MITSUBISHI ELECTRIC
Changes for the Better

家庭から宇宙まで、エコチェンジ。 eco Changes

Output Masking of Tweakable Even-Mansour can be Eliminated for Message Authentication Code

Shoichi Hirose[†] **Yusuke Naito[‡]** Takeshi Sugawara[‡]

[†] University of Fukui

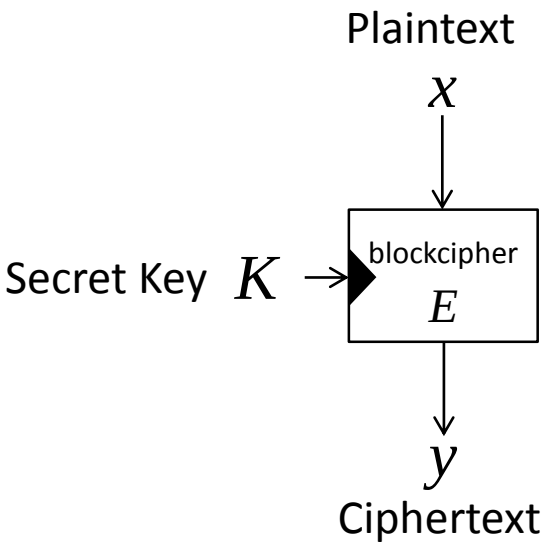
[‡] Mitsubishi Electric Corporation

MITSUBISHI ELECTRIC
Changes for the Better

Starting Point of Our Research

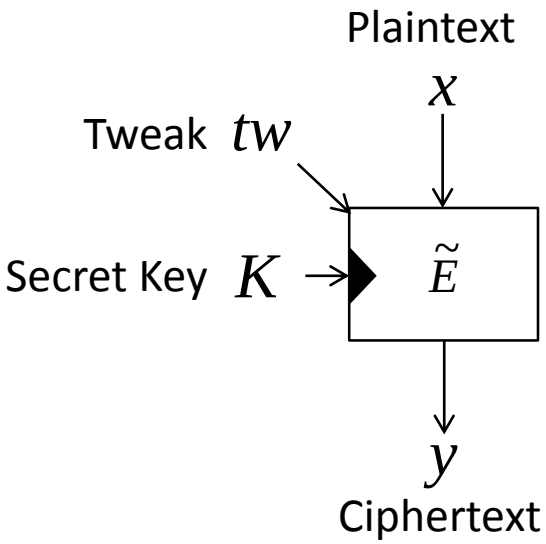
Simplification of Tweakable Blockcipher Design

Blockcipher



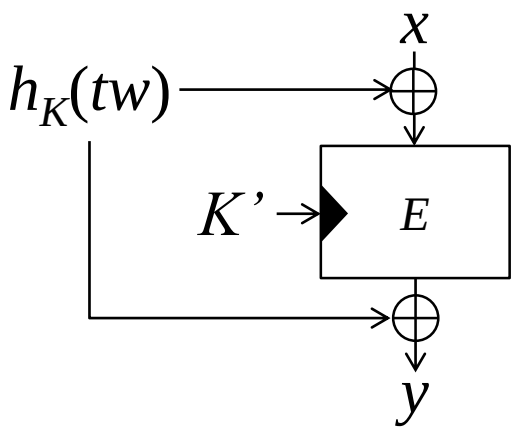
- Input: plaintext and secret key
- Output: ciphertext
- Fixing a secret key, a blockcipher becomes a permutation
- Rekeying is costly

Tweakable BlockCipher (TBC) $\tilde{E}$



- Take an additional input tweak tw
  - ✓ Role: Changing tw = Rekeying
  - ✓ Cost: Changing tw << Rekeying

LRW (Liskov-Rivest-Wagner2002)



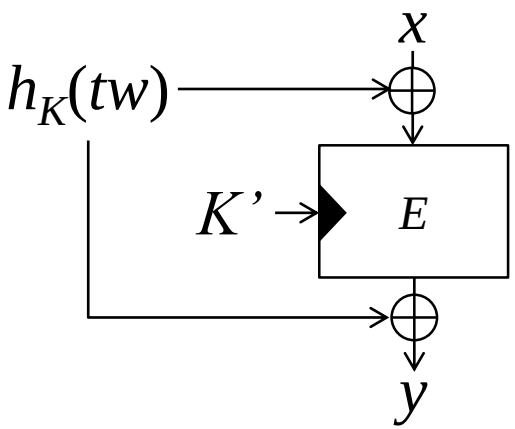
- Based on
  - ✓ blockcipher $E_{K'}$
  - ✓ Keyed hash function h_K
- Security
  - ✓ CCA secure TBC
  - ✓ Birthday bound
  - ✓ Assuming $E_{K'}$: RP and h_K : AXU hash function

(Random Permutation)

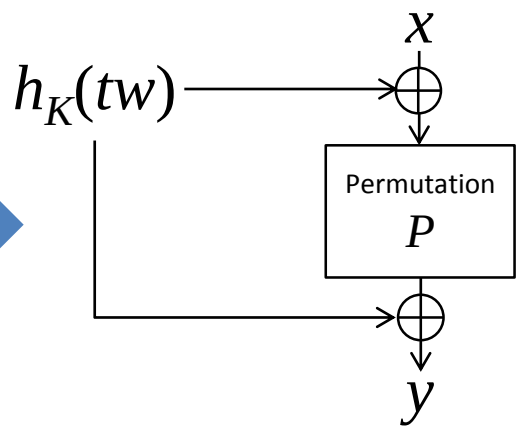
(Uniform and almost XOR universal hash function)

Eliminating Blockcipher's Key (Kurosawa2002)

LRW



TEM (Tweakable Even-Mansour)

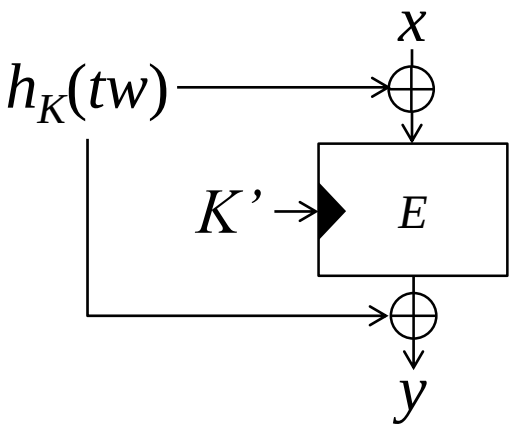


Security

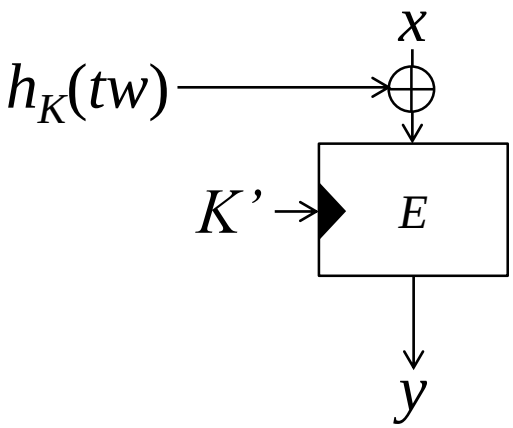
- CCA secure TBC
- Birthday bound
- Assuming P : (public) RP and h_K : AXU hash function

Eliminating Output Masking (Rogaway2004)

LRW



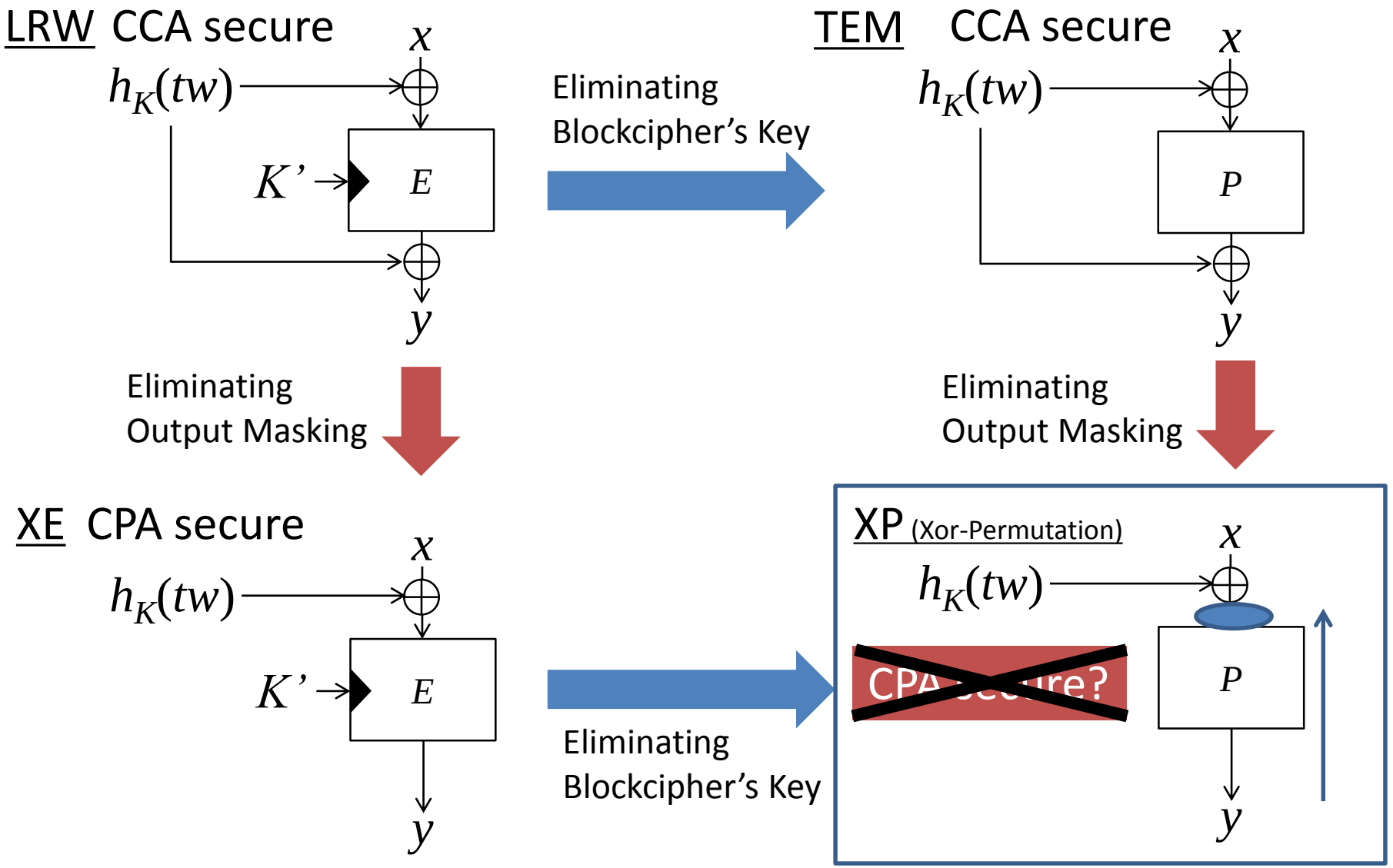
XE



Security

- CPA secure TBC
- Birthday bound
- Assuming $E_{K'}$: RP and h_K : AXU hash function

Target Construction



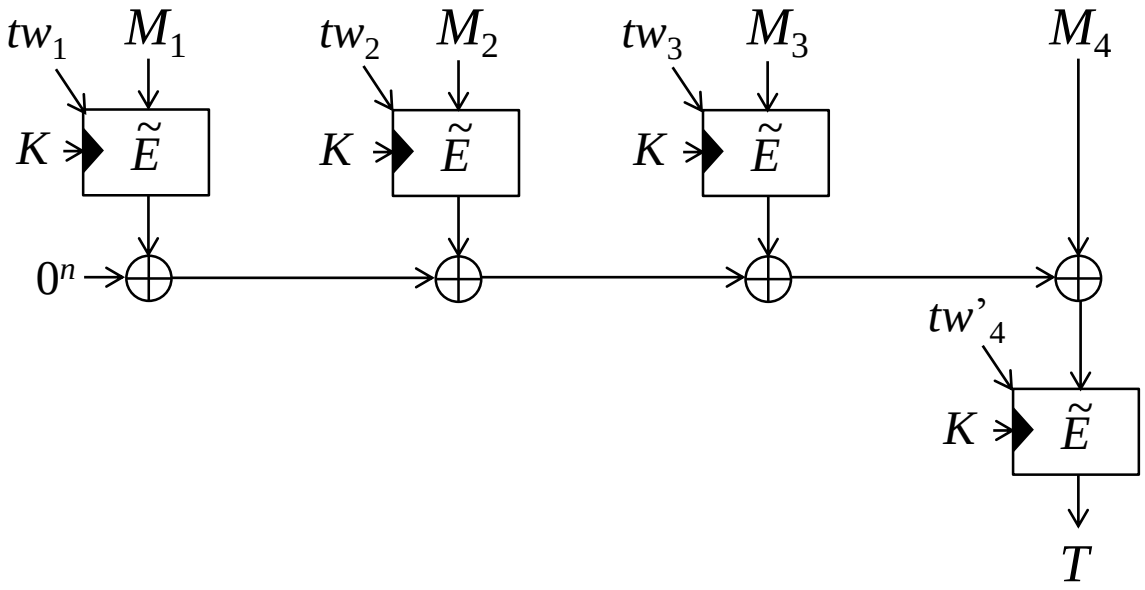
Target Construction

MITSUBISHI ELECTRIC
Changes for the Better

Main Question

- The attack does not imply that incorporating XP with a TBC-based scheme, the resultant scheme is insecure
- Main Question:
  Can we securely incorporate XP with a TBC-based scheme?
- We consider PMAC
  - One of main applications of TBC
  - Parallelizable Message Authentication Code

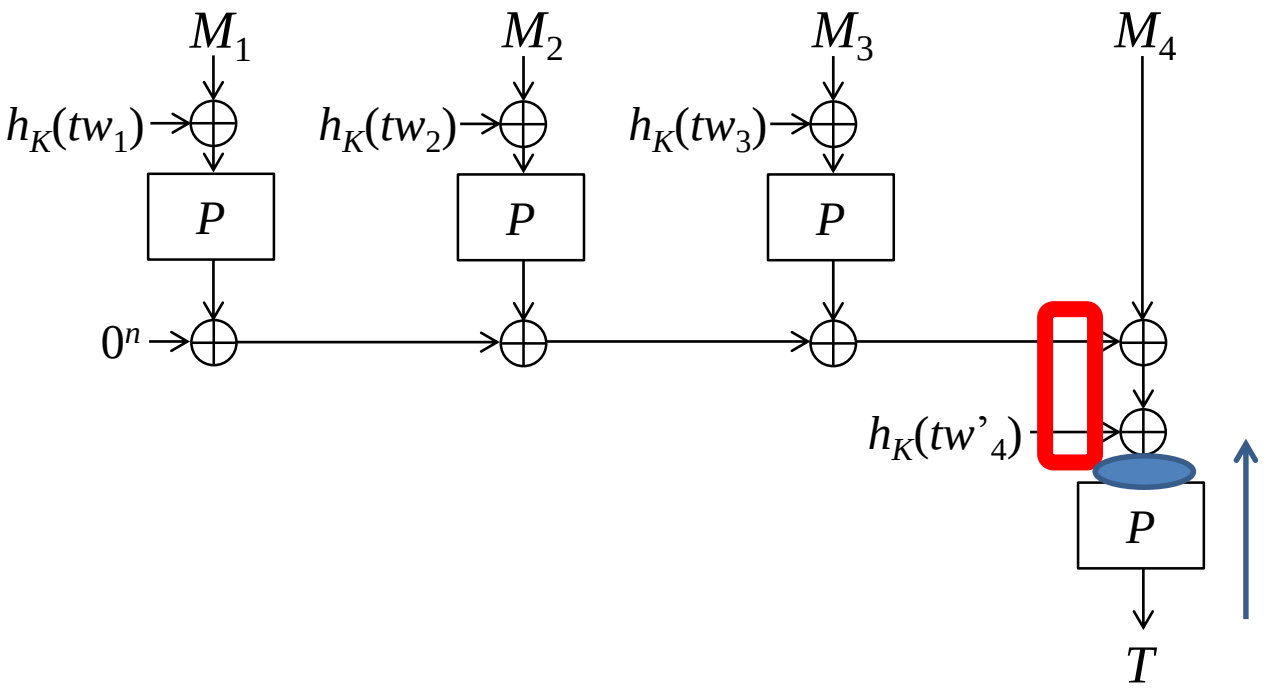
PMAC using TBC $\tilde{E}$



- Secure PRF (PseudoRandom Function)
- Birthday bound
- Assuming $\tilde{E}_K$: CPA secure TBC

LRW, XE, TEM

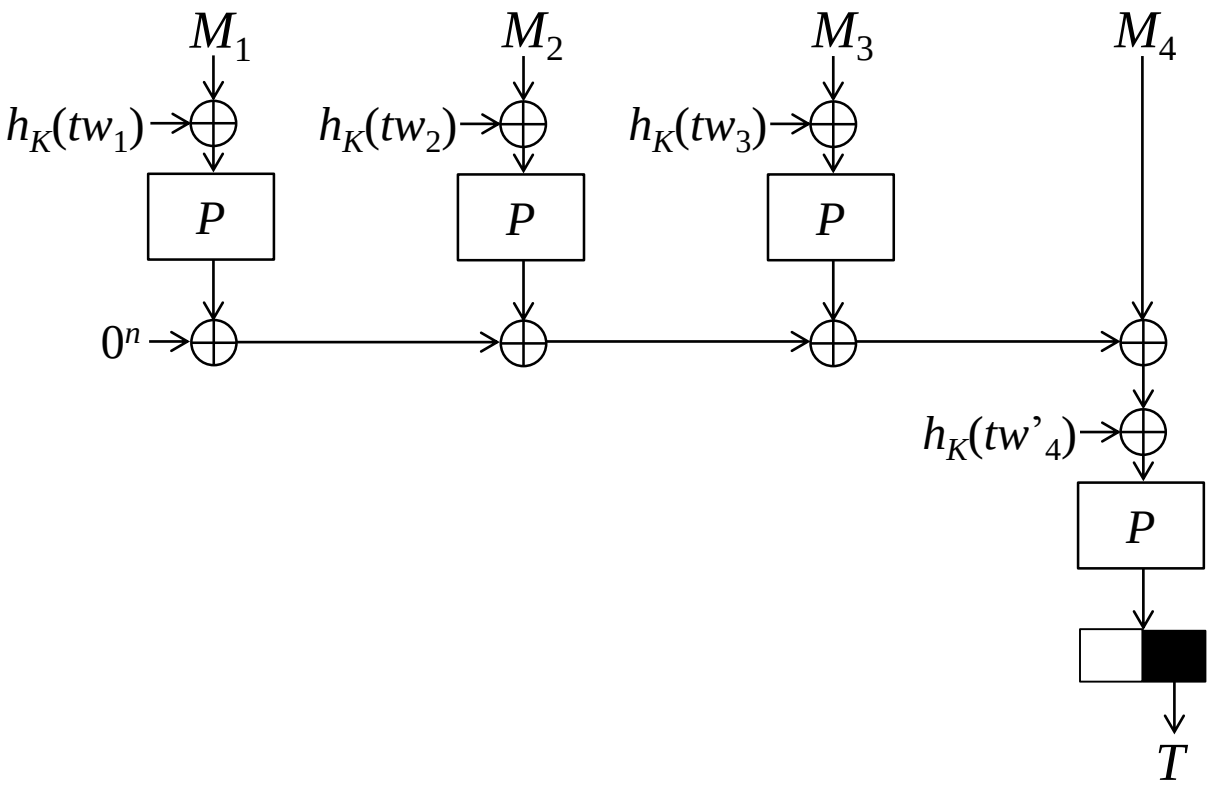
PMAC-XP



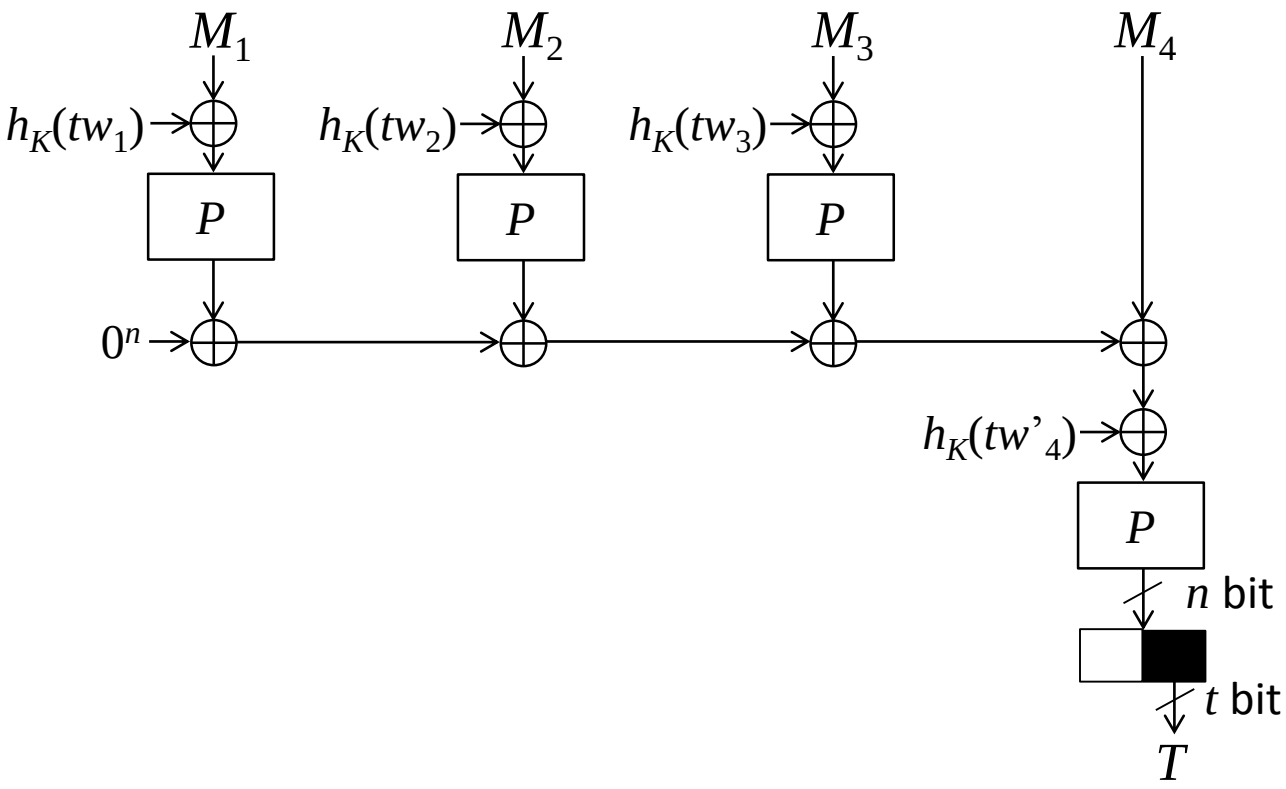
A new pair of message/tag can be generated without a query to PMAC-XP

MITSUBISHI ELECTRIC
Changes for the Better

PMAC-XP with Output Truncation

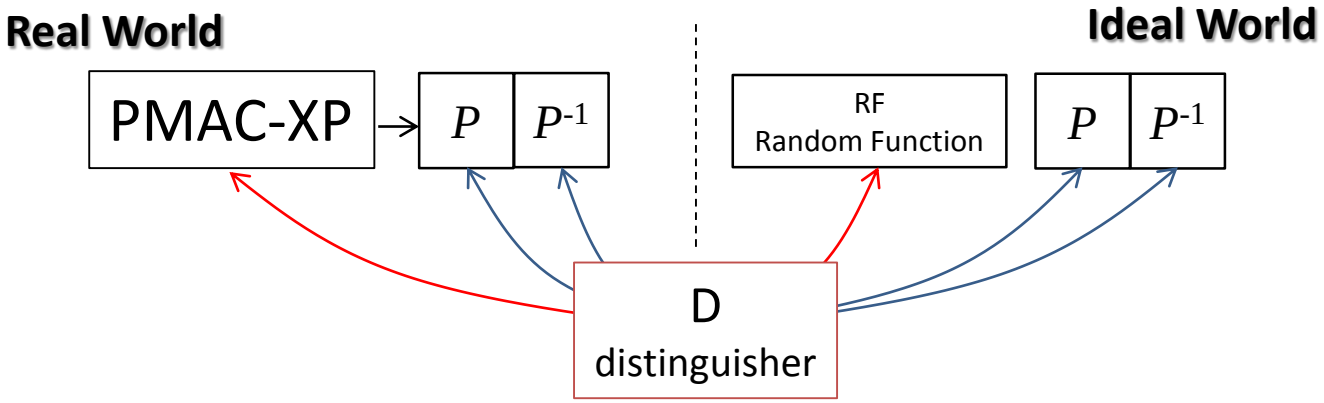


PMAC-XP with Output Truncation



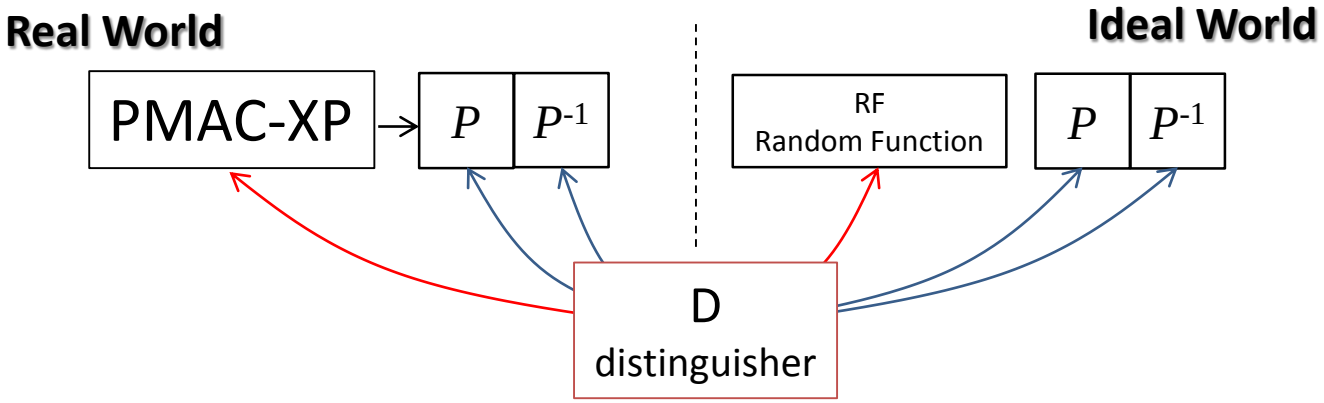
- Permutation size: n bit
- Tag size: t bit

PRF-Security in the Random Permutation Model



- Online queries : D → PMAC-XP/RF
- Offline queries : D → P/P^{-1}

Security Result

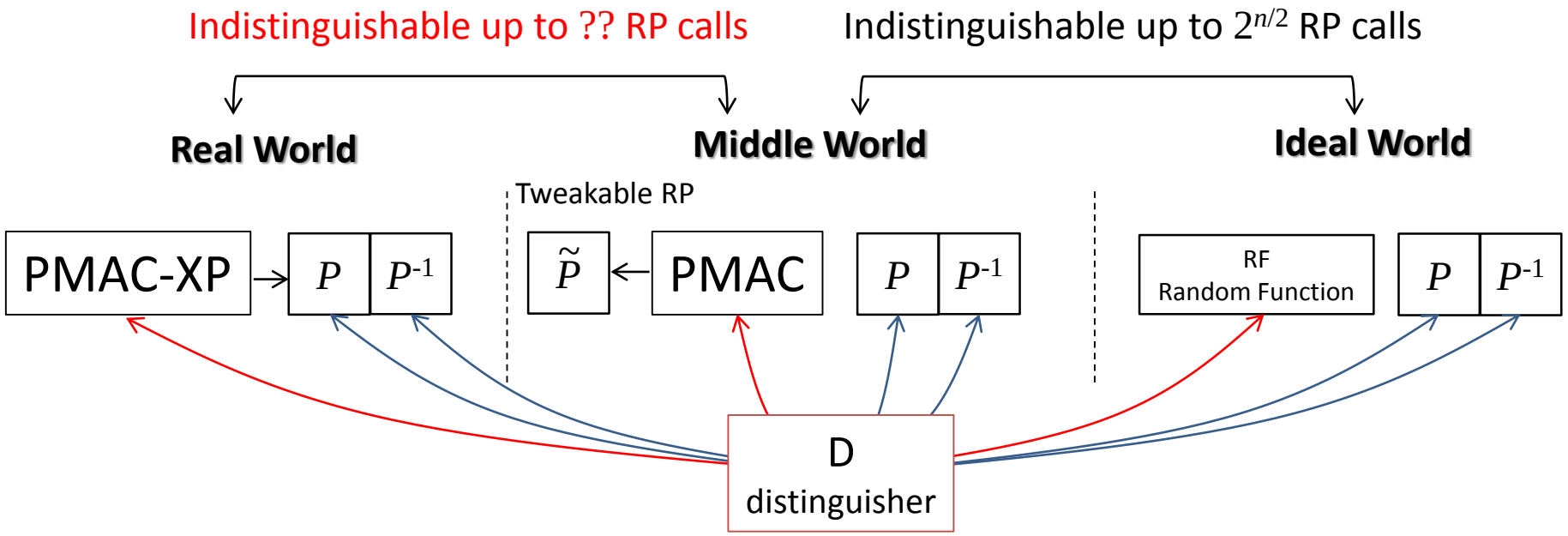


Theorem
PMAC-XP is a secure PRF up to $\min\{2^{n-t}/t, 2^{n/2}\}$ RP calls

Corollary
Defining $t \leqq n/2 - \log_2(n/2)$,
PMAC-XP is a secure PRF up to $2^{n/2}$ RP calls

Birthday bound

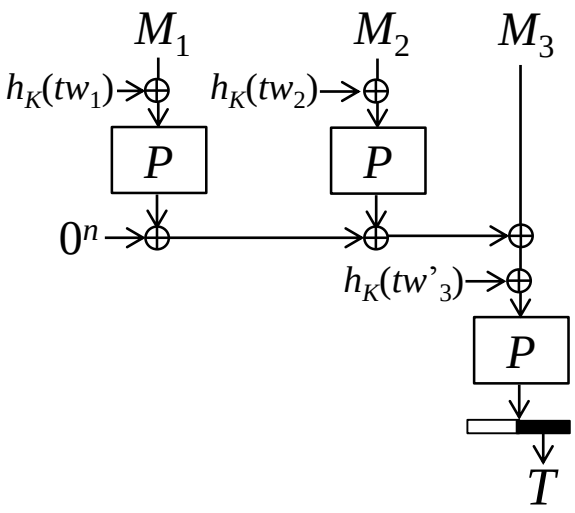
Short Proof


Indistinguishable up to ?? RP calls
Indistinguishable up to $2^{n/2}$ RP calls
Real World
Middle World
Ideal World
Tweakable RP
PMAC-XP
P
P^{-1}
$\tilde{P}$
PMAC
P
P^{-1}
RF
Random Function
P
P^{-1}
D
distinguisher

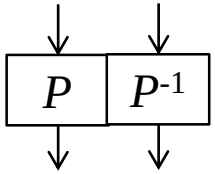
Oracles in Real and Middle Worlds

Real World

PMAC-XP

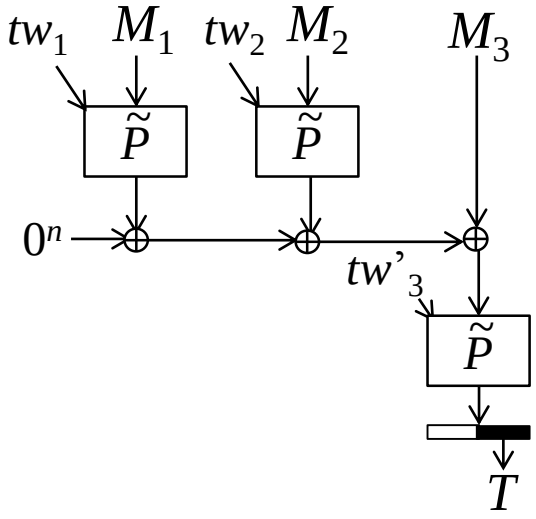


RP

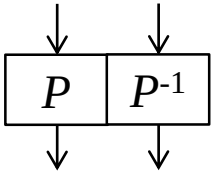


Middle World

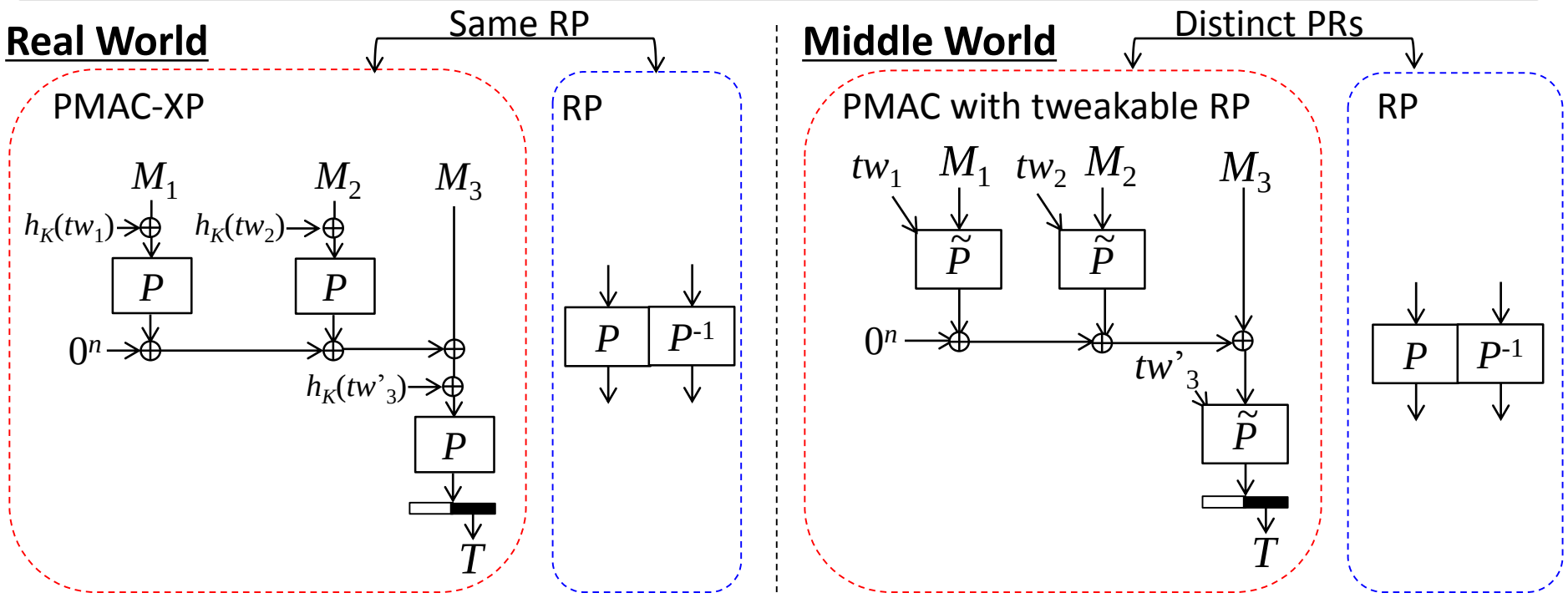
PMAC with tweakable RP



RP



Differences between Real and Middle Worlds



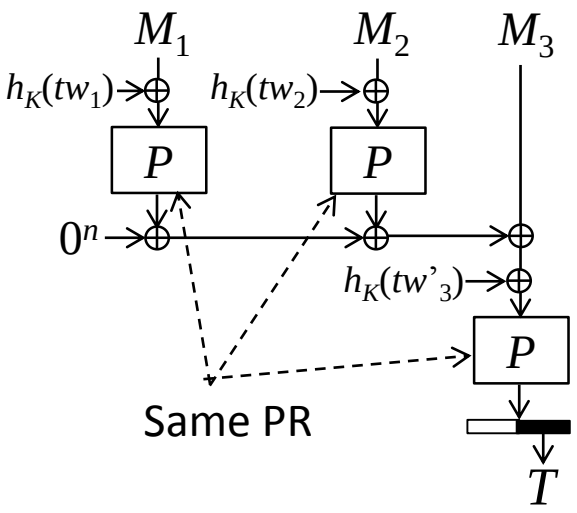
- Difference between real and middle worlds

	1. RPs by online and offline	2. RPs with distinct tweaks in PMAC
Real world	Same RP	Same RP
Middle world	Distinct RPs	Distinct RPs

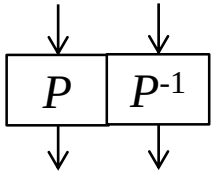
Differences between Real and Middle Worlds

Real World

PMAC-XP

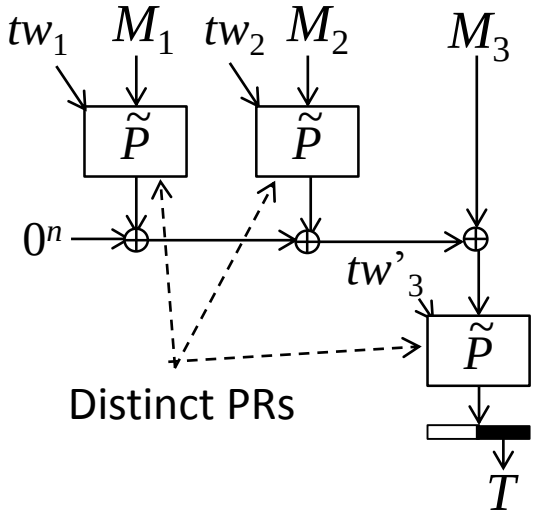


RP

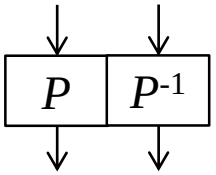


Middle World

PMAC with tweakable RP



RP



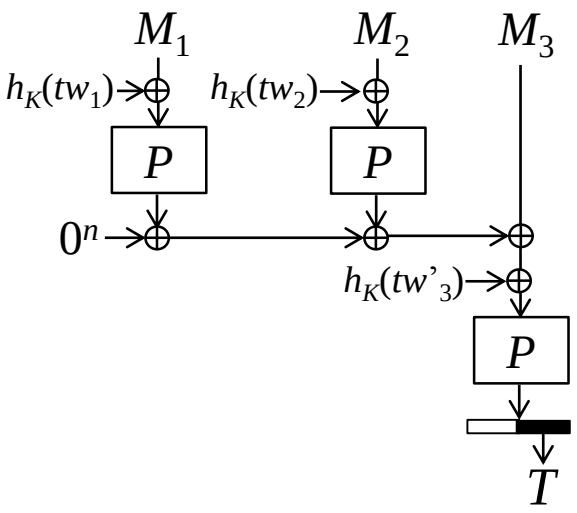
- Difference between real and middle worlds

	1. RPs by online and offline	2. RPs with distinct tweaks in PMAC
Real world	Same RP	Same RP
Middle world	Distinct RPs	Distinct RPs

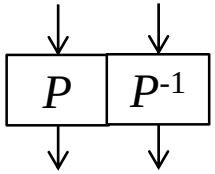
Differences between Real and Middle Worlds

Real World

PMAC-XP

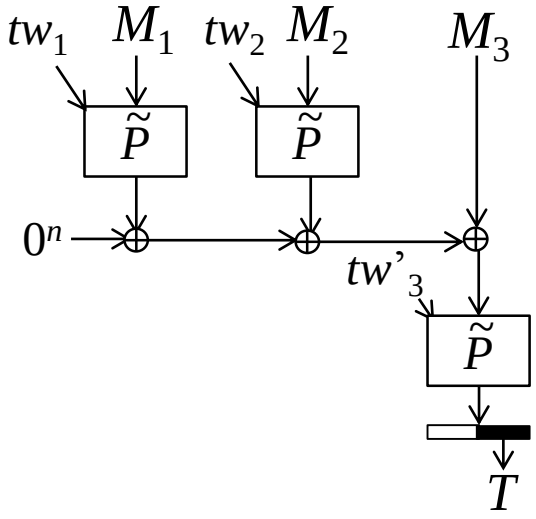


RP

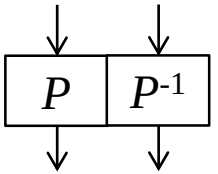


Middle World

PMAC with tweakable RP



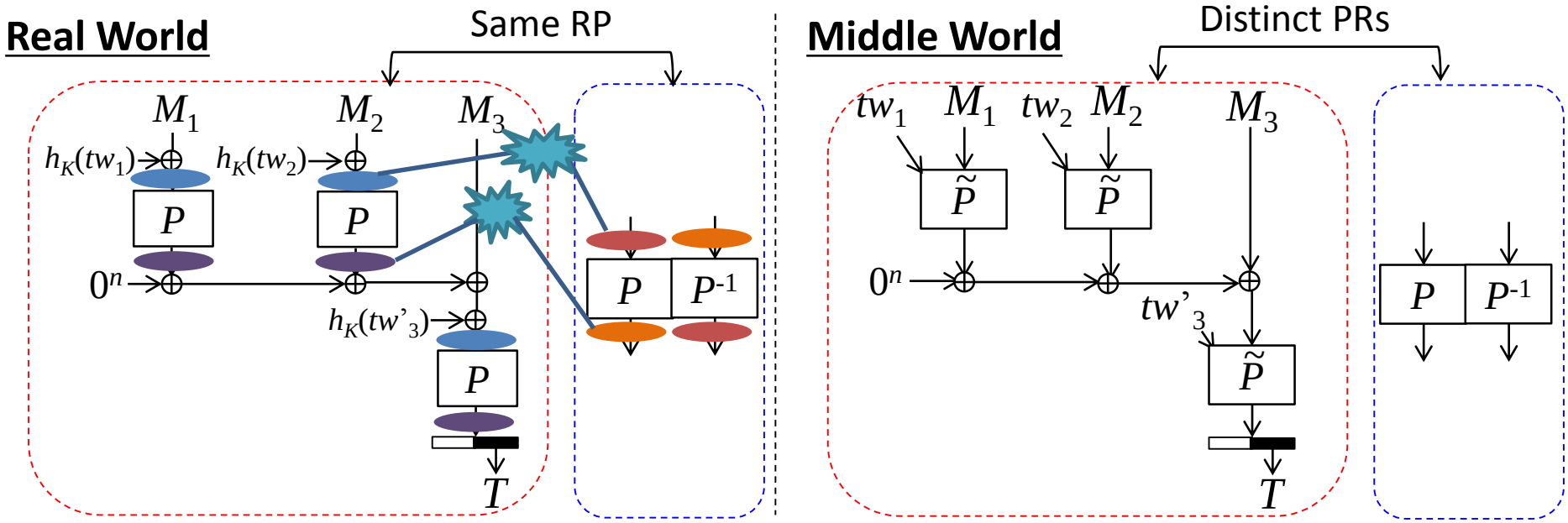
RP



- Difference between real and middle worlds

	1. RPs by online and offline	2. RPs with distinct tweaks in PMAC
Real world	Same RP	Same RP
Middle world	Distinct RPs	Distinct RPs

First Difference

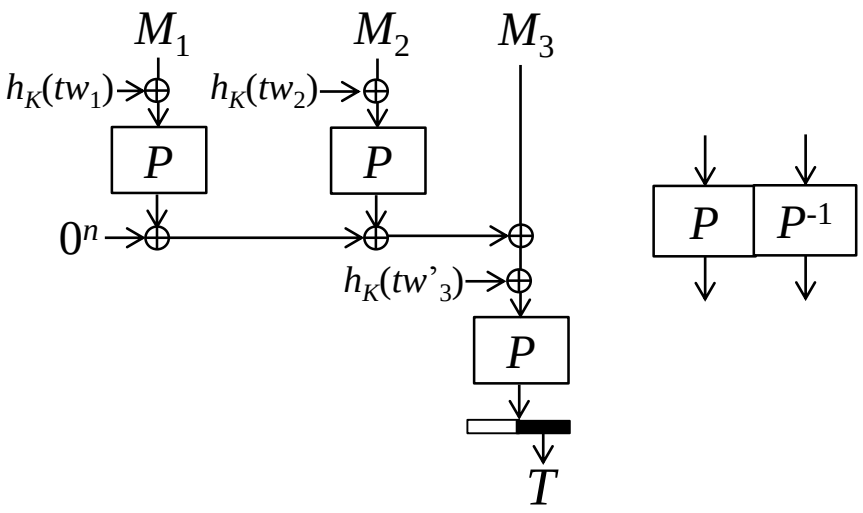


- Distinguishing attacks can be avoided if no collision occurs in the real world
  - Input collision does not occur up to $2^{n/2}$ RP calls
    - ✓ by the property of AXU hash function
  - Output collision does not occur up to $\min\{2^{n-t}/t, 2^{n/2}\}$ RP calls
    - ✓ by a multi-collision analysis and the randomness of outputs of P

Differences between Real and Middle Worlds

Real World

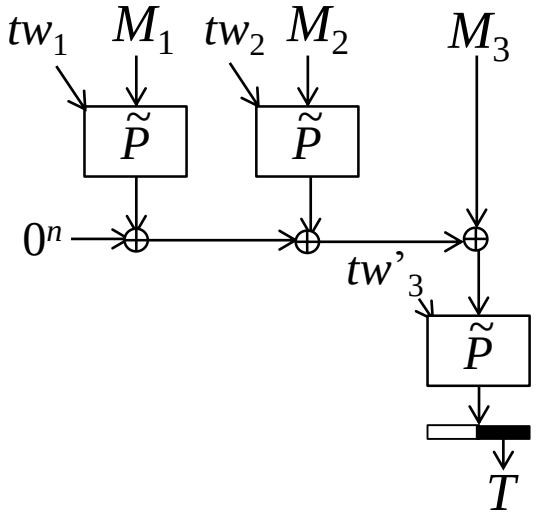
PMAC-XP



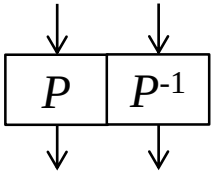
RP

Middle World

PMAC with tweakable RP



RP



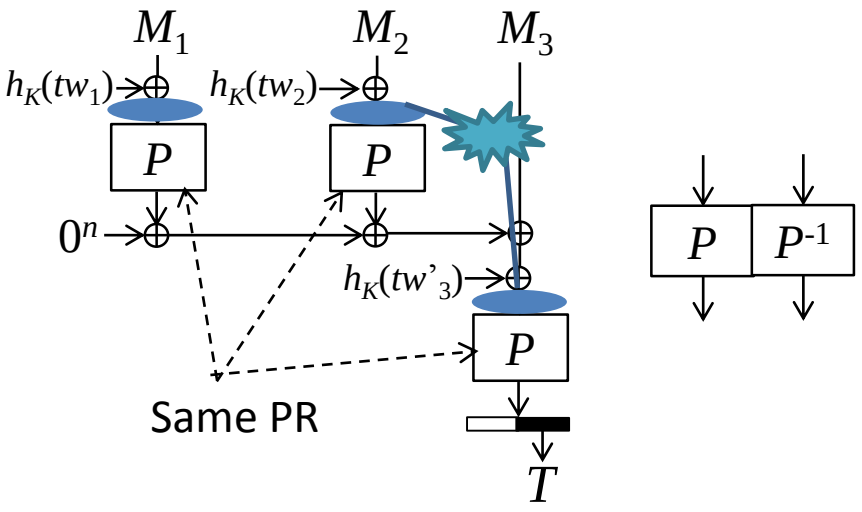
- Difference between real and middle worlds

	1. RPs by online and offline	2. RPs with tweaks in PMAC
Real world	Same RP	Same RP
Middle world	Distinct RPs	Distinct RPs

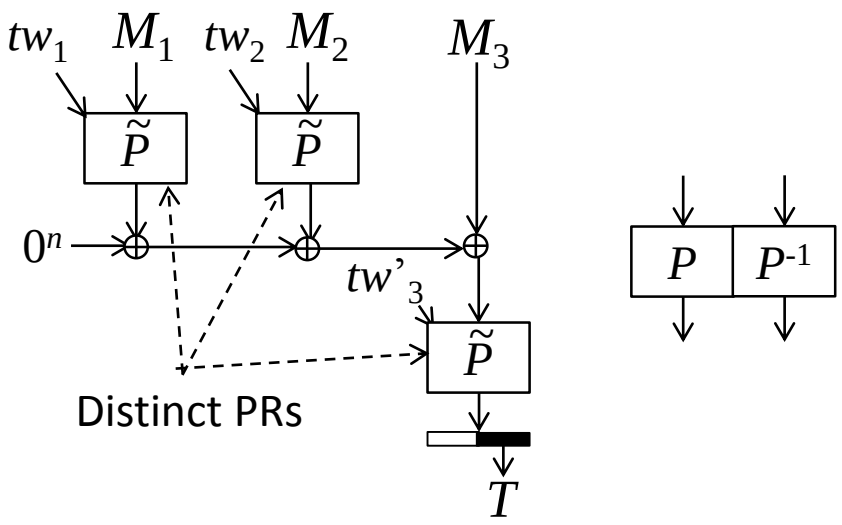
up to $\min\{2^{n-t}/t, 2^{n/2}\}$ RP calls

Second Difference

Real World



Middle World

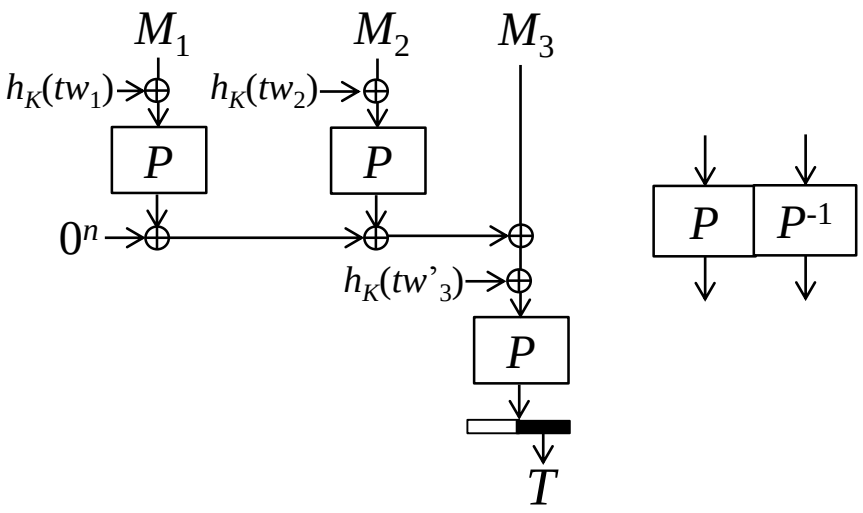


- Distinguishing attacks can be avoided
  if in the real world, no input collision with distinct tweaks occurs
- A collision does not occur up to $2^{n/2}$ RP calls
  - ✓ by the property of AXU hash function

Differences between Real and Middle Worlds

Real World

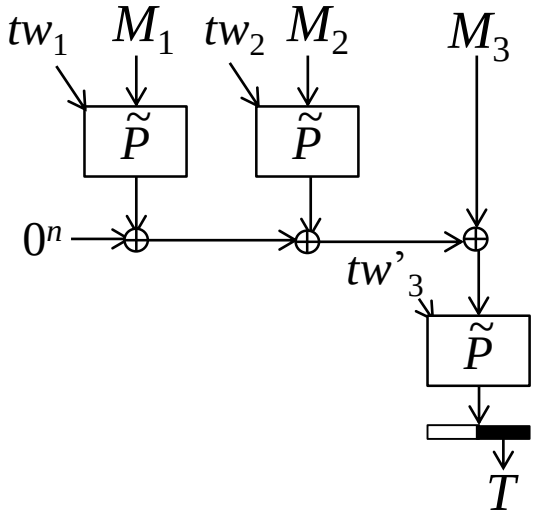
PMAC-XP



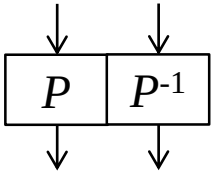
RP

Middle World

PMAC with tweakable RP



RP



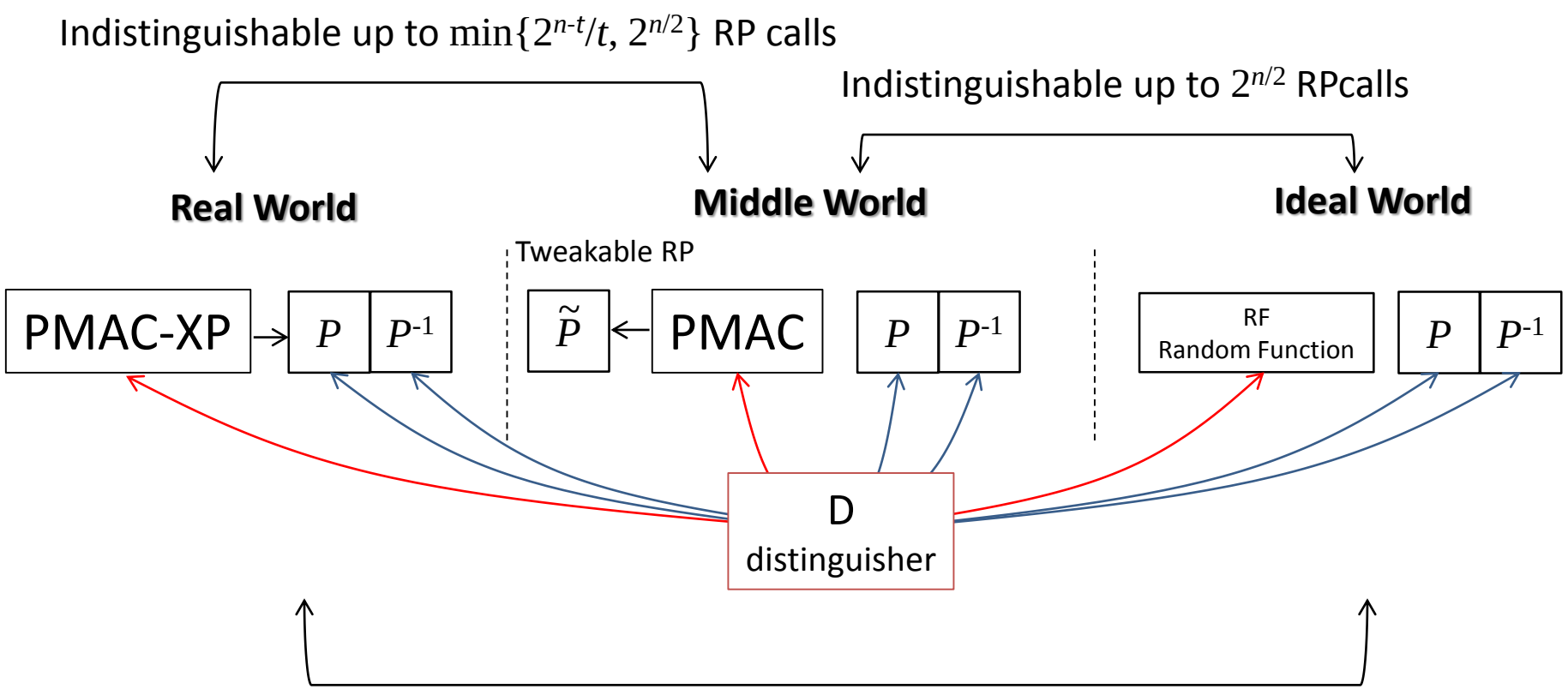
- Difference between real and middle worlds

	1. RPs by online and offline	2. RPs with tweaks in PMAC
Real world	Same RP	Same RP
Middle world	Distinct RPs	Distinct RPs

up to $\min\{2^{n-t}/t, 2^{n/2}\}$ RP calls

up to $2^{n/2}$ RP calls

PRF-Bound



PMAC-XP is a secure PRF up to $\min\{2^{n-t}/t, 2^{n/2}\}$ PP calls

Defining $t \leqq n/2 - \log_2(n/2)$,
PMAC-XP is a secure PRF up to $2^{n/2}$ PR calls

Birthday bound

MITSUBISHI ELECTRIC
Changes for the Better

Conclusion

- Simplification of TBC design
- XP: the simplified construction of LRW, XE and TEM
- PMAC-XP
  - Secure PRF up to the birthday bound
- Future Research
  - Security of PMAC-XP against related key attacks

Thank you for your attention!