Formalizing Known-Key “Distinguishers”
- New Attacks on Feistel Ciphers

Yu Sasaki and Kan Yasuda
NTT Corporation
Formalizing Known-Key “Distinguishers”

- New Attacks on Feistel Ciphers

Yu Sasaki and Kan Yasuda
NTT Corporation
(3-bit) Block Cipher

Key Dependent Permutation

Plaintext

Ciphertext

BLOCK CIPHER

NTT
Choose a key. Permutation is fixed.
Attacker’s Goal on Block Ciphers

Distinguish / Key Recovery

Plaintext

Adv.

Secret

Ciphertext
Attack Models (Classic)

Differential Attack

Plaintext

Ciphertext
Attack Models (Classic)

Differential Attack

Plaintext

Ciphertext

ΔP

ΔC

1 2 3 4 5 6 7 8

1 2 3 4 5 6 7 8

NTT
Attack Models (Adaptively Chosen)

Boomerang Attack

Choose adaptively

Plaintext

Ciphertext

Choose adaptively

NTT
Attack Models (Adaptively Chosen)

Boomerang Attack

Choose adaptively

Plaintext

Ciphertext
Attack Models (Related-Key)

Related-Key (Differential) Attack

\[ \Delta P_1 \]

\[ ?A? \rightarrow \text{Relation} \rightarrow ?B? \]

Plaintext

Ciphertext
Attack Models (Related-Key)

Related-Key (Differential) Attack

Encrypt with A

Encrypt with B

\( \Delta P_1 \)

\( \Delta C_1 \)

Plaintext

Ciphertext
• More and more complicated attack models are considered to recover the key.
• More and more complicated attack models are considered to recover the key.

• Another simple attack model: **Known-Key Attack**

The concept was proposed by Knudsen and Rijmen at Asiacrypt 2007.
Known-Key Model

Plaintext

Ciphertext

NTT
Known-Key Model

The key is given to the attacker!!
Known-Key Model

The attacker can do everything!!

distinguish
recovery
encryption
decryption

Plaintext

Ciphertext
Known-Key Model

The attacker can do everything!!

distinguish
recovery
encryption
decryption

What's the point??
Undesired Situation

secure? if the fixed permutation is identity map

Randomly chosen key
Undesired Situation

secure? if the fixed permutation has strong bias

Randomly chosen key
Undesired Situation

secure? if the fixed permutation has strong bias

Randomly chosen key

Plaintext

Ciphertext

Undesired

Unrequired output

1 2 3 4 5 6 7 8
Known-Key Attacks

Goal is different. No secret any more!!

• Evaluate whether or not the fixed permutation with a randomly chosen key is ideal.
• Useful because block ciphers are often used as key-less primitives such as hash functions.
Our Recent Results
Our Results 1

• Give a formalization of known-key attacks which can cover all previous results.

• Show the separation of known-key and secret-key settings.

Ciphers secure in secret-key model

security in one \[\Rightarrow\] security in the other

Ciphers secure in known-key model
Our Results 2

• Known-key attacks up to 11-rounds of *Feistel-SP*

*Previous [KR07]*

- Round function $F$: 7 rounds are not ideal.

*Ours*

- Round function $F$: 11 rounds are not ideal.
Conclusions

• Known-key distinguishers are useful tools to evaluate the security of key-less primitives.

• Our recent work
  – Formalization
  – Separation of secret/known key settings
  – Attacks on 11-rounds of Feistel-SP

Thank you for your attention !!