Chosen-Key Distinguishers on 12-Round Feistel-SP and 11-Round Collision Attacks on Its Hashing Modes

Xiaoyang Dong and Xiaoyun Wang

Shandong University, Tsinghua University

FSE 2017
Tokyo, Japan

Outline

1. Attack Modes
2. Chosen-Key Attacks
3. Feistel-SP Based Block Ciphers
4. Rebound Attack
5. Hashing Modes: PGV s
6. Collision Attacks

Secret-key and Open-key Models

- Secret-key model
  - the key is random and secret
  - the attacker tries to recovery the key or distinguish from random permutation
- Open-key model
  - known-key, the key is known to the attacker, proposed by Knudsen and Rijmen in ASIACRYPT 2007
  - chosen-key, the key is under the control of the attacker
  - the attacker tries to exhibit some non-ideal property of the primitive

Previous works of chosen-key attacks

Biryukov et al [CRYPTO 2009]	Full AES-256
Lamberger et al [ASIACRYPT 2009]	Full Whirlpool CP func
Gilbert and Peyrin [FSE 2010]	AES-like permutations
PA Fouque et al [CRYPTO 2013]	9-r AES-128
Nikolić et al [ICISC 2010]	Feistel and SPN
Minier et al. [FSE 2011]	Generalized Feistel
Sasaki and Yasuda [FSE 2011]	Feistel-SP and MMO MP
Sasaki et al [ACISP 2012]	Camellia
Sasaki et al [INDOCRYPT 2012]	Double SP-functions

Known-key attacks

Our attacks

- Knudsen and Rijmen (ASIACRYPT 2007)
  - ✓ 7-round Feistel Known-key Distinguisher
  - ✓ 7-round half-collision on hashing modes

➢ Arbitrary Round Function

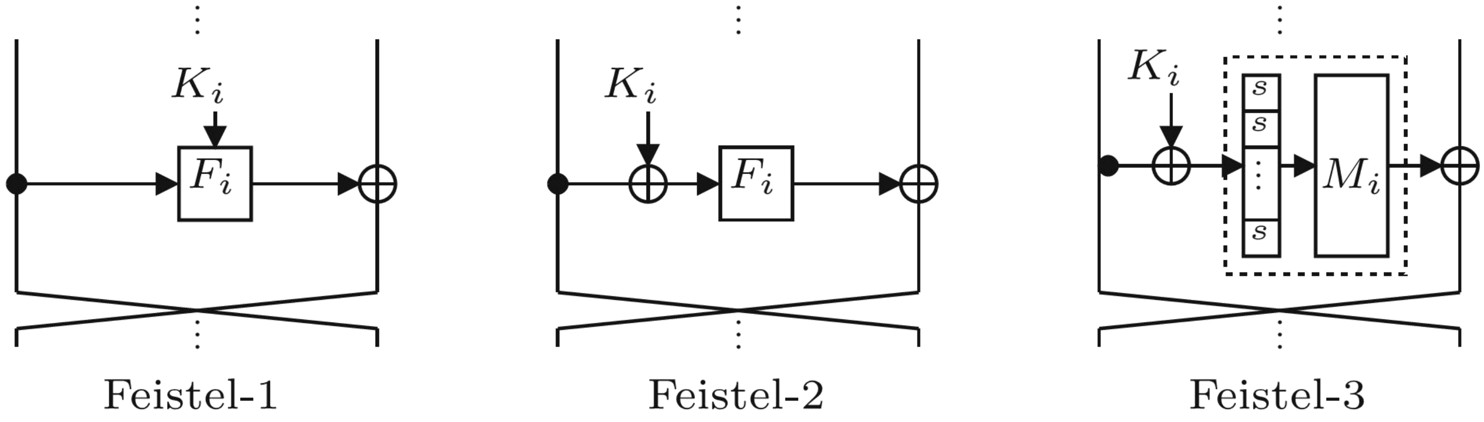
- Sasaki and Yasuda (FSE 2011)
  - ✓ 11-round Feistel Known-key Distinguisher
  - ✓ 9-round full-collision on hashing modes

➢ SP Round Function

- Our works
  - ✓ 12-round Feistel Chosen-key Distinguisher
  - ✓ 11-round full-collision on hashing modes

Classification of Feistels by Round Function

- Isobe and Shibutani [AC 2013] divide Feistels into three types



- Feistel-3 is also called Feistel-SP

Feistel-SP Round Functions

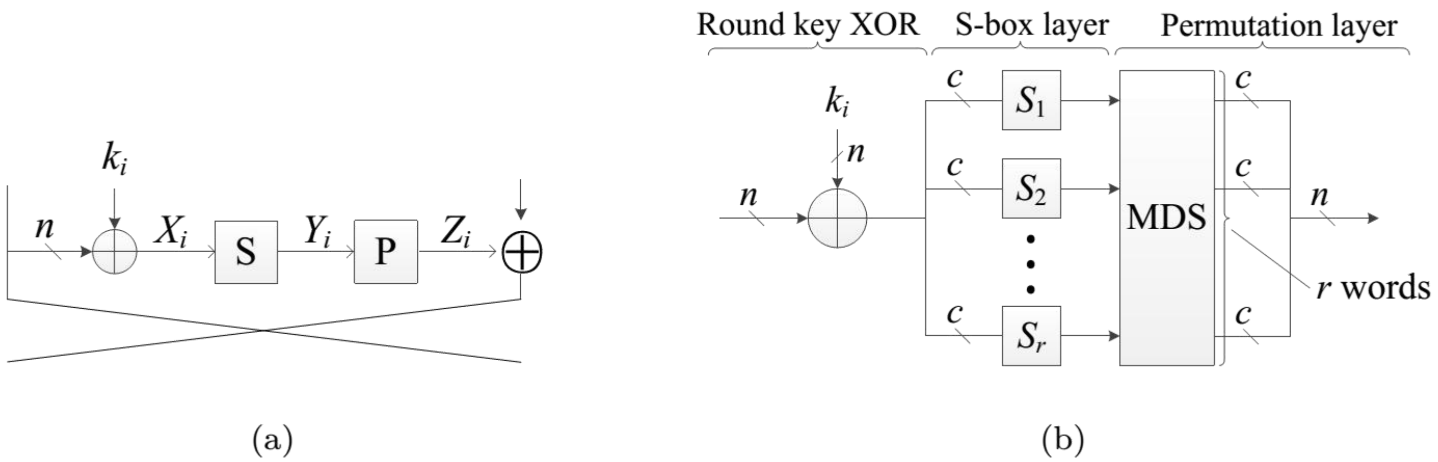
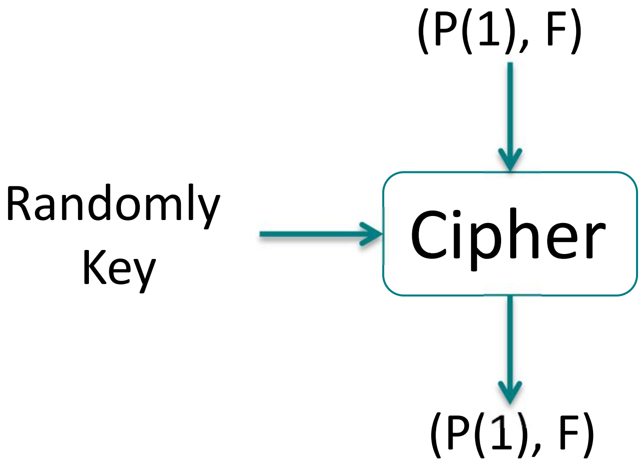


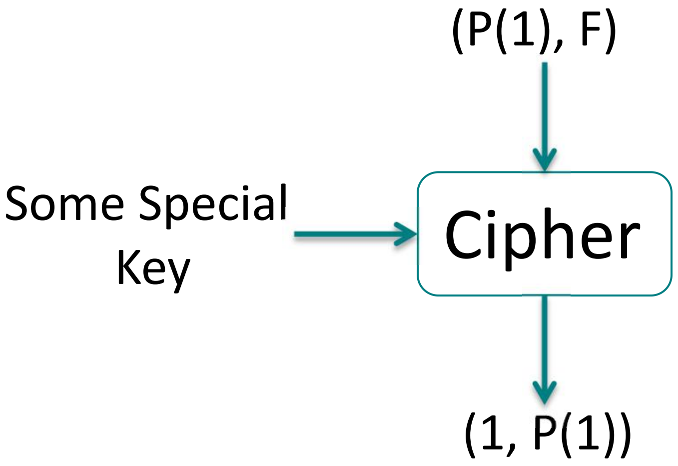
Figure 1: (a) One Round of Feistel-SP block cipher, (b) Detailed Description of the Round Function

Permutation is assumed to be MDS: Maximum distance separable

Known-key and Chosen-key Distinguisher



Sasaki and Yasuda's Known-key Distinguisher

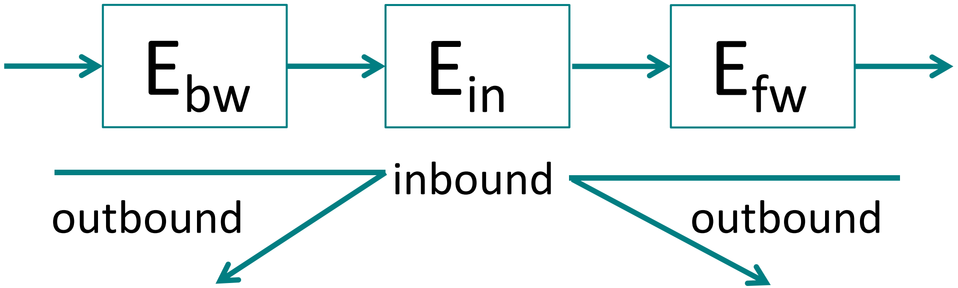


Our Chosen-key Distinguisher

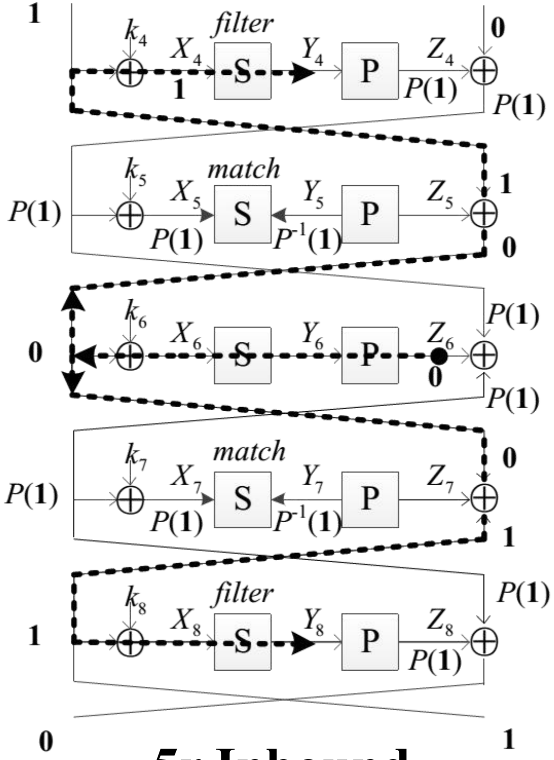
Common: find such a pair for the Feistel network faster than we do for a random permutation

Basic Technique: Rebound Attack

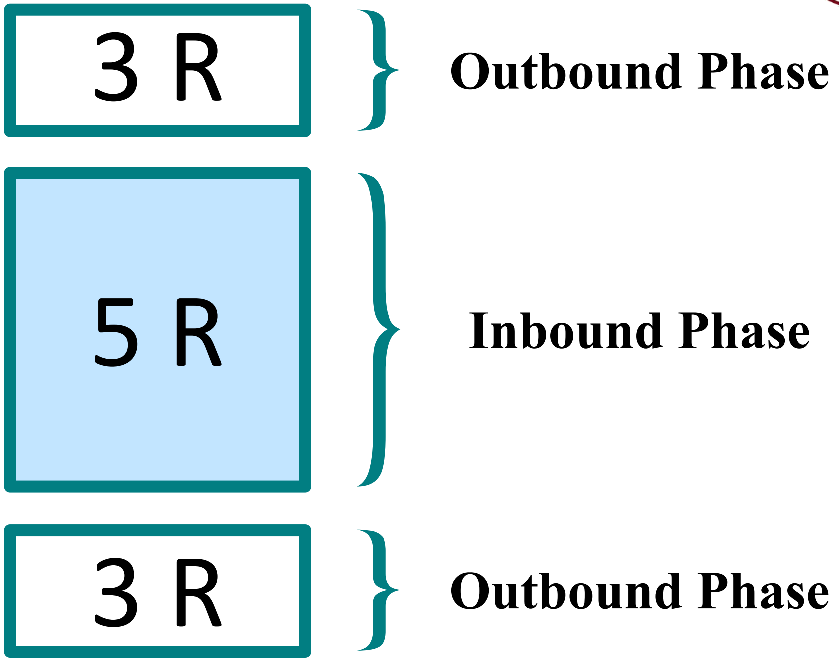
- Rebound attack, proposed by Mendel et al.
- Find pairs meet certain truncated differential
  - Inbound phase: a MITM phase that generate pairs meet the truncated differential in E_{in} in low time
  - Outbound phase: pairs generated in Inbound propagate forward and backward to match the full path
- First of all, find a proper path



Sasaki and Yasuda's work

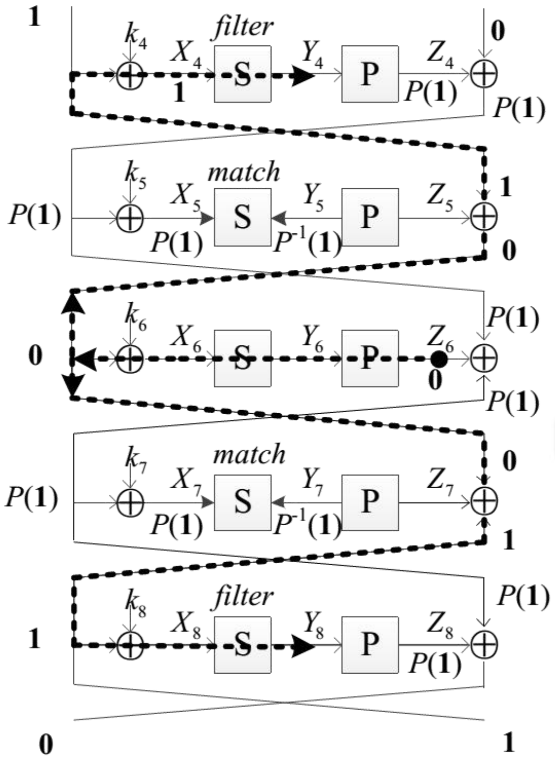


5r Inbound



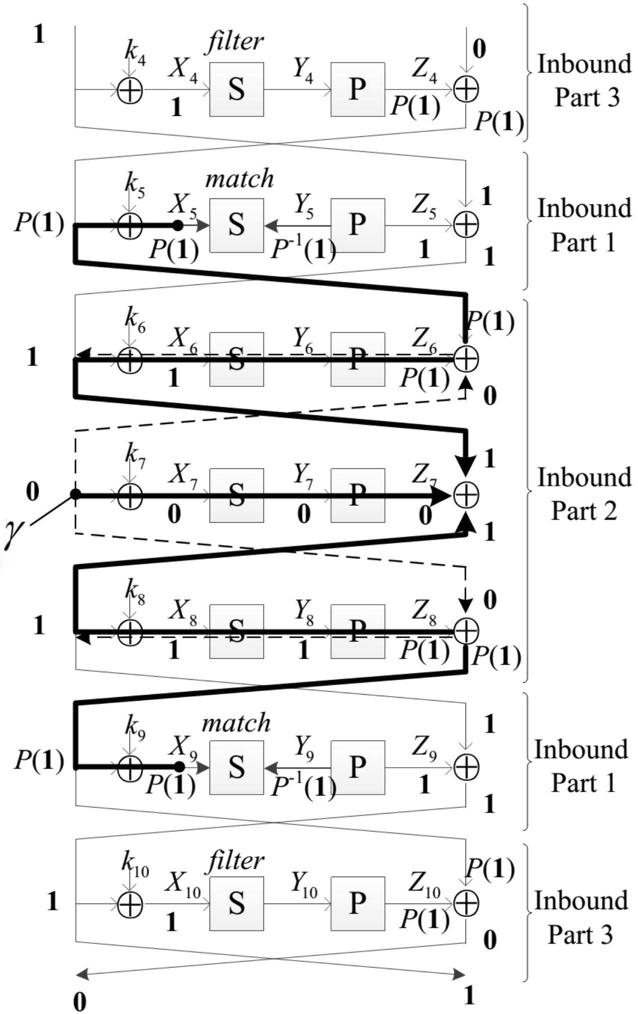
11r Known-key Distinguisher

Our works



5r Inbound

Find a 7r Inbound



Our work

- The equation makes 7r inbound phase right

Only γ is unknwon

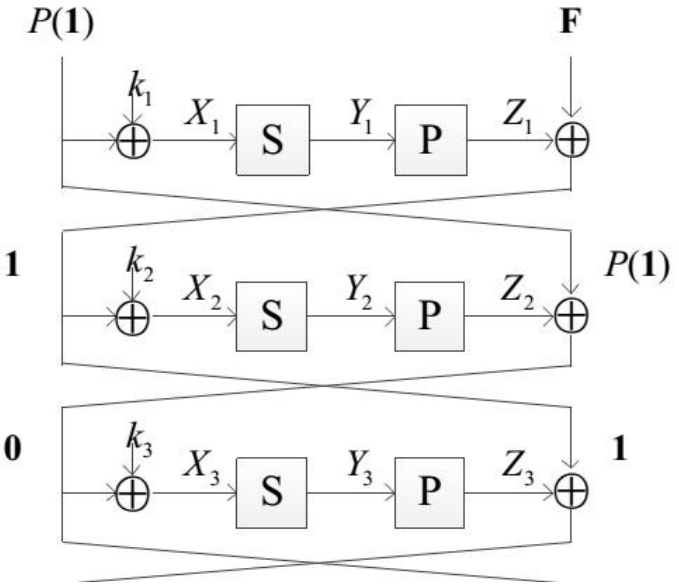
$$S^{-1}(\underline{P^{-1}(X_5 \oplus k_5 \oplus \gamma)}) \oplus k_6 \oplus S^{-1}(\underline{P^{-1}(X_9 \oplus k_9 \oplus \gamma)}) \oplus k_8 = P(S(\gamma \oplus k_7))$$

- One must find γ to make it right
  - if we find it by traversing it, it costs 2^{64} ✗
  - **Our Idea:** suppose the underlined are equal, γ is find immediately
  - In fact, we only choose key to make the underlined equal partially, i.e.

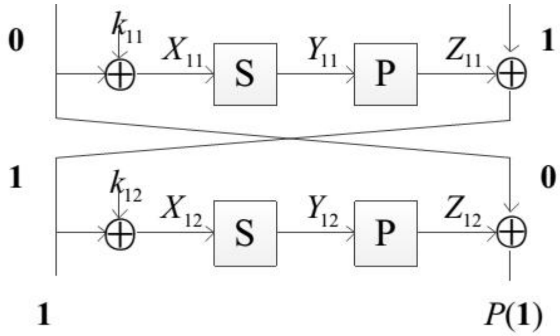
$$(0,0,0,0,0,0,*,*) \oplus k_6 \oplus k_8 = P \circ S(\gamma \oplus k_7)$$

  - Thus we tranverse only 2 bytes to get γ, cost 2^{16}

Our works



3r Outbound phase

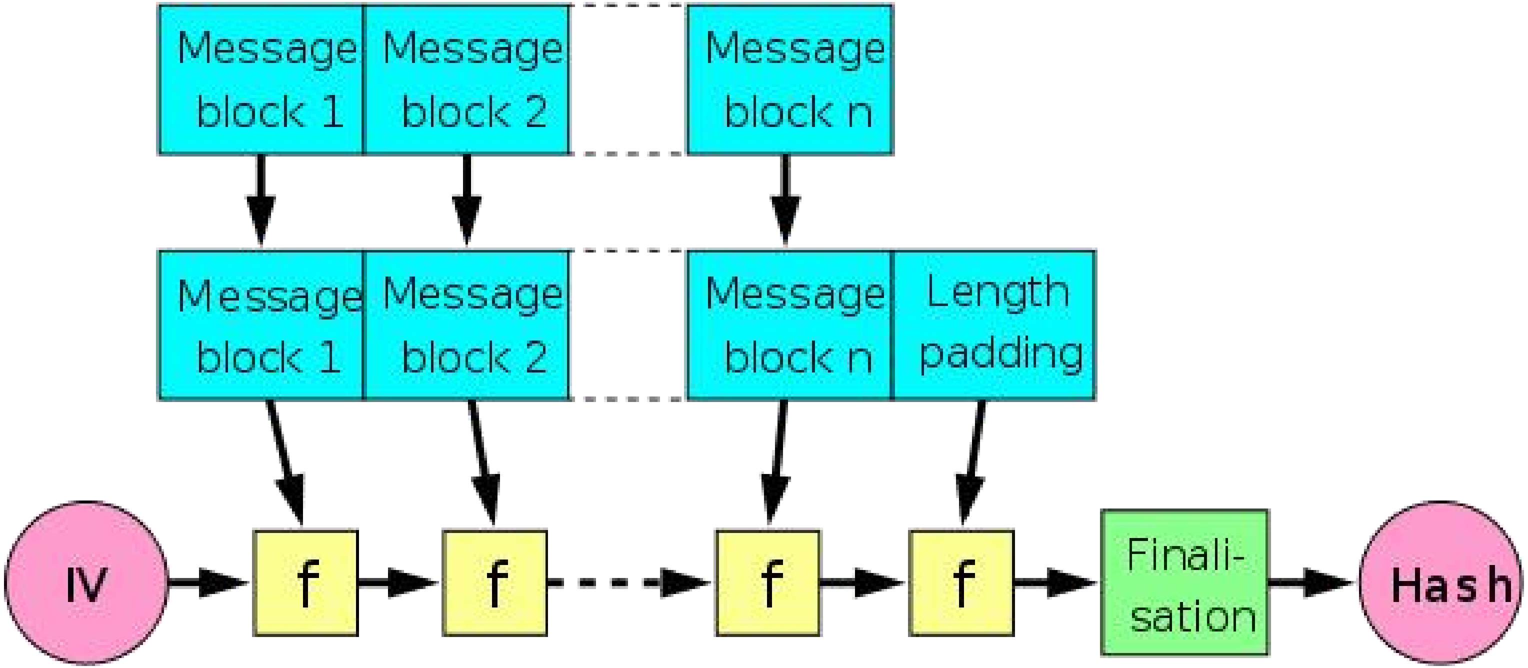


2r Outbound phase

- **We get a 12r Chosen-key Distinguisher**

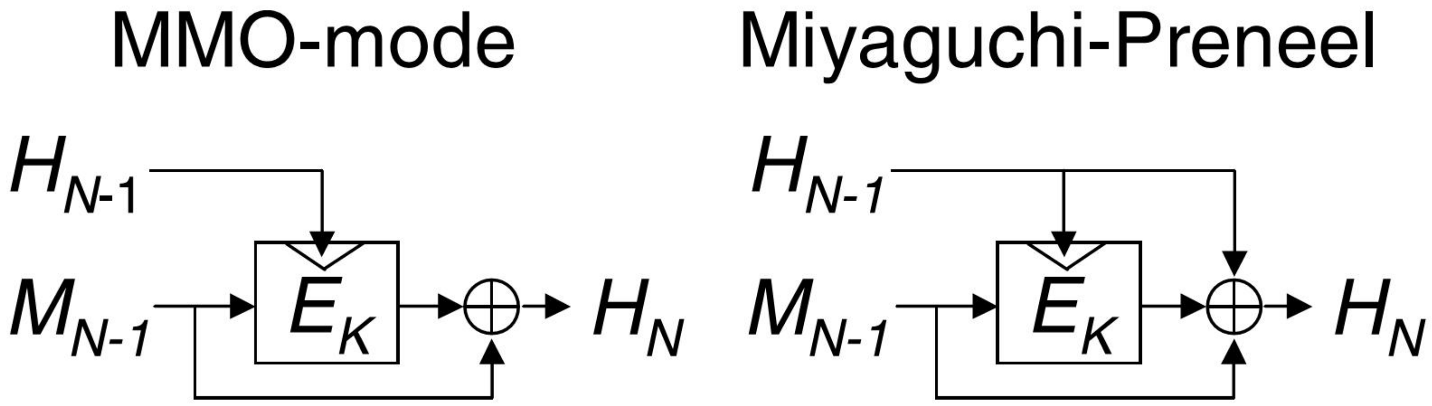
- Application to Hashing Modes

Merkle–Damgård Hash

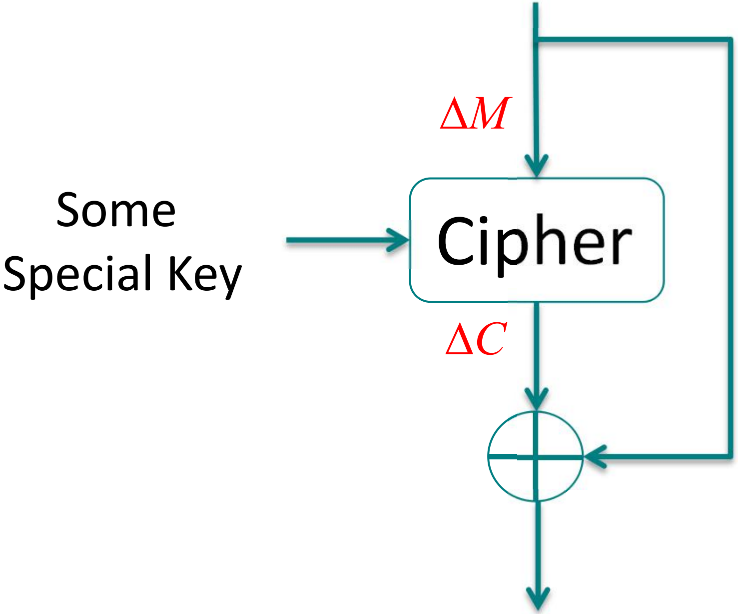


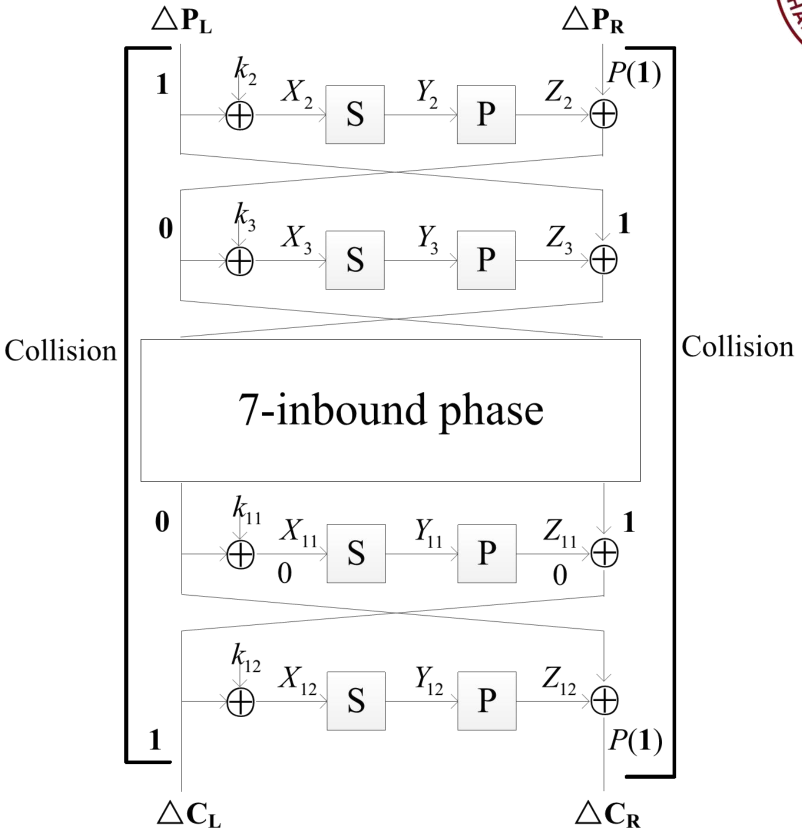
Hashing modes (PGV modes)

- apply to MMO-mode and Miyaguchi-Preneel modes
- keys are the chaining value or IV



Collision: Compression Function

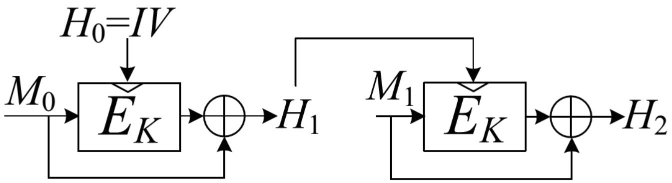


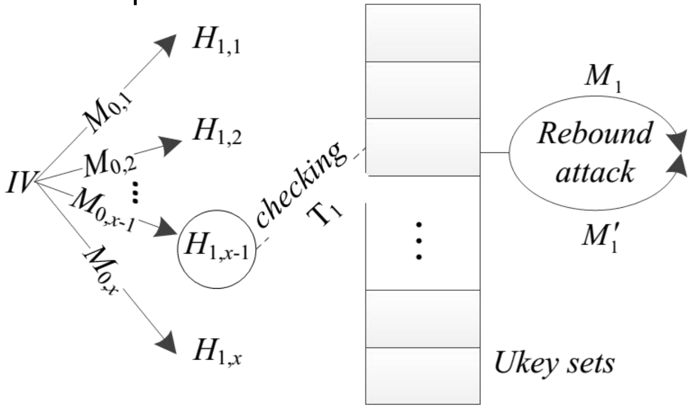


11r Feistel-SP Cipher

Collision: Hash Function

- Translate the collision of Compression Function to Hash
  - Using two blocks to generate collision in H2
  - Rebound attack is in the 2nd block
    - Prepare all (H_1,M_1,M_1'), H_1 as key, that meet the truncated differential
  - Randomly pick M_0, compute H_1, check H_1





计算7轮inbound的起点

Algorithm 1 Calculate Starting Point by the 7-round Inbound Phase

Phase A: Prepare DDTs for all S-boxes.

(a) Choose an active-byte position j for differential $\mathbf{1}$.

(b) **Inbound Part 1:** For 2^c differences of ΔY_4, compute the corresponding ΔX_5 after applying the (forward) permutation layer. For each of the 2^c differences of ΔZ_5, compute the corresponding full-byte difference ΔY_5 after applying the inverse permutation layer, and check whether ΔX_5 matches ΔY_5 by looking up the DDTs. If we pass the check, go to the following steps.

(c) **Inbound Part 1:** For 2^c differences of ΔY_{10}, compute the corresponding ΔX_9 after applying the (forward) permutation layer. For all 2^c differences of ΔZ_9, compute the corresponding full-byte differences ΔY_9 after applying the inverse permutation layer, and check whether ΔX_9 matches ΔY_9 by looking up the DDTs. If we pass the check, go to the next step.

(d) For the matched pairs $(\Delta X_5, \Delta Y_5)$ and $(\Delta X_9, \Delta Y_9)$, we get values (X_5, X_5'), (X_9, X_9') and store values $(P^{-1}(X_5 \oplus X_9), j, X_5, X_5', X_9')$ in a table $\mathcal{T}$.

Phase B:

(i) Randomly choose a master key, and get all the subkeys by the key schedule.

(ii) Check table $\mathcal{T}$ to determine whether the master key belongs to one of the $Ukey$ sets, if it passes the check, go to the next step; else go to step (i) to choose another master key.

(iii) Calculate γ through Eq. (9) (note that the positions of the two unknown bytes may be changed corresponding to the 6-element-array determined in step (ii).) and Eq. (5).

(iv) Follows the dashed lines, we calculate $\Delta X_6 = S^{-1}(P^{-1}(X_5 \oplus k_5 \oplus \gamma)) \oplus S^{-1}(P^{-1}(X_5' \oplus k_5 \oplus \gamma))$ and $\Delta X_8 = S^{-1}(P^{-1}(X_9 \oplus k_9 \oplus \gamma)) \oplus S^{-1}(P^{-1}(X_9' \oplus k_9 \oplus \gamma))$. If $\Delta X_6 = \Delta X_8$, then go to the next step; else go to step (i) to choose another master key.

(v) Calculate $X_6 = S^{-1}(P^{-1}(X_5 \oplus k_5 \oplus \gamma))$ and X_6', X_8, X_8' similarly. Then calculate $X_4 = k_4 \oplus P(S(X_5)) \oplus X_6 \oplus k_6$ and X_4', X_{10}, X_{10}', similarly. Then check the following two equations. If these two hold, we get a starting point under the chosen key; else go to step (i) to choose another master key.

$$S_j(X_4[j]) \oplus S_j(X_4'[j]) \overset{?}{=} \Delta Y_4[j] \tag{11}$$

$$S_j(X_{10}[j]) \oplus S_j(X_{10}'[j]) \overset{?}{=} \Delta Y_{10}[j] \tag{12}$$

Experiment

- We replace the linear permutation of Camellia by block cipher Khazad' MDS [BR00], called Camellia-MDS in following, to give an experiment

$$P = \begin{pmatrix} \text{0x01} & \text{0x03} & \text{0x04} & \text{0x05} & \text{0x06} & \text{0x08} & \text{0x0B} & \text{0x07} \\ \text{0x03} & \text{0x01} & \text{0x05} & \text{0x04} & \text{0x08} & \text{0x06} & \text{0x07} & \text{0x0B} \\ \text{0x04} & \text{0x05} & \text{0x01} & \text{0x03} & \text{0x0B} & \text{0x07} & \text{0x06} & \text{0x08} \\ \text{0x05} & \text{0x04} & \text{0x03} & \text{0x01} & \text{0x07} & \text{0x0B} & \text{0x08} & \text{0x06} \\ \text{0x06} & \text{0x08} & \text{0x0B} & \text{0x07} & \text{0x01} & \text{0x03} & \text{0x04} & \text{0x05} \\ \text{0x08} & \text{0x06} & \text{0x07} & \text{0x0B} & \text{0x03} & \text{0x01} & \text{0x05} & \text{0x04} \\ \text{0x0B} & \text{0x07} & \text{0x06} & \text{0x08} & \text{0x04} & \text{0x05} & \text{0x01} & \text{0x03} \\ \text{0x07} & \text{0x0B} & \text{0x08} & \text{0x06} & \text{0x05} & \text{0x04} & \text{0x03} & \text{0x01} \end{pmatrix}$$

Find a pair has the following differential

P1 = (1f 17 7f 72 7a f5 37 53, 5f f4 d9 23 59 e0 e6 75)

P2 = (8a b5 11 89 23 29 49 9f, a1 9e 90 58 02 e8 fa 25)

key = (69 e4 4a 60 1e ea 50 20, 0a 3b 81 ae ad 3a 79 bc)

Differential of the Experiment Pair for 12-Round *Chosen-Key* Distinguisher

	Input Differences of Each Round	
1st Round	95 a2 6e fb 59 dc 7e cc	fe 6a 49 7b 5b 08 1c 50
2nd Round	32 00 00 00 00 00 00 00	95 a2 6e fb 59 dc 7e cc
3rd Round	00 00 00 00 00 00 00 00	32 00 00 00 00 00 00 00
4th Round	32 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
5th Round	02 06 08 0a 0c 10 16 0e	32 00 00 00 00 00 00 00
6th Round	a9 00 00 00 00 00 00 00	02 06 08 0a 0c 10 16 0e
7th Round	00 00 00 00 00 00 00 00	a9 00 00 00 00 00 00 00
8th Round	a9 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
9th Round	02 06 08 0a 0c 10 16 0e	a9 00 00 00 00 00 00 00
10th Round	51 00 00 00 00 00 00 00	02 06 08 0a 0c 10 16 0e
11th Round	00 00 00 00 00 00 00 00	51 00 00 00 00 00 00 00
12th Round	51 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
13th Round	a2 fb b2 10 eb 79 82 49	51 00 00 00 00 00 00 00

†: all the numbers are in hexadecimal.

Case (N,c)†	Rounds	Time	Memory	Power	Source
(128,8)	7	–	–	known-key distinguisher	[BKN09]
	11	2^{19}	2^{19}	known-key distinguisher	[SEHK12]
	12	2^{38}	2^{35}	chosen-key distinguisher	Section 3.2
	7	–	–	half-collision‡	[BKN09]
	9	2^{27}	2^{27}	full-collision	[SEHK12]
	11	$2^{48.6}$	2^{27}	full-collision	Section 3.3
(128,4)	7	–	–	known-key distinguisher	[BKN09]
	11	2^{12}	2^{12}	known-key distinguisher	[SY11]
	12	2^{34}	$2^{38.9}$	chosen-key distinguisher	Section 4.1
	7	–	–	half-collision	[BKN09]
	9	2^{24}	2^{24}	full-collision	[SEHK12]
	11	2^{44}	$2^{30.9}$	full-collision	Section 4.1
(64,8)	7	–	–	known-key distinguisher	[BKN09]
	9	2^{19}	2^{19}	known-key distinguisher	[SY11]
	7	–	–	half-collision	[BKN09]
	7	2^{24}	2^{24}	full-collision	[SEHK12]
(64,4)	7	–	–	known-key distinguisher	[BKN09]
	11	2^{11}	2^{11}	known-key distinguisher	[SY11]
	12	2^{18}	2^{19}	chosen-key distinguisher	Section 4.2
	7	–	–	half-collision	[BKN09]
	9	2^{16}	2^{16}	full-collision	[SEHK12]
	11	$2^{24.2}$	2^{15}	full-collision	Section 4.2

Thank you