Indifferentiability of Merkle-Damgård Hash Function Revisited: Impact to Practical Cryptosystems

Lei Wang

The University of Electro-Communications

(Joint work with Naito, Yoneyama, Ohta)

@ Hash Workshop in Kyushu University

Indifferentiability of Merkle-Damgård Hash Functio Revisited Impact to Practical Crypt systems

versus Private-interface-leaking Random Oracle

T

@ Hash Workshop in Kyushu University

Indifferentiability of Merkle-Damgård Hash Function Revisited: Impact to Practical Cryptosystems

Lei Wang

- Security of individual protocol using MD:
  Unclear (instead of insecure)!
- Protocols in Weakened Random Oracle:
  Continuously studied!

@ Hash Workshop in Kyushu University

Outline

- Background
- Our Goal
- Private-interface-leaking Random Oracles
- Conclusion

Outline

- **Background**
- Our Goal
- Private-interface-leaking Random Oracles
- Conclusion

A Bad Fact

Any Dedicated Hash Function can be easily distinguished from a Random Oracle

Canetti, Goldreich and Halevi, "The Random Oracle Methodology, Revisited ", STOC 1998.

Countermeasure?

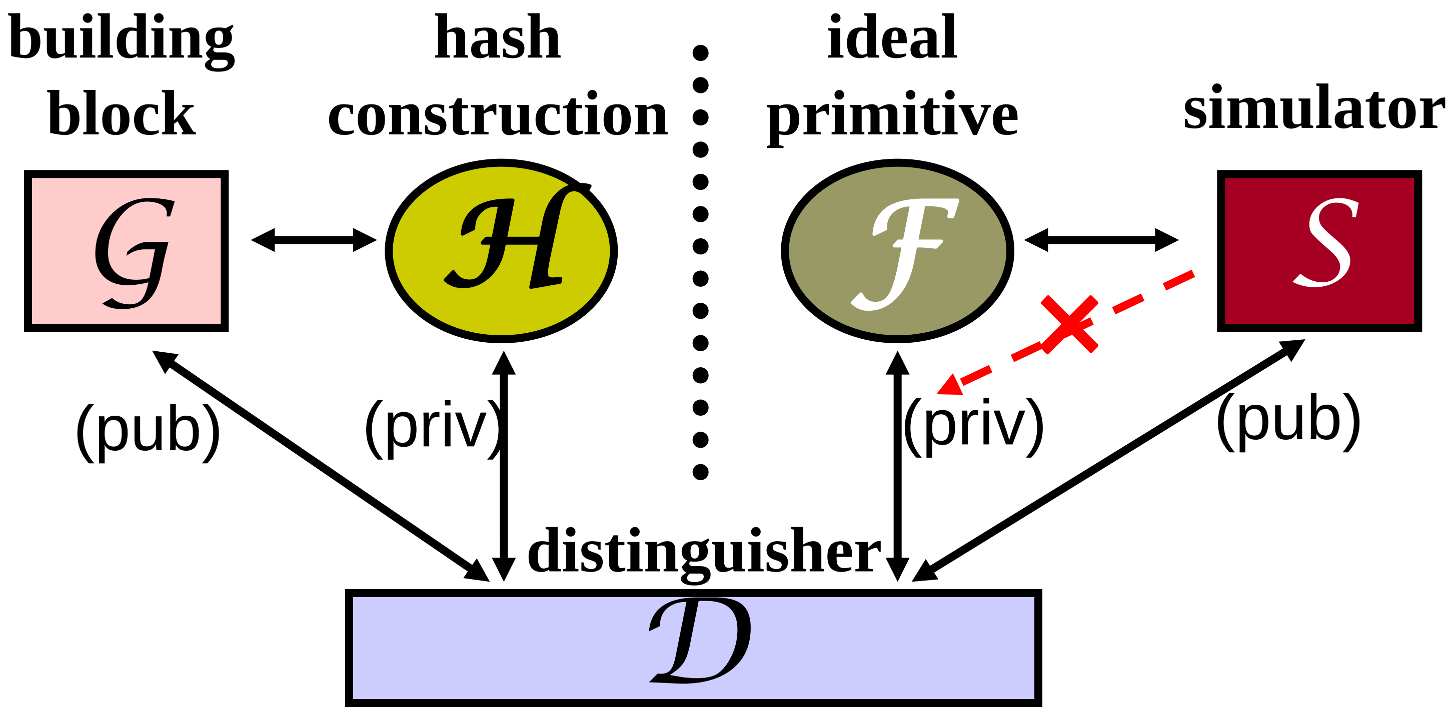
Indifferentiability!!!

- **General Applications: Maurer *et al.***
- **Hash Function: Coron *et al.***

Maurer, Renner and Holenstein, "Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology " , TCC 2004.

Coron, Dodis, Malinaud and Puniya, "Merkle-Damgård Revisited: How to Construct a Hash Function", CRYPTO2005

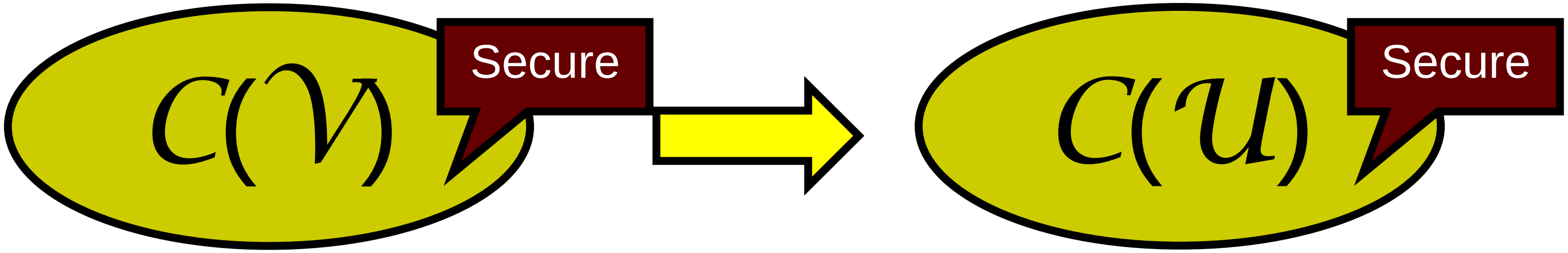
Application to Hash Function



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

Composition Theorem for Cryptosystems

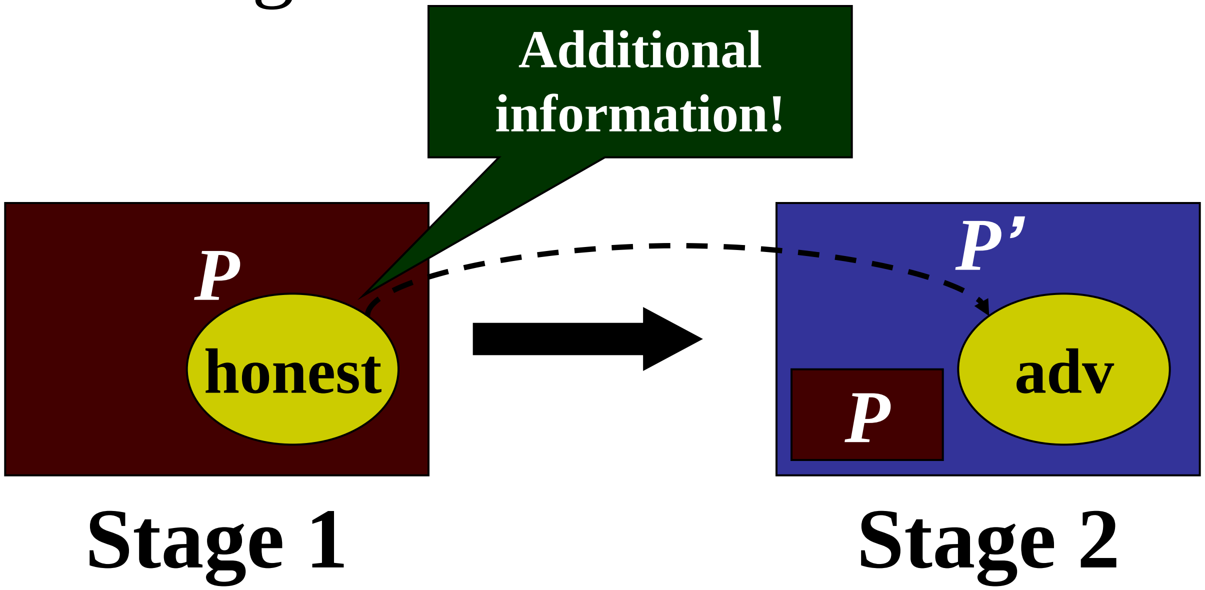
- If a Primitive U is indifferentiable from a Primitive V, (U ⊏ V), for any secure cryptosystem C(V), C(U) is also secure.



C(U) > C(V)

A Remark

- Only for Single Stage
- Multi-Stage: **Reset Indifferentiability!!!**



Ristenpart, Shacham and Shrimpton, "Careful with Composition: Limitations of the Indifferentiability Framework ", EUROCRYPT2011.

A Remark

- Only for Single Stage
- Multi-Stage

This talk deals with cryptosystems with only a single stage!

A Bad Fact

Merkle-Damgård Hash Function is not indifferentiable from a Random Oracle

Coron, Dodis, Malinaud and Puniya, "Merkle-Damgård Revisited: How to Construct a Hash Function", CRYPTO2005

The Consequence

- **MD is most popular hash function mode.**

- **The security of Cryptosystems using popular hash functions becomes unclear, even in the ideal model.**

Countermeasure?

Repair MD!!!

- Tailor the last block operation
- Tailor the message padding algorithm

Actually Cryptographers did more!

Sufficient properties to extend domain of an ideal primitive

- Pre-image Awareness
- Computable Message Awareness

Dodis, Ristenpart and Shrimpton, "Salvaging Merkle-Damgård for Practical Applications", EUROCRYPT2009.

Bhattacharyya, Mandal and Nandi, "Security Analysis of the Mode of JH Hash Function", FSE2011

Outline

- Background
- **Our Goal**
- Private-interface-leaking Random Oracles
- Conclusion

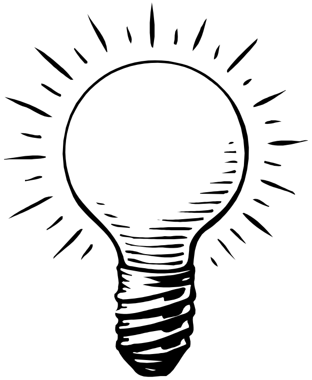
Shall we give up MD completely?

- Many popular hash functions are in MD mode, say SHA-2.
- The impact to cryptosystems is not clear yet.

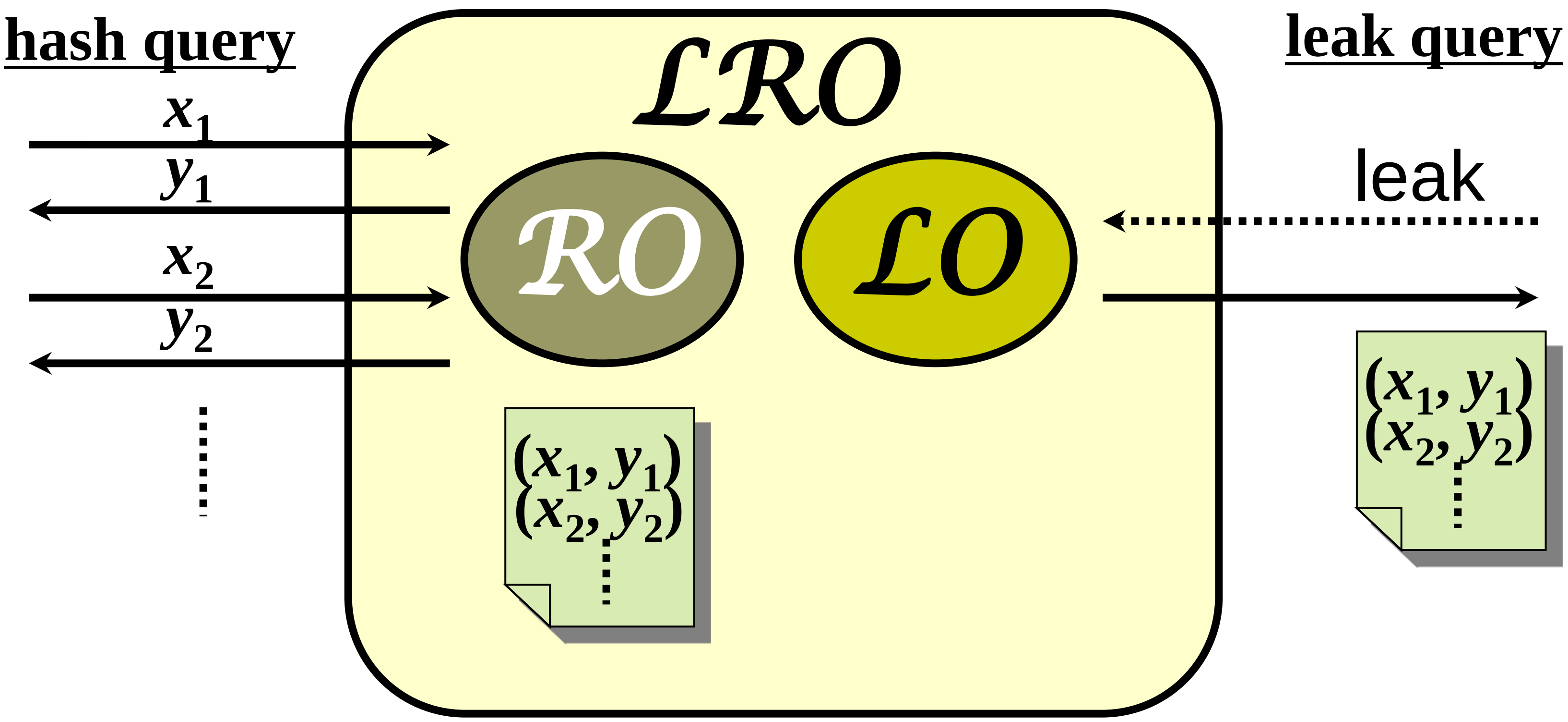
Goal: make it clear!!!

How?

Study of cryptosystems in
Weakened Random Oracle
inspired us!

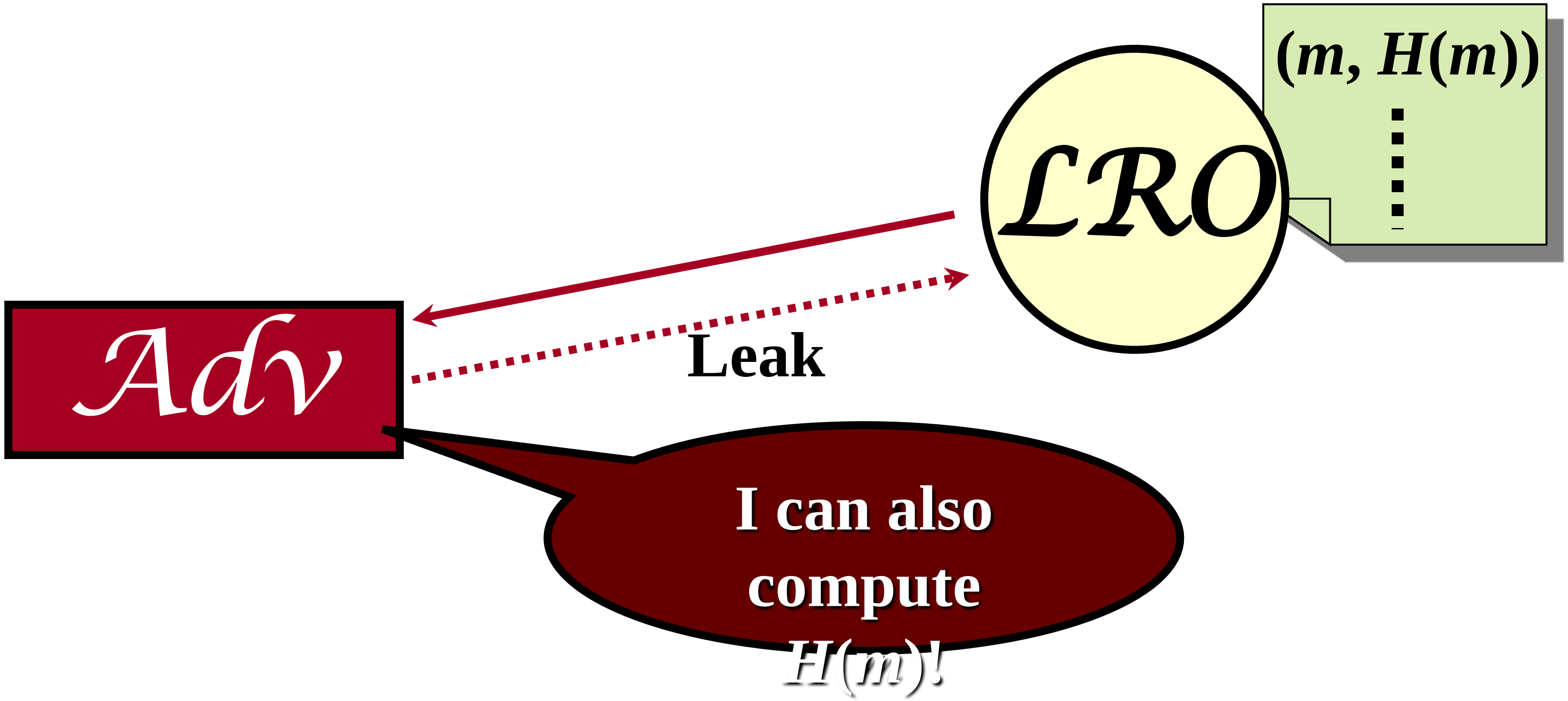


Example: Leaky Random Oracle (LRO)



Yoneyama, Miyagawa and Ohta, "Leaky Random Oracle", ProvSec2008

Full-domain Hash Signature in LRO



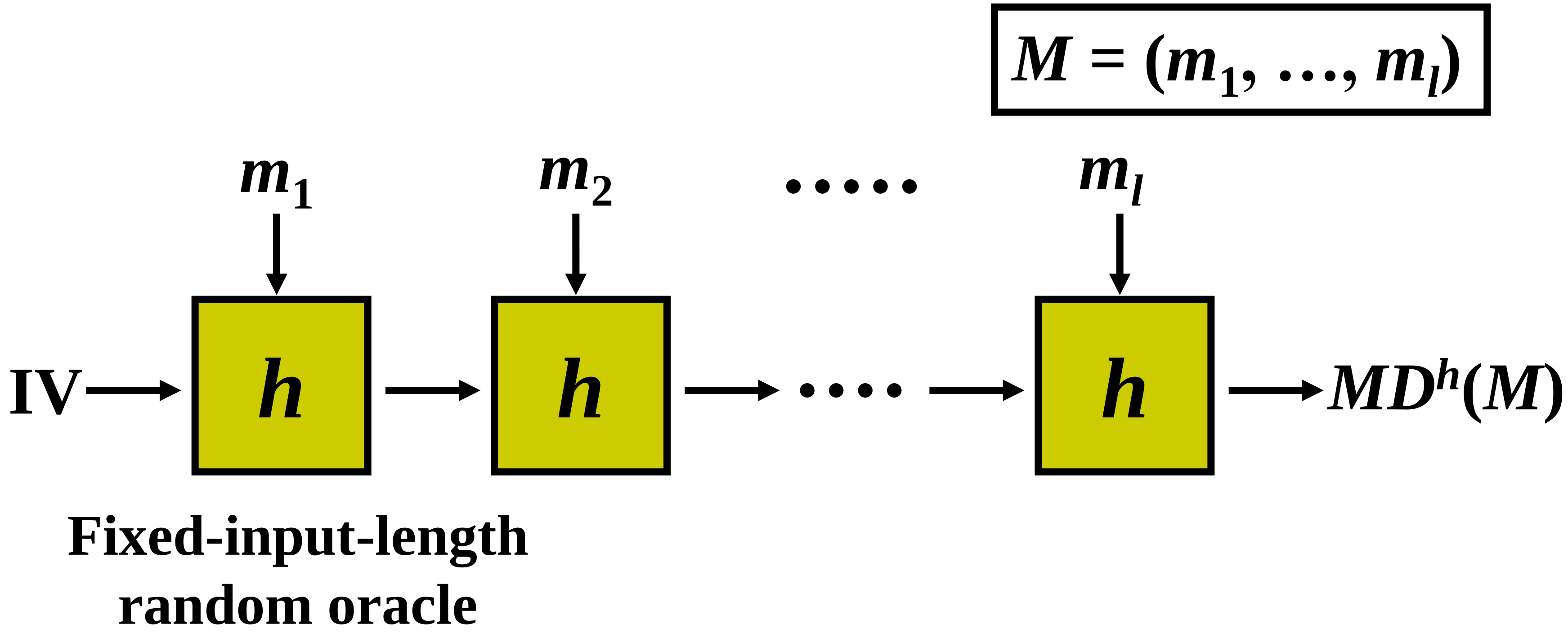
Intuitively, {*(m, H(m))*} is not secret to adversary.

Moreover, we proved that MD is indifferentiable from LRO.

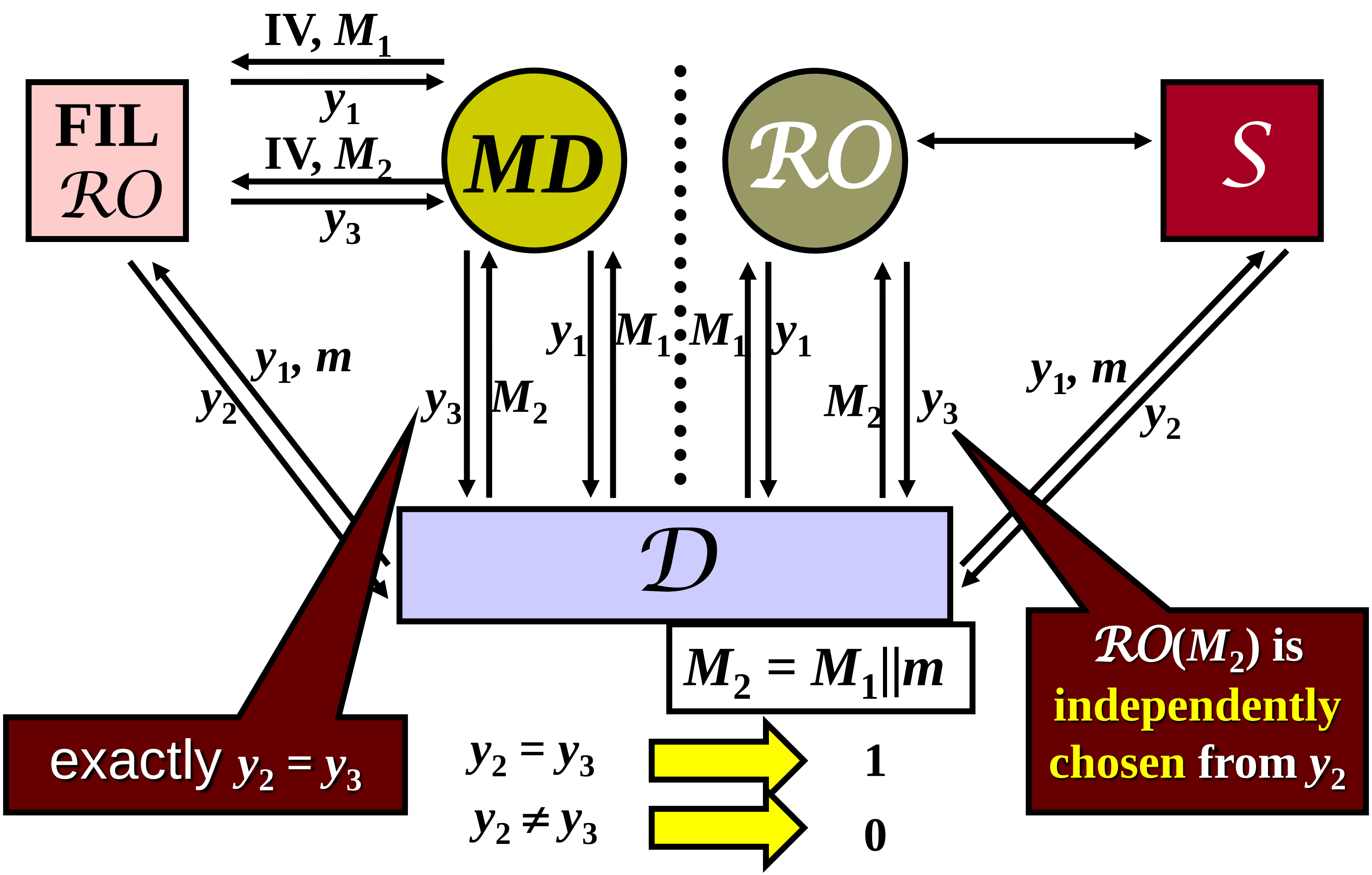
↓

FDH (actually many Digital Signature Schemes) is secure in MD mode.

MD Mode

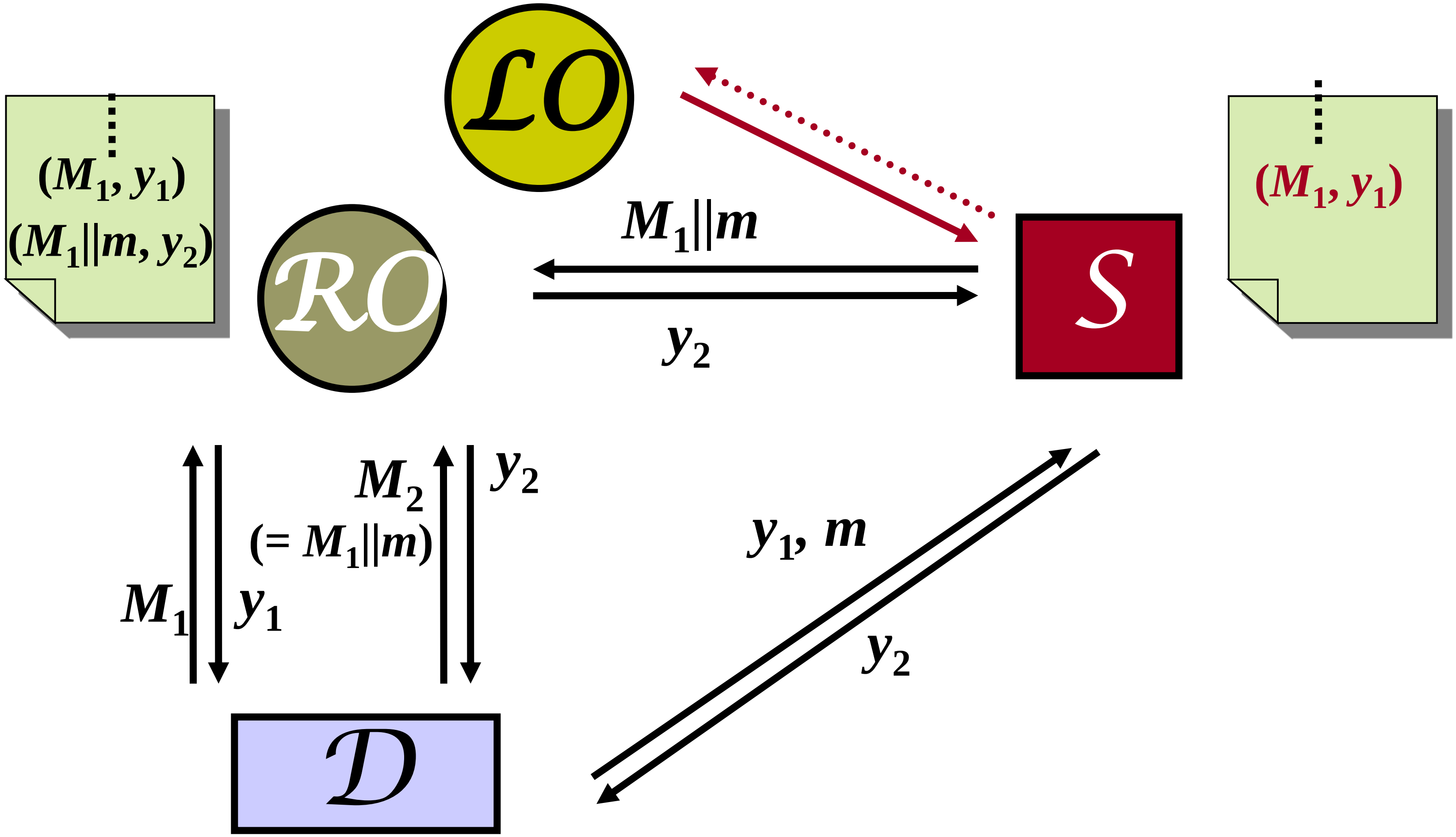


Length Extension Attack (LEA) can distinguish it from RO.



IV, M1
y1
IV, M2
y3
FIL RO
MD
RO
S
y1, m
y2
y3
M2
y1
M1
M1
y1
M2
y3
y1, m
y2
D
M2 = M1||m
exactly y2 = y3
y2 = y3
1
y2 ≠ y3
0
RO(M2) is independently chosen from y2

Intuition of MD ⊏ LRO



Modular Approach

- Define **private-interface-leaking** random oracles $\widetilde{\mathrm{RO}}$: MD $\sqsubset$ $\widetilde{\mathrm{RO}}$.
- **Re-evaluate** the security of **practical cryptosystems** in $\widetilde{\mathrm{RO}}$.

Outline

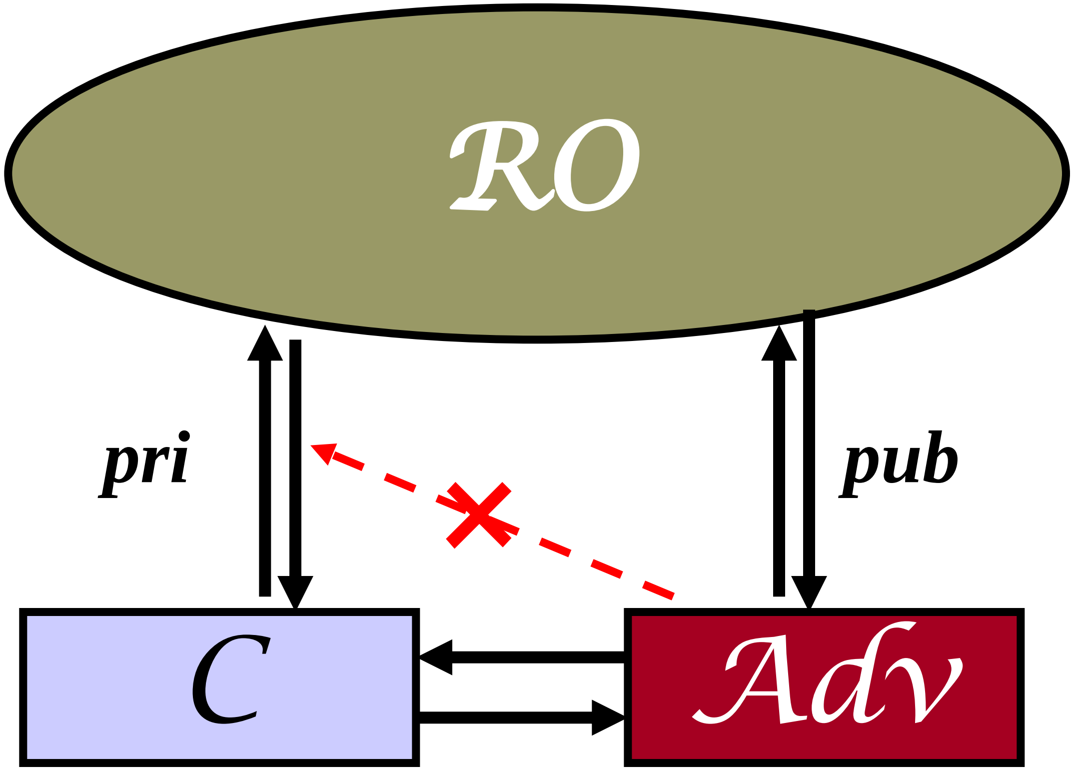
- Background
- Our Goal
- **Private-interface-leaking Random Oracles**
- Conclusion

Leaky Random Oracle

- Independent work by Dodis *et al.*: **Public-use Random Oracle**
- **Secure**: FDH, Fiat-Shamir Signature, …,
- **Insecure**: OAEP, RSA-KEM…
  - Too much information is leaked.

Dodis, Ristenpart and Shrimpton, "Salvaging Merkle-Damgård for Practical Applications", EUROCRYPT2009.

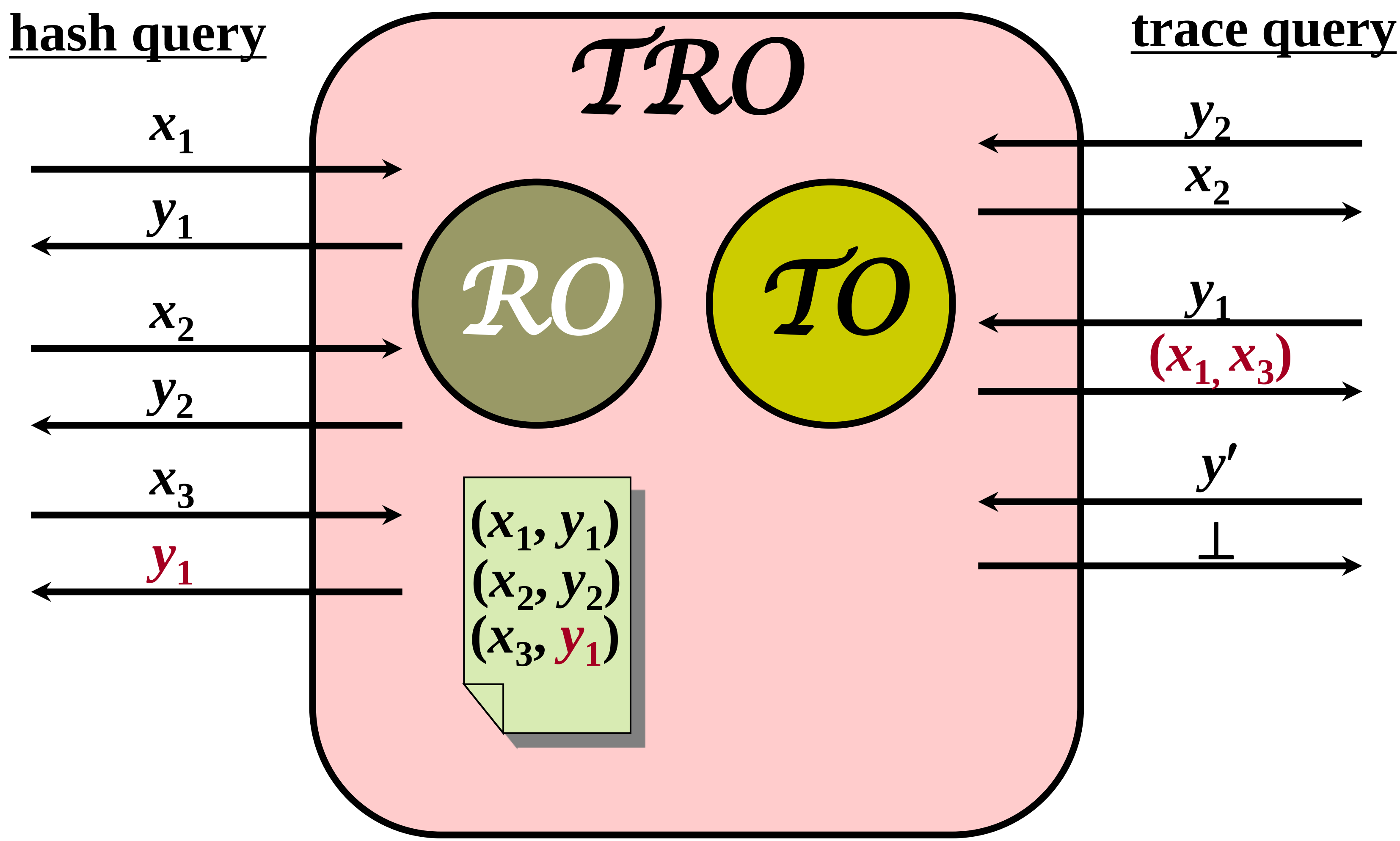
LRO Leaks too much Information



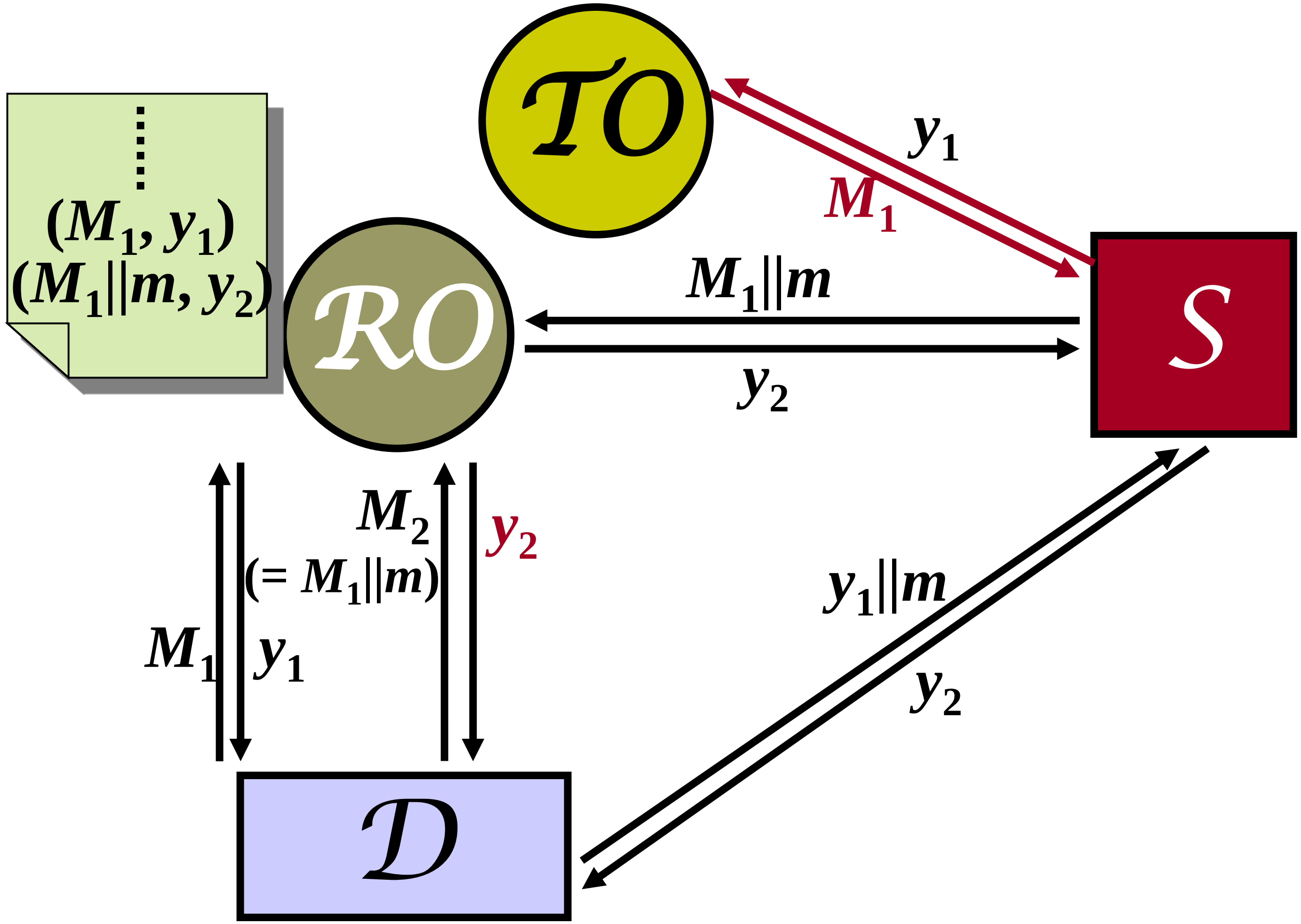
- **OAEP in LRO**

  Adv uses private interface information to simulate decryption of OAEP, and then break IND-CCA!

Traceable Random Oracle (TRO)



Intuition of MD ⊏ TRO

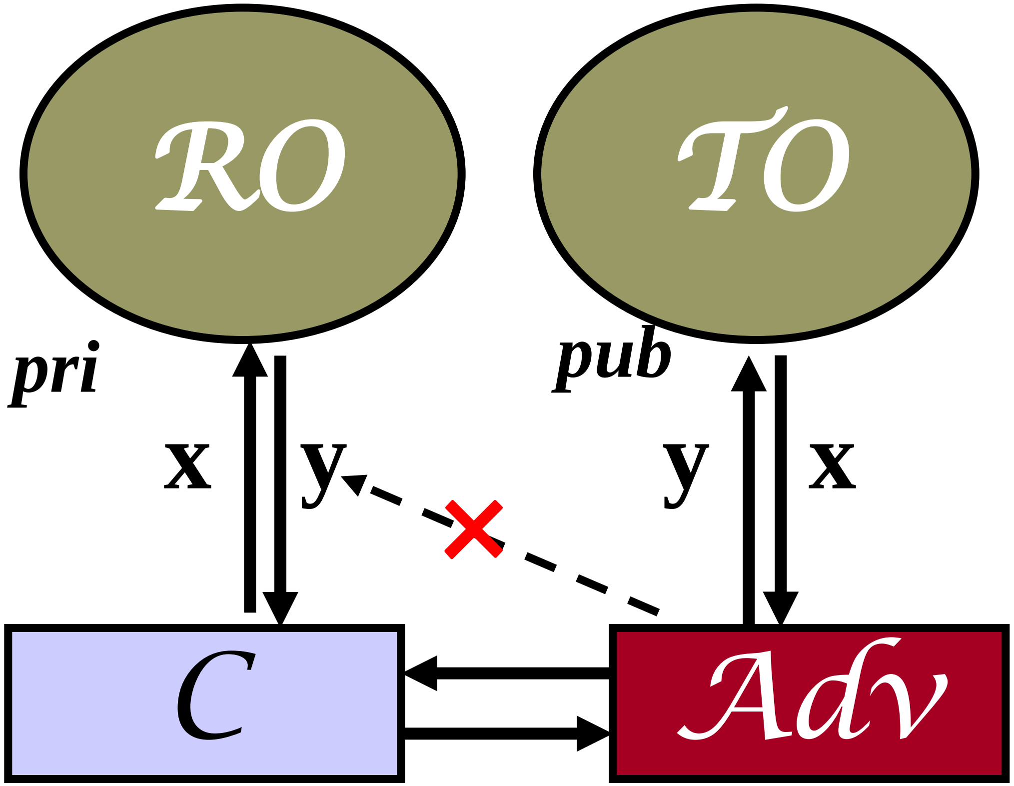


Cryptosystems in TRO

- **Secure:** **OAEP**, …
  - OAEP is **insecure** in LRO.

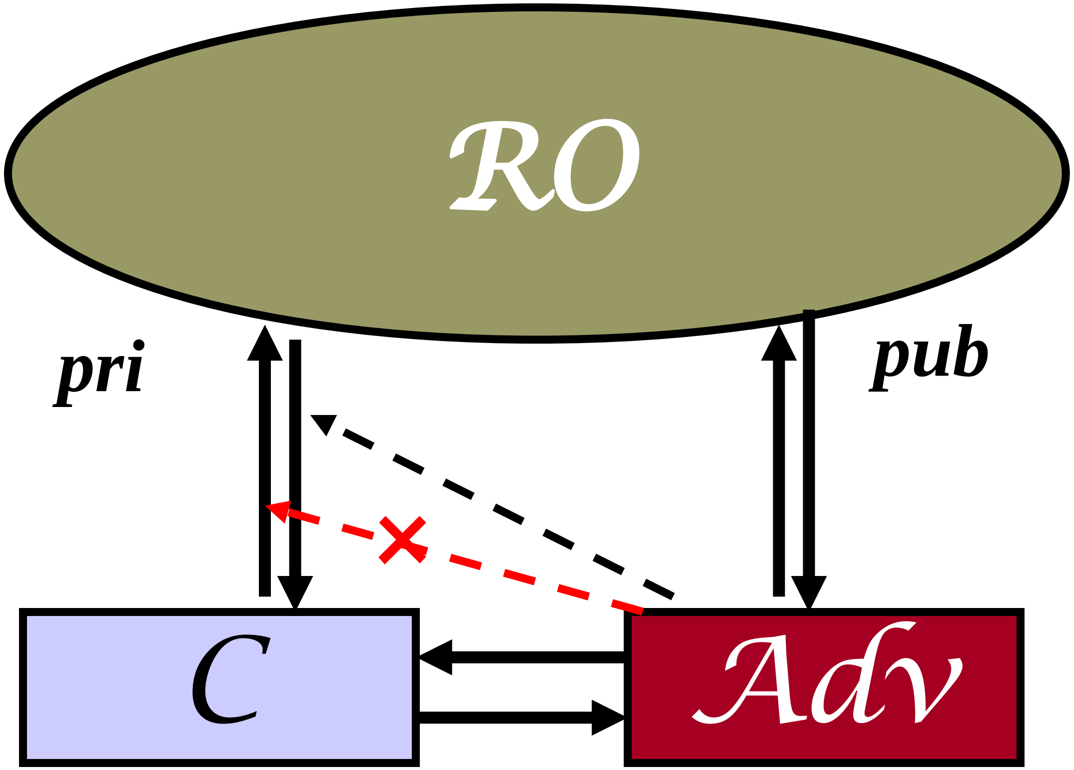
- **Insecure**: RSA-KEM,…
  - TRO requires **no leak** of **both query and response** in the private interface.

Revisit Cryptosystem in TRO

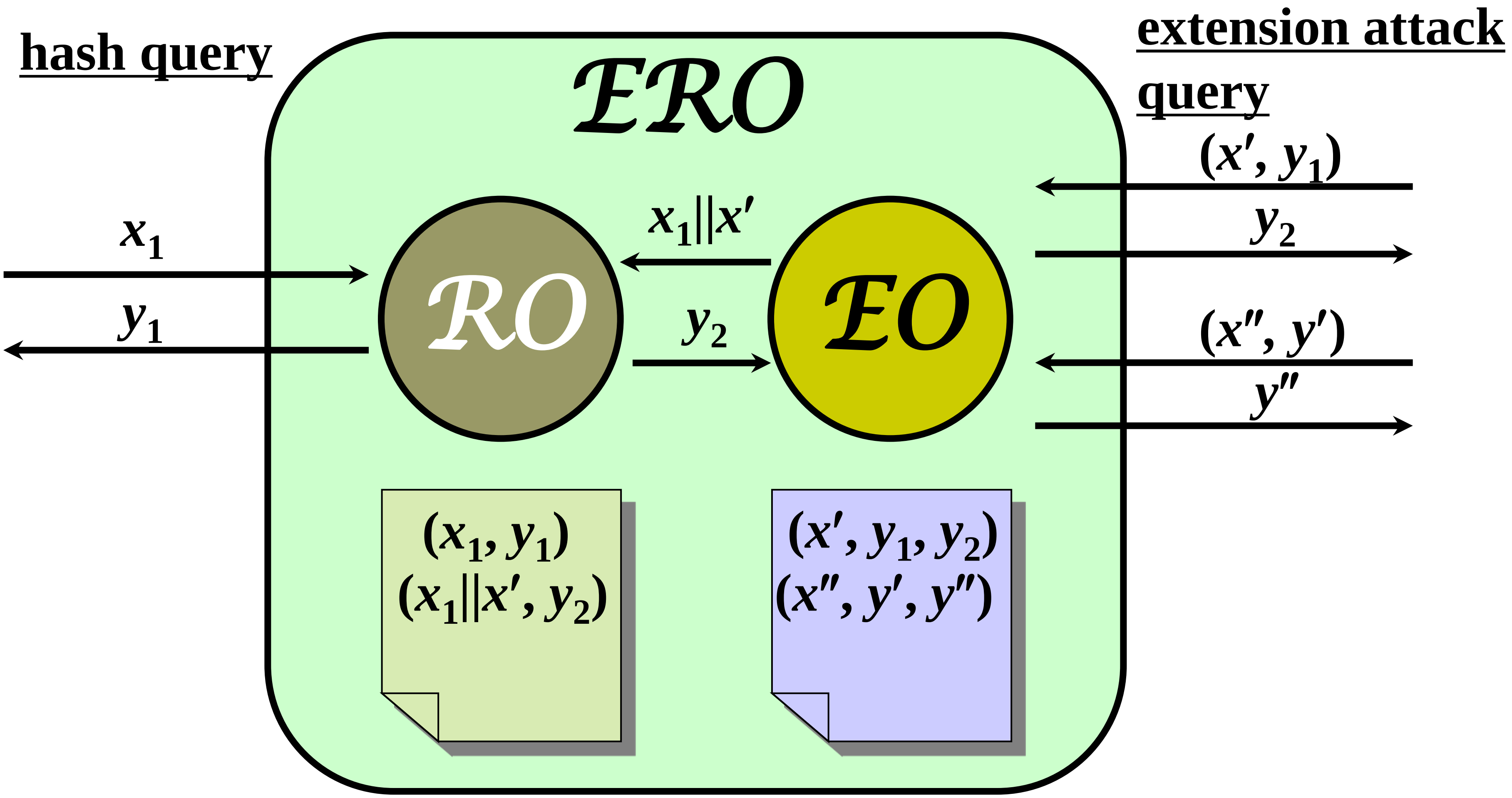


TRO--->LRO

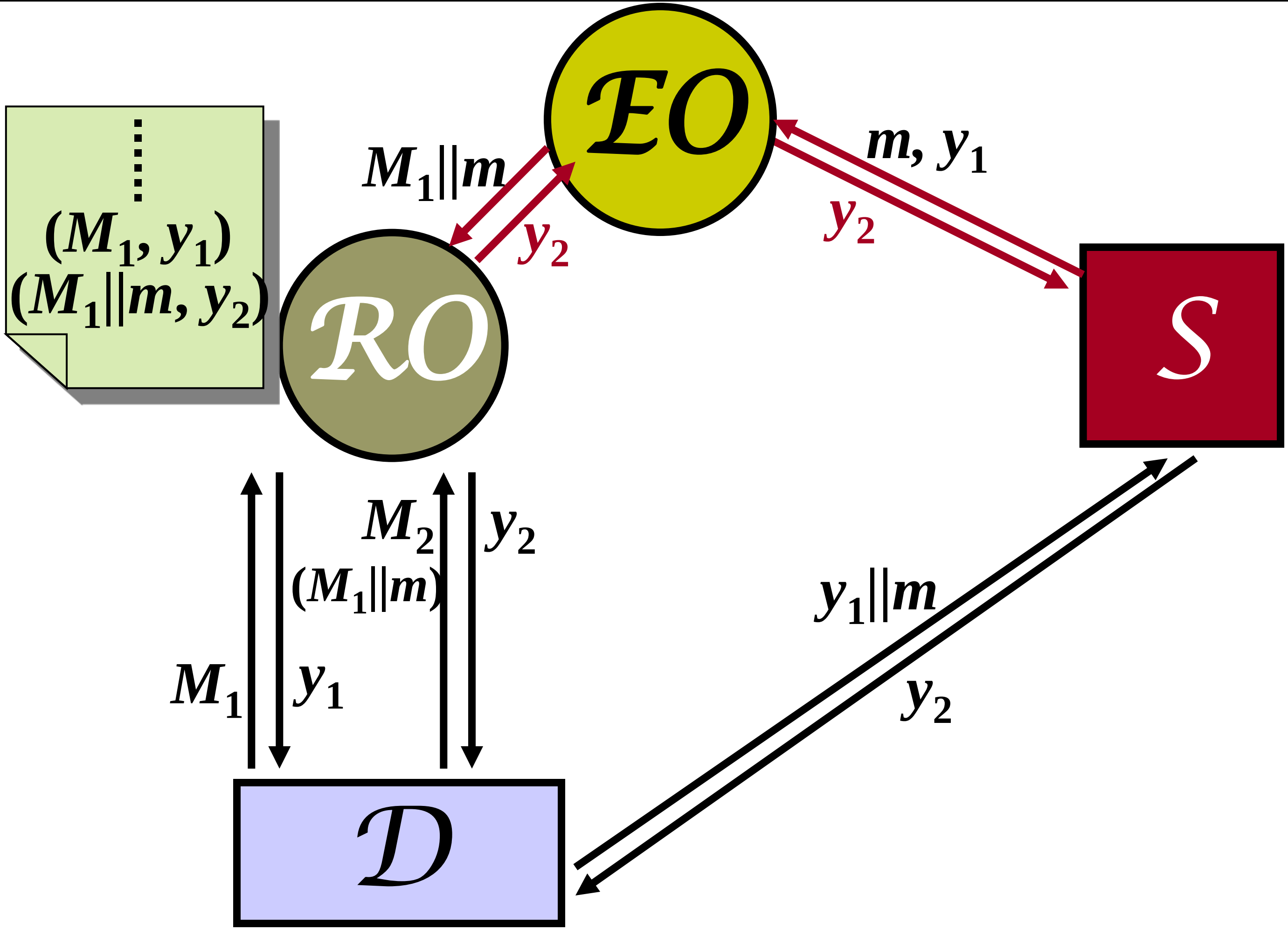
RSA-KEM



Extension Attack Simulatable Random Oracle (ERO)



Intuition of MD ⊏ ERO



Cryptosystems in ERO

- **Secure**: RSA-KEM, OAEP, FDH, …
  - **RSA-KEM** is insecure in TRO and LRO model.
- **Insecure**: Secret-prefix MAC,…
  - LEA breaks EF-CMA of Secret-prefix MAC in MD mode.

Other Concerns

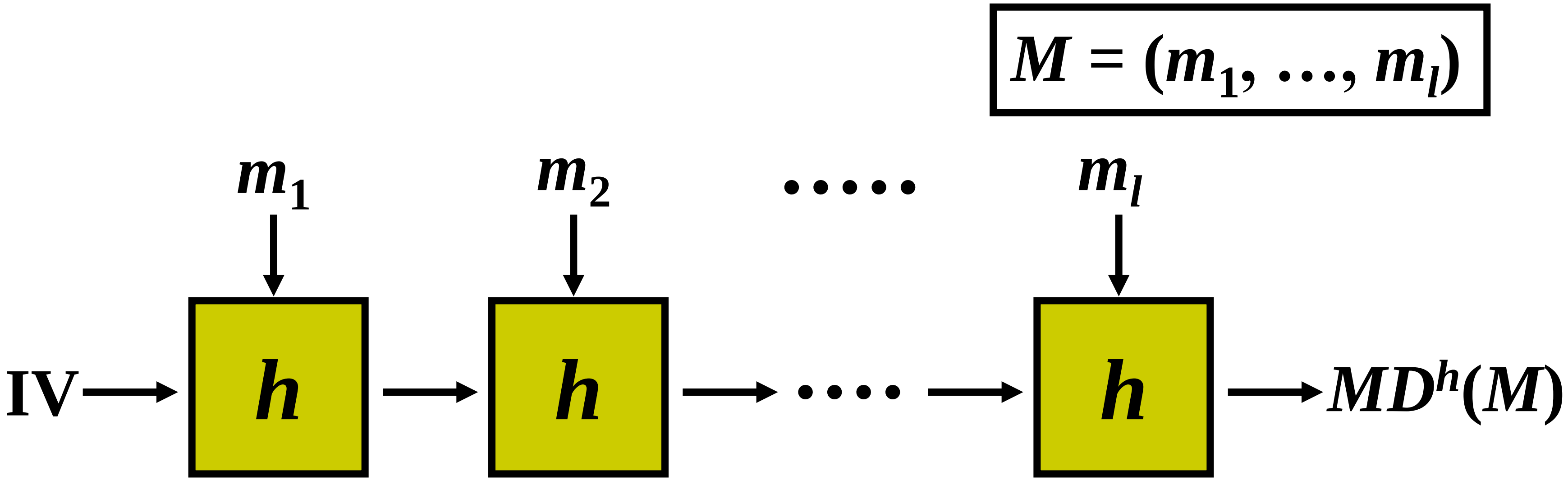
- **Compression function mode:**

  block-cipher-based

- **Range extension:**

  Key derivation function (KDF)

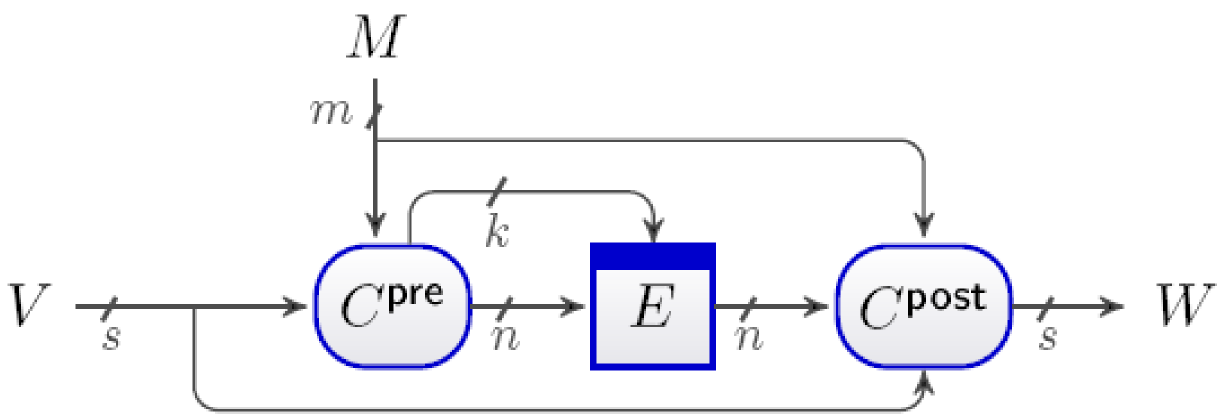
Block-cipher-based MD Mode



Practical *h*: block-cipher based

Revisit cryptosystems in MD based on an ideal block cipher

SCF: Stam's compression function



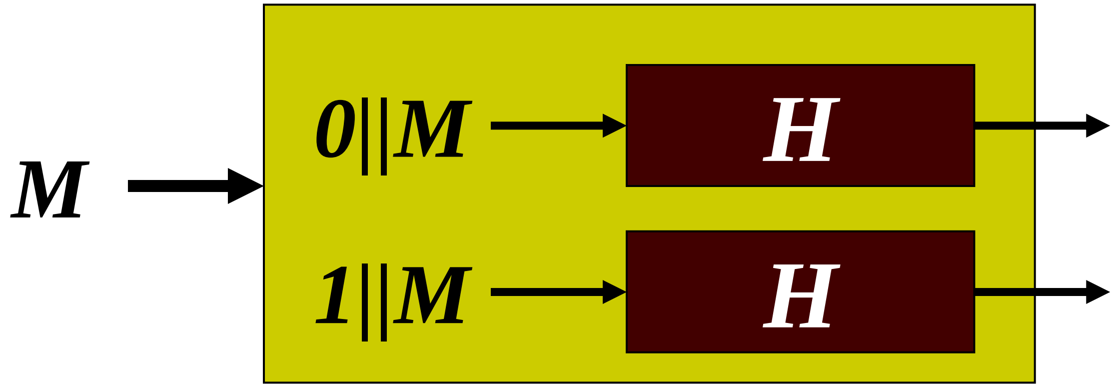
- $C^{pre}(\cdot)$ and $C^{post}(\cdot)$ are public and deterministic functions.
- $E(\cdot,\cdot)$ is an ideal cipher.

Stam, "Blockcipher-Based Hashing Revisited", FSE2009

KDF

- Digests of stand-alone hash function are short.
  - RSA-FDH: at least 1024 bits.
  - SHA-2: at most 512 bits
- Parallel mode

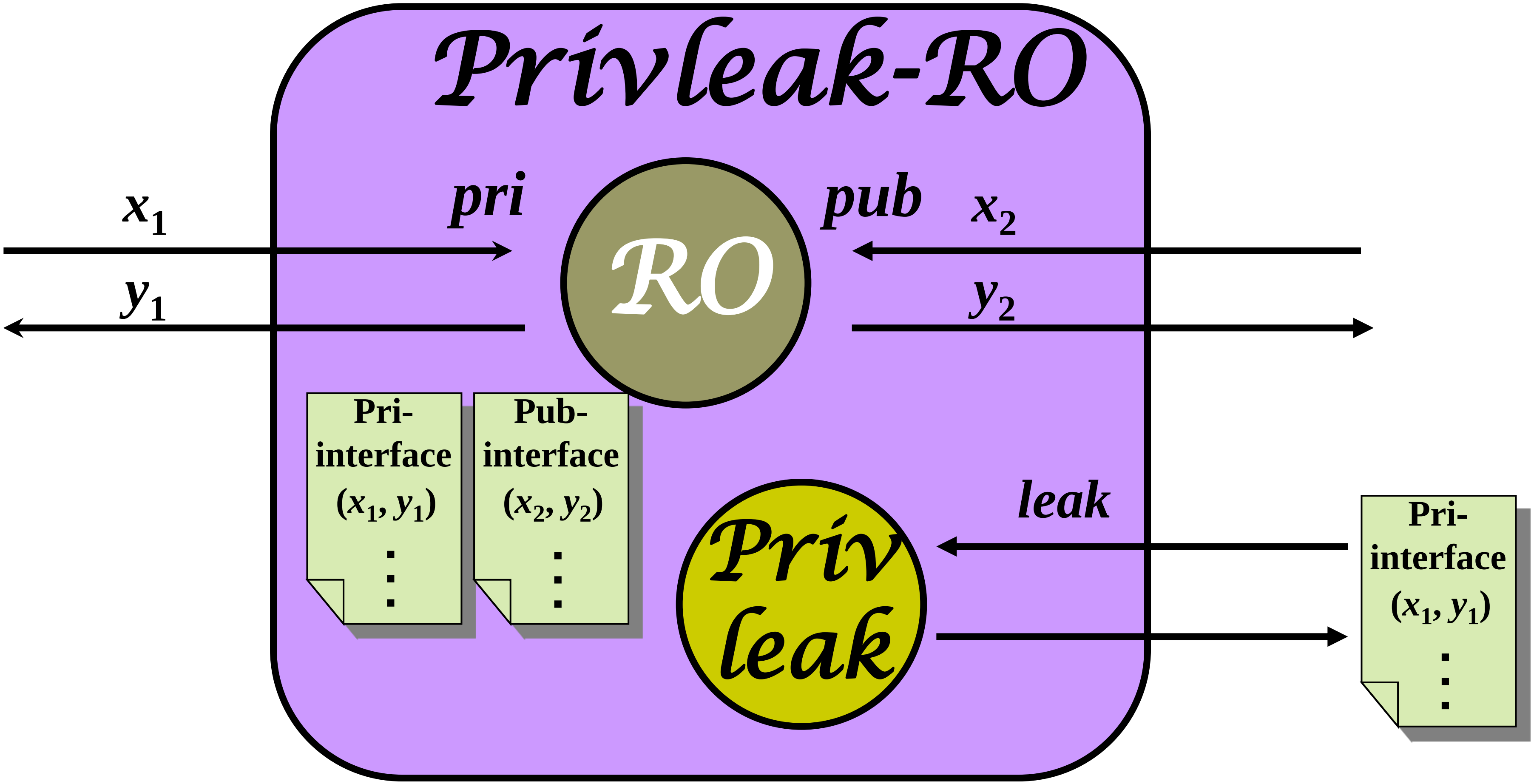
Example:



Cryptosystems in KDF-MD

- KDH, PSS, Fiat-Shamir, OAEP, RSA-KEM, PSEC-KEM, etc are **secure** in
  - KDF-MD based on FILRO
  - KDF-MD-SCFII (block-cipher-based).

Privleak-RO



Privleak-RO
x_1
y_1
pri
RO
pub
x_2
y_2
Pri-interface (x_1, y_1) ⋮
Pub-interface (x_2, y_2) ⋮
leak
Priv leak
Pri-interface (x_1, y_1) ⋮

Reason (brief)

- KDF: parallel mode
  - On a query to one branch, simulator has to simulate all the other branches simultaneously.
  - Difference of hash lists will be used to distinguish KDF-MD from LRO!!!

Outline

- Background
- Motivation
- Leaking Random Oracles
- **Conclusion**

Conclusion

- Merkle-Damgård mode is able to guarantee the security of practical cryptosystems including FDH，OAEP, RSA-KEM etc.

MD mode is still alive!!!

Thank you!