MITSUBISHI ELECTRIC
Changes for the Better

家庭から宇宙まで、エコチェンジ。 eco Changes

New Bounds for Keyed Sponges with Extendable Output: Independence between Capacity and Message Length

Yusuke Naito

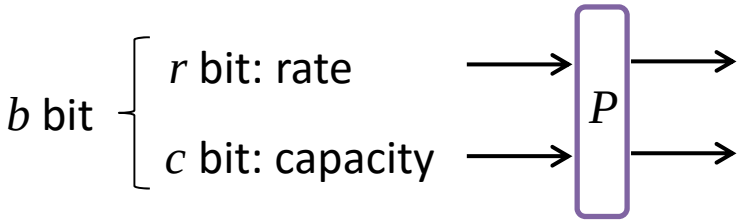
Mitsubishi Electric Corporation

Kan Yasuda

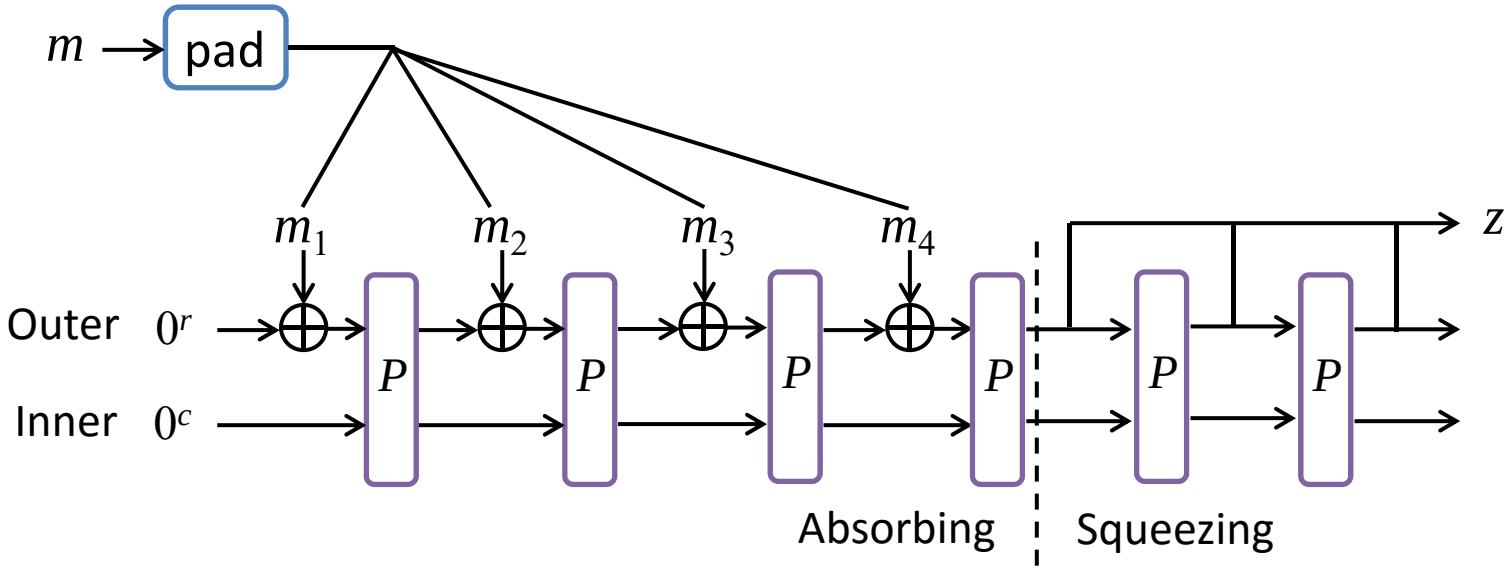
NTT Secure Platform Laboratories

Sponge

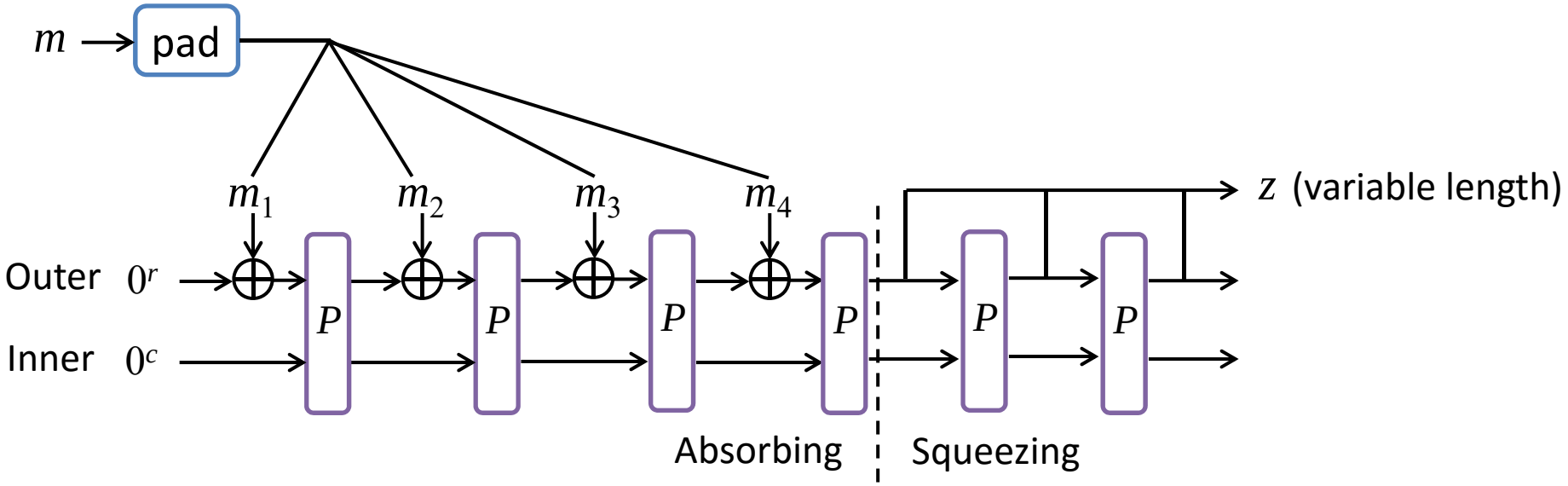
- Based on a permutation $P: \{0,1\}^b \rightarrow \{0,1\}^b$



- Iterate permutation P



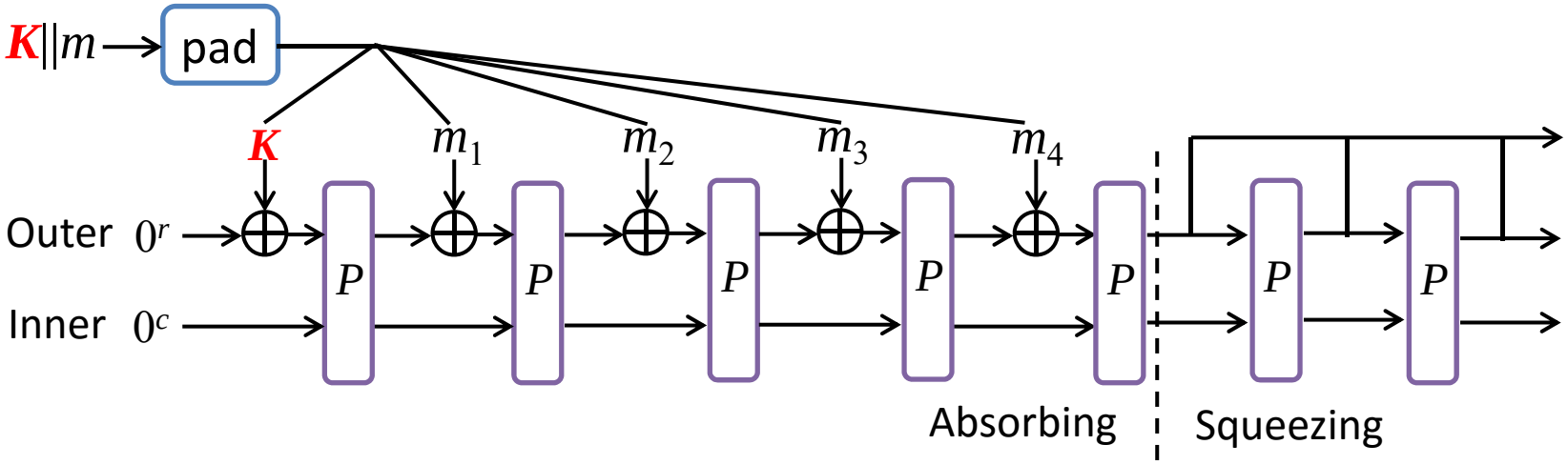
Sponge with Extendable Output



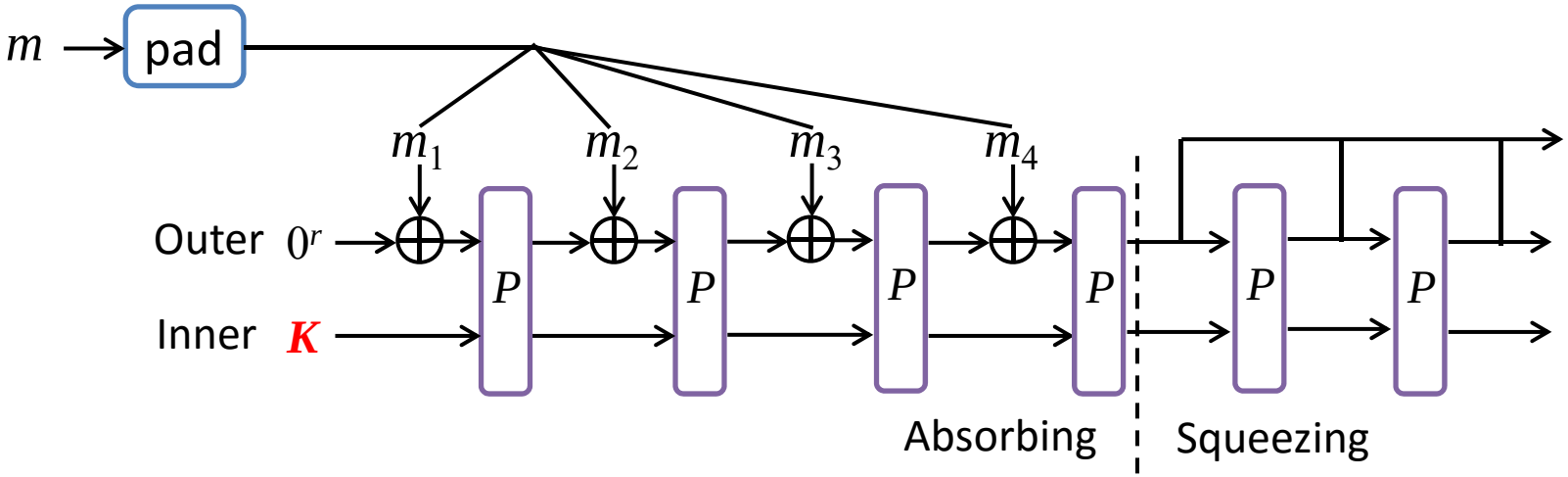
- Sponge with extendable output
  - used as the constructions of SHAKE128, SHAKE256 in FIPS 202
  - Designed to construct key derivation functions

Keyed Sponges with Extendable Output

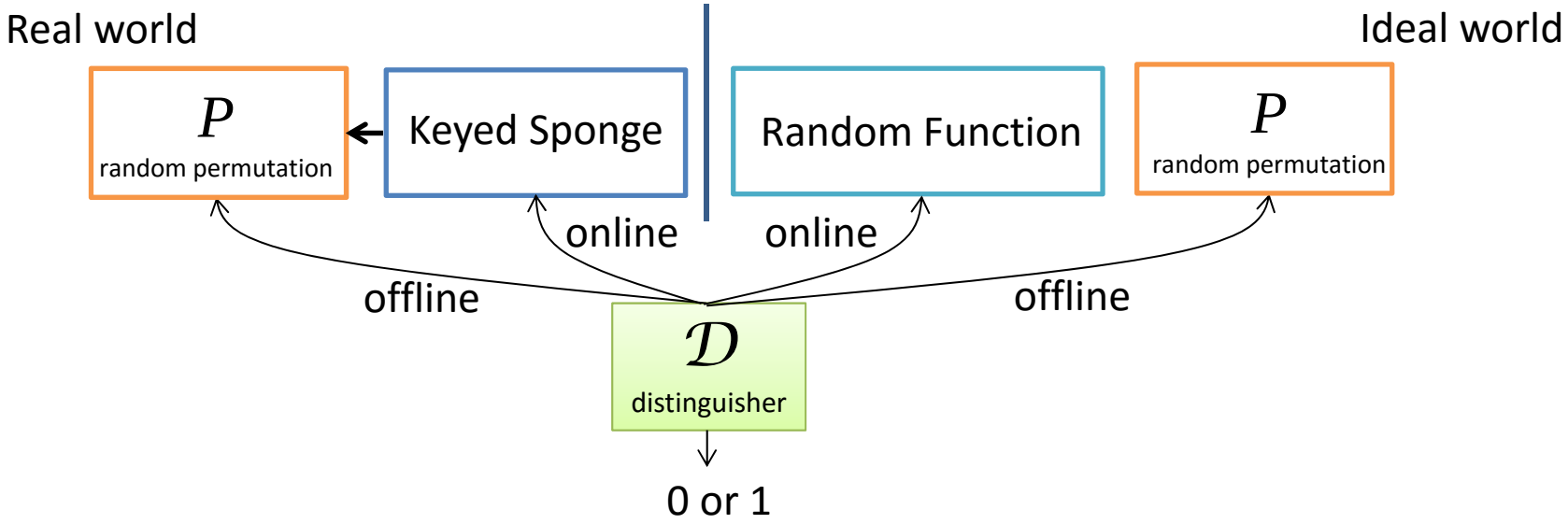
Outer Keyed Sponge (OKS)



Inner Keyed Sponge (IKS)



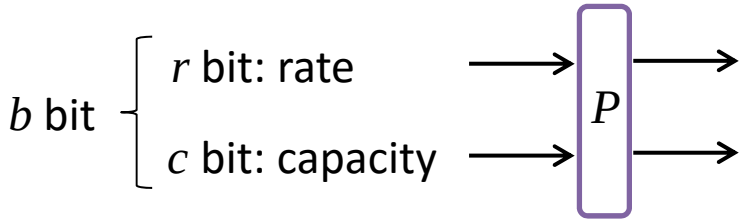
PRF-Security of Keyed Sponges



- Parameters
  - ℓ is the maximum input length to a keyed sponge in blocks
  - q is the number of online queries
  - Q is the number of offline queries

Previous PRF-Security Bounds

- There are two terms:
  - capacity term e.g., $(\ell q+Q)^2/2^c$, $(\ell q)^2/2^c$, etc
  - b-term e.g., $(\ell q)^2/2^b$, $\ell qQ/2^b$, etc



- Since $c < b$ (e.g., b=1600, c=256, 512), the capacity term becomes a dominant term in the PRF-security bounds
- The capacity term has been improved

	Capacity term	Target
Bertoni et al. (Indiff.) (EUROCRYPT'08)	$(\ell q+Q)^2/2^c$	OKS
Andreeva et al. (FSE'15)	$((\ell q)^2+\mu Q)/2^c$ μ is multiplicity: $2\ell q/2^r \leqq \mu \leqq 2\ell q$	OKS and IKS
Gazi et al. (CRYPTO'15)	$(\ell q+q^2+qQ)/2^c$	
Mennink et al. (ASIACRYPT'15)	$(\ell q^2+\mu Q)/2^c$ μ is multiplicity: $2\ell q/2^r \leqq \mu \leqq 2\ell q$	IKS [*]

∃attack with prob. $(q^2+qQ)/2^c$
If $\ell \leqq q$ or $\ell \leqq Q$ then
the bound is tight

[*] Support the constructions with full message state absorption

Comparison and Our Result

Open problem for keyed sponges with extendable output:
Improve the capacity terms so that they become tight terms

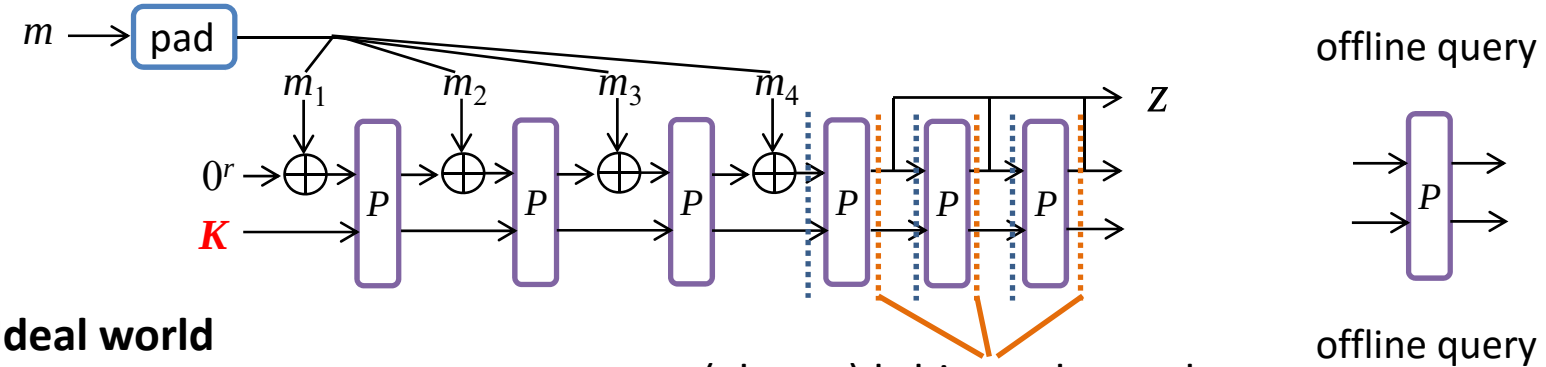
	IKS	OKS	Extendable output	Tightness of c-term
Bertoni et al.		✔	✔	
Andreeva et al.	✔	✔	✔	
Gazi et al.		✔		✔
Mennink et al.	✔		✔	
This paper	✔	✔	✔	✔

Today's talk

PRF-Security Proof of IKS

Real world

online query

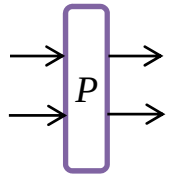


offline query

Ideal world

online query

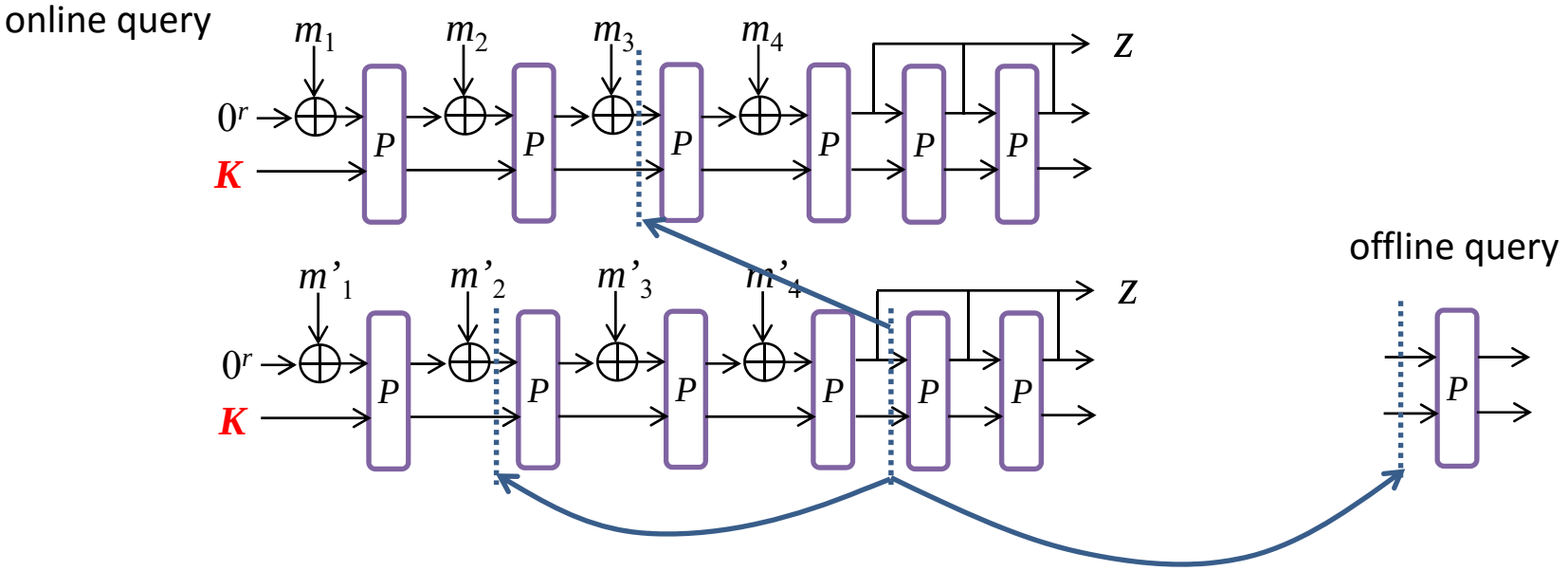
offline query



- For any query to a random function, the response is randomly drawn
- If all outputs of IKS can be seen as random values then the real world and the ideal world are indistinguishable
- If all inputs to P that produces outputs of IKS are new inputs then all outputs of IKS become (almost) random values
- The distinguishing prob.
  ≦The prob. that some input to P that produces the output of IKS is not new

PRF-Security Proof of IKS

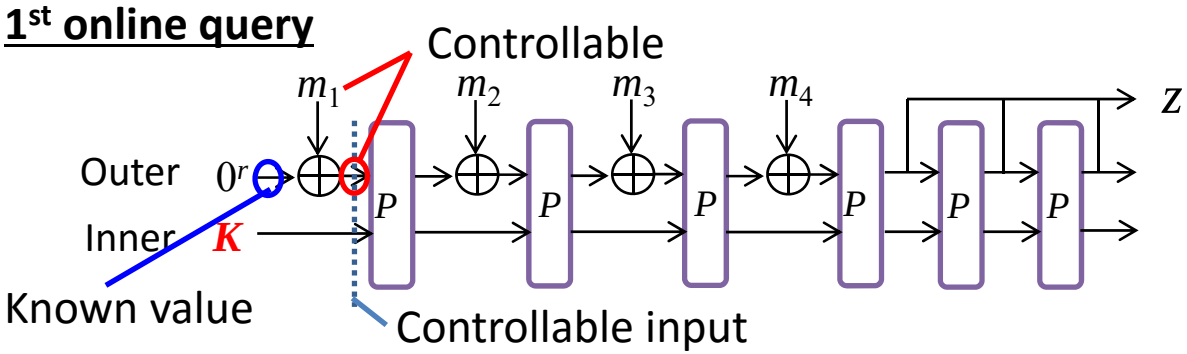
Real world



- The distinguishing prob.
  ≦The prob. that some input to P that produces the output is not a new input
  ≦The prob. that a collision in inputs to P occurs
- We categorize inputs to P in IKS into two sorts of inputs
  - Controllable input
  - Uncontrollable input

Controllable Input and Uncontrollable Input

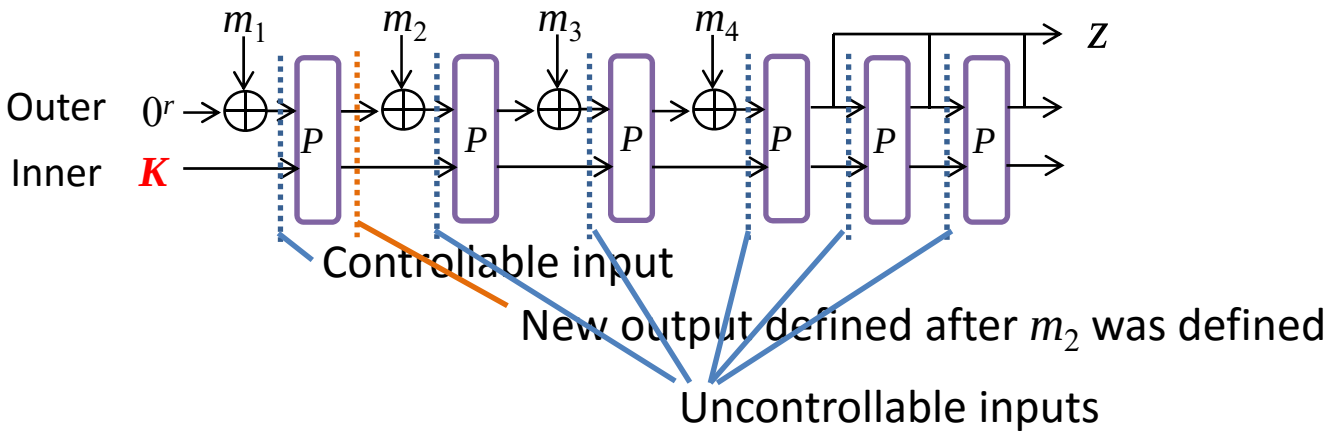
- Controllable input
  - The outer part can be controlled
  - The inner part cannot be controlled
- Uncontrollable input
  - The outer and inner parts cannot be controlled



Controllable Input and Uncontrollable Input

- Controllable input
  - The outer part can be controlled
  - The inner part cannot be controlled
- Uncontrollable input
  - The outer and inner parts cannot be controlled

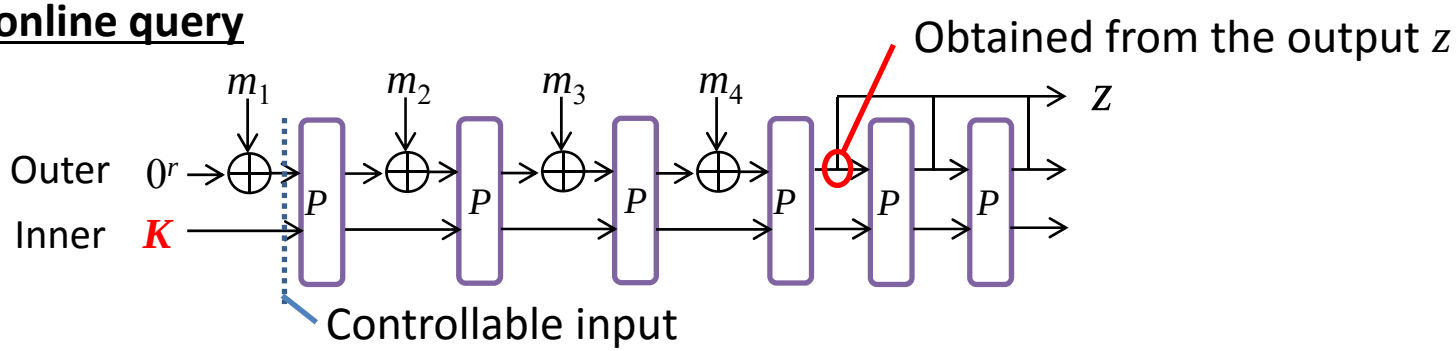
1st online query



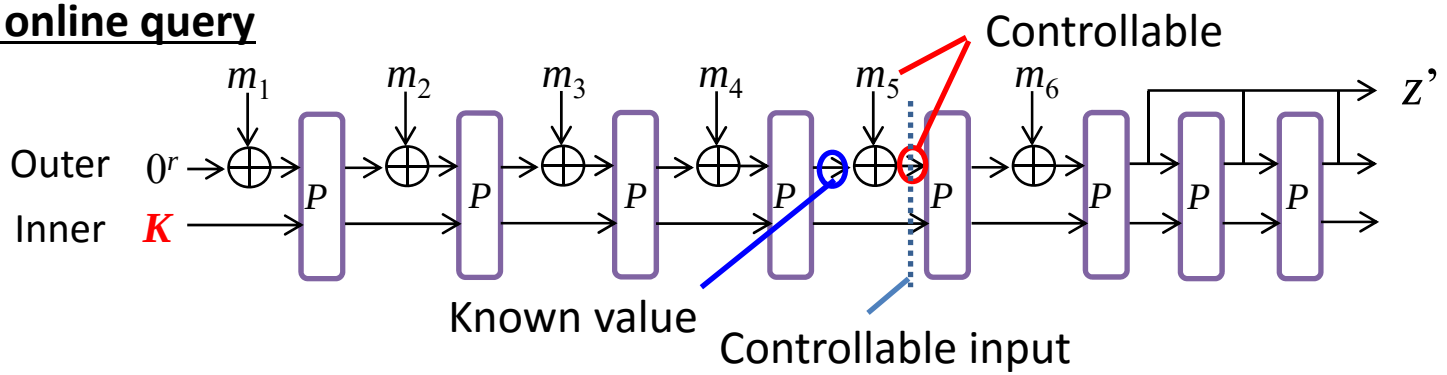
Controllable Input and Uncontrollable Input

- Controllable input
  - The outer part can be controlled
  - The inner part cannot be controlled
- Uncontrollable input
  - The outer and inner parts cannot be controlled

1st online query



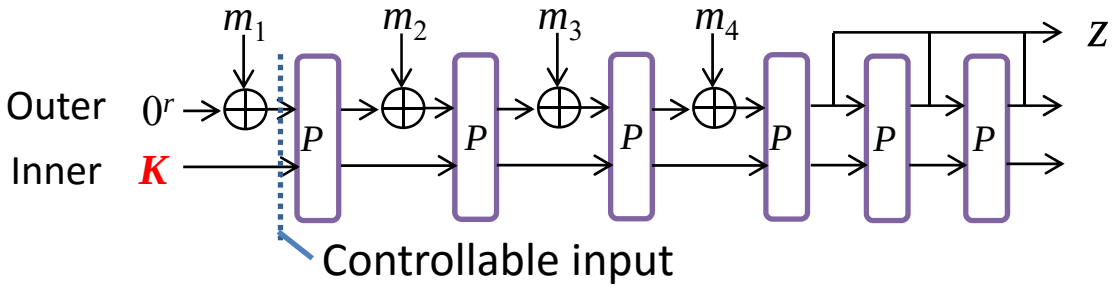
2nd online query



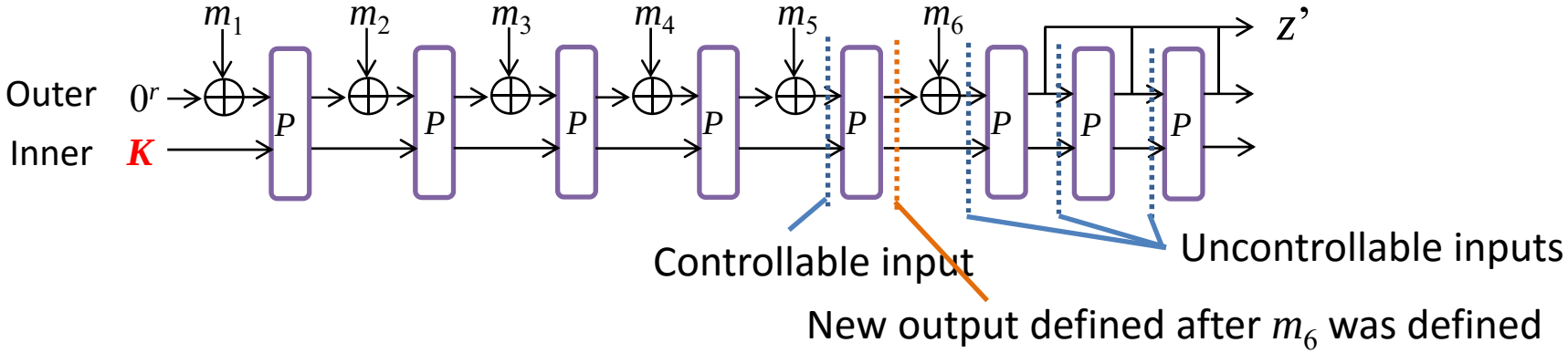
Controllable Input and Uncontrollable Input

- Controllable input
  - The outer part can be controlled
  - The inner part cannot be controlled
- Uncontrollable input
  - The outer and inner parts cannot be controlled

1st online query

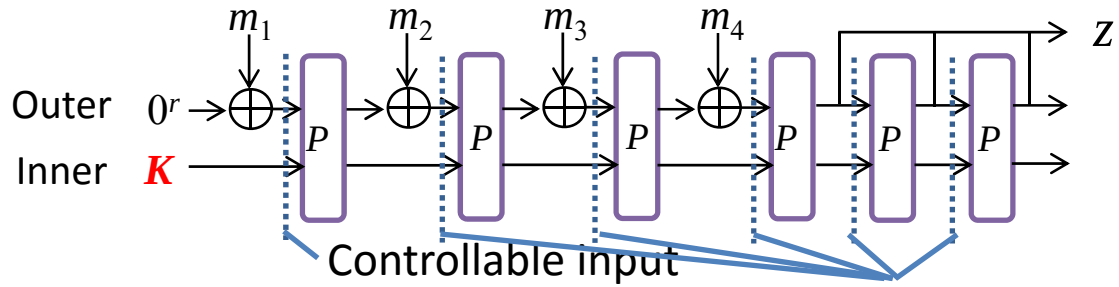


2st online query

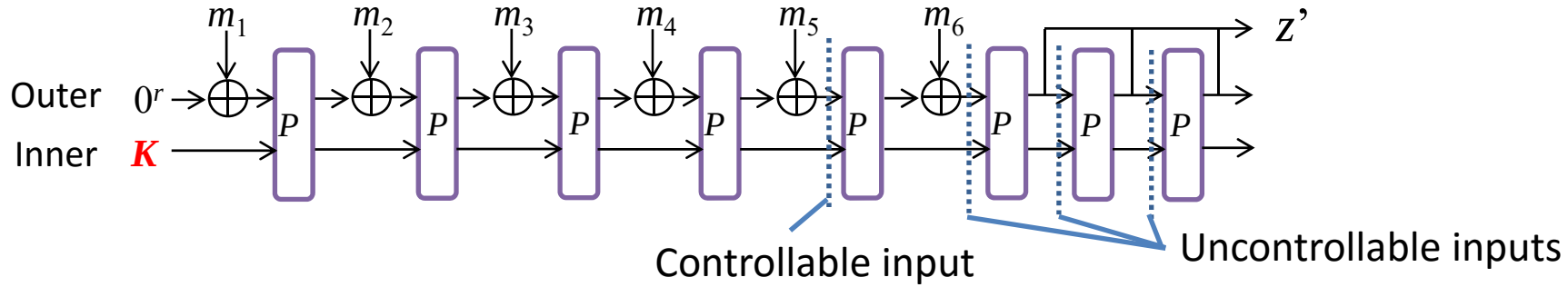


Controllable Input and Uncontrollable Input

1st online query



2st online query



- Controllable inputs
  - For each online query, the number of controllable inputs is at most 1
  - The total number of controllable inputs is at most q
- Uncontrollable inputs
  - The total number of inputs to the random permutation in IKS is at most ℓq
  - The total number of uncontrollable inputs is at most ℓq

Controllable Input and Uncontrollable Input

- The features of controllable inputs and uncontrollable inputs

Inputs to P	Outer part (r bit)	Inner part (c bi)	Number
Controllable input	Not random	Random	q
Uncontrollable input	Random	Random	ℓq

Bound of Distinguishing Probability

- The distinguishing prob. ≦The prob. that a collision in inputs to P occurs

Inputs to P	Outer part (r bits)	Inner part (c bits)	Number
Controllable input	Not random	Random	q
Uncontrollable input	Random	Random	ℓq
Input by offline query	Not random	Not random	Q

- The prob. that a collision in inputs to P occurs is bounded by the sum of probabilities of
  - collision in controllable inputs ⇒ $q^2/2^c$
  - collision in uncontrollable inputs ⇒ $(\ell q)^2/2^b$
  - collision between controllable inputs and uncontrollable inputs ⇒ $\ell q^2/2^b$
  - collision between controllable inputs and inputs by offline queries ⇒ $qQ/2^c$
  - collision between uncontrollable inputs and inputs by offline queries ⇒ $\ell qQ/2^b$
- The distinguishing prob. ≦ $(q^2+qQ)/2^c + (\ell q^2 + (\ell q)^2 + \ell qQ)/2^b$

∃attack with prob. $(q^2+qQ)/2^c$

MITSUBISHI ELECTRIC
Changes for the Better

Conclusion

	Capacity term	Target
Indifferentiability (EUROCRYPT'08)	$(\ell q+Q)^2/2^c$	OKS
Andreeva et al. (FSE'15)	$((\ell q)^2+\mu Q)/2^c$ μ is multiplicity: $2\ell q/2^r \leqq \mu \leqq 2\ell q$	OKS and IKS
Gazi et al. (CRYPTO'15)	$(\ell q+q^2+qQ)/2^c$	OKS with single block output
Mennink et al. (ASIACRYPT'15)	$(\ell q^2+\mu Q)/2^c$ μ is multiplicity: $2\ell q/2^r \leqq \mu \leqq 2\ell q$	IKS
This paper	$(q^2+qQ)/2^c$ (Tight)	IKS and OKS

MITSUBISHI ELECTRIC
Changes for the Better

Thank You!