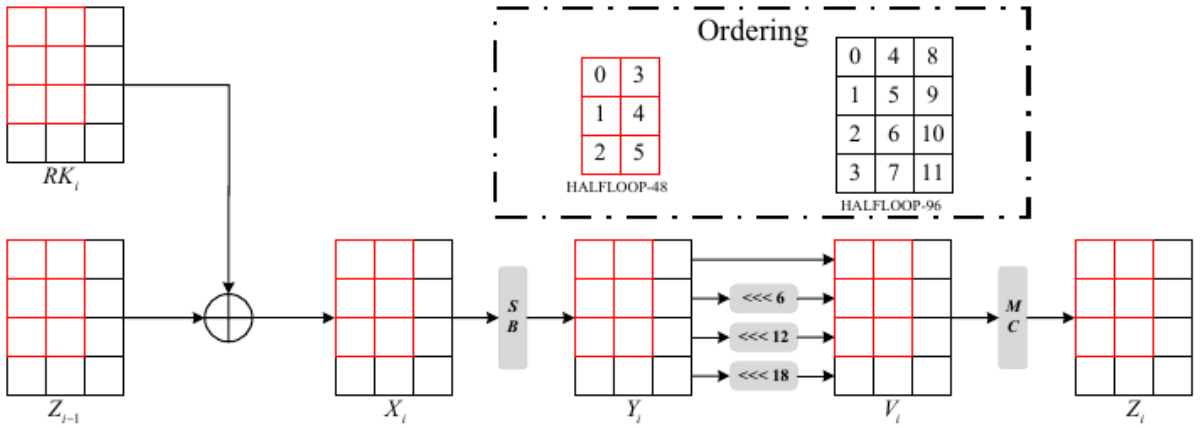
Related-Key Boomerang Attacks on Two Larger Variants of HALFLOOP

Kangkang SHI, Jiongjiong REN, Shaozhen CHEN

Frontiers of Computer Science, DOI: 10.1007/s11704-025-40755-0

Problems & Ideas

- Problems on cryptanalysis of two larger variants of HALFLOOP, standardized by U.S. DoD to encrypt data during ALE:
  - The best attacks are generic without relying on the structure of ciphers.
  - Searching for the stronger non-generic attack is a pending issue to explore design flaws and improve the security.
- Ideas: An evaluation of two larger variants of HALFLOOP against related-key boomerang attacks, since the low diffusion in the key schedule.



The round function of HALFLOOP-48(red) and HALFLOOP-96(black)

Main Contributions

- Contributions:
  - An enhanced model search for sandwich distinguishers of ciphers with non-linear key schedules that combines deriving more constraints to improve efficiency and overcoming the limitations of non-linear key schedule to avoid possible weak-key attacks or invalid trails.
  - Nearly full-round key recovery attacks on HALFLOOP. For HALFLOOP-48, the time complexity is improved compared with other non-generic attacks. For HALFLOOP-96, A 9-round non-weak-key attack is achieved.

Table 1 Summary of analysis results against two larger variants of HALFLOOP. CP = chosen-plaintexts, CPT = chosen-plaintext-tweak, ACC = chosen-plaintexts-and-adaptively-chosen-ciphertexts and CC = chosen-ciphertexts.

Cipher	Attack	Rounds	Data	Time	Memory	Ref.
HALFLOOP-48	Related-Tweak Differential	8	$2^{33.27}$ CP	$2^{92.71}$	$2^{36.85}$	[5]
	Related-Key Differential	10	$2^{47.34}$ CP	$2^{123.91}$	$2^{33.34}$	[5]
	DS-MITM	10	13 CPT	2^{121}Enc. + 2^{122}LUT	$2^{53.6}$	[3]
	Related-Key Boomerang	10	2^{35} ACC	2^{88}	$2^{36.58}$	Sect. 4.2
	TDM-TO	10	2^{65} CPT	2^{65}Enc. + 2^{64}LUT	$2^{70.58}$	[3]
HALFLOOP-96	DS-MITM	7	15 CPT	$2^{113.3}$Enc. + 2^{114}LUT	2^{105}	[3]
	Related-Key Boomerang	8	2^{82} ACC	$2^{82.58}$	$2^{46.12}$	Sect. 5.2
	Related-Key Differential†	9	$2^{92.96}$ CP	$2^{92.96}$	$2^{56.96}$	[4]
	Related-Key Rectangle	9	2^{87} CC	2^{102}	$2^{107.17}$	Sect. 5.3
	TDM-TO	10	2^{64} CPT	2^{64}Enc. + 2^{64}LUT	$2^{70.58}$	[3]

† It only retrieves 38.77 bits of equivalent key information and it is a weak-key attack which is effective against only 2^{94} key pairs with a specified difference.