National Institute of Advanced Industrial Science and Technology
AIST

情報技術研究部門
Information Technology Research Institute

Black-Box Separations of Hash-and-Sign Signatures in the Non-Programmable Random Oracle Model

Zongyang Zhang, Yu Chen, *Sherman S. M. Chow*,
Goichiro Hanaoka, Zhenfu Cao, Yunlei Zhao

中國科學院 CHINESE ACADEMY OF SCIENCES
香港中文大學 The Chinese University of Hong Kong
華東師範大學 EAST CHINA NORMAL UNIVERSITY
復旦大學 FUDAN UNIVERSITY

ProvSec 2015@金沢Kanazawa
November 26, 2015

National Institute of Advanced Industrial Science and Technology
AIST
情報技術研究部門
Information Technology Research Institute

Outline

- ❑ **Random Oracle Model**
- ❑ **Schnorr Signature**
- ❑ **Existing Results**
- ❑ **Malleable Hash-and–Sign Signature**
- ❑ **Applications**

National Institute of Advanced Industrial Science and Technology AIST

情報技術研究部門 Information Technology Research Institute

Outline

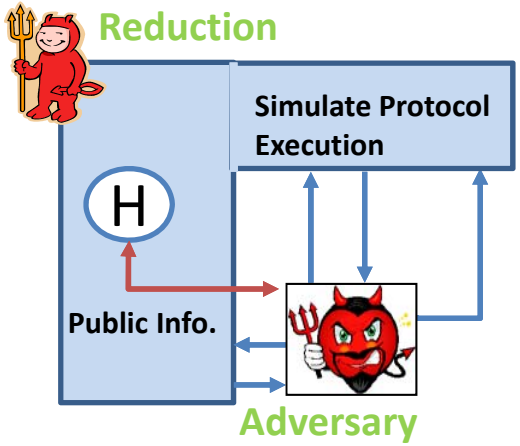
- **Random Oracle Model**
- Schnorr Signature
- Existing Results
- Malleable Hash-and–Sign Signature
- Applications

RO as a Tool for "Simple" Constructions

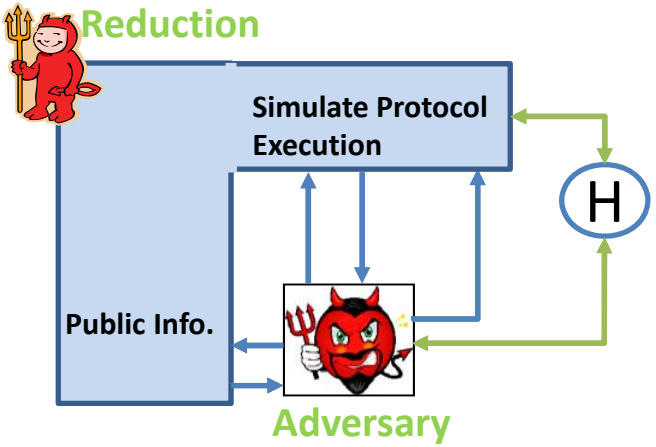
- Random Oracle : $R: \{0,1\}^* \rightarrow \{0,1\}^*$
  - each bit of $R(x)$ is random
  - the output is uniform and independent
- How to design protocols in ROM
  - Find a formal security definition for the problem in ROM
  - Devise an efficient protocol that solves the problem
  - Prove that the protocol satisfies the security definition
  - Instantiate RO with cryptographic hash functions, e.g, SHA3
- Applications
  - Optimal Asymmetric Encryption Padding (OAEP), BR'94
  - Fiat-Shamir Transformation, FS'86
  - Full-Domain Hash, BR'96
  - Fujisaki-Okamoto transformation, FO'99

Reductions in ROM

- Programmability: reduction can program the output 
- Observability: Reduction can see oracle queries
- The output is uniform and independent!



Fully-Programming Reduction



Non-Programming Reduction, e.g., OAEP

National Institute of Advanced Industrial Science and Technology AIST
情報技術研究部門 Information Technology Research Institute

Random Oracle Model

- Pros 
  - (Significantly) better than no proof at all
  - No real-world attacks on any natural schemes
  - Efficient, Simplified Construction
- Cons 
  - Hard to instantiate RO (maybe via UCE, BHK'13)
  - Observability might be unrealistic
  - Other subtleties, e.g., CGH'98, GK'03

Discard ROM vs. Use weaker ROM 

National Institute of Advanced Industrial Science and Technology AIST

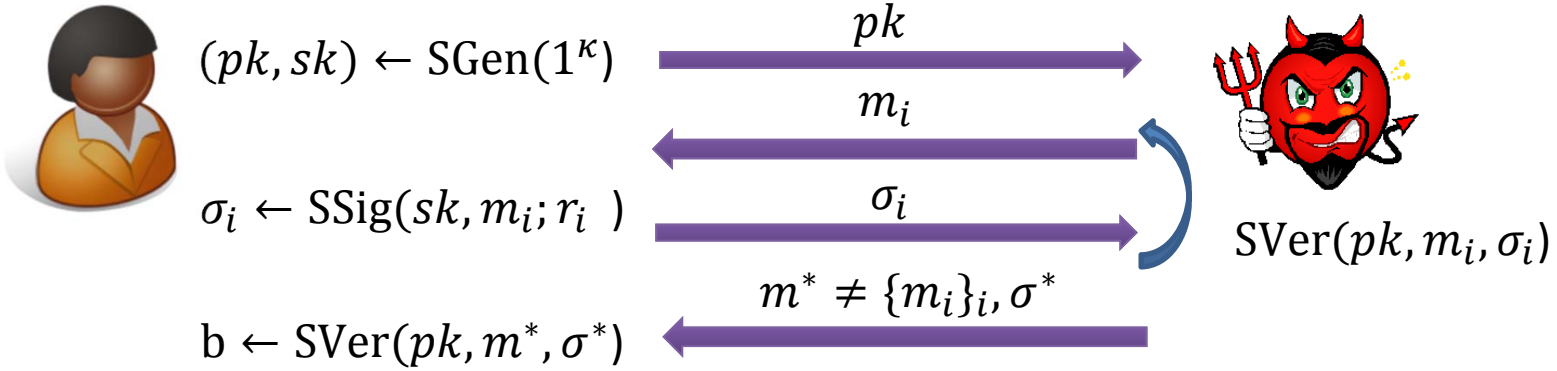
情報技術研究部門 Information Technology Research Institute

Outline

- ❑ Random Oracle Model
- ❑ **Schnorr Signature**
- ❑ Existing Results
- ❑ Malleable Hash-and–Sign Signature
- ❑ Applications

Signature Scheme

- Key Generation: $\mathrm{SGen}(1^\kappa)$: generate public/private key pair (pk, sk)
- Signature Generation: $\mathrm{SSig}(sk, m; r)$: output a signature σ.
- Verification: $\mathrm{SVer}(pk, m, \sigma)$: output 0/1



Existentially UnForgeable under adaptive Chosen-Message Attacks
iff for any adv., its success probability in the above game is neg.

Schnorr Signature

- $\mathbb{G}$: cyclic group of prime order p
- g : generator of $\mathbb{G}$
- H: $\{0,1\}^* \times \mathbb{G} \to \mathbb{Z}_p$: a random oracle

Key Generation: $\mathrm{SGen}(1^\kappa)$

$sk \leftarrow_R \mathbb{Z}_p$, $pk := g^{sk}$, output (pk, sk)

Signature Generation: $\mathrm{SSig}(sk, m; r)$

$R := g^r$

$c := H(R, m)$,

$y := r + sk \cdot c \bmod p$

output $\sigma := (c, y)$

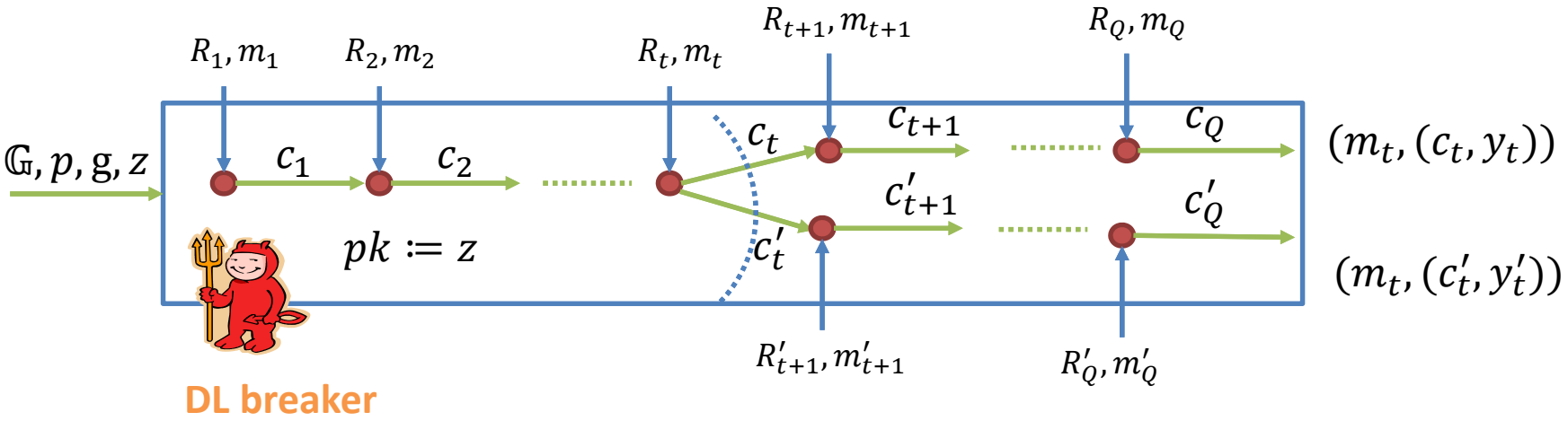
Verification: $\mathrm{SVer}(pk, m, \sigma)$

Parse σ as (c, y), check whether c $= H(g^y \cdot pk^{-c}, m)$

If so, output 1; otherwise, output 0.

Security Proof in FROM

- For a single message m,
- generate two valid signatures (c_t, y_t) and (c'_t, y'_t)
- where the corresponding $R_t = R'_t$,
- then one can compute $sk = (y_t - y'_t) \cdot (c_t - c'_t)^{-1}$

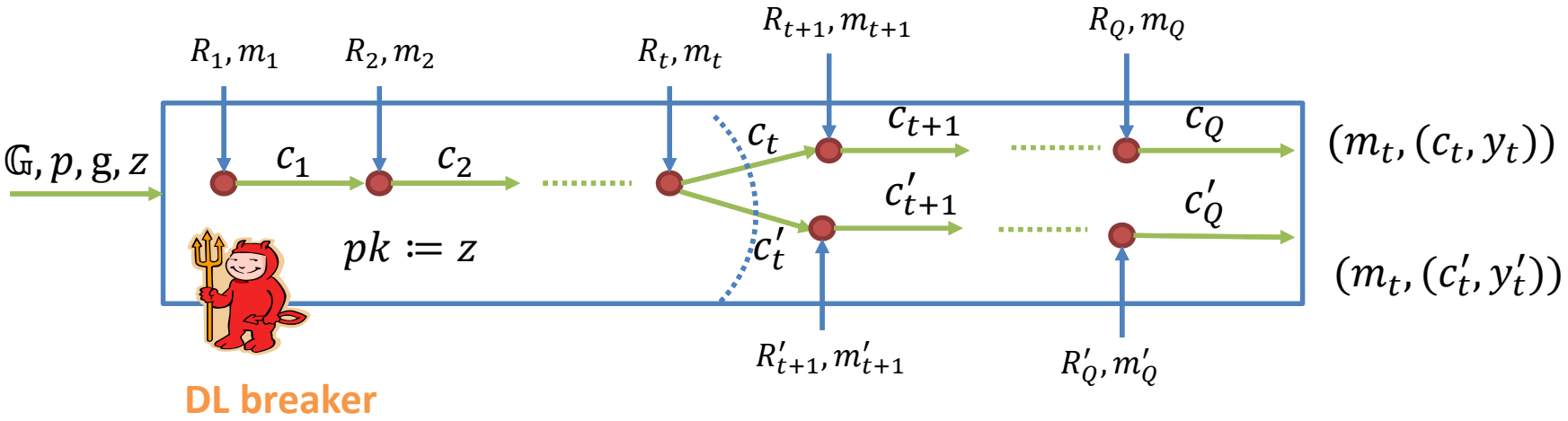


Signing Oracle without $sk = \log_g z$:

on input m, pick $c, y \leftarrow_R \mathbb{Z}_p$, set $c = H(g^y \cdot pk^{-c}, m)$

Forking Lemma

Let S be Schnorr's signature scheme with security parameter κ.
Let A be a PPT forger that breaks EUF-CMA with probability $\epsilon \geq 7Q/2^{\kappa}$ and time bound T. Here Q is the number of queries that A can ask to the RO.
Then there is another algorithm which produces two valid signatures (m, c_1, y_1) and (m, c_2, y_2) (while $R_1 = R_2$) in expected time $84480QT/\epsilon$.



Signing Oracle without $sk = \log_g z$:
on input m, pick $c, y \leftarrow_R \mathbb{Z}_p$, set $c = H(g^y \cdot pk^{-c}, m)$

National Institute of Advanced Industrial Science and Technology
AIST
情報技術研究部門
Information Technology Research Institute

Outline

- ❑ Random Oracle Model
- ❑ Schnorr Signature
- ❑ **Existing Results**
- ❑ Malleable Hash-and–Sign Signature
- ❑ Applications

National Institute of Advanced Industrial Science and Technology AIST
情報技術研究部門 Information Technology Research Institute

Security: Tightness

Related Work	Time to break DL	Note
Pointcheval & Stern Eurocrypt'96	$O(q_H/\epsilon)\cdot T$	PROM
Paillier & Vergnaud Asiacrypt'05	At least $O(\sqrt{q_H}/\epsilon)\cdot T$	Algebraic reduction OMDL assumption
Garg et al. Crypto'08	At least $O(q_H^{2/3}/\epsilon)\cdot T$	Algebraic reduction OMDL assumption
Seurin Eurocrypt'12	At least $O(f(\epsilon)\cdot q_H/\epsilon)\cdot T$	Algebraic reduction OMDL assumption
Fleischhacker, Jager, Schröder AC'14	No tight reduction to any natural comp. problem	Generic reduction

q_H: RO queries, ϵ: forgery's probability, T: time

PROM: Programmable Random Oracle Model

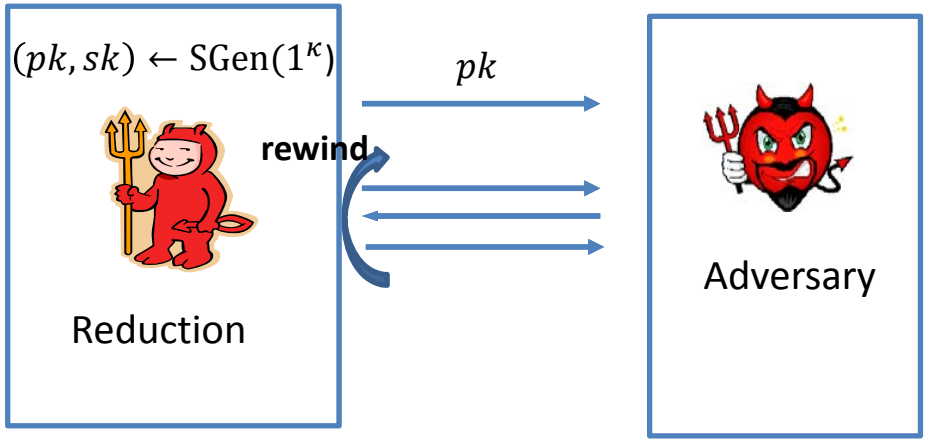
OMDL: One-More Discrete Logarithm

$f(\epsilon)$ is close to 1 as long as $\epsilon < 1$

Security: Programmability

- Secure, PROM, DL assumption (Pointcheval & Stern'96)
- Cannot be shown secure under DL assumption by algebraic reductions, standard model, One-more DL assumption, (Paillier & Vergnaud'05)
- Cannot be shown secure under DL assumption by single-instance reductions, NPROM, OMDL assumption

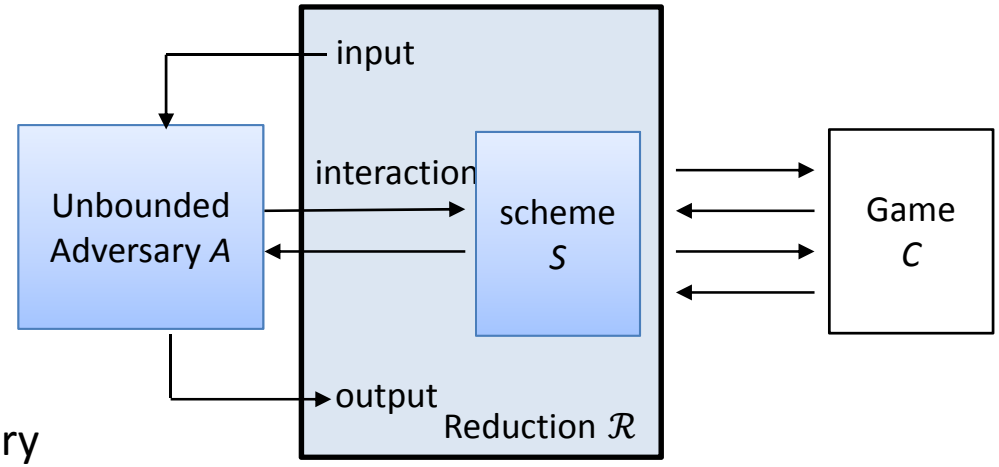
  (Fischlin & Fleischhacker'13 / **FF'13**)



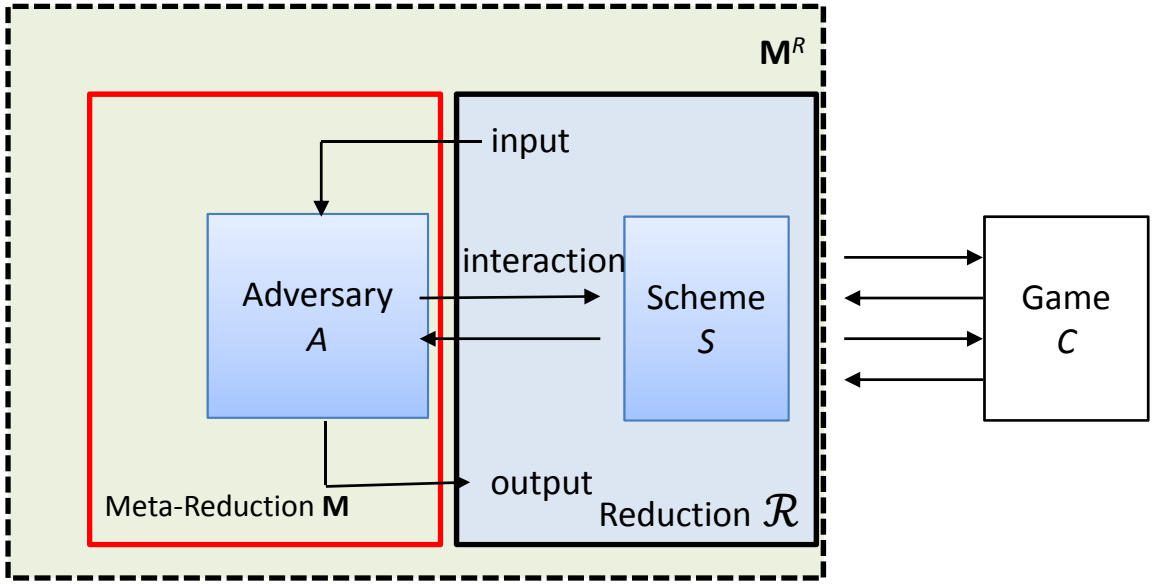
Single-instance reductions

Security in NPROM (FF'13): Meta-reduction

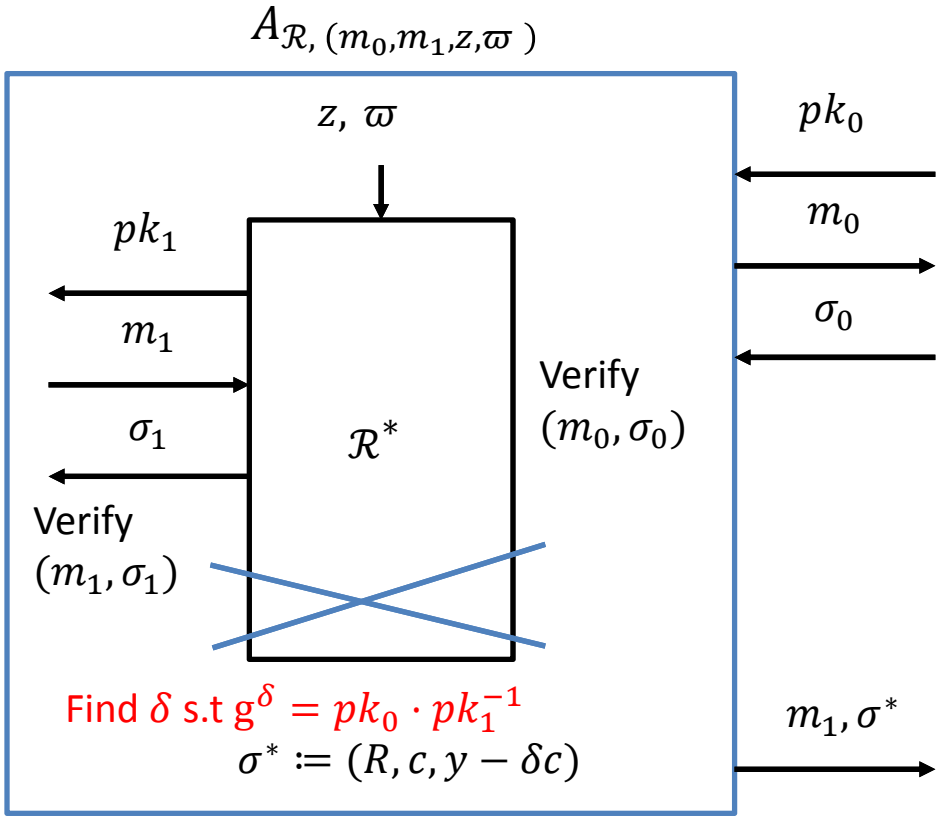
"Reduction against the Reduction"



1. Design an all-powerful adversary *A* that breaks the scheme.
2. Replace the adversary by the efficient meta-reduction.
3. Show the meta-reduction's behavior is sufficiently close to the one of *A*

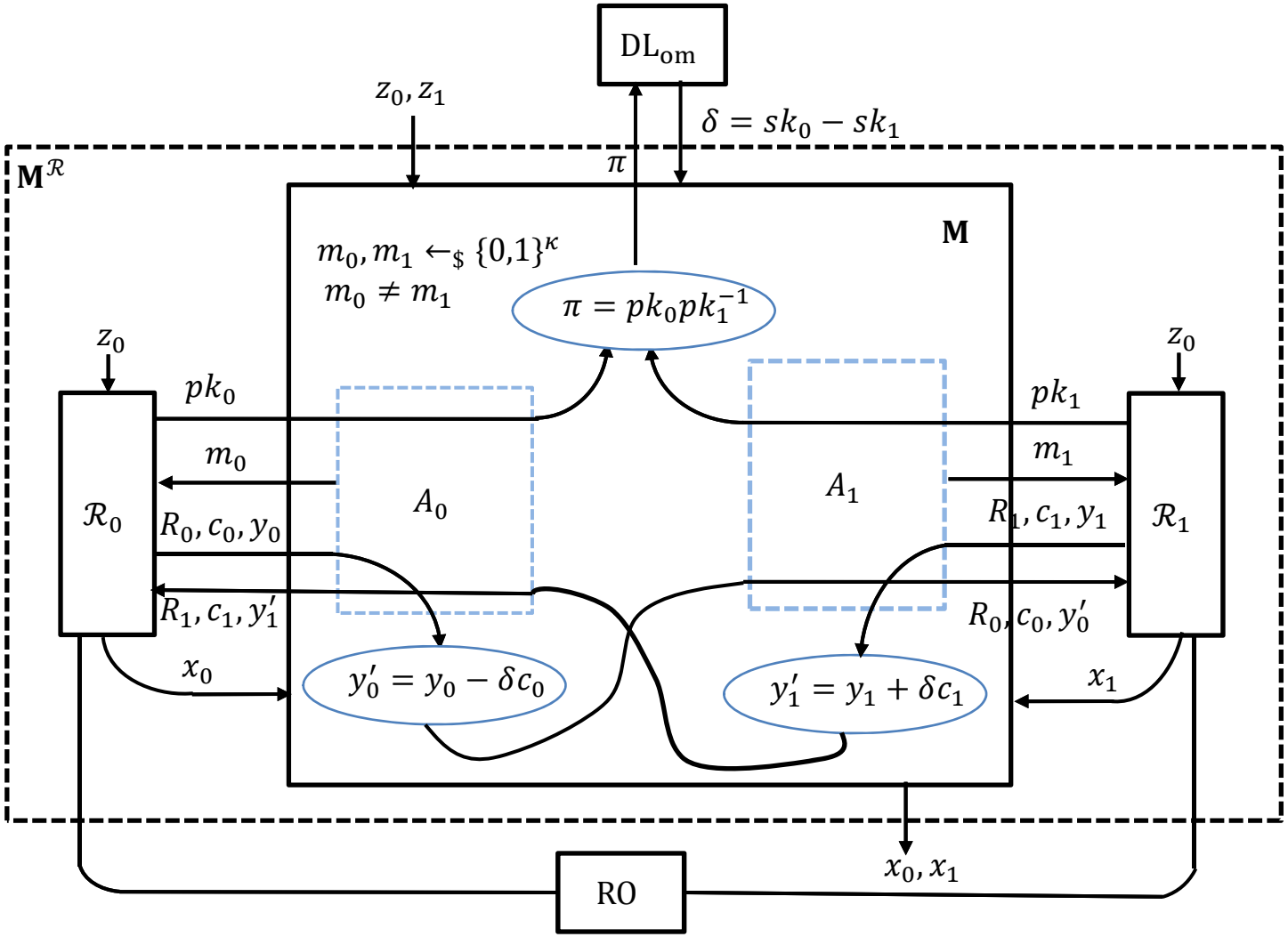


Unbounded Adversary



For each reduction $\mathcal{R}$,
the associated unbounded adversary $A_{\mathcal{R}}$
works by choosing two messages (m_0, m_1),
an instance z of the DL problem and
a random tape ϖ for R

Meta-Reduction



Why the technique works

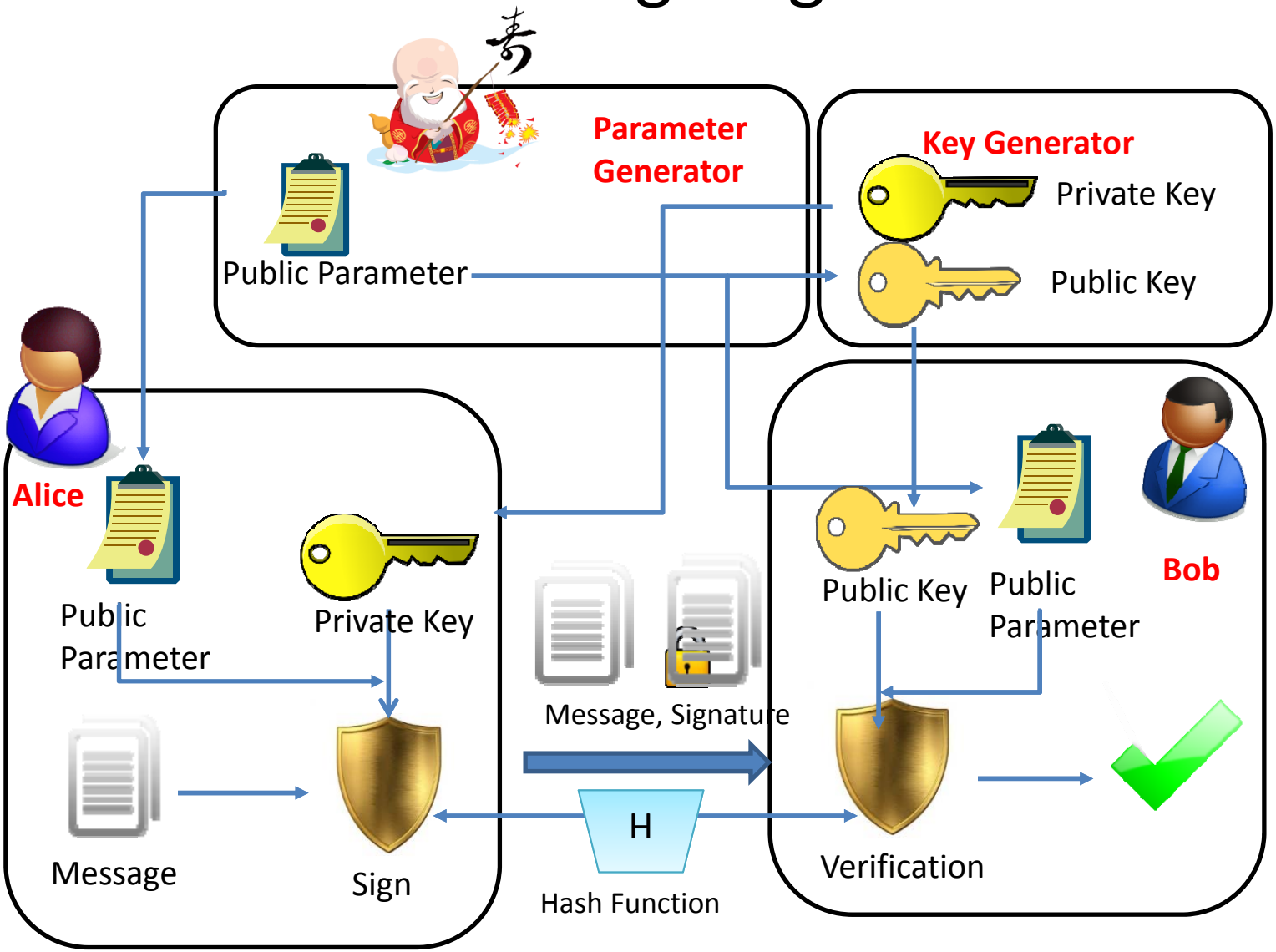
- Structure: the hash value does not contain RO(*pk*,*)
- Same global public parameters
  vs. Different global public parameters
- Single Instance vs. Multiple Instance
- Relationship with related-key attacks:
  - Meta-reduction mounts an RKA to reduction R_b by querying (ϕ_{1-b}, m_{1-b}) for a linear function $\phi_{1-b}(x) = x - sk_{1-b}$
- Limitations of the meta-reduction:
  - Interactive assumption (OMDL) is inherent

National Institute of Advanced Industrial Science and Technology
AIST
情報技術研究部門
Information Technology Research Institute

Outline

- ❑ Random Oracle Model
- ❑ Schnorr Signature
- ❑ Existing Results
- ❑ **Malleable Hash-and–Sign Signature**
- ❑ Applications

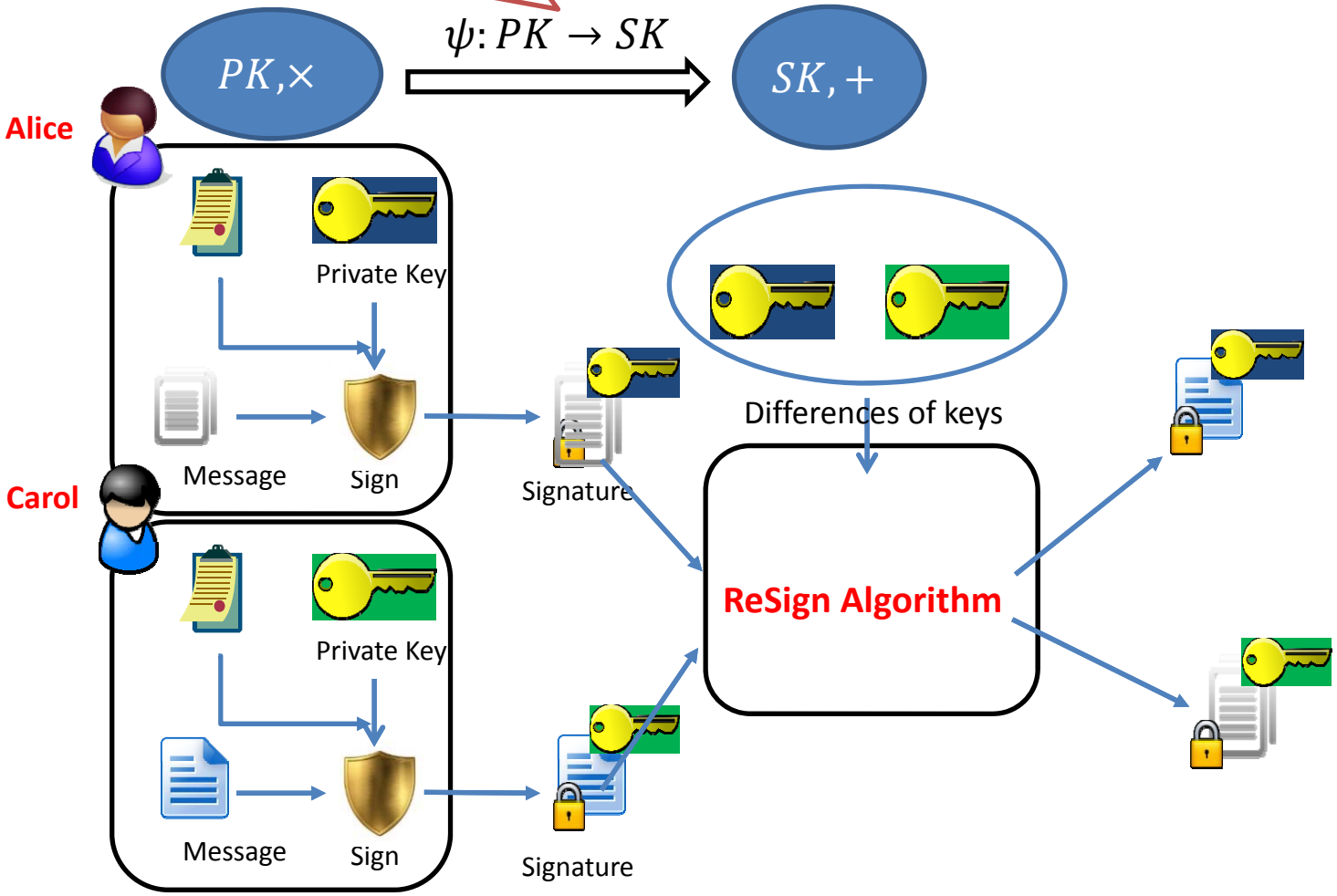
Hash-and-Sign Signature



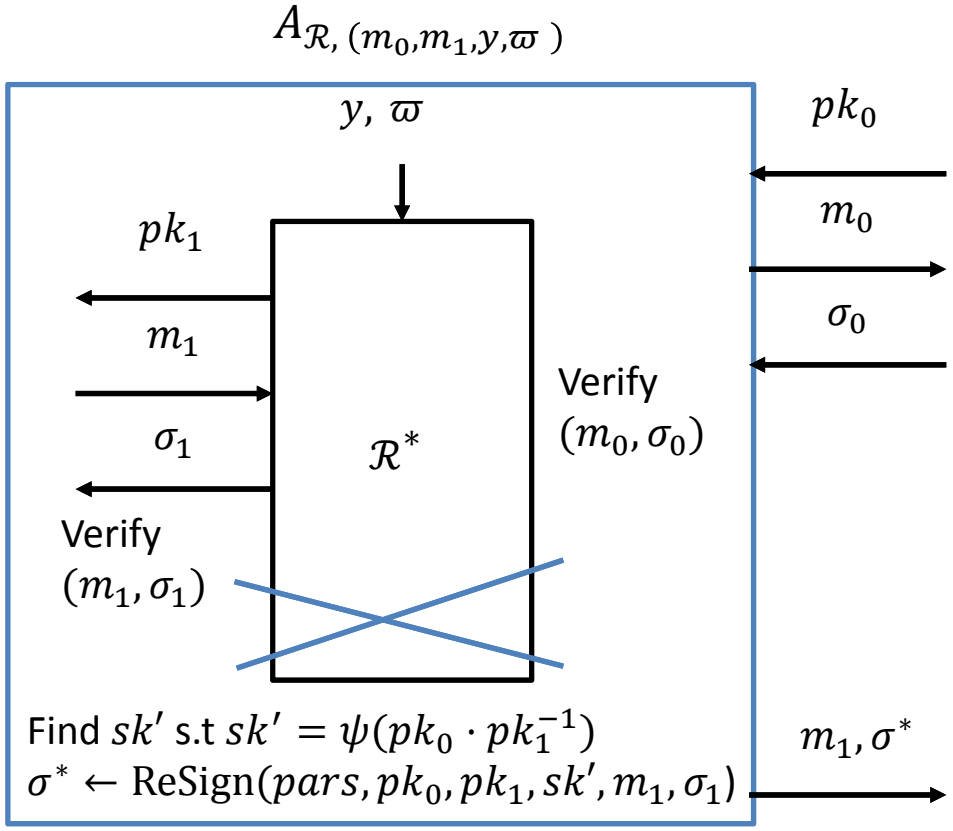
Malleable Hash-and Sign Signature

$$\psi(pk_1 \times pk_2) = \psi(pk_1) + \psi(pk_2)$$

Hard to compute except with an oracle that solves a hard non-interactive problem P_2



Unbounded Adversary

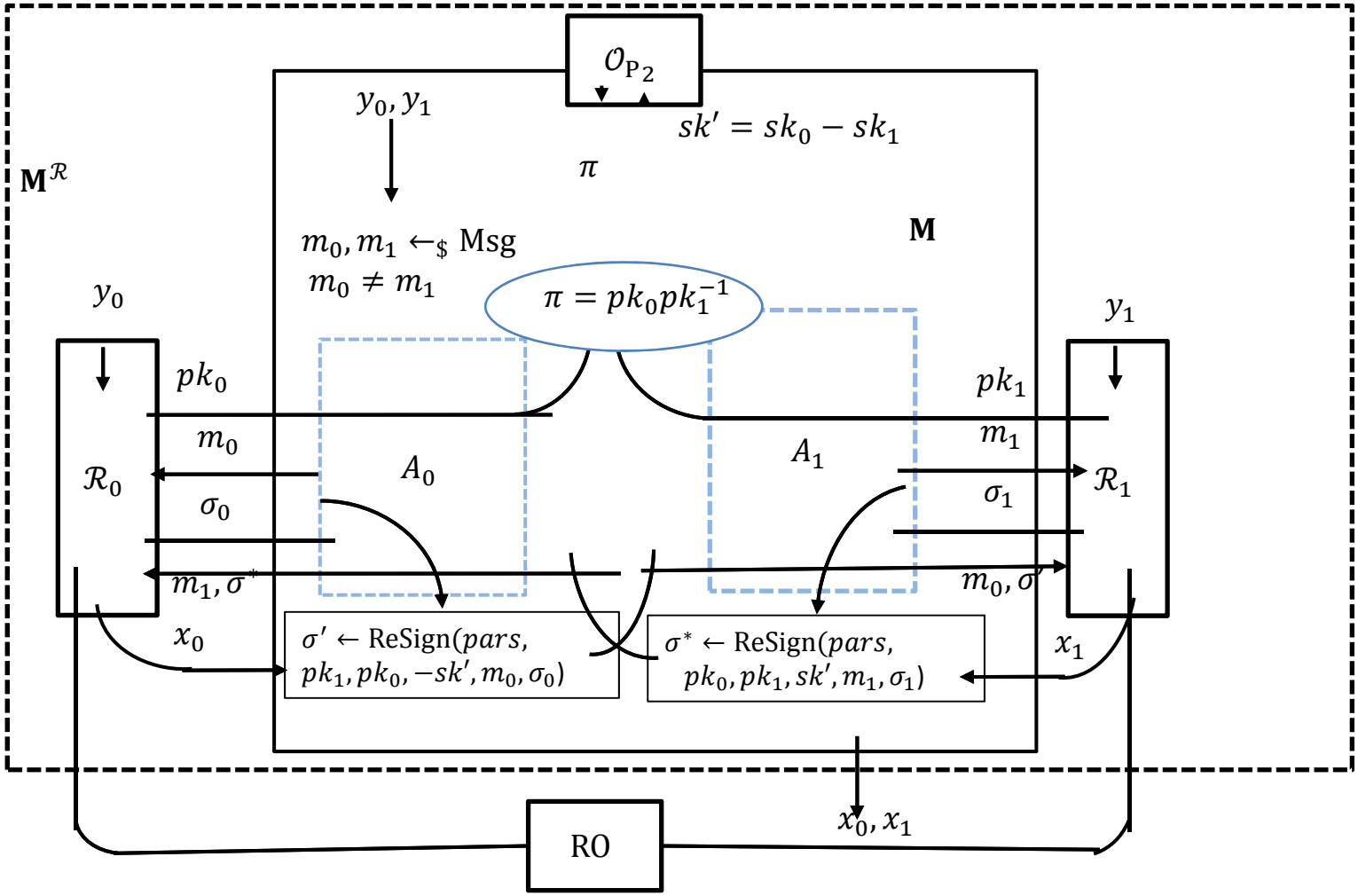


For each reduction $\mathcal{R}$,
the associated unbounded adversary
works by choosing two messages (m_0, m_1),
an instance y of the P_1 problem and
a random tape ϖ for R

National Institute of Advanced Industrial Science and Technology AIST

情報技術研究部門 Information Technology Research Institute

Meta-Reduction



National Institute of Advanced Industrial Science and Technology AIST

情報技術研究部門 Information Technology Research Institute

Outline

- ❑ Random Oracle Model
- ❑ Schnorr Signature
- ❑ Existing Results
- ❑ Malleable Hash-and–Sign Signature
- ❑ **Applications**

Applications (Signatures)

- Signature Schemes
  - Encompass the result of FF'13, Fiat-Shamir Signature
  - Restriction: does not work for RO(*pk*,*)
- Γ-signature, Yao & Zhao (IEEE TIFS'14)
  - EUF-CMA secure, DL, ROM
  - E.g., The DL-based Γ-signature cannot be proven equivalent to the DL in NPROM assuming single-instance BB reductions and OMDL

National Institute of Advanced Industrial Science and Technology AIST

情報技術研究部門 Information Technology Research Institute

Applications (Identity-Based Crypto.)

- Identity-Based Encryption
  - Boneh & Franklin IBE (BF'01, BF'03, Galindo'05)
  - BasicIdent / FullIdent, IND-CPA/IND-CCA, ROM, CBDH
  - BF-IBE scheme cannot be proven equivalent to the CBDH in NPROM assuming single-instance BB reductions and one-more CBDH
- SOK Identity-based non-interactive key exchange
  - fully adaptive secure, ROM, CBDH
  - SOK IB-NIKE cannot be proven equivalent to the CBDH in NPROM assuming single-instance BB reductions and one-more CBDH

National Institute of Advanced Industrial Science and Technology AIST
情報技術研究部門 Information Technology Research Institute

Summary

- Non-programmable random oracle model
- BB separation for malleable hash-and sign signature
- Many applications including IBE, signature, IB-NIKE