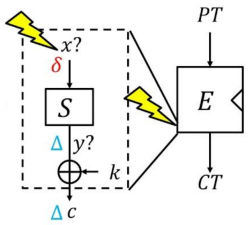
Differential Fault Analysis of Feistel-based Ciphers



Feistel networks are one of the most fundamental structures in symmetric-key cryptography and are widely used in the design of block ciphers due to their simplicity, flexibility, and provable invertibility. Previous research has identified structural properties of Feistel ciphers that enable the construction of distinguishers using different techniques, including differential cryptanalysis, often independently of the specific choice of round function. These results highlight how differences propagate between the left and right branches across multiple rounds, revealing important insights into the diffusion behavior of Feistel constructions. However, comparatively less attention has been given to how these structural properties interact with implementation-level attacks such as fault injections. Since fault attacks introduce controlled faults during the computation of intermediate states, they provide a practical mechanism to observe how differences propagate inside the cipher without relying solely on statistical assumptions.

This proposal aims to study Feistel-based ciphers in the setting of differential fault analysis by combining classical differential techniques with fault injection methods. The research will investigate how injected faults propagate through the Feistel structure and how the resulting differences can be exploited to construct distinguishers or key-recovery attacks on reduced-round variants. Particular attention will be given to identifying structural conditions under which fault-induced differences produce predictable patterns in the final rounds, enabling more efficient recovery of subkey information. The study will analyze how the round structure, number of rounds, and placement of the fault influence attack complexity, and whether combining differential propagation in early rounds with fault-based analysis in later rounds improves efficiency compared to standalone attacks. Analytical findings will be supported by experimental evaluation on representative Feistel constructions. The expected outcome is a deeper understanding of how structural diffusion properties influence vulnerability to differential fault attacks, contributing both to cryptanalytic techniques and to the secure design of Feistel-based symmetric primitives.

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		

 © 2026 – 2027 COSIC