Formalizing Known-Key "Distinguishers" - New Attacks on Feistel Ciphers

Yu Sasaki and Kan Yasuda

NTT Corporation

NTT

CRYPTO 2010 Rump Session 17/Aug./2010 @ UCSB

1.

Formalizing Known-Key "Distinguishers" - New Attacks on Feistel Ciphers

2.

Yu Sasaki and Kan Yasuda

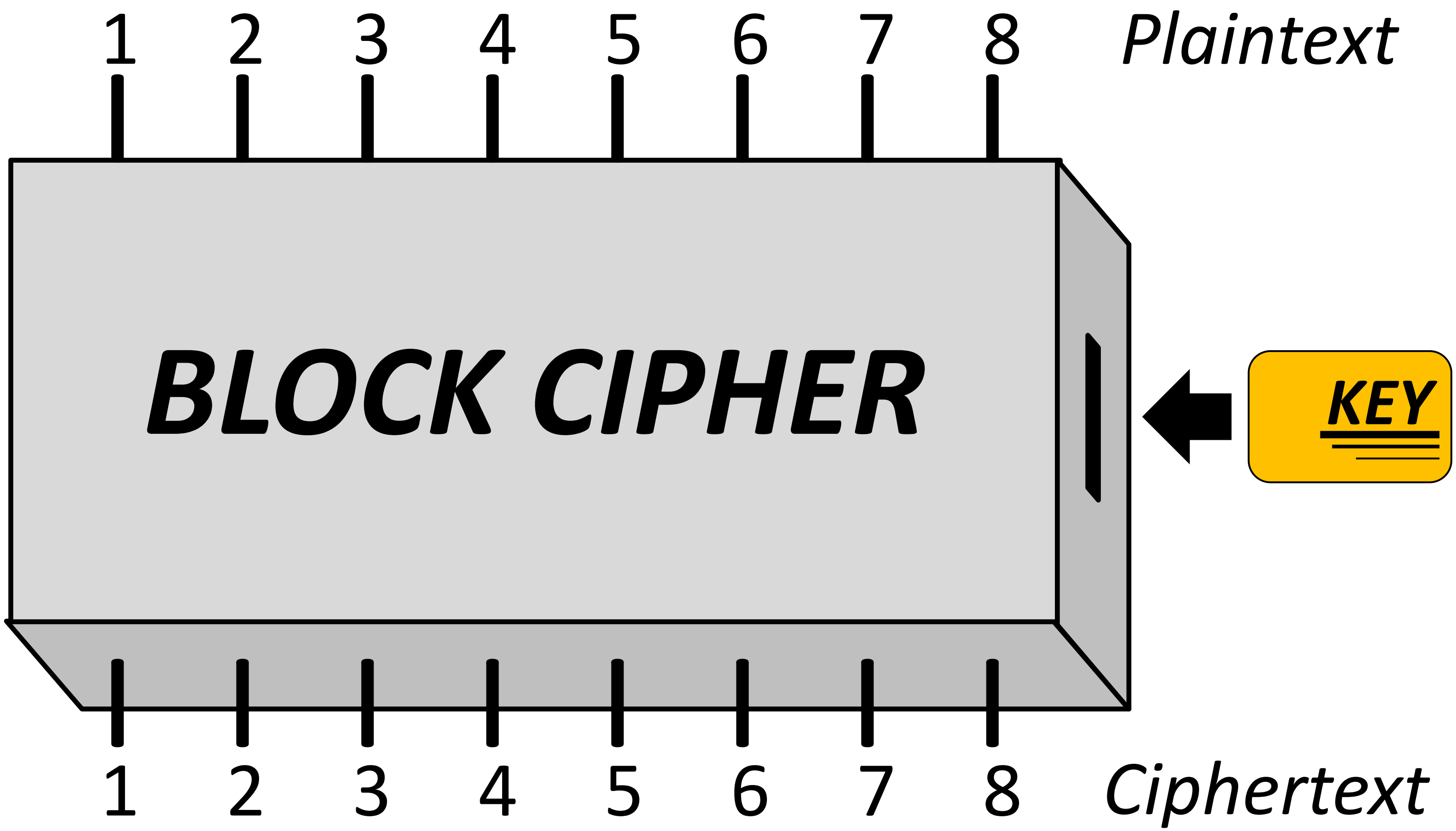
NTT Corporation

NTT

CRYPTO 2010 Rump Session 17/Aug./2010 @ UCSB

(3-bit) Block Cipher

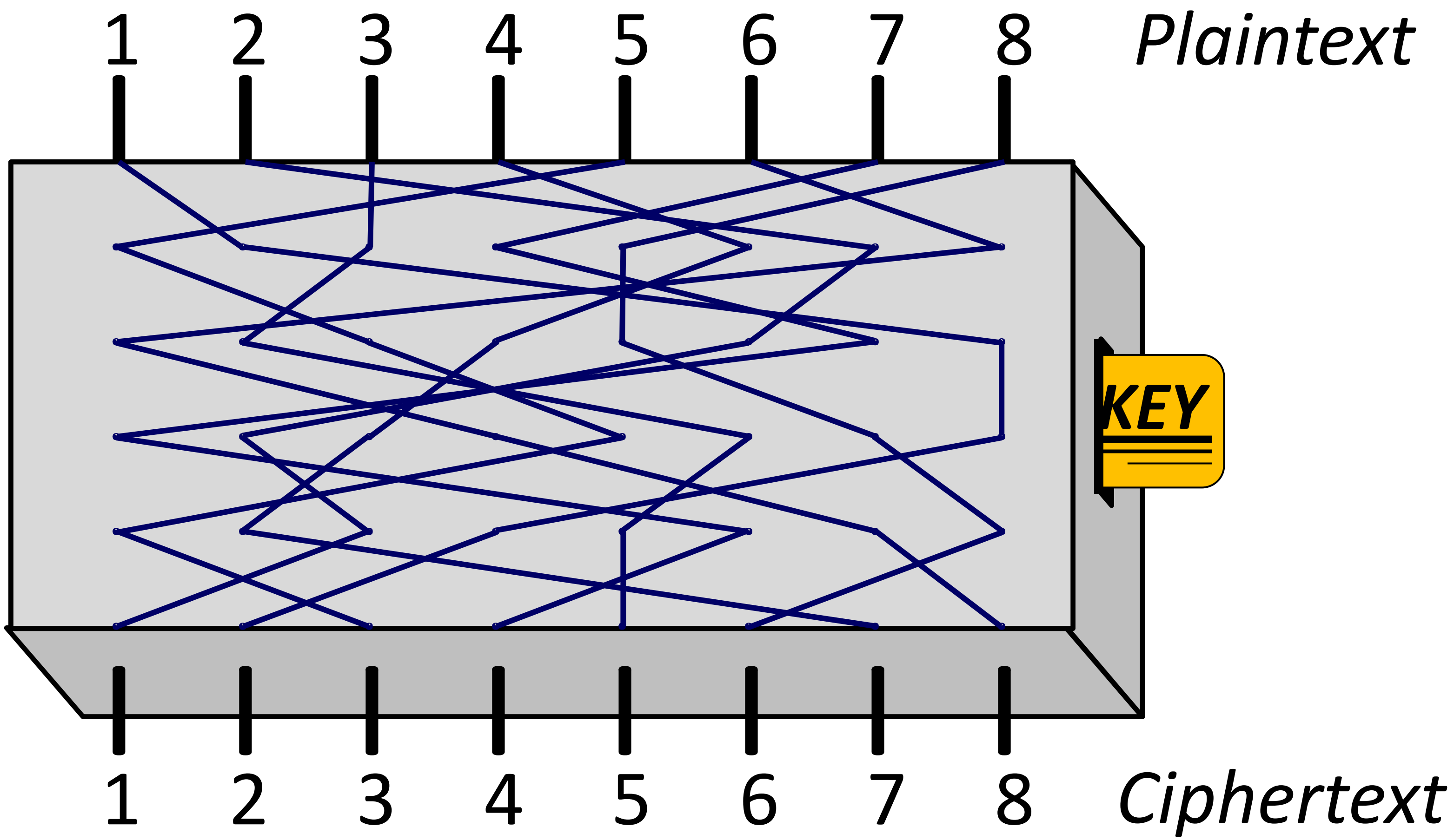
Key Dependent Permutation



NTT

(3-bit) Block Cipher

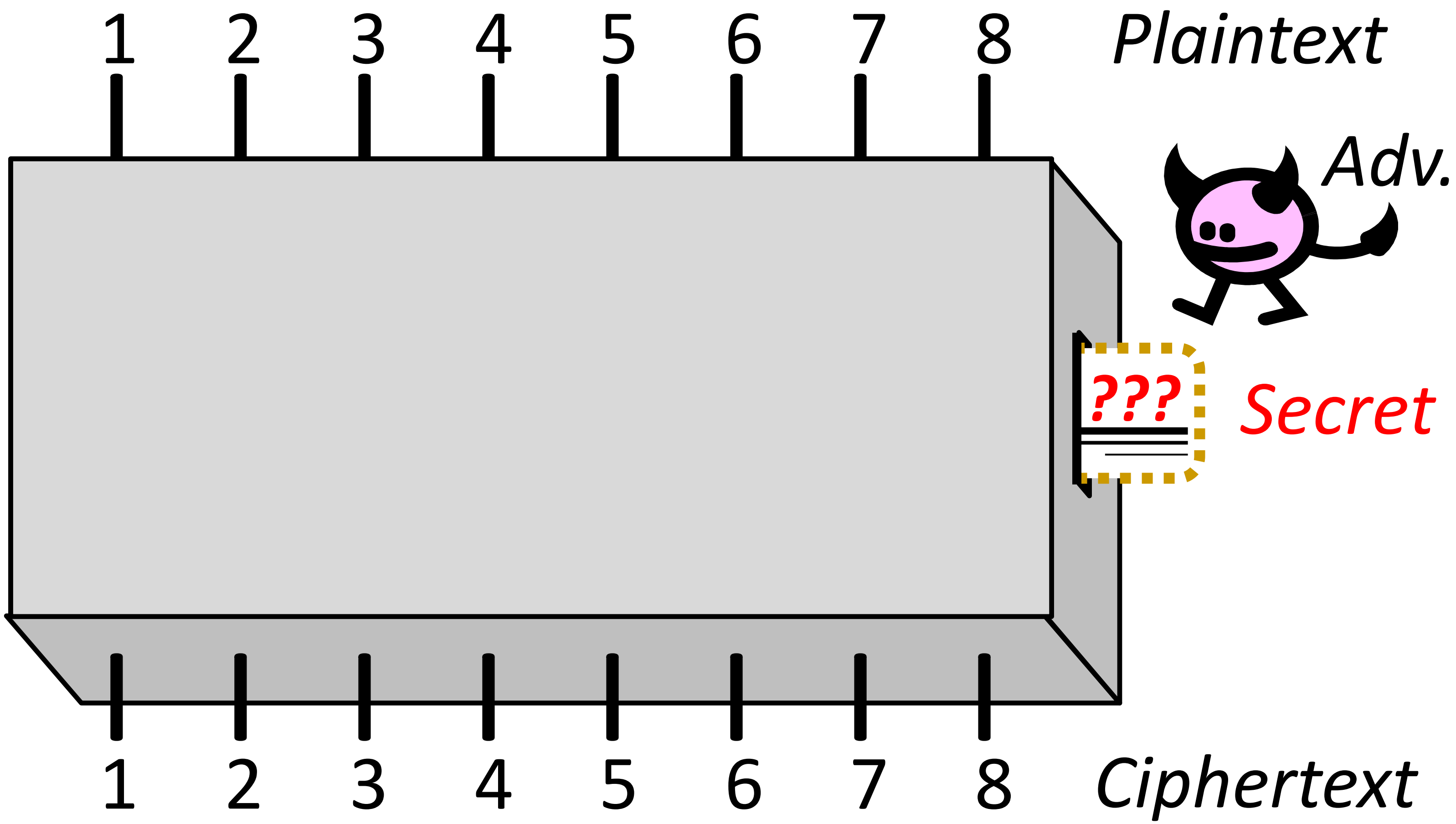
Choose a key. ➡ Permutation is fixed.



NTT

Attacker's Goal on Block Ciphers

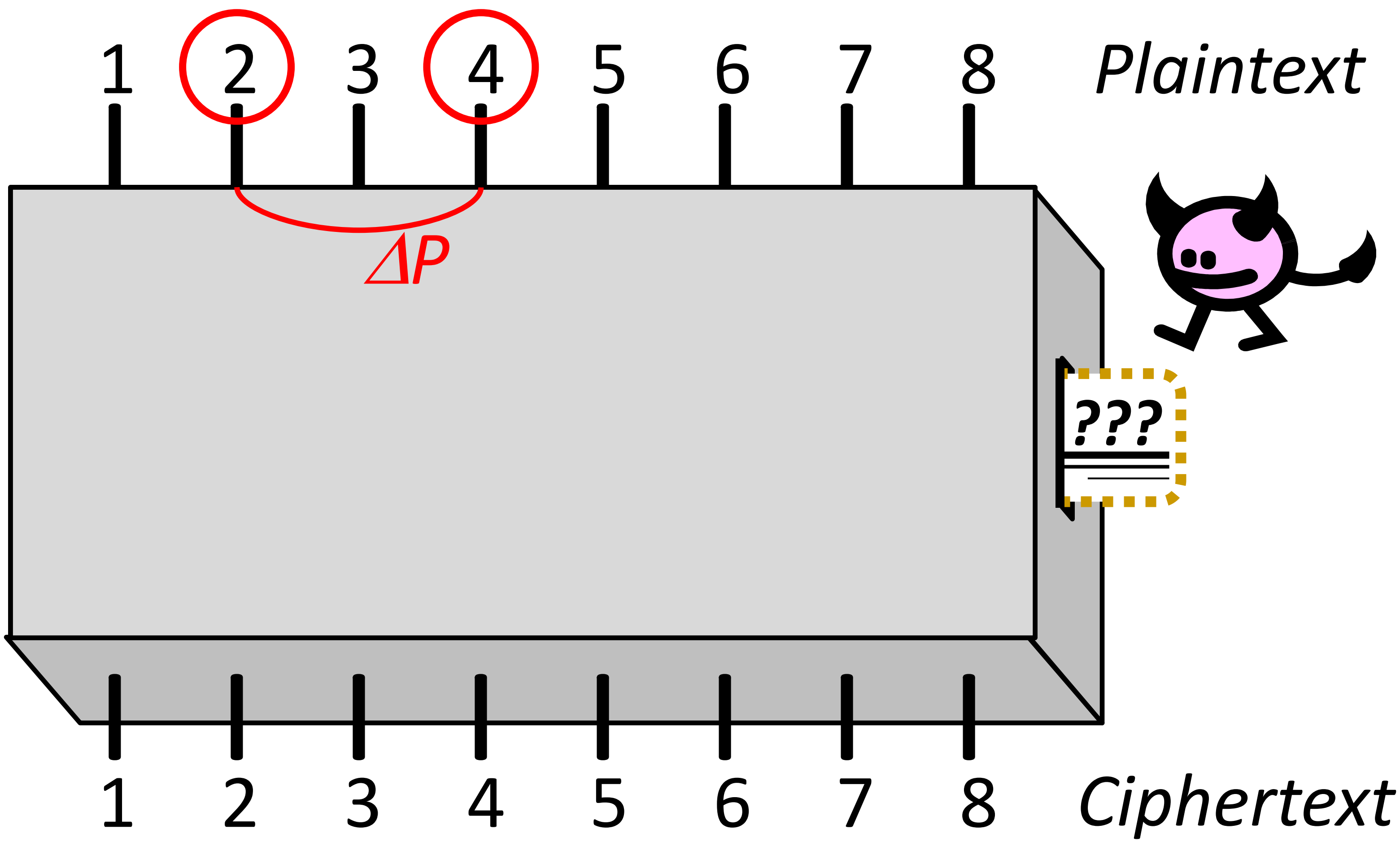
Distinguish / Key Recovery



NTT

Attack Models (Classic)

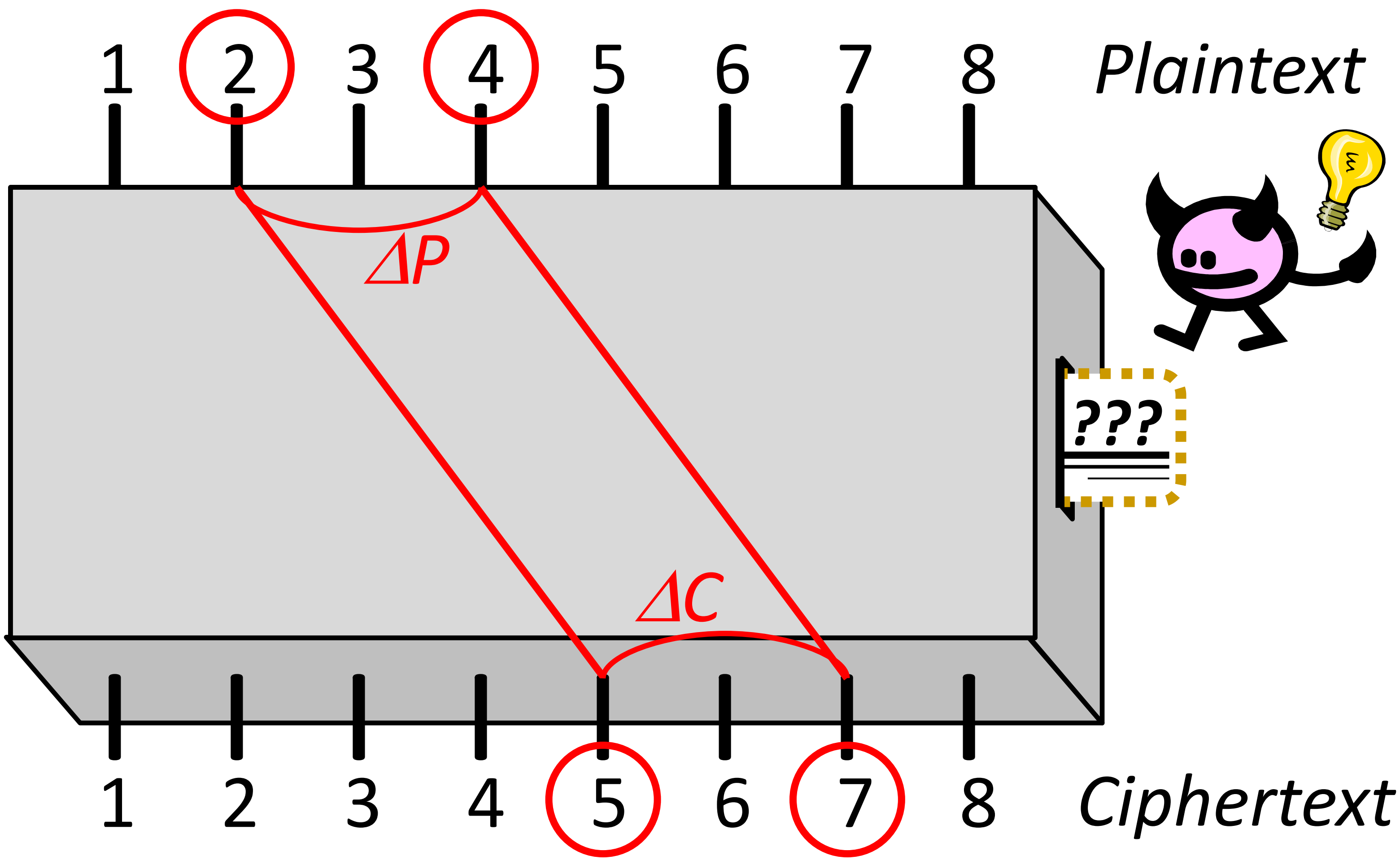
Differential Attack



NTT

Attack Models (Classic)

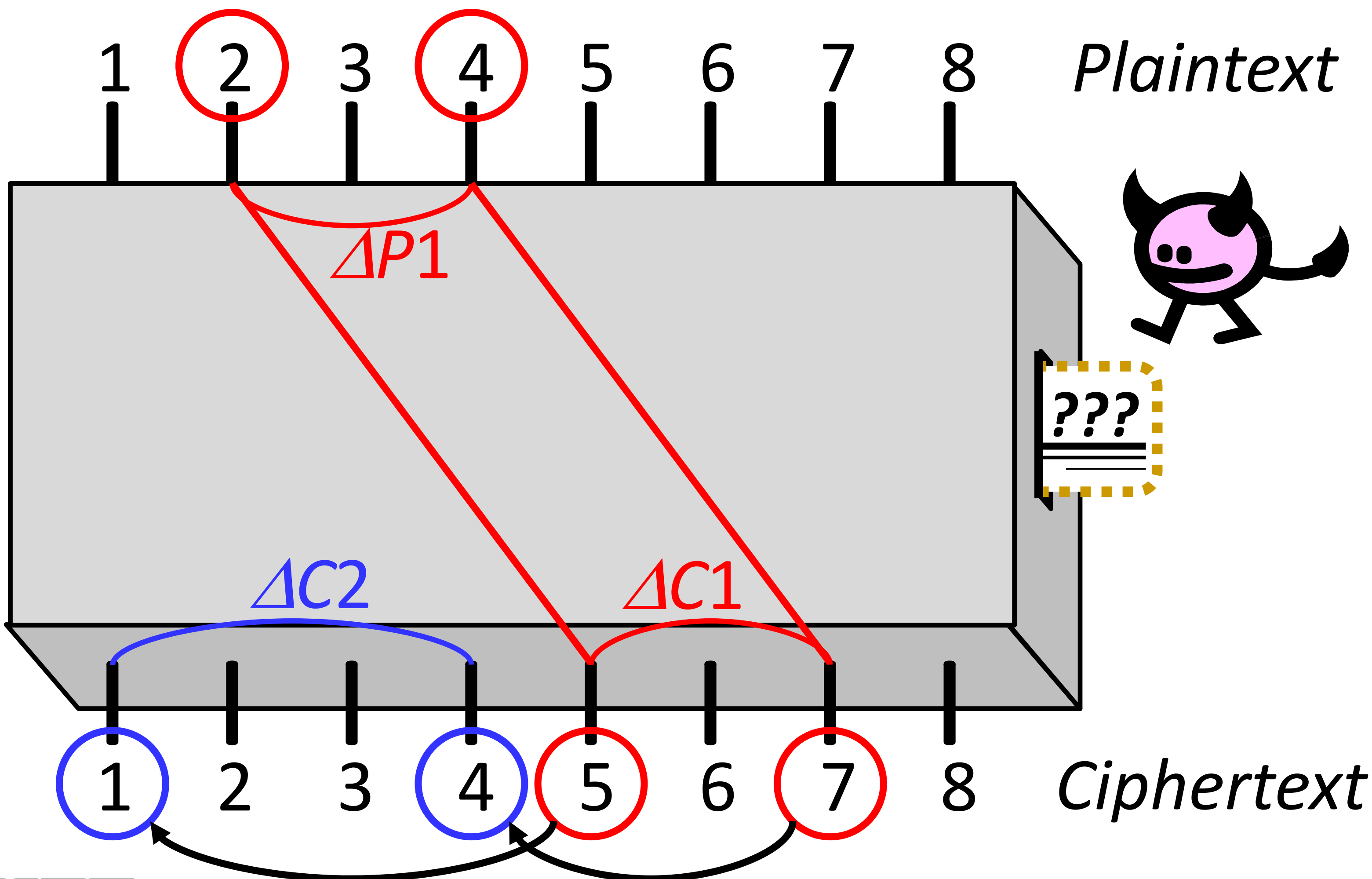
Differential Attack



NTT

Attack Models (Adaptively Chosen)

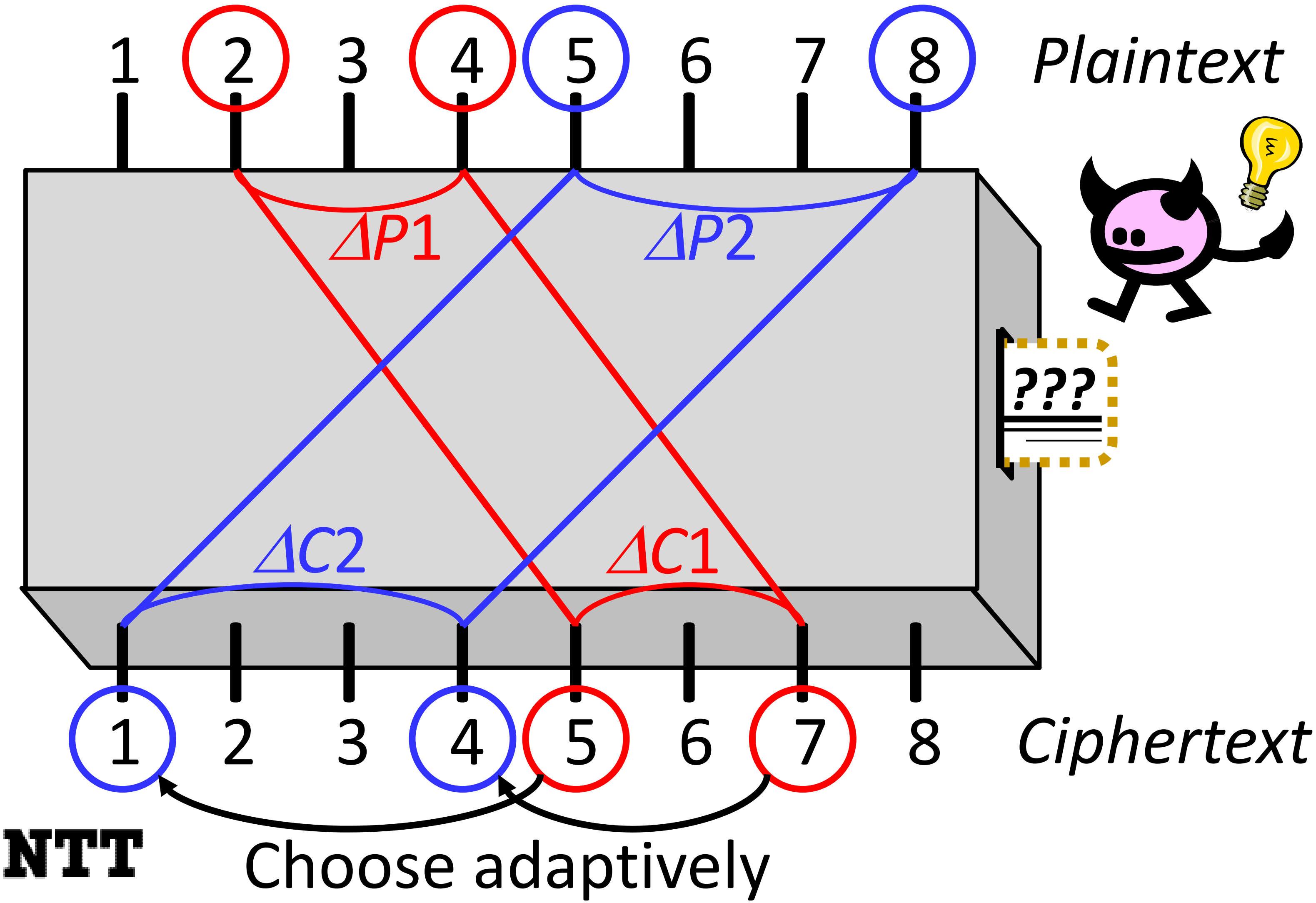
Boomerang Attack



NTT

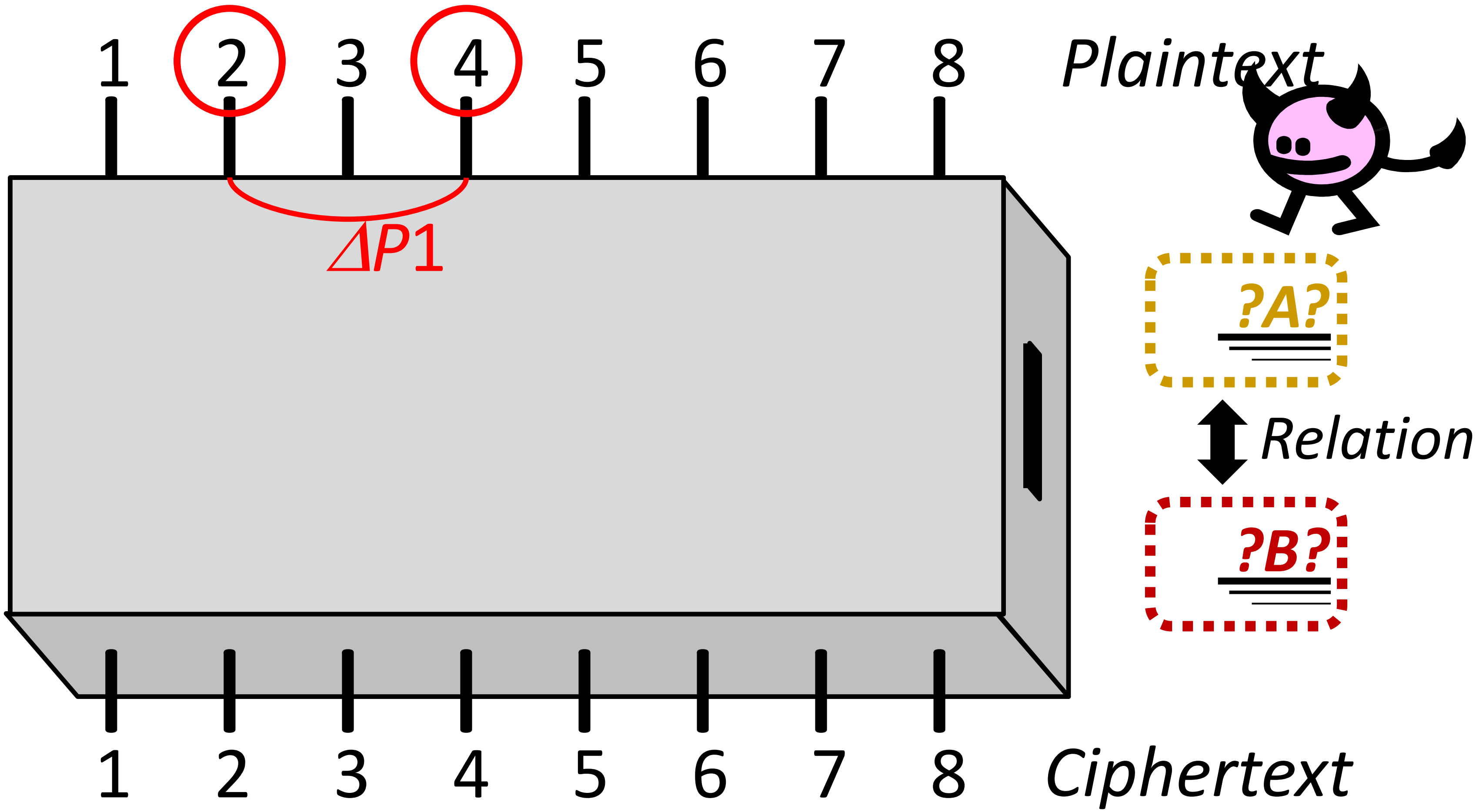
Attack Models (Adaptively Chosen)

Boomerang Attack



Attack Models (Related-Key)

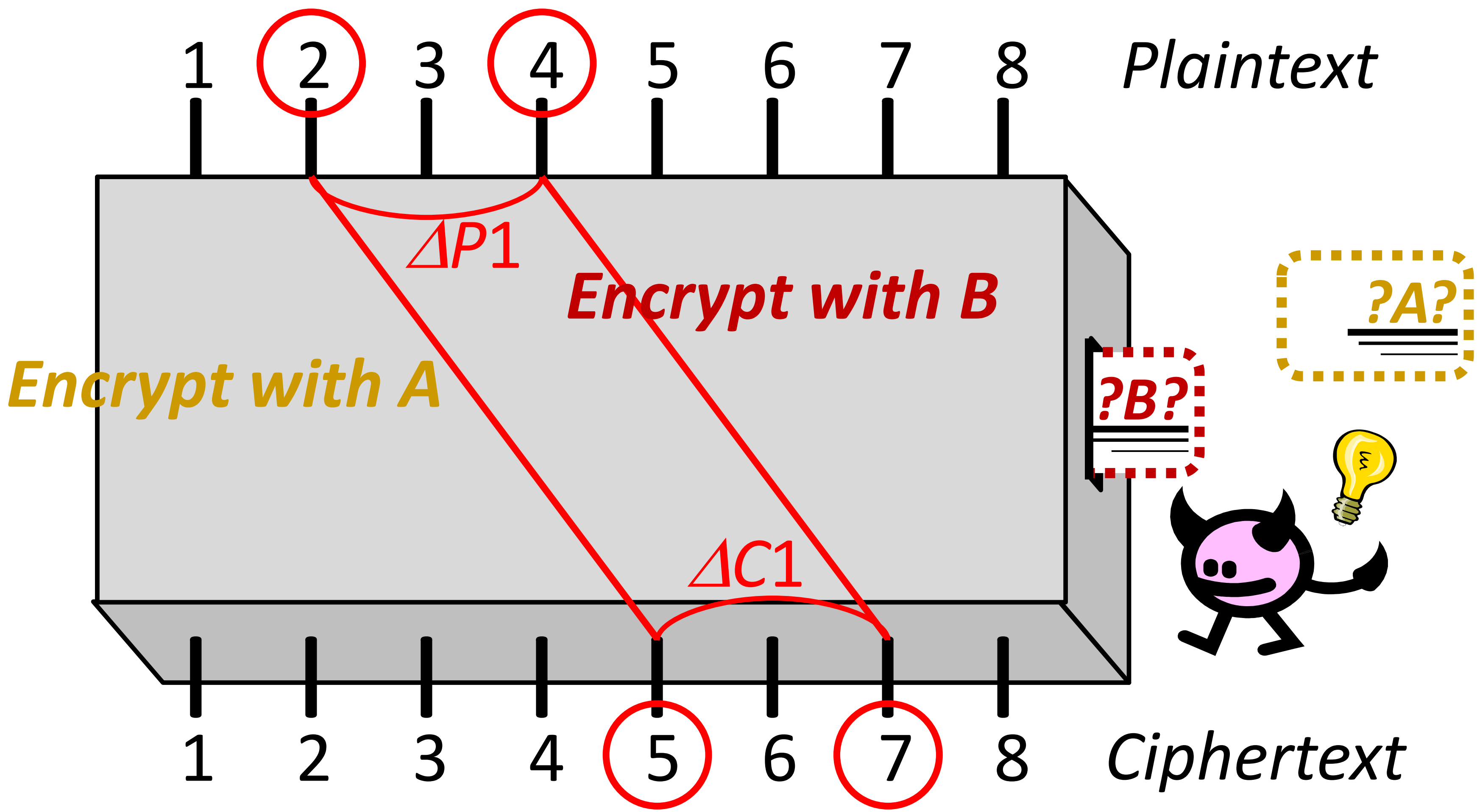
Related-Key (Differential) Attack



NTT

Attack Models (Related-Key)

Related-Key (Differential) Attack



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

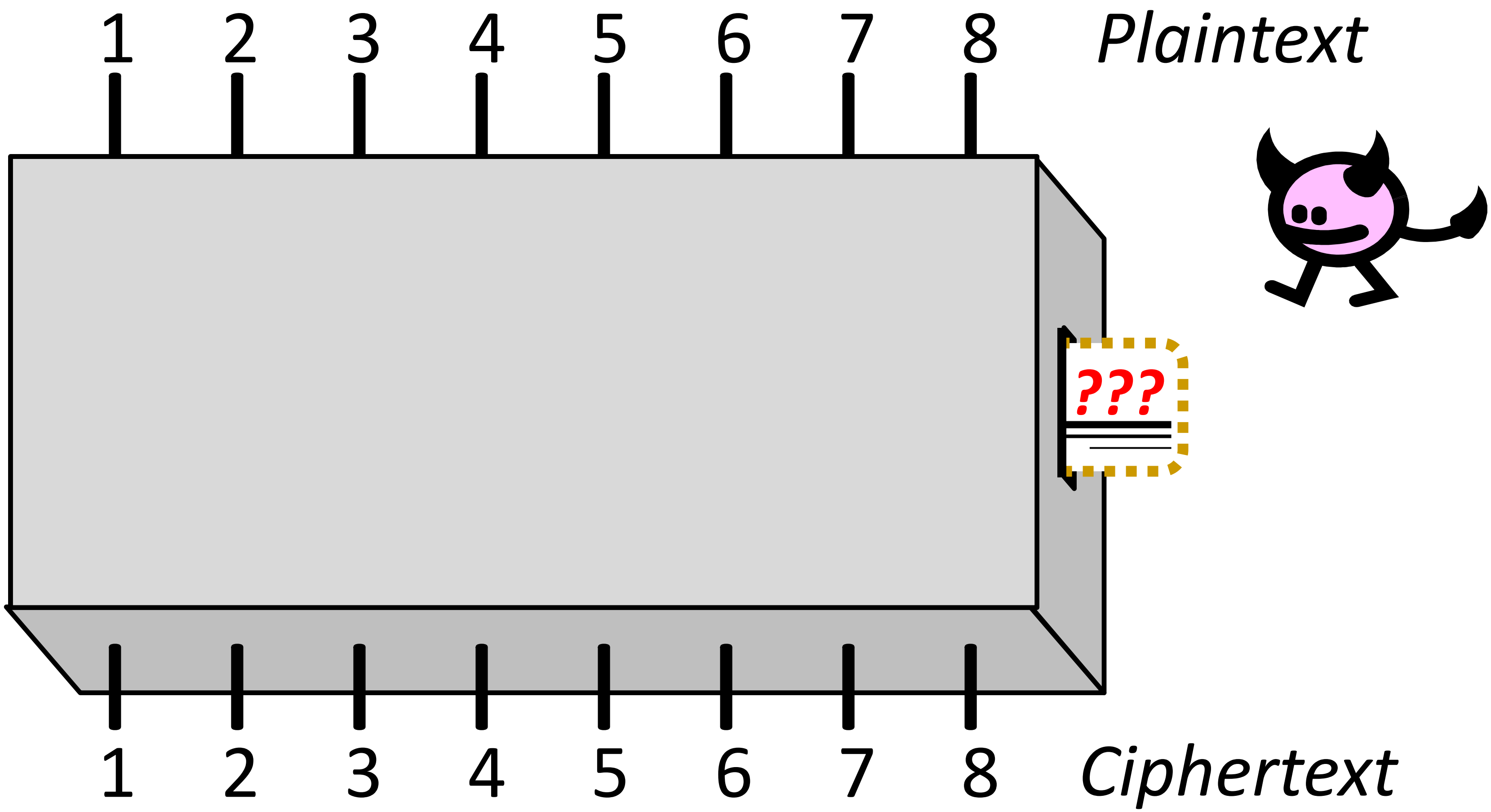
- More and more complicated attack models are considered to recover the key.

- Another simple attack model:

Known-Key Attack

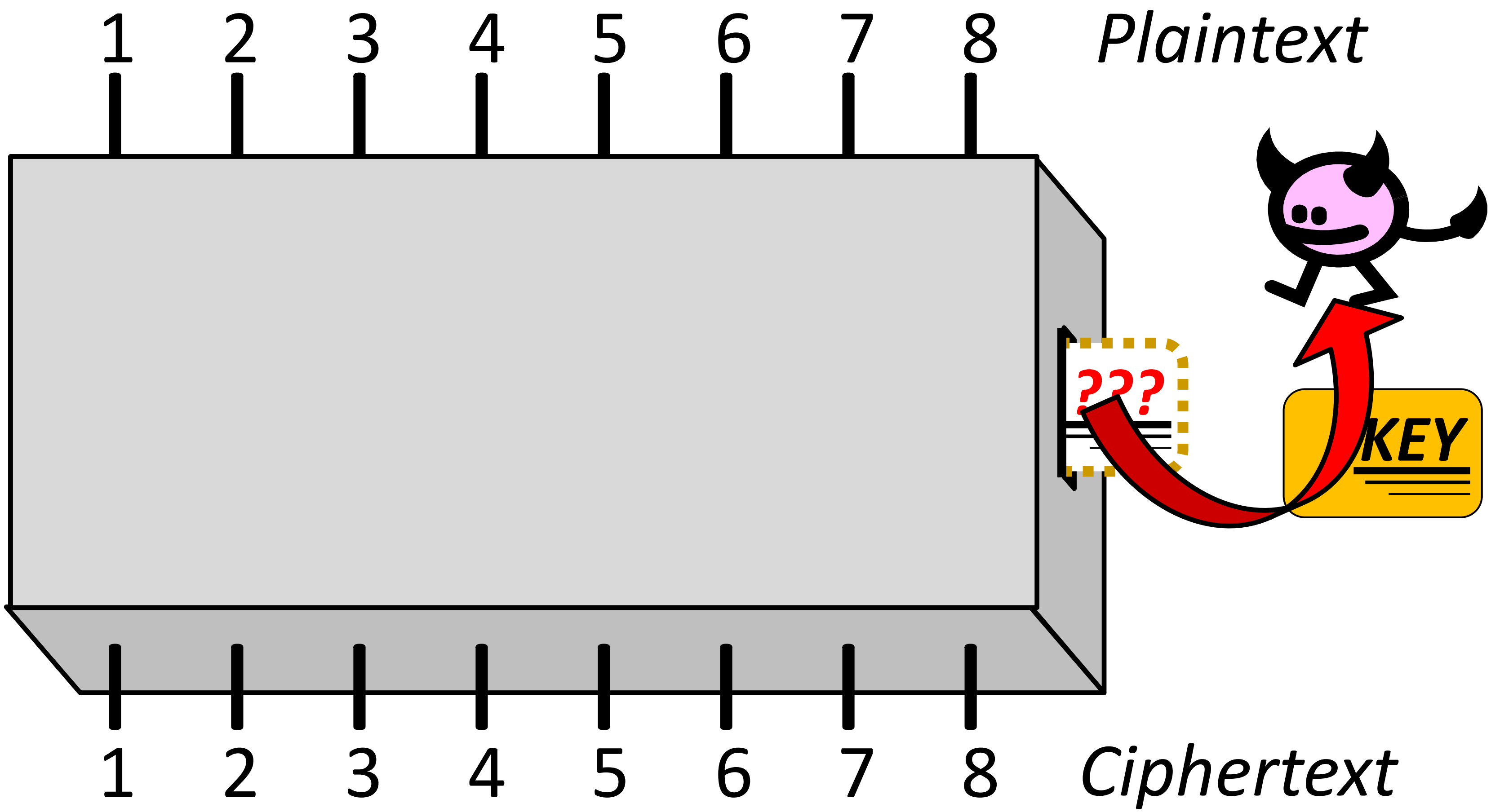
The concept was proposed by Knudsen and Rijmen at Asiacrypt 2007.

Known-Key Model



Known-Key Model

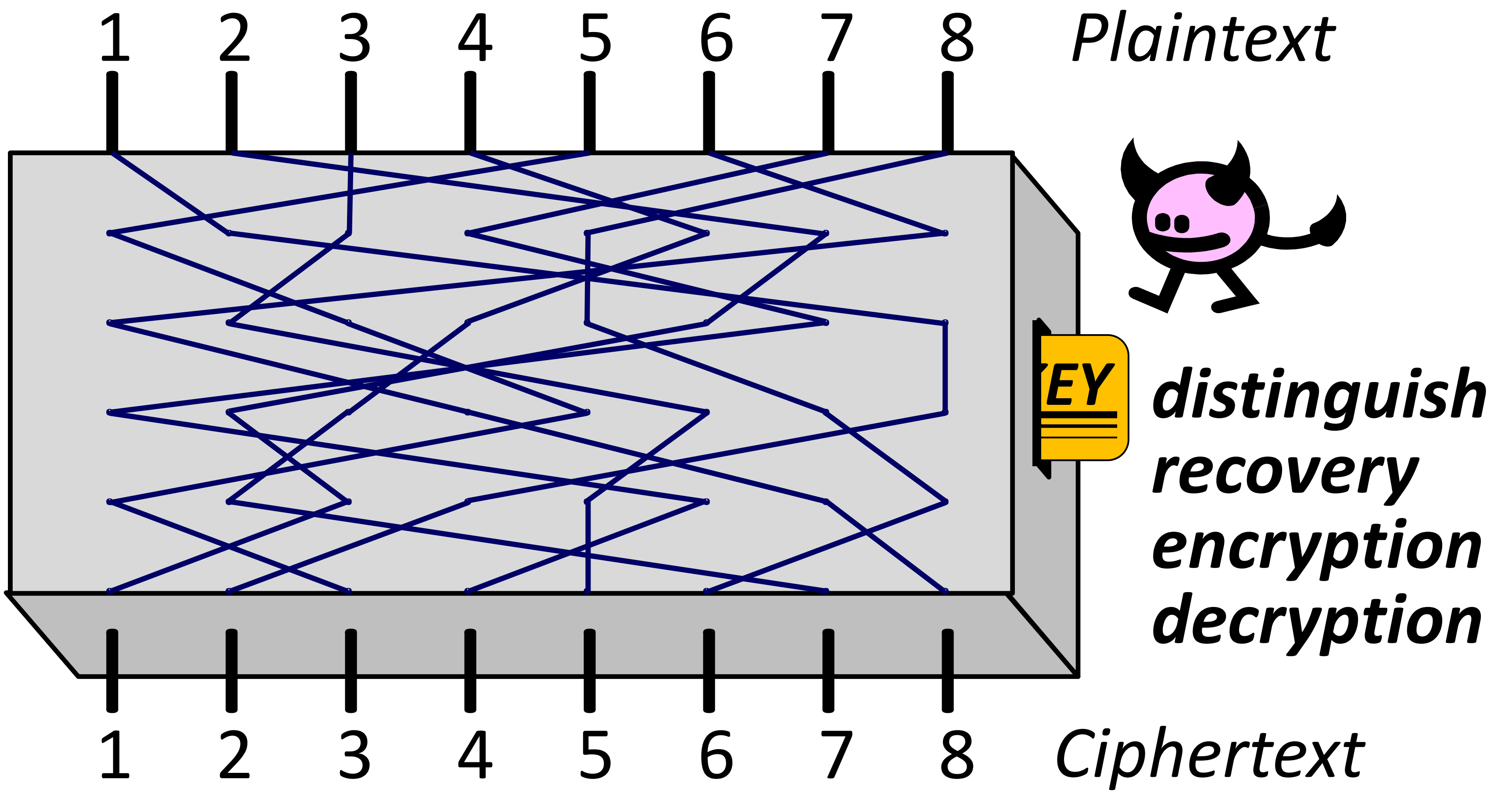
The key is given to the attacker !!



NTT

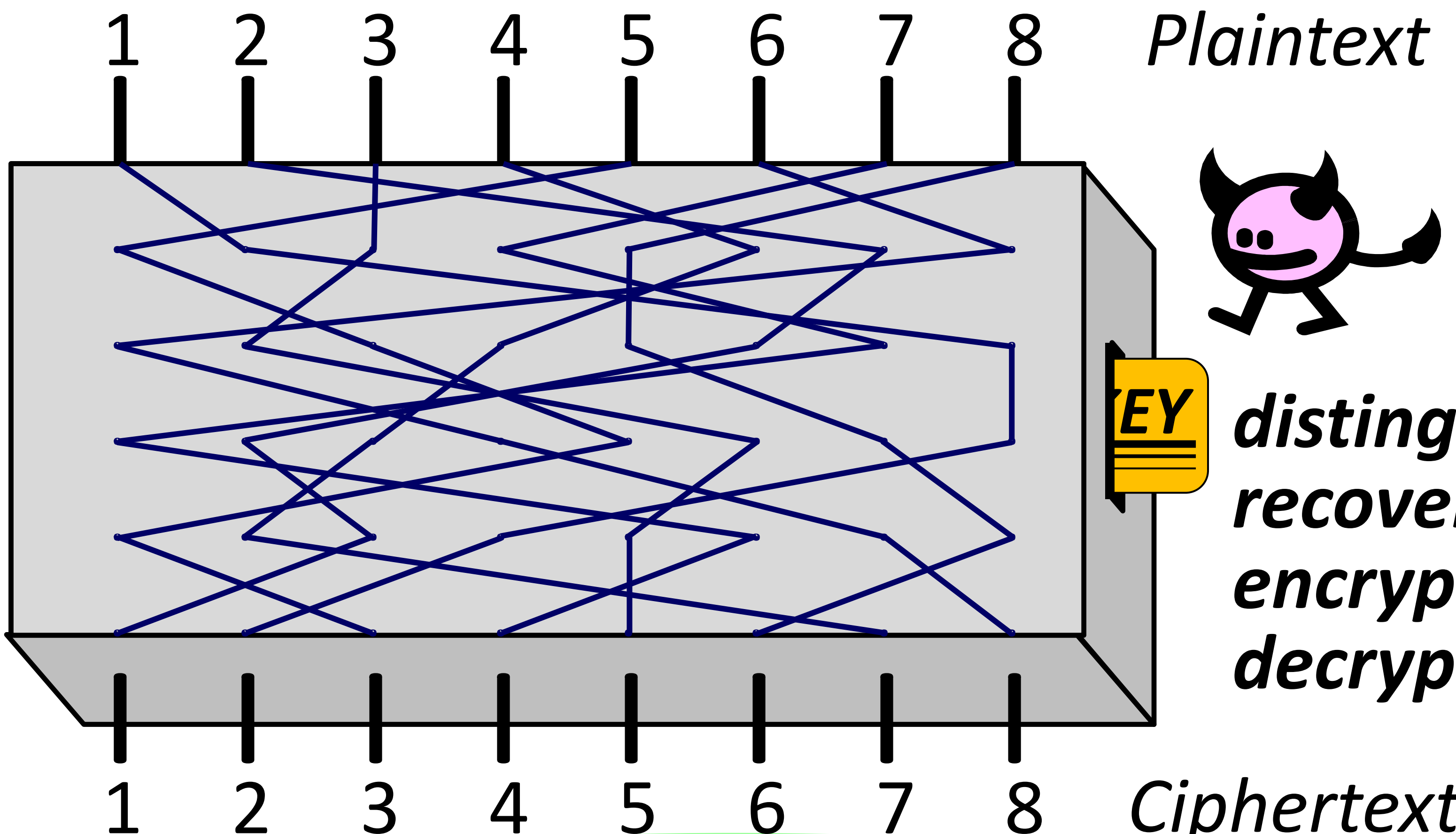
Known-Key Model

The attacker can do everything !!



Known-Key Model

The attacker can do everything !!



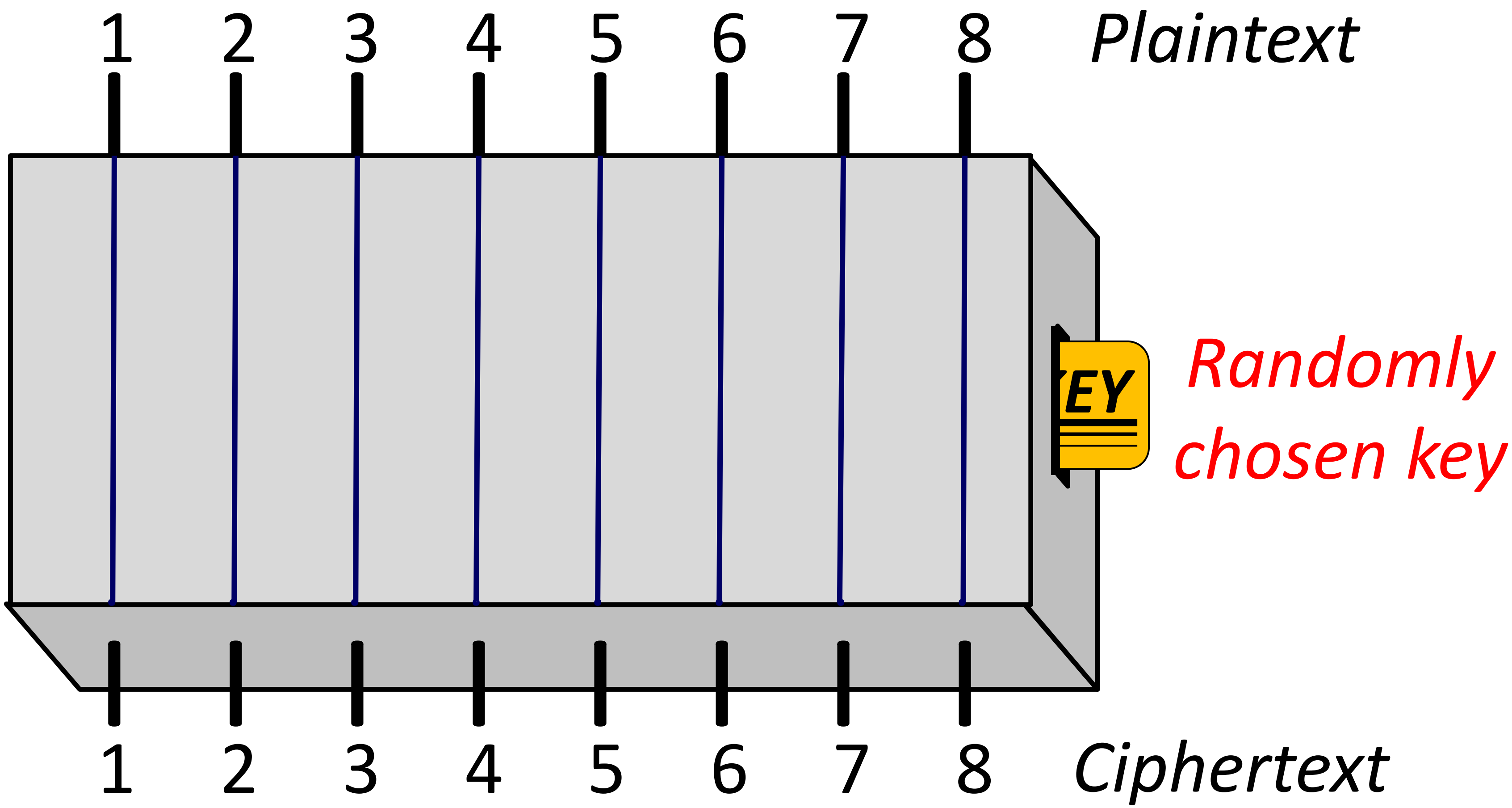
distinguish
recovery
encryption
decryption

What's the point??

NTT

Undesired Situation

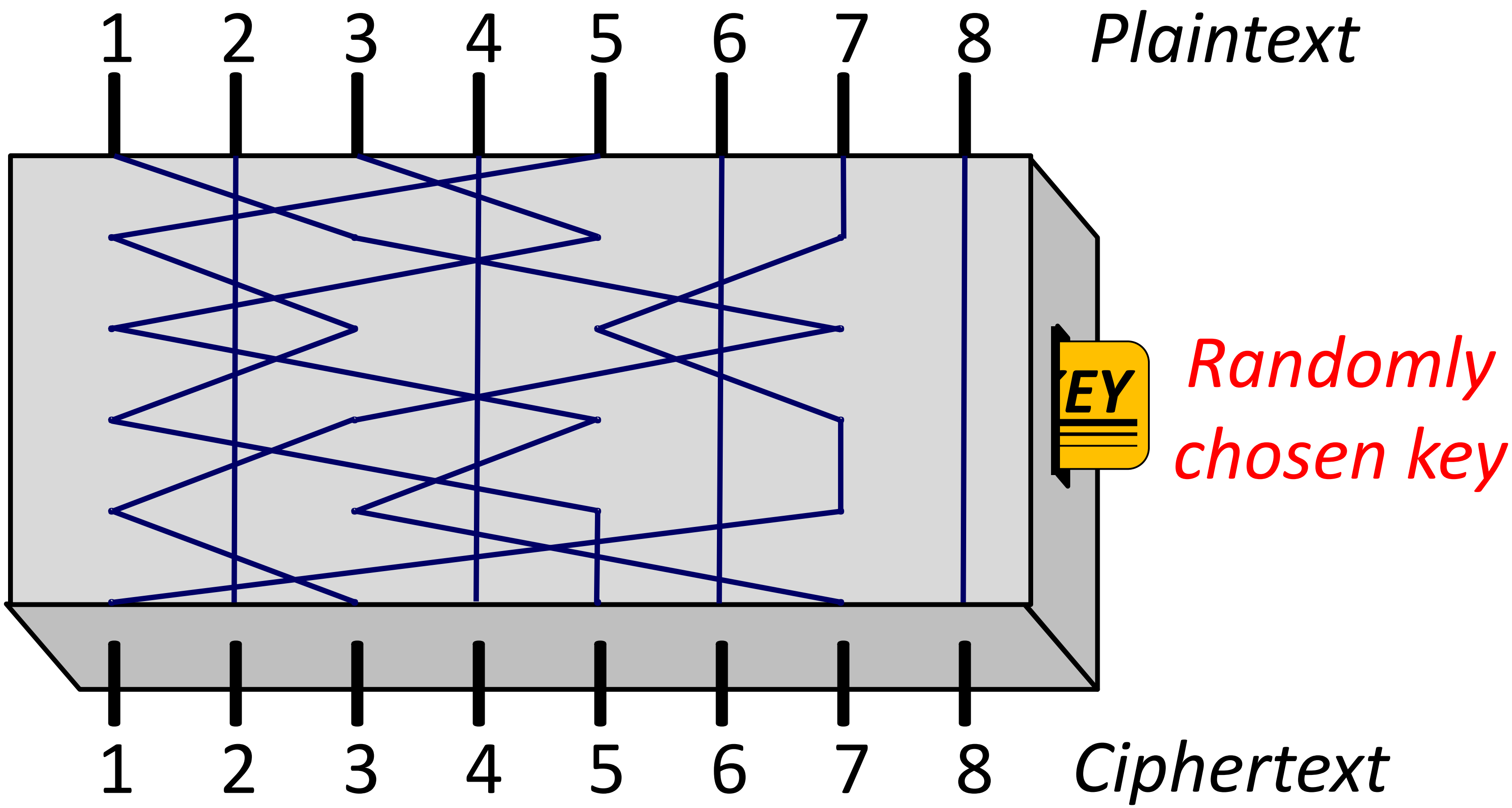
secure? if the fixed permutation is identity map



NTT

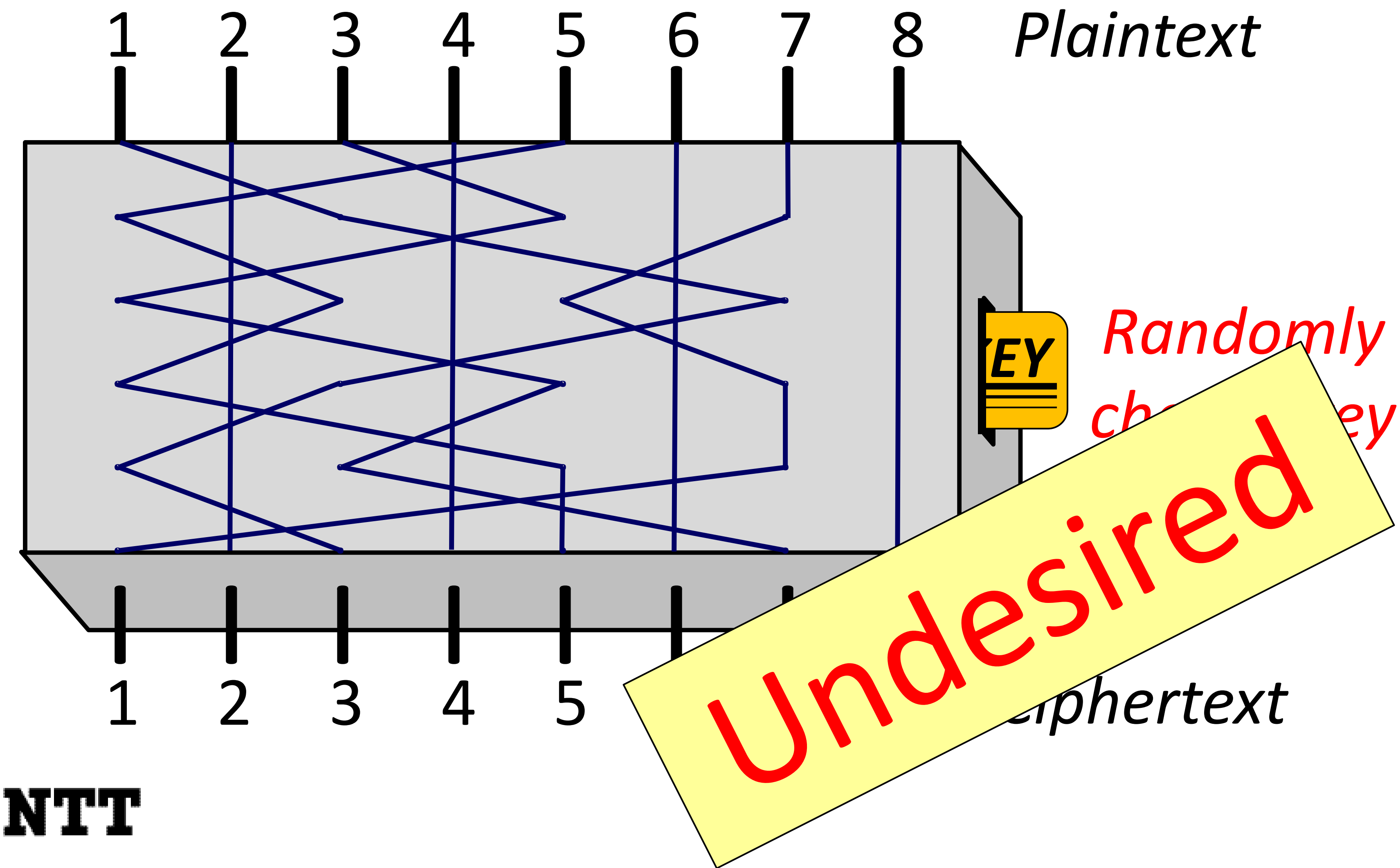
Undesired Situation

secure? if the fixed permutation has strong bias



Undesired Situation

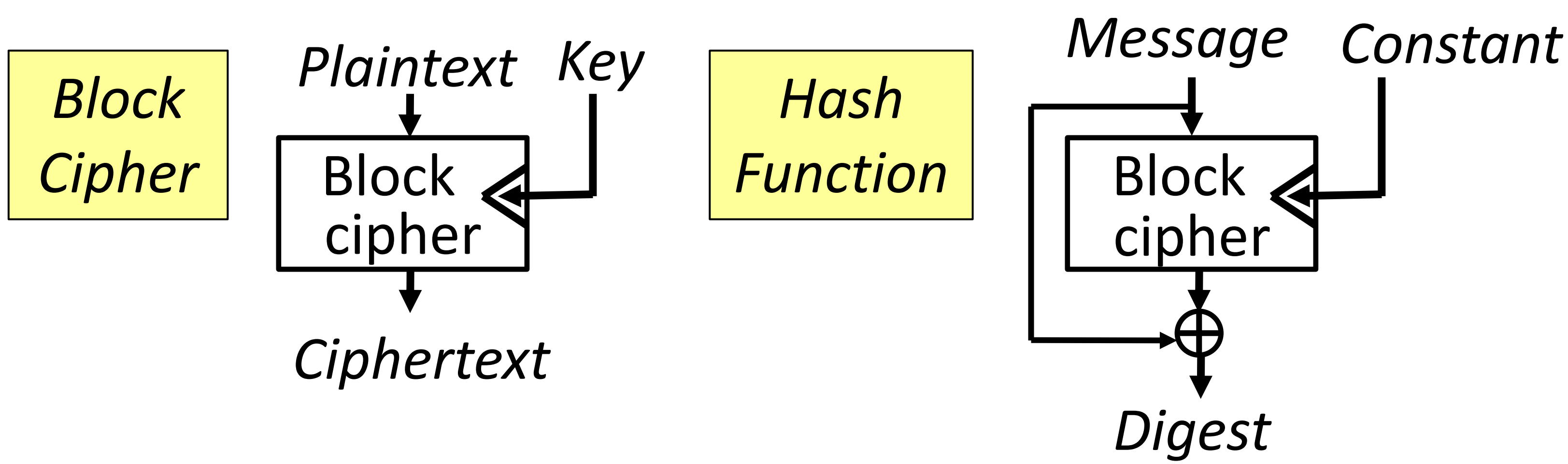
secure? if the fixed permutation has strong bias



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.

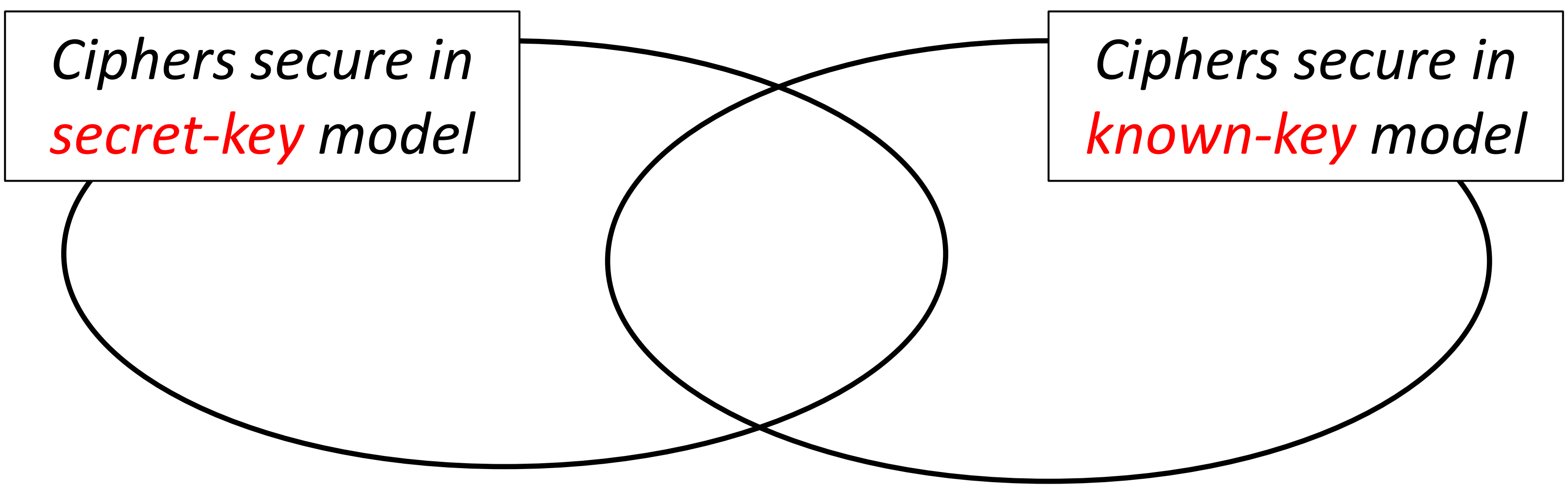


Secure ⇏ Secure

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.

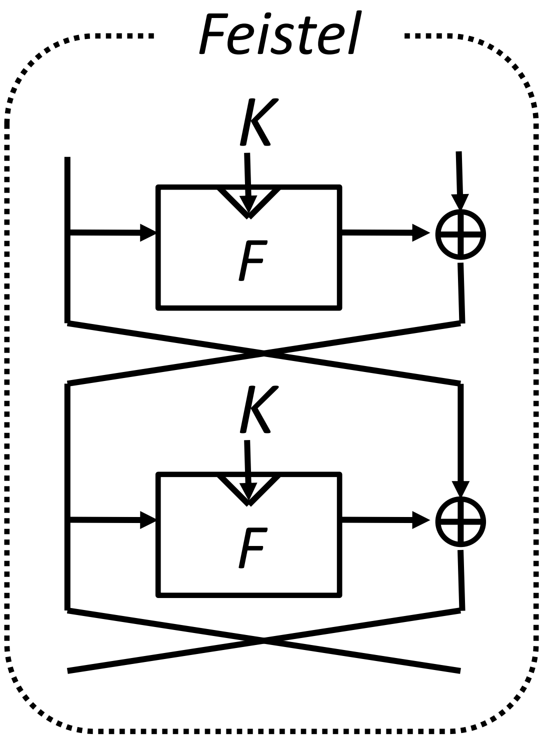


security in one $\not\Rightarrow$ security in the other

NTT

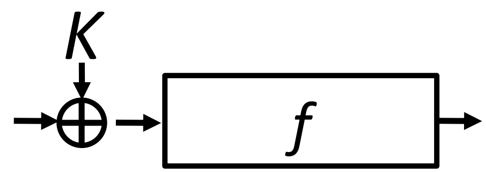
Our Results 2

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



Previous [KR07]

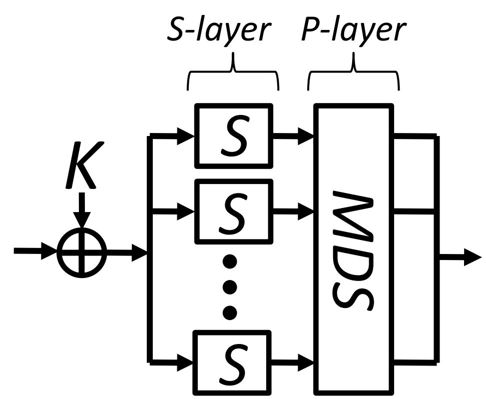
- Round function *F* :



- 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 !!

NTT