Weakened Random Oracle Models with Target Prefix

Masayuki Tezuka, Yusuke Yoshida, Keisuke Tanaka

Tokyo Institute of Technology

Version: 2020/12/23

SecITC 2018 Full presentation slide

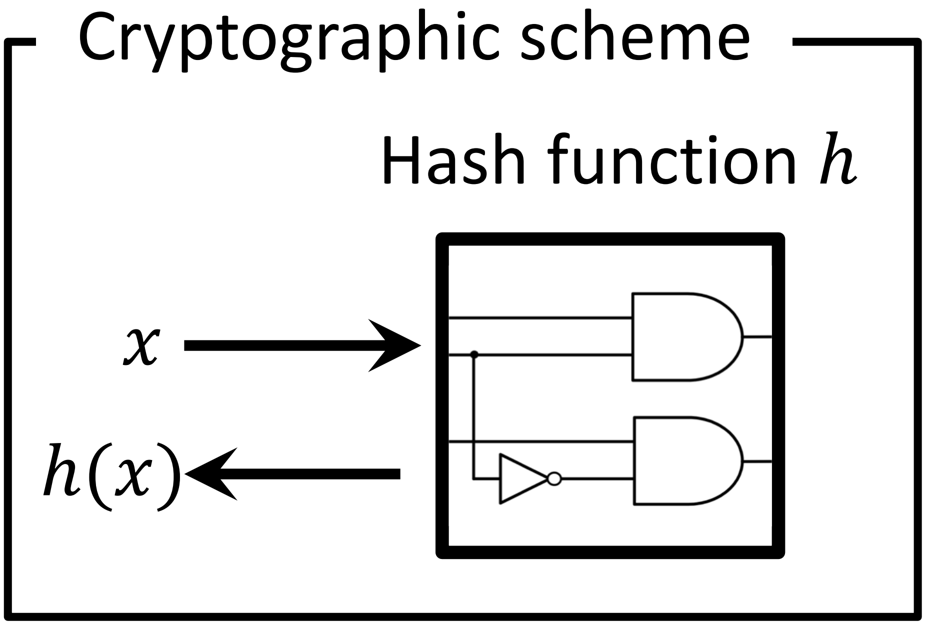
Our results

We extend three weakened random oracle models to capture the chosen prefix attack and its variants.

We analyze the security of signature schemes under the chosen prefix collision attack its variants for a hash function.

Background

A hash function is used to construct cryptographic schemes.



Cryptographic scheme

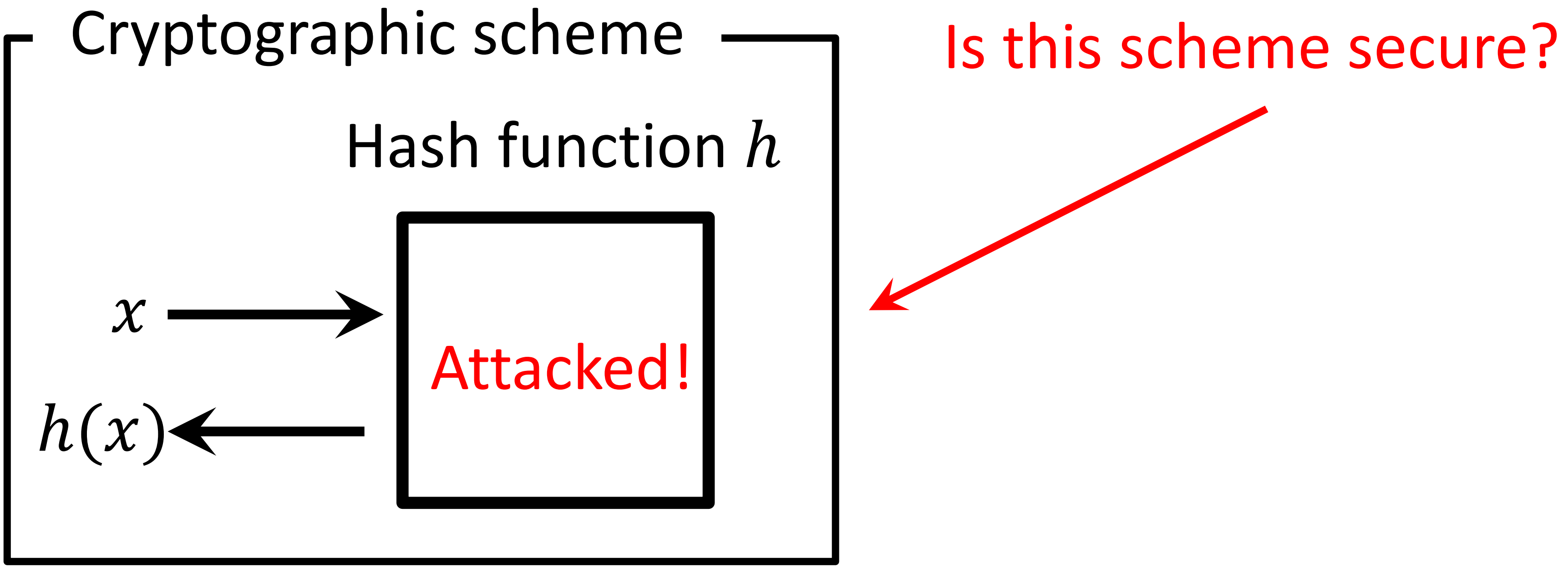
Hash function h

x

$h(x)$

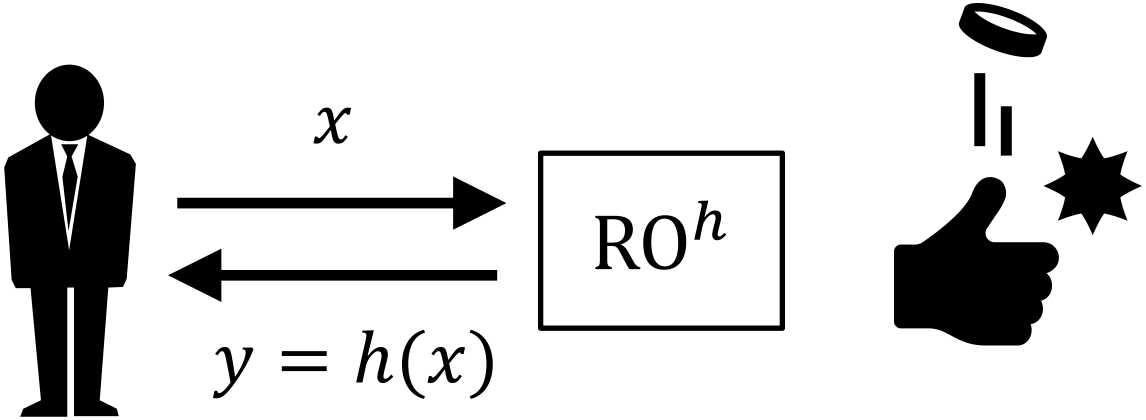
Background

A hash function is used to construct cryptographic schemes.



Random oracle model (ROM)
Bellare, Rogaway (CCS' 93)

Random oracle model (ROM)



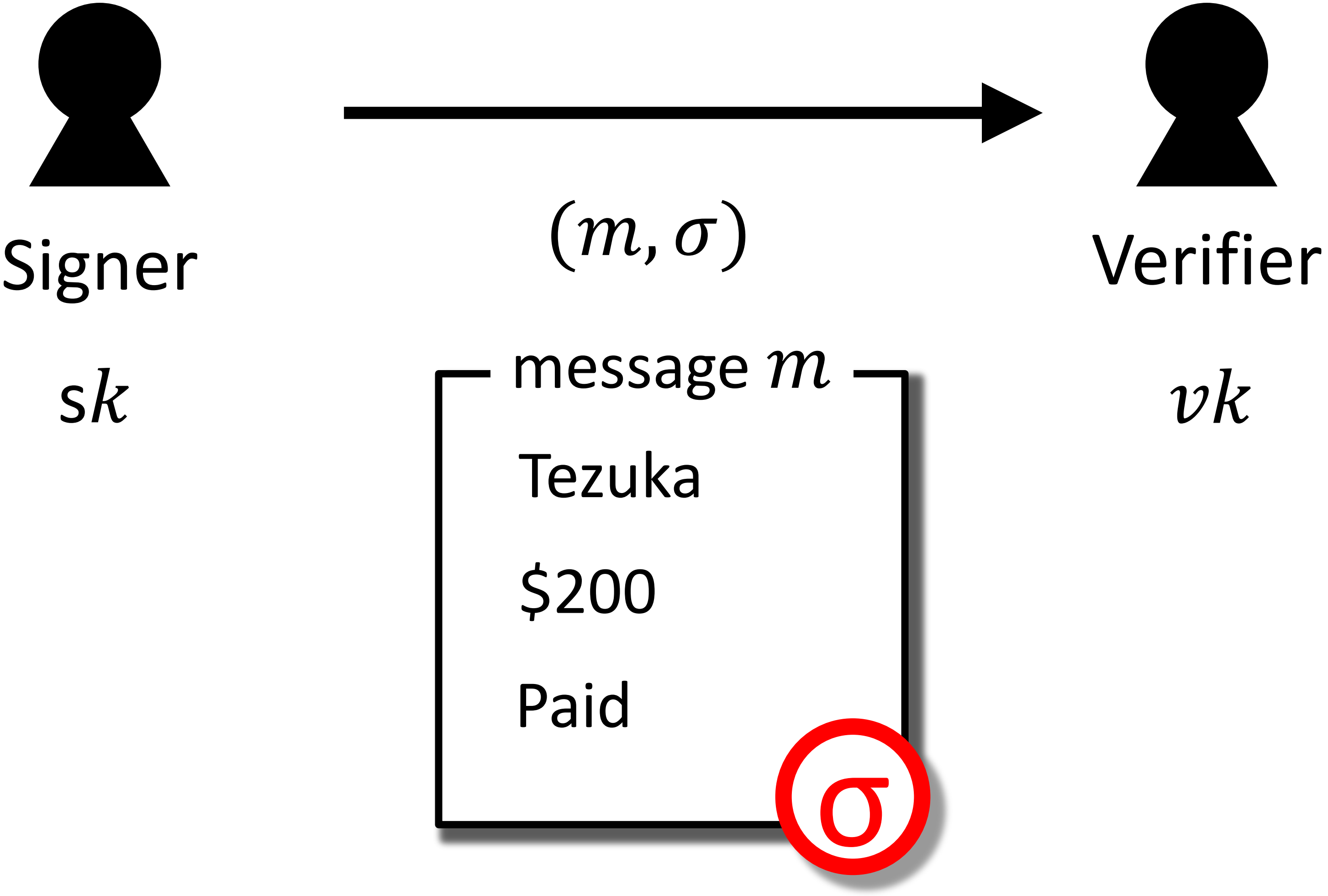
x

RO^h

$y = h(x)$

When we implement a cryptographic scheme, the random oracle is replaced by a hash function.

Digital signature scheme



Signer

sk

(m, σ)

Verifier

vk

message m

Tezuka

$200

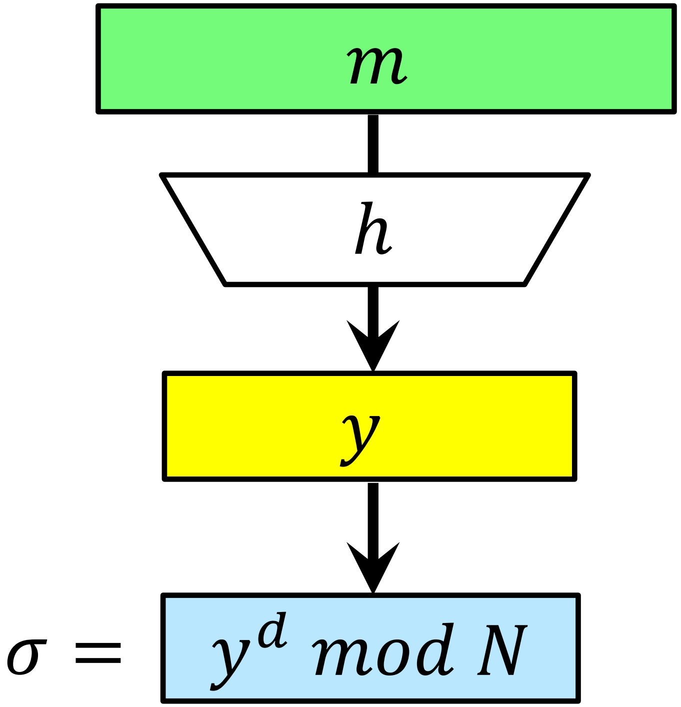
Paid

σ

RSA–FDH (Digital signature scheme)

RSA-FDH

Sign$(sk = d, m)$

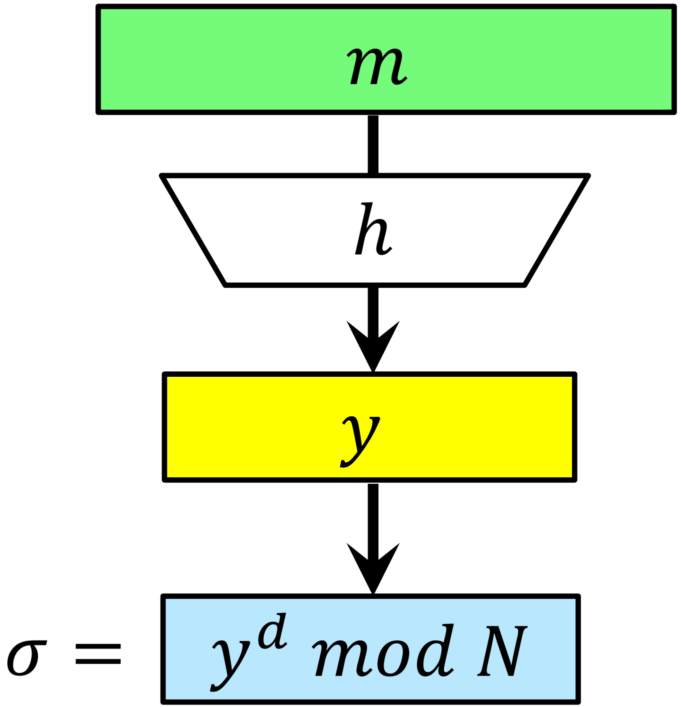


RSA-FDH is EUF-CMA secure in ROM.

RSA–FDH (Digital signature scheme)

RSA-FDH

Sign$(sk = d, m)$



RSA-FDH is EUF-CMA secure in ROM.

signature (m, σ)

and

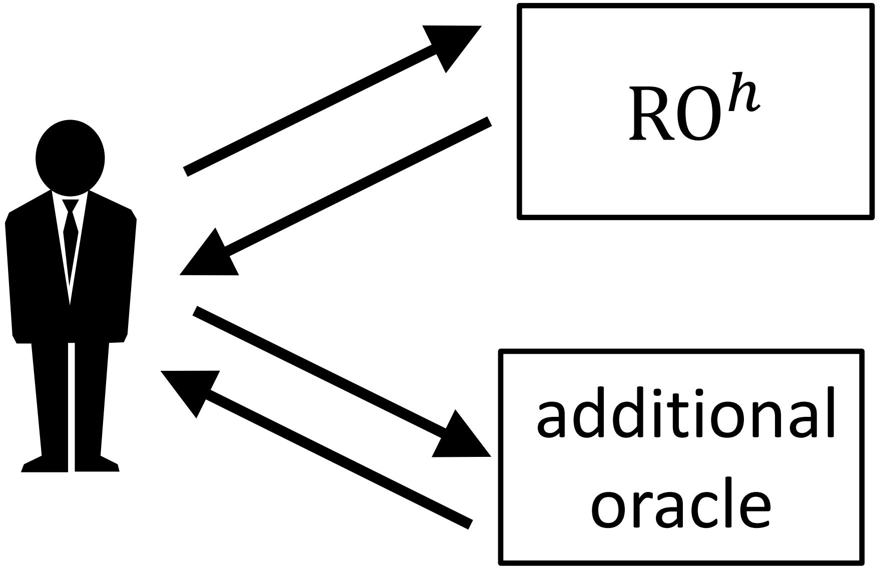
collision (m, m') satisfying $h(m) = h(m')$

⬇

valid forgery (m', σ)

Weakened random oracle model (WROM)
Liskov (SAC’ 06)

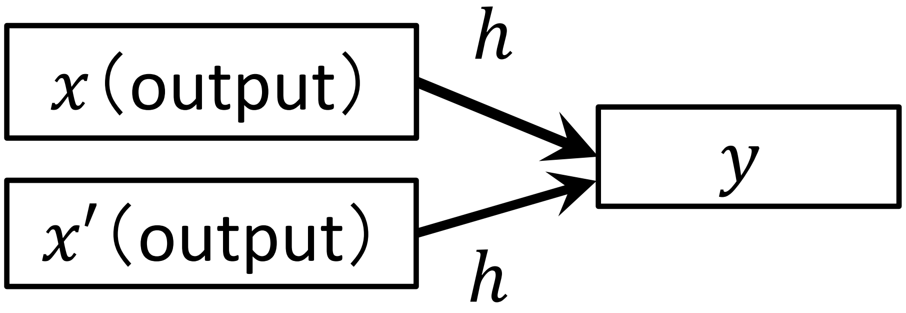
Weakened random oracle model (WROM)



In WROMs, each model has the additional oracle that breaks the specific property of a hash function.

Properties of a hash function h

Collision resistance



x (output)

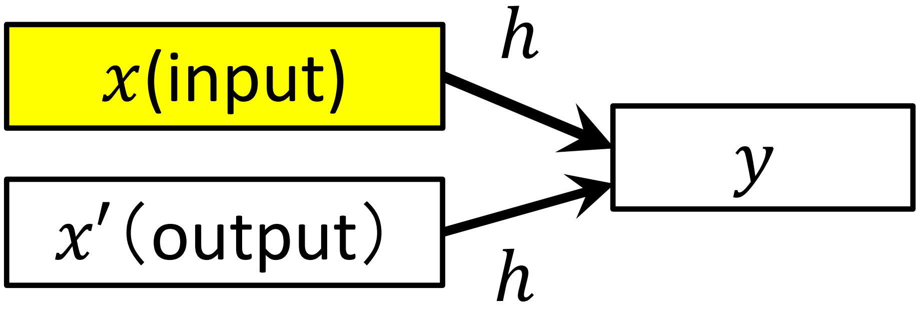
x' (output)

h

h

y

Second preimage resistance



x(input)

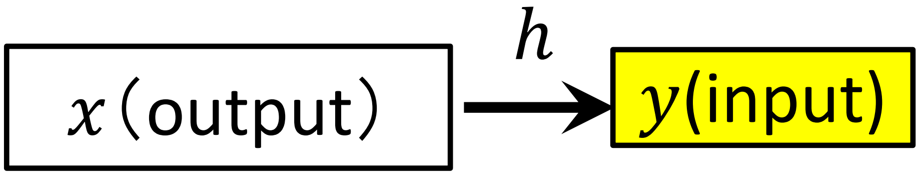
x' (output)

h

h

y

First preimage resistance



x (output)

h

y(input)

Additional oracles in WROMs
Numayama, Isshiki, Tanaka (PKC’08)

Additional oracles in WROMs
Numayama, Isshiki, Tanaka (PKC’08)

CT-ROM

CT()

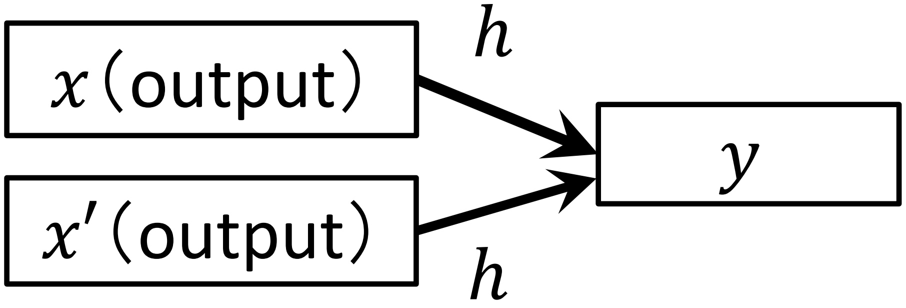
It uniformly outputs a collision (x, x').

Additional oracles in WROMs
Numayama, Isshiki, Tanaka (PKC’08)

CT-ROM

CT()

It uniformly outputs a collision (x, x').

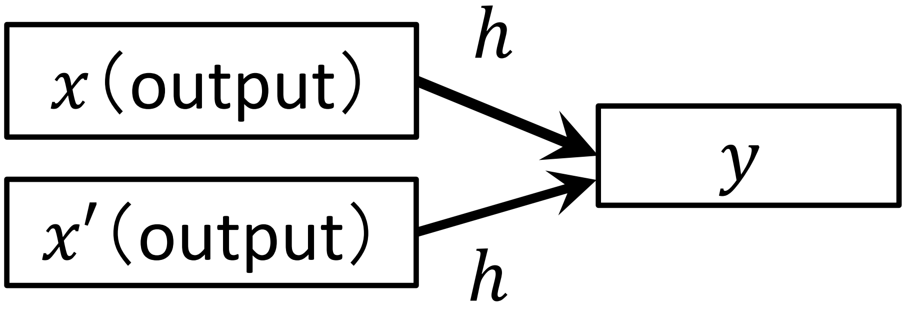


Additional oracles in WROMs
Numayama, Isshiki, Tanaka (PKC’08)

CT-ROM

CT()

It uniformly outputs a collision (x, x').



x (output)

x' (output)

h

h

y

SPT-ROM

SPT(x)

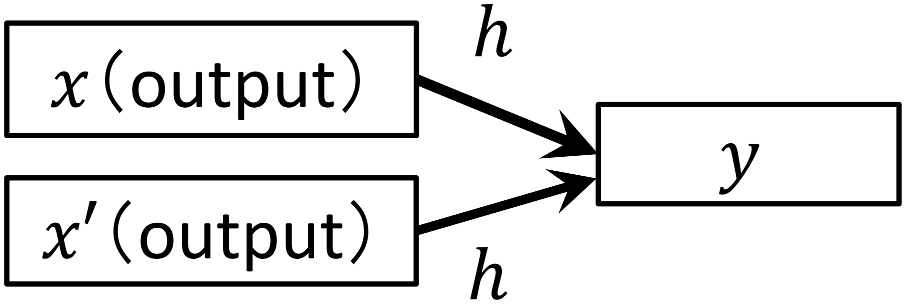
It uniformly outputs x' such that $h(x) = h(x')$.

Additional oracles in WROMs
Numayama, Isshiki, Tanaka (PKC’ 08)

CT-ROM

CT()

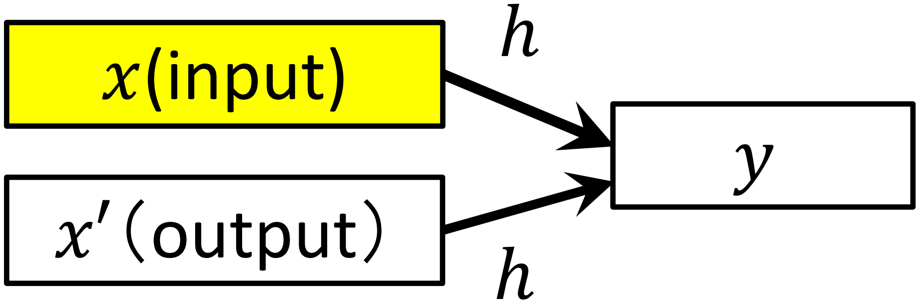
It uniformly outputs a collision (x, x').



SPT-ROM

SPT(x)

It uniformly outputs x' such that $h(x) = h(x')$.

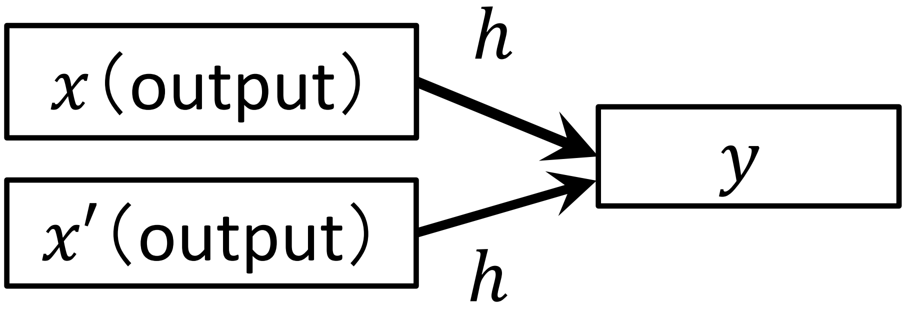


Additional oracles in WROMs
Numayama, Isshiki, Tanaka (PKC’08)

CT-ROM

CT()

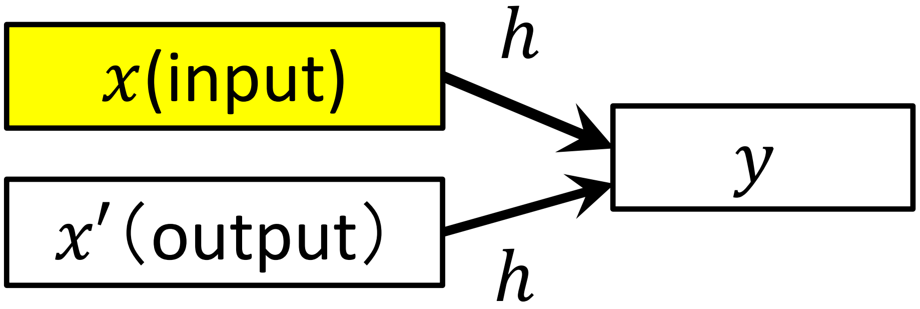
It uniformly outputs a collision (x, x').



SPT-ROM

SPT(x)

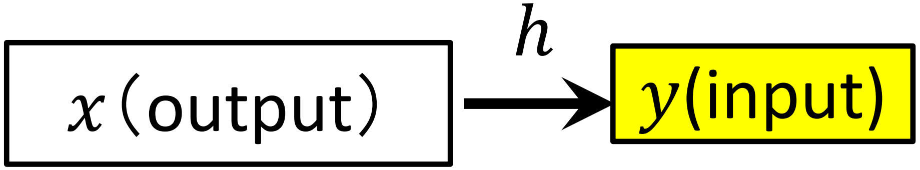
It uniformly outputs x' such that $h(x) = h(x')$.



FPT-ROM

FPT(y)

It uniformly outputs x such that $y = h(x)$.



EUF-CMA security of signature schemes in WROMs
Numayama, Isshiki, Tanaka (PKC' 08)

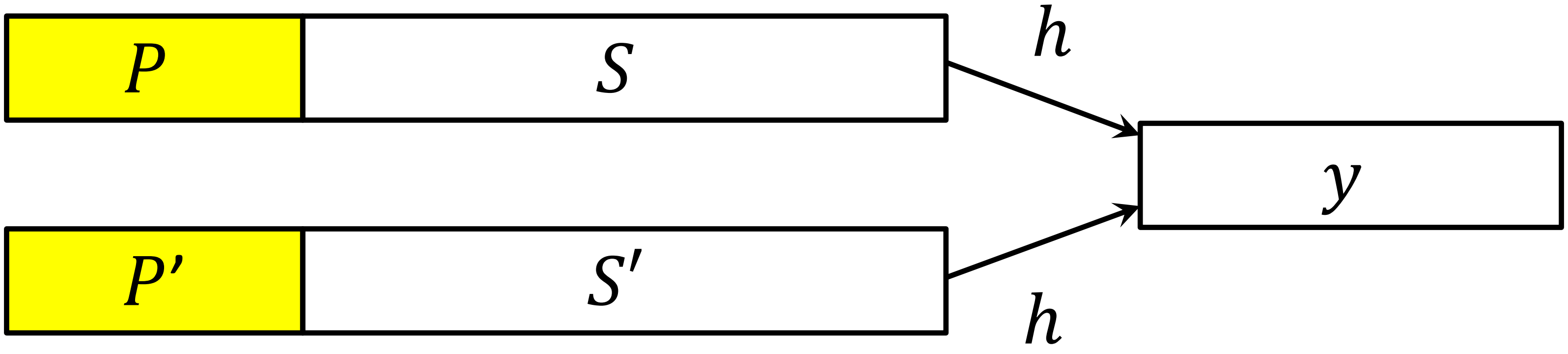
Models become weaker as it goes right.

	ROM	CT-ROM	SPT-ROM	FPT-ROM
RSA-FDH	✓	×	×	×
RSA-PFDH	✓	✓	×	×
RSA-PFDH^{+}	✓	✓	✓	×
RSA-PFDH$^{\oplus}$	✓	✓	✓	✓

The chosen prefix collision attack
Stevens, Lenstra, and de Weger (EUROCRYPT' 07)

The chosen prefix collision attack

The chosen prefix collision attack is used to attack against MD5.



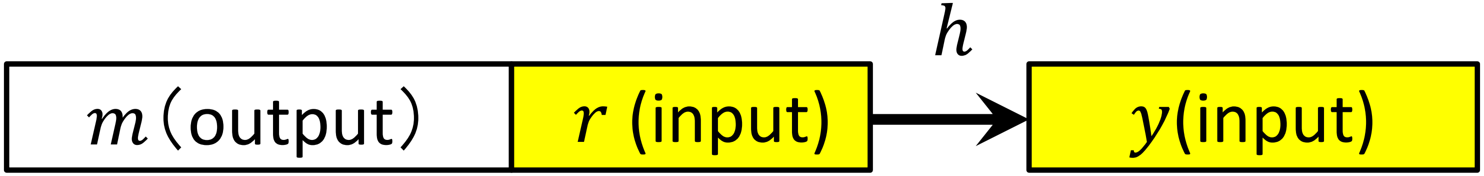
In this attack, an adversary decide a pair (P, P') of prefixes beforehand and find a collision$(P||S, P'||S')$.

Generalized FPT–ROM (GFPT–ROM)
Tan, Wong (ACISP’ 12)

GFPT-ROM

GFPT oracle

Given an input (y, r), it uniformly returns $x = m||r$ such that $h(m||r) = y$.

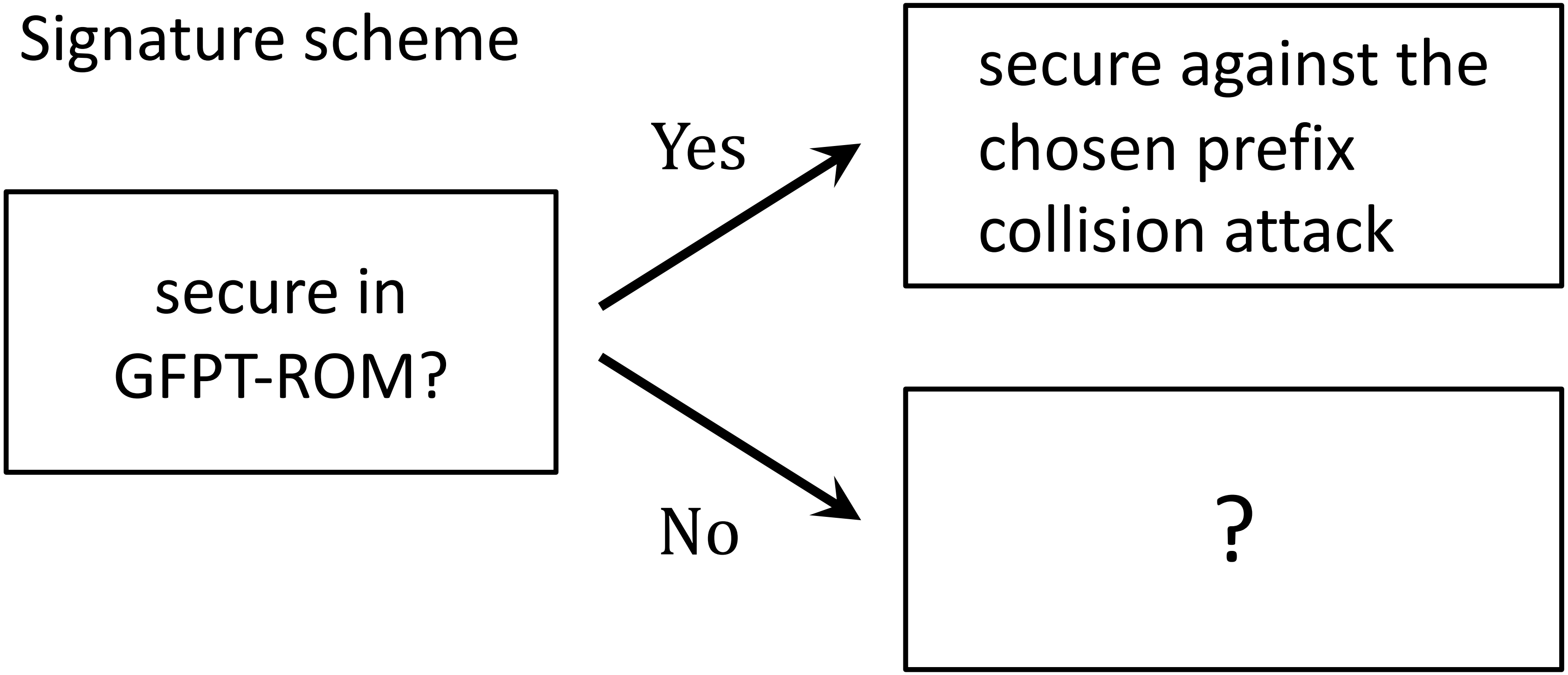


m (output) r (input) $\xrightarrow{h}$ y(input)

We can choose the part of the prefix for a preimage.

Generalized FPT-ROM (GFPT-ROM)
Tan, Wong (ACISP' 12)

Signature scheme



secure in GFPT-ROM?

Yes

secure against the chosen prefix collision attack

No

?

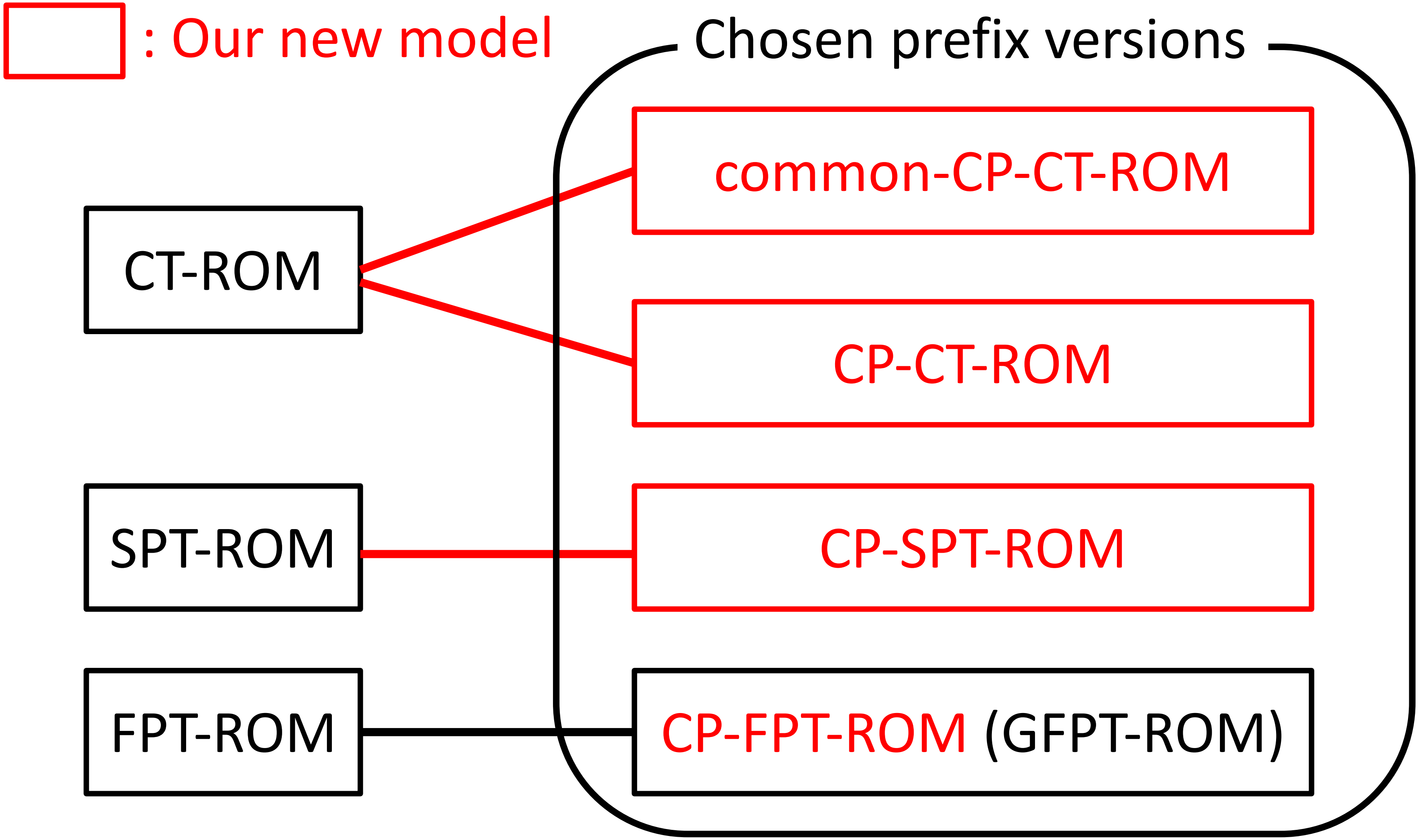
To analyze a security of signature schemes for the chosen prefix collision attack, we need new WROMs.

Our results

We extend three weakened random oracle models to capture the chosen prefix attack and its variants.

We analyze the security of signature schemes under the chosen prefix collision attack and its variants for a hash function.

Our results



□ : Our new model

Chosen prefix versions

CT-ROM

SPT-ROM

FPT-ROM

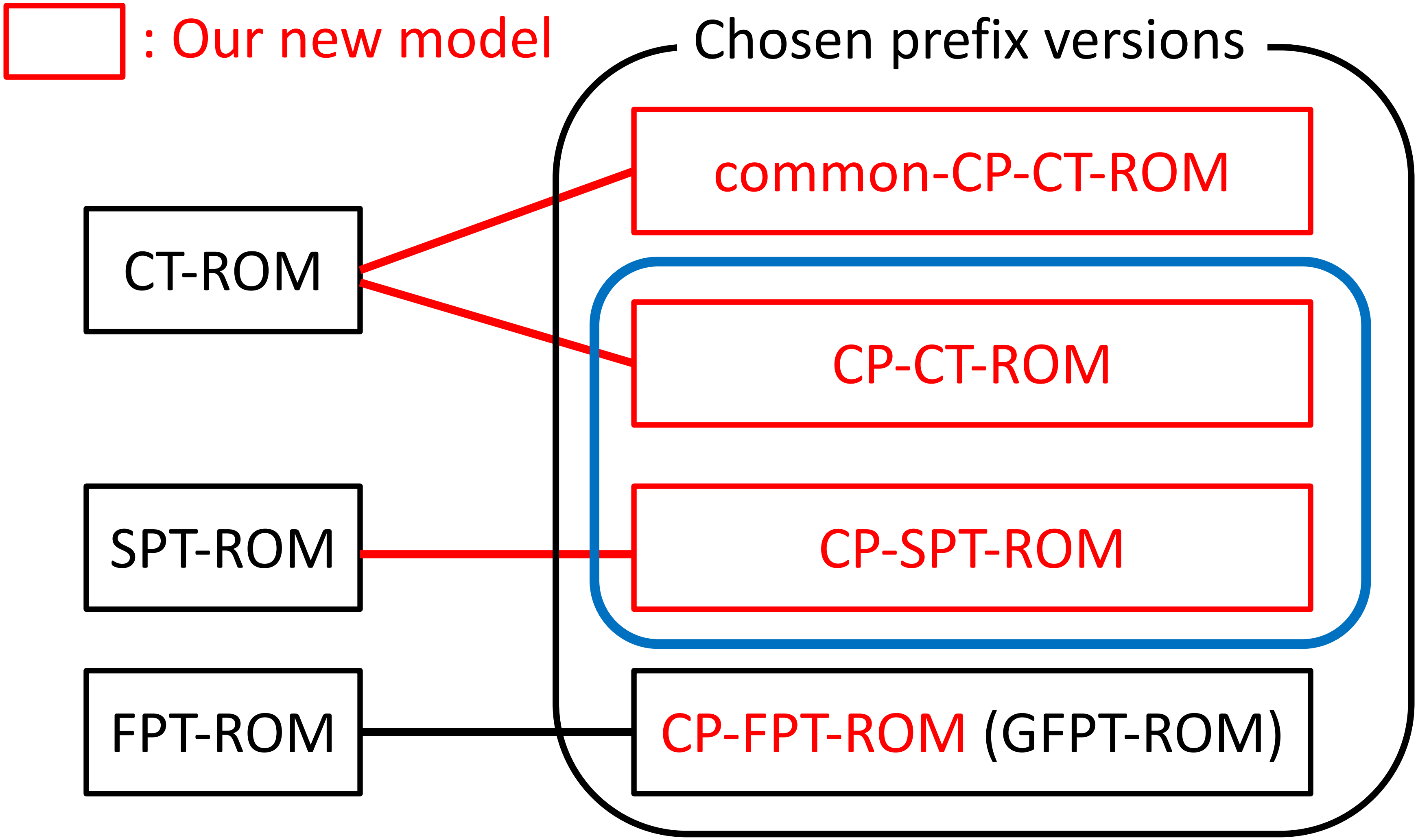
common-CP-CT-ROM

CP-CT-ROM

CP-SPT-ROM

CP-FPT-ROM (GFPT-ROM)

Our results



□ : Our new model

Chosen prefix versions

CT-ROM

SPT-ROM

FPT-ROM

common-CP-CT-ROM

CP-CT-ROM

CP-SPT-ROM

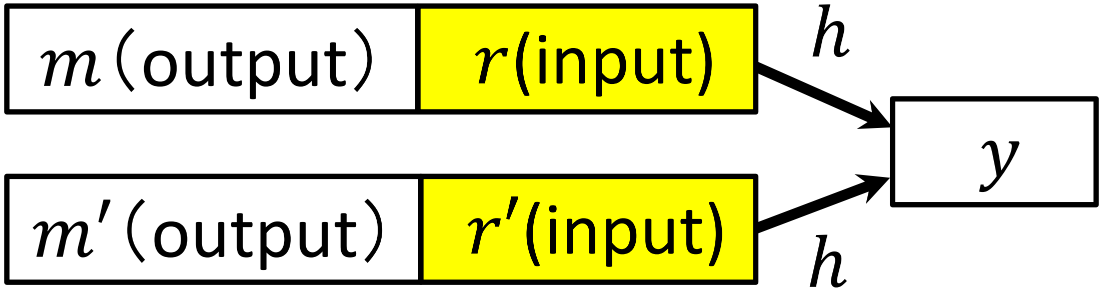
CP-FPT-ROM (GFPT-ROM)

Our results
CP–CT–ROM and CP–SPT–ROM

CP-CT-ROM

$\text{CP-CT}(r, r')$

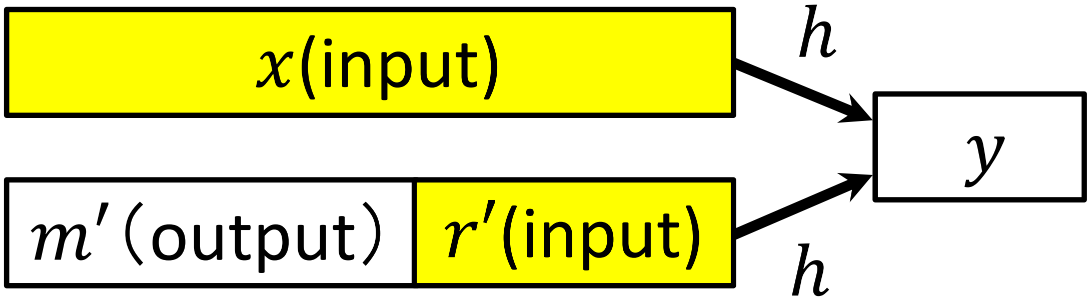
It uniformly outputs a collision such that $(m||r, m'||r')$.



CP-SPT-ROM

$\text{CP-SPT}(x, r')$

It uniformly outputs $m'||r'$ such that $h(x) = h(m'||r')$.

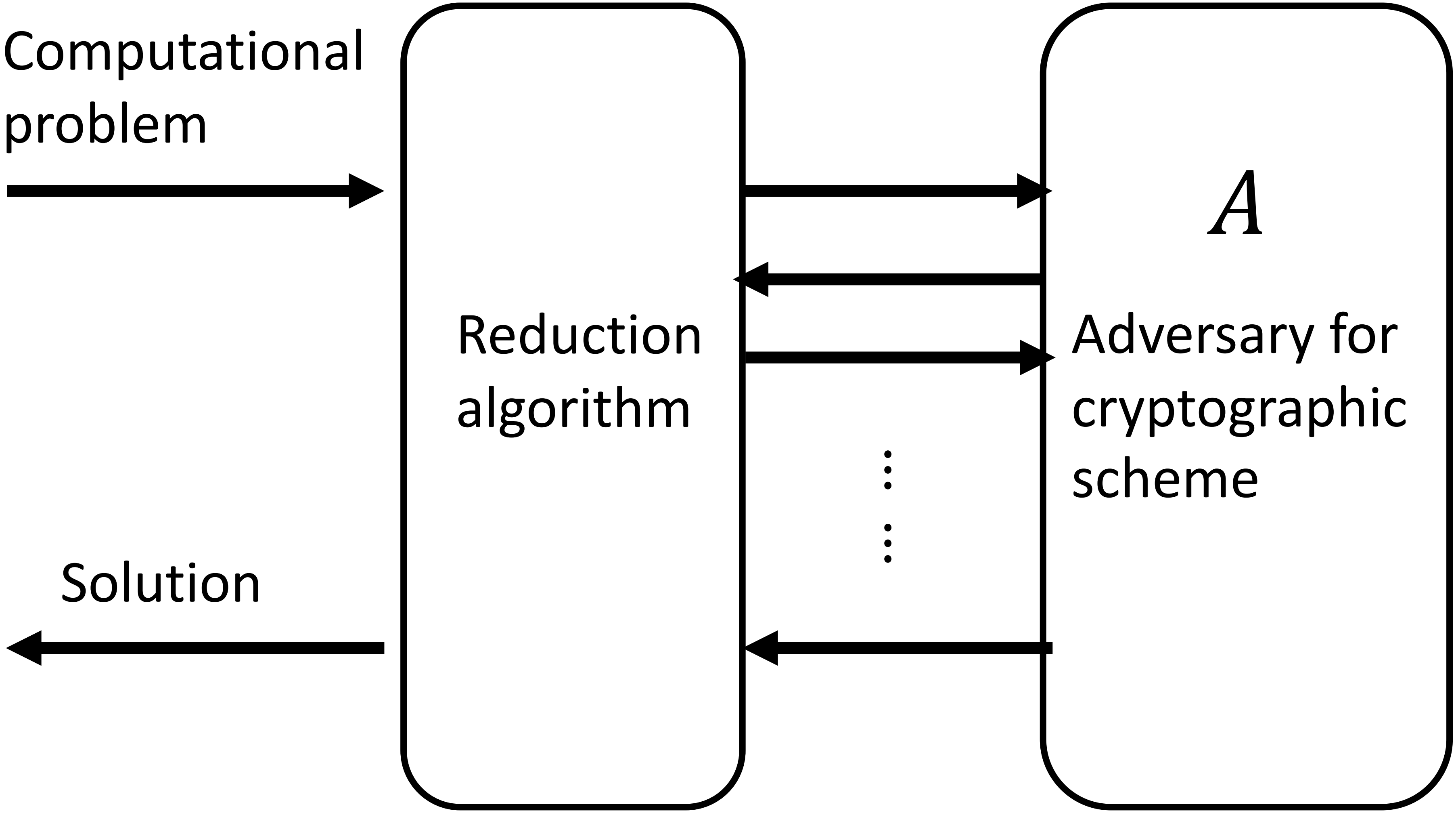


Our results
EUF−CMA security of signature schemes in WROMs

Chosen prefix collision attack

	ROM	CP-CT-ROM	CP-SPT-ROM	CP-FPT-ROM
RSA-FDH	✓	×	×	×
RSA-PFDH	✓	✓	×	×
RSA-PFDH$^{\oplus}$	✓	✓	×	×
RSA-FDH^{+}	✓	✓	✓	✓

Technique for simulating in ROM



Computational problem

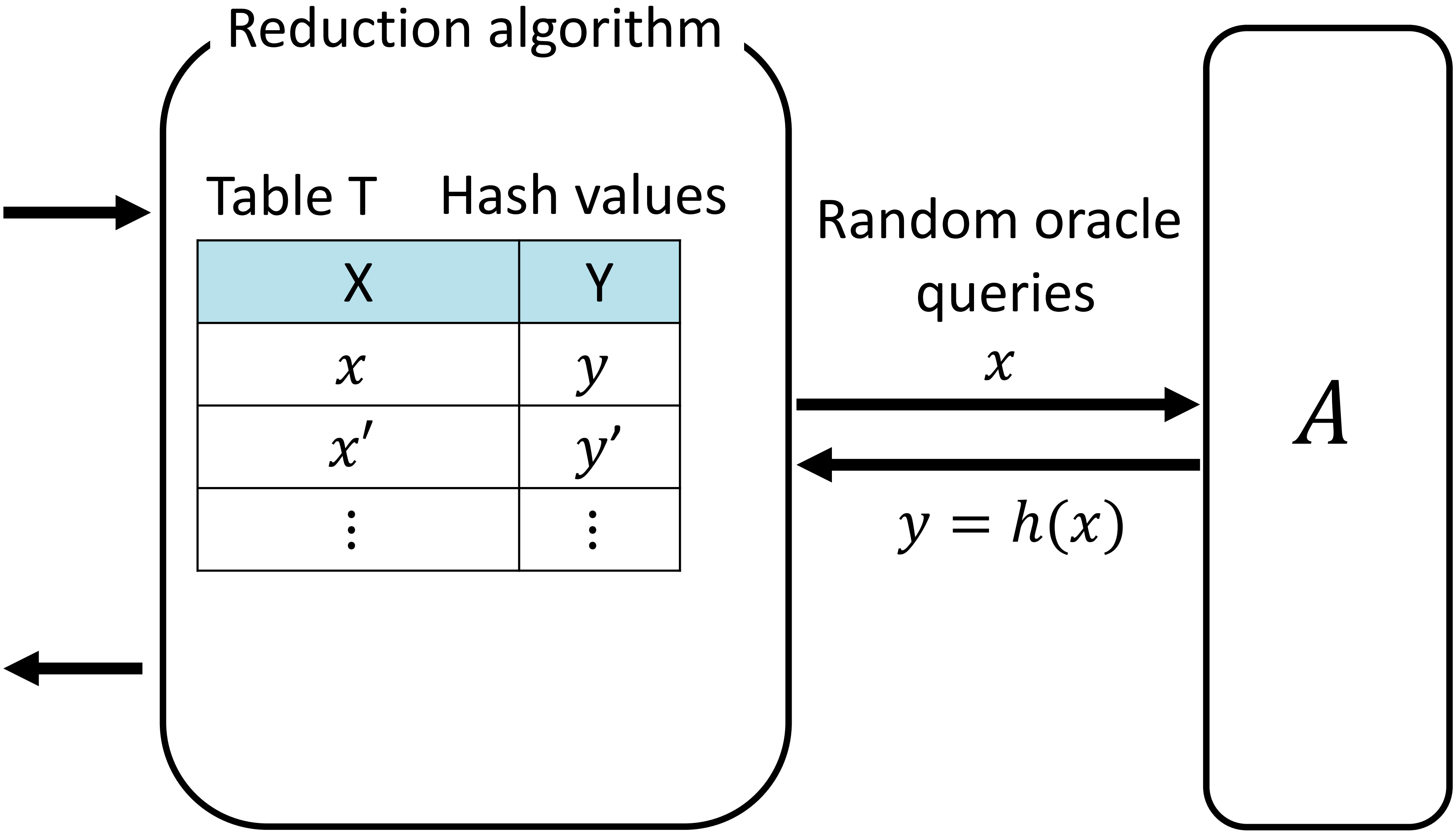
Reduction algorithm

A

Adversary for cryptographic scheme

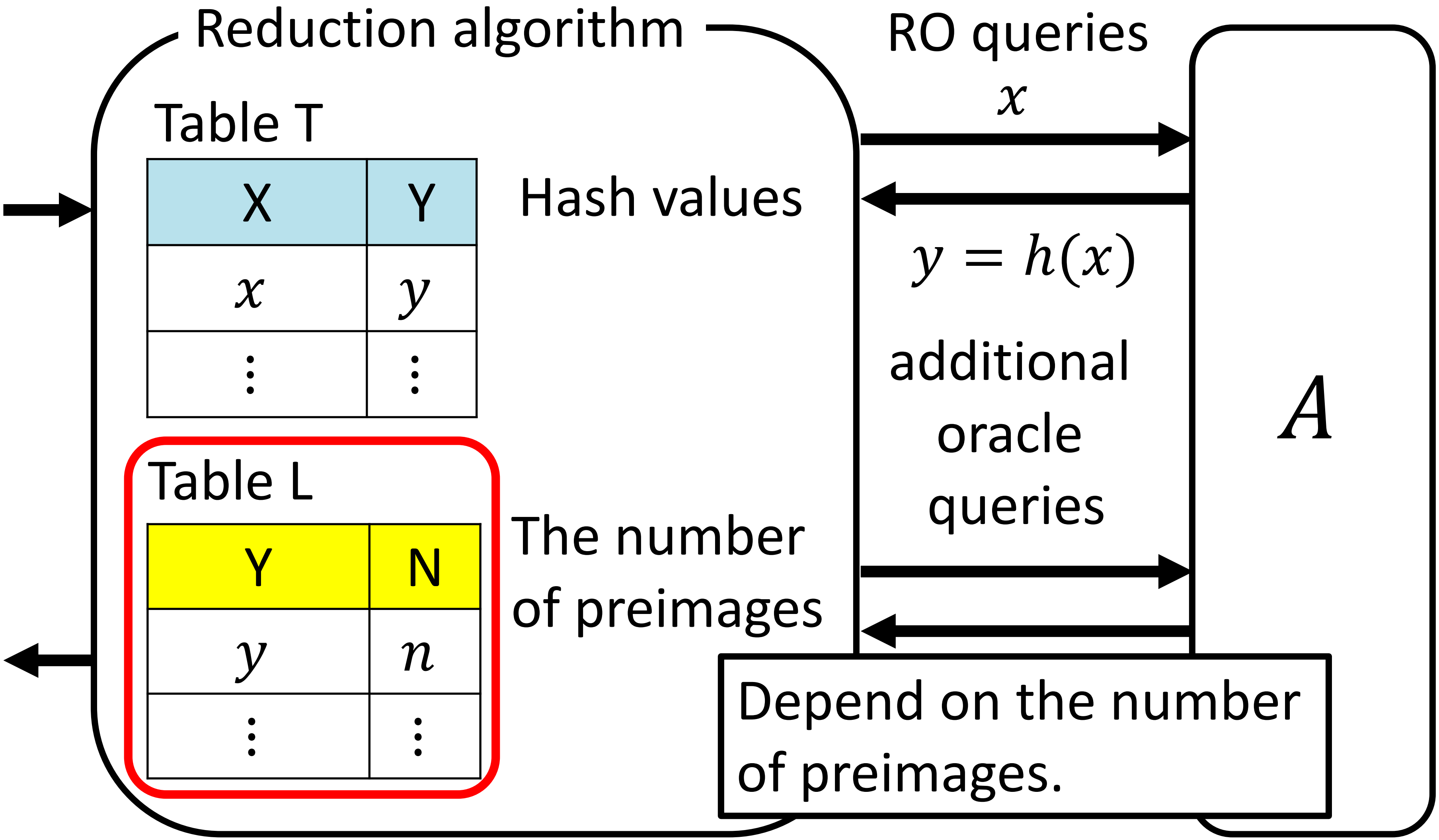
Solution

Technique for simulating in ROM



X	Y
x	y
x'	y'
$\vdots$	$\vdots$

Technique for simulating WROMs in CT-ROM, SPT-ROM, FPT-ROM



Reduction algorithm

Table T

X	Y
x	y
⋮	⋮

Hash values

Table L

Y	N
y	n
⋮	⋮

The number of preimages

RO queries

x

$y = h(x)$

additional oracle queries

A

Depend on the number of preimages.

Technique for simulating WROMs in CP−CT−ROM, CP−SPT−ROM, CP−FPT−ROM

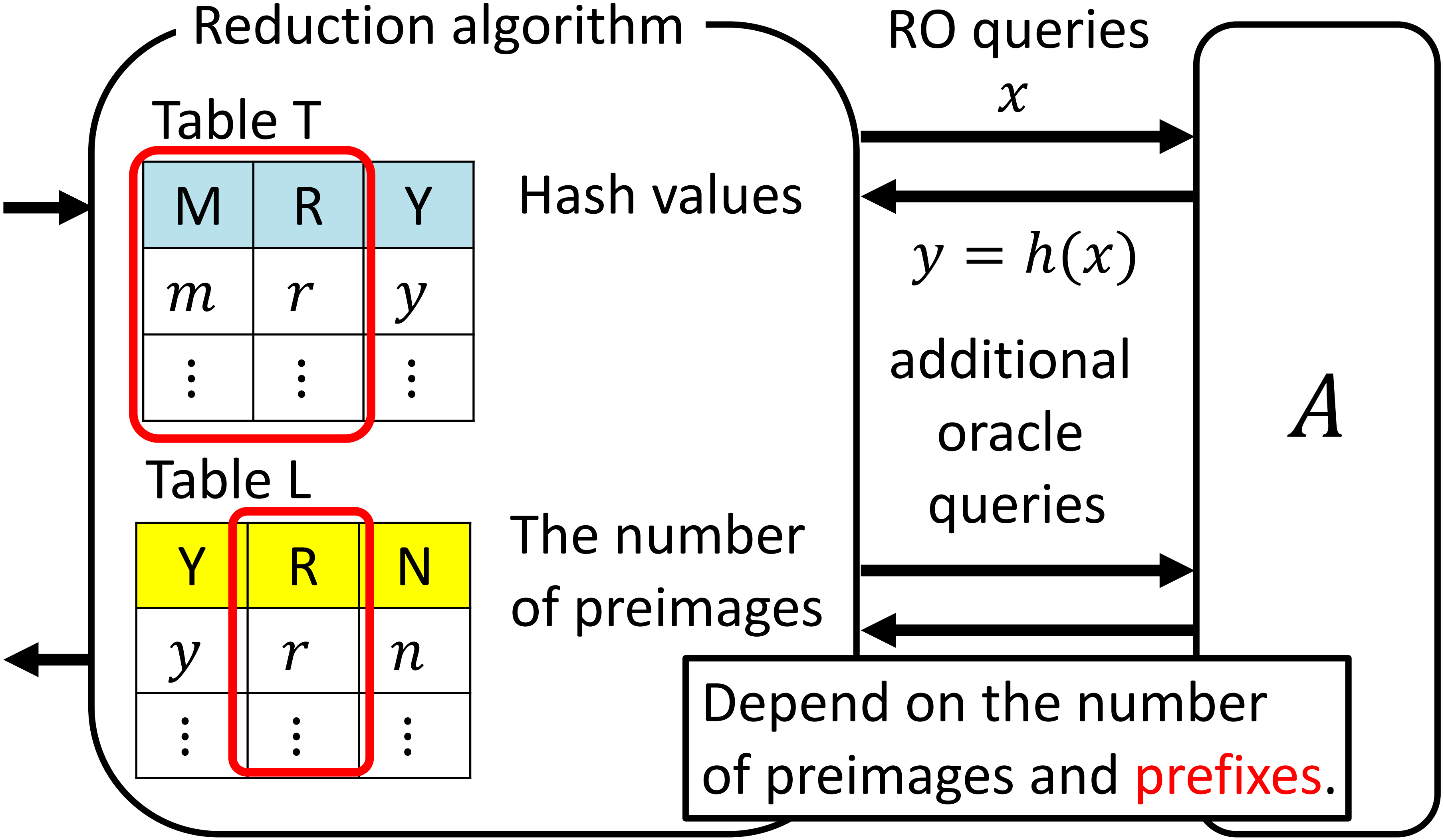


Table T

M	R	Y
m	r	y
⋮	⋮	⋮

Hash values

Table L

Y	R	N
y	r	n
⋮	⋮	⋮

The number of preimages

Depend on the number of preimages and prefixes.

Future works

There are practical signature schemes that have not been analyzed in WROMs.

We want to analyze more signature schemes in WROMs. (RSA-PSS, Shnorr signarure)

Appendix: RSA problem (N, e, z)

p, q : λ – bits primes

$N = pq, \qquad \phi(N) = (p-1)(q-1)$

$e \xleftarrow{r} Z_{\phi(N)}, \quad de = 1\, mod$

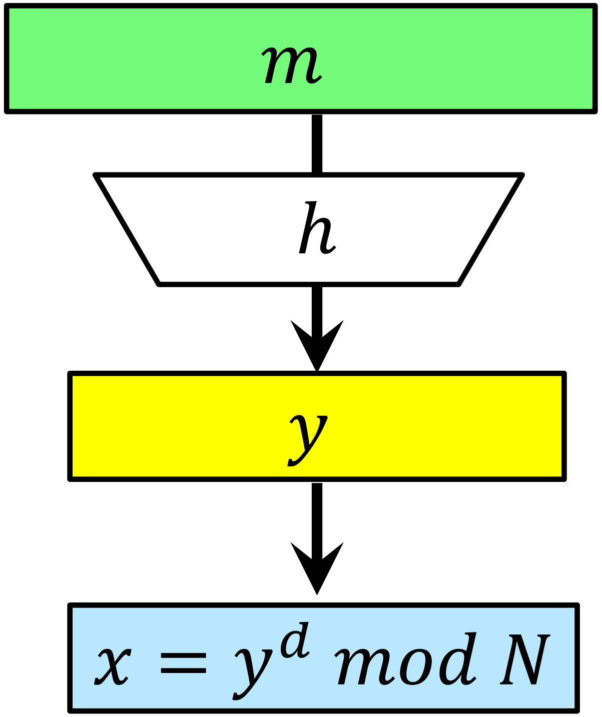
$z \xleftarrow{r} Z_N^*$

Given an instance (N, e, z),

compute $z^{1/e}$.

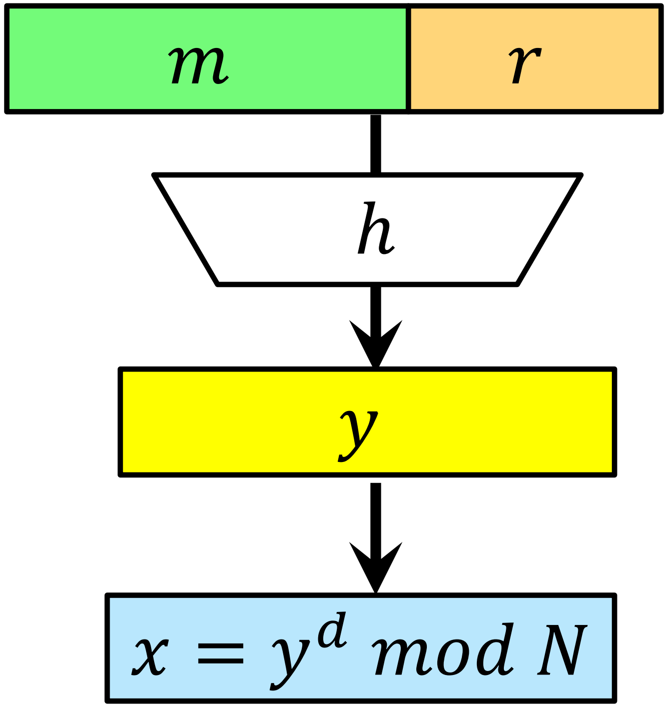
Appendix: RSA–FDH, RSA–PFDH

RSA-FDH Sign$(sk = d, m)$



Return $\sigma = x$

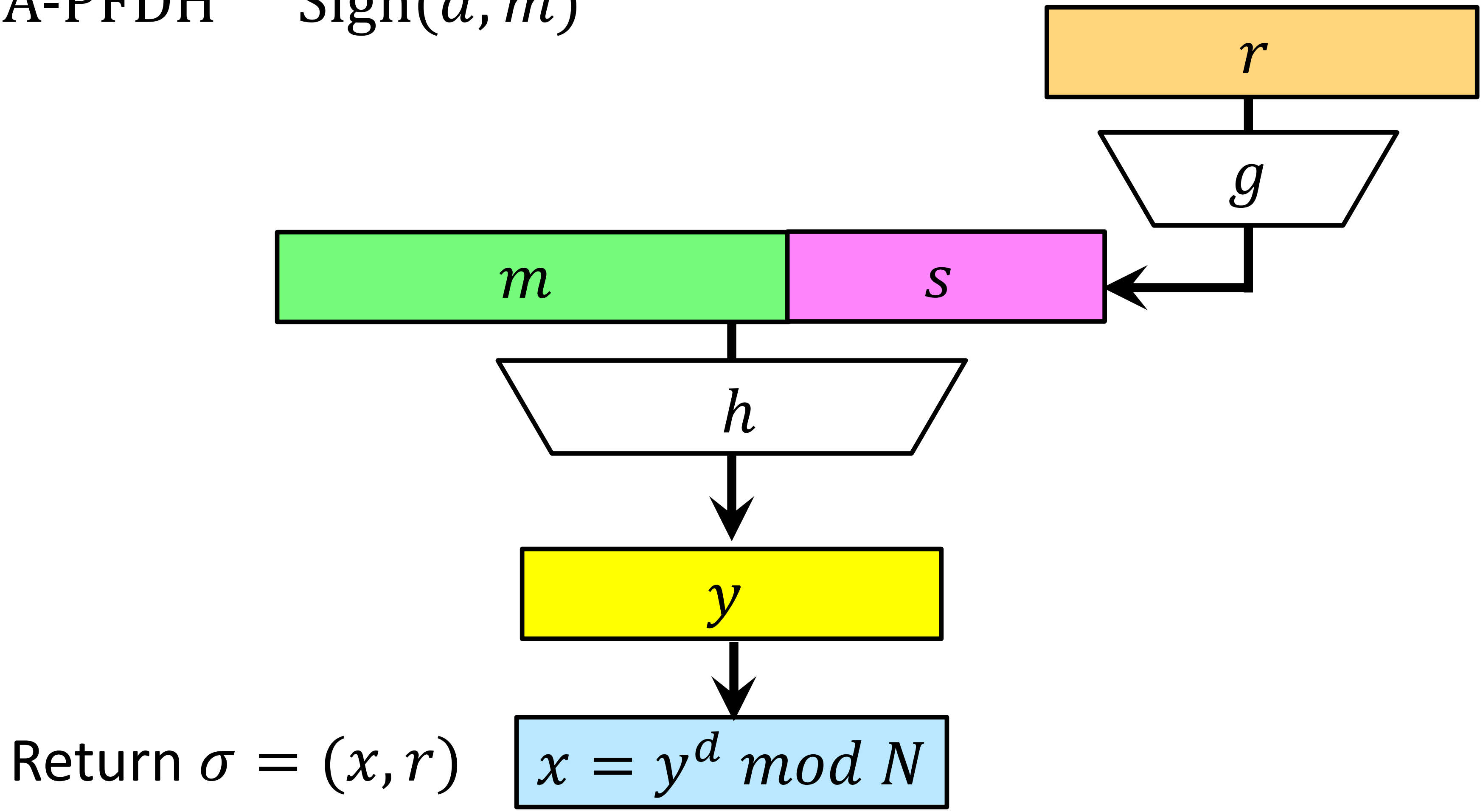
RSA-PFDH Sign(sk, m)



Return $\sigma = (x, r)$

Appendix: RSA−PFDH$^+$

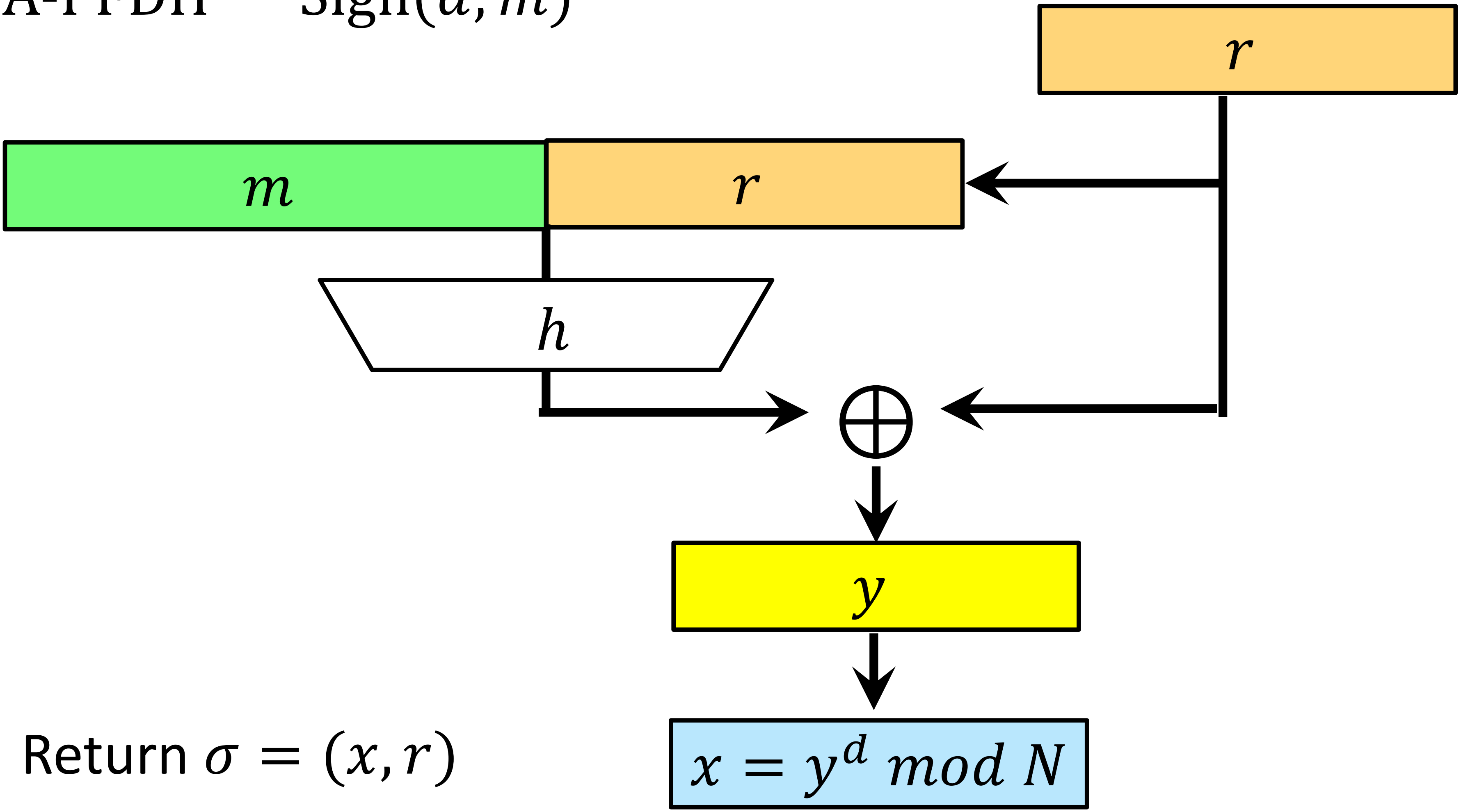
RSA-PFDH$^+$ Sign(d, m)



Return $\sigma = (x, r)$

Appendix: RSA−PFDH$^{\oplus}$

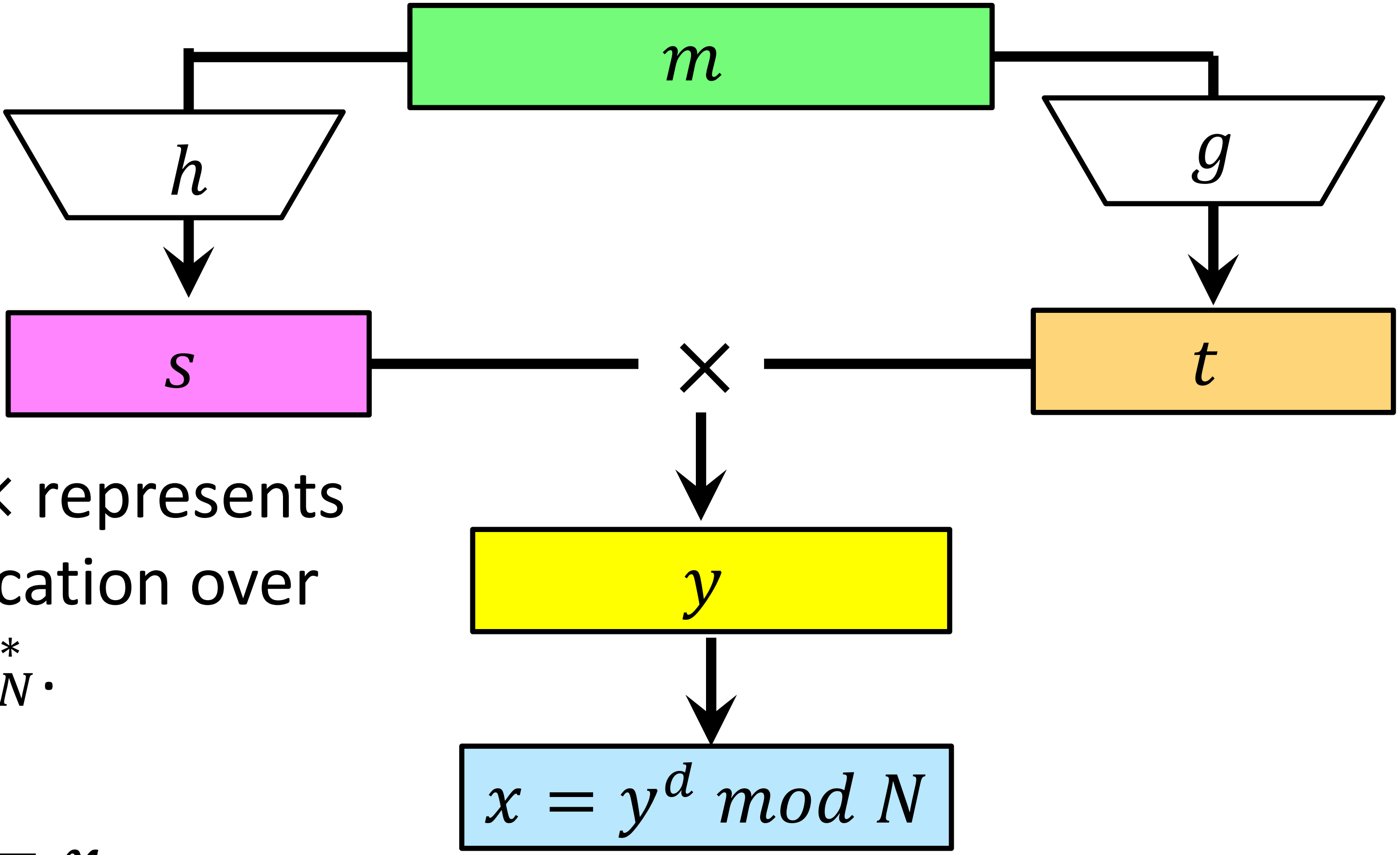
RSA-PFDH$^{\oplus}$ Sign(d, m)



Return $\sigma = (x, r)$

Appendix: RSA–FDH^{+}

RSA-FDH^{+} $\mathrm{Sign}(d, m)$



Operation × represents the multiplication over the group Z_N^*.

Return $\sigma = x$