [20] Y. Yuan, L. Wu, X. Zhang and Y. Yang, “Side-channel collision attack based on multiple-bits,” 2017 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID), Xiamen, 2017: pp. 1-5, 2017.

FIGURE 8: Square of difference between each subtrace in set $\{\tilde{t}_1^{mj_1}\}_{j_1=0}^{15}$ and all subtraces in set $\{\tilde{t}_2^{mj_1}\}_{j_1=0}^{15}$.

References

- [1] Y. Yuan, L. Wu, Y. Yang, and X. Zhang, "A novel multiple-bits collision attack based on double detection with error-tolerant mechanism," *Security and Communication Networks*, vol. 2018, Article ID 2483619, 13 pages, 2018.
- [2] Y. Yuan, L. Wu, X. Zhang, and Y. Yang, "Side-channel collision attack based on multiple-bits," in *Proceedings of the 2017 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID)*, pp. 1–5, Xiamen, China, 2017.