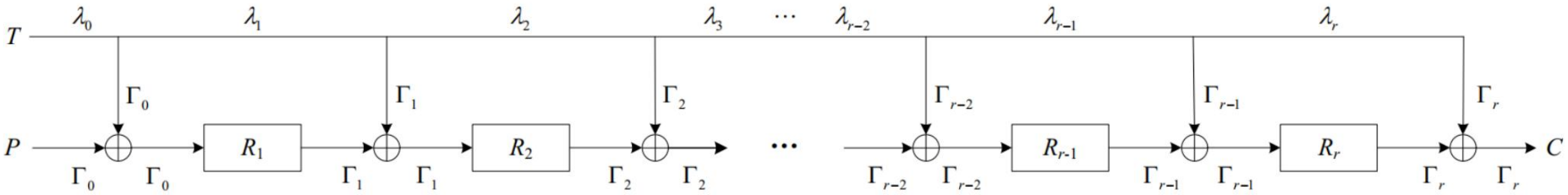
Zero-Correlation Linear Attack on Reduced-Round SKINNY

Yi ZHANG, Ting CUI, Congjun WANG

Frontiers of Computer Science, DOI: 10.1007/s11704-022-2206-2

Problems & Ideas

- Problems of previous zero-correlation linear attack
  - Previous studies ignored the propagation of linear masks in the (twea)-key schedules;
  - There are no clear methods to find zero-correlation linear distinguishers when (twea)key schedules are considered.
- Ideas: Describe the propagation of linear masks in the (twea)key schedule accurately and find the condition to construct zero-correlation linear distinguishers.



This is an example to describe the propagation of linear masks in the (twea)key schedule. Since we establish the relation between the masks in the (twea)key schedule and the masks in round functions, whether a linear hull is zero-correlation linear can be verified in an automatic way.

Main Contributions

- Contributions:
  - A model to search zero-correlation linear distinguishers of AES-like block cipher under related-(twea)key model;
  - A 15-round and a 17-round zero-correlation linear distinguishers of SKINNY-n-2n and SKINNY-n-3n, respectively;
  - A zero-correlation linear attack on 22-round SKINNY-n-2n and 26-round SKINNY-n-3n.

Input plaintext mask	**000000000*00*0
Output mask	000000000000000*
Input tweakey mask	**0**********|| **0**********

15-round zero-correlation linear distinguisher of SKINNY-n-2n

Input plaintext mask	**000000000*00*0
Output mask	000000000000000*
Input tweakey mask	**0**********|| **0**********|| **0**********

17-round zero-correlation linear distinguisher of SKINNY-n-3n

Version	Rounds	Time	Data	Memory
SKINNY-64-128	22	2^{95}	2^{68}	2^{80}
SKINNY-128-256	22	2^{185}	2^{136}	2^{160}
SKINNY-64-192	26	2^{161}	2^{76}	2^{144}
SKINNY-128-384	26	2^{313}	2^{152}	2^{288}

Result of zero-correlation attacks on SKINNY