Computational and Symbolic Proofs of Security
(Spring School & Workshop: 4/6-9:2009 Atagawa)

Cryptographic Applications of Indifferentiability via Leaking Random Oracle Models

Kazuo Ohta
University of Electro-Communications
(Joint work with Naito, Yoneyama, Wang Lei)

Overview

- Indifferentiability is useful for Random Oracle methodology and the design and security analysis of hash functions.
- Coron proved that Merkle-Damgård (MD) hashing is not indifferentiable from $\mathcal{RO}$.

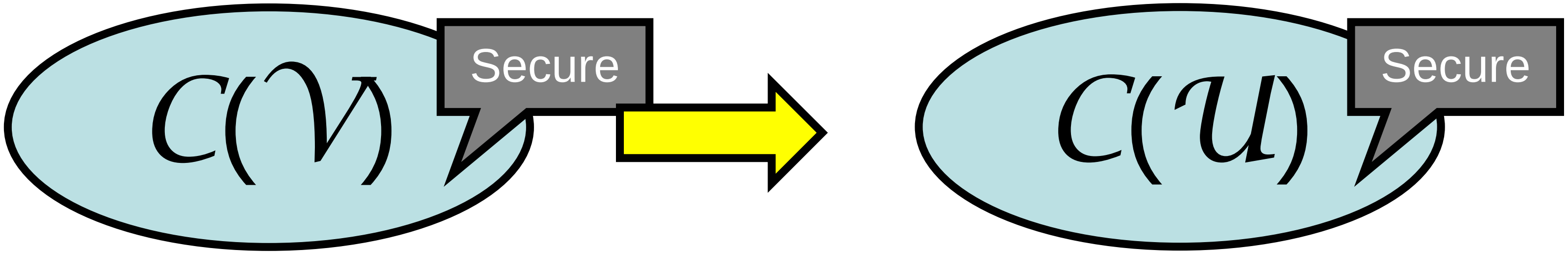
> There exists a protocol secure in the $\mathcal{RO}$ model but insecure if $\mathcal{RO}$ is instantiated by MD hash

- How to rescue MD hashing
  - Approach 1 : using modified MD hashings
  - Approach 2 : using leaking $\mathcal{RO}$ models

Indifferentiability framework

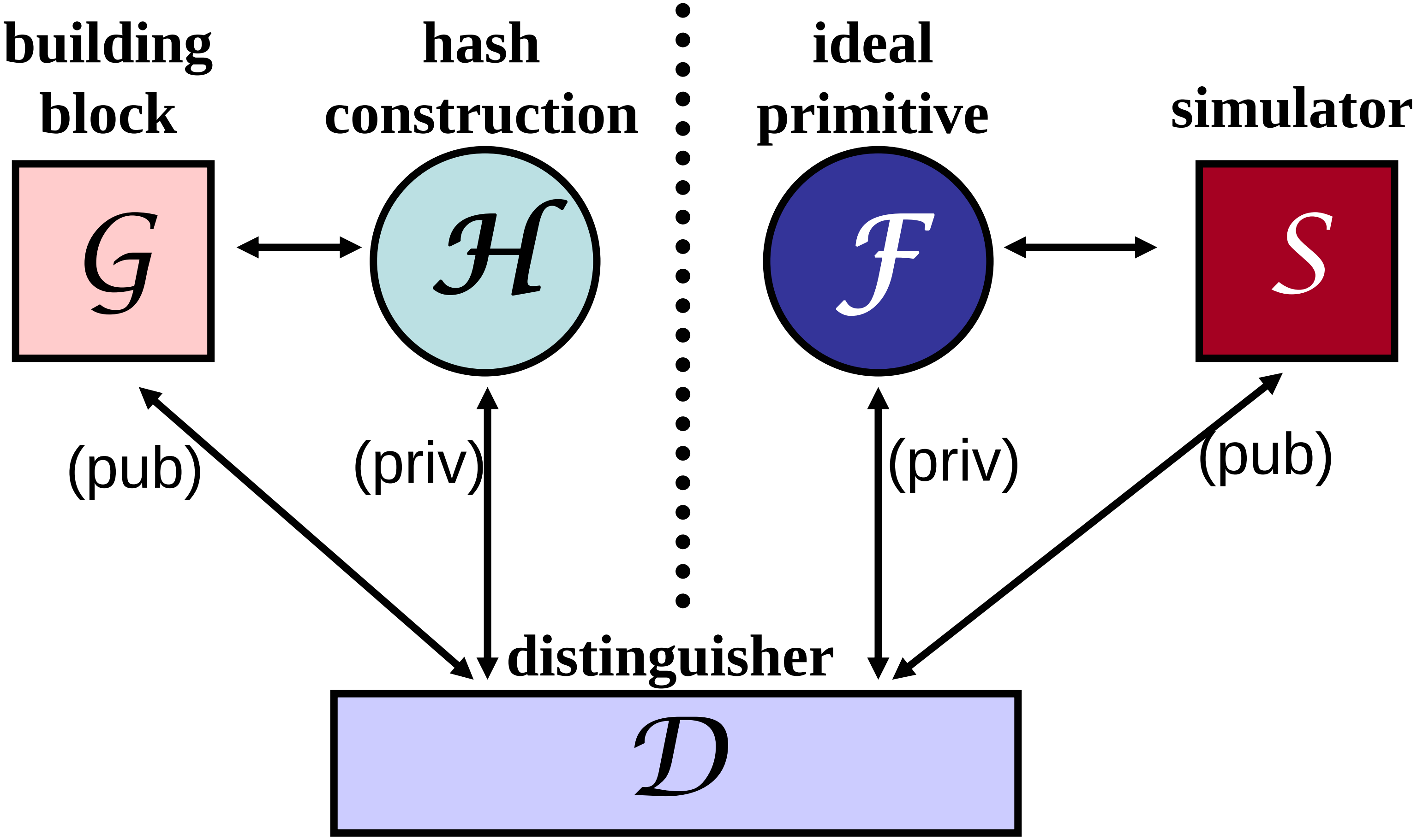
- General : by Maurer (TCC’04),
  for hash : by Coron (CRYPTO’05)

- If primitive $\mathcal{U}$ is indifferentiable from $\mathcal{V}$ ($\mathcal{U} \sqsubset \mathcal{V}$) and cryptosystem $\mathcal{C}(\mathcal{V})$ is secure, then $\mathcal{C}(\mathcal{U})$ is also secure.



$$\mathcal{C}(\mathcal{U}) > \mathcal{C}(\mathcal{V})$$

Def. of indifferentiability for hash



$| \Pr[\mathcal{D}(\mathcal{H},\mathcal{G}) = 1] - \Pr[\mathcal{D}(\mathcal{F},\mathcal{S}) = 1] | <$ negl. iff $\mathcal{H} \sqsubset \mathcal{F}$

Application to hash construction

- Iterated hash function $\boldsymbol{H^g}$
  - Compression function $\boldsymbol{g}$ & domain extension $\boldsymbol{H}$
  - MD hashing is the most popular one.

- Iff $\boldsymbol{H^g} \sqsubset \mathcal{R}O$,

for $\forall$ cryptosystem C, the security of $C(\boldsymbol{H^g})$ is obtained from the security of $C(\mathcal{R}O)$.

$$\boldsymbol{H^g} \sqsubset \mathcal{R}O \Longleftrightarrow \begin{array}{c} C(\boldsymbol{H^g}) > C(\mathcal{R}O) \\ \text{for } \forall C \end{array}$$

Impossibility of Instantiation

Random Oracle methodology does not hold.

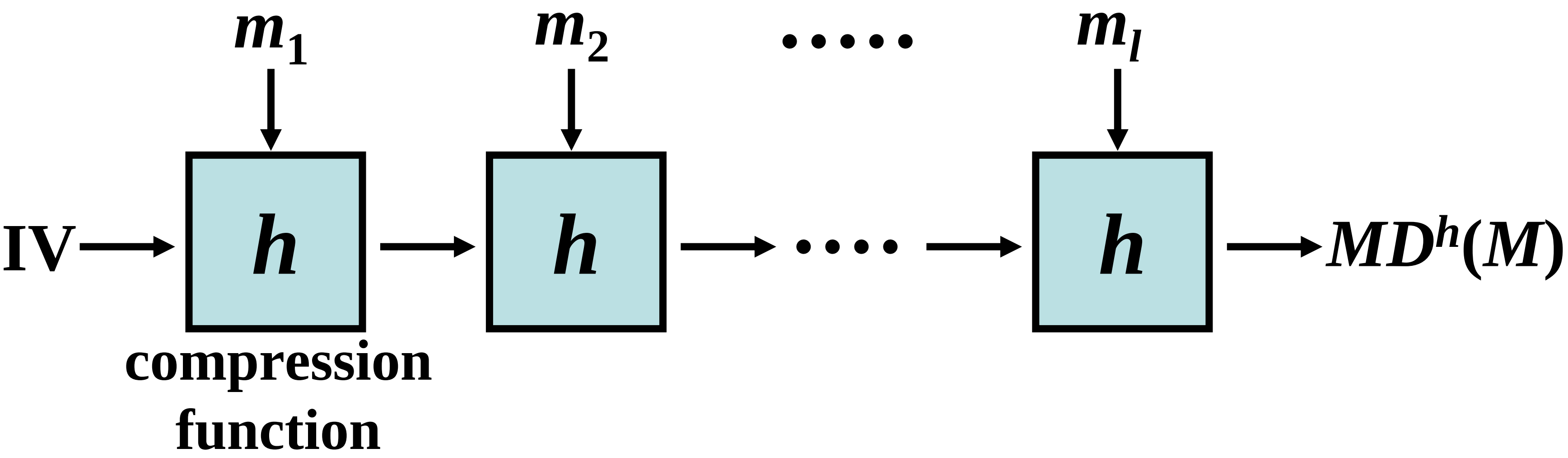
For any g (program) $\boldsymbol{H}^g \not\sqsubset \mathcal{RO}$

$$\boldsymbol{H}^g \not\sqsubset \mathcal{RO} \Longleftrightarrow \exists C \; s.t. \; C(\boldsymbol{H}^g) \ntriangleright C(\mathcal{RO})$$

[MRH04] Maurer, Renner, Holenstein, “Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology”, TCC 2004

(Original) Merkle-Damgård hashing MD^h

$M = (m_1, \ldots, m_l)$



- adopted by MD5, SHA-1, SHA-256…

Coron’s work (CRYPTO’05)

- Negative result
  - $\boldsymbol{MD}^{\mathbf{FIL}\mathcal{RO}} \not\sqsubset \mathcal{RO}$
  - Due to extension attack

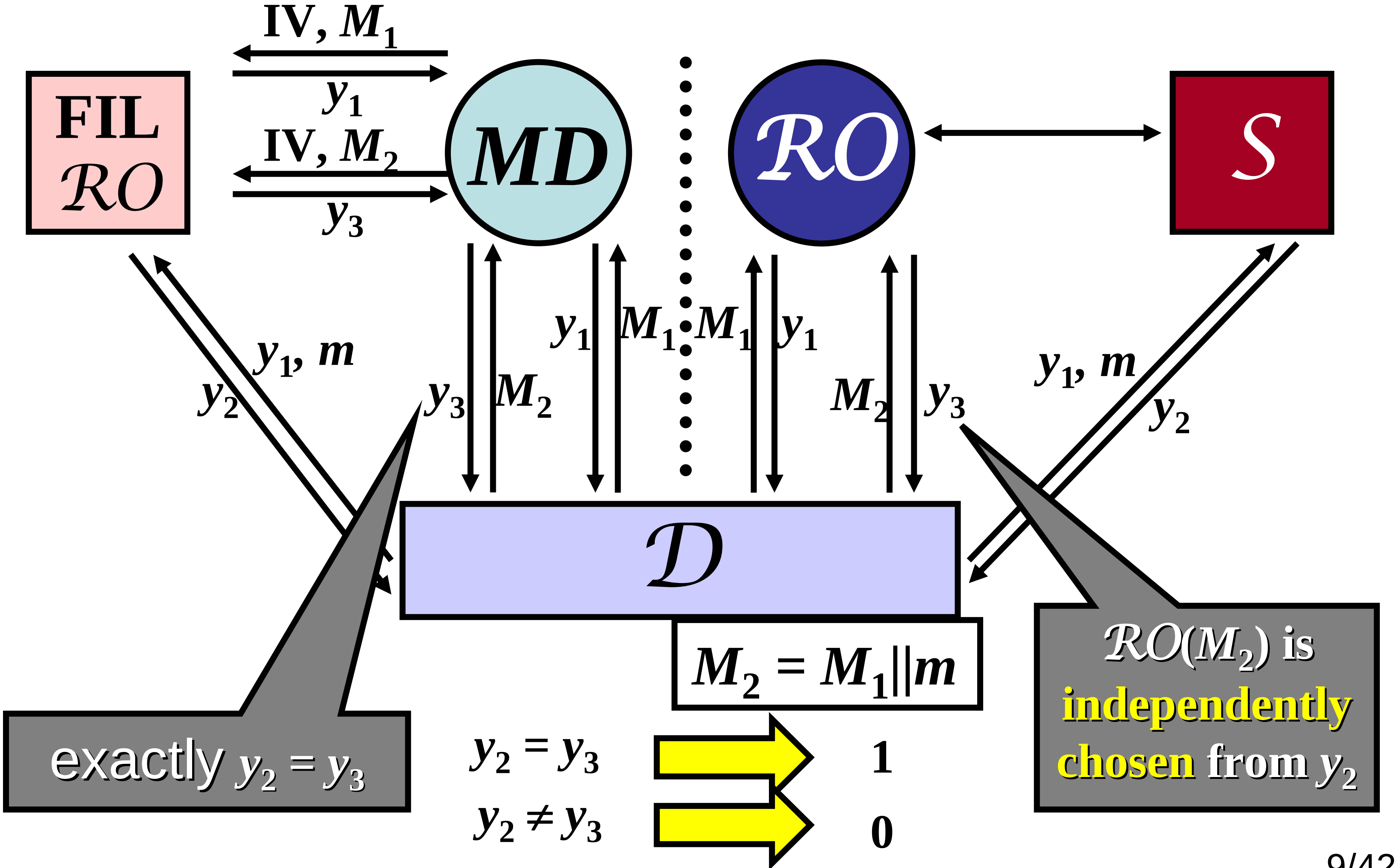
$\mathbf{FIL}\mathcal{RO}$: fixed input-length $\mathcal{RO}$

- Positive result
  - $\widetilde{\boldsymbol{MD}}^{\mathbf{FIL}\mathcal{RO}} \sqsubset \mathcal{RO}$
  - Prefix MD, Chopped MD…

$\widetilde{\boldsymbol{MD}}$: modified MD hashing

rescue using modified MD hashings

Extension attack



$M_2 = M_1 || m$

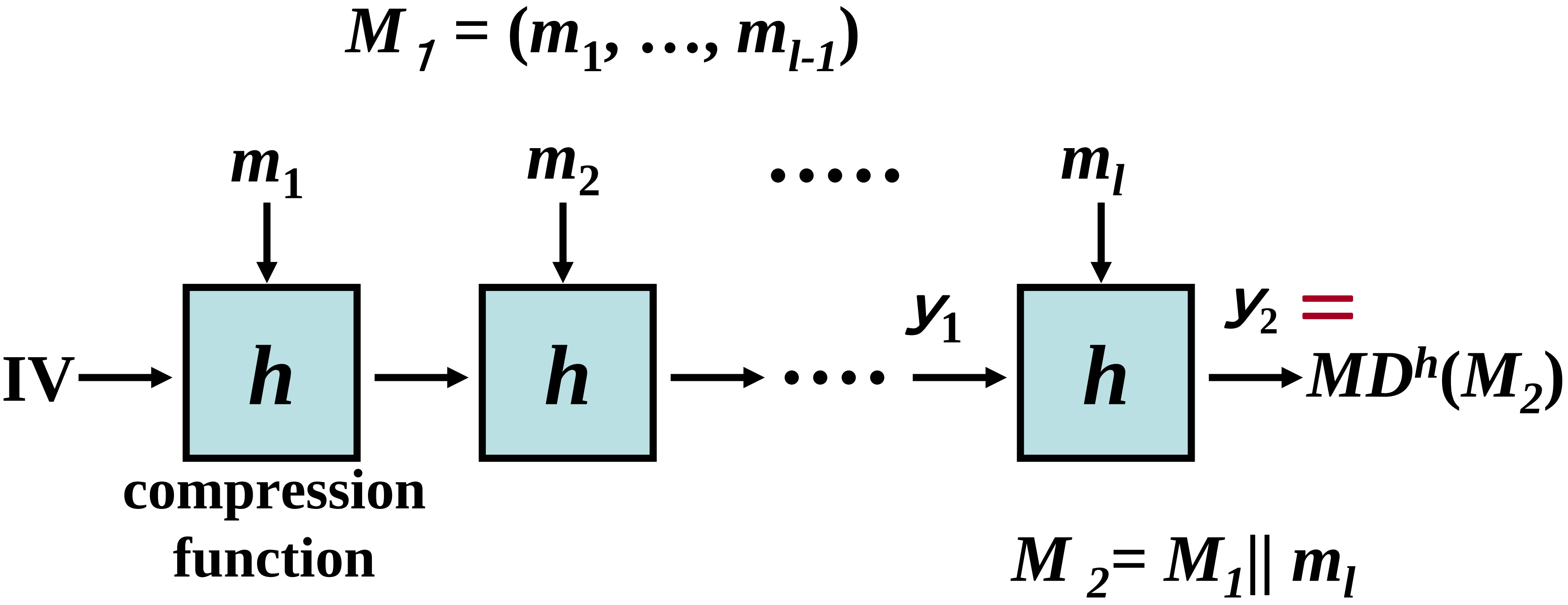
exactly $y_2 = y_3$

$\mathcal{RO}(M_2)$ is **independently chosen** from y_2

$y_2 = y_3$ ⇒ 1

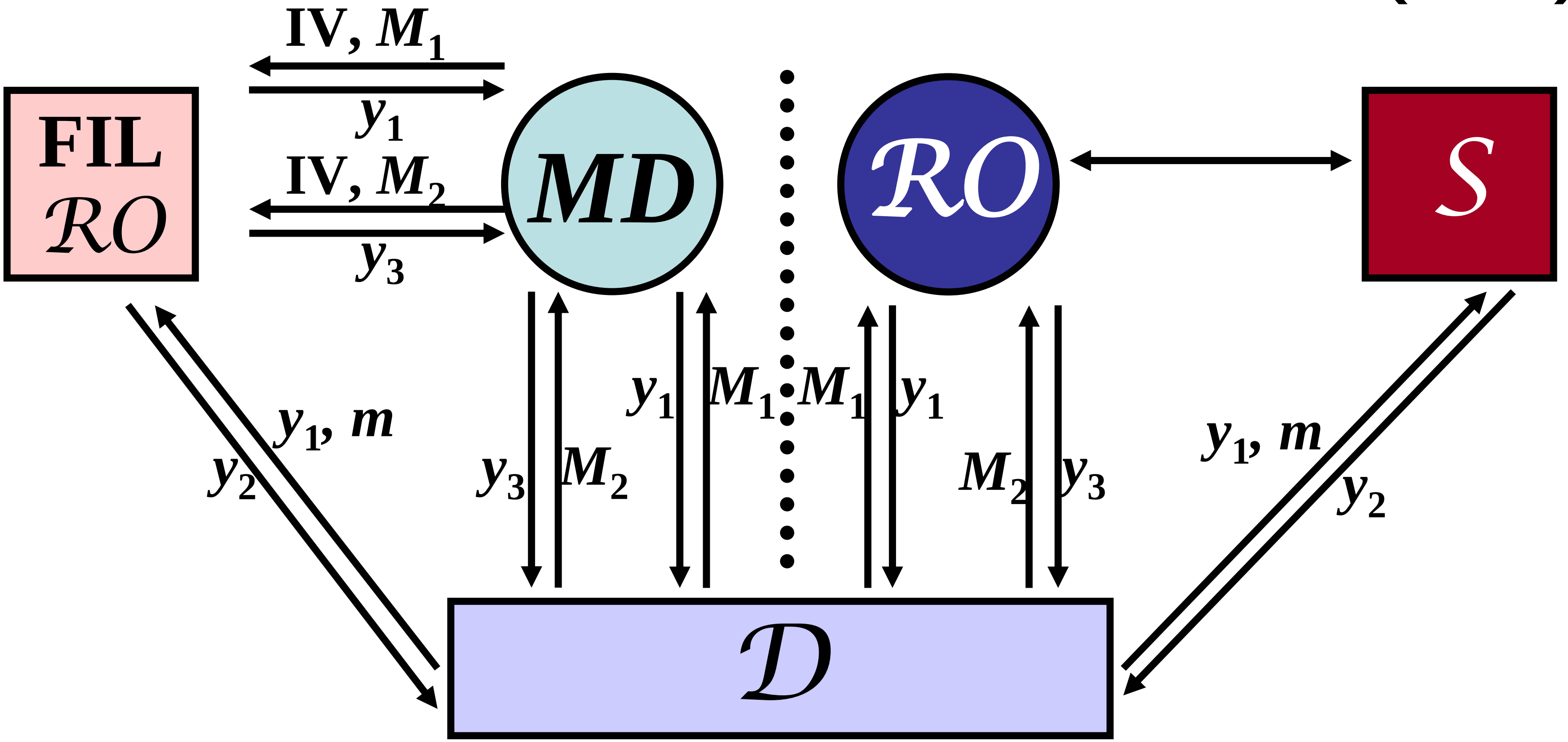
$y_2 \neq y_3$ ⇒ 0

Rationale of the Correctness by D



- RO(M_2) is independently chosen from y_2.

How to resist extension attack(1/2)

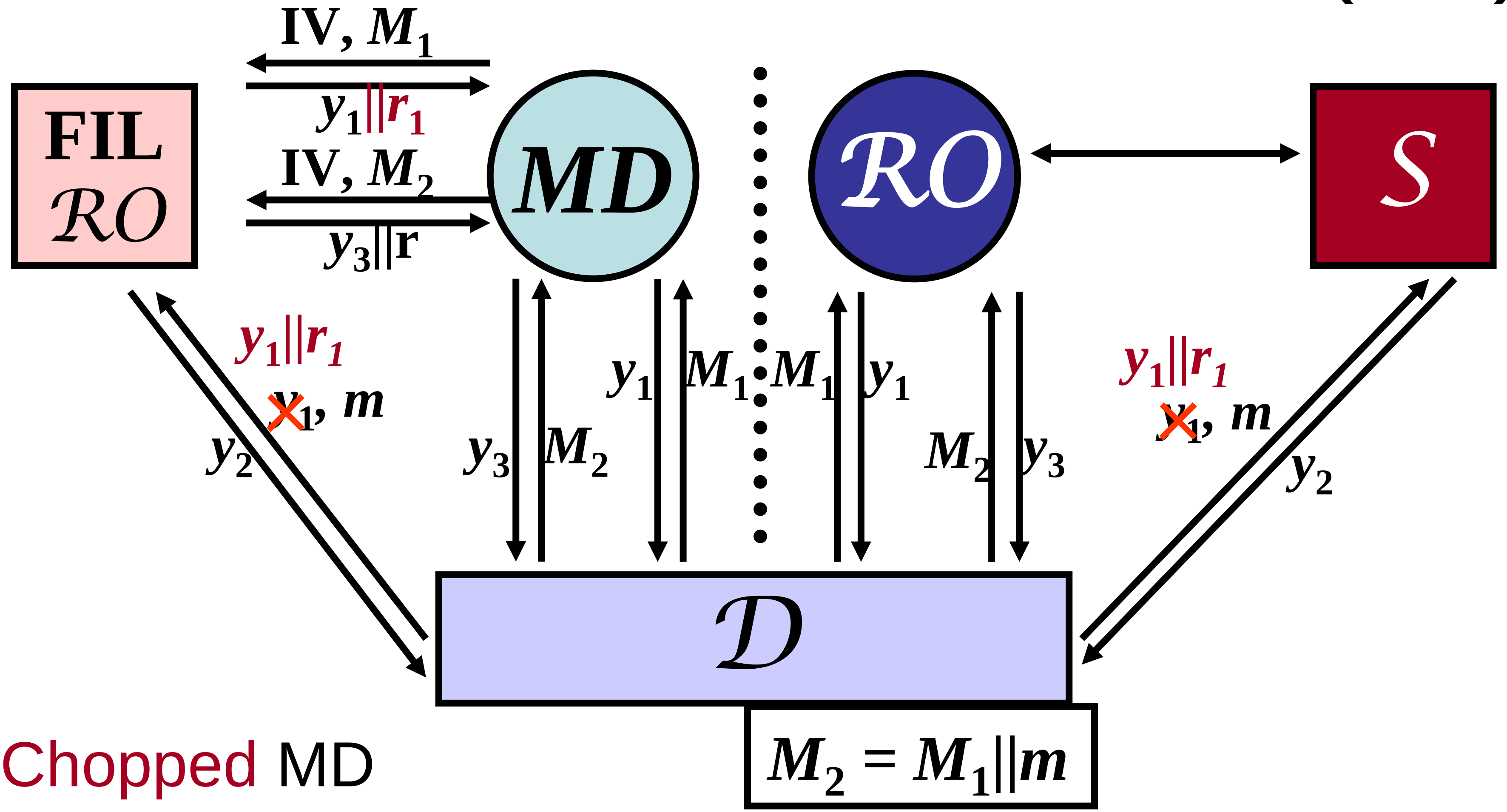


$\boxed{\xcancel{M_2 = M_1 || m}}$

- Prefix-free MD:

Prefix-free padding makes sure that no M_1 and M_2 can satisfy Pad(M_2)=Pad(M_1)||m.

How to resist extension attack(2/2)



- Chopped MD

y_1 is obtained by chopping r_1 of **FIL**RO(IV||M_1). D has to guess the value r_1.

Our Concern

$$\boldsymbol{H}^g \sqsubset \mathcal{RO} \Longleftrightarrow \begin{array}{c} C(\boldsymbol{H}^g) > C(\mathcal{RO}) \\ \text{for } \forall C \end{array}$$

$$\boldsymbol{MD}^g \not\sqsubset \mathcal{RO} \Longleftrightarrow \begin{array}{l} \exists C \; s.t. \\ C(\boldsymbol{MD}^g) \not> C(\mathcal{RO}) \end{array}$$

Is (original) MD construction dead ?

Answer: It is still alive !!

Our approaches

- Approach using modified MD hashings (approach 1) cannot rescue original MD.

- We will show other two approaches
  - using leaking $\mathcal{RO}$ models (approach 2)
  - using indifferentiability with conditions (approach 3)

Approach 2 (for $\boldsymbol{MD}^{\mathbf{FIL}\mathcal{RO}}$)

See the details

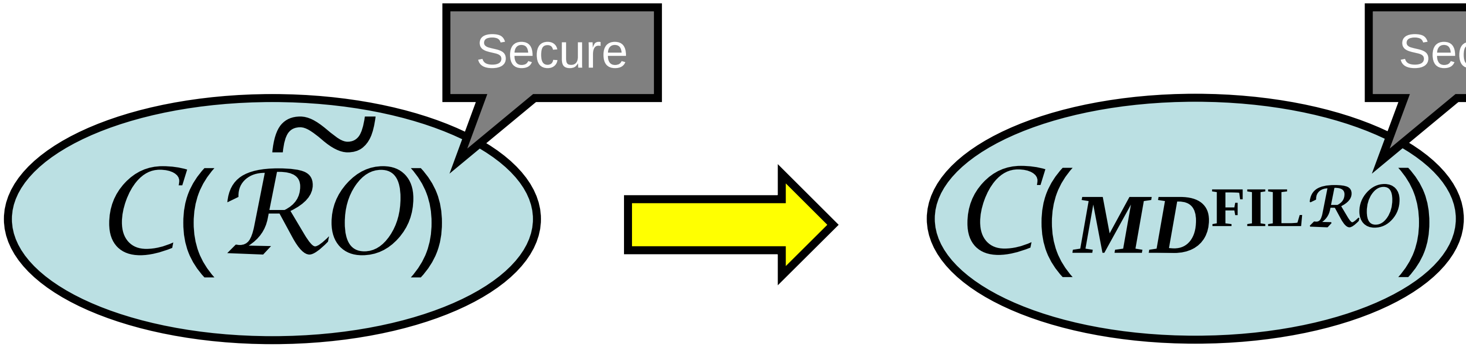
in [NYWO 09a]

Strategy for approach 2

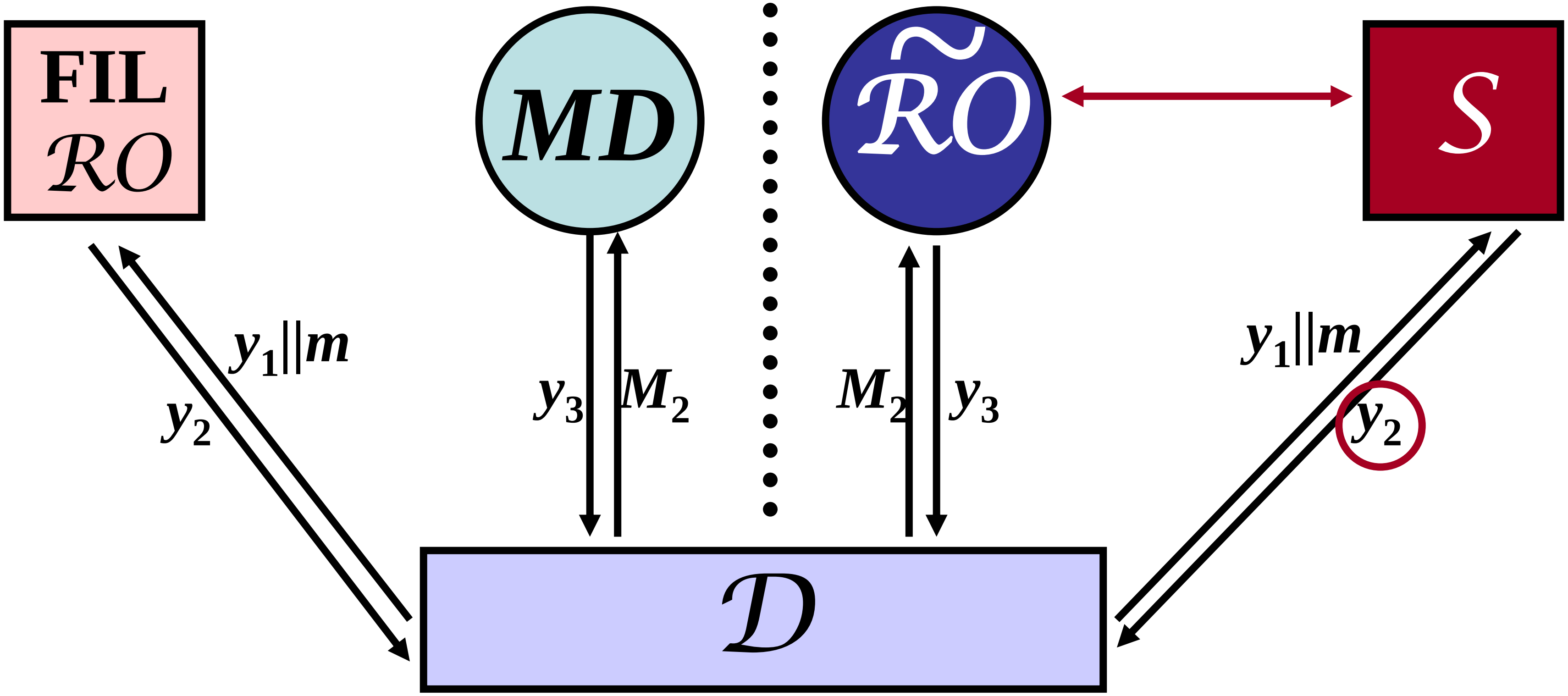
leaking $\mathcal{RO}$ model

1. find an ideal primitive $\widetilde{\mathcal{RO}}$ from which $\boldsymbol{MD}^{\mathrm{FIL}\mathcal{RO}}$ is indifferentiable.

2. prove that cryptosystem C is secure in the $\widetilde{\mathcal{RO}}$ model.


Secure
$C(\widetilde{\mathcal{RO}})$
Secure
$C(\boldsymbol{MD}^{\mathrm{FIL}\mathcal{RO}})$

How to find $\widetilde{\mathcal{RO}}$



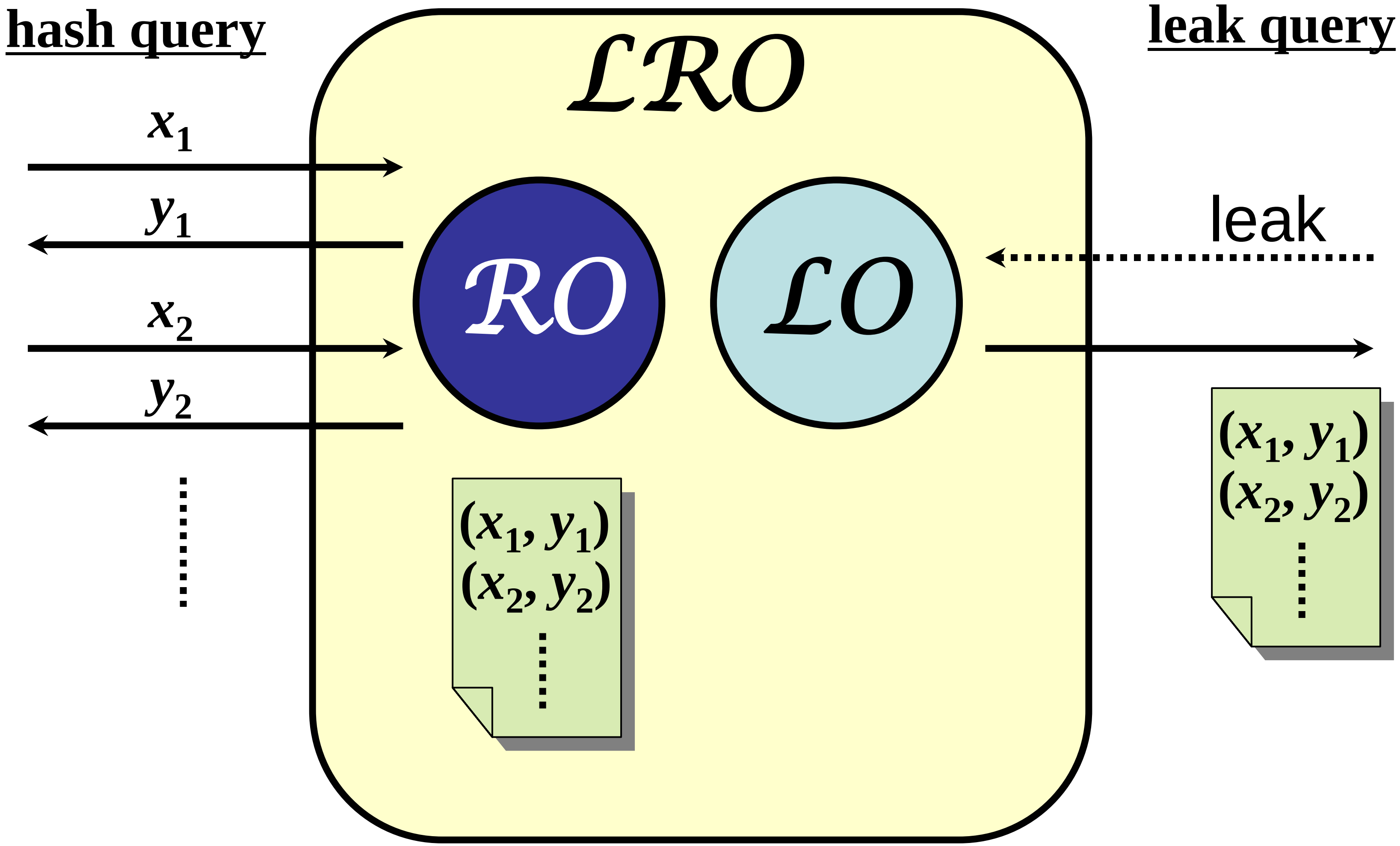
- $\widetilde{\mathcal{RO}}$ has to send information so that simulator can simulate $\boldsymbol{y_2}$ s.t. $\boldsymbol{y_2} = \boldsymbol{y_3}$.

Leaky random oracle model [YMO08]

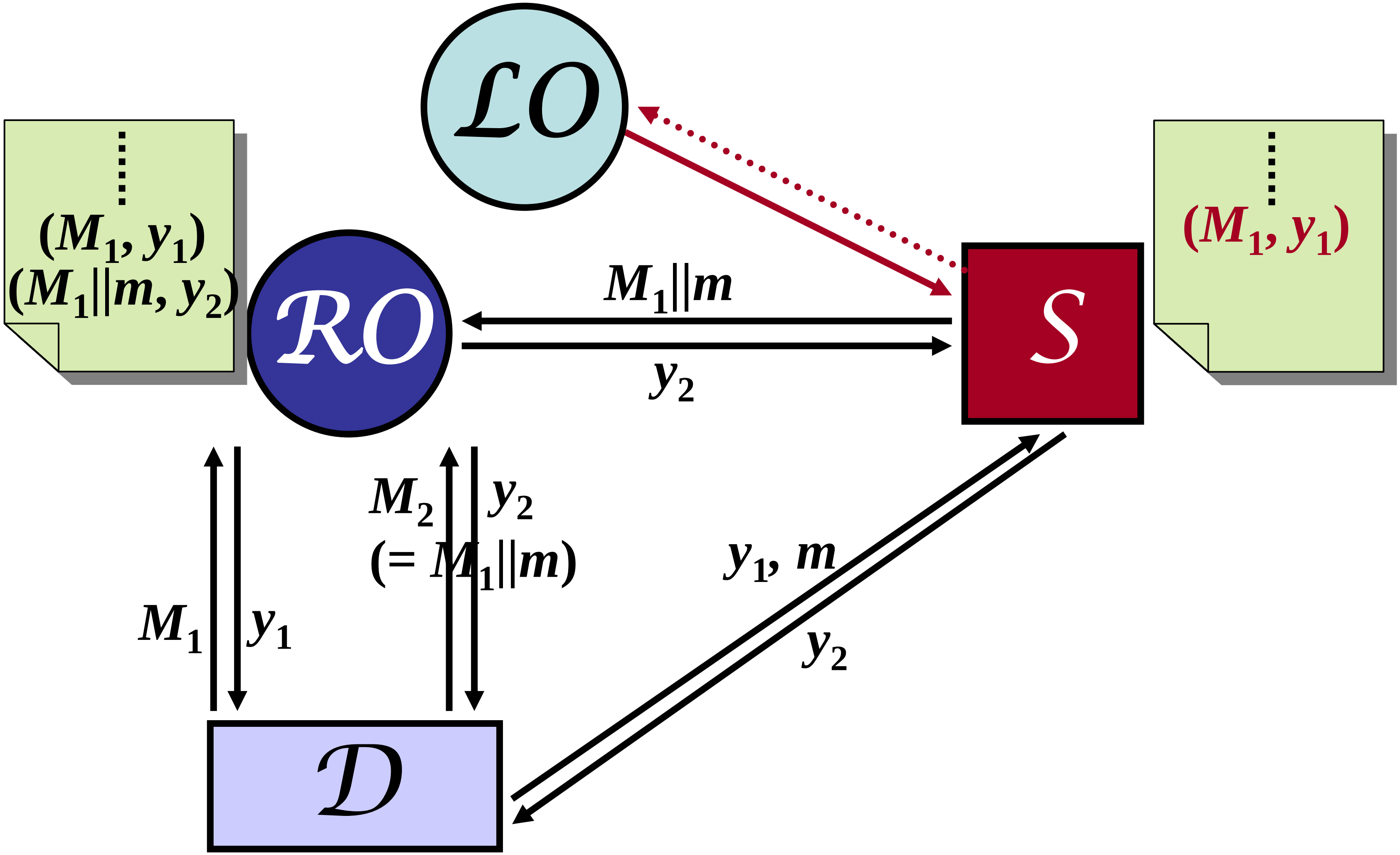
- a weakened $\mathcal{RO}$ model to analyze the security against leakage of the hash list

- Security in LROM
  - secure: majority of signatures, Cramer-Shoup-PKE etc [DRS09]
  - insecure: OAEP, KurosawaDesmedt-PKE

Def. of leaky random oracle model

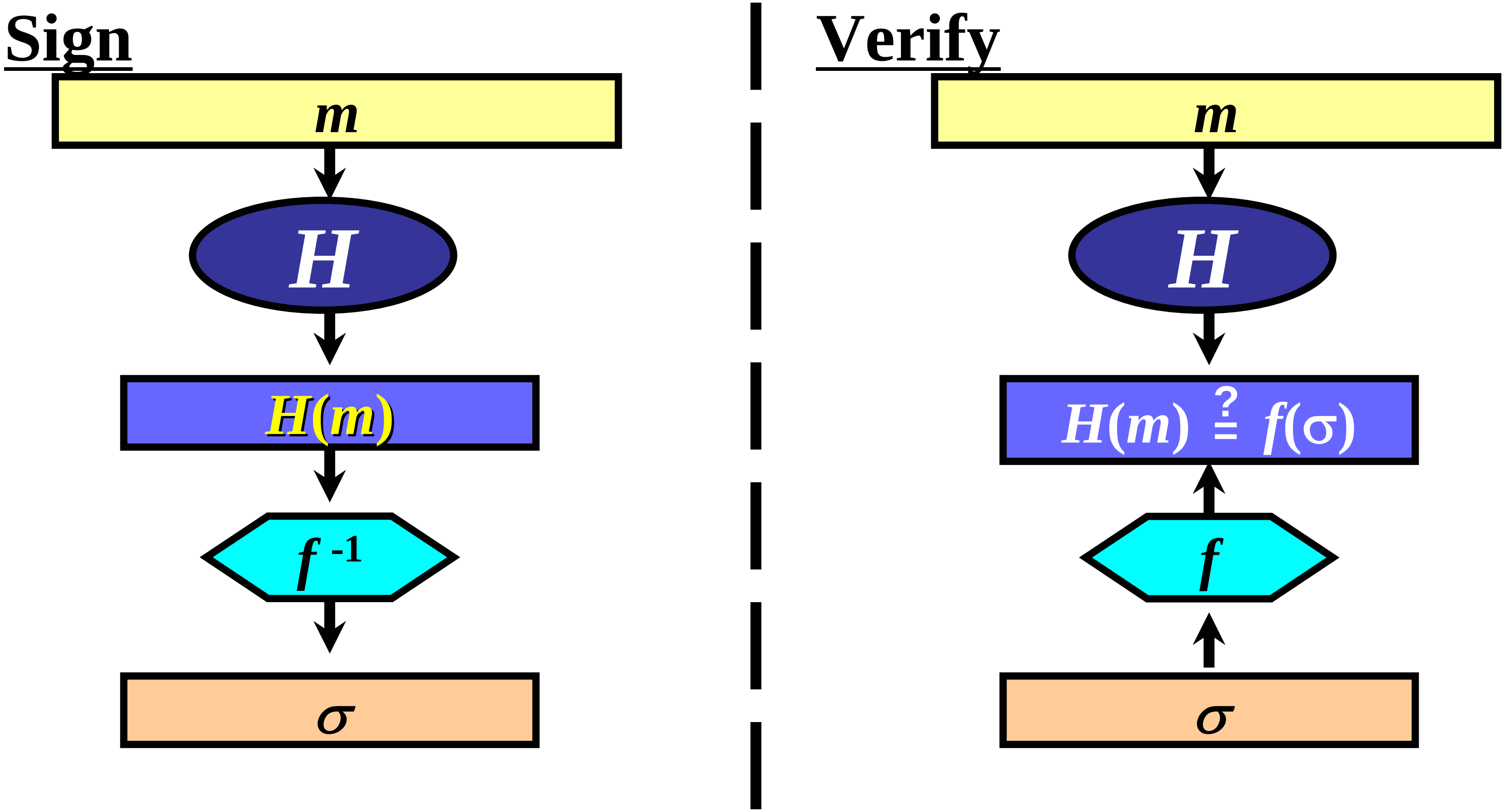


Intuition of $\boldsymbol{MD}^{\mathrm{FIL}^{\mathcal{RO}}} \sqsubset \mathcal{LRO}$



FDH is secure in $\mathcal{RO}$ model

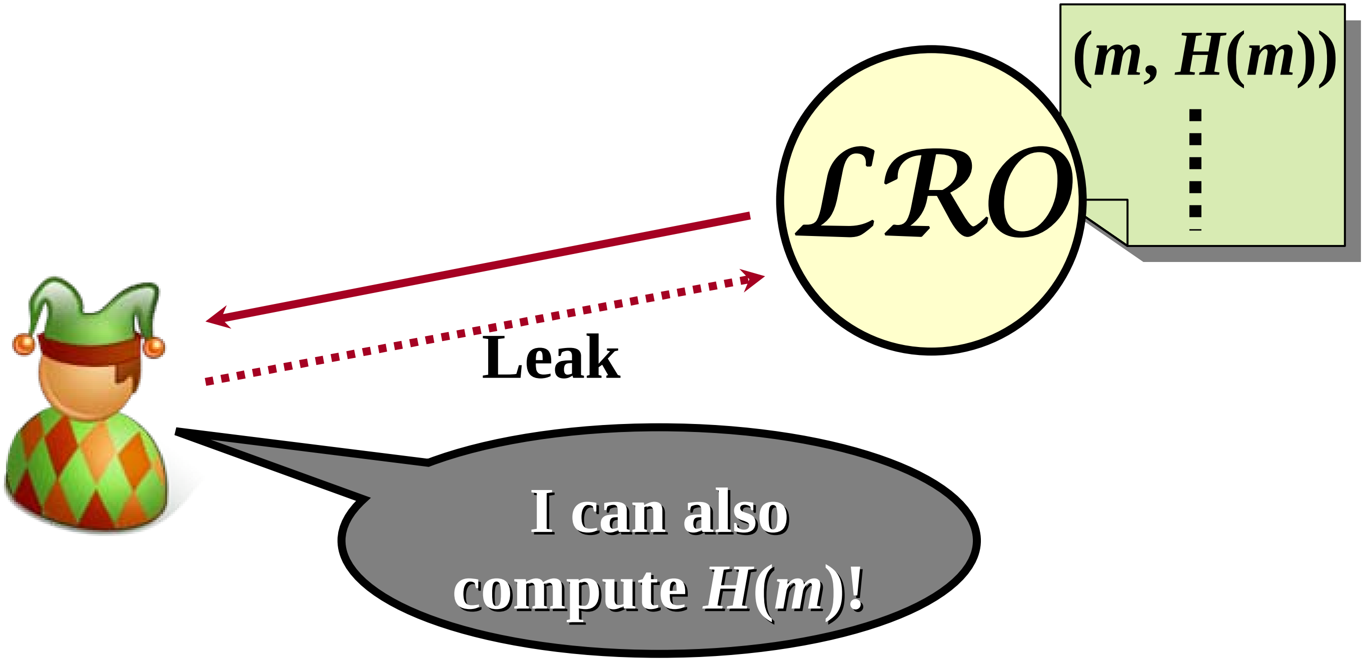
- FDH is a signature scheme which is EF-CMA secure in the $\mathcal{RO}$ model.



FDH is still secure in $\mathcal{LRO}$ model

- FDH is EF-CMA secure in the $\mathcal{LRO}$ model.
  - Intuition:

    $(m, H(m))$ is not secret information for adv.



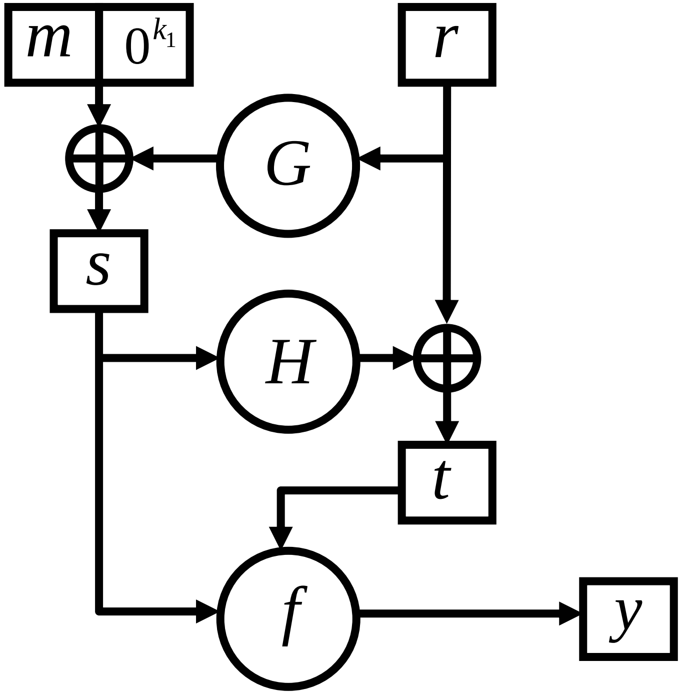
  - Thus, leak query gives no advantage to adv.

Security of OAEP in $\mathcal{RO}$ model

- OAEP is a padding scheme for PKEs, which is IND-CCA in the $\mathcal{RO}$ model.

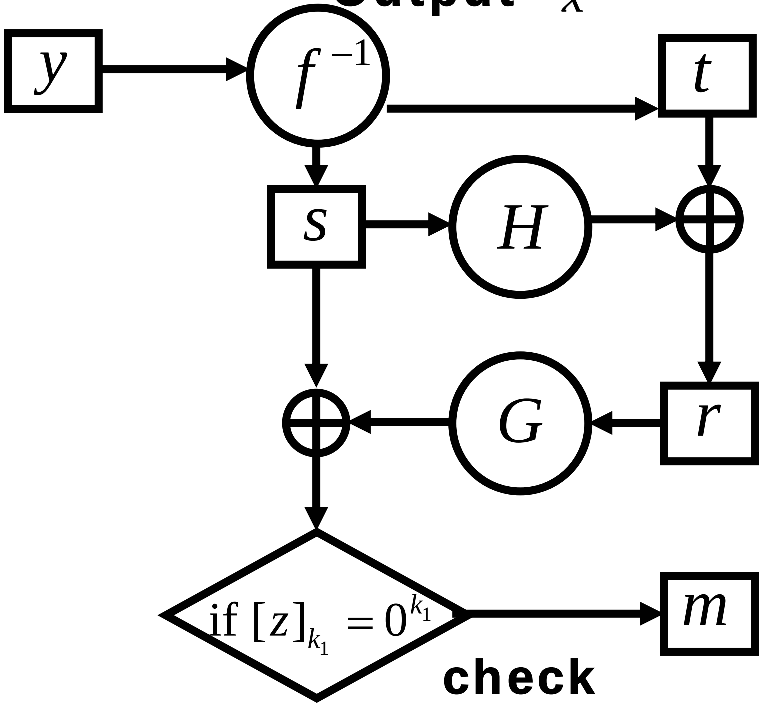
Enc.

input $m \leftarrow \{0,1\}^n$
Output y



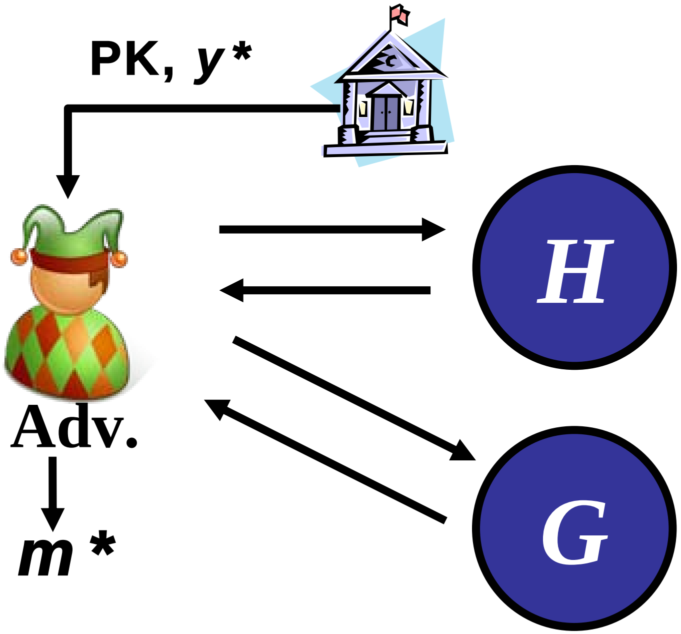
Dec.

input y
Output x



Insecurity of OAEP in $\mathcal{LRO}$ model

- OAEP is not one-way in the $\mathcal{LRO}$ model.



H-List

s_i	$H(s_i)$
⋮	⋮
s^*	$H(s^*)$
⋮	⋮

G-List

r_j	$G(r_j)$
⋮	⋮
r^*	$G(r^*)$
⋮	⋮

Step 1. compute $y' = f(s_i \,\|\, r_j \oplus H(s_i))$ **and find a pair** (s^*, r^*) **s.t.** $(y' = y^*) \wedge ([s^* \oplus G(r^*)]_{k1} = 0^{k1})$.

Step 2. compute $m^* = [s^* \oplus G(r^*)]^n$.

This procedure is the same as the simulation of the decryption oracle in the $\mathcal{RO}$ model.

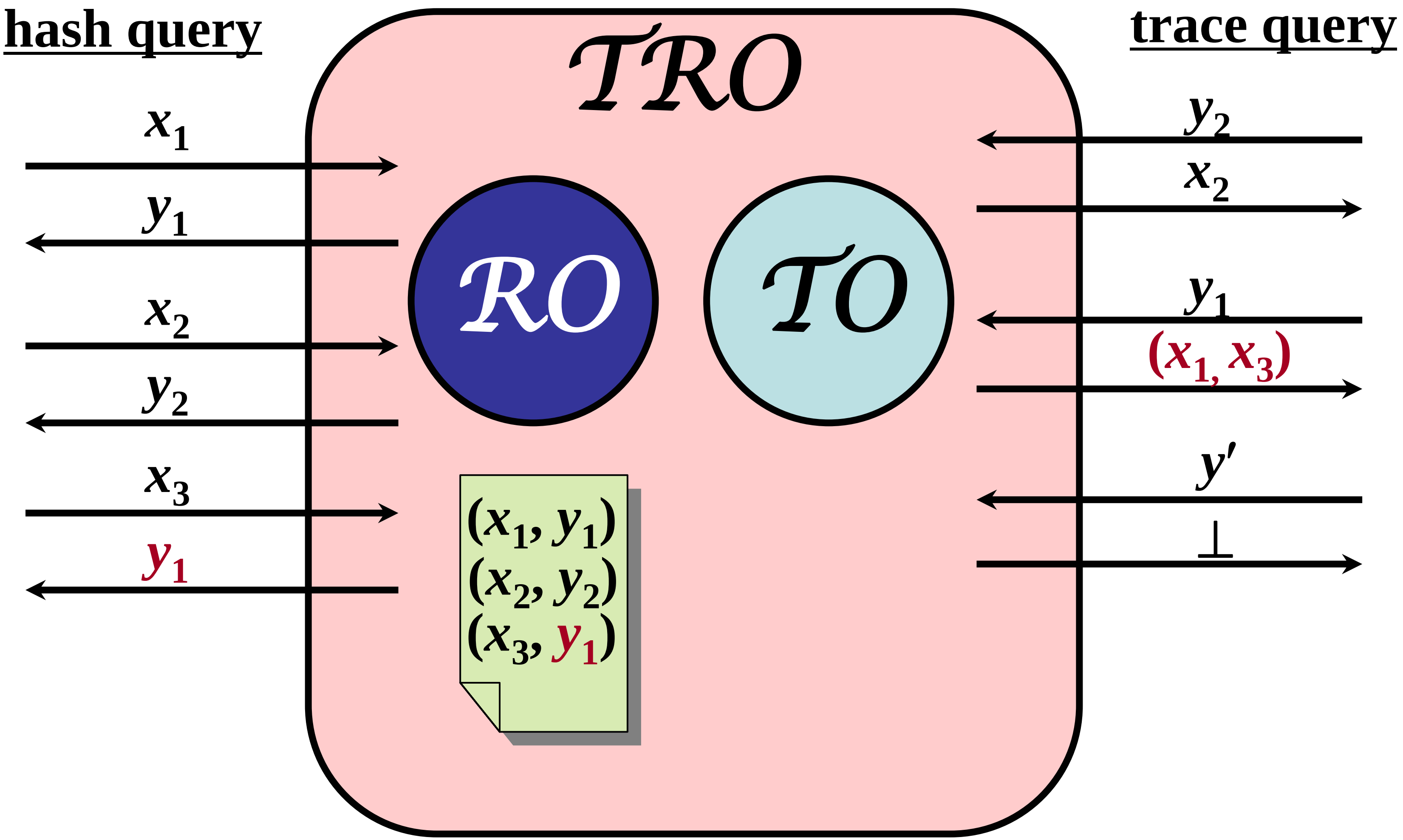
Traceable random oracle model

- $\mathcal{LRO}$ model reveals much information.
  - OAEP is insecure.

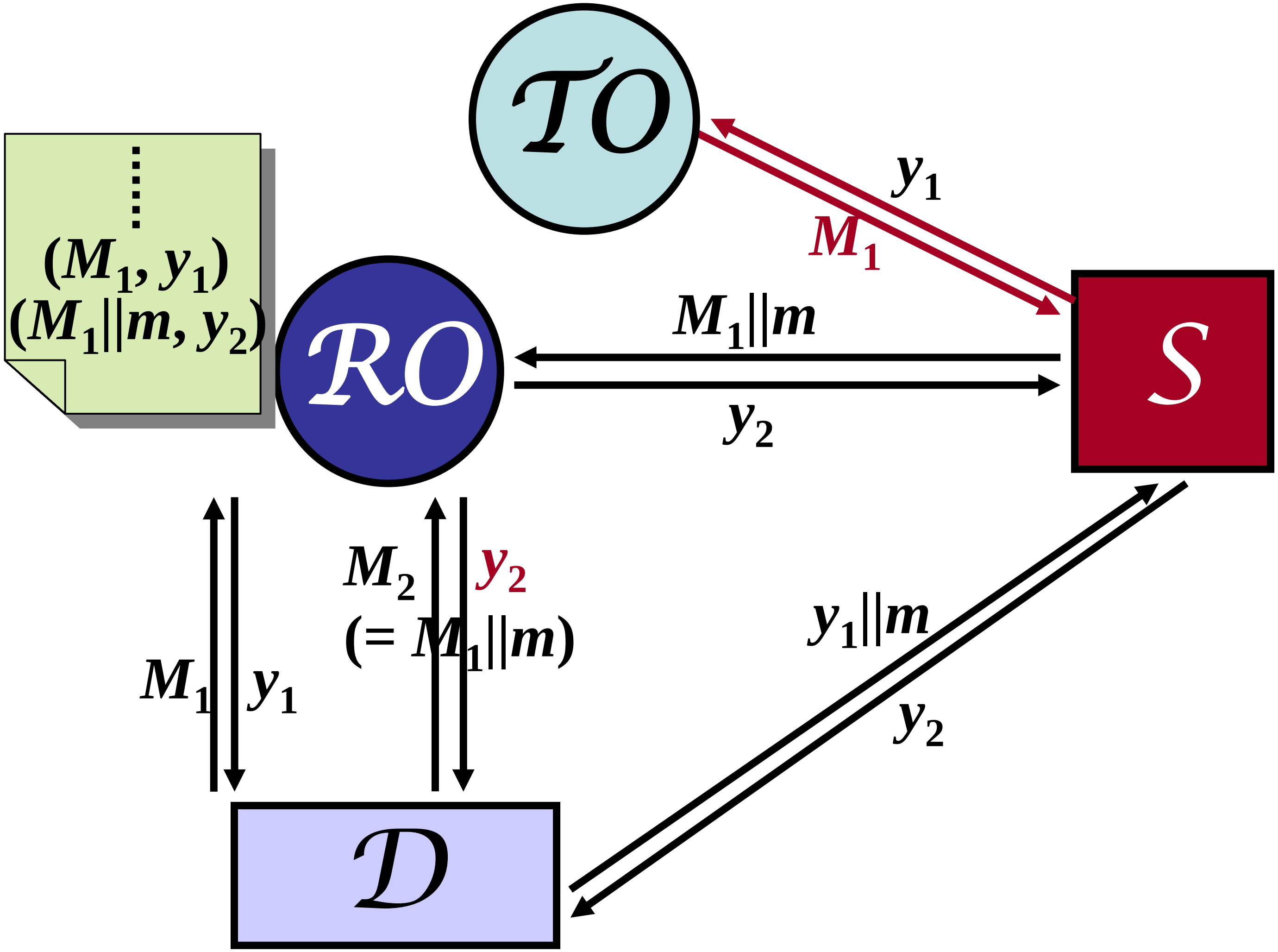
- Traceable random oracle ($\mathcal{TRO}$) model

  Revealing less information than $\mathcal{LRO}$
  - OAEP becomes secure. (IND-CCA)
  - $\boldsymbol{MD}^{\mathbf{FIL}\mathcal{RO}}$ is indifferentiable.

Def. of traceable random oracle model



Intuition of $\boldsymbol{MD}^{\mathrm{FIL}^{\mathcal{RO}}} \sqsubset \mathcal{TRO}$

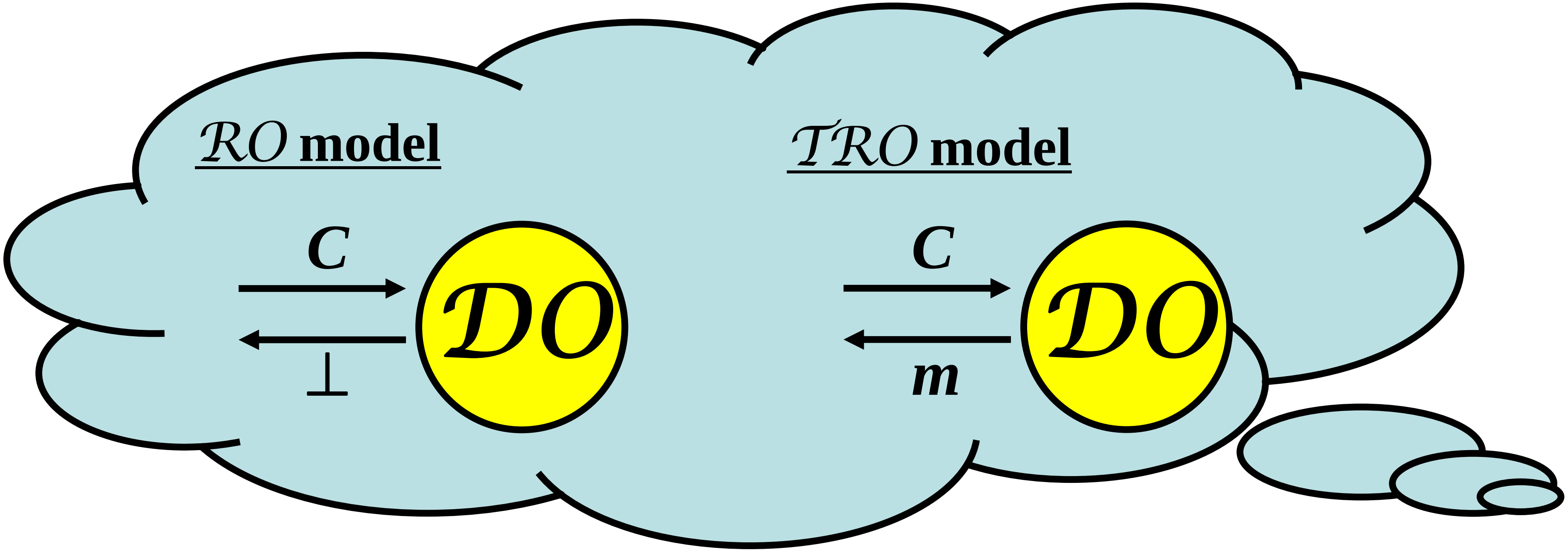


OAEP is secure in $\mathcal{TRO}$ model

- Influence of trace query
  - adv. obtains some information about plaintext.
  - trace query may strengthen power of CCA.

- Suc. prob. to reduce (t', ε')-pdTOWP
  - $\mathcal{RO}$ model : $\epsilon' \geq \frac{1}{q_{RH}} \cdot \Big(\frac{\epsilon}{2} - \frac{2q_D q_{RG} + q_D + q_{RG}}{2^{k_0}} - \frac{2q_D}{2^{k_1}} \Big)$
  - $\mathcal{TRO}$ model : $\epsilon' \geq \frac{1}{q_{RH}} \cdot \Big(\frac{\epsilon}{2} - \frac{2q_D q_{RG} + q_D + q_{RG}}{2^{k_0}} - \frac{2q_D}{2^{k_1}} \boxed{- \frac{q_{TG}}{2^{n+k_1}} \Big) - \frac{q_{TH}}{2^{k_0}}}$

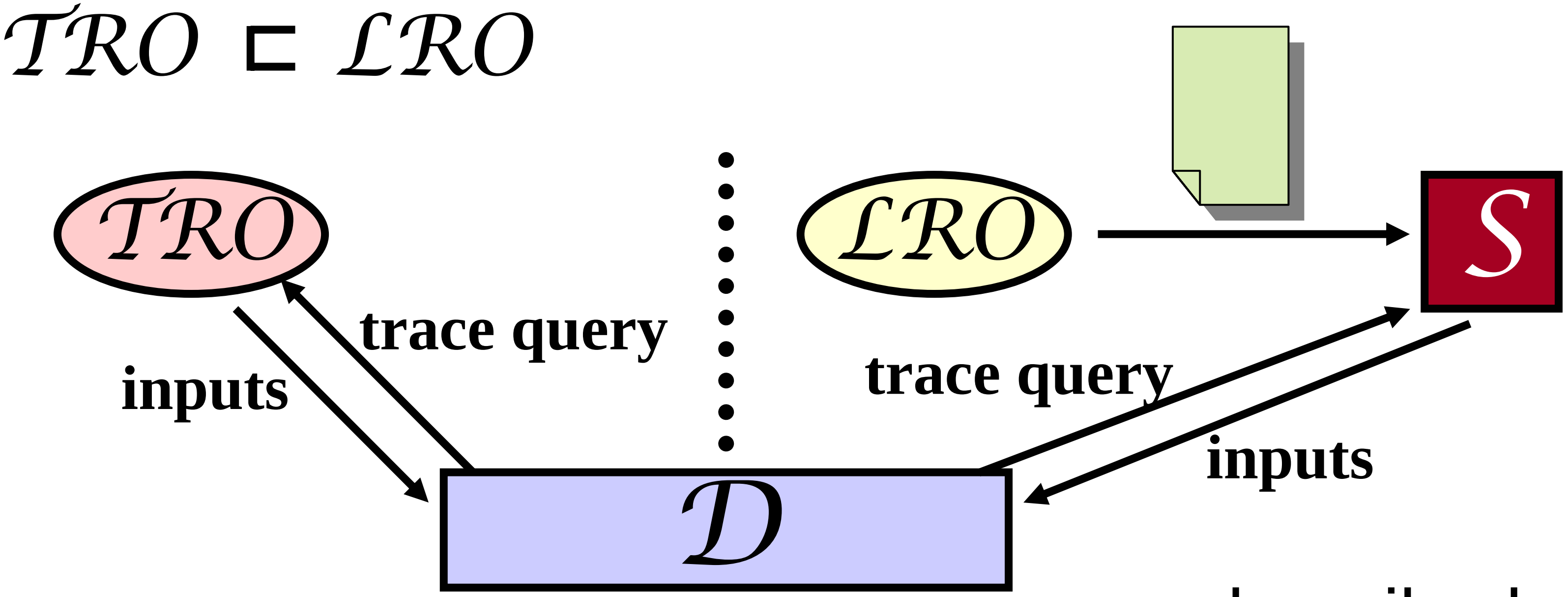
Does $\mathcal{TO}$ strengthen power of CCA?



- No.
  - $\mathcal{TO}$ does not update the hash lists of H and G regardless of trace query used.
  - The number of valid ciphertexts is not increased by $\mathcal{TO}$.

Relation between $\mathcal{LRO}$ and $\mathcal{TRO}$

- $\mathcal{TRO} \sqsubset \mathcal{LRO}$



described only
public channel

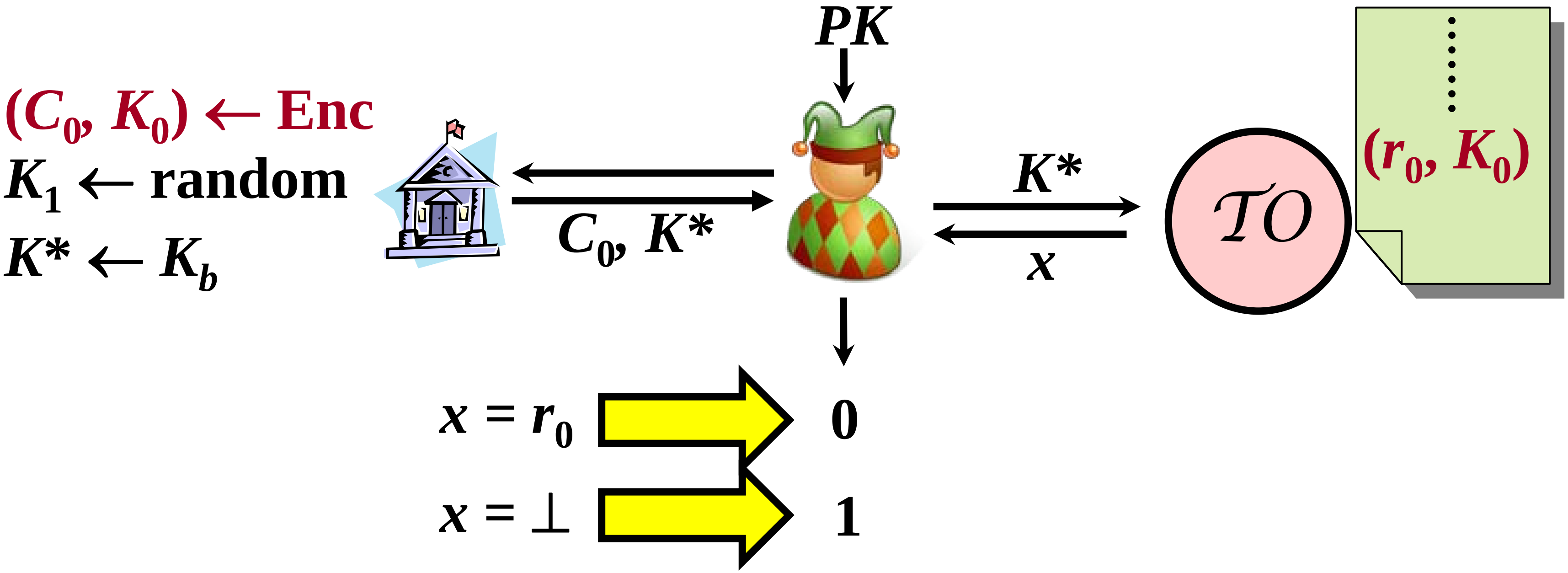
- $\mathcal{LRO} \not\sqsubset \mathcal{TRO}$
  - OAEP is evidence.

Insecurity of RSA-KEM in $\mathcal{TRO}$ model

- RSA-KEM is not IND-CPA in the $\mathcal{TRO}$ model.

Enc. $PK : n, e \quad SK : d$

- $r \leftarrow_R \mathbf{Z}_n$
- The ciphertext $c = r^e \bmod n$, the key $K = H(r)$.



$(C_0, K_0) \leftarrow$ Enc

$K_1 \leftarrow$ random

$K^* \leftarrow K_b$

C_0, K^*

PK

K^*

x

$\mathcal{TO}$

(r_0, K_0)

$x = r_0 \Rightarrow 0$

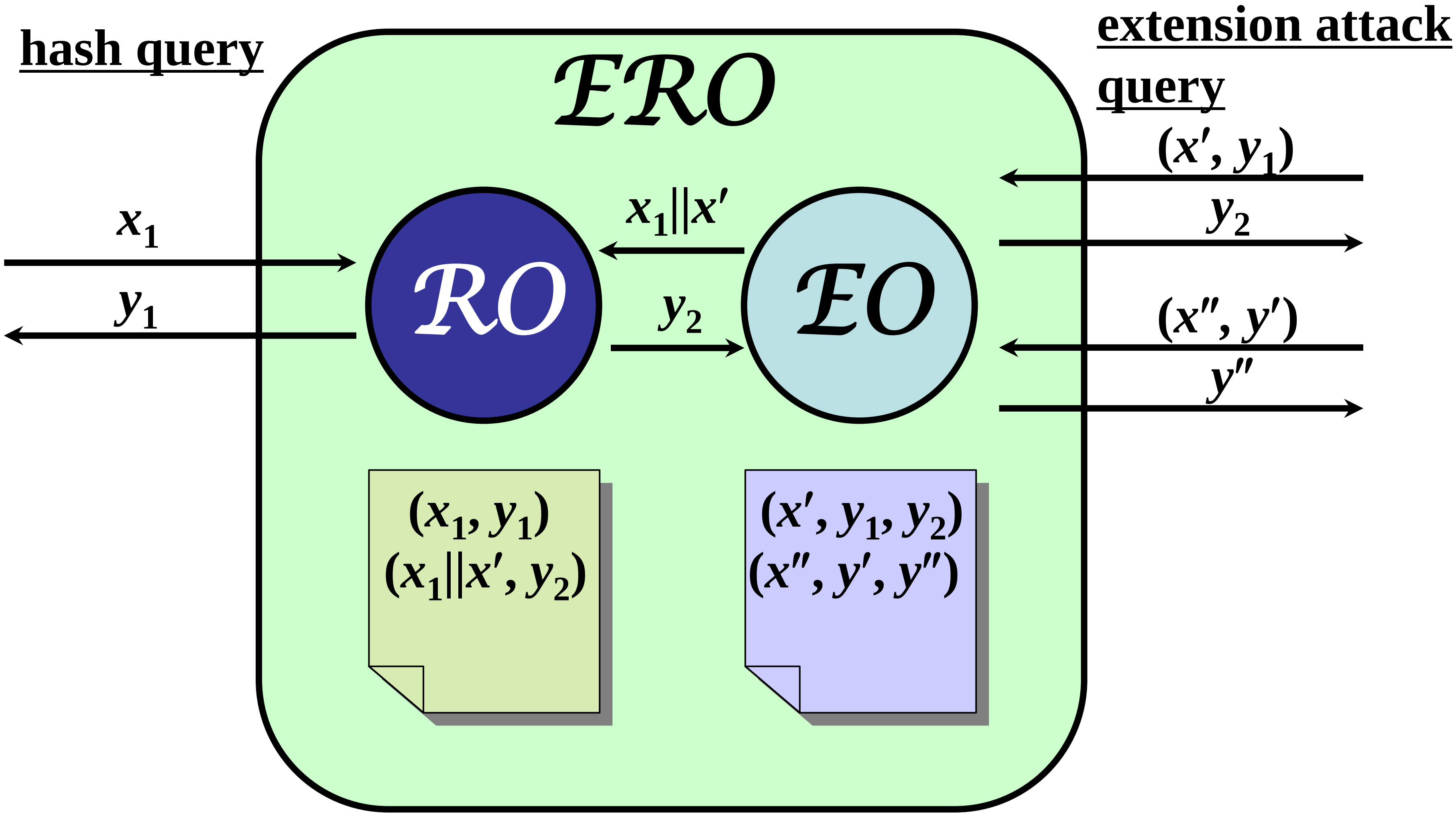
$x = \perp \Rightarrow 1$

Extension attack simulatable random oracle model

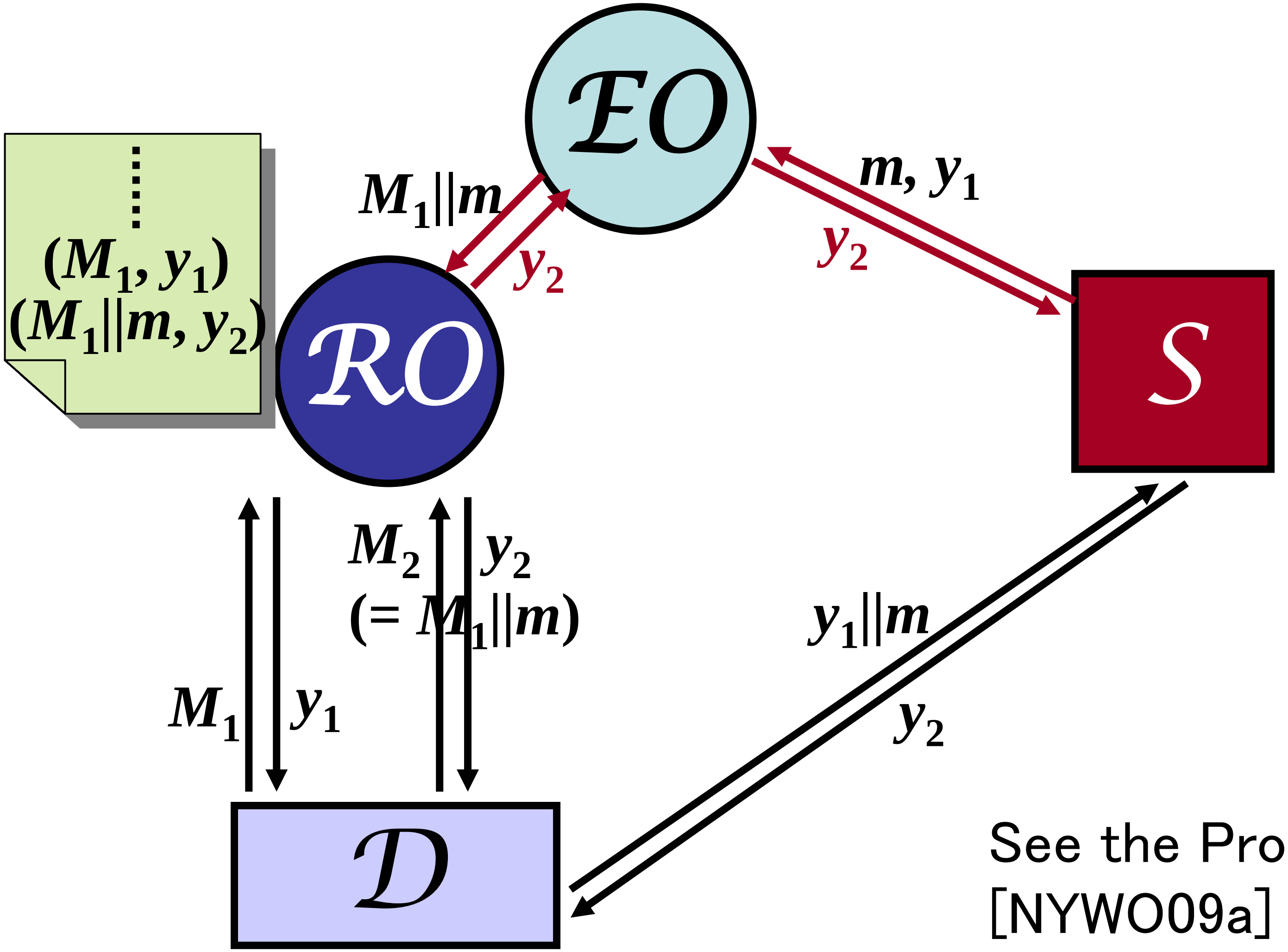
- $\mathcal{TRO}$ model still reveals information.
  - RSA-KEM is insecure.

- Extension attack simulatable random oracle ($\mathcal{ERO}$) model
  - RSA-KEM becomes secure. (IND-CCA)
  - **also,** $MD^{\mathrm{FIL}\mathcal{RO}}$ is indifferentiable.

Def. of extension attack simulatable random oracle model



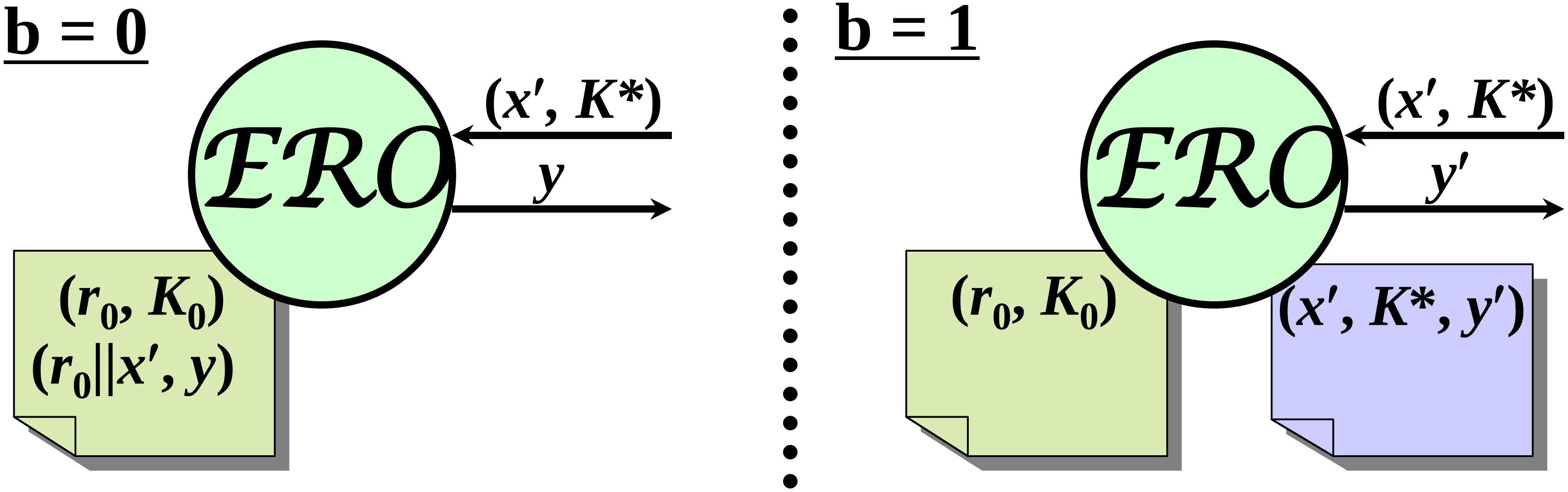
Intuition of $\boldsymbol{MD}^{\mathrm{FIL}^{\mathcal{RO}}} \sqsubset \mathcal{ERO}$



See the Proof in [NYWO09a]

Security of RSA-KEM in $\mathcal{ERO}$ model

- $\mathcal{EO}$ gives no advantage.



b = 0

$\mathcal{ERO}$

(x', K^*)

y

(r_0, K_0)

$(r_0||x', y)$

b = 1

$\mathcal{ERO}$

(x', K^*)

y'

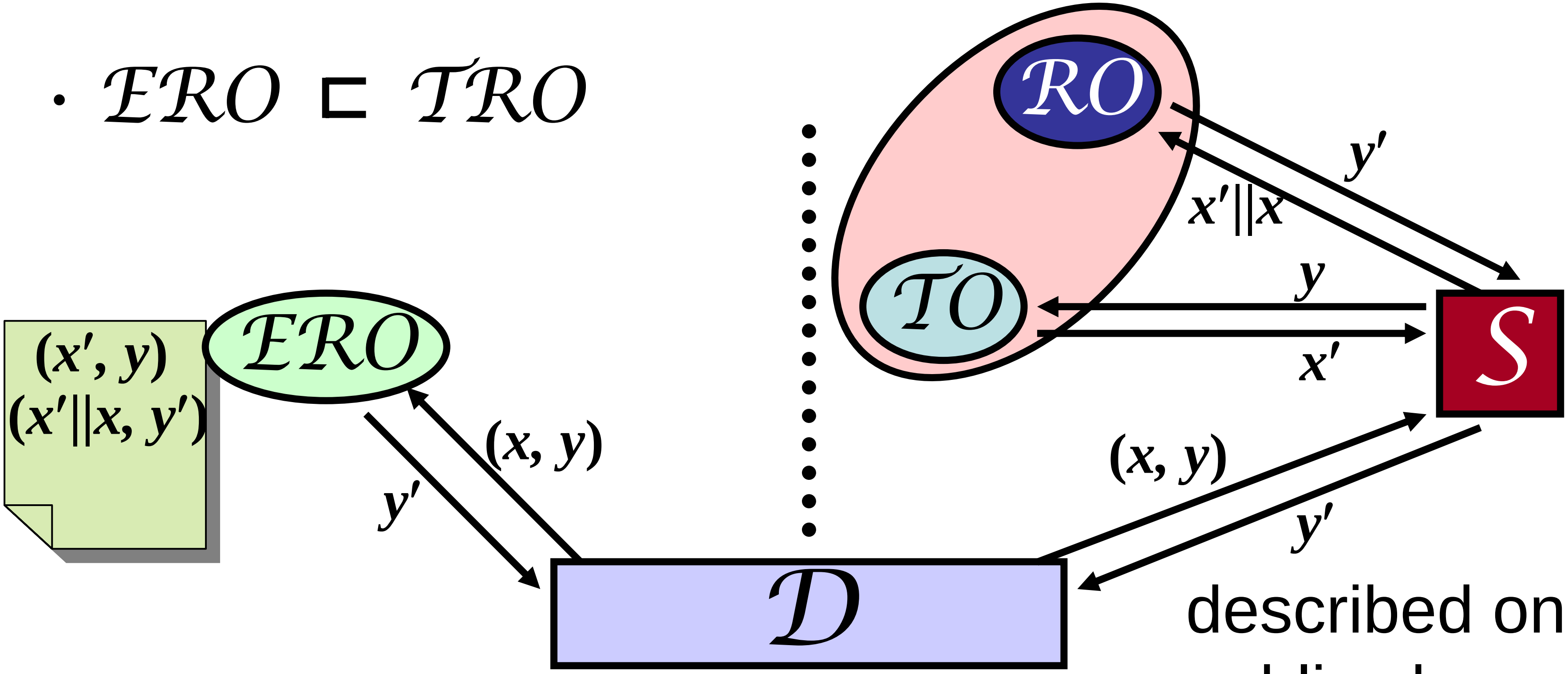
(r_0, K_0)

(x', K^*, y')

y and y' are indistinguishable
until r_0 or $r_0||x'$ is posed to $\mathcal{RO}$
as M_1 or M_2

Relation between $\mathcal{TRO}$ and $\mathcal{ERO}$

- $\mathcal{ERO} \sqsubset \mathcal{TRO}$



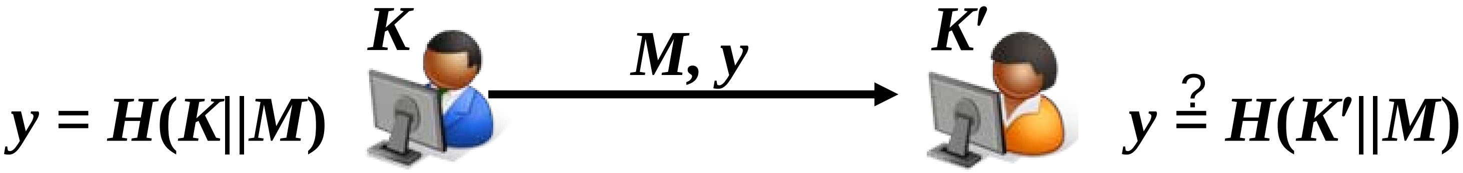
described only public channel

- $\mathcal{TRO} \not\sqsubset \mathcal{ERO}$
  – RSA-KEM is evidence.

Relation between $\mathcal{ERO}$ and $\mathcal{RO}$

- $\mathcal{RO} \sqsubset \mathcal{ERO}$
  - trivial. ($\mathcal{ERO} = (\mathcal{RO}, \mathcal{EO})$)

- $\mathcal{ERO} \not\sqsubset \mathcal{RO}$
  - Prefix MAC is secure in the $\mathcal{RO}$ model, but insecure in the $\mathcal{ERO}$ model.



K

M, y

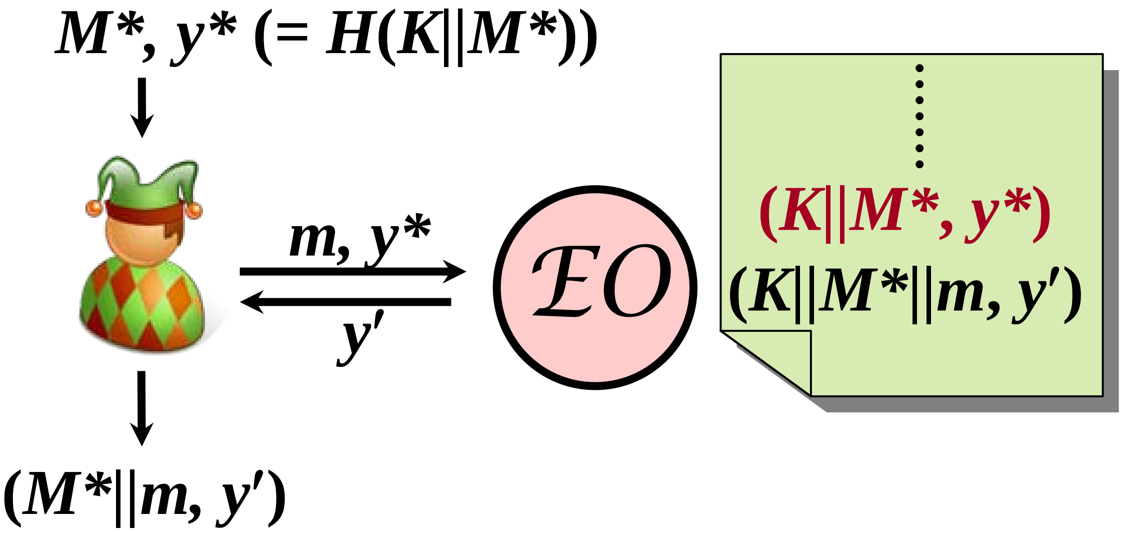
K'

$y = H(K||M)$

$y \overset{?}{=} H(K'||M)$

Insecurity of Prefix MAC in $\mathcal{ERO}$ model

- Prefix MAC is not EF-KMA secure in the $\mathcal{ERO}$ model.



M^*, y^* (= $H(K||M^*)$)

m, y^*

y'

$\mathcal{EO}$

$\vdots$

$(K||M^*, y^*)$

$(K||M^*||m, y')$

$(M^*||m, y')$

Conclusion (app. 2 for MD)

- Relations among models

$$\mathcal{RO} \underset{\not\sqsupset}{\sqsubset} \mathbf{MD}^{\mathrm{FIL}\mathcal{RO}} \sqsubset \mathcal{ERO} \underset{\not\sqsupset}{\sqsubset} \mathcal{TRO} \underset{\not\sqsupset}{\sqsubset} \mathcal{LRO}$$

- Securities of cryptosystems in leaking $\mathcal{RO}$ models.

	$\mathcal{LRO}$	$\mathcal{TRO}$	$\mathcal{ERO}$	$\mathcal{RO}$
FDH	secure	secure	secure	secure
OAEP	insecure	secure	secure	secure
RSA-KEM	insecure	insecure	secure	secure
Prefix MAC	insecure	insecure	insecure	secure

Conclusion (1)

- Indifferentiability is a useful concept for discussing the security of composed crypto systems as well as the UC framework.
- This theory gives a negative result on the Random Oracle methodology. (No program can instantiate RO indifferentiably.)
- This theory also gives a negative result on the original Merkle-Damgard construction.

These are the negative results of I.D. theory.

Conclusion (2)

- Practical protocols（FDH，OAEP, RSA-KEM）are provably secure even with the original MD.
- Approaches: Prove that by considering various leaking Random Oracle Models

1. the original MD Hashing is indifferentiable from the leaking RO, and
2. the protocol is secure within the leaking RO.

- The Theory of Indifferentiability ensures the security of these protocols under the assumption of the FILRO compression function.

Papers related to this talk

- **[NYWO09a] Naito, Yoneyama, Wang, Ohta, “How to Prove the Security of Practical Cryptosystems with Merkle-Damgård Hashing by Adopting Indifferentiability”, ePrint 2009/040**
- **[YMO08] Yoneyama, Miyagawa, Ohta, “Leaky Random Oracle”, ProvSec 2008**
- **[MRH04] Maurer, Renner, Holenstein, “Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology”, TCC 2004**
- **[CDMP05] Coron, Dodis, Malinaud, Puniya, “Merkle-Damgård Revisited: How to Construct a Hash Function”, CRYPTO 2005**