NTT

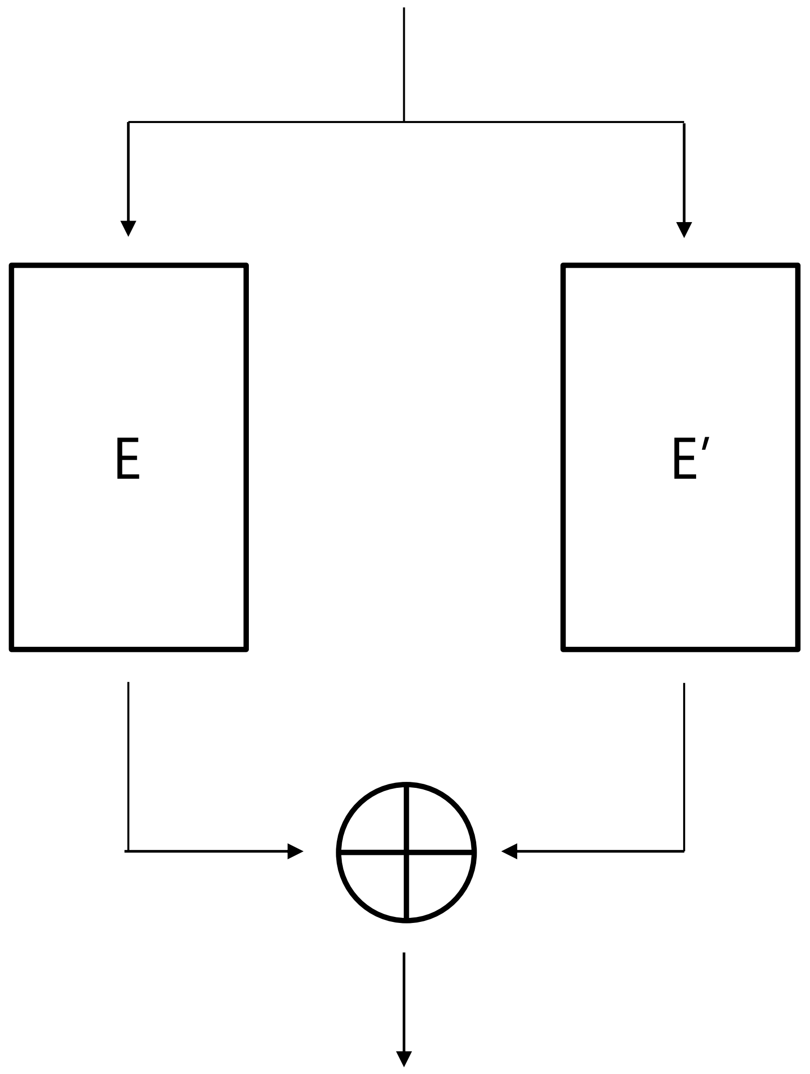
General Practical Cryptanalysis of the Sum of Round-Reduced Block Cipher and ZIP-AES

Antonio Flórez-Gutiérrez[1], Lorenzo Grassi[2], Gregor Leander[2], Ferdinand Sibleyras[1], Yosuke Todo[1]

1, NTT Social Informatics Laboratories, 2, RUB

Motivation

- Sum of PRP = PRF
- Do we really need PRP here?
  - **e.g.) Orthros (Banik et al. ToSC 2021)**
    we explore the setting that E and E′ are rather weak as a stand-alone block cipher, using a small number of very simple rounds. The point is that the outputs of E and E′ are never given in clear, hence we can hope that both can cover each weakness, and consequently the sum of them can tolerate dedicated attacks as a PRF.
  - Each output is invisible.
  - PRP might be over-security.

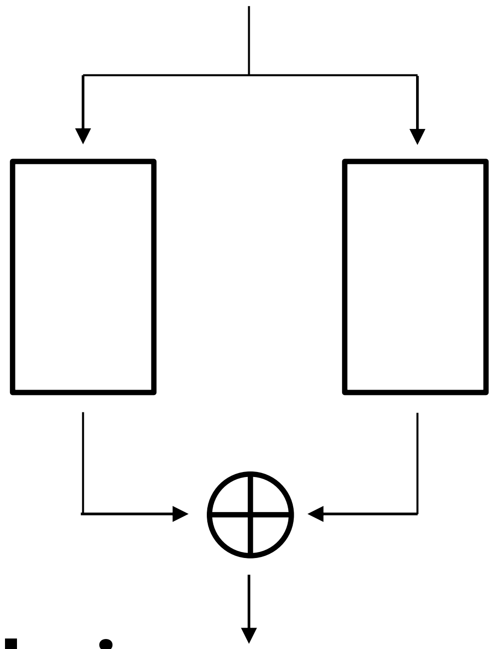


Our approach

NTT

Provable security

- When each branch is PRP, it's PRF.
- It's unlikely to be possible to weaken the assumption, PRP.



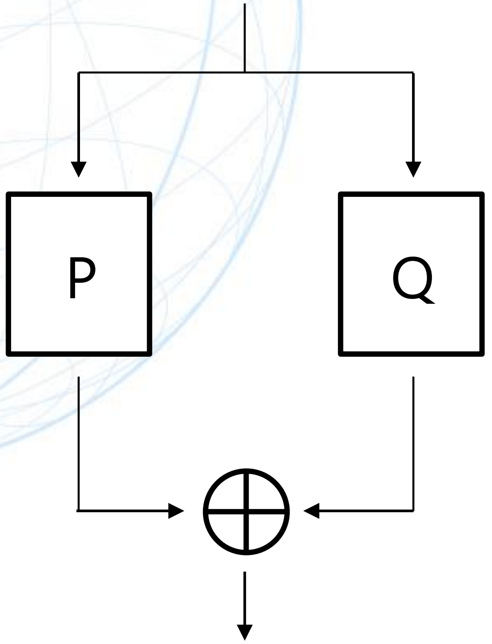
Dedicated analysis

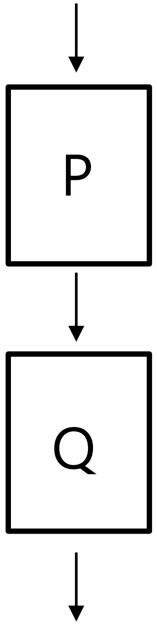
- Like the analysis against Orthros...
- New primitive, new analysis from the scratch.
- Heavy design cost.

General practical cryptanalysis

- We analyze this construction like the dedicated analysis.
- But, we don't suppose each specification.
  - Like the generic attack on Feistel network...
- Consider the link with another construction.
  - Like the security reduction...

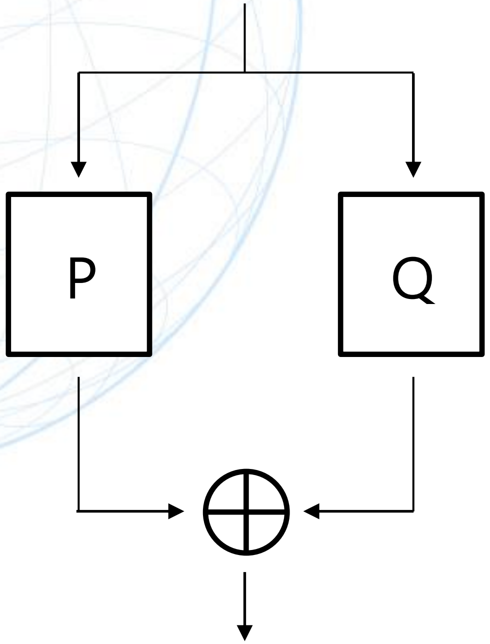
Dream

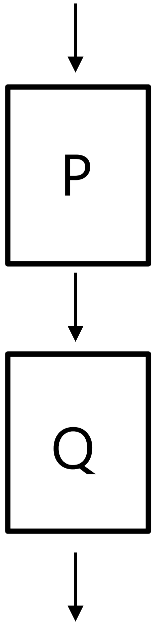




- Assuming an attacker can break the $P \oplus Q$, he also break $Q \circ P$.
- This is the security reduction
  - If we can say it, $P \oplus Q$ is equivalently secure of $Q \circ P$.
  - This is too dream; then, this problem should be solved as provable security.

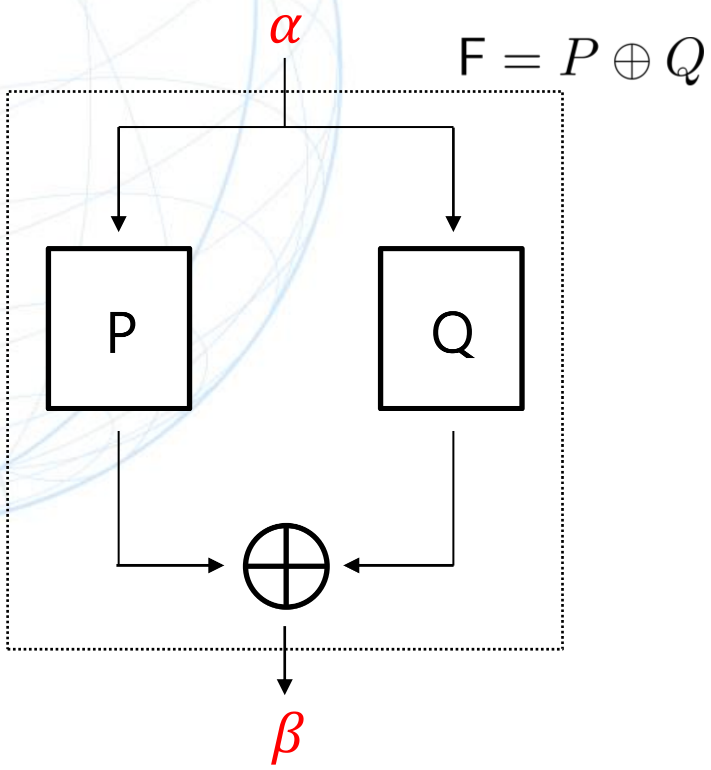
Reality from Dream

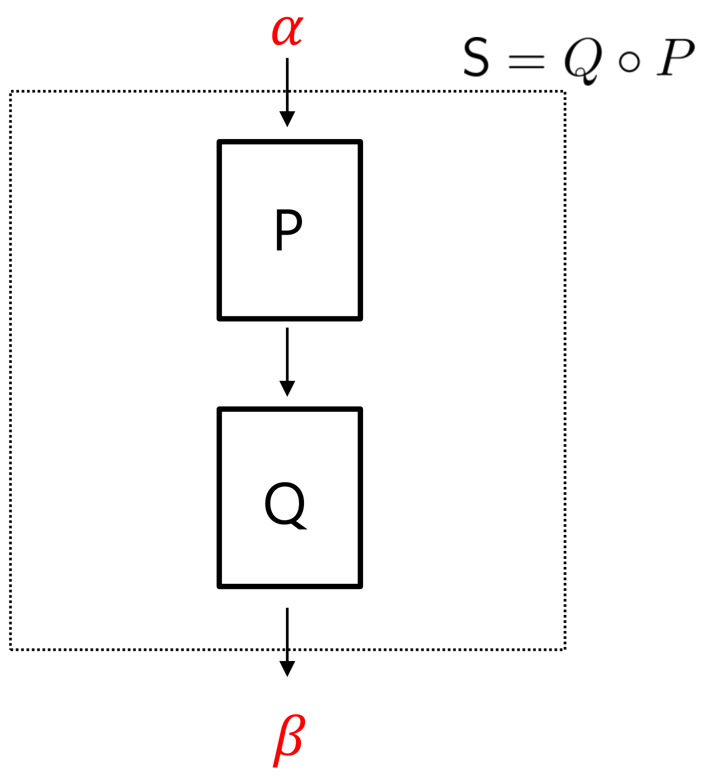




- We restrict the attacker.
  - Differential, linear, differential-linear, truncated differential, algebraic/integral, zero-correlation linear, meet-in-the-middle, etc.
  - Generally compare these two constructions by these attacks.
    - e.g.) if the sum construction is broken by the differential attack, we can also break the composition too with high chance.

Differential cryptanalysis





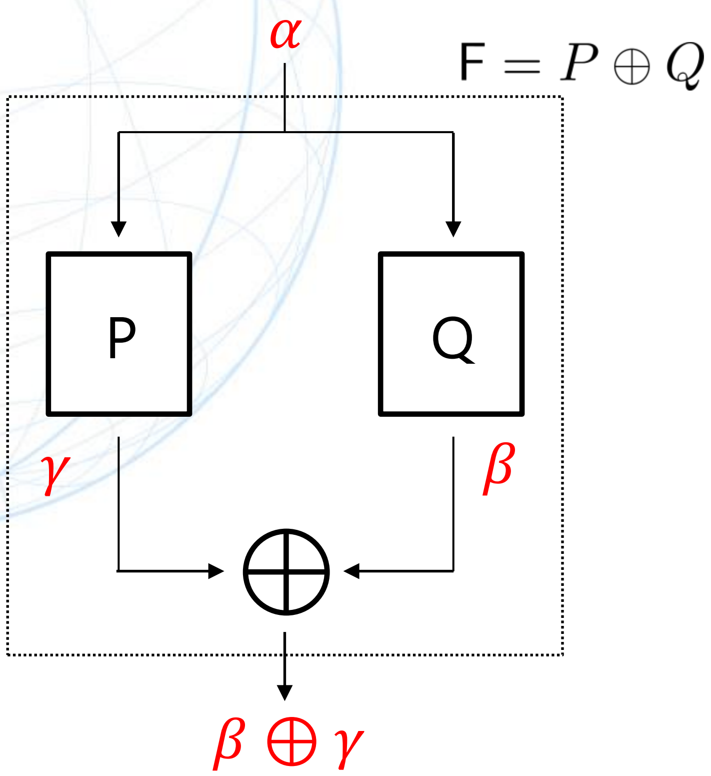
$$DP^{\mathsf{F}}_{\alpha,\beta} = \mathrm{Prob}[\mathsf{F}(x) \oplus \mathsf{F}(x \oplus \alpha) = \beta]$$

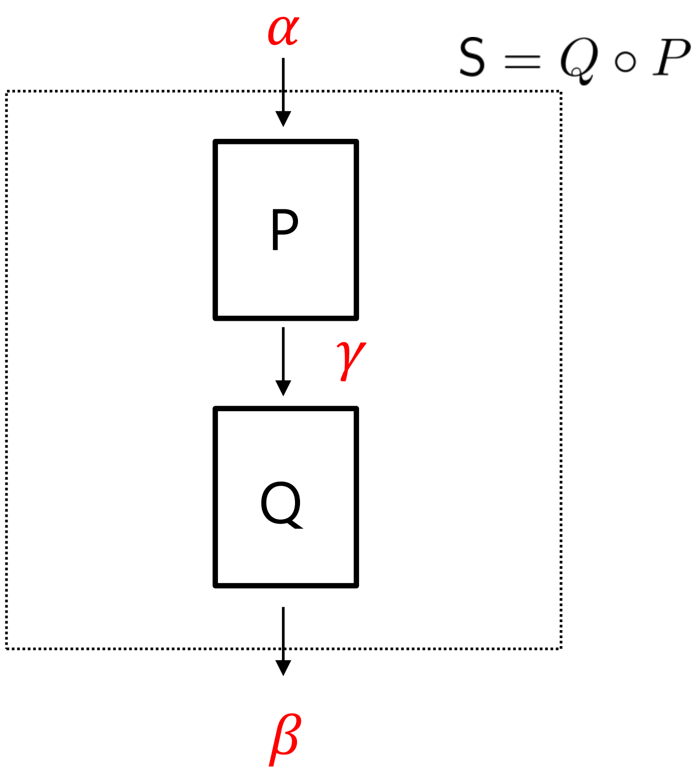
$$DP^{\mathsf{S}}_{\alpha,\beta} = \mathrm{Prob}[\mathsf{S}(x) \oplus \mathsf{S}(x \oplus \alpha) = \beta]$$

$$DP^{\mathsf{F}}_{\alpha,\beta} \neq DP^{\mathsf{S}}_{\alpha,\beta}$$

Differential cryptanalysis

NTT

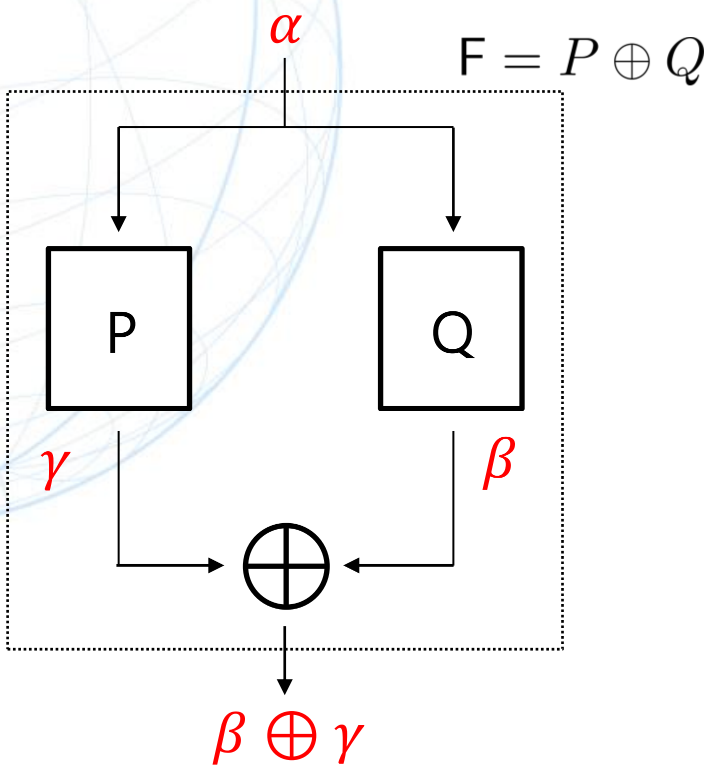


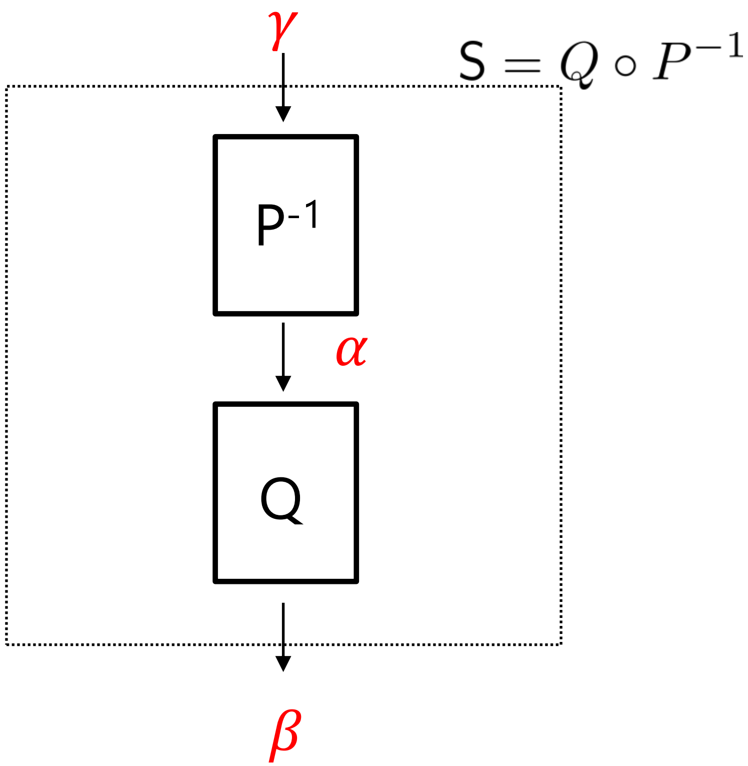


$$DP^{\mathsf{F}}_{\alpha,\beta\oplus\gamma} \approx DCP^{\mathsf{F}}_{\alpha,\gamma,\beta} = DP^{P}_{\alpha,\gamma} \times DP^{Q}_{\alpha,\beta}$$

$$DP^{\mathsf{S}}_{\alpha,\beta} \approx DCP^{\mathsf{S}}_{\alpha,\gamma,\beta} = DP^{P}_{\alpha,\gamma} \times DP^{Q}_{\gamma,\beta}$$

Differential cryptanalysis



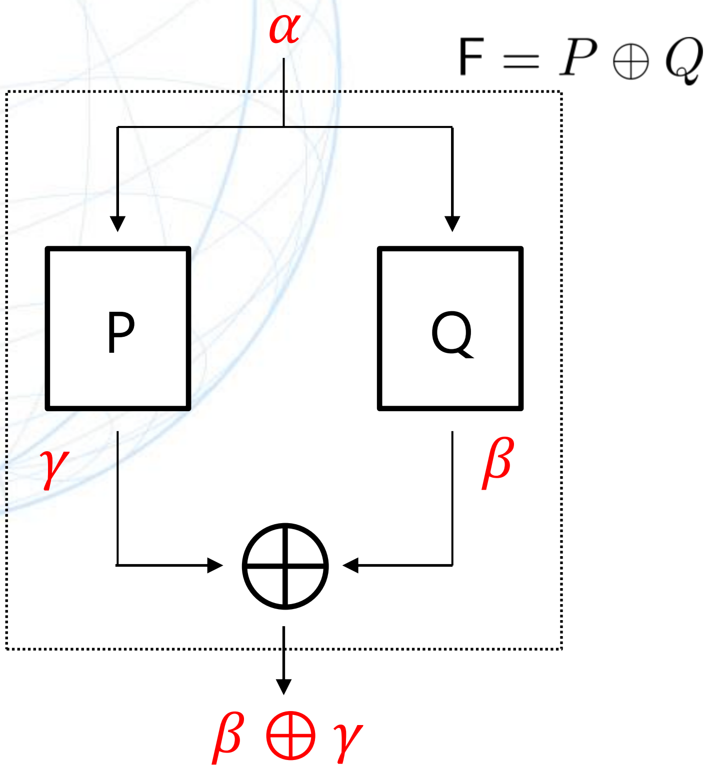


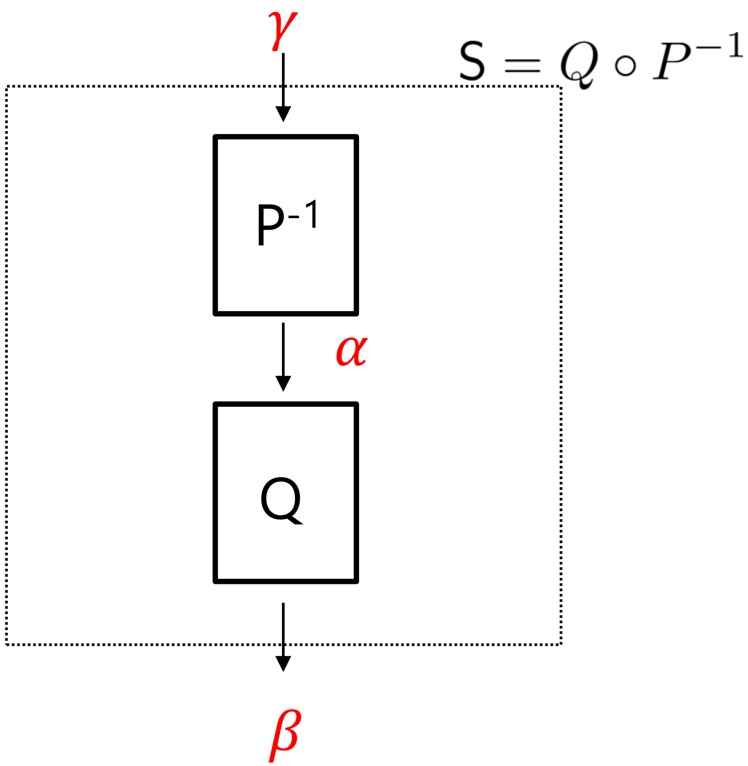
$$DP^{\mathsf{F}}_{\alpha,\beta\oplus\gamma} \approx DCP^{\mathsf{F}}_{\alpha,\gamma,\beta} = DP^{P}_{\alpha,\gamma} \times DP^{Q}_{\alpha,\beta}$$

$$DP^{\mathsf{S}}_{\gamma,\beta} \approx DCP^{\mathsf{S}}_{\gamma,\alpha,\beta} = DP^{P}_{\alpha,\gamma} \times DP^{Q}_{\alpha,\beta}$$

$$DCP^{\mathsf{F}}_{\alpha,\gamma,\beta} = DCP^{\mathsf{S}}_{\gamma,\alpha,\beta}$$

Differential cryptanalysis





$$DP^{\mathsf{F}}_{\alpha,\beta\oplus\gamma} \approx DCP^{\mathsf{F}}_{\alpha,\gamma,\beta} = DP^{P}_{\alpha,\gamma} \times DP^{Q}_{\alpha,\beta}$$

$$DP^{\mathsf{S}}_{\gamma,\beta} \approx DCP^{\mathsf{S}}_{\gamma,\alpha,\beta} = DP^{P}_{\alpha,\gamma} \times DP^{Q}_{\alpha,\beta}$$

$$DP^{\mathsf{F}}_{\alpha,\beta\oplus\gamma} \approx DP^{\mathsf{S}}_{\gamma,\beta}$$

Differential cryptanalysis

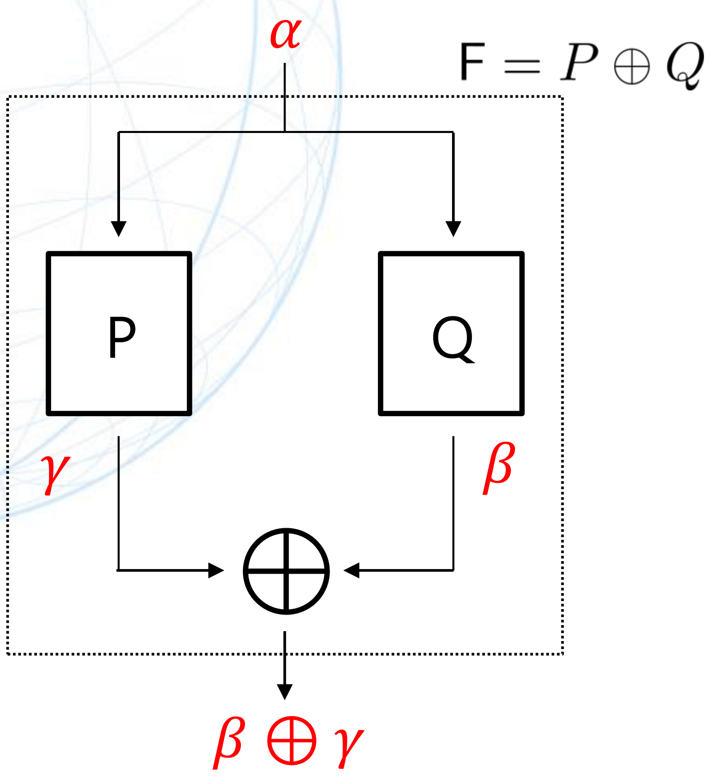
NTT

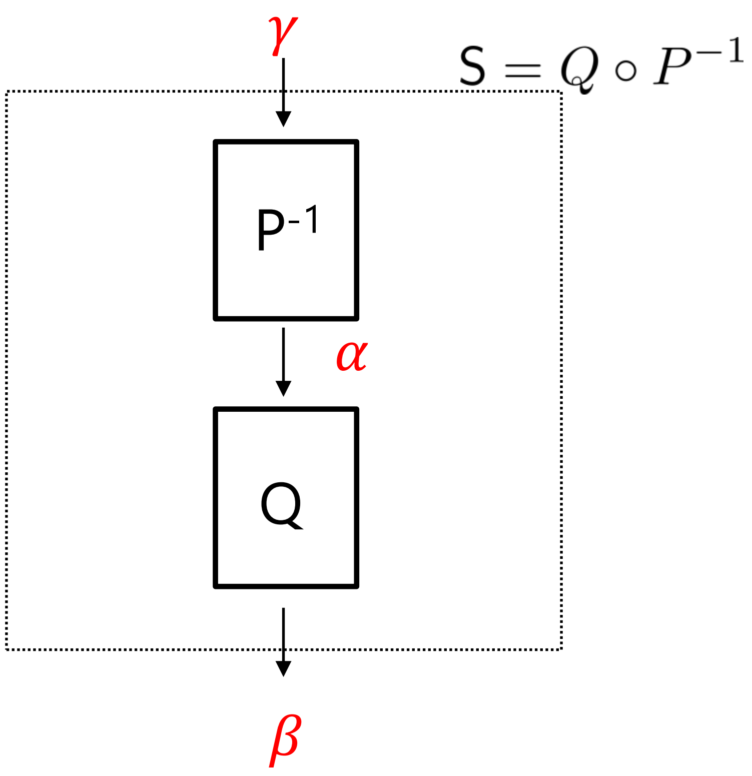
- Both constructions have **different DPs**.
  - $DP^{\mathsf{F}}_{\alpha,\beta} \neq DP^{\mathsf{S}}_{\alpha,\beta}$

- In practice, to mount the attack,
  we use the differential characteristic instead of the differential.

- Both constructions have **the same DCPs**.
  - $DP^{\mathsf{F}}_{\alpha,\beta\oplus\gamma} \approx DCP^{\mathsf{F}}_{\alpha,\gamma,\beta} = DCP^{\mathsf{S}}_{\gamma,\alpha,\beta} \approx DP^{\mathsf{S}}_{\gamma,\beta}$

When P and Q are Independent





$$DP^{\mathsf{F}}_{\alpha,\beta\oplus\gamma} = \sum_{\gamma} DP^{P}_{\alpha,\gamma} \times DP^{Q}_{\alpha,\beta}$$

$$DP^{\mathsf{S}}_{\gamma,\beta} = \sum_{\alpha} DP^{P}_{\alpha,\gamma} \times DP^{Q}_{\alpha,\beta}$$

The two probabilities are different ways of adding the same values.

It's even difficult to construct examples they differ artificially.

Differential key recovery

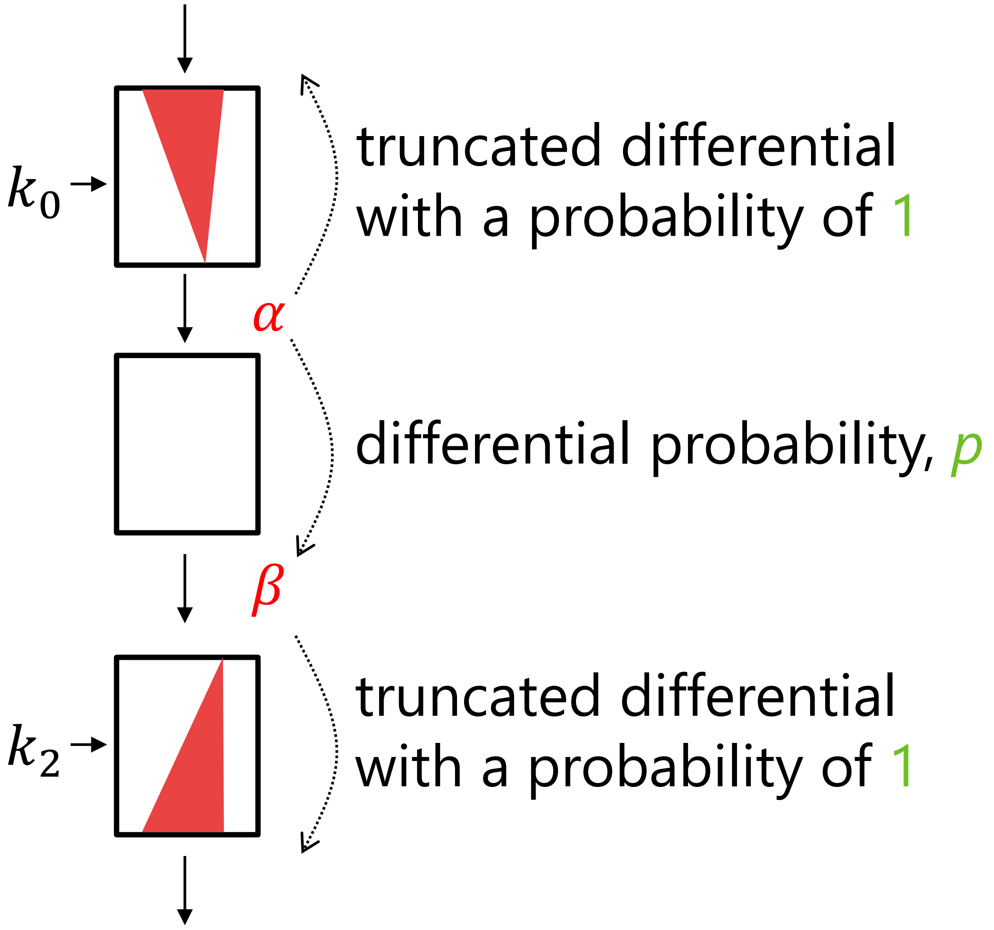
NTT

- Both constructions share almost the same immunity against the differential cryptanalysis looking at DPs.

- How about key-recovery attack?

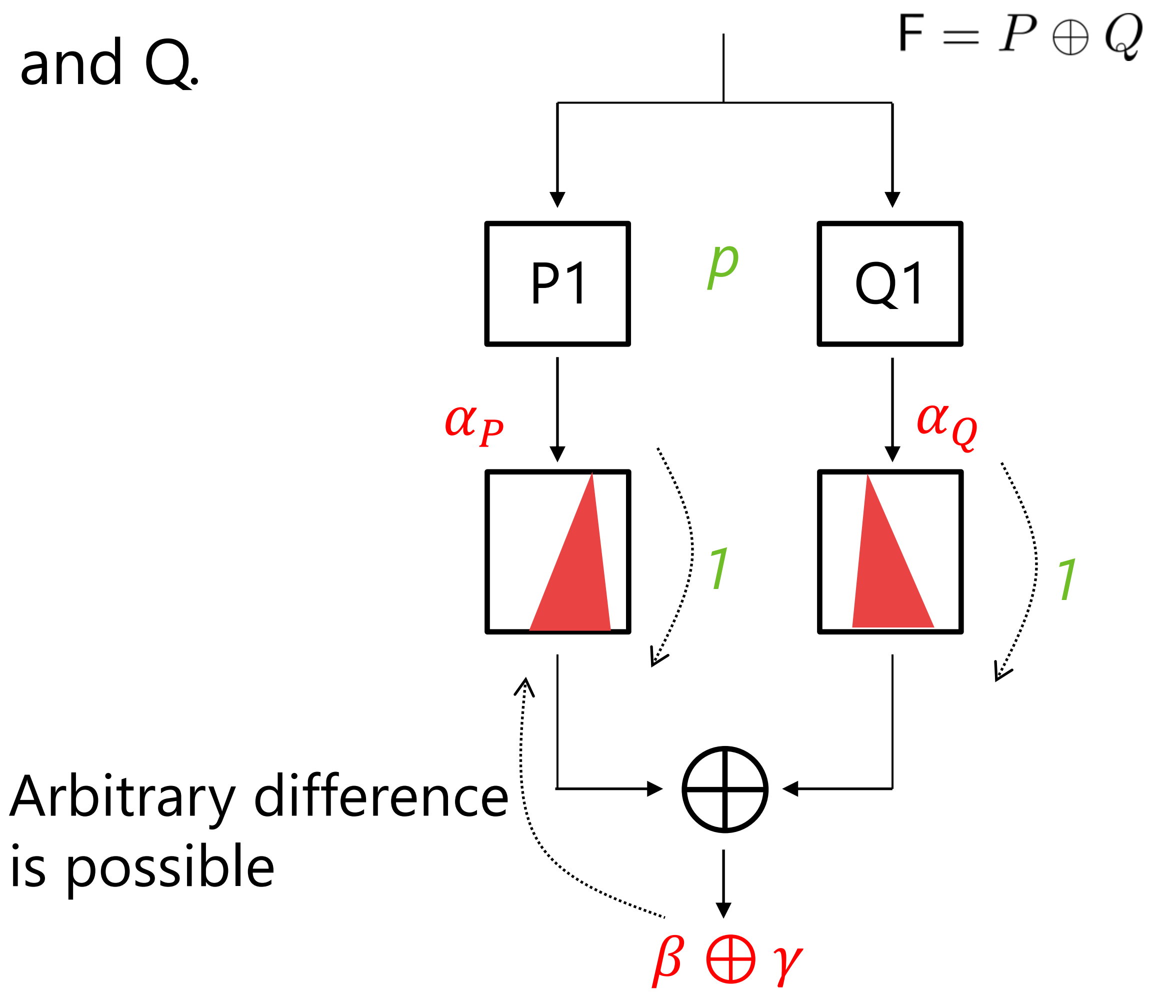
What is differential key recovery?

- Procedure
  - We guess k_0 and k_2.
  - Find the pair satisfying differential.
- Data complexity
  - It's at least p^{-1}.
  - When the correct k_0 and k_2 are guessed, we need $2p^{-1}$ queries to detect the pair.
  - We might need more because the attacker doesn't know the correct keys.
    - It depends on the cipher.



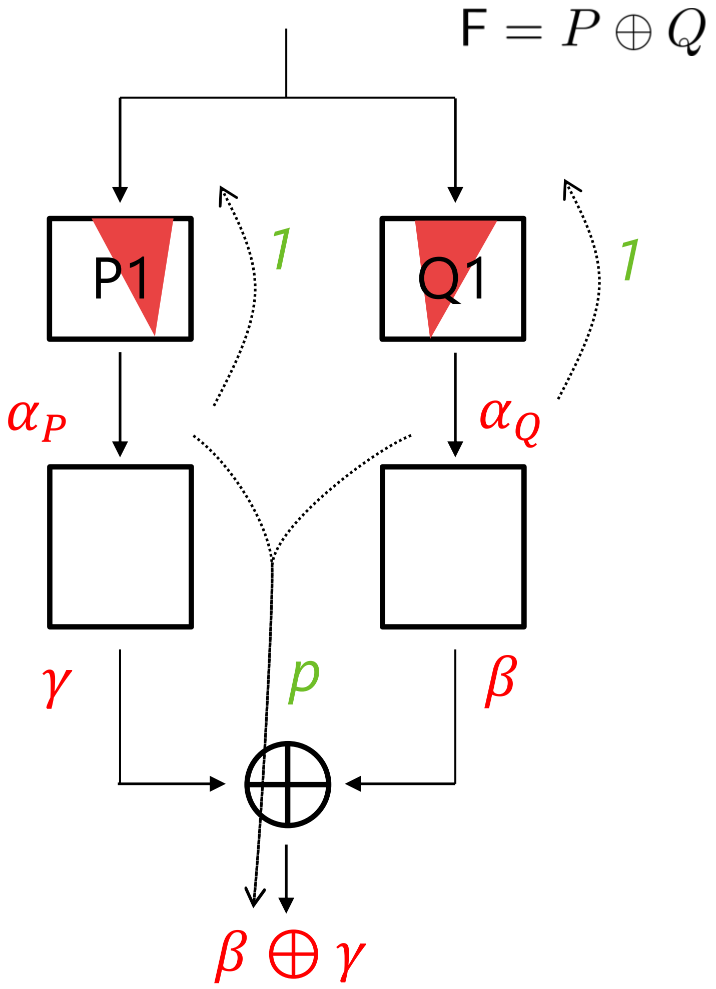
Differential key recovery against the sum

- Key recovery to the output side.
  - The attacker cannot get the output of P and Q.



Differential key recovery against the sum

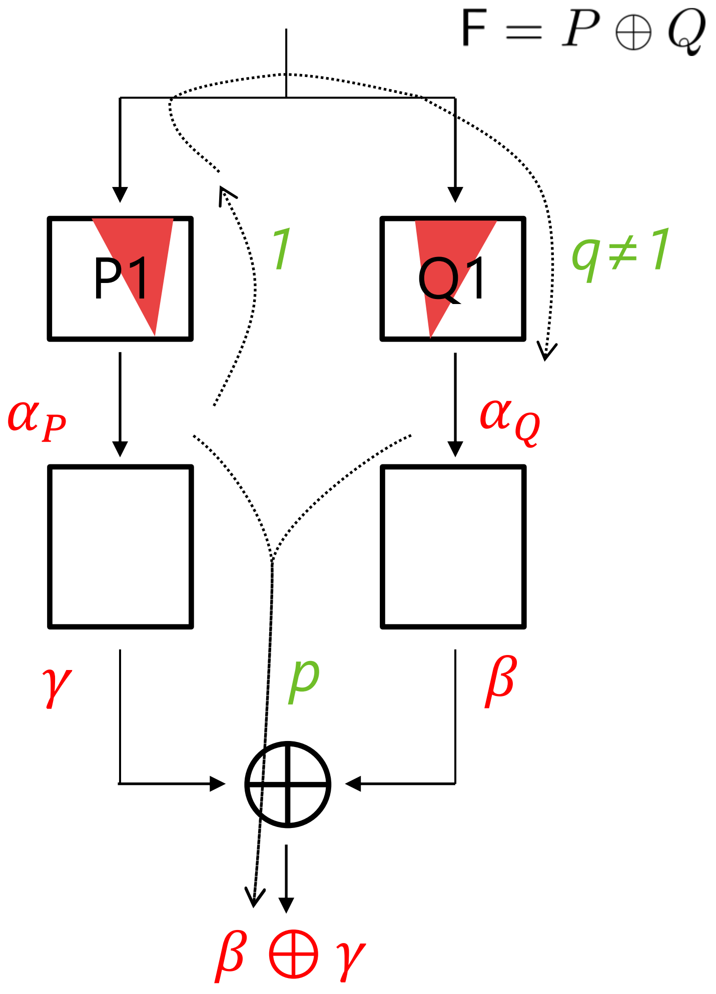
- Key recovery to the output side.
  - The attacker cannot get the output of P and Q.
- Key recovery to the input side.
  - At the first glance, it looks the same as the differential key recovery on the composition.



Differential key recovery against the sum

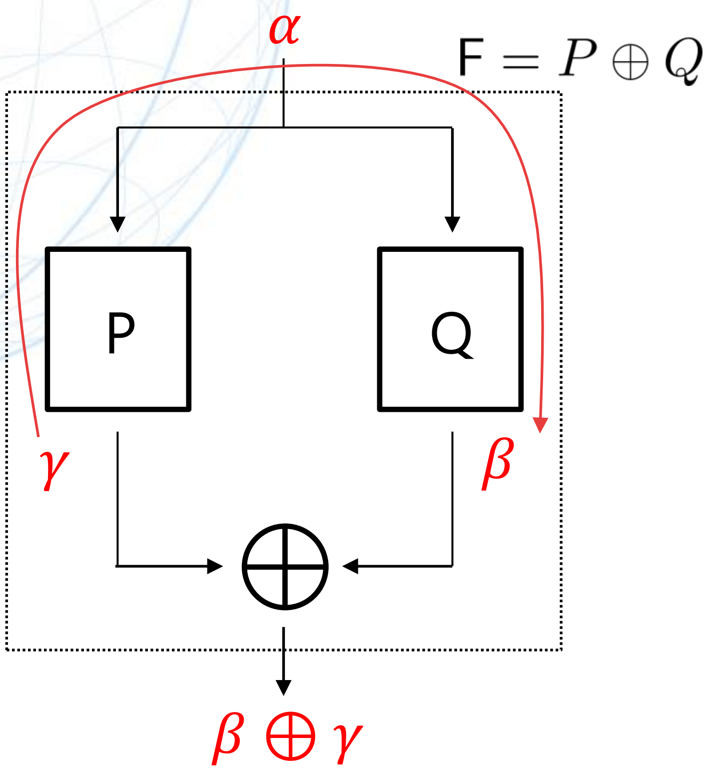
NTT

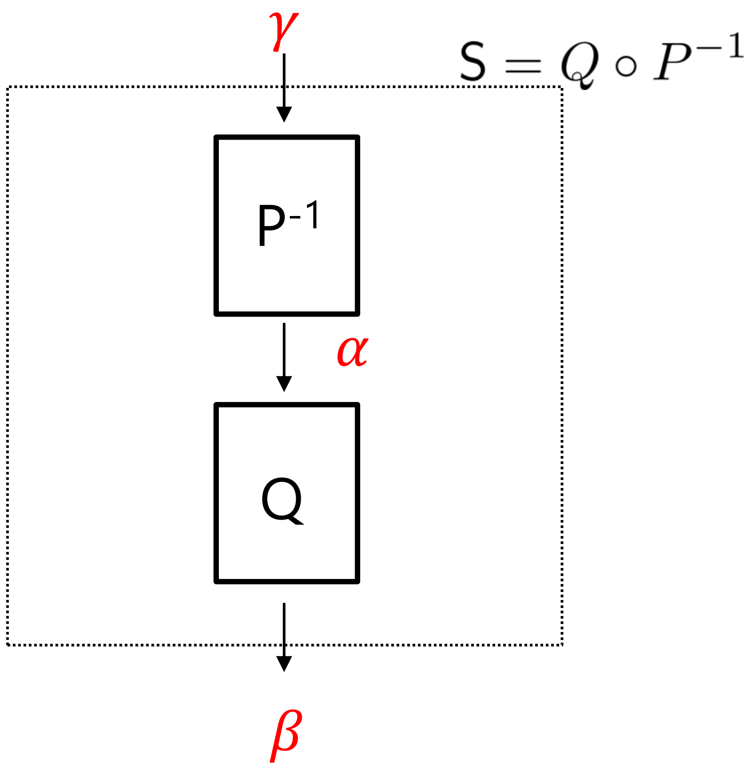
- Key recovery to the output side.
  - The attacker cannot get the output of P and Q.
- Key recovery to the input side.
  - At the first glance, it looks the same as the differential key recovery on the composition.
- Remark
  - Even if we know the correct key, it's impossible to find the pair satisfying differential with p^{-1} pairs.
  - $\mathrm{Prob}\left[\alpha_P \xrightarrow{Q_1 \circ P_1^{-1}} \alpha_Q\right] = q \ll 1$ in practice.
  - We need at least $p^{-1} \times q^{-1}$ pairs.



How about linear cryptanalysis?

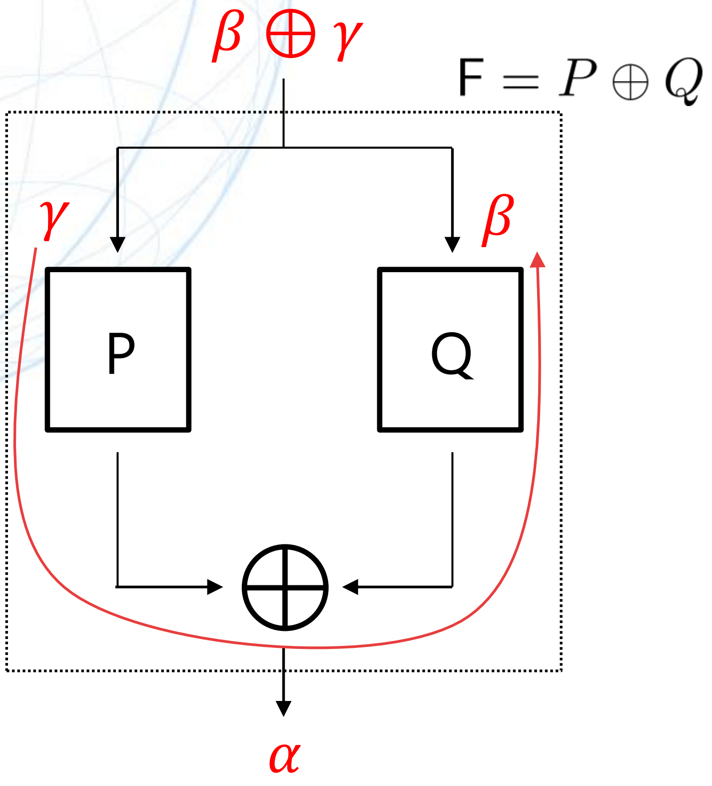
Differential cryptanalysis

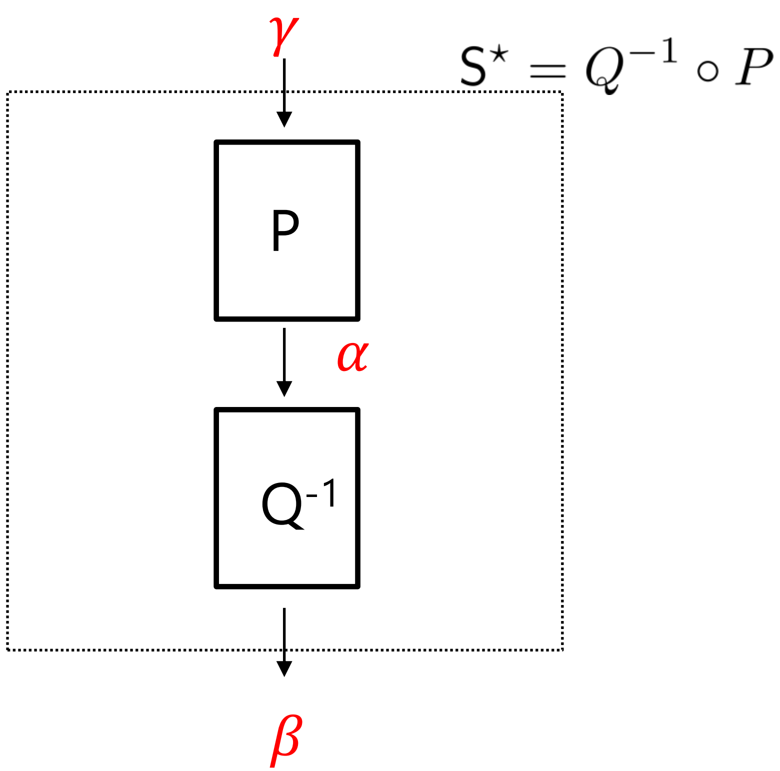




How about linear cryptanalysis?

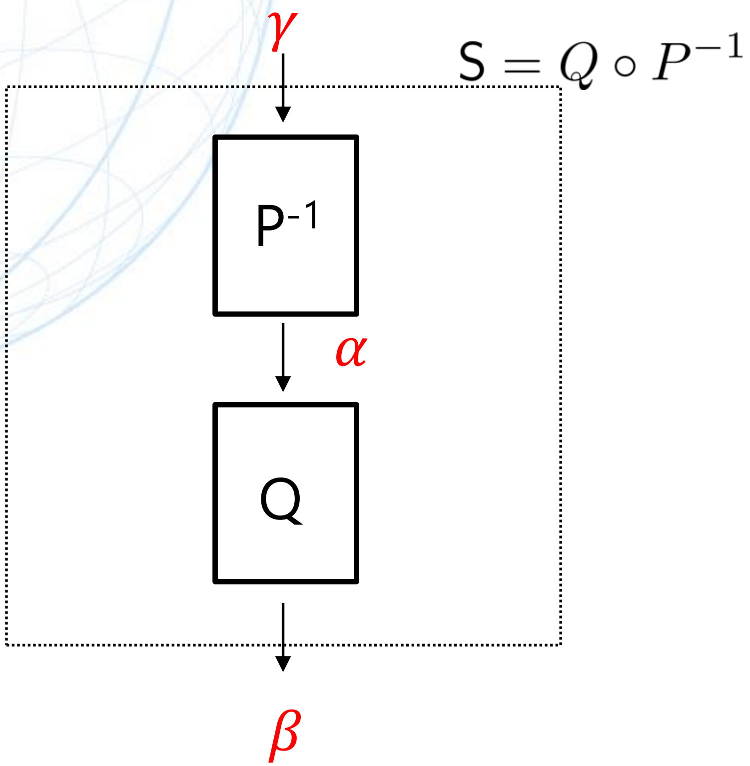
Linear cryptanalysis

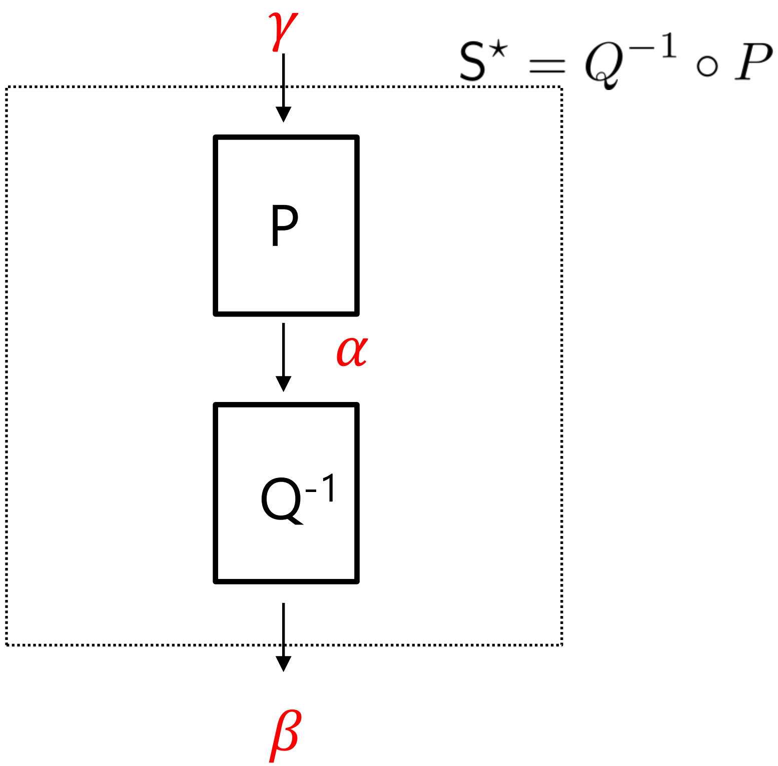




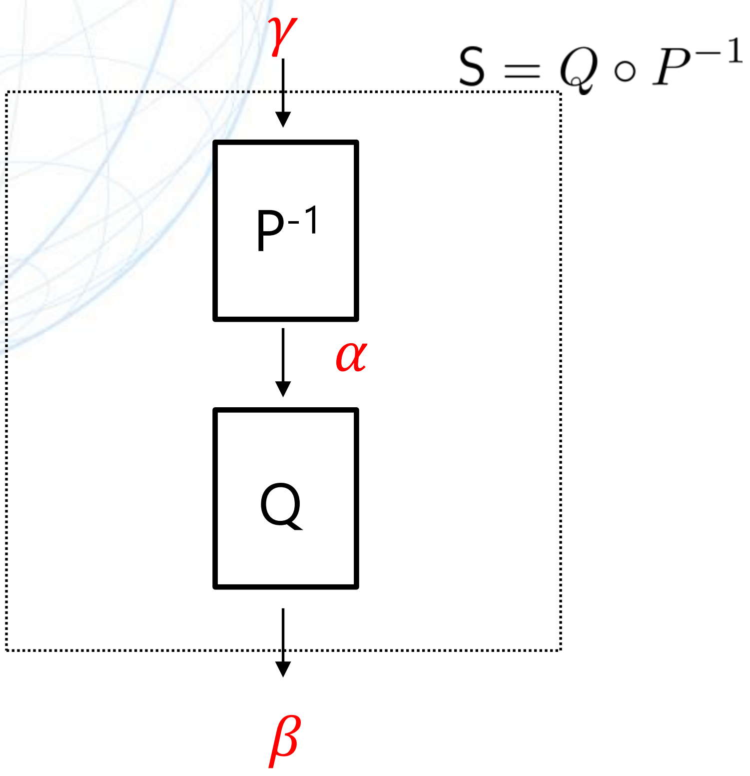
We have the same conclusion in the linear cryptanalysis.
The corresponding compassion is slightly different.

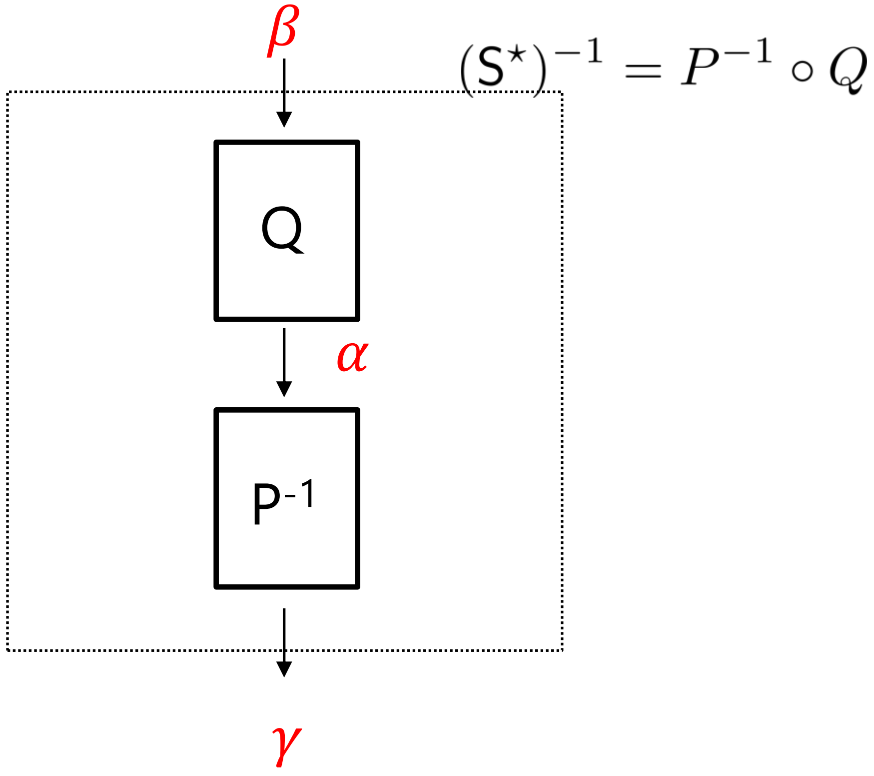
$S^\star = S$ in practice



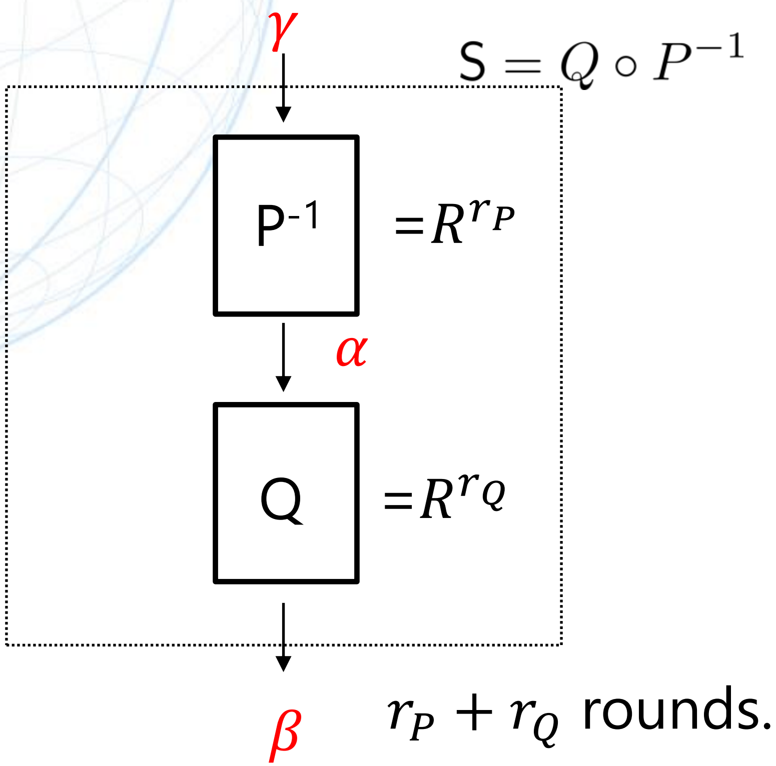


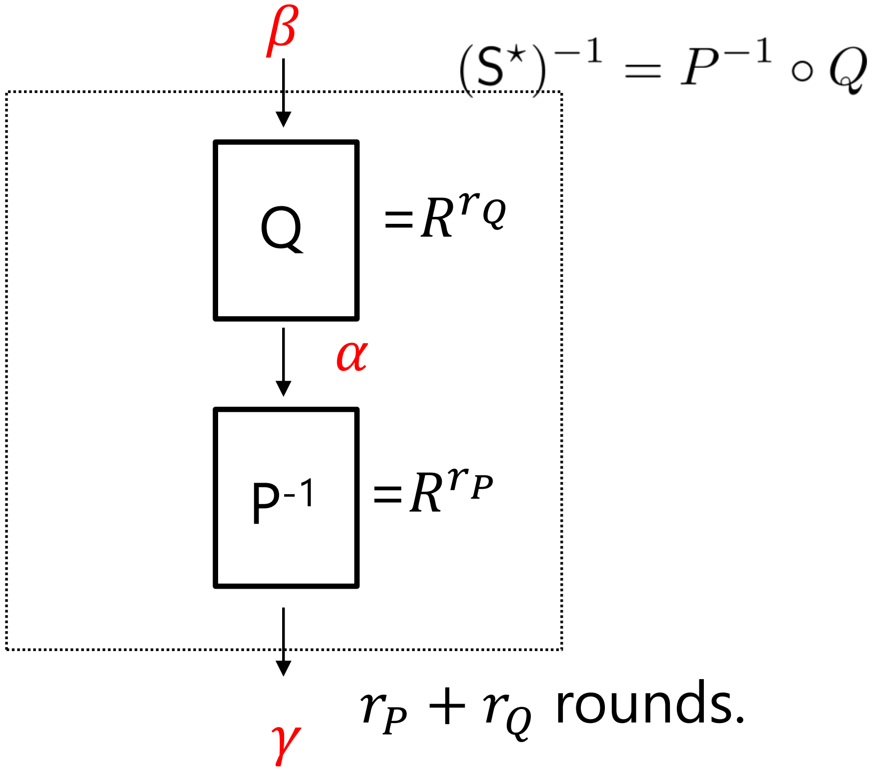
$S^\star = S$ in practice





$S^\star = S$ in practice



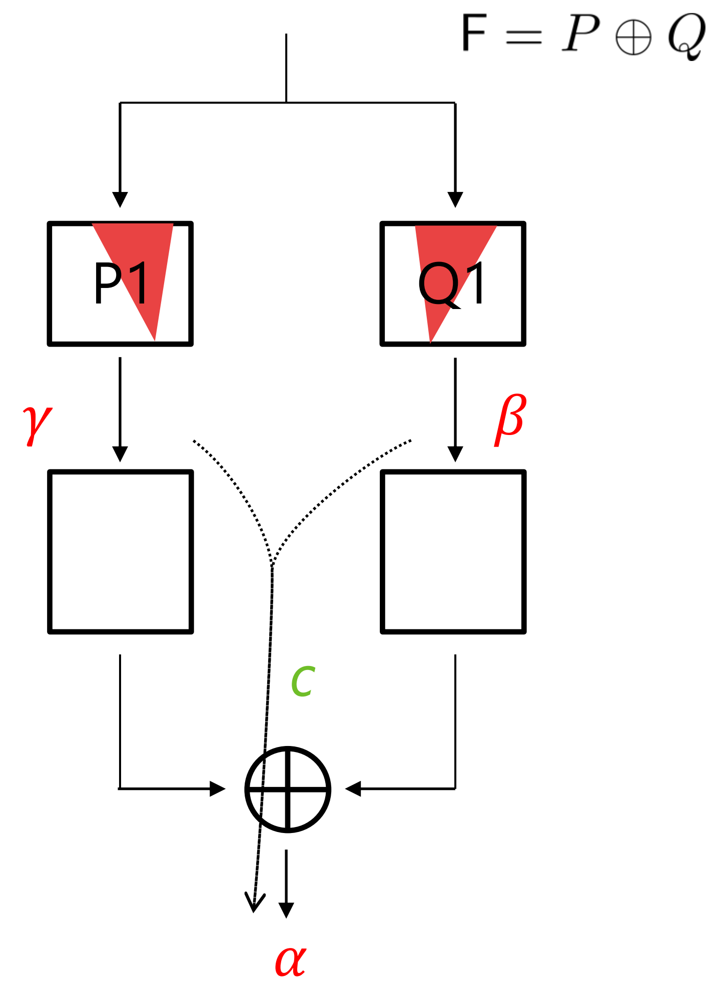


Supposing the iteration of the same round function (with different keys), $\boldsymbol{S}^\star$ and $\boldsymbol{S}$ are equivalent in practice.

Linear key recovery against the sum

NTT

- The key-recovery map is the sum of two Boolean functions.
- We don't have dependency issue like the differential cryptanalysis.
- The linear cryptanalysis is more promising strategy than the differential cryptanalysis considering the freedom of the key recovery.



Other attacks and summary

NTT

- The following statement is almost true.

$\mathsf{F} = P \oplus Q$		$\mathsf{S} = Q \circ P^{-1}$
differential linear diff-lin KR 2^{nd} order diff MitM	≈	differential Linear diff-lin boomerang MitM
Truncated diff (Diff-lin) Integral	?	

The integral attack can be the most critical attack against P ⊕ Q.
The algebraic degree is the maximum degree of either P or Q.

Other attacks and summary

- The following statement is almost true.

$\mathsf{F} = P \oplus Q$		$\mathsf{S} = Q \circ P^{-1}$
differential		differential
linear		Linear
diff-lin KR	$\approx$	diff-lin
2nd order diff		boomerang
MitM		MitM

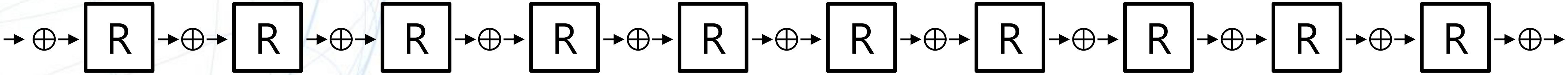
Truncated diff
(Diff-lin)
Integral

?

Differential-type attacks have critical drawback in the key recovery.
Roughly speaking, the attack doesn't work unless the full-round secret-key distinguisher.

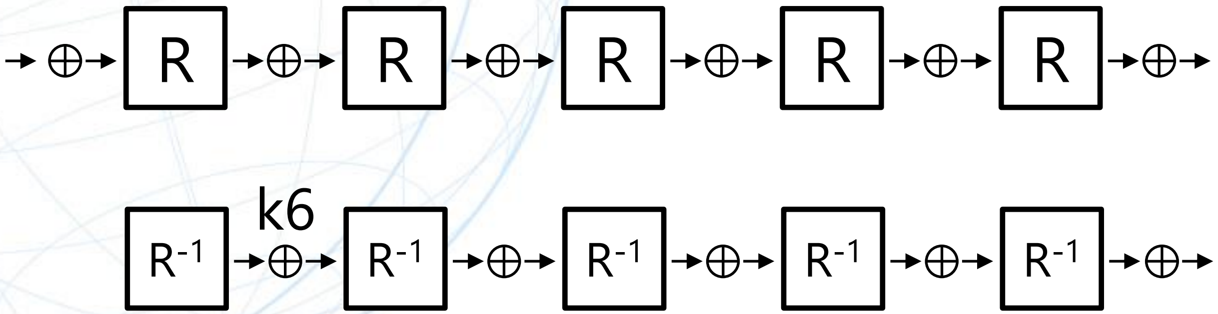
Instantiation, ZIP-AES

AES-128



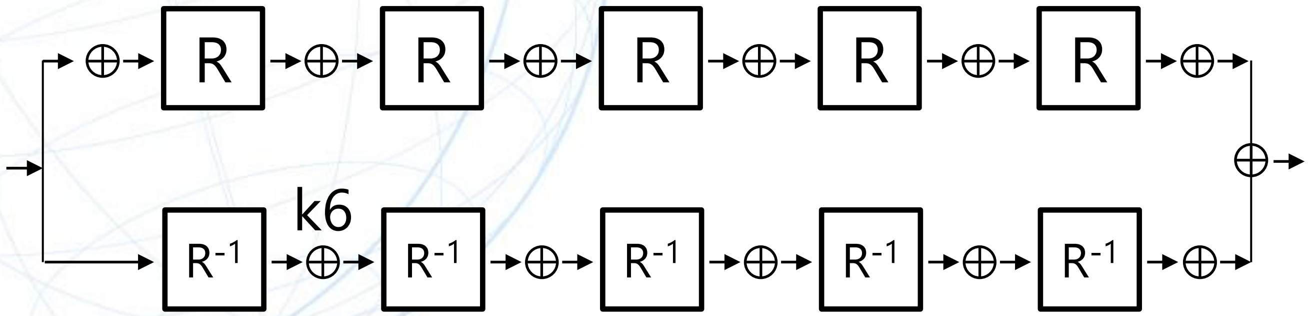
Instantiation, ZIP-AES

AES-128 … cut and



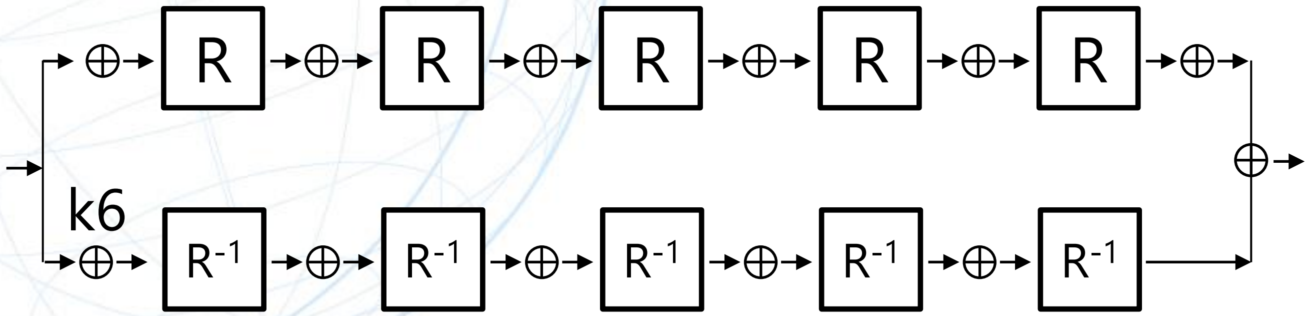
Instantiation, ZIP-AES

AES-128 … cut and zip



Instantiation, ZIP-AES

ZIP-AES



Security analysis of ZIP-AES

NTT

- We inherit almost the same security from the AES.
- We only analyze some exceptions.
  - Differential-linear
    - So far, the best autocorrelation of 5-round AES is $2^{-55.66}$.
    - Thus, the autocorrelation is lower than $2^{-111.32}$.
    - The 3-roud AES has the autocorrelation of $2^{-7.66}$, but the autocorrelation of another branch is significantly lower than it.
  - Integral
    - We have the distinguisher on 4-round ZIP-AES with 2^{64} CPs.
    - It's unlikely we add key recovery.
      - Both branch takes the input of the integral distinguisher simultaneously.
      - If we add 1-round key recovery, we need to construct such a set via 2 rounds.
  - Truncated differential, and Mixture
    - So far, 2+2 or 3+3 has slightly higher probability than a generic attack.
    - No successful attack from 4+4.

Performance

Table 2: Performance comparison on the counter mode.

	cycle-per-byte						counter
	16B	32B	256B	2KB	16KB	128KB	
AES	3.56	1.84	0.51	0.36	0.34	0.34	integer
AES-PRF	3.63	1.94	0.55	0.39	0.37	0.37	integer
ZIP-AES	2.96	1.58	0.53	0.41	0.39	0.39	integer

- As expected, ZIP-AES is lower latency than the others.
- It's unfortunate for us that AES-NI doesn't support the straightforward AES inverse round function.
  - Straightforward inverse function, $AK \circ SB^{-1} \circ SR^{-1} \circ MC^{-1}$.
  - AESDEC, $AK \circ MC^{-1} \circ SR^{-1} \circ SB^{-1}$.
  - We need MC^{-1} additionally, but MC^{-1} is double slower than the round function and its inverse.

Performance

NTT

Table 2: Performance comparison on the counter mode.

	cycle-per-byte						counter
	16B	32B	256B	2KB	16KB	128KB	
AES	3.53	1.81	0.47	0.35	0.34	0.33	gray code
AES-PRF	3.57	1.88	0.51	0.36	0.34	0.34	gray code
ZIP-AES	2.90	1.61	0.47	0.34	0.33	0.33	gray code

- We use the gray code counter instead of the integer counter.
- The increment is linear.
  - We apply MC^{-1} to the initial state and counter in advance.
  - We can avoid MC^{-1}, and the throughput is improved.

Conclusion

NTT

- General practical cryptanalysis
  - Analyze the cipher without detailed specification (like a generic attack).
  - Compare the security from well-studied construction (like a reduction security).
- The sum is almost equivalently secure to the composition.
  - Besides, it's more secure if we focus on the key-recovery efficiency.
  - We reported an error in the existing attack against Orthros because of the difficulty of the key recovery.
  - Linear-type attack is more suited considering the key recovery.
- ZIP-AES
  - Cut AES and zip them.