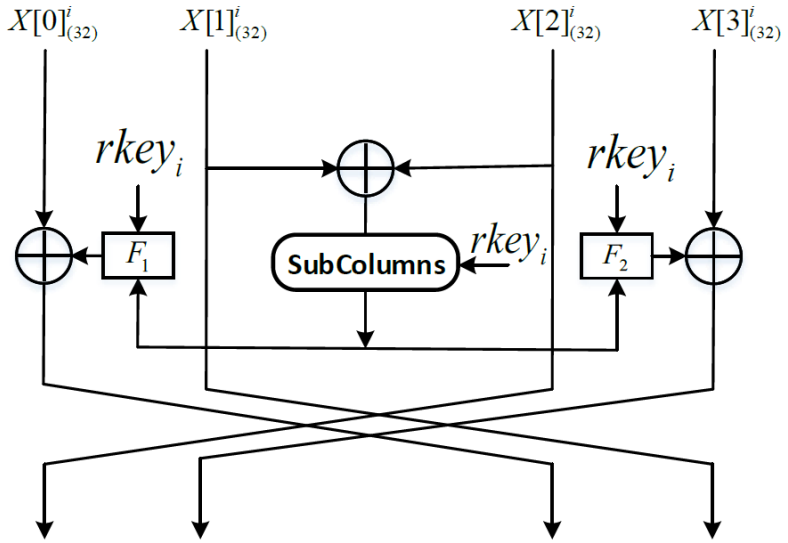
Cryptanalysis of DBST a lightweight block ciphere

Sadegh SADEGHI, Nasour BAGHERI

Frontiers of Computer Science, DOI: 10.1007/s11704-024-3480-y

Problems & Ideas

- A cipher would not be used in the industry unless it was thoroughly tested for security against existing attacks.
- DBST is a recently proposed block cipher.
- A round function of the cipher is as follows:



- Its security has not been evaluated independently so far.
- We aim to shed the light on its security.

Main Contributions

- Contributions:
- We present compelling evidence that challenges the security claims associated with DBST.
- Our analysis reveals significant vulnerabilities within its structure, enabling the identification of distinguishers that can effectively differentiate it from a random permutation with a probability of one, as depicted in the figure.
- These findings starkly contradict the assertions made by the designers of the algorithm.