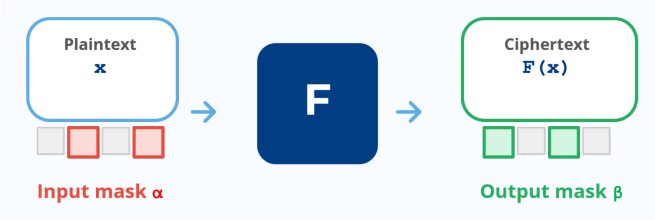
Multidimensional Linear Cryptanalysis of Generalized Feistel Ciphers



Multidimensional linear cryptanalysis extends classical linear cryptanalysis by considering multiple linear approximations simultaneously, enabling stronger distinguishers and more accurate statistical models of cipher behaviour. Recent work has shown that multidimensional techniques can capture structural properties of Feistel-based constructions that remain hidden when analysing single linear approximations. While existing results primarily focus on standard generalized Feistel ciphers (GFC) [1], many modern symmetric-key primitives employ GFC with heterogeneous diffusion layers, including varying branch permutations and round-function placements. These structural differences complicate the derivation of general linear bounds, since the correlation of multidimensional linear approximations depends not only on the round function but also on how masks propagate across branches.

This proposal aims to extend and adapt the multidimensional linear cryptanalysis framework to a broader class of generalized Feistel constructions not previously covered. A central challenge lies in handling the structural diversity among GFC variants. In some designs, round functions are applied to selected branches and their outputs are XORed into multiple target branches, as in Extended Generalized Feistel Networks. Other constructions employ more complex diffusion layers, such as the two-layered permutation strategy used in $\text{GMiMC}_{\text{mrf}}$, which alters how linear masks propagate between rounds. The research will investigate how multidimensional linear attacks behave under different branch permutations and mixing layers across multiple GFC designs. The expected outcome is a set of generalized bounds on linear attack and an improved understanding of how diffusion mechanisms influence resistance against multidimensional linear cryptanalysis of different GFC variants.

[1] Betül Aşkın Özdemir and Vincent Rijmen. Analysis of Diffusion Properties in Generalized Feistel Ciphers under Multidimensional Linear Cryptanalysis. IACR Transactions on Symmetric Cryptology, ToSC 2026, No. 1: 376–409.

Practicalities

Promotor:	Prof. Dr. Ir. Vincent Rijmen
Daily supervisor:	Betul Askin Ozdemir betul.askinozdemir@esat.kuleuven.be office B01.05
Nature of the work:	60% literature, 40% software
Number of students:	1