IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN XXXX-XXXX, Vol. 0, No. 0, pp. 1–2. DOI:XXXXXXXX

Fault Attacks

Jiahao Xiang[1] and Lang Li[1]

Hengyang Normal University, College of Computer Science and Technology, Hengyang, China

Abstract. TODO: Write an abstract

Keywords: Fault attack

1 Introduction

Widely used primitives like the AES [AES01] do not have perfect security, and can be analysed with linear cryptanalysis [DLNS20], differential cryptanalysis, and a variety of implementation attacks. Among these, fault attacks have emerged as a powerful class of physical attacks that exploit hardware vulnerabilities to induce errors during cryptographic computations. Since the first demonstration of fault attacks on AES, numerous techniques have been developed to recover secret keys by injecting faults and analyzing the resulting faulty ciphertexts [ZZJ+20, SBR+20]. Persistent fault attacks, for example, can compromise the security of AES implementations even in the presence of countermeasures [ZZJ+20]. To address these threats, researchers have proposed various protection mechanisms, such as statistical ineffective fault attack countermeasures [DDE+20]. Despite these advances, fault attacks remain a significant concern for the practical security of AES and other symmetric ciphers, motivating ongoing research into both new attack strategies and robust defenses.

2 Main Result

References

[AES01] Advanced Encryption Standard (AES). National Institute of Standards and Technology, NIST FIPS PUB 197, U.S. Department of Commerce, November 2001.

[DDE+20] Joan Daemen, Christoph Dobraunig, Maria Eichlseder, Hannes Gross, Florian Mendel, and Robert Primas. Protecting against statistical ineffective fault attacks. *IACR TCHES*, 2020(3):508–543, 2020.

[DLNS20] Amit Deo, Benoît Libert, Khoa Nguyen, and Olivier Sanders. Lattice-based E-cash, revisited. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 318–348. Springer, Cham, December 2020.

[SBR+20] Sayandeep Saha, Arnab Bag, Debapriya Basu Roy, Sikhar Patranabis, and Debdeep Mukhopadhyay. Fault template attacks on block ciphers exploiting fault propagation. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part I*, volume 12105 of *LNCS*, pages 612–643. Springer, Cham, May 2020.

[ZZJ+20] Fan Zhang, Yiran Zhang, Huilong Jiang, Xiang Zhu, Shivam Bhasin, Xinjie Zhao, Zhe Liu(0), Dawu Gu, and Kui Ren. Persistent fault attack in practice. *IACR TCHES*, 2020(2):172–195, 2020.