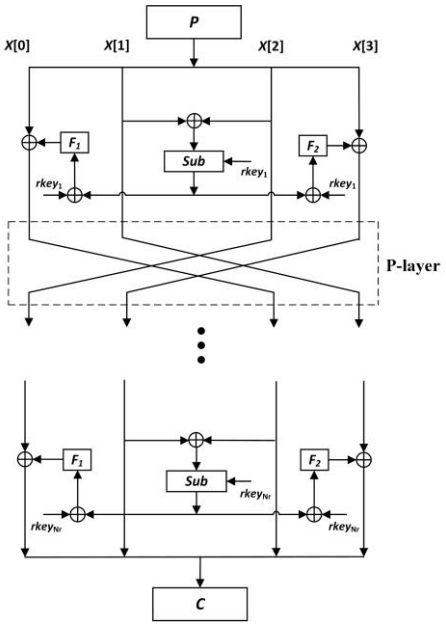
Structure Attack on Full-Round DBST

Chenhao JIA, Qing LING, Ting WU, Tingting CUI

Frontiers of Computer Science, DOI: 10.1007/s11704-024-3438-0

Problems & Ideas

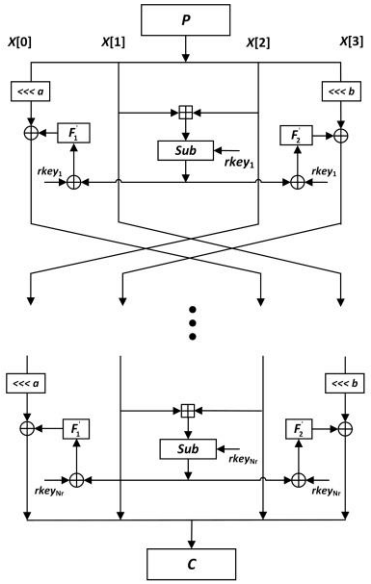
- Problems of original DBST cipher:
  - If the attacker knows one plaintext-ciphertext pair, then he can deduce (2^{64}-1) plaintext-ciphertext pairs without querying encryption engine.
  - The linear part and nonlinear part of DBST are not sufficiently secure to avoid iterative differential characteristics.
- Ideas: Modify DBST both on linear part and nonlinear part and propose a modification version of DBST which can resist all structure attacks.



Encryption process of DBST.

Main Contributions

- Contributions:
  - By finding (2^{64}-1) differential characteristics with probability 1 for full-round DBST, we implement a structure attack on full-round DBST;
  - We find such structure attack is mainly caused by three linear XOR operations in round function located on the first and fourth branches and before Subcolumns operations, and at least one of these XOR operations should be nonlinear;
  - We propose a modification version of DBST, which can resist all structure attacks.



Modification version of DBST (the XOR before Subcolumns is replaced by modulo addition, as well as two bit-rotatioins are added on the firsr branch and the fourth branch).