CCA2 Key-Privacy for Code-Based Encryption in the Standard Model

Yusuke Yoshida
with Kirill Morozov and Keisuke Tanaka
from Tokyo Institute of Technology, Japan

Contents

Key-Privacy for PKE

Indistinguishability of keys (IK)

Contents

Key-Privacy for PKE

Indistinguishability of keys (IK)

Code-Based Encryption

Niederreiter

Contents

Key-Privacy for PKE

Indistinguishability of keys (IK)

Code-Based Encryption

Niederreiter

CCA2 secure PKE in the standard model

k-repetition paradigm

Contents

Key-Privacy for PKE

Indistinguishability of keys (IK)

Code-Based Encryption

Niederreiter

CCA2 secure PKE in the standard model

k-repetition paradigm

Our result:

CCA2 Key-Privacy for Code-Based Encryption in the Standard Model

We proved that the k-repetition paradigm instantiated with Niederreiter is IK-CCA2 in the standard model.

Contents

Key-Privacy for PKE

Indistinguishability of keys (IK)

Code-Based Encryption

Niederreiter

CCA2 secure PKE in the standard model

k-repetition paradigm

Our result:

CCA2 Key-Privacy for Code-Based Encryption in the Standard Model

We proved that the k-repetition paradigm instantiated with Niederreiter is IK-CCA2 in the standard model.

Key-Privacy (Anonymity) for PKE

Indistinguishability of keys (IK)

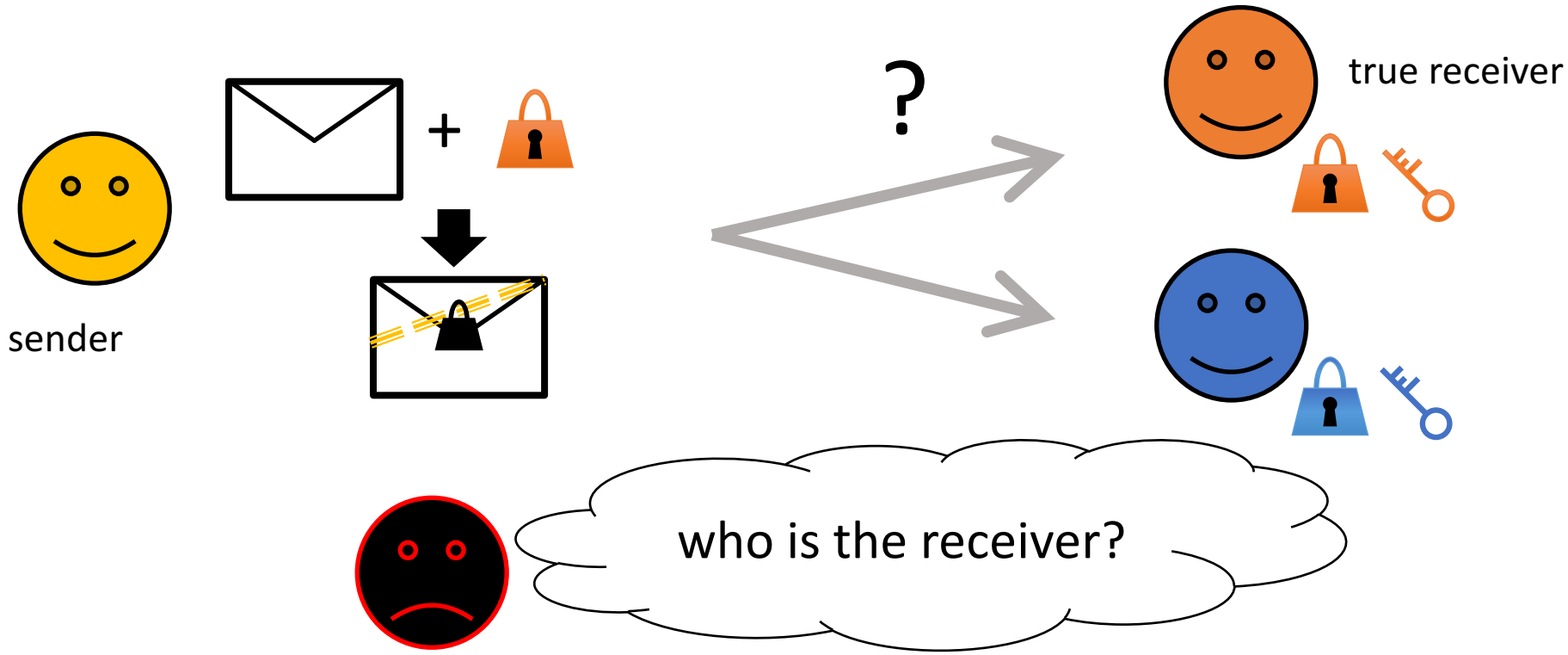
- was proposed by Bellare et al.*

*Bellare, M., Boldyreva, A., Desai, A., Pointcheval, D.: Key-privacy in public-key encryption. In: Boyd, C. (ed.) ASIACRYPT 2001.

Key-Privacy (Anonymity) for PKE

Indistinguishability of keys (IK)

- was proposed by Bellare et al.*
- means a ciphertext does not leak information about pk.



*Bellare, M., Boldyreva, A., Desai, A., Pointcheval, D.: Key-privacy in public-key encryption. In: Boyd, C. (ed.) ASIACRYPT 2001.

Key-Privacy (Anonymity) for PKE

Indistinguishability of keys (IK)

- was proposed by Bellare et al.*
- means a ciphertext does not leak information about pk.
- against CPA, CCA2 could be considered.

IK-CPA < IK-CCA2

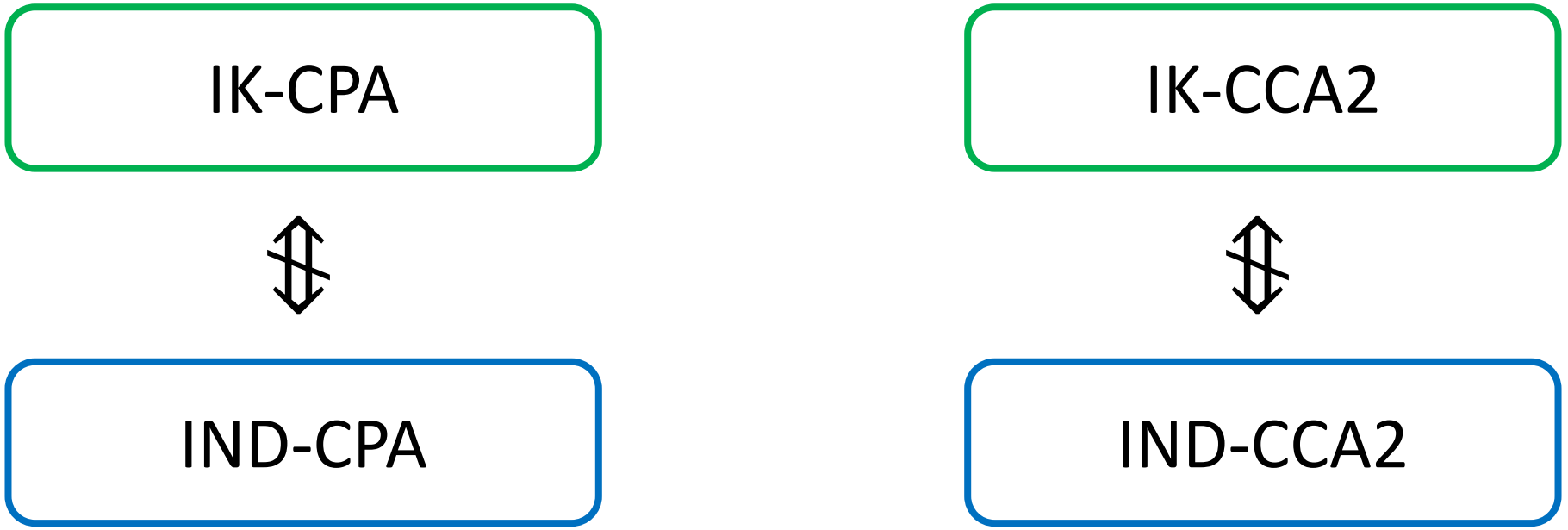
cf.) IND-CPA < IND-CCA2

*Bellare, M., Boldyreva, A., Desai, A., Pointcheval, D.: Key-privacy in public-key encryption. In: Boyd, C. (ed.) ASIACRYPT 2001.

Key-Privacy (Anonymity) for PKE

Indistinguishability of keys (IK)

- was proposed by Bellare et al.*
- means a ciphertext does not leak information about pk.
- against CPA, CCA2 could be considered.
- does not imply / is not implied by IND security.



*Bellare, M., Boldyreva, A., Desai, A., Pointcheval, D.: Key-privacy in public-key encryption. In: Boyd, C. (ed.) ASIACRYPT 2001.

Definition of IK-CPA

$pk_0, sk_0 \leftarrow Gen(1^\lambda)$

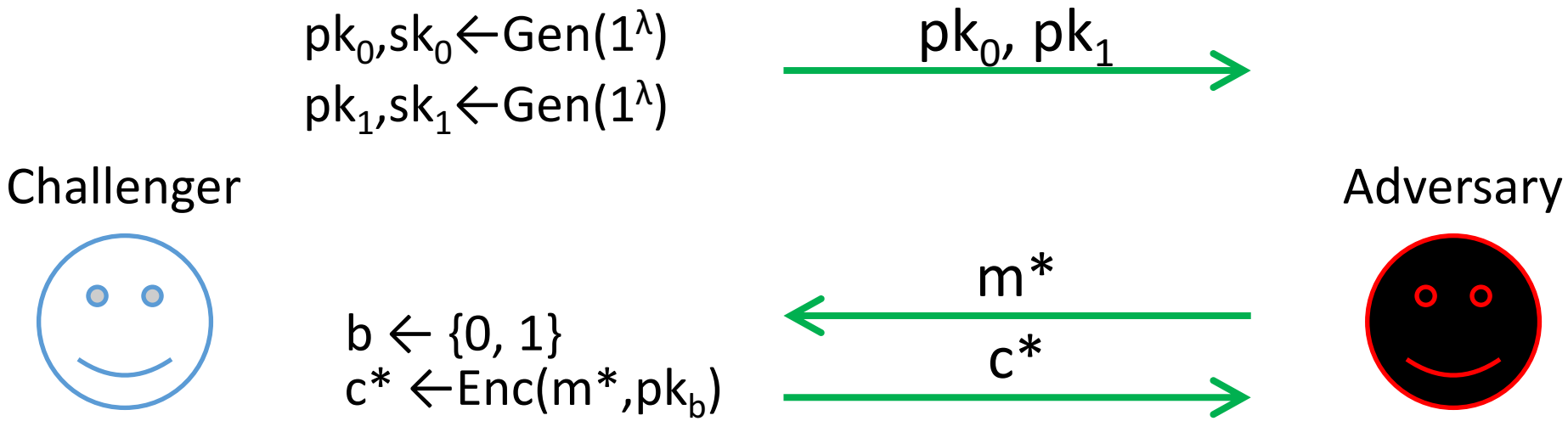
$pk_1, sk_1 \leftarrow Gen(1^\lambda)$

pk_0, pk_1 →

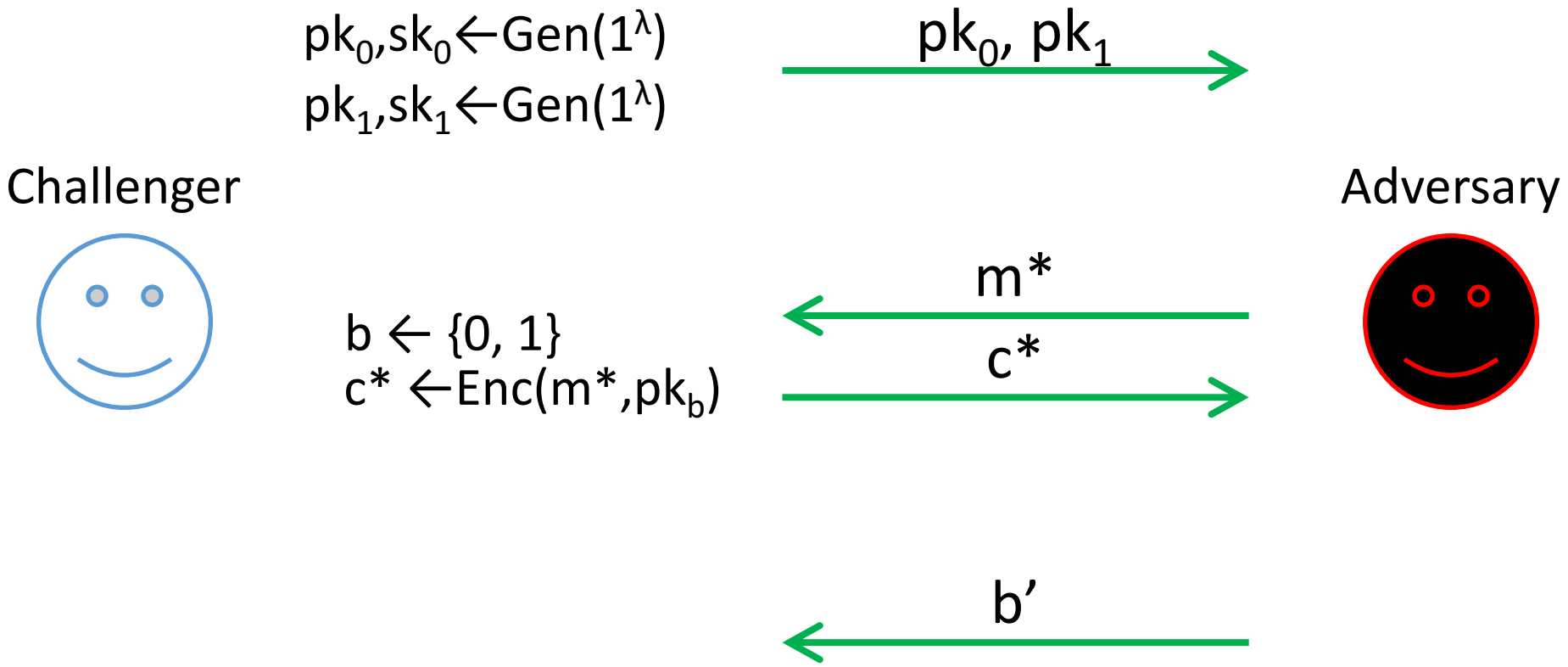
Challenger

Adversary

Definition of IK-CPA



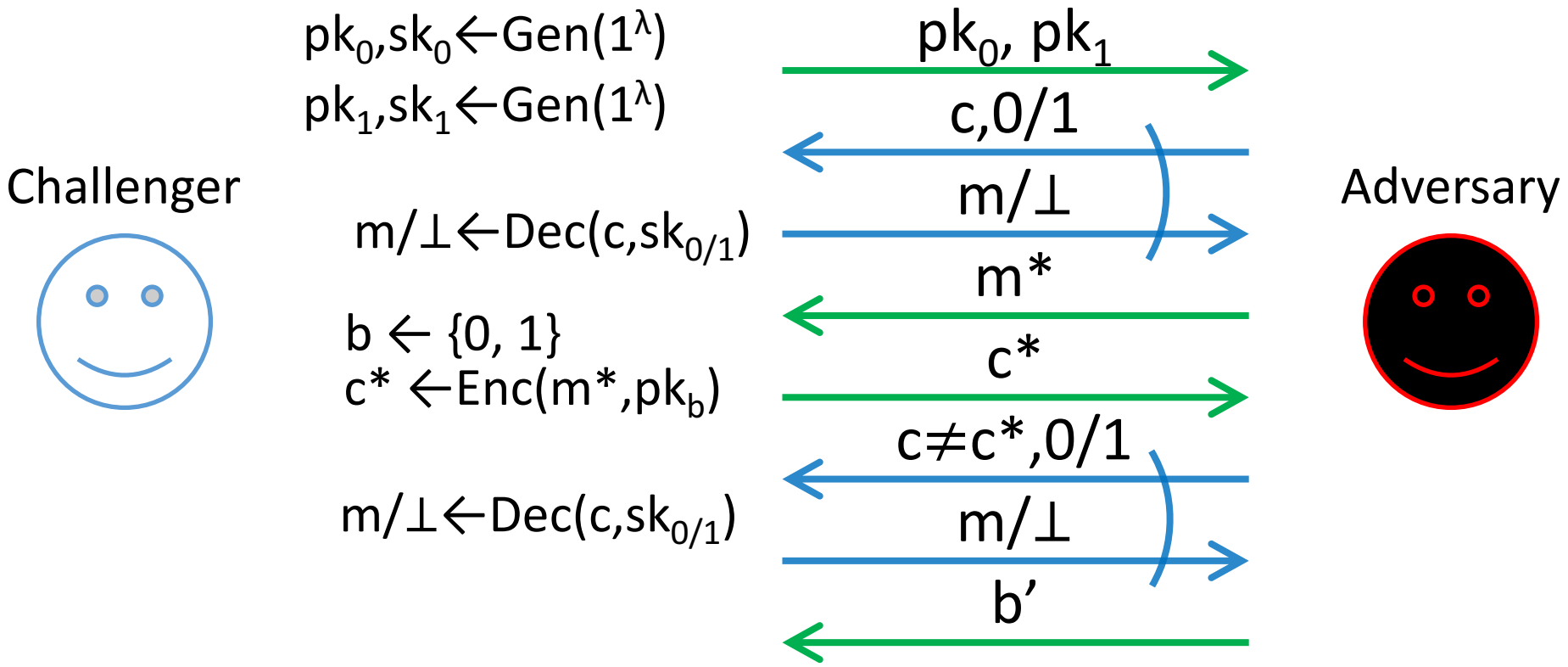
Definition of IK-CPA



A PKE is IK-CPA

$\Leftrightarrow |Pr[b = b'] - ½|$ is negligible

Definition of IK-CCA2



A PKE is IK-CCA2

$\Leftrightarrow |Pr[b = b'] - ½|$ is negligible

Contents

Key-Privacy for PKE

Indistinguishability of keys (IK)

Code-Based Encryption

Niederreiter

CCA2 secure PKE in the standard model

k-repetition paradigm

Our result:

CCA2 Key-Privacy for Code-Based Encryption in the Standard Model

We proved that the k-repetition paradigm instantiated with Niederreiter is IK-CCA2 in the standard model.

Linear Codes

A binary $[n, k]$ linear code $\mathcal{C}$

is a k-dimensional subspace of $\mathbb{F}_2^n$.

Linear Codes

A binary $[n, k]$ linear code $\mathcal{C}$

is a k-dimensional subspace of $\mathbb{F}_2^n$.

$= \{xG \in \mathbb{F}_2^n | \ x \in \mathbb{F}_2^k\}$ for a generator matrix G.

→ McEliece encryption.

Linear Codes

A binary $[n, k]$ linear code $\mathcal{C}$

is a k-dimensional subspace of $\mathbb{F}_2^n$.

$= \{xG \in \mathbb{F}_2^n \mid x \in \mathbb{F}_2^k\}$ for a generator matrix G.

⟶ McEliece encryption.

$= \{x \in \mathbb{F}_2^n \mid Hx^T = 0\}$ for a parity check matrix H.

⟶ Niederreiter encryption.

Linear Codes

A binary $[n, k]$ linear code $\mathcal{C}$

is a k-dimensional subspace of $\mathbb{F}_2^n$.

$= \{xG \in \mathbb{F}_2^n \mid x \in \mathbb{F}_2^k\}$ for a generator matrix G.

⟶ McEliece encryption.

$= \{x \in \mathbb{F}_2^n \mid Hx^T = 0\}$ for a parity check matrix H.

⟶ Niederreiter encryption.

Linear Codes

A binary $[n, k]$ linear code $\mathcal{C}$

is a k-dimensional subspace of $\mathbb{F}_2^n$.

$= \{xG \in \mathbb{F}_2^n \mid x \in \mathbb{F}_2^k\}$ for a generator matrix G.

⟶ McEliece encryption.

$= \{x \in \mathbb{F}_2^n \mid Hx^T = 0\}$ for a parity check matrix H.

⟶ Niederreiter encryption.

is error-correcting up to Hamming weight t.

⇔ Can compute x from syndrome $s = Hx^T$, if $wt(x) \leq t$.

Syndrome Decoding Problem

Syndrome Decoding Problem
Given a parity check matrix of random code R and a syndrome $s = Rx^T$ for a random low-weight error x. Find x.

*Fischer, J.-B., Stern, J.: An efficient pseudo-random generator provably as secure as syndrome decoding. In: Maurer, U. (ed.) EUROCRYPT 1996.

Syndrome Decoding Problem

Syndrome Decoding Problem

Given a parity check matrix of random code R and a syndrome $s = Rx^T$ for a random low-weight error x. Find x.

Decisional version of SD problem

Given (R,u) where u is a uniform random vector or (R, s), where $s = Rx^T$ as above.

Decide, which is the case.

If SD problem is hard, the decisional version is also hard*.

*Fischer, J.-B., Stern, J.: An efficient pseudo-random generator provably as secure as syndrome decoding. In: Maurer, U. (ed.) EUROCRYPT 1996.

Niederreiter*

Key generation H': parity check matrix of t-error correcting code.

S: random non-singular matrix, P: random permutation matrix

Public key $pk = H = SH'P$

(We assume H is indistinguishable from random R)

Secret key $sk = (S, H', P)$

*Niederreiter, H.: Knapsack-type cryptosystems and algebraic coding theory. Probl. Control Inf. Theory-Probl. Upravleniya I Teorii Informatsii 15(2), 159–166 (1986)

Niederreiter*

Key generation H': parity check matrix of t-error correcting code.

S: random non-singular matrix, P: random permutation matrix

Public key $pk = H = SH'P$

(We assume H is indistinguishable from random R)

Secret key $sk = (S, H', P)$

Encryption Plaintext is $m \in \mathbb{F}_2^n, wt(m) \leq t.$

Ciphertext is $c = Hm^T$

*Niederreiter, H.: Knapsack-type cryptosystems and algebraic coding theory. Probl. Control Inf. Theory-Probl. Upravleniya I Teorii Informatsii 15(2), 159–166 (1986)

Niederreiter*

Key generation H': parity check matrix of t-error correcting code.

S: random non-singular matrix, P: random permutation matrix

Public key $pk = H = SH'P$

(We assume H is indistinguishable from random R)

Secret key $sk = (S, H', P)$

Encryption Plaintext is $m \in \mathbb{F}_2^n, wt(m) \leq t.$

Ciphertext is $c = Hm^T$

Decryption Compute $P^{-1}Correct(S^{-1}c) = P^{-1}Pm^T = m^T$

$Correct$ is the error correction algorithm for H'.

*Niederreiter, H.: Knapsack-type cryptosystems and algebraic coding theory. Probl. Control Inf. Theory-Probl. Upravleniya I Teorii Informatsii 15(2), 159–166 (1986)

Randomized Niederreiter*

Key generation H': parity check matrix of t-error correcting code.

S: random non-singular matrix, P: random permutation matrix

Public key $pk = H = SH'P$

(We assume H is indistinguishable from random R)

Secret key $sk = (S, H', P)$

Encryption Plaintext is m, Take a random padding vector r

$m||r \in \mathbb{F}_2^n, wt(m||r) \leq t.$

Ciphertext is $c = H(m||r)^T$

Decryption Compute $P^{-1}Correct(S^{-1}c) = P^{-1}P(m||r)^T = (m||r)^T$

Pick m from $(m||r)^T$.

*Nojima, R., Imai, H., Kobara, K., Morozov, K.: Semantic security for the McEliece cryptosystem without random oracles. Des. Codes Crypt. 49(1–3), 289–305 (2008)

Key-Privacy for Code-Based Encryption

Yamakawa et al.* first studied key-privacy for code-based encryption, and show

	not IK-CPA	IK-CPA	IK-CCA2
	McEliece		

*Yamakawa, S., Cui, Y., Kobara, K., Hagiwara, M., Imai, H.: On the key-privacy issue of McEliece public-key encryption. In: Boztaş, S., Lu, H.-F.F. (eds.) AAECC 2007.

Key-Privacy for Code-Based Encryption

Yamakawa et al.* first studied key-privacy for code-based encryption, and show

	not IK-CPA	IK-CPA	IK-CCA2
	McEliece	Randomized McEliece	

*Yamakawa, S., Cui, Y., Kobara, K., Hagiwara, M., Imai, H.: On the key-privacy issue of McEliece public-key encryption. In: Boztaş, S., Lu, H.-F.F. (eds.) AAECC 2007.

Key-Privacy for Code-Based Encryption

Yamakawa et al.* first studied key-privacy for code-based encryption, and show

	not IK-CPA	IK-CPA	IK-CCA2
Standard Model	McEliece	Randomized McEliece	
Random Oracle			Kobara and Imai's conversion† Persichetti's hybrid encryption‡

*Yamakawa, S., Cui, Y., Kobara, K., Hagiwara, M., Imai, H.: On the key-privacy issue of McEliece public-key encryption. In: Boztaş, S., Lu, H.-F.F. (eds.) AAECC 2007.

†Kobara, K., Imai, H.: Semantically secure McEliece public-key cryptosystems-conversions for McEliece PKC. In: Kim, K. (ed.) PKC 2001.

‡Persichetti, E.: Secure and anonymous hybrid encryption from coding theory. In: Gaborit, P. (ed.) PQCrypto 2013.

Key-Privacy for Code-Based Encryption

Yamakawa et al.* first studied key-privacy for code-based encryption, and show

	not IK-CPA	IK-CPA	IK-CCA2
Standard Model	McEliece	Randomized McEliece	?
Random Oracle			Kobara and Imai's conversion† Persichetti's hybrid encryption‡

IK-CCA2 for code-based encryption in the standard model?

*Yamakawa, S., Cui, Y., Kobara, K., Hagiwara, M., Imai, H.: On the key-privacy issue of McEliece public-key encryption. In: Boztaş, S., Lu, H.-F.F. (eds.) AAECC 2007.

†Kobara, K., Imai, H.: Semantically secure McEliece public-key cryptosystems-conversions for McEliece PKC. In: Kim, K. (ed.) PKC 2001.

‡Persichetti, E.: Secure and anonymous hybrid encryption from coding theory. In: Gaborit, P. (ed.) PQCrypto 2013.

Contents

Key-Privacy for PKE

Indistinguishability of keys (IK)

Code-Based Encryption

Niederreiter

CCA2 secure PKE in the standard model

k-repetition paradigm

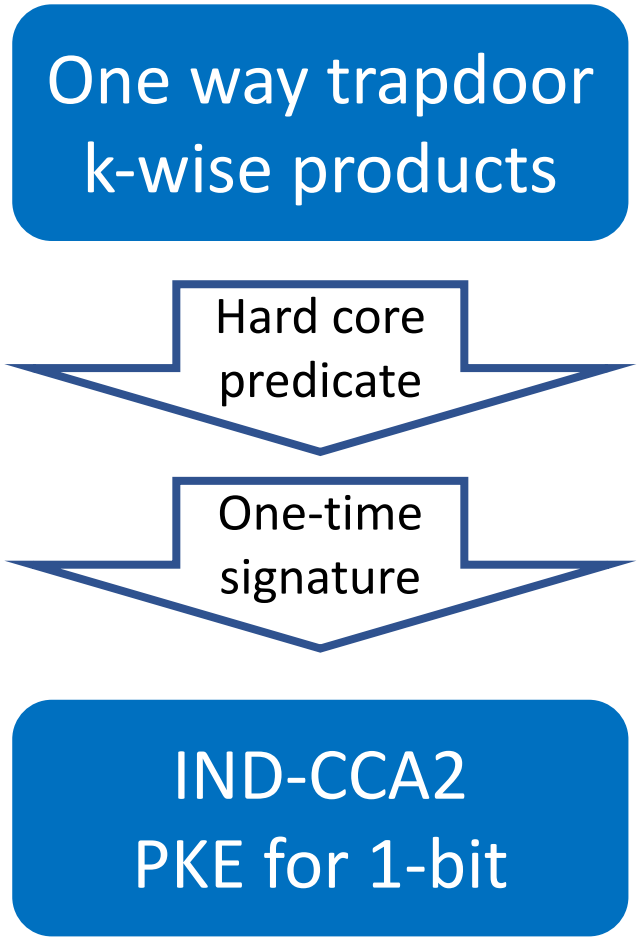
Our result:

CCA2 Key-Privacy for Code-Based Encryption in the Standard Model

We proved that the k-repetition paradigm instantiated with Niederreiter is IK-CCA2 in the standard model.

k-repetition Paradigm

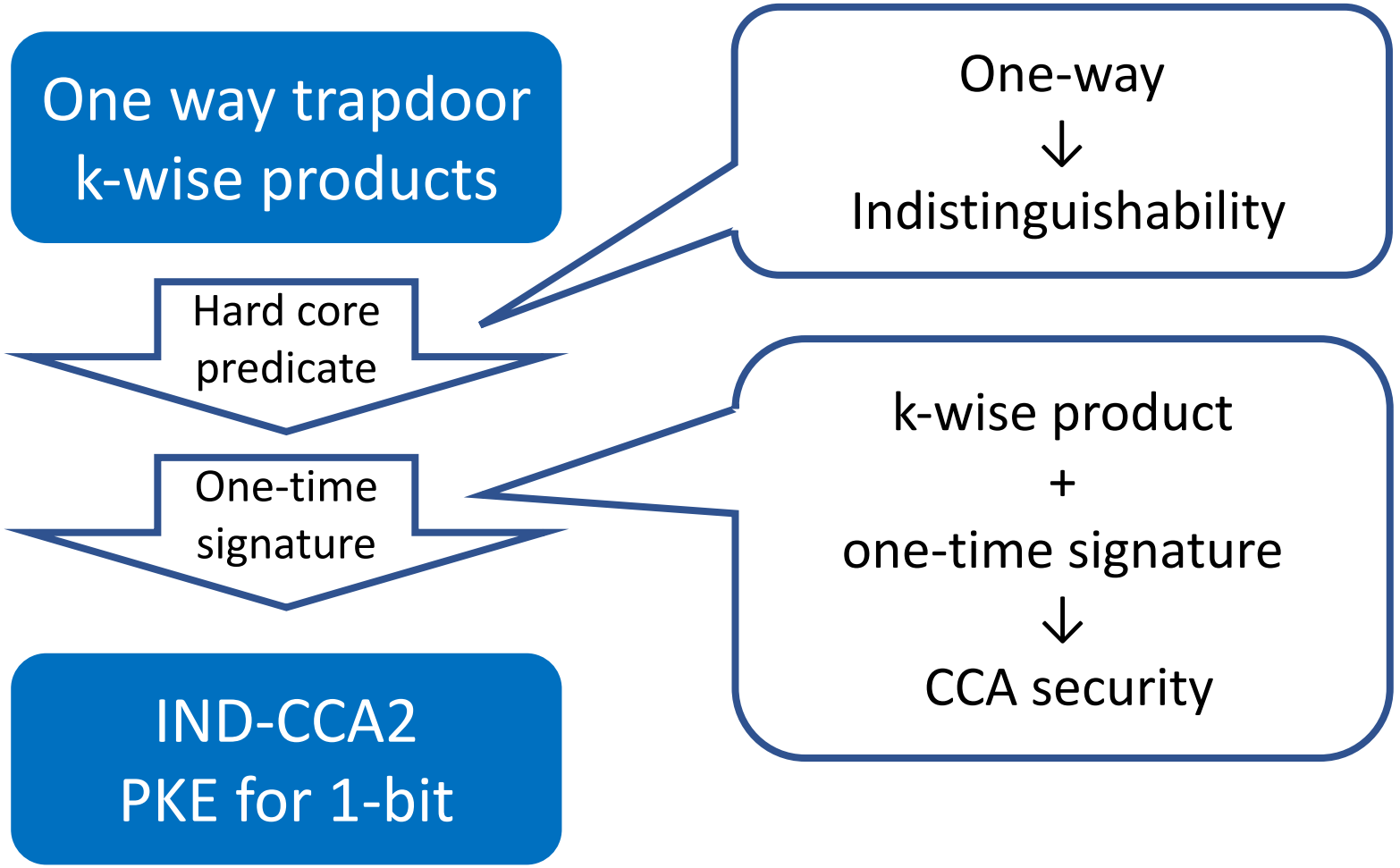
Rosen and Segev*



*Rosen, A., Segev, G.: Chosen-ciphertext security via correlated products. In: Reingold, O. (ed.) TCC 2009.

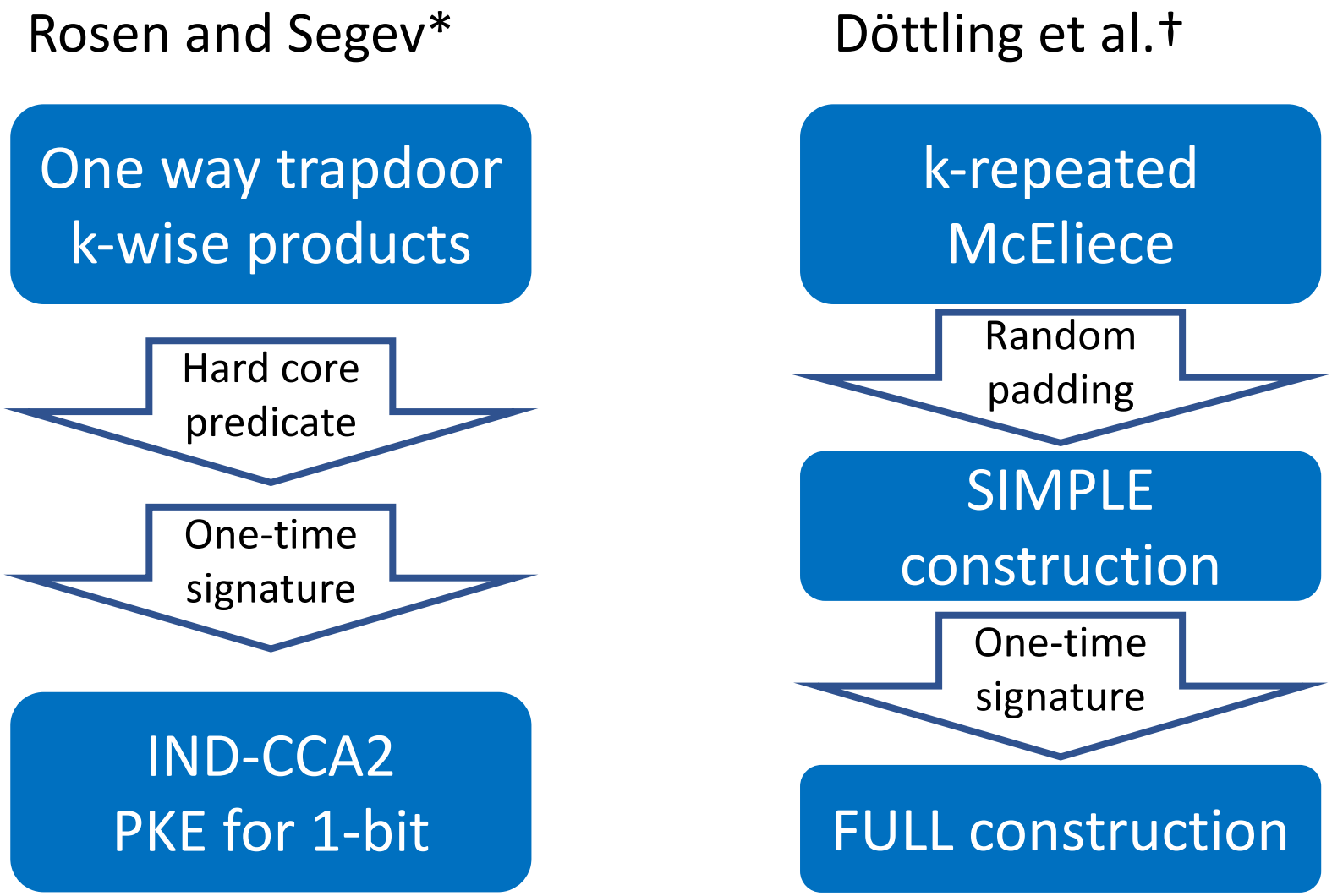
k-repetition Paradigm

Rosen and Segev*



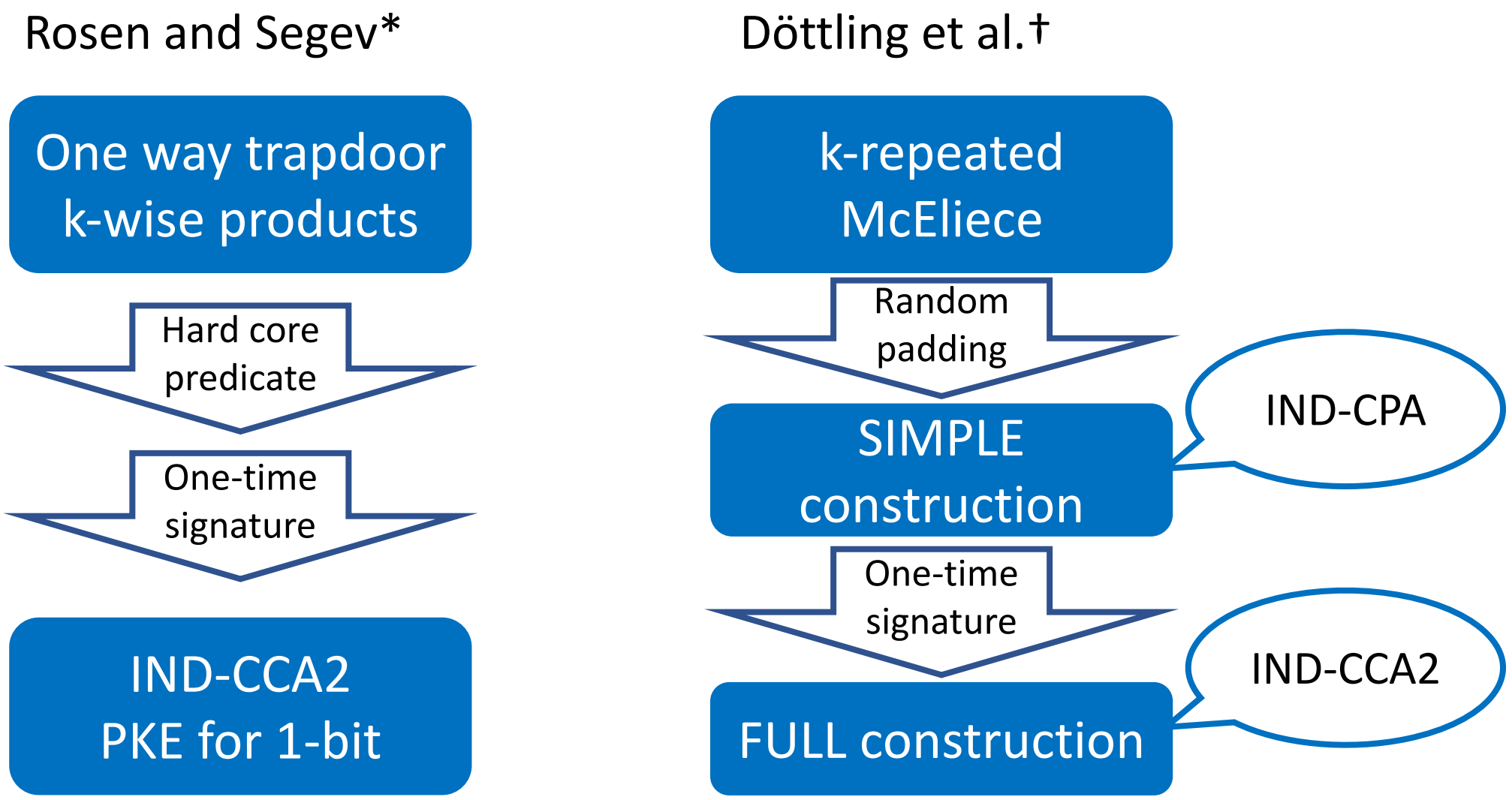
*Rosen, A., Segev, G.: Chosen-ciphertext security via correlated products. In: Reingold, O. (ed.) TCC 2009.

Code-Based CCA Construction



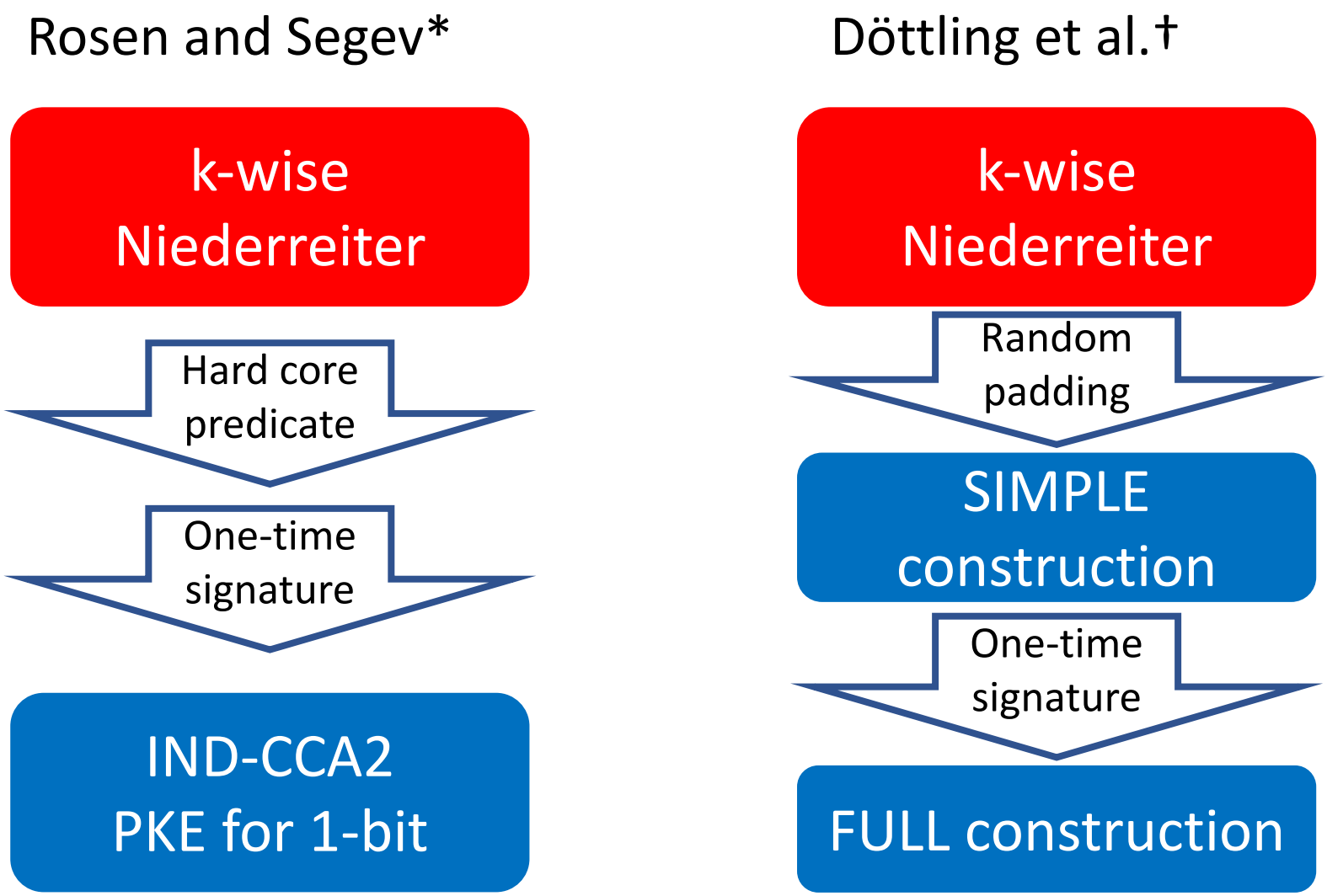
*Rosen, A., Segev, G.: Chosen-ciphertext security via correlated products. In: Reingold, O. (ed.) TCC 2009.
†Döttling, N., Dowsley, R., Muller-Quade, J., Nascimento, A.C.A.: A CCA2 secure variant of the mceliece cryptosystem. IEEE Trans. Inf. Theory 58(10), 6672–6680 (2012)

Code-Based CCA Construction



*Rosen, A., Segev, G.: Chosen-ciphertext security via correlated products. In: Reingold, O. (ed.) TCC 2009.
†Döttling, N., Dowsley, R., Muller-Quade, J., Nascimento, A.C.A.: A CCA2 secure variant of the mceliece cryptosystem. IEEE Trans. Inf. Theory 58(10), 6672–6680 (2012)

Code-Based CCA Construction



*Rosen, A., Segev, G.: Chosen-ciphertext security via correlated products. In: Reingold, O. (ed.) TCC 2009.
†Döttling, N., Dowsley, R., Muller-Quade, J., Nascimento, A.C.A.: A CCA2 secure variant of the mceliece cryptosystem. IEEE Trans. Inf. Theory 58(10), 6672–6680 (2012)

Contents

Key-Privacy for PKE

Indistinguishability of keys (IK)

Code-Based Encryption

Niederreiter

CCA2 secure PKE in the standard model

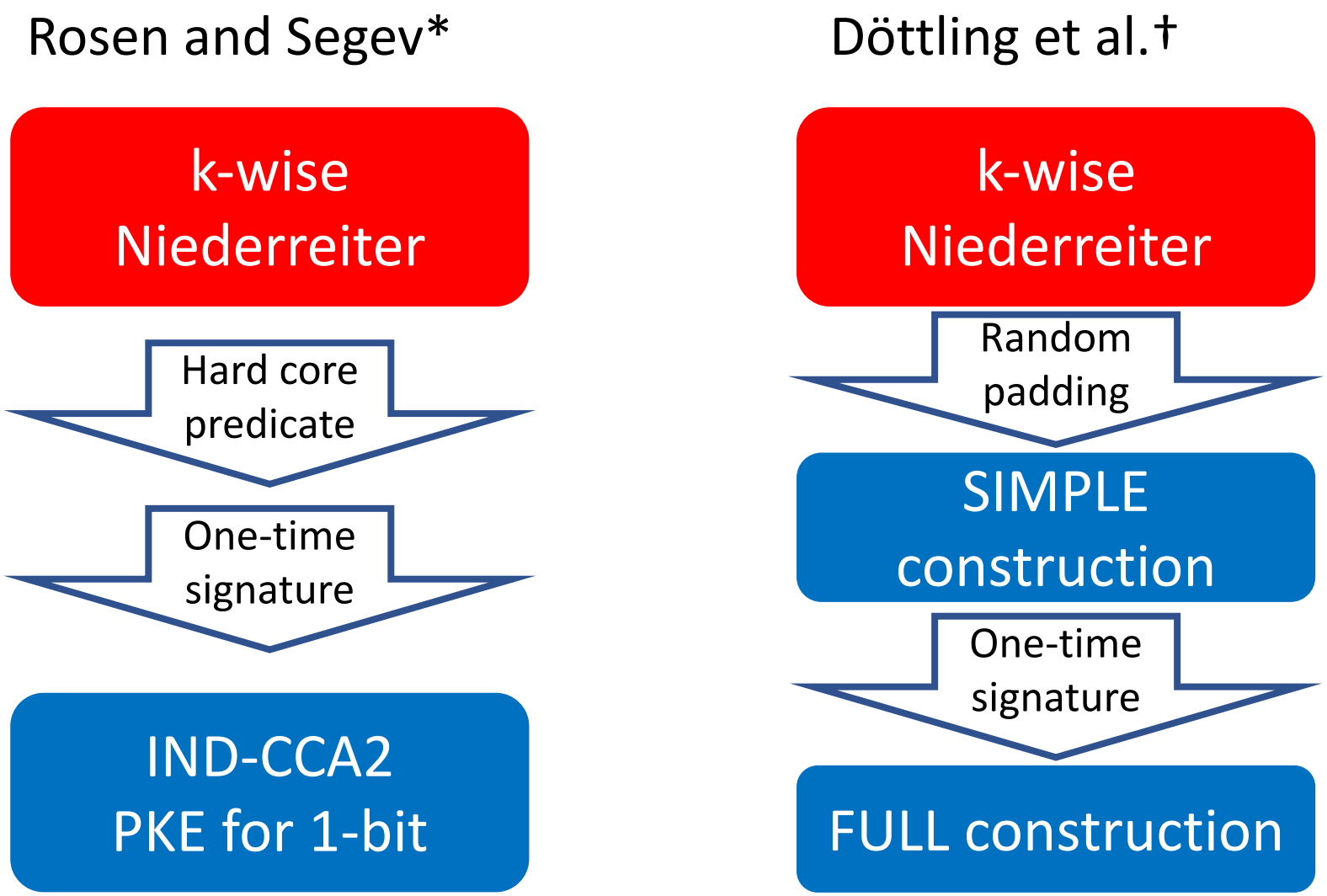
k-repetition paradigm

Our result:

CCA2 Key-Privacy for Code-Based Encryption in the Standard Model

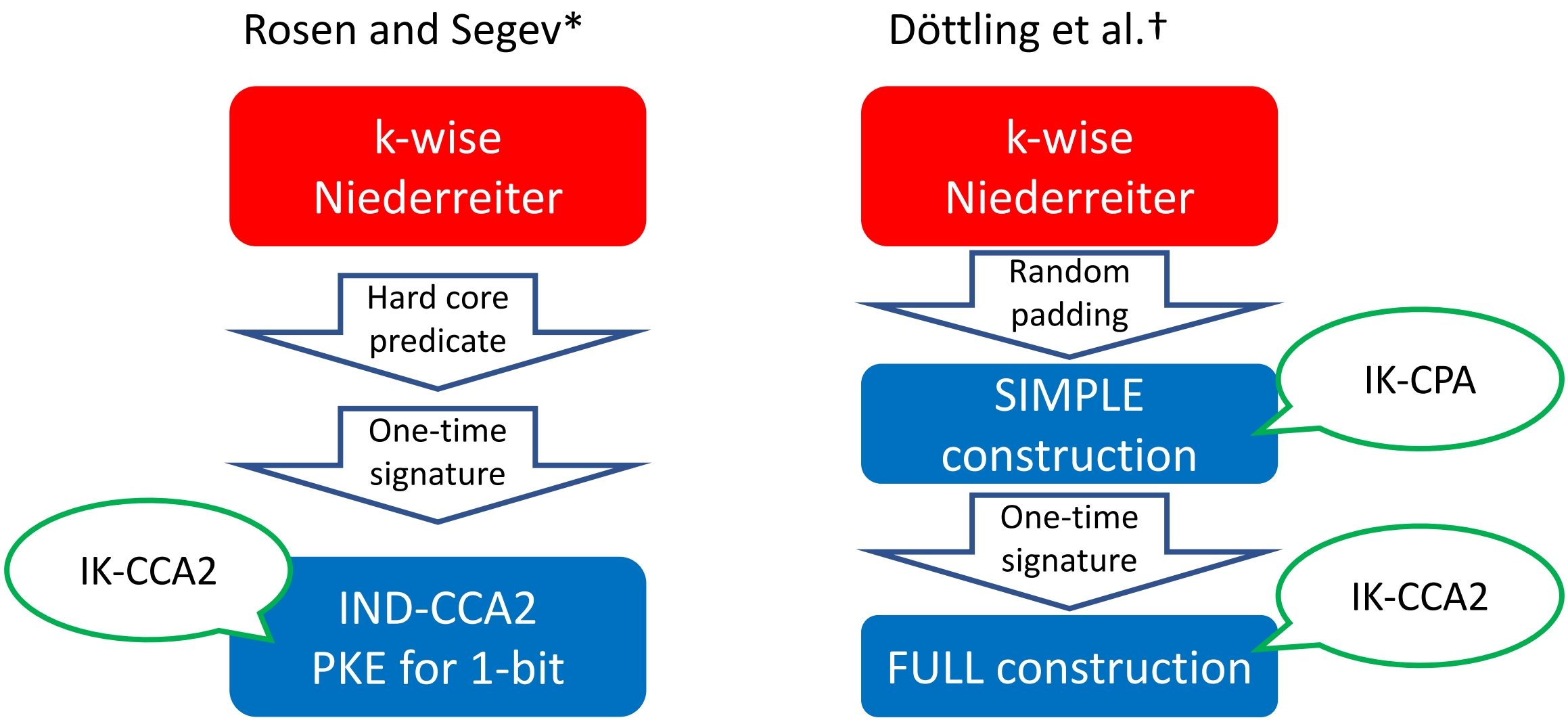
We proved that the k-repetition paradigm instantiated with Niederreiter is IK-CCA2 in the standard model.

Instantiation with Niederreiter and its key-privacy



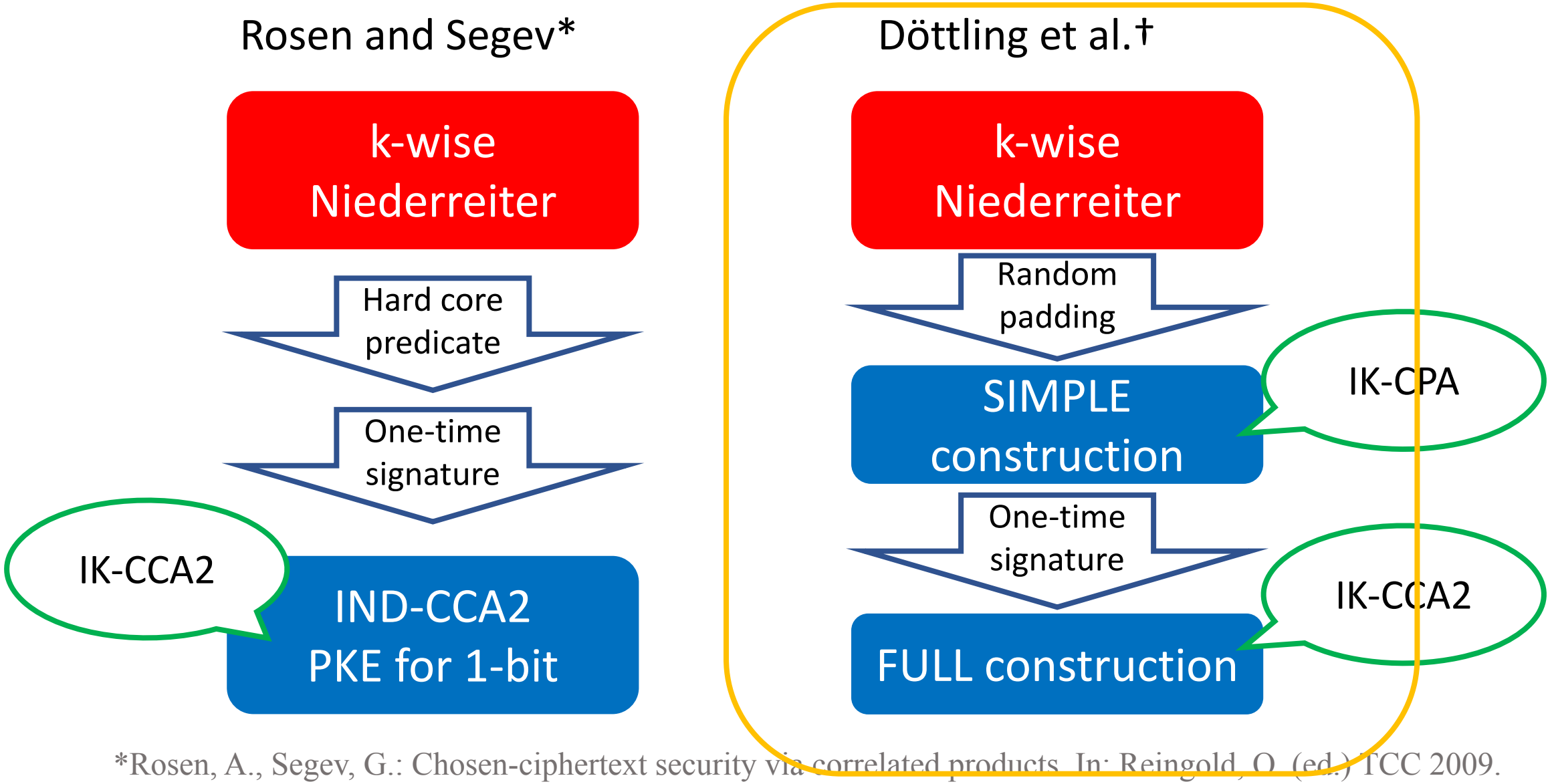
*Rosen, A., Segev, G.: Chosen-ciphertext security via correlated products. In: Reingold, O. (ed.) TCC 2009.
†Döttling, N., Dowsley, R., Muller-Quade, J., Nascimento, A.C.A.: A CCA2 secure variant of the mceliece cryptosystem. IEEE Trans. Inf. Theory 58(10), 6672–6680 (2012)

Instantiation with Niederreiter and its key-privacy



*Rosen, A., Segev, G.: Chosen-ciphertext security via correlated products. In: Reingold, O. (ed.) TCC 2009.
†Döttling, N., Dowsley, R., Muller-Quade, J., Nascimento, A.C.A.: A CCA2 secure variant of the mceliece cryptosystem. IEEE Trans. Inf. Theory 58(10), 6672–6680 (2012)

Instantiation with Niederreiter and its key-privacy



*Rosen, A., Segev, G.: Chosen-ciphertext security via correlated products. In: Reingold, O. (ed.) TCC 2009.

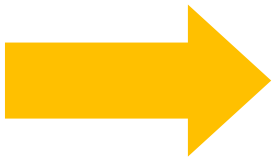
†Döttling, N., Dowsley, R., Muller-Quade, J., Nascimento, A.C.A.: A CCA2 secure variant of the mceliece cryptosystem. IEEE Trans. Inf. Theory 58(10), 6672–6680 (2012)

How to prove the FULL construction is IK-CCA2

The SIMPLE construction with the Niederreiter/McEliece is IK-CPA

If SIMPLE construction is IK-CPA and signature is secure (OT-sEUF-CMA)

then the FULL construction is IK-CCA2

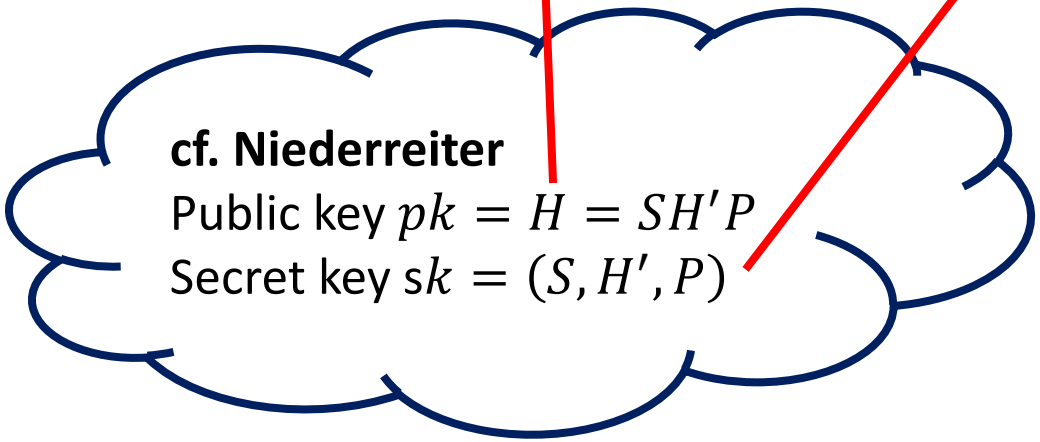


The FULL construction with the Niederreiter/McEliece is IK-CCA2

SIMPLE Construction with Niederreiter

Key generation

$$pk = (H_1, H_2, \ldots, H_k),\ sk = \{(S_i, H_i', P_i),\ 1 \le i \le k\}$$



SIMPLE Construction with Niederreiter

Key generation

$$pk = (H_1, H_2, \ldots, H_k),\ sk = \{(S_i, H_i', P_i),\ 1 \le i \le k\}$$

Encryption

Pick a random padding vector r.

$$c = (H_1 \times (m||r)^T, H_2 \times (m||r)^T, \ldots, H_k \times (m||r)^T)$$

cf. Randomized Niederreiter

Ciphertext is $c = H(m||r)^T$

SIMPLE Construction with Niederreiter

Key generation

$$pk = (H_1, H_2, \ldots, H_k), \mathrm{sk} = \{(S_i, H_i', P_i),\ 1 \le i \le k\}$$

Encryption

Pick a random padding vector r.

$$c = (H_1 \times (m||r)^T, H_2 \times (m||r)^T, \ldots, H_k \times (m||r)^T)$$

Decryption

Decrypt all elements in c.

Confirm that all decrypted $m||r$ are the same.

FULL Construction with Niederreiter

Key generation

$$pk = \begin{pmatrix} H_{1,0}, H_{2,0}, \dots, H_{k,0} \\ H_{1,1}, H_{2,1}, \dots, H_{k,1} \end{pmatrix}, sk = \left\{ \left(S_{i,b}, H'_{i,b}, P_{i,b} \right), \begin{matrix} 1 \le i \le k \\ b = 0,1 \end{matrix} \right\}$$

Encryption

generate verification/signing key pair of one-time signature

$$\left(vk = vk_1 \circ \cdots \circ vk_k \in \{0,1\}^k, dsk \right)$$

$$c = \left(H_{1,vk_1} \times (m||r)^T, \dots, H_{k,vk_k} \times (m||r)^T \right), \sigma \leftarrow sign(dsk, c)$$

output (vk, c, σ).

Decryption

Verify the signature σ. Decrypt all elements in c.

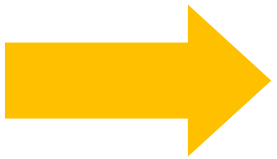
Confirm that all decrypted $m||r$ are the same.

Key-Privacy for These Construction

The SIMPLE construction with the Niederreiter/McEliece is IK-CPA

If SIMPLE construction is IK-CPA and signature is secure (OT-sEUF-CMA)

then the FULL construction is IK-CCA2



The FULL construction with the Niederreiter/McEliece is IK-CCA2

Key-Privacy for These Construction

The SIMPLE construction with the Niederreiter/McEliece is IK-CPA

If SIMPLE construction is IK-CPA and signature is secure (OT-sEUF-CMA)

then the FULL construction is IK-CCA2

The FULL construction with the Niederreiter/McEliece is IK-CCA2

Proof Outline

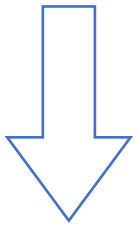
$$pk_0 = \left(H_{0,1}, H_{0,2}, \dots, H_{0,k}\right)$$
$$pk_1 = \left(H_{1,1}, H_{1,2}, \dots, H_{1,k}\right)$$

$$Enc(pk_b, m) = \begin{pmatrix} H_{b,1} \times (m||r)^T \\ H_{b,2} \times (m||r)^T \\ \vdots \\ H_{b,k} \times (m||r)^T \end{pmatrix}$$

Proof Outline

$$pk_0 = (H_{0,1}, H_{0,2}, \dots, H_{0,k})$$
$$pk_1 = (H_{1,1}, H_{1,2}, \dots, H_{1,k})$$

$$Enc(pk_b, m) = \begin{pmatrix} H_{b,1} \times (m||r)^T \\ H_{b,2} \times (m||r)^T \\ \vdots \\ H_{b,k} \times (m||r)^T \end{pmatrix}$$



the public keys are indistinguishable from random matrices.

$$pk_0 = (R_{0,1}, R_{0,2}, \dots, R_{0,k}),$$
$$pk_1 = (R_{1,1}, R_{1,2}, \dots, R_{1,k}),$$

$$Enc(pk_b, m) = \begin{pmatrix} R_{b,1} \times (m||r)^T \\ R_{b,2} \times (m||r)^T \\ \vdots \\ R_{b,k} \times (m||r)^T \end{pmatrix}$$

Proof Outline

$$pk_0 = \left(R_{0,1}, R_{0,2}, \ldots, R_{0,k}\right)$$
$$pk_1 = \left(R_{1,1}, R_{1,2}, \ldots, R_{1,k}\right)$$

$$Enc(pk_b, m) = \begin{pmatrix} R_{b,1} \times (m||r)^T \\ R_{b,2} \times (m||r)^T \\ \vdots \\ R_{b,k} \times (m||r)^T \end{pmatrix}$$

Proof Outline

$$pk_0 = (R_{0,1}, R_{0,2}, \dots, R_{0,k})$$
$$pk_1 = (R_{1,1}, R_{1,2}, \dots, R_{1,k})$$

$$Enc(pk_b, m) = \begin{pmatrix} R_{b,1} \times (m||r)^T \\ R_{b,2} \times (m||r)^T \\ \vdots \\ R_{b,k} \times (m||r)^T \end{pmatrix}$$

write them together

$$pk_0 = R_0$$
$$pk_1 = R_1$$

$$Enc(pk_b, m) = R_b \times (m||r)^T$$

Proof Outline

$$pk_0 = R_0$$
$$pk_1 = R_1$$

$$Enc(pk_b, m) = R_b \times (m||r)^T$$

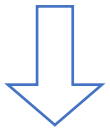
$$R_b \times (m||r)^T = R_{m,b} \times m^T + \underline{R_{r,b} \times r^T}$$

Proof Outline

$$pk_0 = R_0$$
$$pk_1 = R_1$$

$$Enc(pk_b, m) = R_b \times (m||r)^T$$

$$R_b \times (m||r)^T = R_{m,b} \times m^T + R_{r,b} \times r^T$$



Decisional version of SD

$$R_{m,b} \times m^T + u$$

Proof Outline

$$pk_0 = R_0$$
$$pk_1 = R_1$$

$$Enc(pk_b, m) = R_b \times (m||r)^T$$

$$R_b \times (m||r)^T = R_{m,b} \times m^T + \underline{R_{r,b} \times r^T}$$

⇩ Decisional version of SD

$$\underline{R_{m,b} \times m^T + u}$$

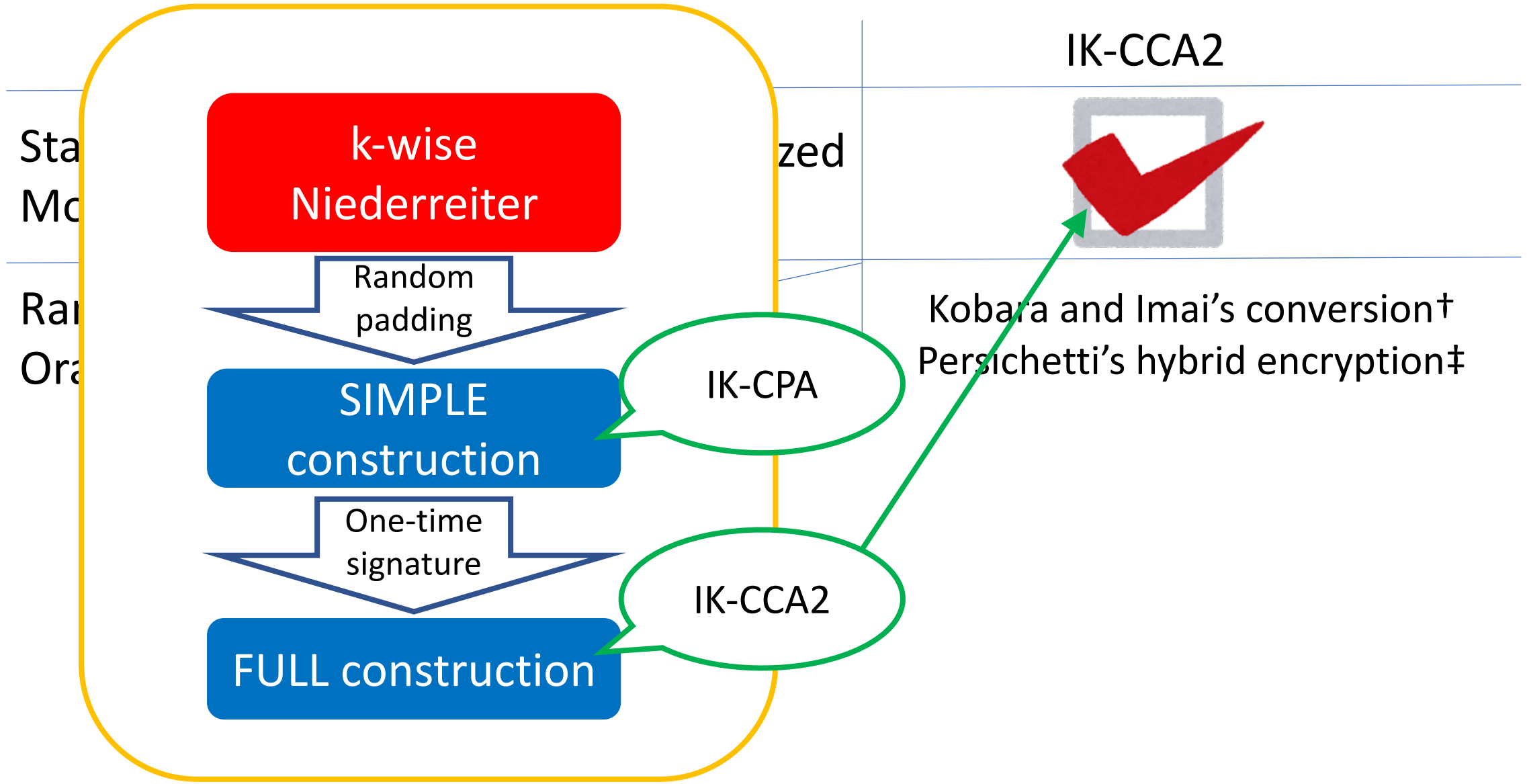
⇩

u **No information** about b!

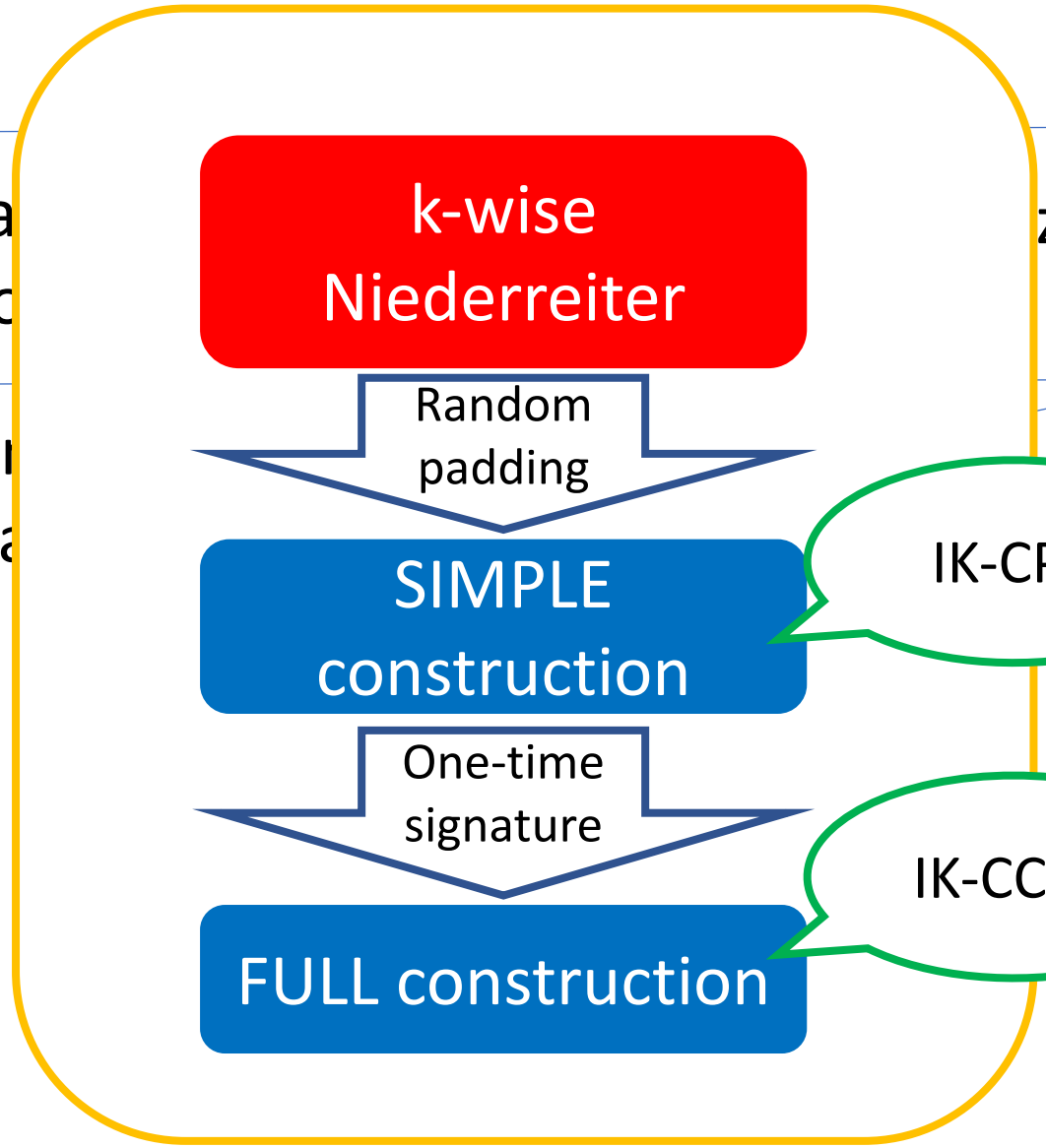
Conclusion

	not IK-CPA	IK-CPA	IK-CCA2
Standard Model	McEliece	Randomized McEliece	?
Random Oracle			Kobara and Imai's conversion† Persichetti's hybrid encryption‡

Conclusion


IK-CCA2
k-wise Niederreiter
Random padding
SIMPLE construction
IK-CPA
One-time signature
IK-CCA2
FULL construction
Kobara and Imai's conversion†
Persichetti's hybrid encryption‡

Conclusion



IK-CPA

IK-CCA2

IK-CCA2

Kobara and Imai's conversion†
Persichetti's hybrid encryption‡

?????? Open Question ??????

More efficient scheme

in the standard model?

Thank you!