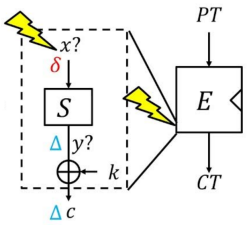
Generalizing SDDT-Based Operation-Skip Fault Analysis to Bitsliced Lightweight Block Ciphers



This thesis aims to investigate the generalizability of the Skip-induced Difference Distribution Table (SDDT) methodology introduced for operation-skip fault analysis in bitsliced cryptographic implementations [1]. The original work demonstrates the approach on the PIPO lightweight block cipher, showing how skipped Boolean operations can produce structured fault-induced differences that can be exploited for differential fault analysis (DFA). Building on this work, the proposed thesis will investigate whether the same methodology can be systematically applied to other bitsliced lightweight block ciphers, such as GIFT, RECTANGLE, or ASCON (the exact target cipher to be determined). The first stage of the project will involve studying and reproducing the SDDT-based analysis for PIPO, followed by the development of a software-based framework capable of modelling operation-skip faults and generating SDDTs for different bitsliced cipher implementations.

The second stage will evaluate the effectiveness of the methodology on the selected cipher. Experiments will systematically investigate the influence of the skipped Boolean operation, fault location, and round on the resulting differential patterns and key-recovery process. The analysis will compare metrics such as the number of faults required for key recovery, remaining key candidates, attack success rate, and computational complexity against the published PIPO results. The goal is to identify common characteristics and differences in the vulnerability of bitsliced lightweight ciphers to operation-skip faults, and to determine to what extent the SDDT-based methodology can be generalized beyond PIPO. The expected outcome is an experimental framework and a comparative security analysis that can provide insight into the relationship between Boolean circuit structure and susceptibility to operation-skip fault attacks.

Practicalities

Promotor:	Prof. Dr. Ir. Vincent Rijmen		
Daily supervisor:	Betul Askin Ozdemir	betul.askinozdemir@esat.kuleuven.be	office B01.05
	Dilara Toprakhisar	dilara.toprakhisar@esat.kuleuven.be	office B01.05
Nature of the work:	50% literature, 50% software		
Number of students:	1		

[1] Dongwoo Kang, Hanbeom Shin, DongHyeon Kim, Seokhie Hong, and HeeSeok Kim. SDDT: An Operation Skip Attack Framework for Bitslice Ciphers – Validated on PIPO. *IACR Cryptol. ePrint Arch.*, 2026:1368, 2026. `https://eprint.iacr.org/2026/1368`.