Known-Key Distinguishers on 11-Round Feistel and Collision Attacks on Its Hashing Modes

Yu Sasaki and Kan Yasuda
NTT Corporation, Japan

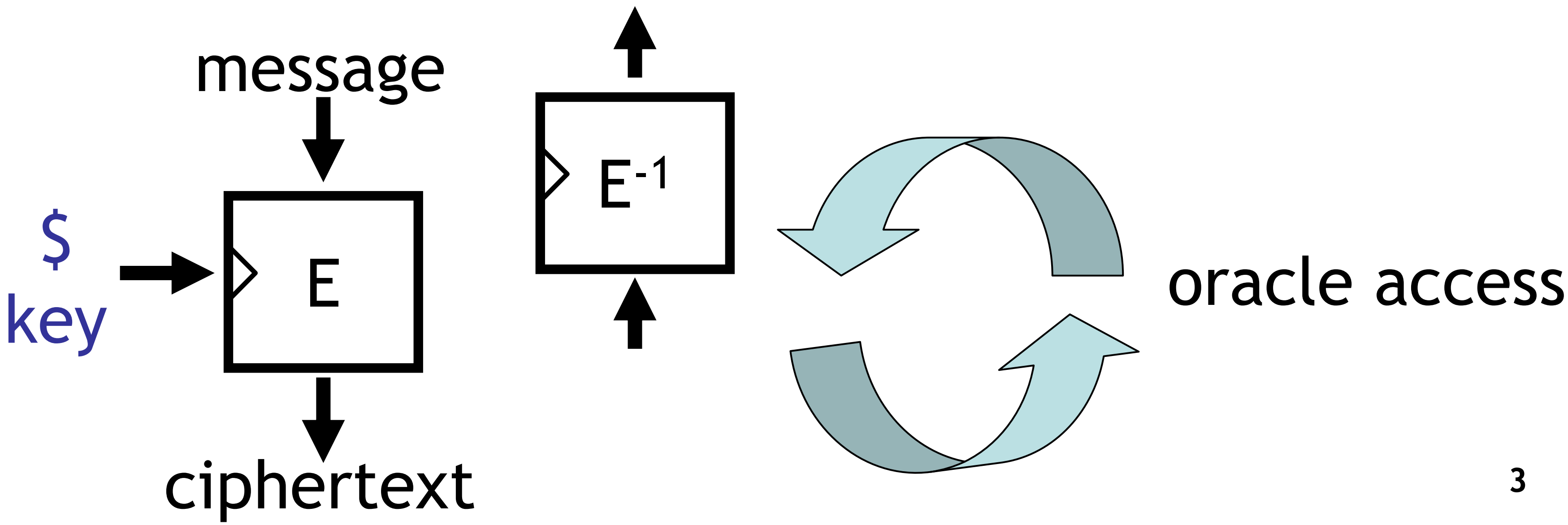
FSE 2011
Lyngby, Denmark
Feb. 16, 2011

Outline

1. Known-key attacks on block ciphers
2. Our attacks on 11-round Feistel cipher
3. Our attacks on Its hash functions

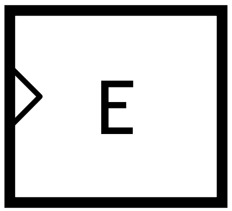
Secret-key security

- A key is chosen random and kept secret
- Given oracle access, an adversary tries to recover the key or distinguish from random permutation



Known-key security

- A key is chosen random and revealed
- An adversary tries to find "something different" from random permutation
- No oracle access needed



(description of the cipher algorithm)

$
key

Key value given to adversary

Previous work of known-key attacks

- Introduced by Knudsen and Rijmen [AC2007] — 7R AES, 7R Feistel
- Mendel et al. [SAC2009] — 7R AES
- Minier et al. [Africacrypt 2009] — Rijndael
- Gilbert and Peyrin [FSE2010] — 8R AES
- Bouillaguet et al. [SAC2010] — Generalized Feistel
- Sasaki' [IWSEC 2010] — Rijndael
- Nikolic et al. [ICISC 2010] — several ciphers
- Minier et al. [FSE 2011] — Generalized Feistel

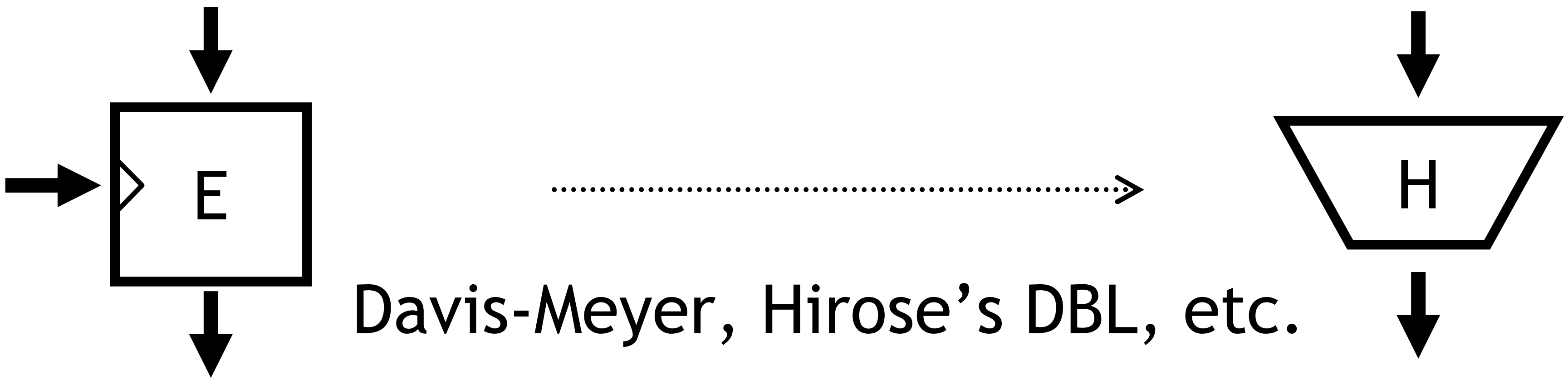
. . . Many attacks published

Formalization of known-key attacks

- Raised as an open problem by Knudsen and Rijmen
- Previous work only partially succeeded [Minier et al. 2009]
- Seems quite difficult to formalize the notion of known-key attacks in its generality

"Sufficient condition"

- Known-key attacks may be meaningful when used in hashing modes
- Meaningful if meaningful in a hash setting (collision, preimage, etc.)



Outline

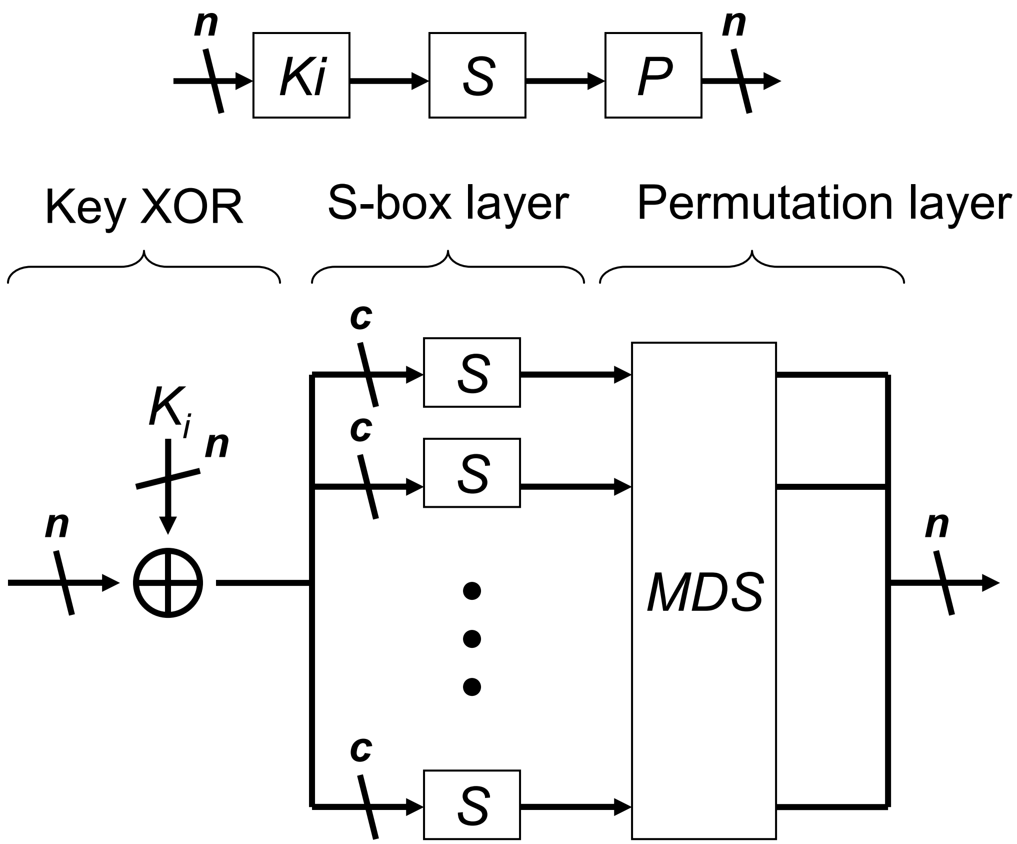
1. Known-key attacks on block ciphers
2. Our attacks on 11-round Feistel cipher
3. Our attacks on Its hash functions

Our results

- Previous best attack: 7R Feistel

  [Knudsen and Rijmen, AC2007]
- Our new attack: 11R Feistel
- Difference in round functions
  - AC2007 assumed key xor followed by an arbitrary function
  - We assume key xor followed by an SP function

SP round function



Assume “good” S-boxes

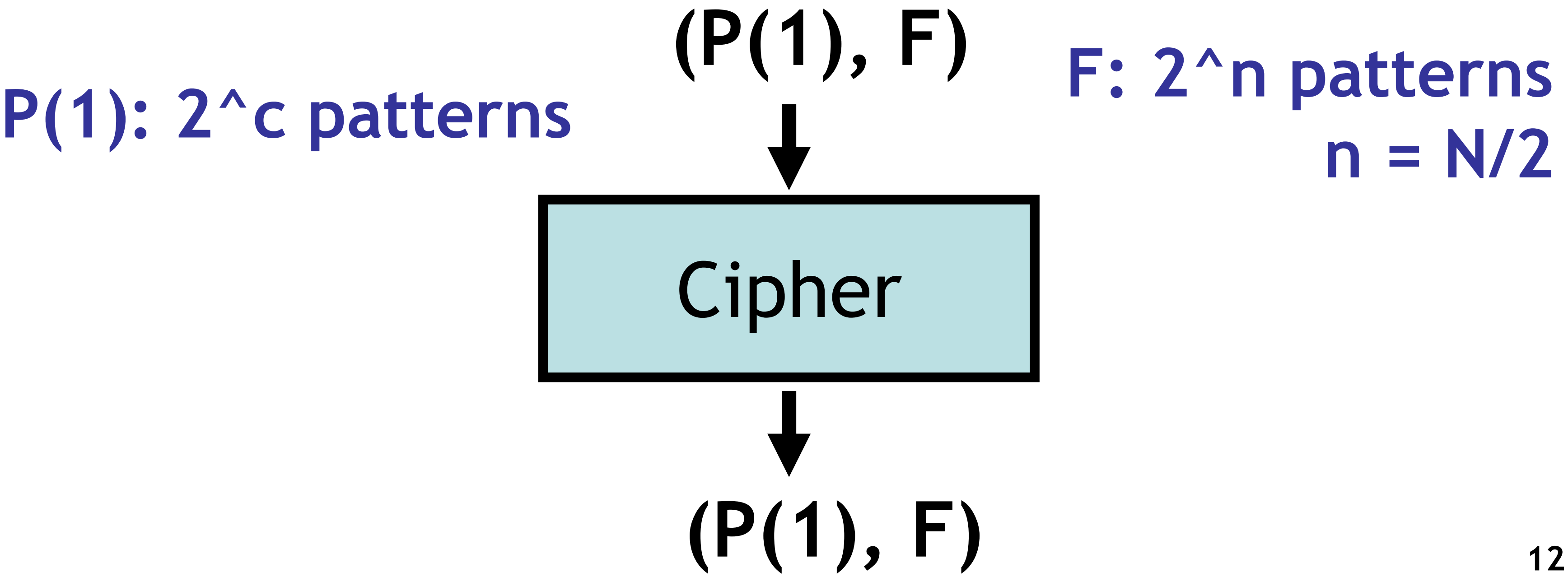
n: half the block size
c: byte size
MDS: Maximum distance separable

Attack strategy

- Find a message pair having a specific truncated difference such that the corresponding ciphertext pair also has the same truncated difference
- We can find such a pair for the Feistel network faster than we do for a random permutation

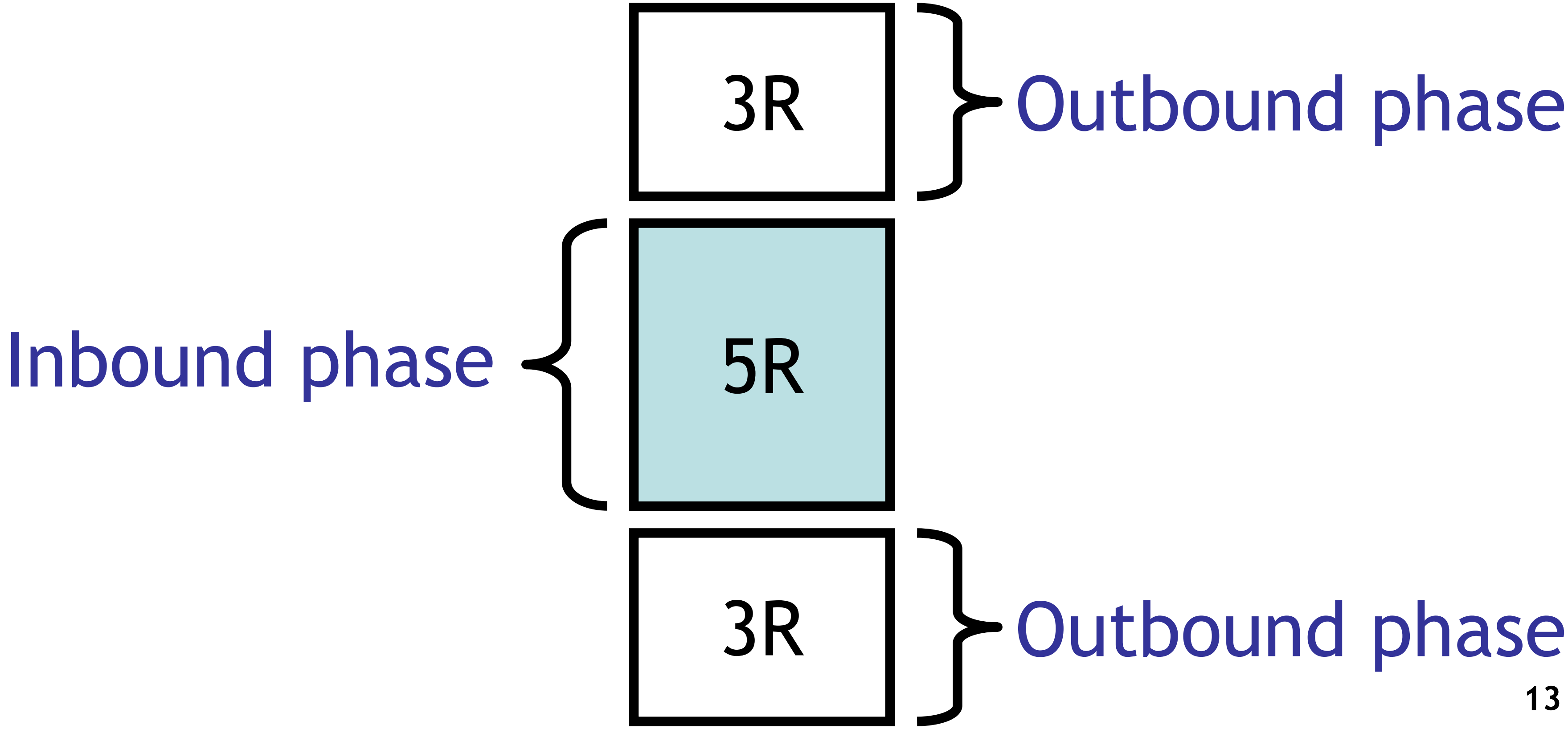
Attack parameters

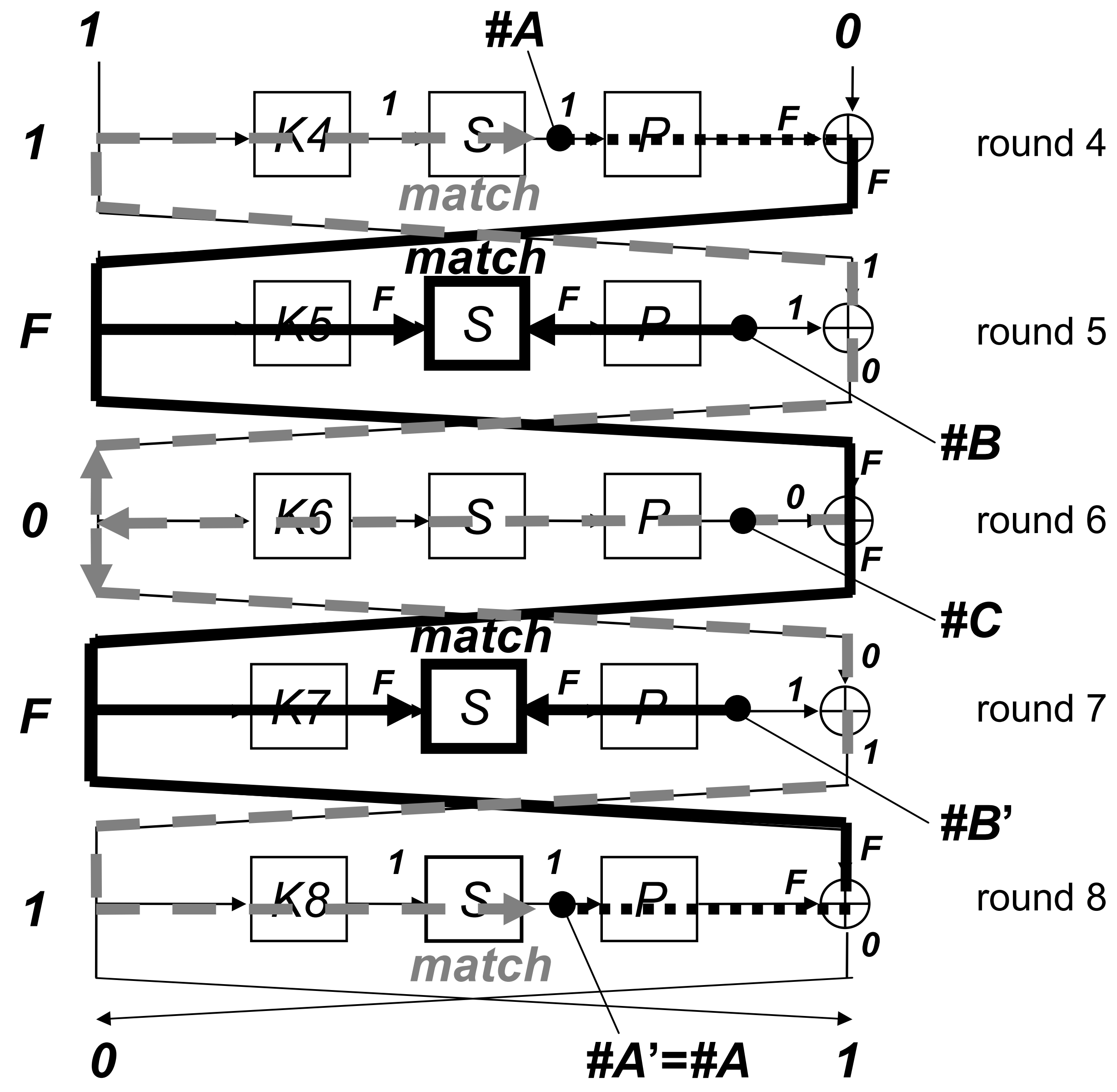
- Block size N = 128 bit with byte size c = 4 or 8 bit S-boxes
- Block size N = 64 bit with byte size c = 4 bit S-boxes
- We use the truncated difference (P(1), F)



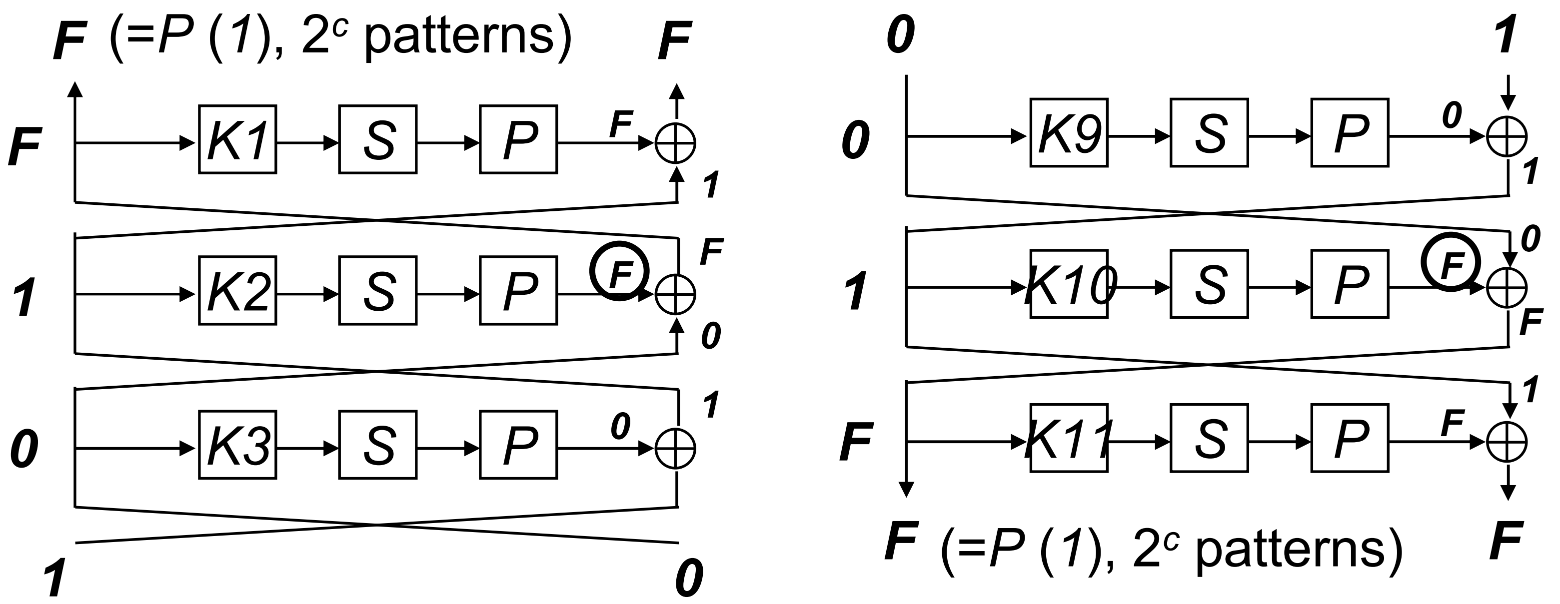
Attack techniques

- Based on the rebound attack developed by Mendel et al. [FSE 2009]




1
#A
0
1
K4
1
S
1
P
F
F
match
round 4
match
F
K5
F
S
F
P
1
1
0
round 5
#B
0
K6
S
P
0
F
F
round 6
#C
match
F
K7
F
S
F
P
1
0
1
round 7
#B'
1
K8
1
S
1
P
F
F
0
match
round 8
0
#A'=#A
1

and here is the outbound.



Outbound differential path satisfied with a probability 1

Outline

1. Known-key attacks on block ciphers

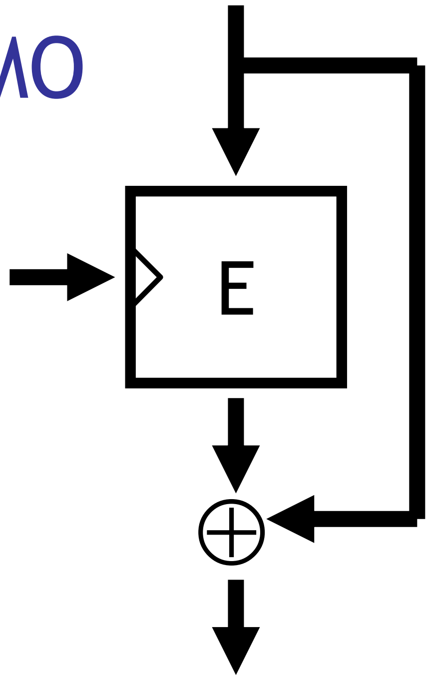
2. Our attacks on 11-round Feistel cipher

3. Our attacks on Its hash functions

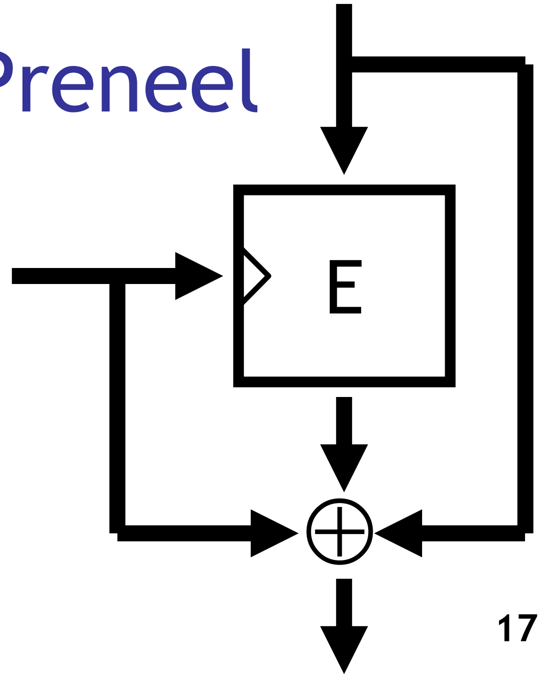
Application to hashing modes

- Can be applied to **Matyas-Meyer-Oseas (MMO)** and **Miyaguchi-Preneel** modes
- The key value corresponds to chaining variable or to IV

MMO

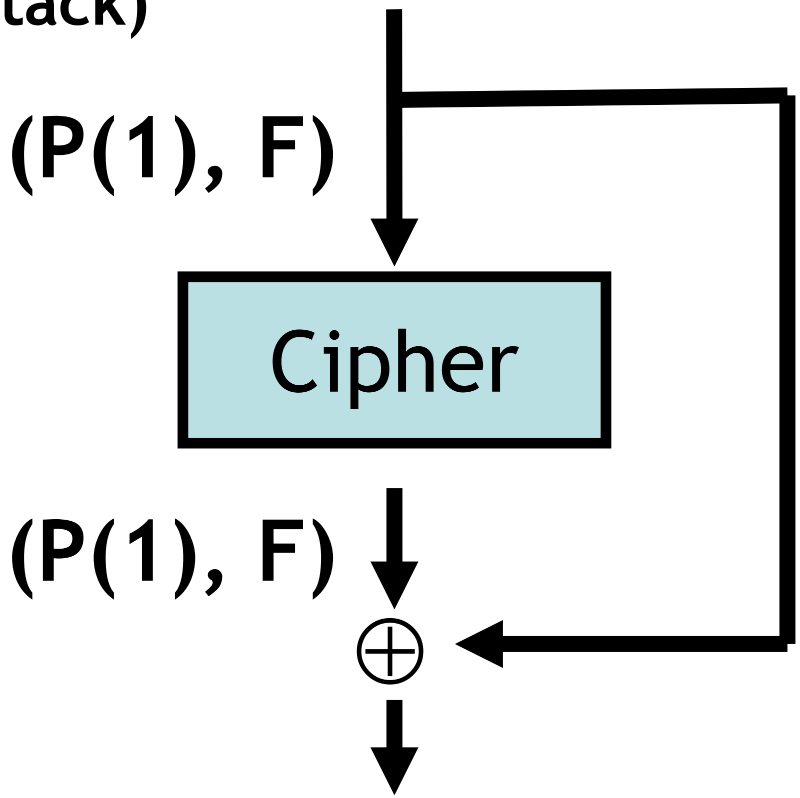


Miyaguchi-Preneel



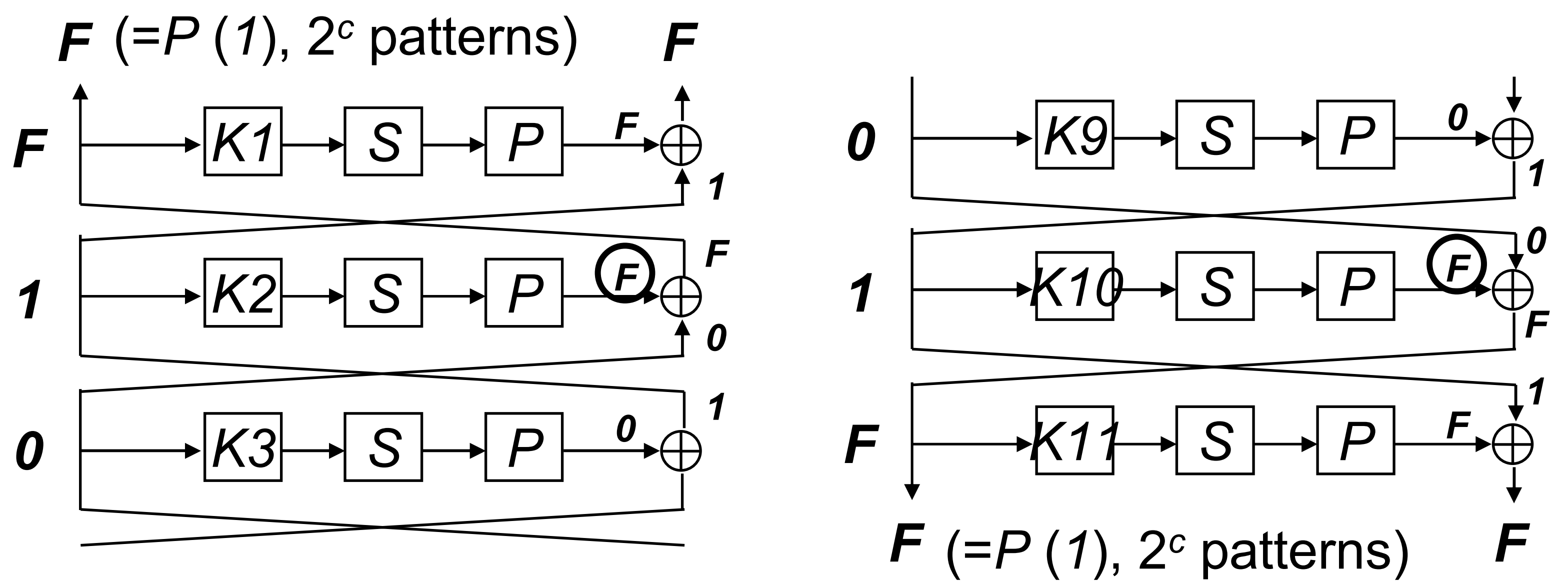
Half-collision attacks

- Direct translation of 11R distinguisher yields partial collision of its MMO / Miyaguchi-Preneel hash function
- Rebound attack can generate many (e.g. 2^c) pairs, yielding half-collision in the left half (faster than the naïve birthday attack)



Full-collision attacks

- Reduce # of rounds in the outbound phase from 3 to 2 by removing the 1st and the 11th rounds (so 2 + 5 + 2 = 9R in total)
- The truncated difference is now (1,P(1)), making full-collision attack possible (faster than the birthday bound)



Concluding remarks

- The case of 64bit block with 8-bit S-boxes can also be analyzed (but # of rounds has to be reduced)
- Restrictions of "good" S-boxes and of MDS matrix are not quite mandatory for the attack to work
- Future work: application to actual ciphers

Thank you.