[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

NONCE-BASED CRYPTOGRAPHY
RETAINING SECURITY WHEN RANDOMNESS FAILS

Mihir Bellare and Björn Tackmann
University of California, San Diego

Eurocrypt 2016, Vienna — May 11, 2016

[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

WEAK RANDOMNESS

bugs and bad implementations

PlayStation 3

ECDSA randomness

debian OpenSSL

insufficient entropy

RSA Certificate Keys

coinciding prime factors [1]

Netscape

insufficient entropy

/dev/random

... is not robust [2]

targeted attack(s)

DUAL EC

NIST RSA

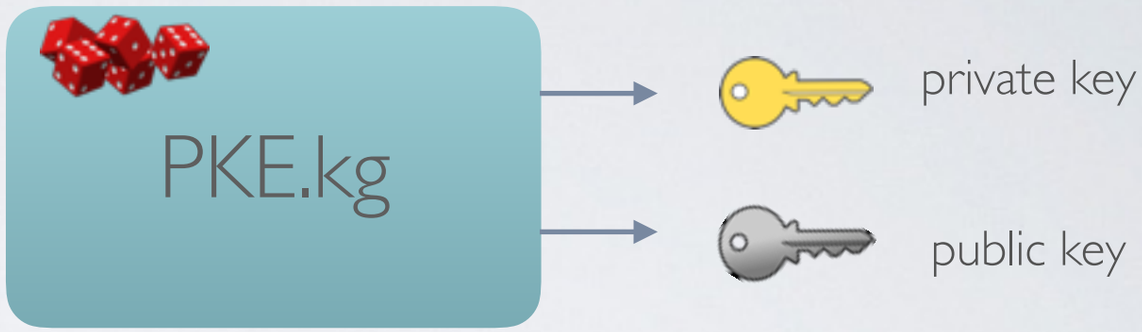
… and more?

[1; Heninger, Durumeric, Wustrow, Halderman, 2012; Lenstra, Hughes, Augier, Bos, Kleinjung, and Wachter, 2012]
[2; Dodis, Pointcheval, Ruhault, Vergnaud, Wichs, 2013]

[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

PUBLIC-KEY ENCRYPTION

1. key generation



2. encryption

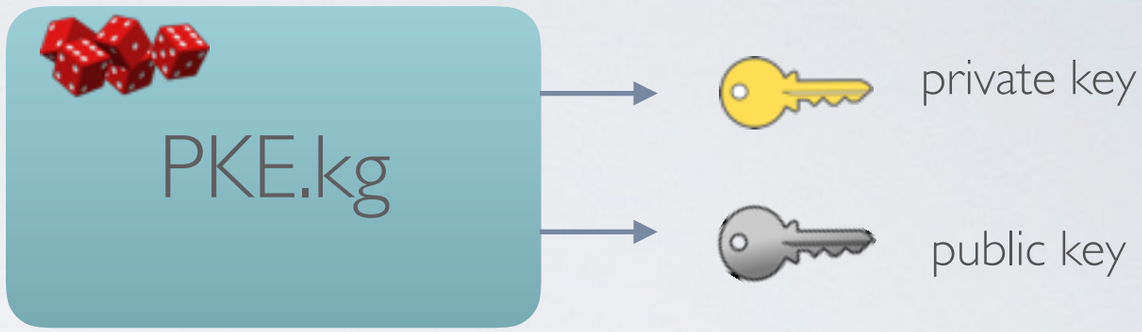
3. decryption

[Goldwasser, Micali, 1984]

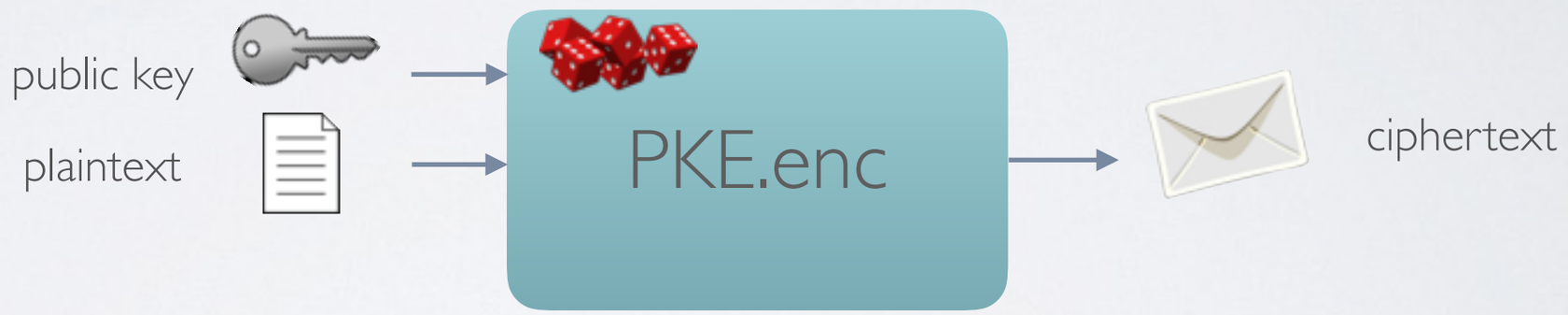
[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

PUBLIC-KEY ENCRYPTION

1. key generation



2. encryption

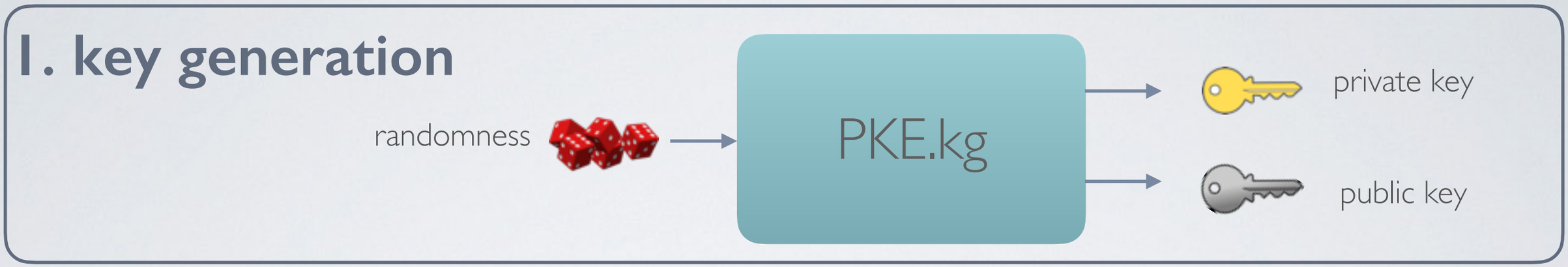


3. decryption

[Goldwasser, Micali, 1984]

[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

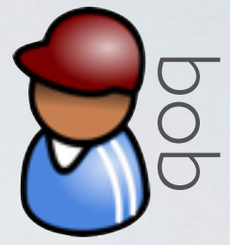
PUBLIC-KEY ENCRYPTION



[Goldwasser, Micali, 1984]

[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

USING PUBLIC-KEY ENCRYPTION



pk

(authenticated)

$(sk, pk) \leftarrow^{\$} \mathsf{PKE.kg}$

sk

sk

$c \leftarrow^{\$} \mathsf{PKE.enc}(pk, m)$

c

$m \leftarrow \mathsf{PKE.dec}(sk, c)$

m message
c ciphertext
pk public key
sk secret key

SYMMETRIC ENCRYPTION AND NONCES

1. encryption

2. decryption

[Bellare, Desai, Jokipii, Rogaway, 1997; Rogaway, 2004]

[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

SYMMETRIC ENCRYPTION AND NONCES

1. encryption

2. decryption

[Bellare, Desai, Jokipii, Rogaway, 1997; Rogaway, 2004]

[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

SYMMETRIC ENCRYPTION AND NONCES

1. encryption

2. decryption

[Bellare, Desai, Jokipii, Rogaway, 1997; Rogaway, 2004]

[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

WHAT ABOUT NONCE-BASED PKE?

all input values may be known to an attacker!

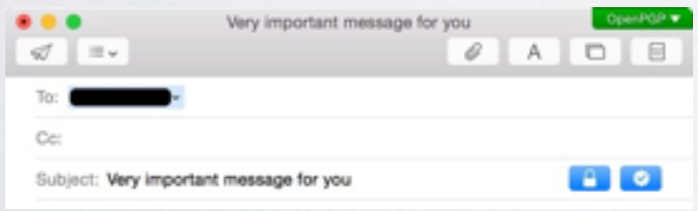
[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

THE INTUITION

1. setup: generation of *good* random seed

2. keep state: *sender* stores seed

but we hedge scheme against exposure



3. encryption: use seed along with nonce

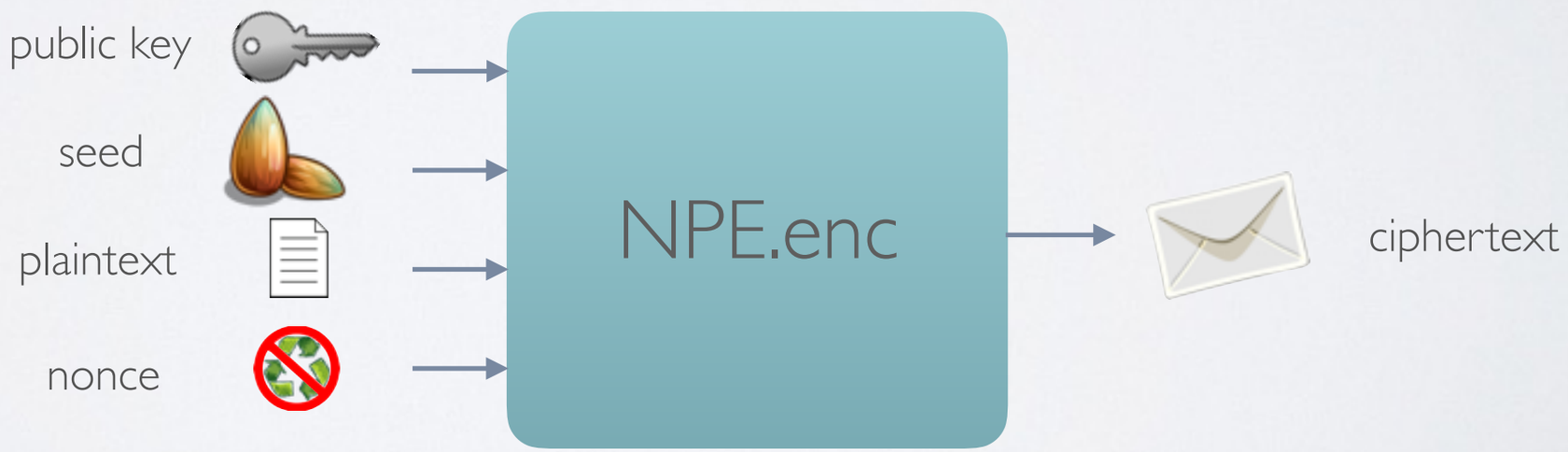
[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

NONCE-BASED PKE

1a. receiver key generation as before

1b. sender key generation

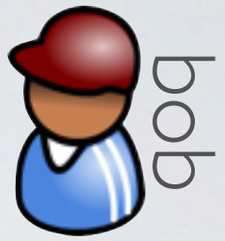
2. encryption



3. decryption as before

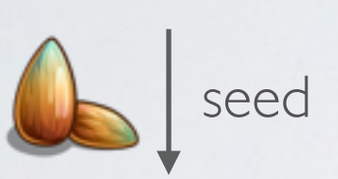
[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

USING NONCE-BASED PKE

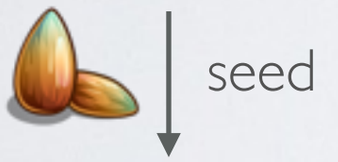


seed ←$ NPE.skg

(*sk*, *pk*) ←$ NPE.rkg



(*authenticated*)



c ← NPE.enc(*pk*, seed, *m*, nonce)

m ← NPE.dec(*sk*, *c*)

m message
c ciphertext
pk public key
sk secret key

[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

USING NONCE-BASED PKE

[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

SECURITY GUARANTEES

security is guaranteed if **either**

sender seed secret **and** (nonce, message) pairs unique

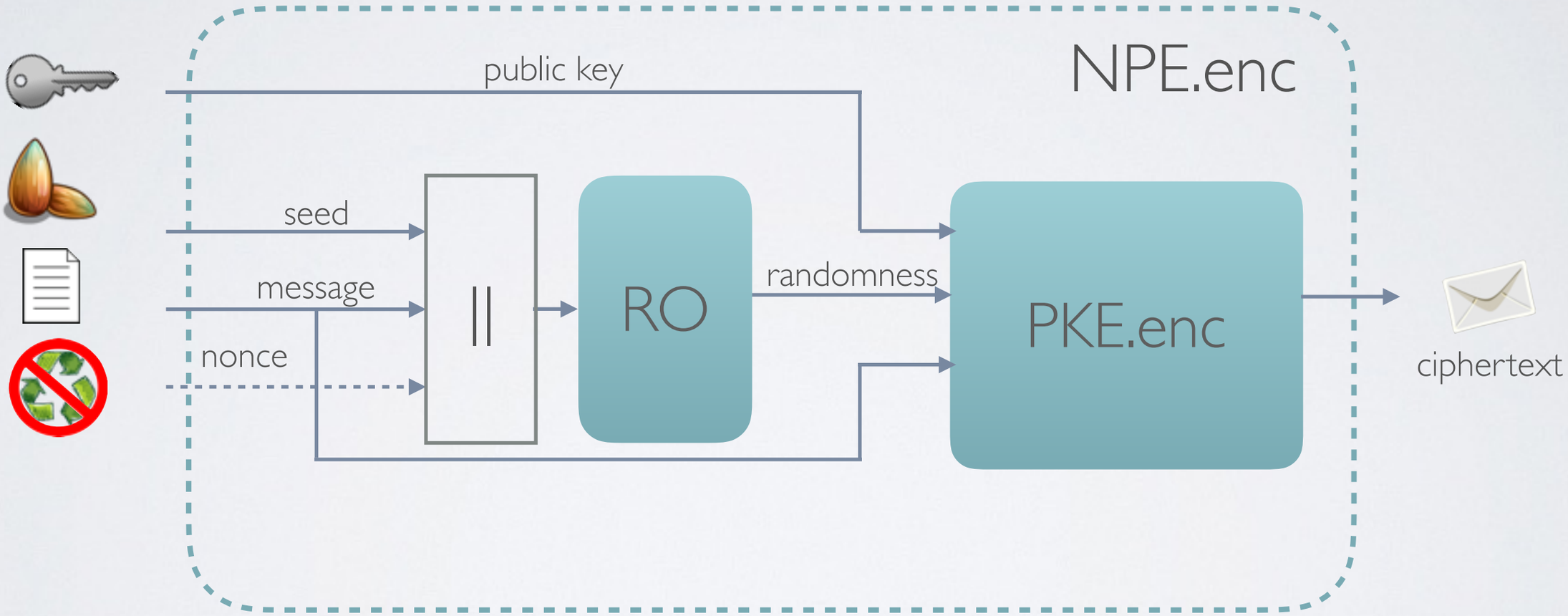
or

sender seed public **and** nonces secret and unpredictable.

include in nonces, e.g., sender and receiver addresses, time, system RNG output

[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

A RANDOM-ORACLE-BASED SCHEME



decryption remains unchanged

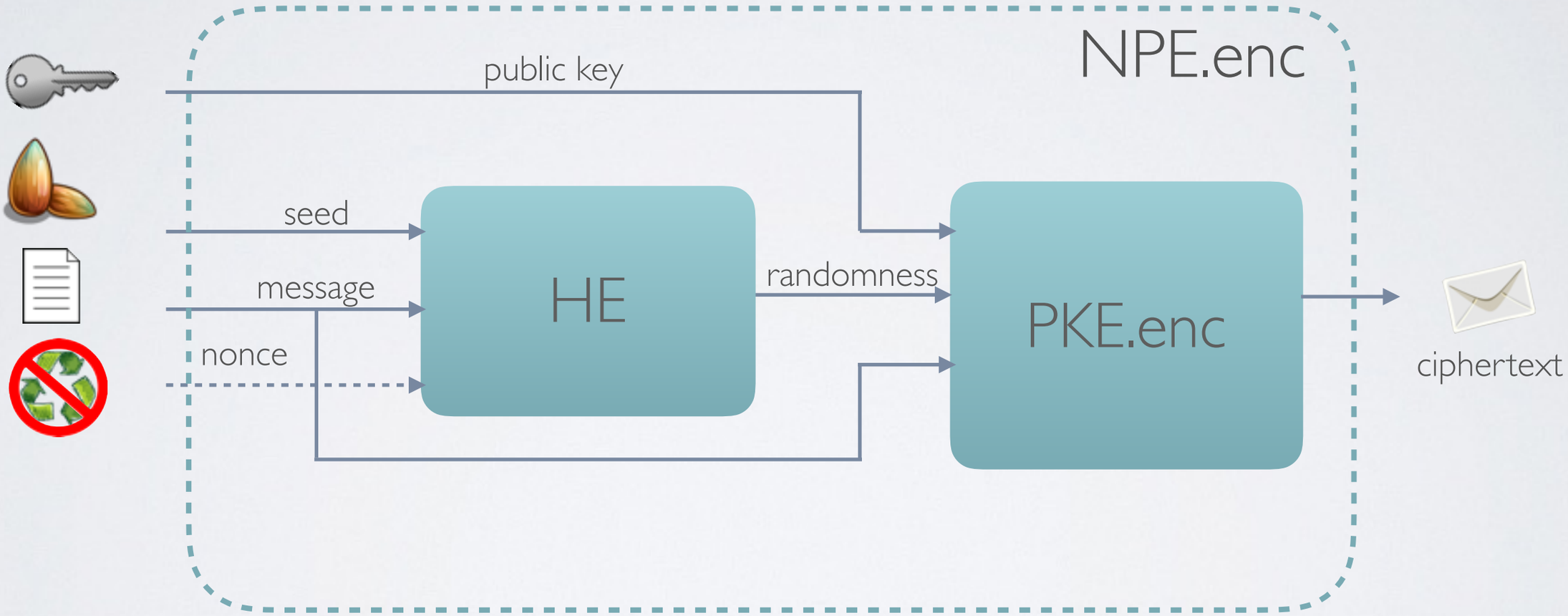
[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

MAIN TOOL: HEDGED EXTRACTORS

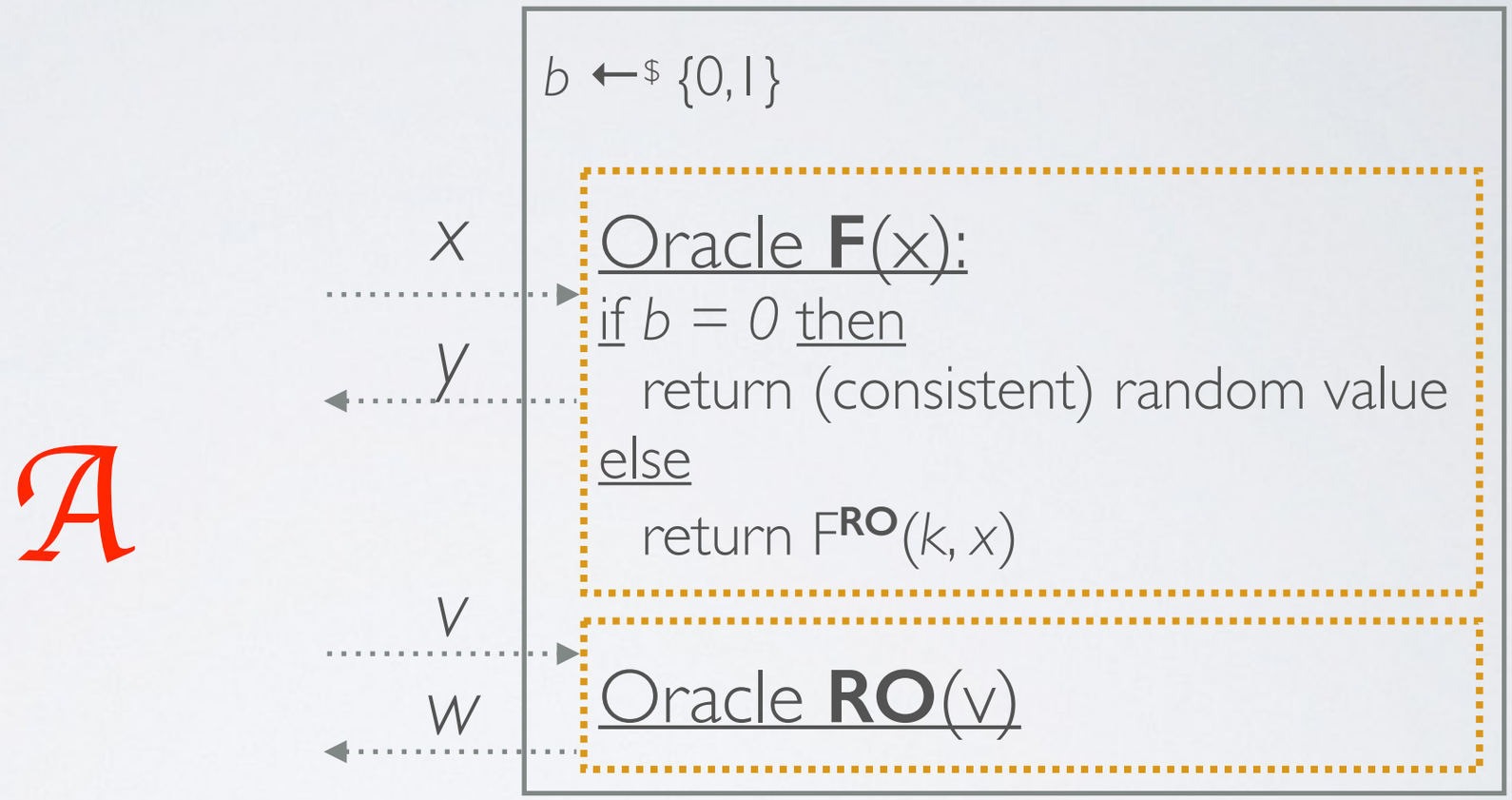
(a) PRF **if** seed is secret
(b) strong extractor **if** seed public but random

[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

ADAPTING TO HEDGED-EXTRACTORS



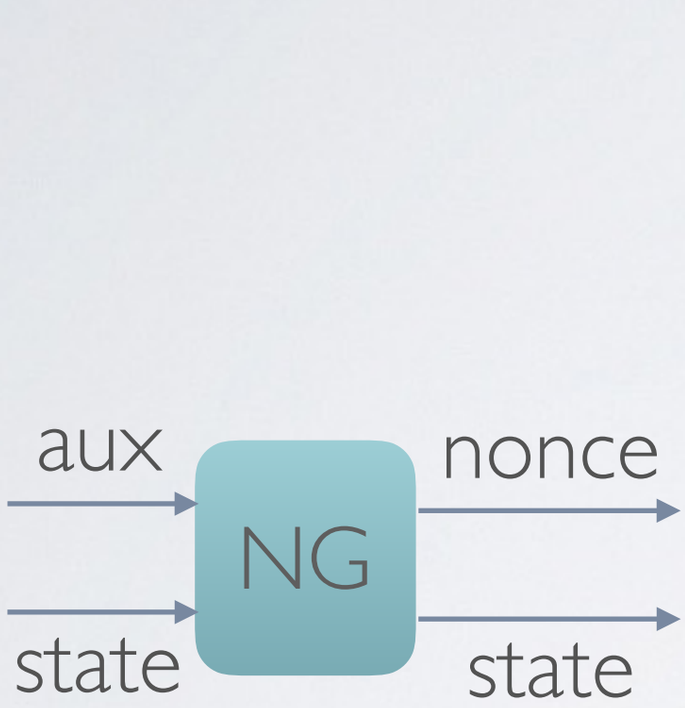
SECURITY 1: PSEUDO-RANDOMNESS

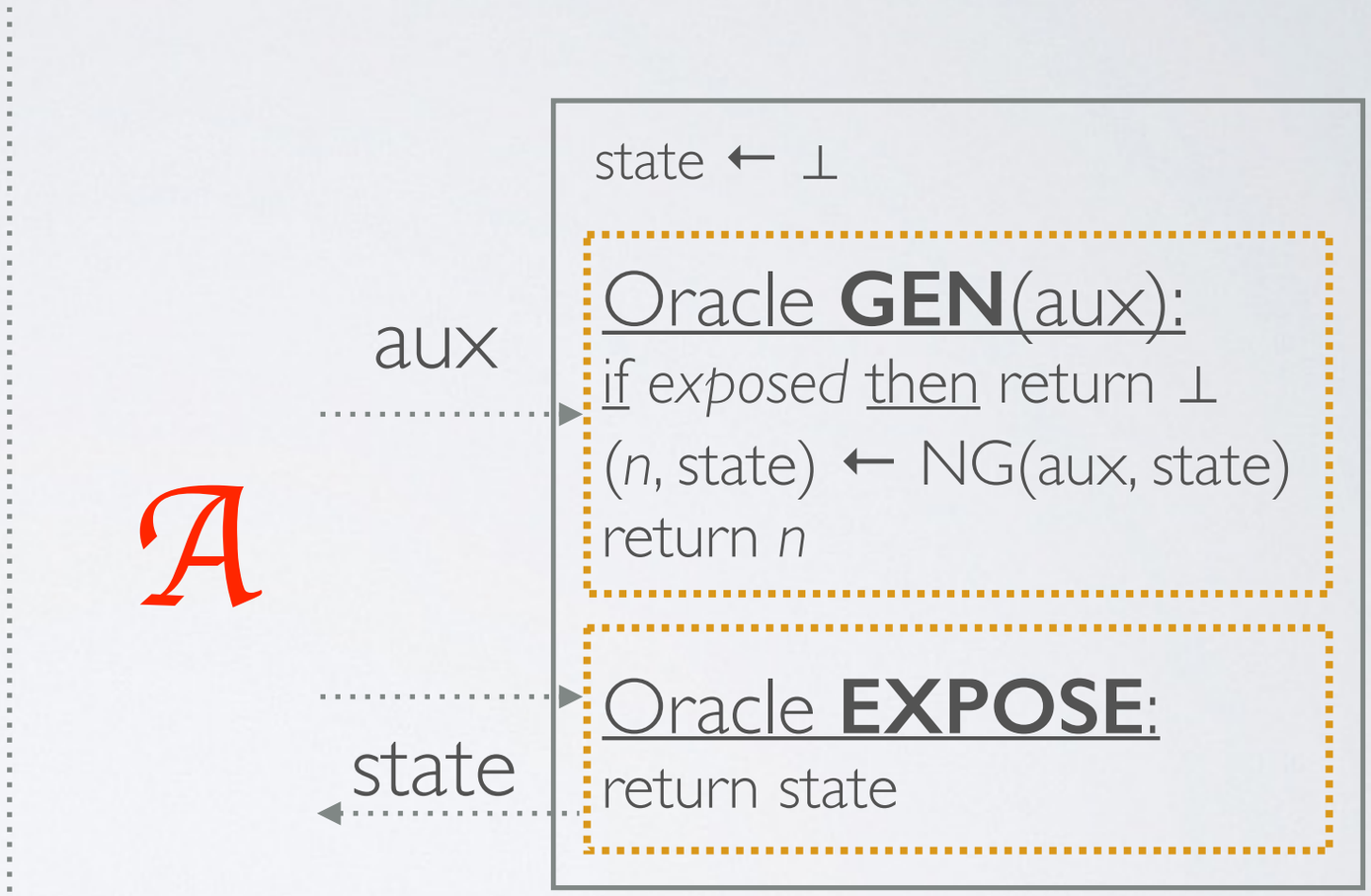


$$\mathrm{Adv}^{\mathbf{prf}}(F, \mathcal{A}) \;=\; 2\,\Pr[\, b' \leftarrow^{\$} \mathcal{A}^{\mathbf{F},\mathbf{RO}};\, b = b' \,] - 1$$

[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

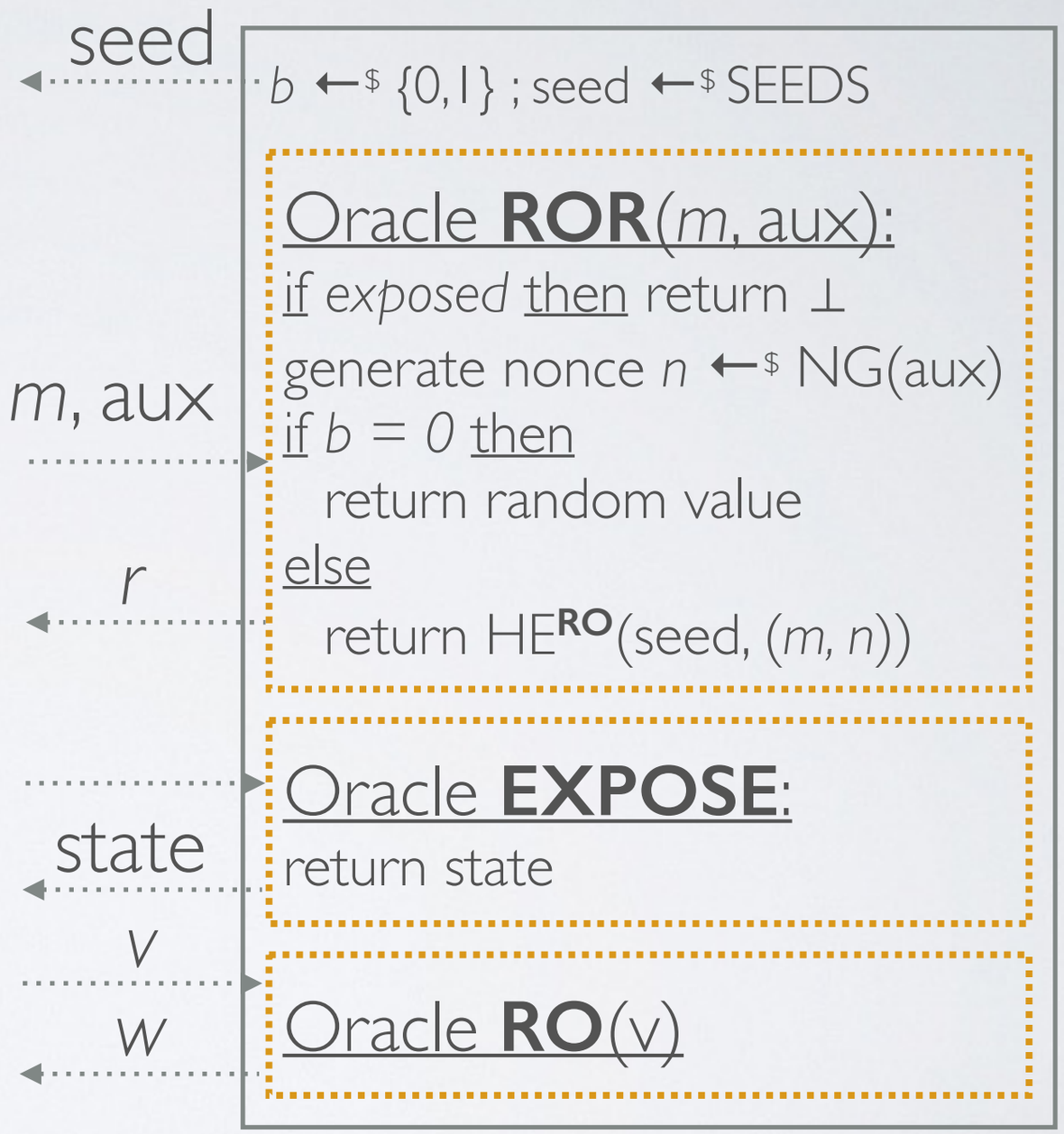
(UNPREDICTABLE) NONCE GENERATORS





$$\mathrm{Adv}^{\mathbf{pred}}(\mathrm{NG}, \mathcal{A}) = \Pr[\, n \leftarrow\!\!\$\ \mathcal{A}^{\mathbf{GEN},\mathbf{EXPOSE}};\ n \in N \text{ or } \mathit{collision} \,]$$

SECURITY 2: EXTRACTION

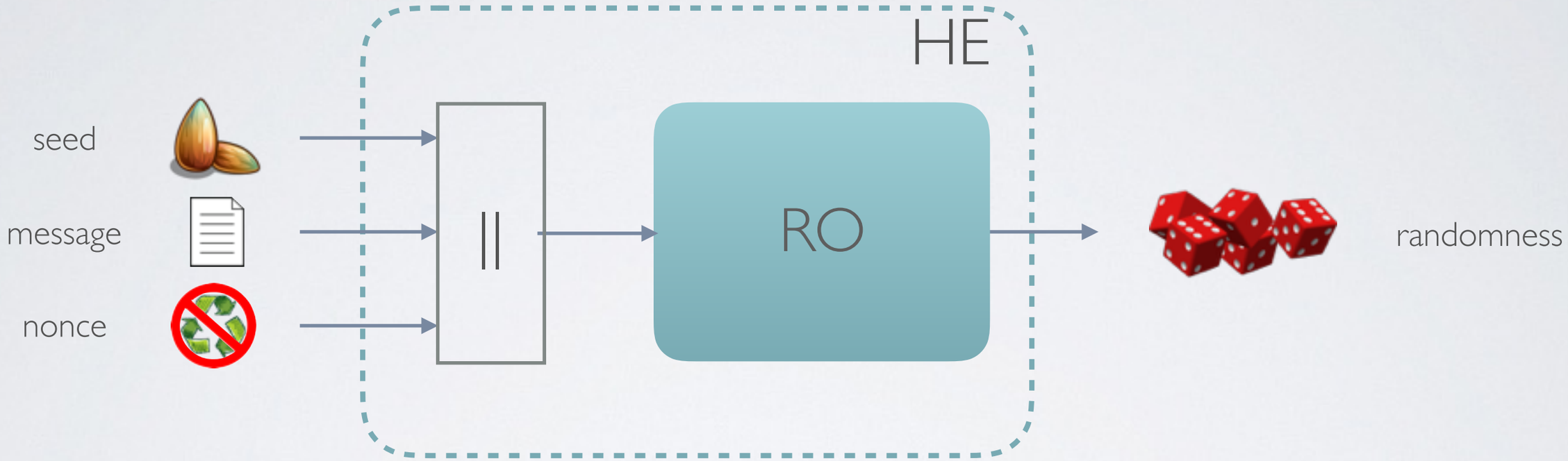


$\mathcal{A}$

$$\mathrm{Adv}^{\mathbf{ror}}(\mathrm{HE}, \mathrm{NG}, \mathcal{A}) = 2\,\Pr[\, b' \leftarrow\!\!\$\ \mathcal{A}^{\mathbf{ROR},\mathbf{EXPOSE},\mathbf{RO}};\ b = b' \,] - 1$$

[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

THE RANDOM-ORACLE SCHEME



$\mathrm{Adv}^{\mathbf{prf}}(\mathrm{HE}, \mathcal{A}) \leq q \bullet 2^{-k}$

$\mathrm{Adv}^{\mathbf{ror}}(\mathrm{HE}, \mathrm{NG}, \mathcal{A}) \leq q \bullet \mathrm{Adv}^{\mathbf{pred}}(\mathrm{NG}, \mathcal{B})$

q RO queries

seed length k

[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

RECALL: ALMOST-UNIVERSAL HASHING

Definition: F: $K \times X \to Z$ is ε-AUHF if

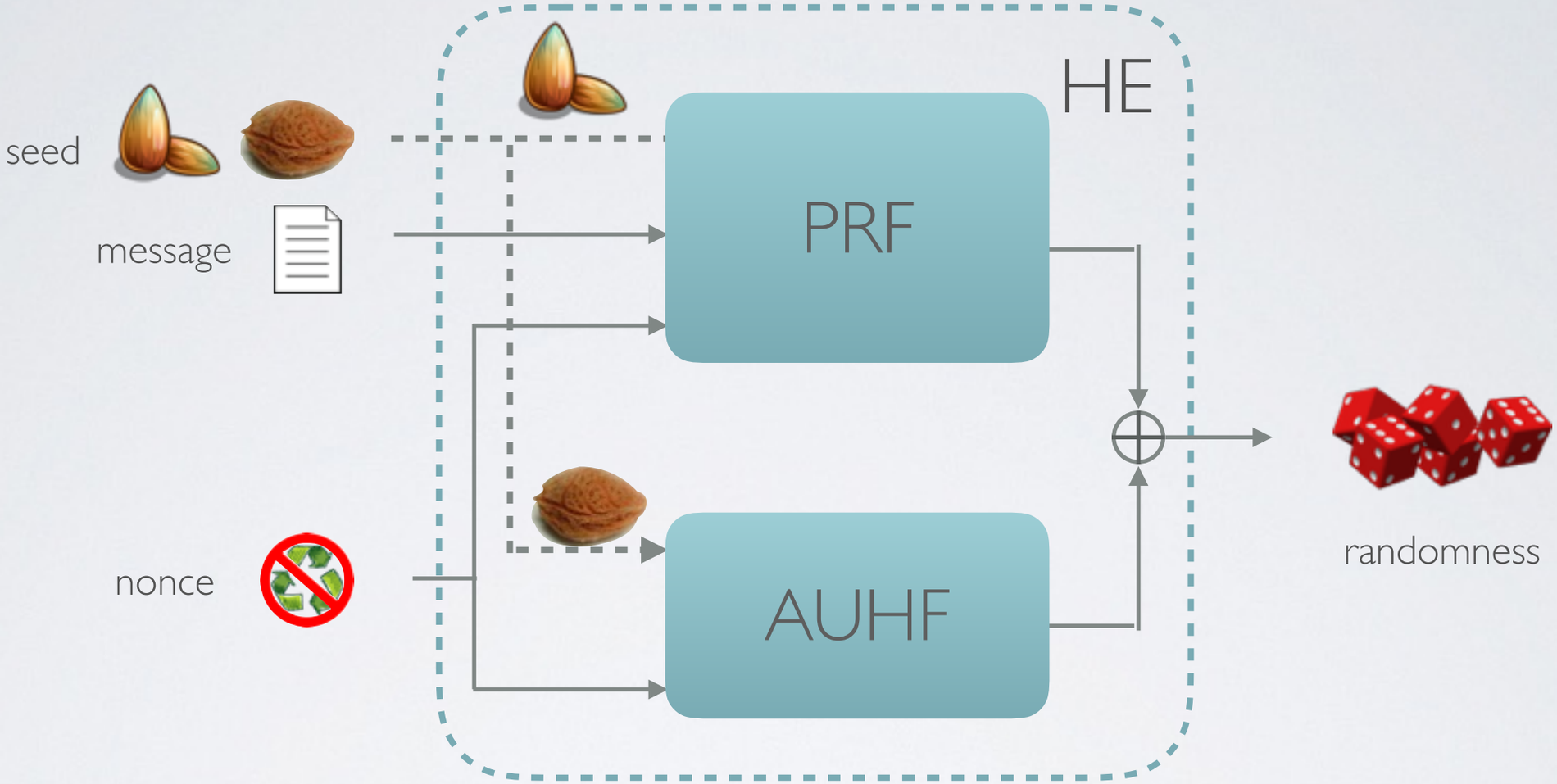
$$\forall\, x \neq y\colon\ \Pr_k[\, F(k, x) = F(k, y)\,] \leq \varepsilon$$

Leftover Hash Lemma: Let F be ε-AUHF, then

$k, z \approx_{\varepsilon'(k)} k, F(k, x)$ with $k \leftarrow\!\!\$\ K$; $z \leftarrow\!\!\$\ Z$; x with min-entropy k

[Impagliazzo, Levin, Luby, 1989]

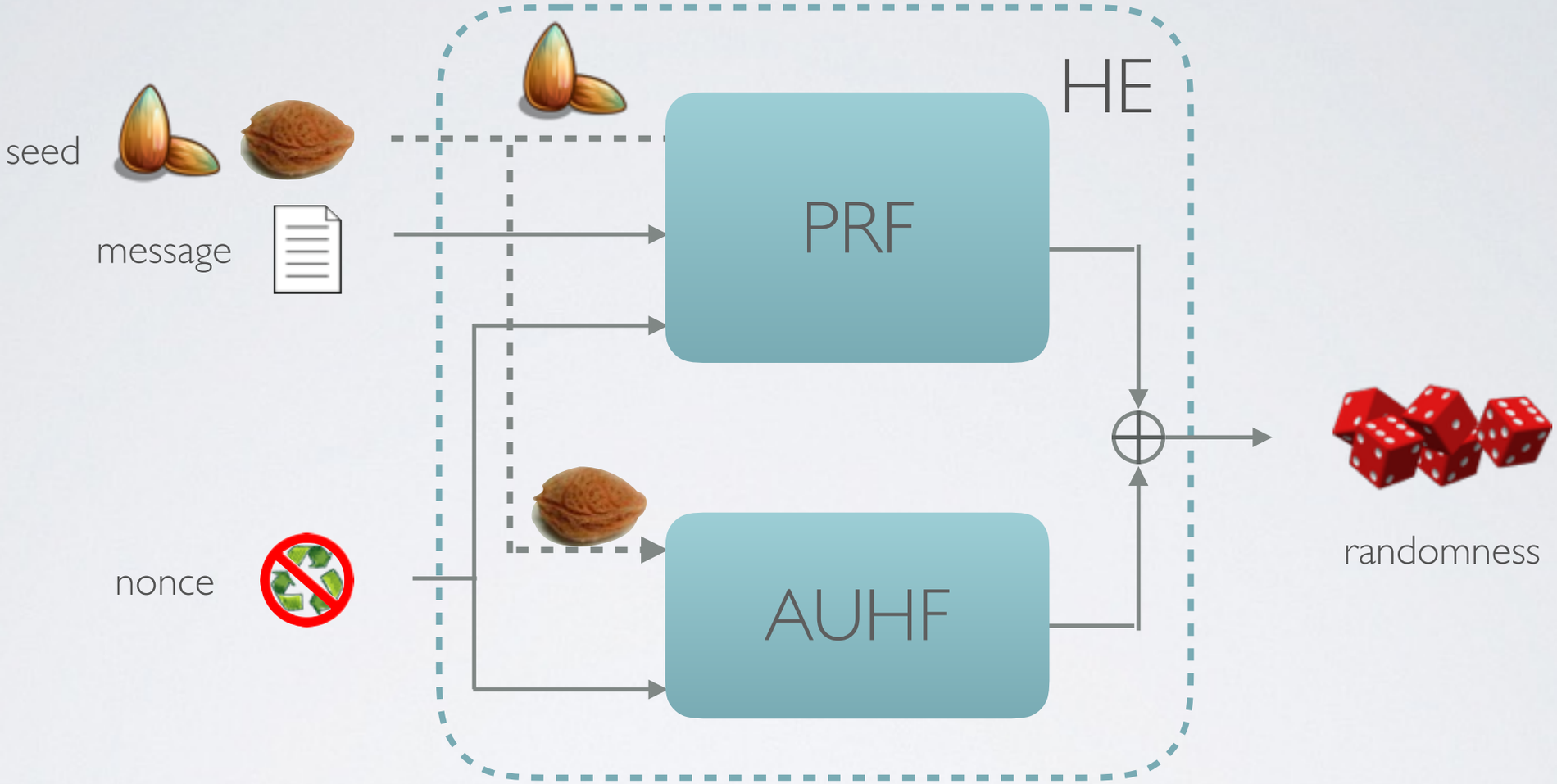
THE STANDARD-MODEL SCHEME



$\mathrm{Adv}^{\mathbf{prf}}(\mathrm{HE}, \mathcal{A}) \leq \mathrm{Adv}^{\mathbf{prf}}(\mathrm{PRF}, \mathcal{B})$

$\mathrm{Adv}^{\mathbf{ror}}(\mathrm{HE}, \mathrm{NG}, \mathcal{A}) \leq q \bullet \varepsilon'(k)$ if $\mathrm{Adv}^{\mathbf{pred}}(\mathrm{NG}, \mathcal{C}) \leq 2^{-k}$

THE STANDARD-MODEL SCHEME

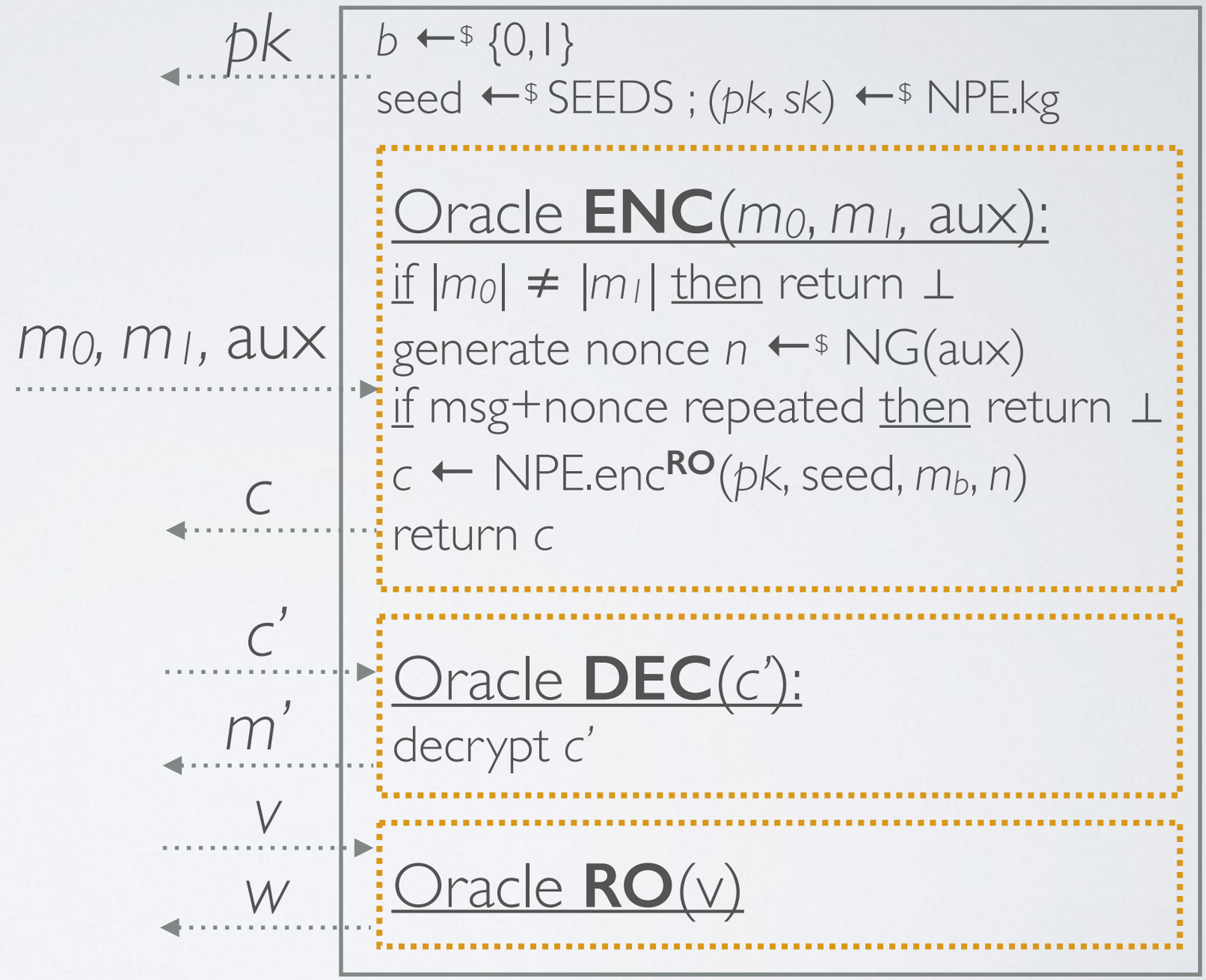


caveat: nonces must be independent of seed

$\mathrm{Adv}^{\mathbf{prf}}(\mathrm{HE}, \mathcal{A}) \leq \mathrm{Adv}^{\mathbf{prf}}(\mathrm{PRF}, \mathcal{B})$

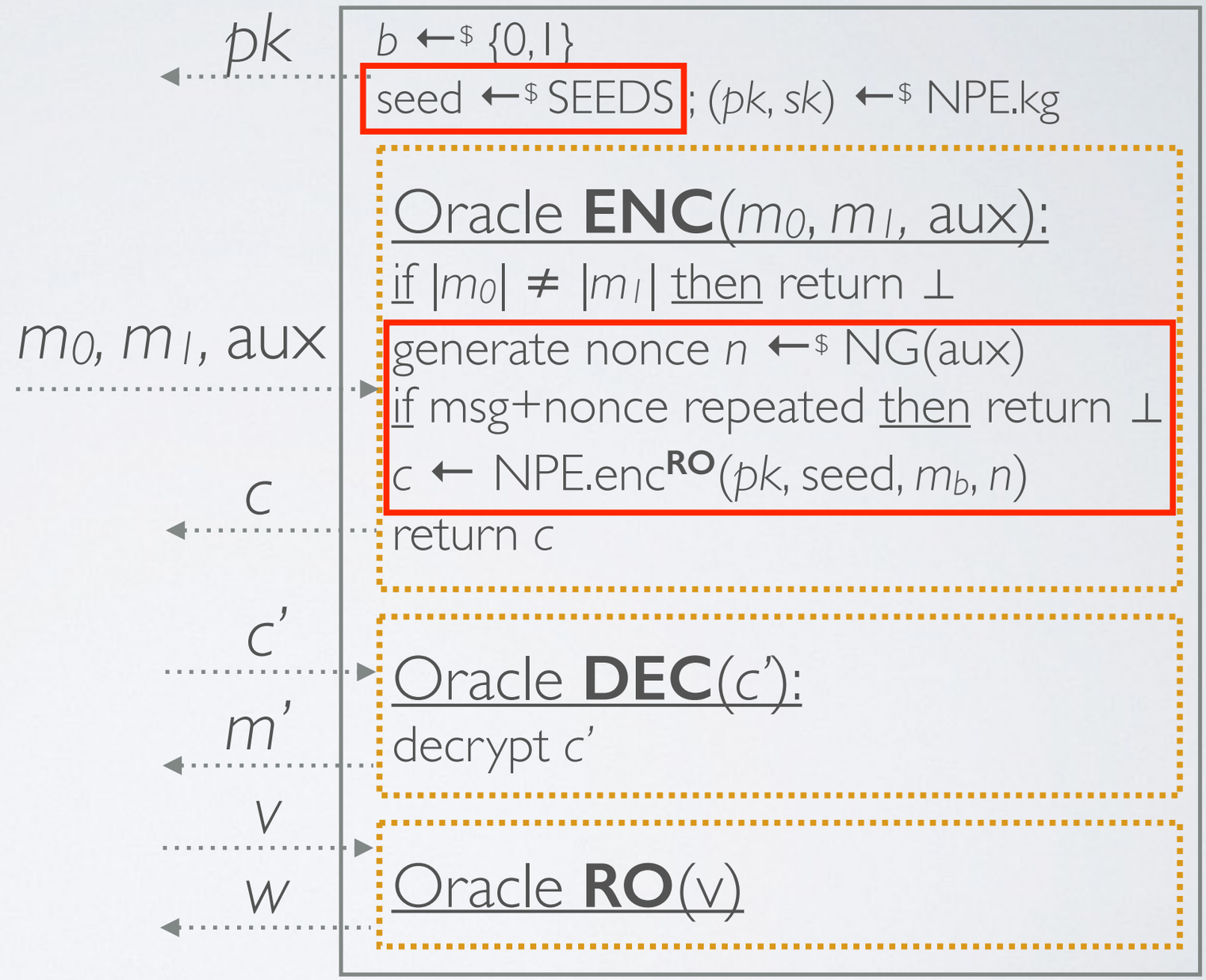
$\mathrm{Adv}^{\mathbf{ror}}(\mathrm{HE}, \mathrm{NG}, \mathcal{A}) \leq q \bullet \varepsilon'(k)$ if $\mathrm{Adv}^{\mathbf{pred}}(\mathrm{NG}, \mathcal{C}) \leq 2^{-k}$

NONCE-BASED PRIVACY, ONE



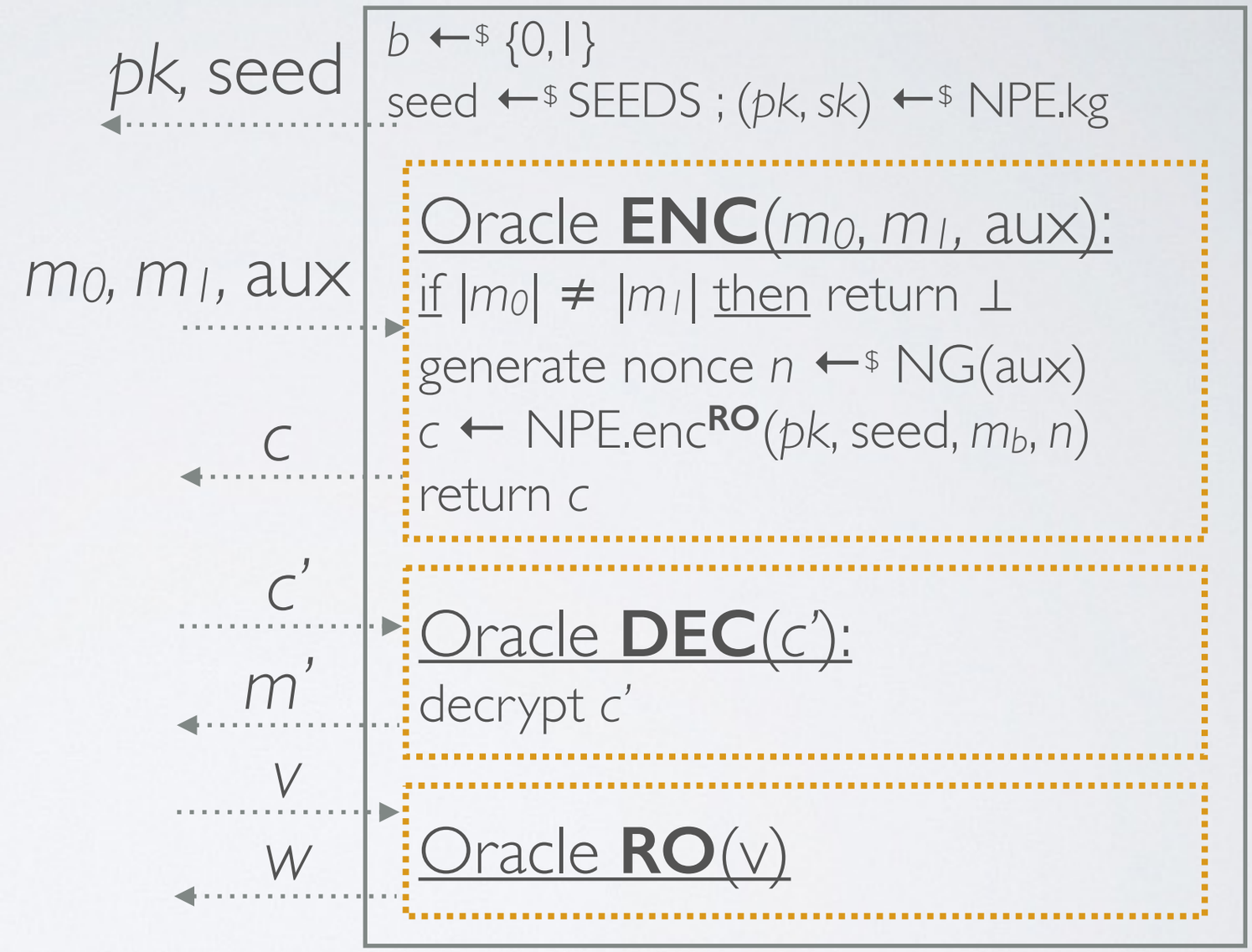
$$\mathrm{Adv}^{\mathbf{nbp1}}(\mathrm{NPE}, \mathcal{A}) \;=\; 2\,\Pr[\, b' \leftarrow\!\!\$\; \mathcal{A}^{\mathbf{ENC},\mathbf{DEC},\mathbf{RO}};\, b = b' \,] - 1$$

NONCE-BASED PRIVACY, ONE



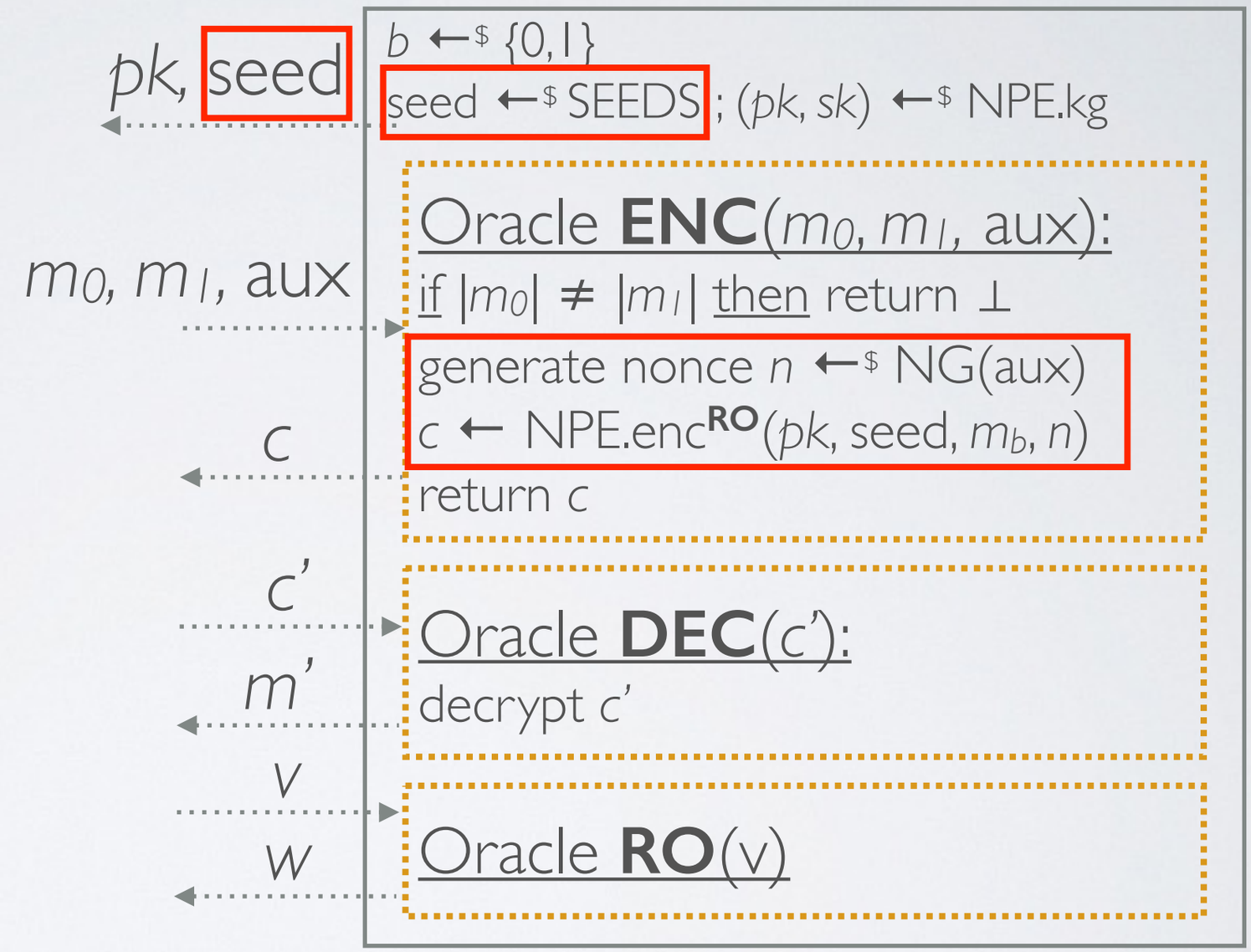
$$\mathrm{Adv}^{\mathbf{nbp1}}(\mathrm{NPE}, \mathcal{A}) \;=\; 2\,\Pr[\, b' \leftarrow\!\!\$\; \mathcal{A}^{\mathbf{ENC},\mathbf{DEC},\mathbf{RO}};\, b = b' \,] - 1$$

NONCE-BASED PRIVACY, TWO



$$\mathrm{Adv}^{\mathbf{nbp2}}(\mathrm{NPE}, \mathcal{A}) \;=\; 2\,\Pr[\, b' \leftarrow\!\!\$\; \mathcal{A}^{\mathbf{ENC},\mathbf{DEC},\mathbf{RO}};\, b = b' \,] - 1$$

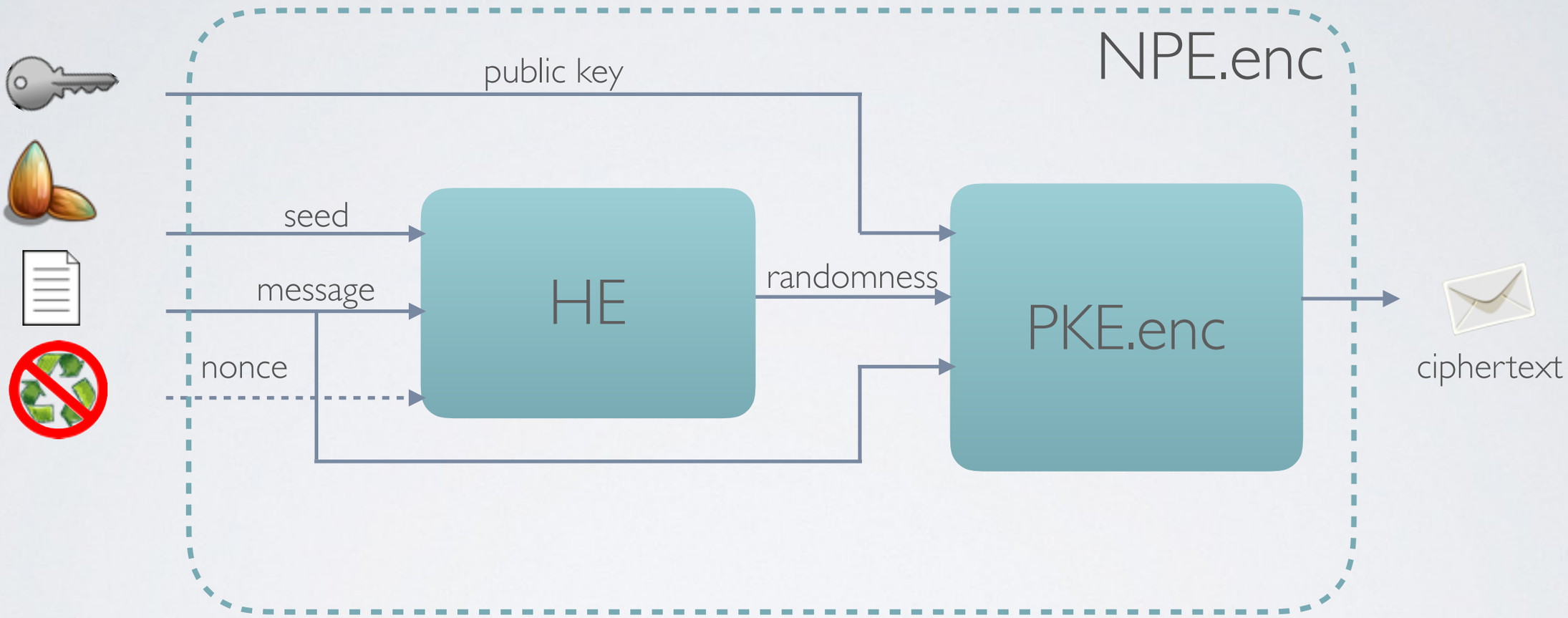
NONCE-BASED PRIVACY, TWO



$$\mathrm{Adv}^{\mathbf{nbp2}}(\mathrm{NPE}, \mathcal{A}) \;=\; 2\,\Pr\left[\, b' \leftarrow\!\!\$\; \mathcal{A}^{\mathbf{ENC},\mathbf{DEC},\mathbf{RO}};\, b = b' \,\right] - 1$$

[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

BUILDING NONCE-BASED PUBLIC-KEY ENCRYPTION



$$\mathrm{Adv}^{\mathbf{nbp1}}(\mathrm{NPE}, \mathcal{A}) \leq 2 \bullet \mathrm{Adv}^{\mathbf{prf}}(\mathrm{HE}, \mathcal{B}) + \mathrm{Adv}^{\mathbf{ind}}(\mathrm{PKE}, \mathcal{C})$$

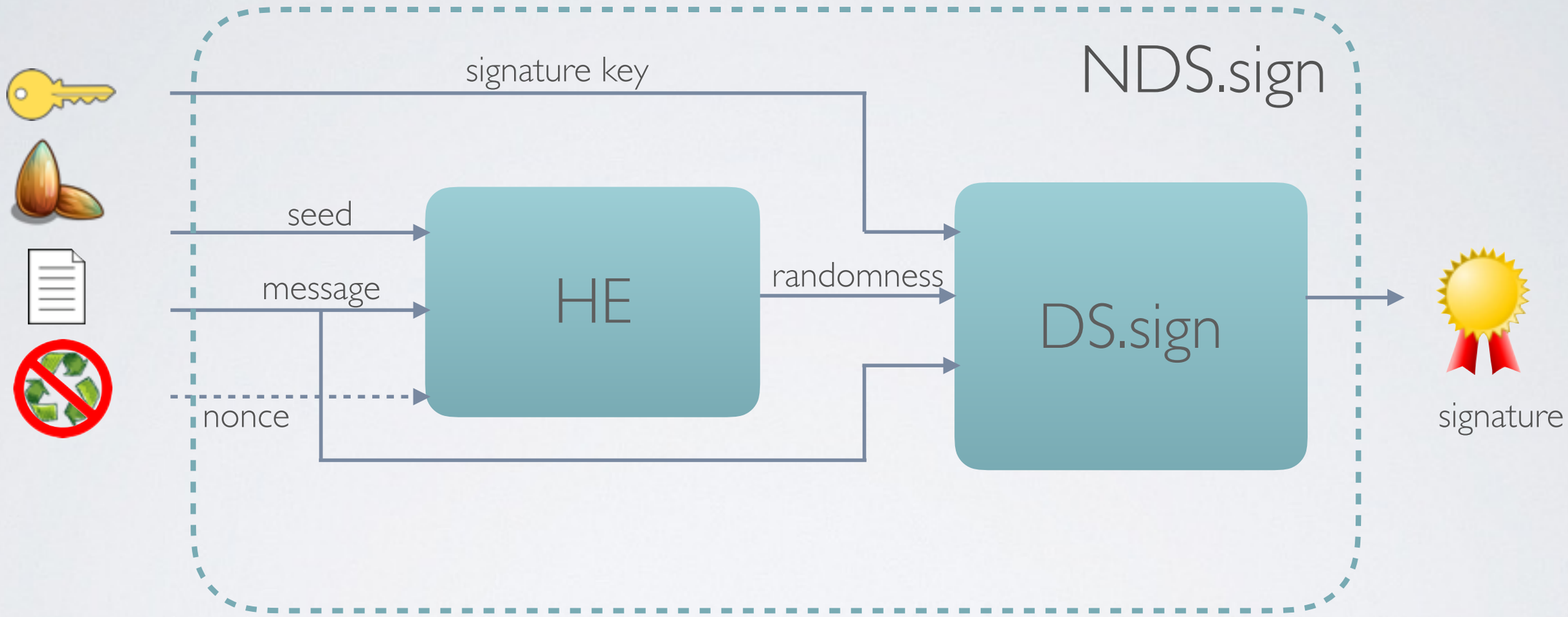
$$\mathrm{Adv}^{\mathbf{nbp2}}(\mathrm{NPE}, \mathcal{A}) \leq 2 \bullet \mathrm{Adv}^{\mathbf{ror}}(\mathrm{HE}, \mathcal{B}) + \mathrm{Adv}^{\mathbf{ind}}(\mathrm{PKE}, \mathcal{C})$$

[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

RELATED APPROACHES

	assumption
standard pke	encryptor has access to fresh uniform randomness
deterministic pke	messages contain a certain entropy
hedged pke	message and nonce *together* have a certain entropy
nonce-based pke	seed secret, nonce unique **or** seed random, nonce entropic

NONCE-BASED SIGNATURES



$$\mathrm{Adv}^{\mathbf{nbuf1}}(\mathrm{NDS}, \mathcal{A}) \leq 2 \bullet \mathrm{Adv}^{\mathbf{prf}}(\mathrm{HE}, \mathcal{B}) + \mathrm{Adv}^{\mathbf{uf}}(\mathrm{DS}, \mathcal{C})$$

$$\mathrm{Adv}^{\mathbf{nbuf2}}(\mathrm{NDS}, \mathcal{A}) \leq 2 \bullet \mathrm{Adv}^{\mathbf{ror}}(\mathrm{HE}, \mathcal{B}) + \mathrm{Adv}^{\mathbf{uf}}(\mathrm{DS}, \mathcal{C})$$

[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

THANKS!

QUESTIONS?

[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

NONCE-BASED UNFORGEABILITY, ONE

$\mathcal{A}$

pk

m, aux

s

V

W

$b \leftarrow^{\$} \{0,1\}$; state $\leftarrow \perp$; seed $\leftarrow^{\$}$ SEEDS
$(pk, sk) \leftarrow^{\$}$ NDS.kg

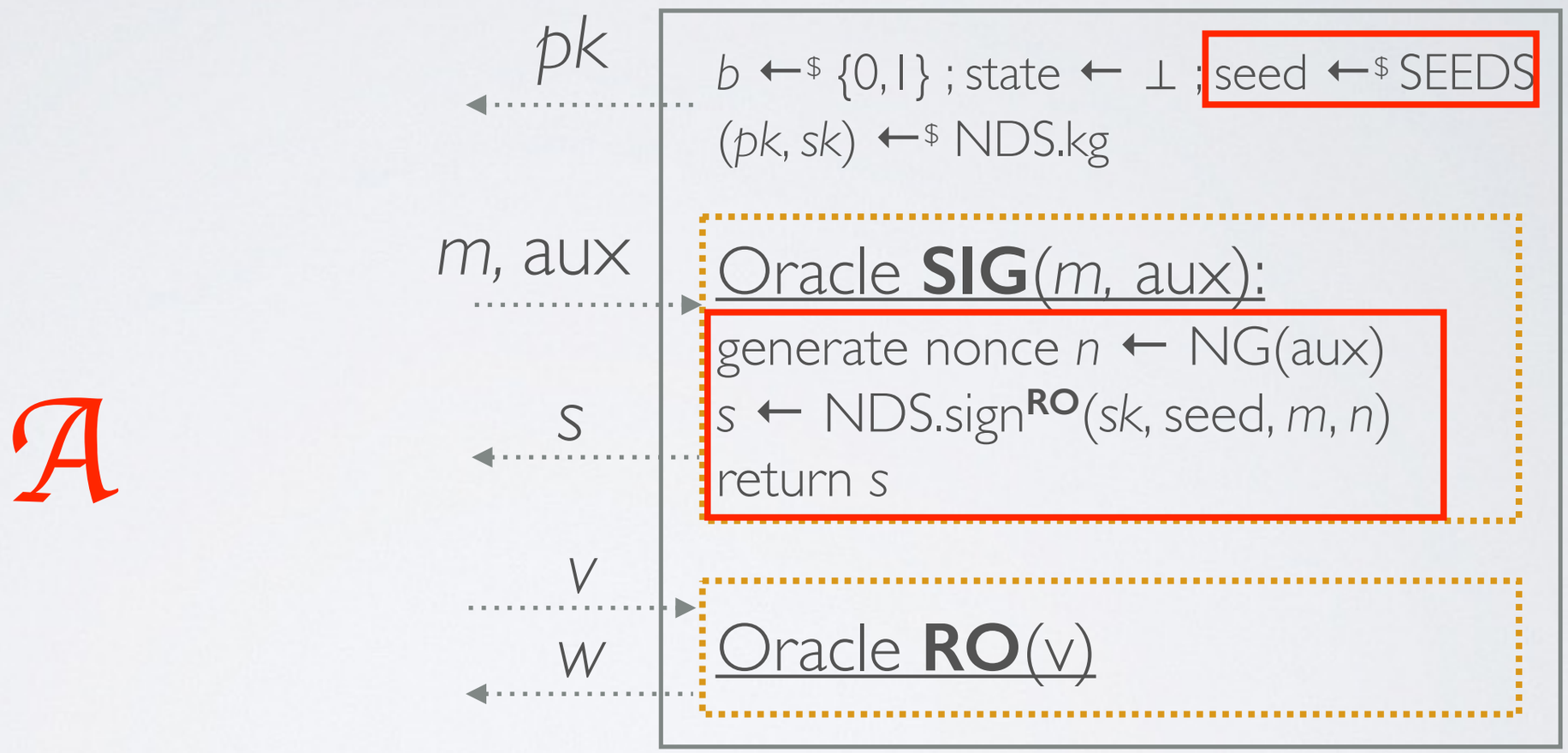
Oracle **SIG**(*m*, aux):
generate nonce $n \leftarrow$ NG(aux)
$s \leftarrow$ NDS.sign$^{\mathbf{RO}}(sk, \text{seed}, m, n)$
return *s*

Oracle **RO**(v)

$$\mathrm{Adv}^{\mathbf{nbufl}}(\mathrm{NDS}, \mathcal{A}) = \Pr[\, s' \leftarrow^{\$} \mathcal{A}^{\mathbf{SIG},\mathbf{RO}};\ s' \text{ valid and fresh }]$$

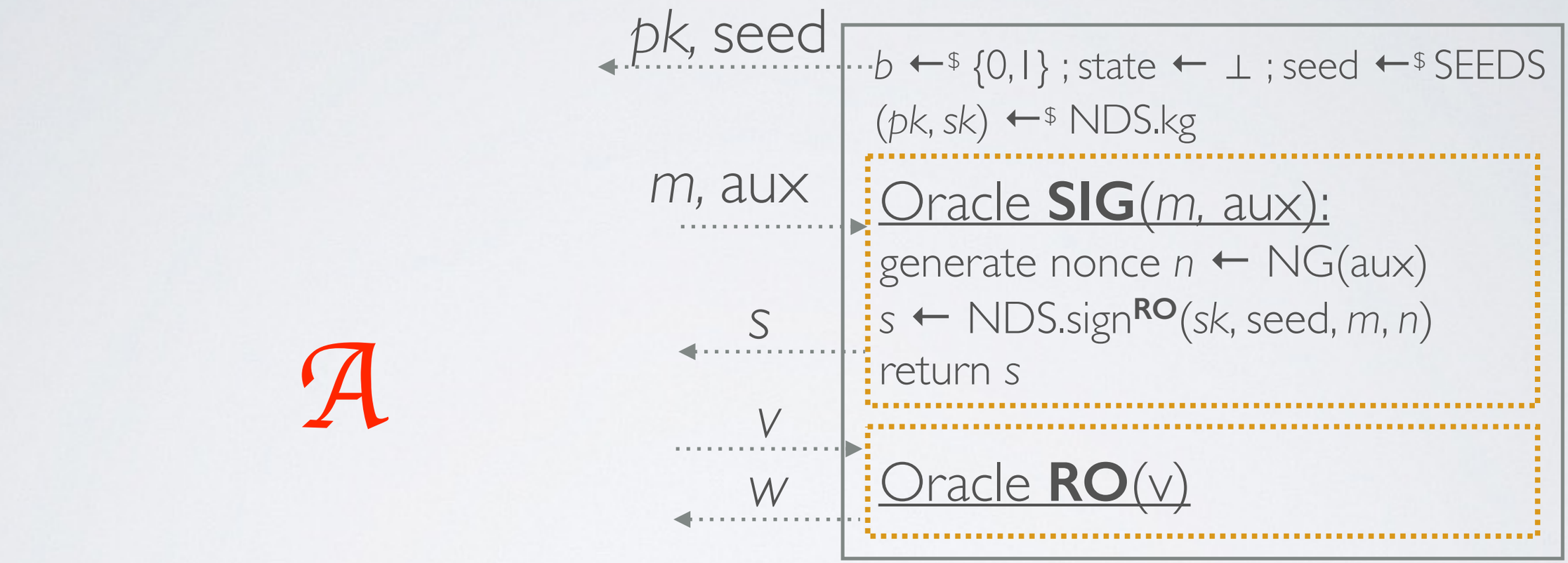
[Bellare-Tackmann, EC 2016, Nonce-based Cryptography]

NONCE-BASED UNFORGEABILITY, ONE



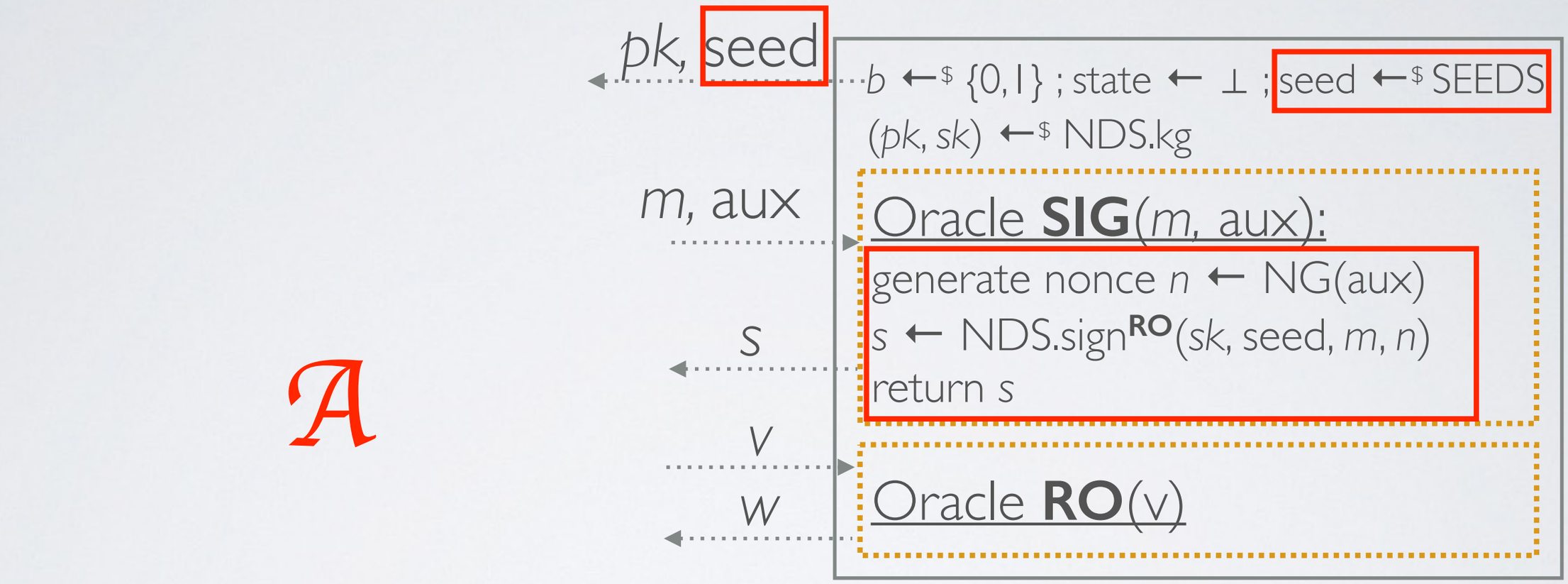
$$\mathrm{Adv}^{\mathbf{nbufl}}(\mathrm{NDS}, \mathcal{A}) \;=\; \Pr\left[\, s' \leftarrow\!\!\$\ \mathcal{A}^{\mathbf{SIG},\mathbf{RO}};\ s' \text{ valid and fresh} \,\right]$$

NONCE-BASED UNFORGEABILITY, TWO



$$\mathrm{Adv}^{\mathbf{nbuf2}}(\mathrm{NDS}, \mathcal{A}) \;=\; \Pr\left[\, s' \leftarrow\!\!\$\ \mathcal{A}^{\mathbf{SIG},\mathbf{RO}};\ s' \text{ valid and fresh} \,\right]$$

NONCE-BASED UNFORGEABILITY, TWO



$$\mathrm{Adv}^{\mathbf{nbuf2}}(\mathrm{NDS}, \mathcal{A}) = \Pr[\, s' \leftarrow\!\!\$\ \mathcal{A}^{\mathbf{SIG},\mathbf{RO}};\ s' \text{ valid and fresh }]$$