Anonymous, Robust Post-Quantum Public Key Encryption

Varun Maram
Applied Cryptography Group
ETH Zurich

Joint work with Paul Grubbs and Kenneth G. Paterson

[Full version of paper: https://eprint.iacr.org/2021/708.pdf]

NIST PQC Round-3 KEMs

PQC Standardization Process: Third Round Candidate Announcement

NIST is announcing the third round finalists of the NIST Post-Quantum Cryptography Standardization Process. More details are included in NISTIR 8309.

July 22, 2020

It has been almost a year and a half since the second round of the NIST PQC Standardization Process began. After careful consideration, NIST would like to announce the candidates that will be moving on to the third round.

Third Round Finalists	**Alternate Candidates**
Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

ORGANIZATIONS

Information Technology Laboratory

Computer Security Division

Cryptographic Technology Group

NIST PQC Round-3 KEMs

PQC Standardization Process: Third Round Candidate Announcement

NIST is announcing the third round finalists of the NIST Post-Quantum Cryptography Standardization Process. More details are included in NISTIR 8309.

July 22, 2020

It has been almost a year and a half since the second round of the NIST PQC Standardization Process began. After careful consideration, NIST would like to announce the candidates that will be moving on to the third round.

Third Round Finalists	Alternate Candidates
Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

ORGANIZATIONS

Information Technology Laboratory

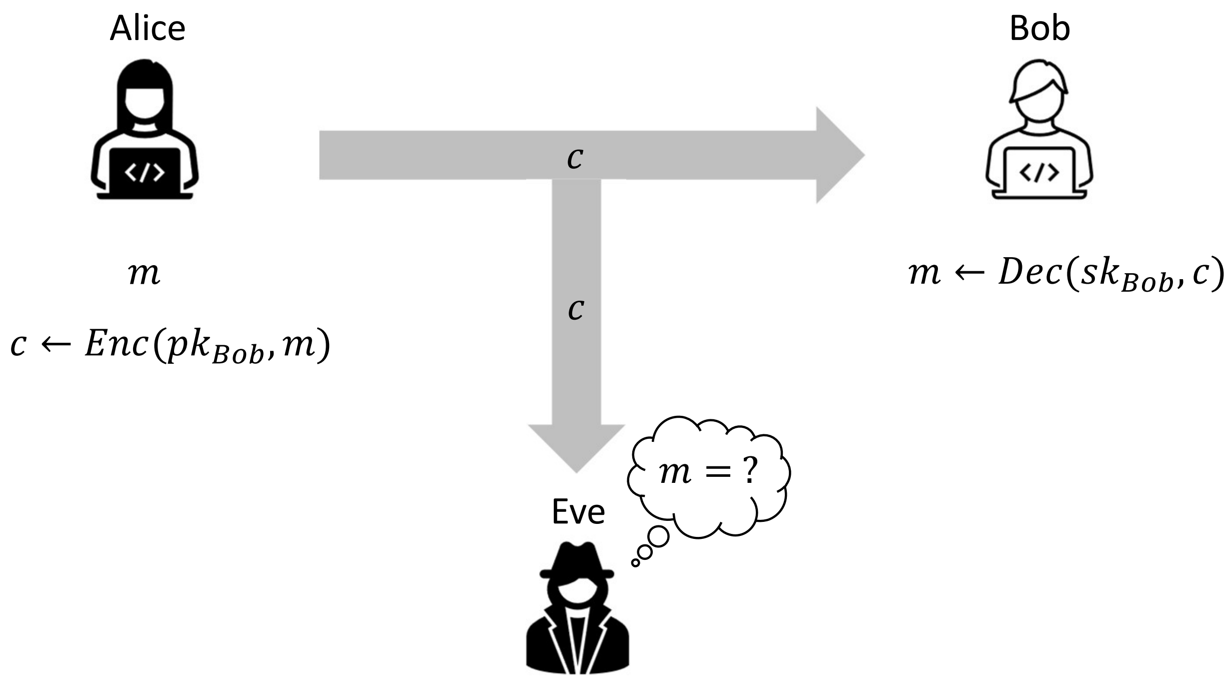
Computer Security Division

Cryptographic Technology Group

4.A.2 Security Definition for Encryption/Key-Establishment
NIST intends to standardize one or more schemes that enable "semantically secure" encryption or key encapsulation with respect to adaptive chosen ciphertext attack, for general use. This property is generally denoted *IND-CCA2 security* in academic literature.

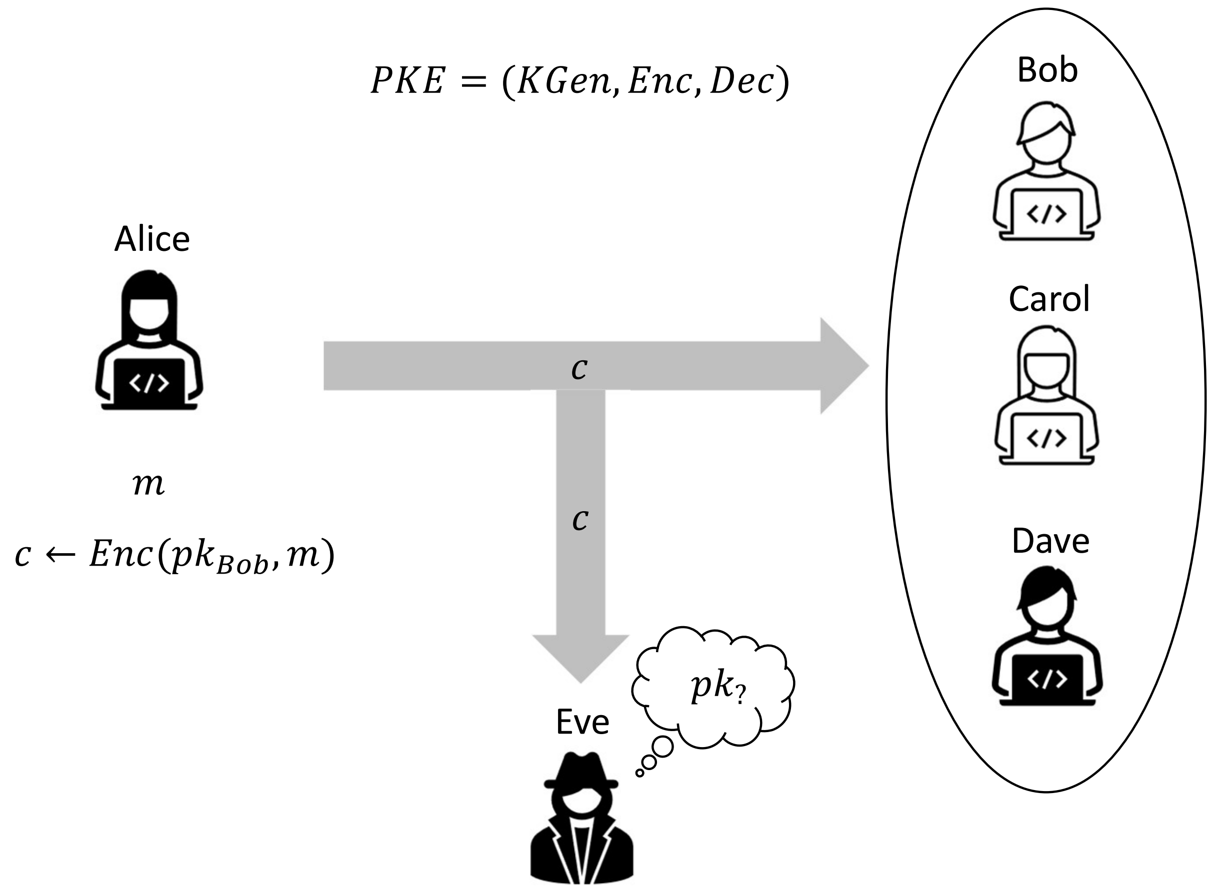
IND-CCA Security

$$PKE = (KGen, Enc, Dec)$$



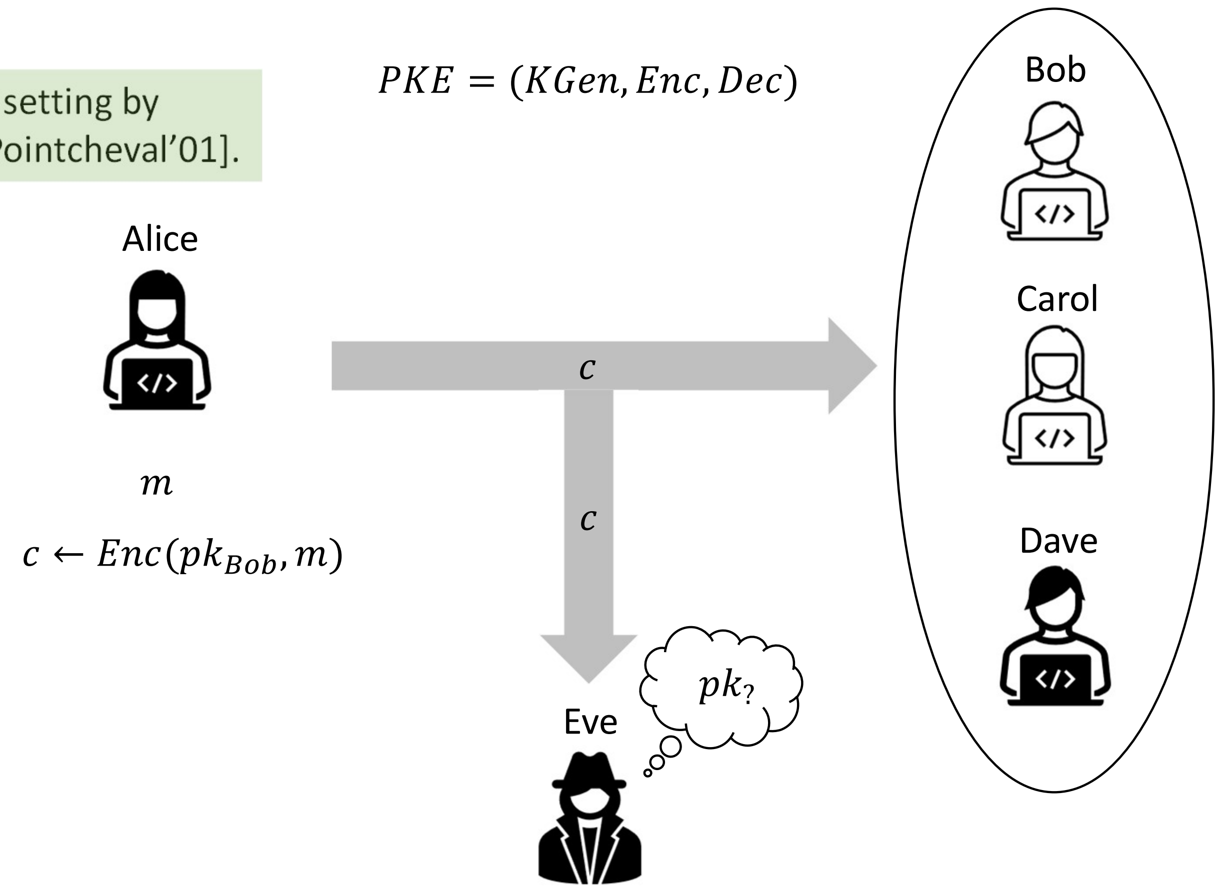
Anonymity (ANO-CCA security)

$PKE = (KGen, Enc, Dec)$



Anonymity (ANO-CCA security)

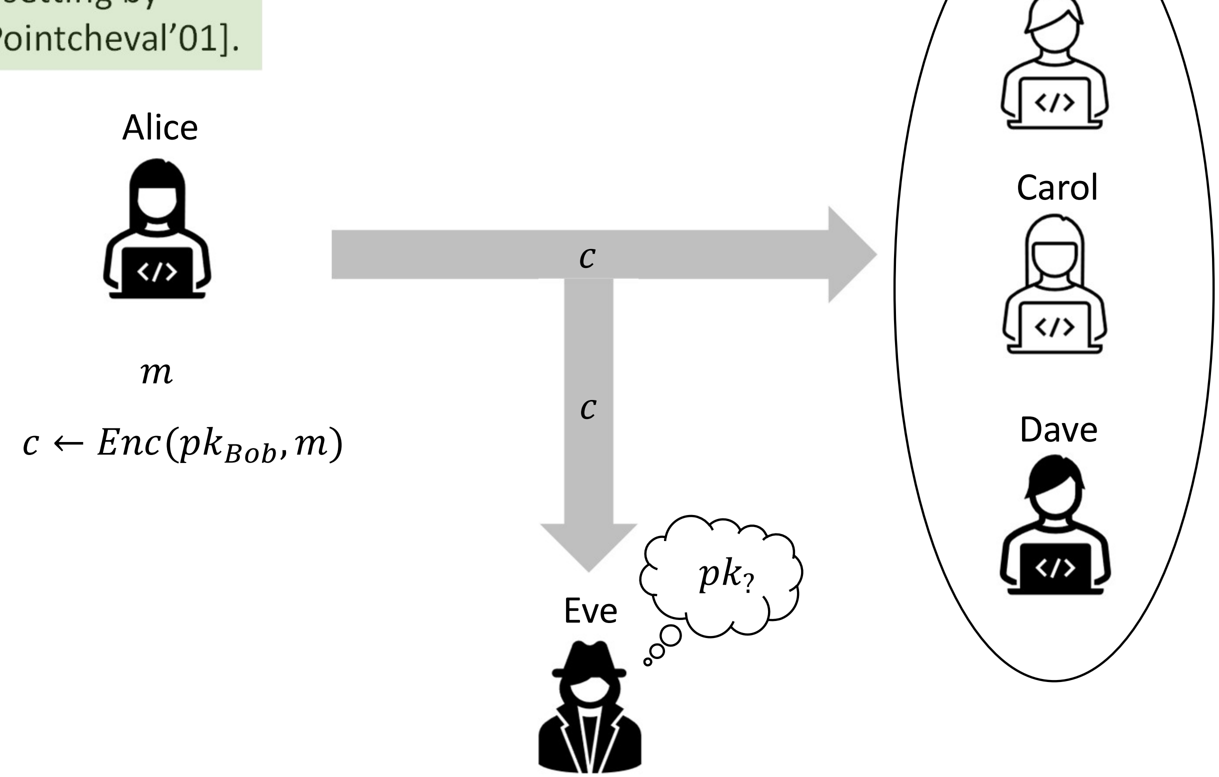
Formalized in a public-key setting by [Bellare-Boldyreva-Desai-Pointcheval'01].



Anonymity (ANO-CCA security)

Formalized in a public-key setting by [Bellare-Boldyreva-Desai-Pointcheval'01].

$PKE = (KGen, Enc, Dec)$



Anonymity (ANO-CCA security)

Formalized in a public-key setting by [Bellare-Boldyreva-Desai-Pointcheval’01].

$PKE = (KGen, Enc, Dec)$

Alice

m

$c \leftarrow Enc(pk_{Bob}, m)$

c

c

Bob

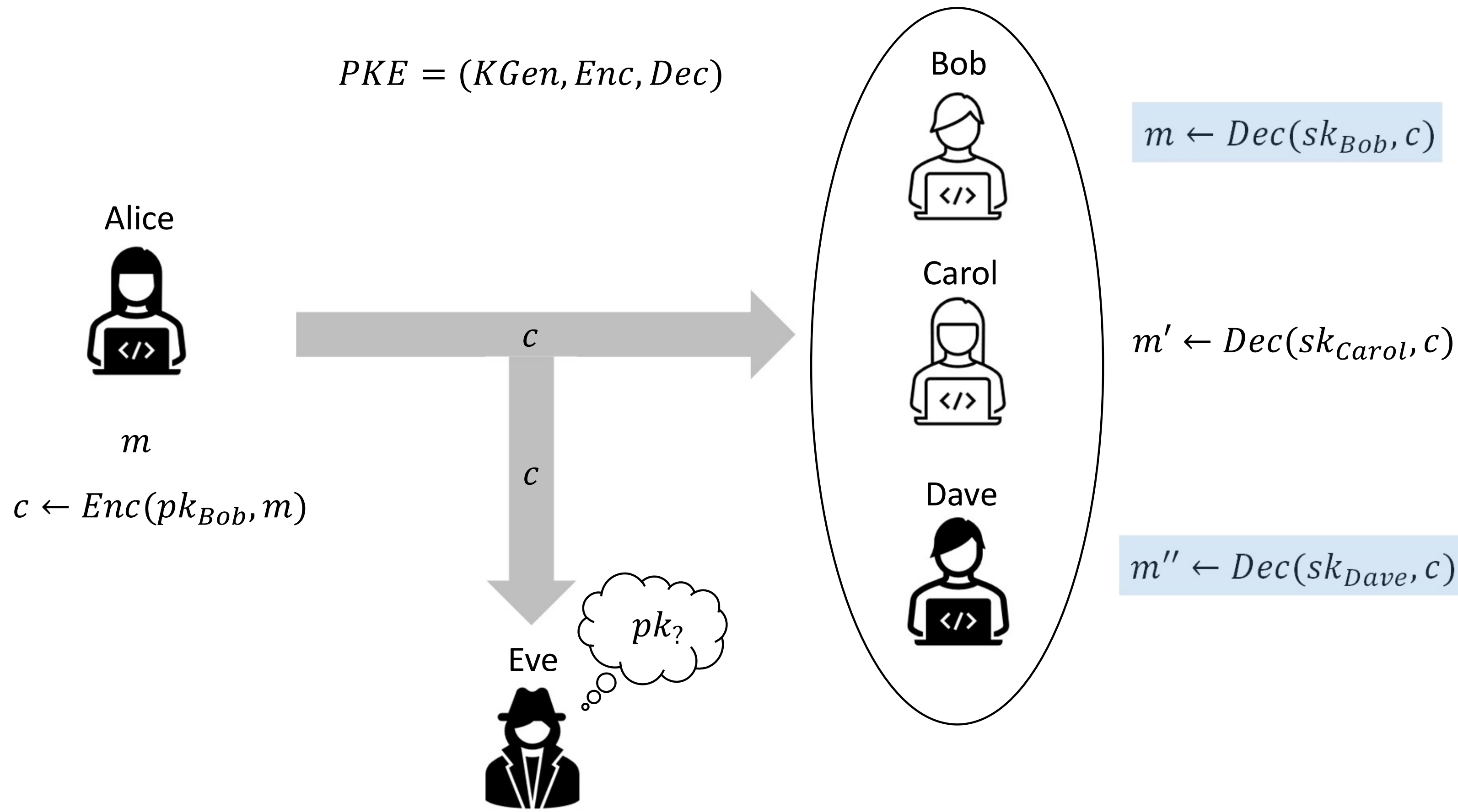
Carol

Dave

Eve

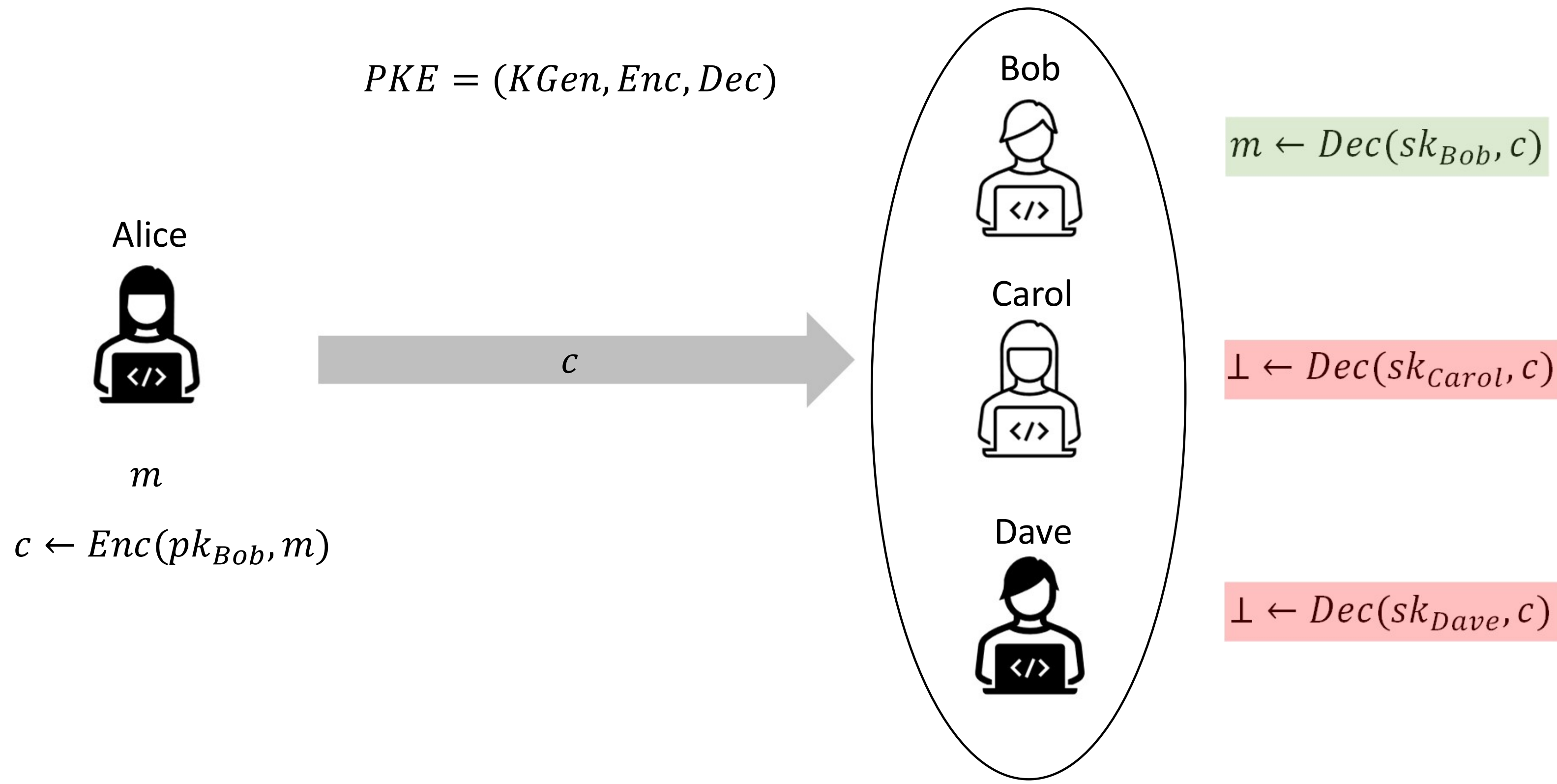
$pk_?$

Anonymity (ANO-CCA security)



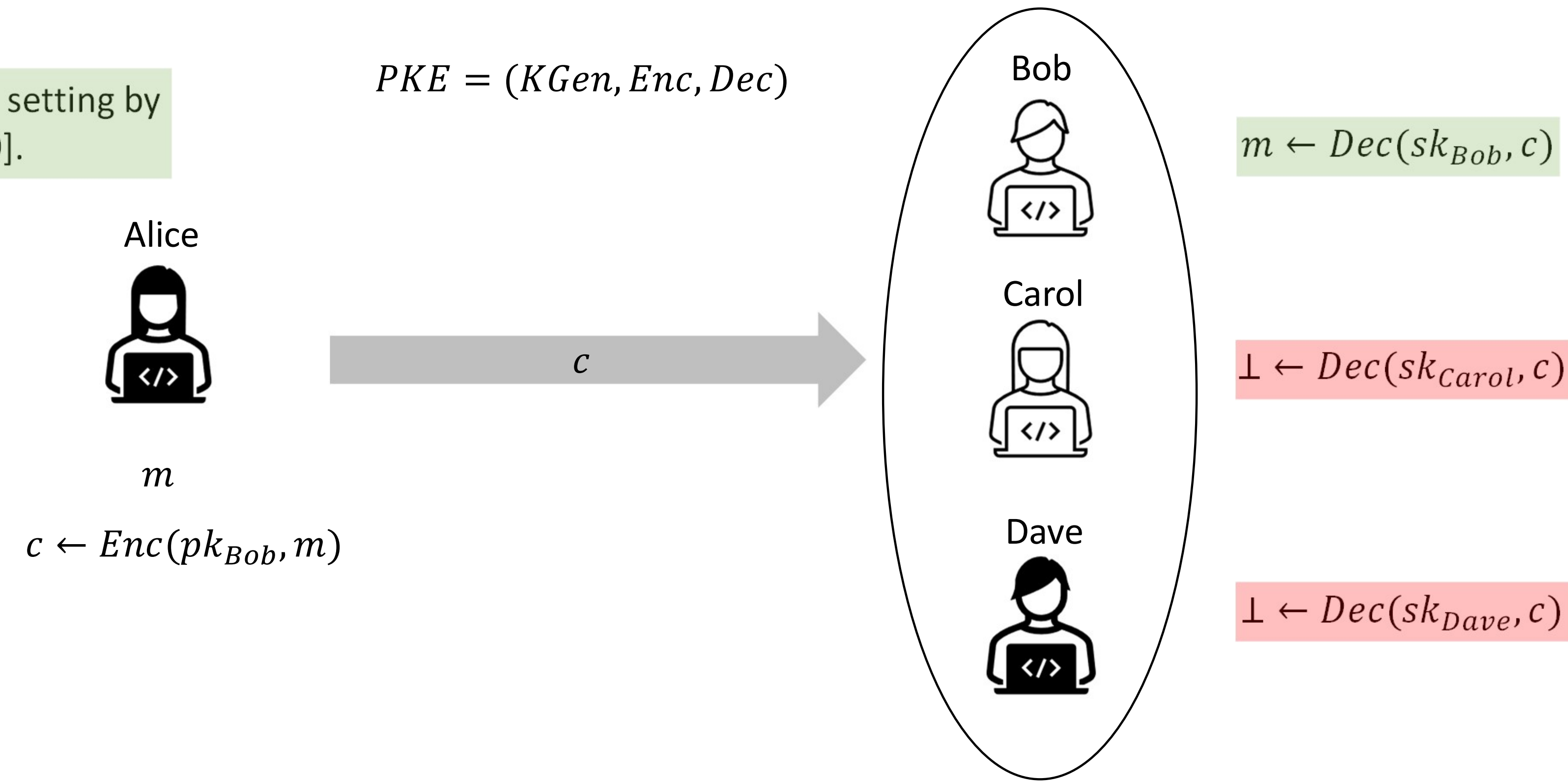
Robustness (SROB-CCA security)

$PKE = (KGen, Enc, Dec)$



Robustness (SROB-CCA security)

Formalized in a public-key setting by [Abdalla-Bellare-Neven'10].



KEM-DEM Paradigm

Public-Key Encryption/KEMs

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

Public-Key Encryption/KEMs

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

KEM-DEM Paradigm

Public-Key Encryption/KEMs

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

Public-Key Encryption/KEMs

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

$PKE = (KGen, Enc, Dec)$

IND-CCA secure

KEM-DEM Paradigm

Public-Key Encryption/KEMs

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

$KEM = (KGen, Encap, Decap)$

KEM

IND-CCA secure

Public-Key Encryption/KEMs

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

$PKE = (KGen, Enc, Dec)$

PKE

IND-CCA secure

KEM-DEM Paradigm

Public-Key Encryption/KEMs

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

Public-Key Encryption/KEMs

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

KEM + DEM = PKE

IND-CCA secure

(one-time) authenticated encryption

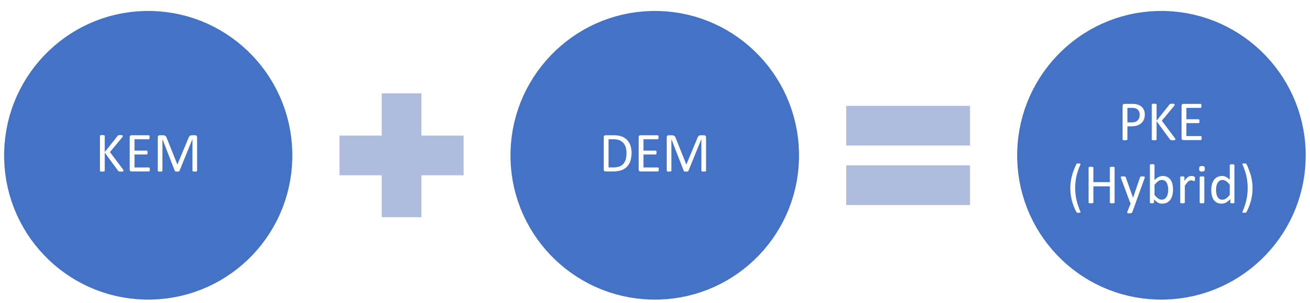
IND-CCA secure

KEM-DEM Paradigm

Public-Key Encryption/KEMs
- Classic McEliece
- CRYSTALS-KYBER
- NTRU
- SABER

Public-Key Encryption/KEMs
- BIKE
- FrodoKEM
- HQC
- NTRU Prime
- SIKE

$KEM = (KGen, Encap, Decap)$ $\quad DEM = (Enc^{sym}, Dec^{sym})$ $\quad PKE = (KGen, Enc, Dec)$



$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA secure

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

(one-time) authenticated encryption

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure

KEM-DEM Paradigm

Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

$KEM = (KGen, Encap, Decap)$ $\quad$ $DEM = (Enc^{sym}, Dec^{sym})$ $\quad$ $PKE = (KGen, Enc, Dec)$

KEM + DEM = PKE (Hybrid)

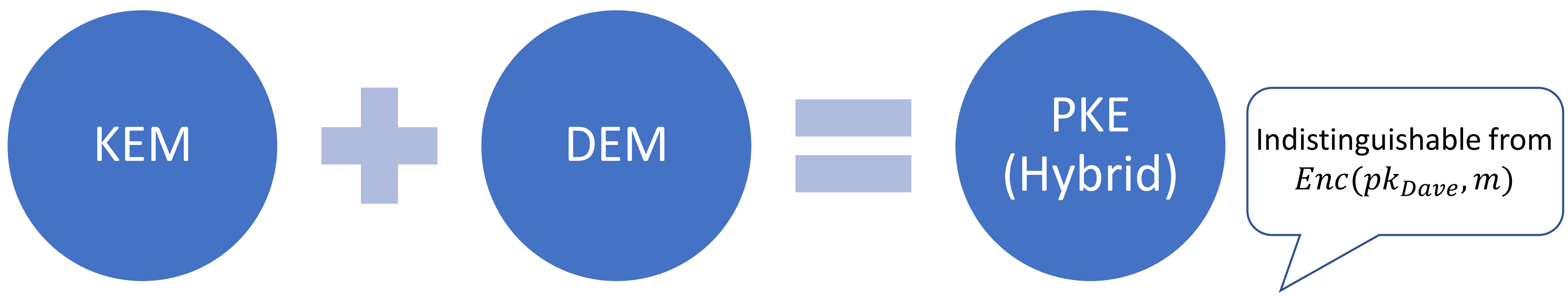
$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$ $\quad$ $c_{DEM} \leftarrow Enc^{sym}(k, m)$ $\quad$ $(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure +
ANO-CCA secure

KEM-DEM Paradigm

Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$



$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$ $c_{DEM} \leftarrow Enc^{sym}(k, m)$ $(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure +
ANO-CCA secure

KEM-DEM Paradigm

Public-Key Encryption/KEMs

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

Public-Key Encryption/KEMs

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

Shown in [Grubbs-Maram-Paterson'22]; generalization of [Mohassel'10].

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

KEM + DEM = PKE (Hybrid)

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$ $c_{DEM} \leftarrow Enc^{sym}(k, m)$ $(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

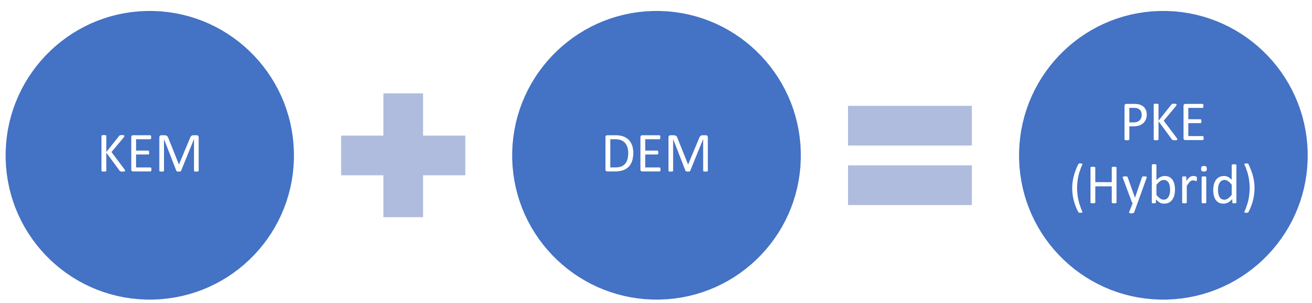
IND-CCA secure + ANO-CCA secure

KEM-DEM Paradigm

Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

Shown in [Grubbs-Maram-Paterson'22]; generalization of [Mohassel'10].

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$



$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$ $c_{DEM} \leftarrow Enc^{sym}(k, m)$ $(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA

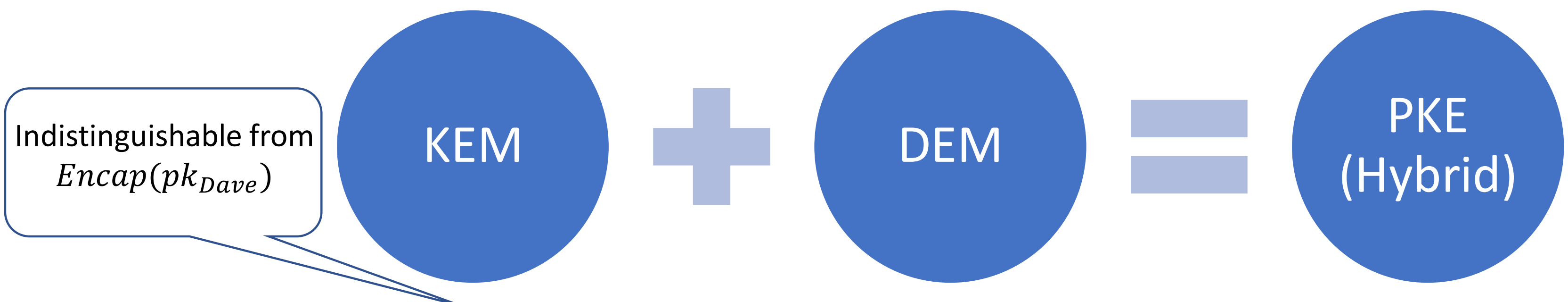
IND-CCA secure + ANO-CCA secure

KEM-DEM Paradigm

Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

Shown in [Grubbs-Maram-Paterson'22]; generalization of [Mohassel'10].

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$



$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$ $c_{DEM} \leftarrow Enc^{sym}(k, m)$ $(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA + ANO-CCA secure

IND-CCA secure + ANO-CCA secure

KEM-DEM Paradigm

Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

Shown in [Grubbs-Maram-Paterson'22]; generalization of [Mohassel'10].

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

$Decap(sk_{Dave}, c_{KEM}) = \perp$

KEM + DEM = PKE (Hybrid)

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$ $c_{DEM} \leftarrow Enc^{sym}(k, m)$ $(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA + ANO-CCA secure + weakly robust (WROB)

IND-CCA secure + ANO-CCA secure

KEM-DEM Paradigm

Public-Key Encryption/KEMs

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

Public-Key Encryption/KEMs

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

Shown in [Grubbs-Maram-Paterson'22]; generalization of [Mohassel'10].

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

KEM + DEM = PKE (Hybrid)

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + weakly robust (WROB)

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

(one-time) authenticated encryption

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure ✓

KEM-DEM Paradigm

Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

Shown in [Grubbs-Maram-Paterson'22]; generalization of [Mohassel'10].

[Mohassel'10] only considered KEMs constructed directly from PKE schemes.

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

KEM + DEM = PKE (Hybrid)

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + weakly robust (WROB)

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

(one-time) authenticated encryption

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure ✓

KEM-DEM Paradigm

Public-Key Encryption/KEMs

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

Public-Key Encryption/KEMs

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

Shown in [Grubbs-Maram-Paterson'22]; generalization of [Mohassel'10].

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

$Decap(sk_{Dave}, c_{KEM}) = \perp$

KEM + DEM = PKE (Hybrid)

$Dec(sk_{Dave}, c) = \perp$

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + weakly robust (WROB)

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

(one-time) authenticated encryption

$(c) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure + WROB ✓

KEM-DEM Paradigm

<u>Public-Key Encryption/KEMs</u>

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

<u>Public-Key Encryption/KEMs</u>

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

Shown in [Grubbs-Maram-Paterson'22]; generalization of [Mohassel'10].

$KEM = (KGen, Encap, Decap)$ $\quad DEM = (Enc^{sym}, Dec^{sym})$ $\quad PKE = (KGen, Enc, Dec)$

$Decap(sk_{Bob}, c^*_{KEM}) = \perp$
or,
$Decap(sk_{Dave}, c^*_{KEM}) = \perp$

c^*_{KEM}
arbitrary

KEM + DEM = PKE (Hybrid)

$Dec(sk_{Bob}, c^*) = \perp$
or,
$Dec(sk_{Dave}, c^*) = \perp$

(c^*)
arbitrary

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + strongly robust (SROB)

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

(one-time) authenticated encryption

$(c) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure + SROB ✓

KEM-DEM Paradigm

<u>Public-Key Encryption/KEMs</u>

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

<u>Public-Key Encryption/KEMs</u>

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

Shown in [Grubbs-Maram-Paterson'22]; generalization of [Mohassel'10].

$KEM = (KGen, Encap, Decap)$ $\quad DEM = (Enc^{sym}, Dec^{sym})$ $\quad PKE = (KGen, Enc, Dec)$

$Decap(sk_{Dave}, c_{KEM}) = \perp$

KEM + DEM = PKE (Hybrid)

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + weakly robust (WROB)

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

(one-time) authenticated encryption

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure + WROB

KEM-DEM Paradigm

Public-Key Encryption/KEMs

Classic McEliece
CRYSTALS-KYBER
NTRU
SABER

"Implicit-rejection" KEMs!

Public-Key Encryption/KEMs

BIKE
FrodoKEM
HQC
NTRU Prime
SIKE

Shown in [Grubbs-Maram-Paterson'22]; generalization of [Mohassel'10].

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

$Decap(sk_{Dave}, c_{KEM}) = \perp$

KEM + DEM = PKE (Hybrid)

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + weakly robust (WROB)

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

(one-time) authenticated encryption

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure + WROB

KEM-DEM Paradigm

Public-Key Encryption/KEMs

- Classic McEliece
- CRYSTALS-KYBER
- NTRU
- SABER

"Implicit-rejection" KEMs!

Cannot be even weakly robust.

Public-Key Encryption/KEMs

- BIKE
- FrodoKEM
- HQC
- NTRU Prime
- SIKE

Shown in [Grubbs-Maram-Paterson'22]; generalization of [Mohassel'10].

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

$Decap(sk_{Dave}, c_{KEM}) = \perp$

KEM + DEM = PKE (Hybrid)

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + weakly robust (WROB)

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

(one-time) authenticated encryption

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure + WROB

Implicit-rejection KEMs

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

$Decap(sk_{Dave}, c_{KEM}) = \perp$

KEM + DEM = PKE (Hybrid)

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure
+ weakly robust (WROB)

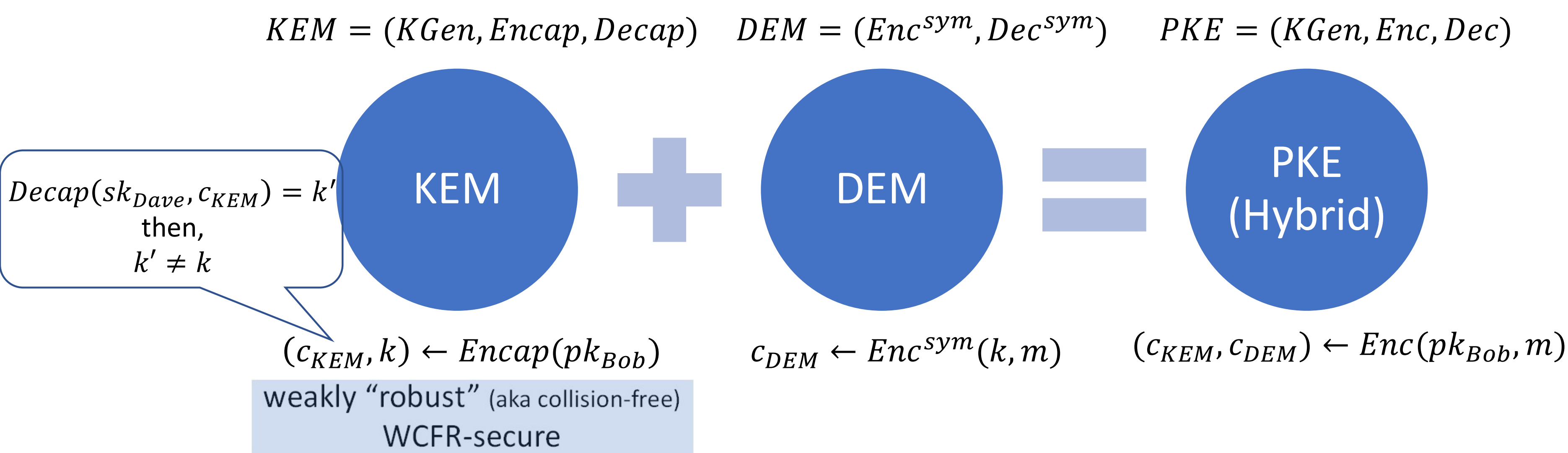
$c_{DEM} \leftarrow Enc^{sym}(k, m)$

(one-time) authenticated encryption

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure +
ANO-CCA secure
+ WROB

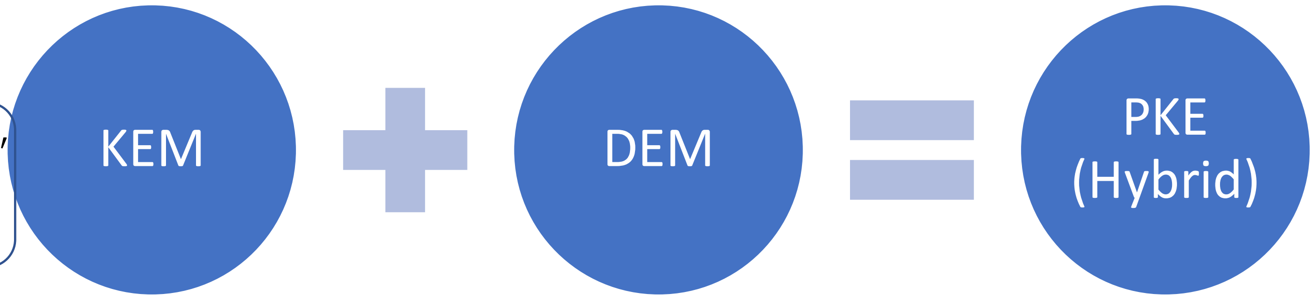
Implicit-rejection KEMs



Implicit-rejection KEMs

$KEM = (KGen, Encap, Decap)$ $\quad DEM = (Enc^{sym}, Dec^{sym})$ $\quad PKE = (KGen, Enc, Dec)$

$Decap(sk_{Dave}, c_{KEM}) = k'$
then,
$k' \neq k$



$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

weakly "robust" (aka collision-free)
WCFR-secure

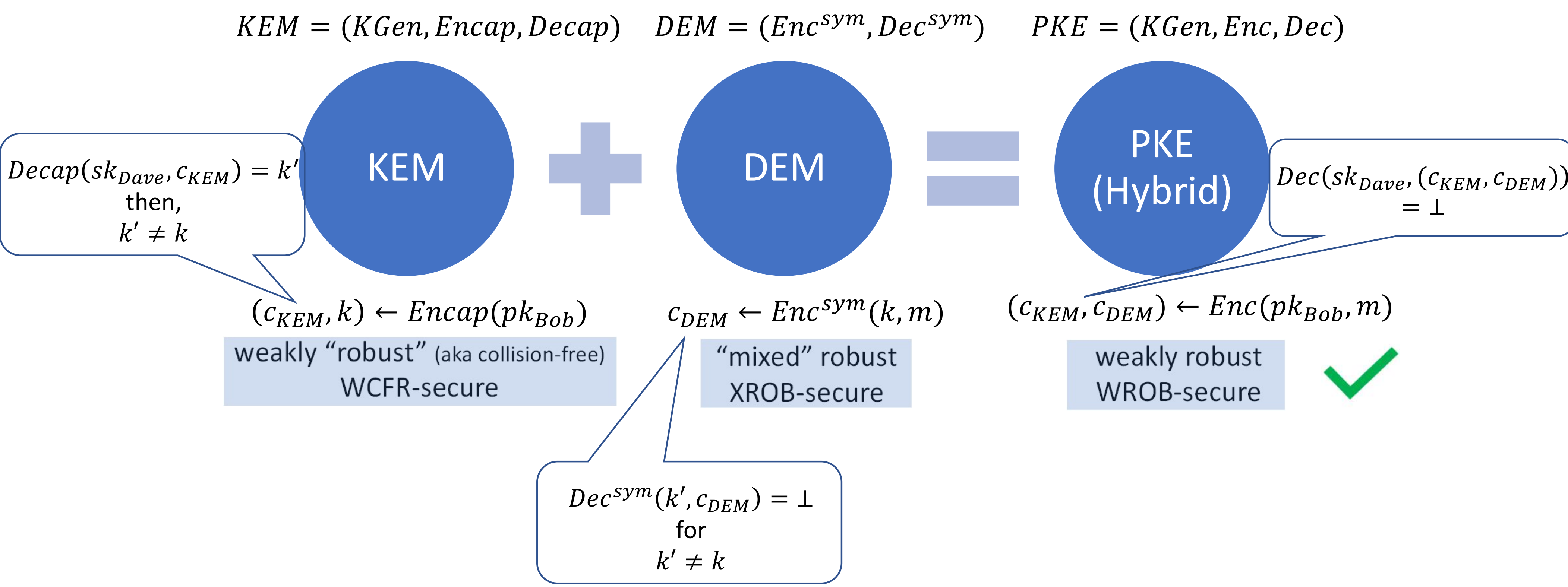
$c_{DEM} \leftarrow Enc^{sym}(k, m)$

"mixed" robust
XROB-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

$Dec^{sym}(k', c_{DEM}) = \perp$
for
$k' \neq k$

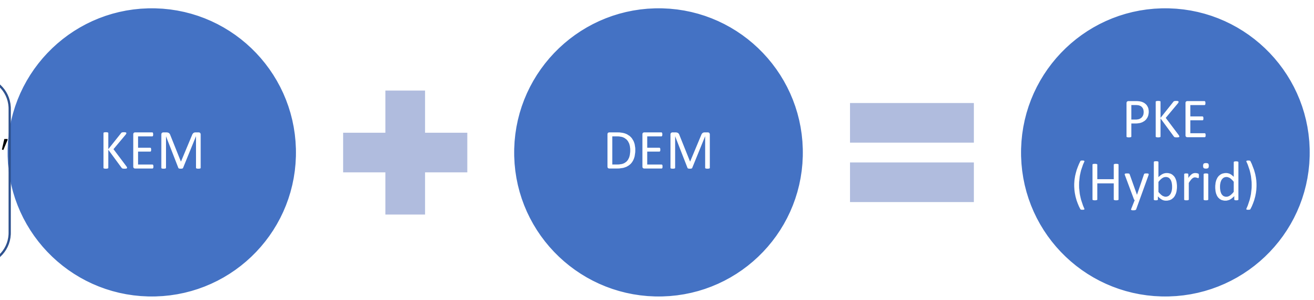
Implicit-rejection KEMs



Implicit-rejection KEMs

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

$Decap(sk_{Bob}, c^*_{KEM}) = k'$
$Decap(sk_{Dave}, c^*_{KEM}) = k''$
then,
$k'' \neq k'$



c^*_{KEM}
arbitrary

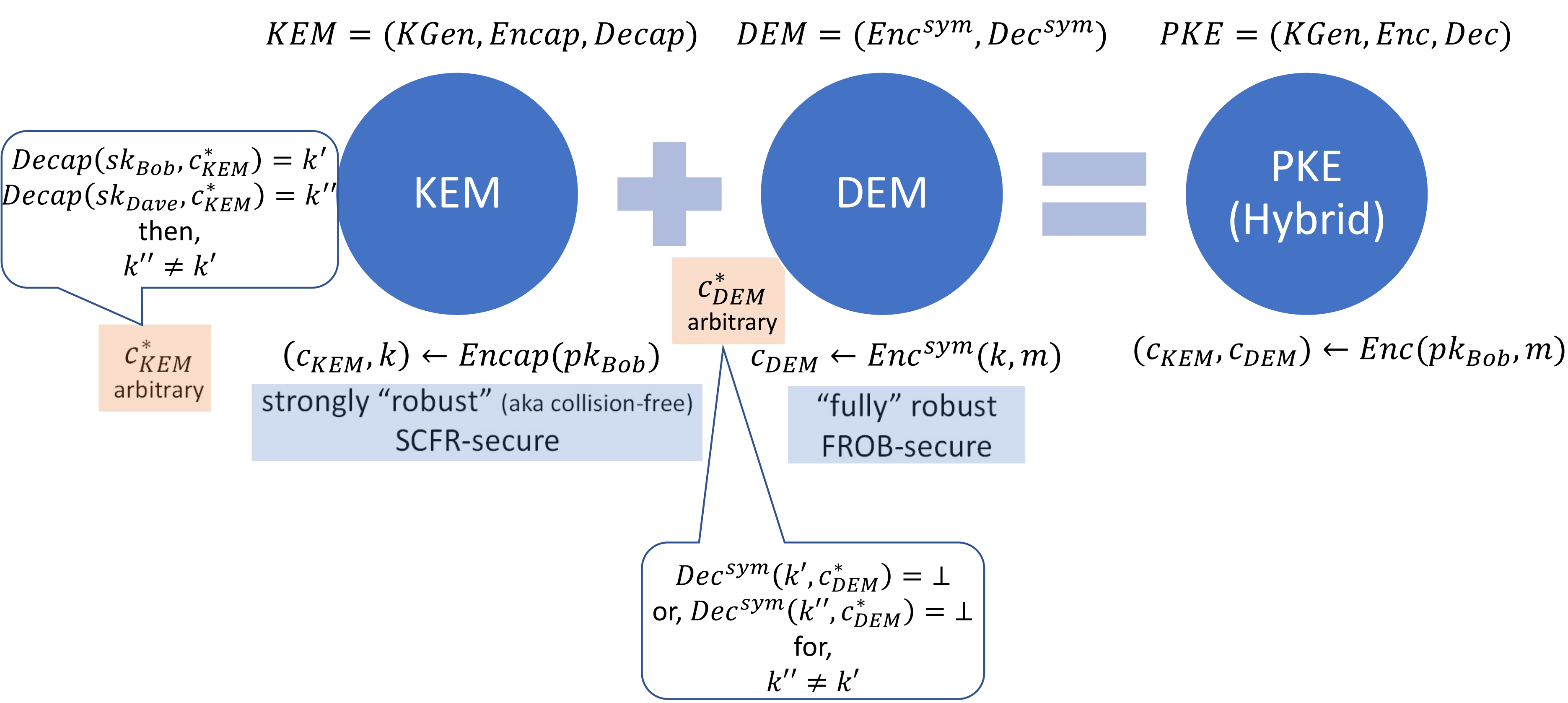
$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

strongly "robust" (aka collision-free)
SCFR-secure

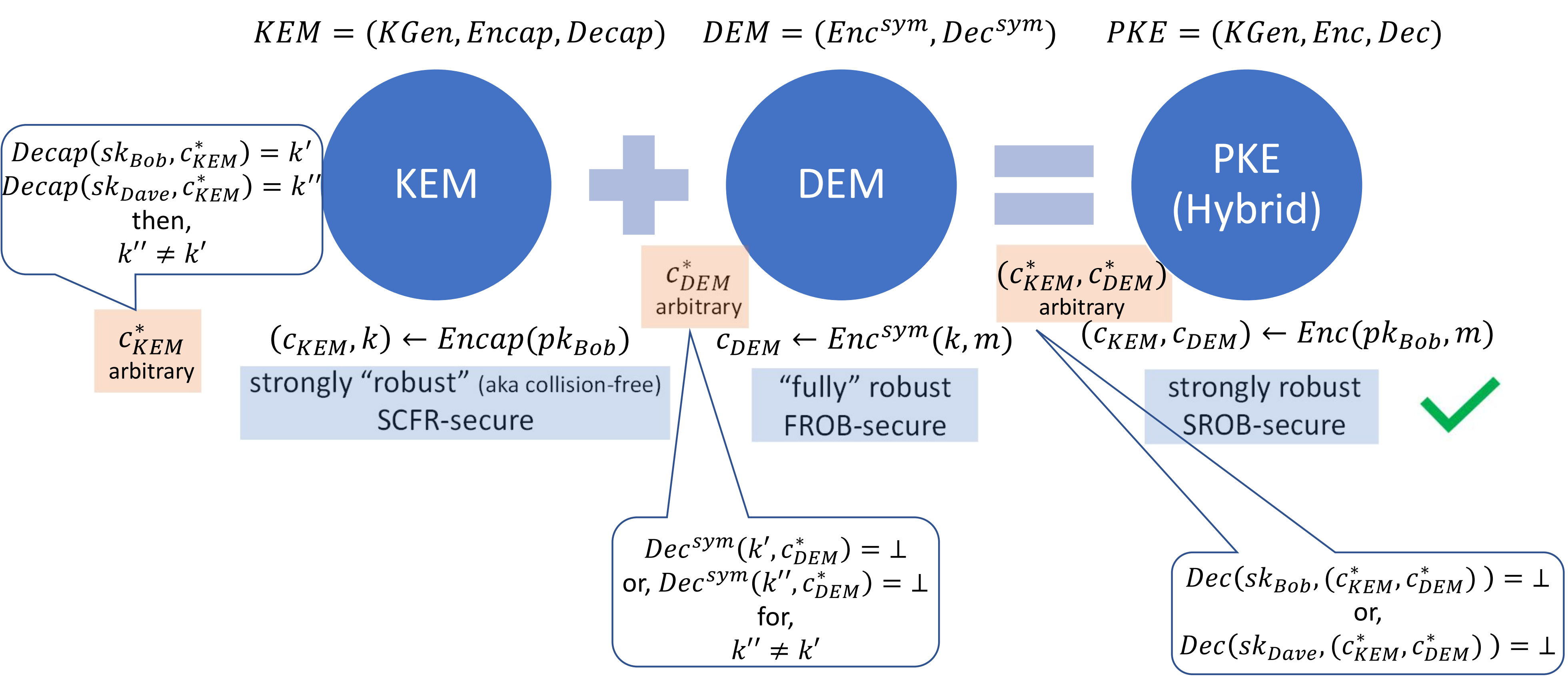
$c_{DEM} \leftarrow Enc^{sym}(k, m)$

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

Implicit-rejection KEMs



Implicit-rejection KEMs



Implicit-rejection KEMs

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

KEM + DEM = PKE (Hybrid)

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

strongly "robust" (aka collision-free)
SCFR-secure

weakly "robust" (aka collision-free)
WCFR-secure

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

"fully" robust
FROB-secure

"mixed" robust
XROB-secure

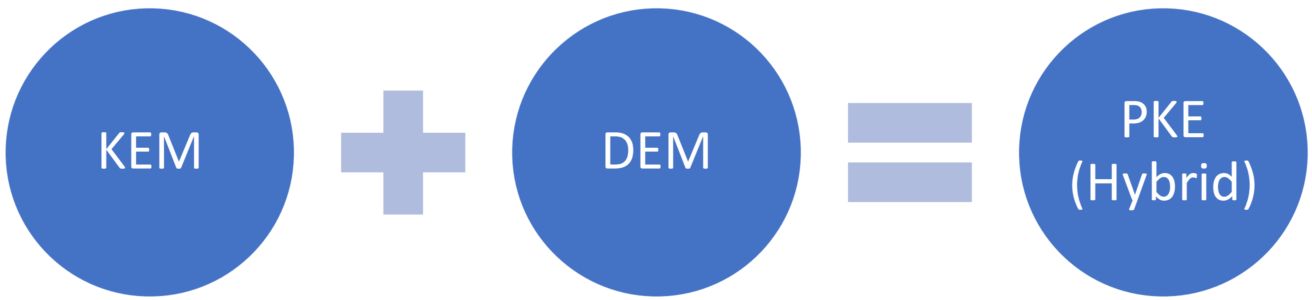
$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

strongly robust
SROB-secure

weakly robust
WROB-secure

Implicit-rejection KEMs

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$



$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

strongly "robust" (aka collision-free)
SCFR-secure

weakly "robust" (aka collision-free)
WCFR-secure

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

"fully" robust
FROB-secure

"mixed" robust
XROB-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

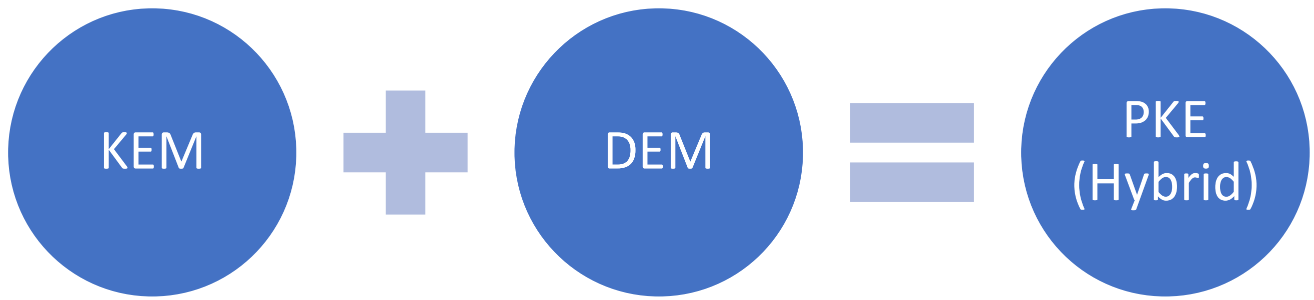
strongly robust
SROB-secure ✓

weakly robust
WROB-secure ✓

[Farshim-Orlandi-Roşie'17] provide "efficient" constructions of XROB-, FROB-secure AE schemes.

Implicit-rejection KEMs

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$



$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

strongly "robust" (aka collision-free)
SCFR-secure

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

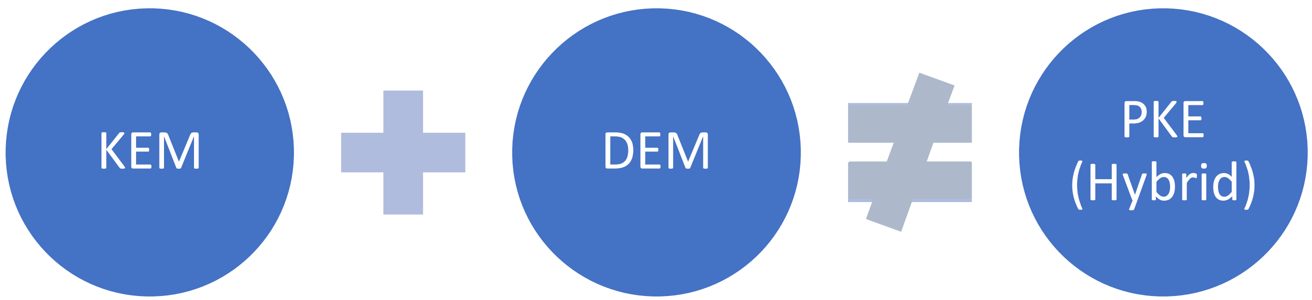
"fully" robust
FROB-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

strongly robust
SROB-secure ✓

Implicit-rejection KEMs

$KEM = (KGen, Encap, Decap)$ $\quad DEM = (Enc^{sym}, Dec^{sym})$ $\quad PKE = (KGen, Enc, Dec)$



$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

strongly "robust" (aka collision-free)
SCFR-secure

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure
(not FROB)

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

strongly robust
SROB-secure

Implicit-rejection KEMs

$KEM = (KGen, Encap, Decap)$ $\quad$ $DEM = (Enc^{sym}, Dec^{sym})$ $\quad$ $PKE = (KGen, Enc, Dec)$

KEM + DEM = PKE (Hybrid)

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure
+ weakly robust (WROB)

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

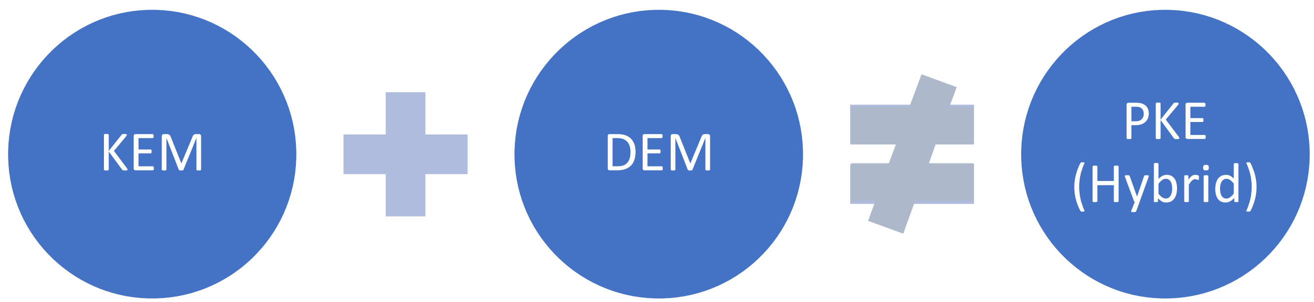
AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

ANO-CCA secure

Implicit-rejection KEMs

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$



$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$ $c_{DEM} \leftarrow Enc^{sym}(k, m)$ $(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA + ANO-CCA secure
+ strongly “robust” (SCFR)

AE-secure
(and XROB)

ANO-CCA secure

Implicit-rejection KEMs

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

KEM + DEM ≠ PKE (Hybrid)

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure
+ ~~strongly "robust" (SCFR)~~

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure
(and XROB)

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

ANO-CCA secure

This strengthens an analogous negative result of [Mohassel'10].

NIST PQC Round-3 KEMs

PQC Standardization Process: Third Round Candidate Announcement

NIST is announcing the third round finalists of the NIST Post-Quantum Cryptography Standardization Process. More details are included in NISTIR 8309.

July 22, 2020

It has been almost a year and a half since the second round of the NIST PQC Standardization Process began. After careful consideration, NIST would like to announce the candidates that will be moving on to the third round.

Third Round Finalists	Alternate Candidates
Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

ORGANIZATIONS

Information Technology Laboratory

Computer Security Division

Cryptographic Technology Group

4.A.2 Security Definition for Encryption/Key-Establishment
NIST intends to standardize one or more schemes that enable "semantically secure" encryption or key encapsulation with respect to adaptive chosen ciphertext attack, for general use. This property is generally denoted *IND-CCA2 security* in academic literature.

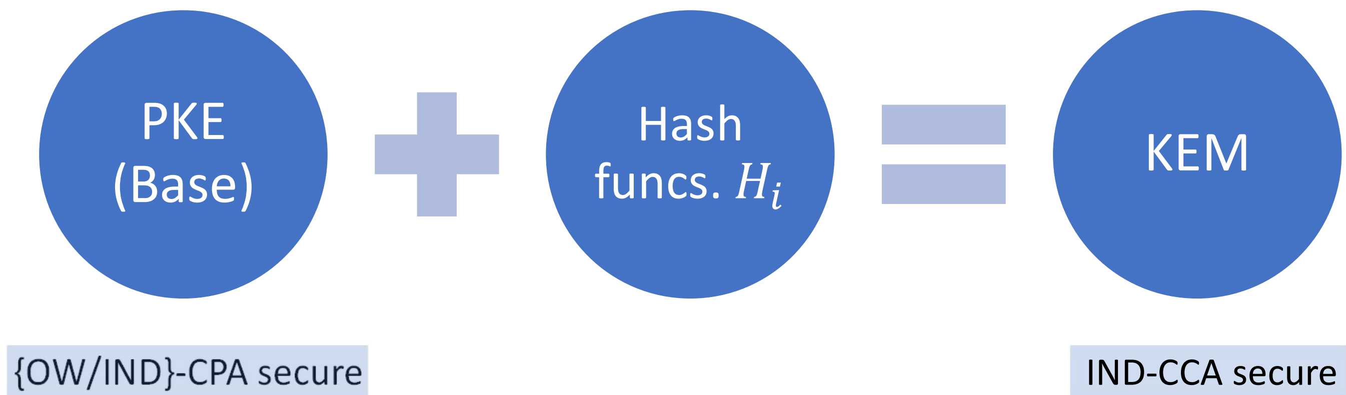
Fujisaki-Okamoto Transformation

KEM

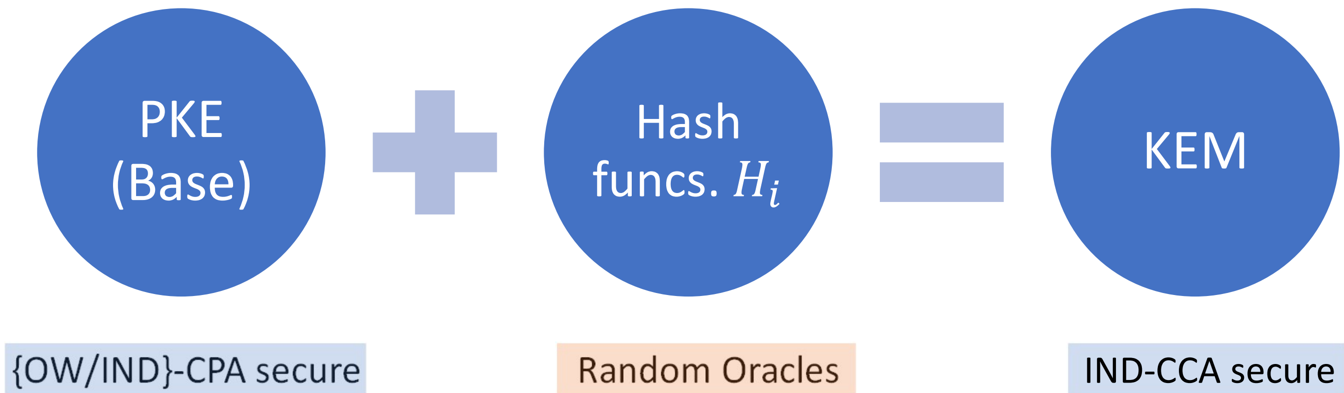
IND-CCA secure

Fujisaki-Okamoto Transformation

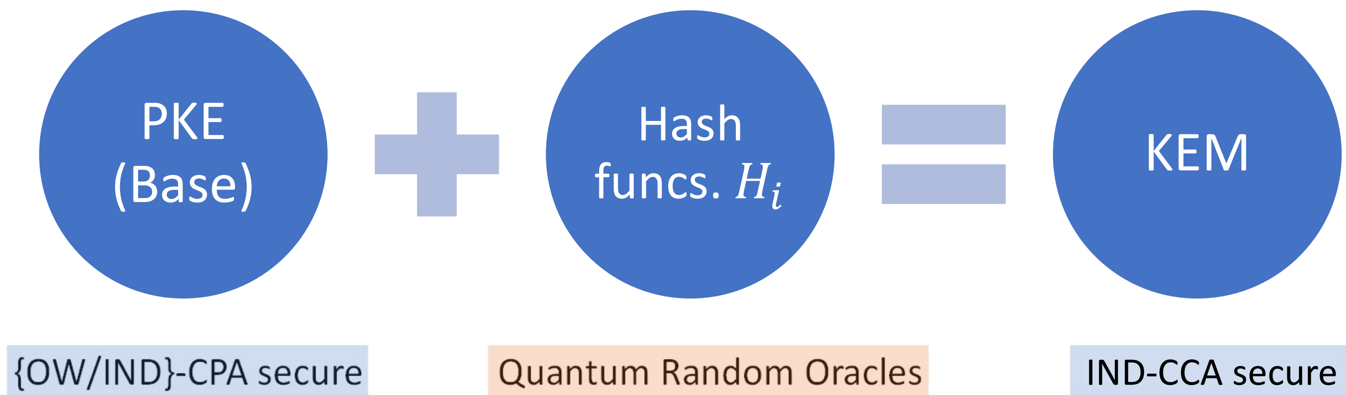
Fujisaki-Okamoto Transformation



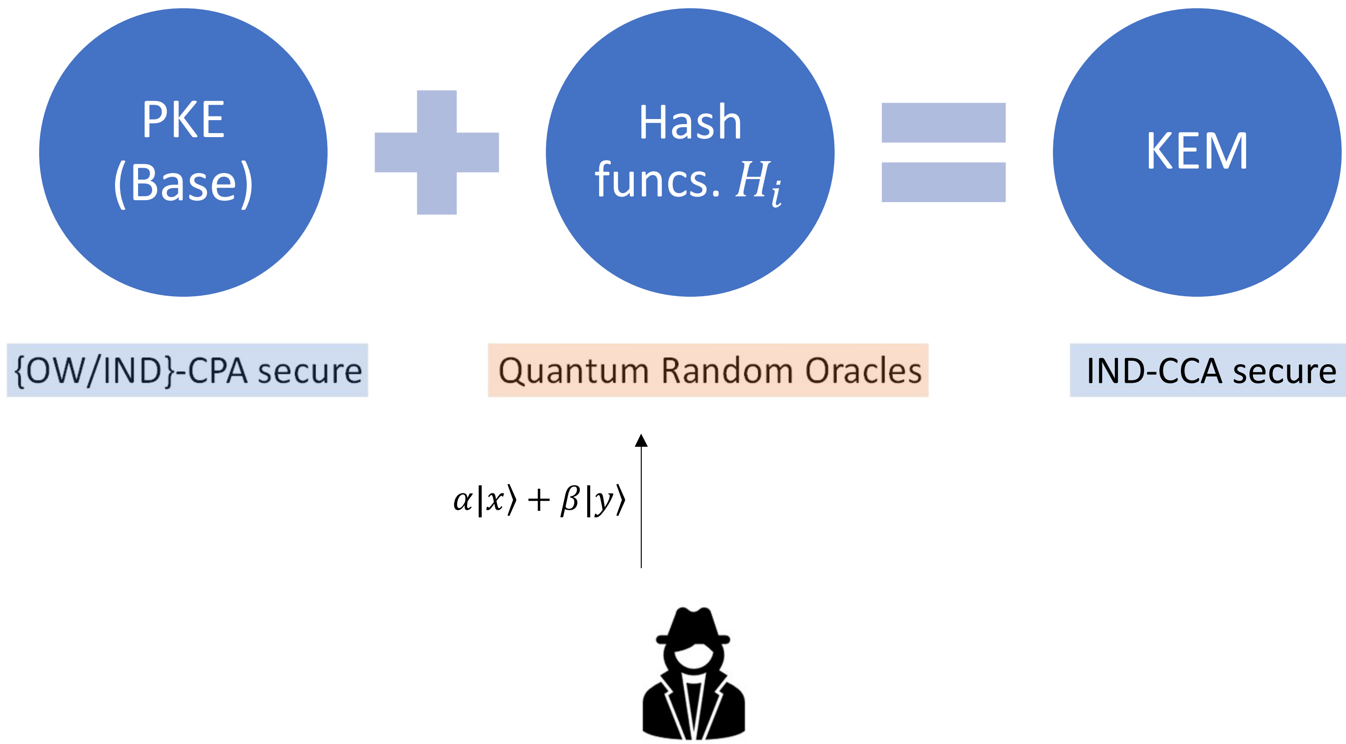
Fujisaki-Okamoto Transformation



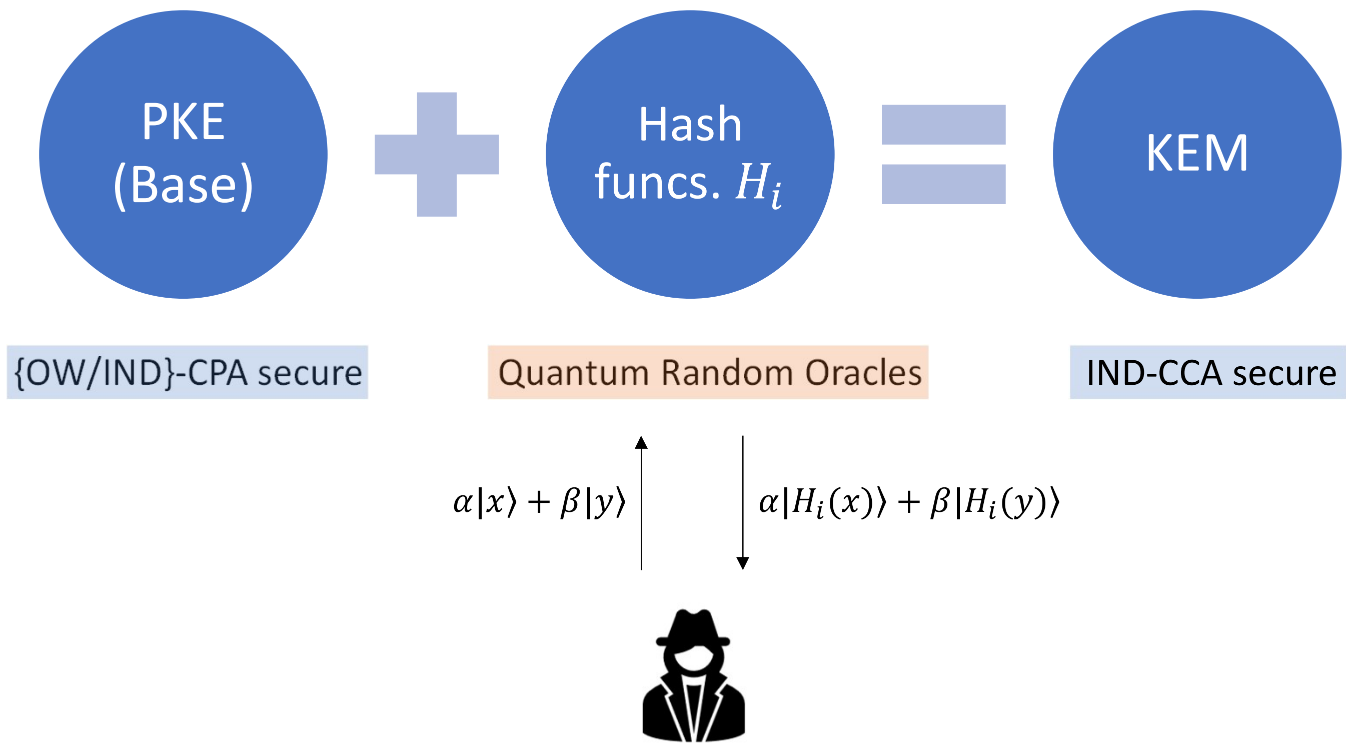
Fujisaki-Okamoto Transformation



Fujisaki-Okamoto Transformation



Fujisaki-Okamoto Transformation



Fujisaki-Okamoto Transformation

Classic McEliece

CRYSTALS-KYBER

SABER

NTRU

Fujisaki-Okamoto Transformation

- Classic McEliece
- CRYSTALS-KYBER
- SABER
- NTRU

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_{\$} \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_{\$} \mathcal{M}$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
return $(\mathsf{pk}, \mathsf{sk}')$	**return** (c, k)	**if** $c' = c$ **then**
		return $H(m', c)$
		else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

Fujisaki-Okamoto Transformation

Classic McEliece

CRYSTALS-KYBER

SABER

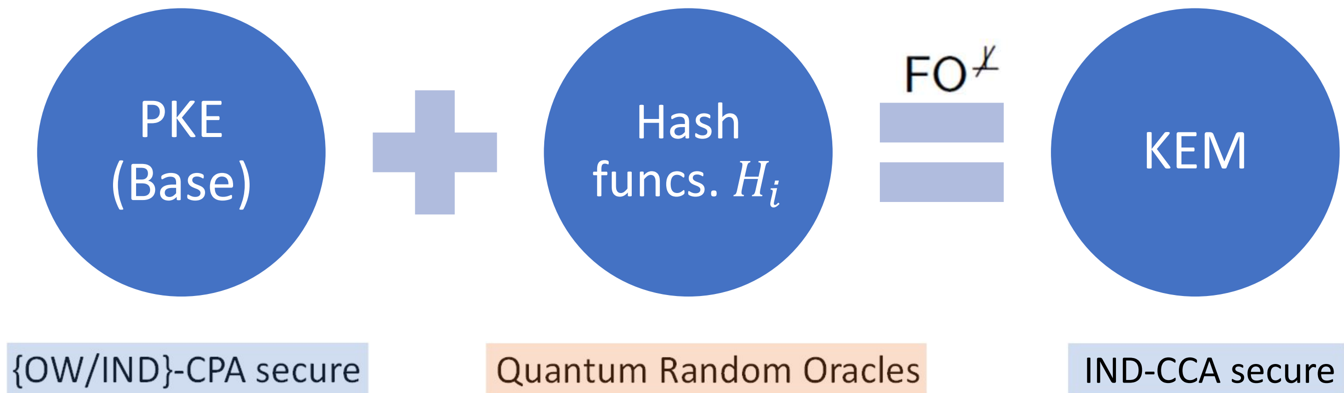
NTRU

FrodoKEM

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_{\$} \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_{\$} \mathcal{M}$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
return $(\mathsf{pk}, \mathsf{sk}')$	**return** (c, k)	**if** $c' = c$ **then**
		return $H(m', c)$
		else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

Anonymity from FO transforms



Shown in [Jiang-Zhang-Chen-Wang-Ma’18]

Anonymity from FO transforms

PKE (Base) + Hash funcs. H_i $\overset{\mathrm{FO}^{\not\perp}}{=}$ KEM

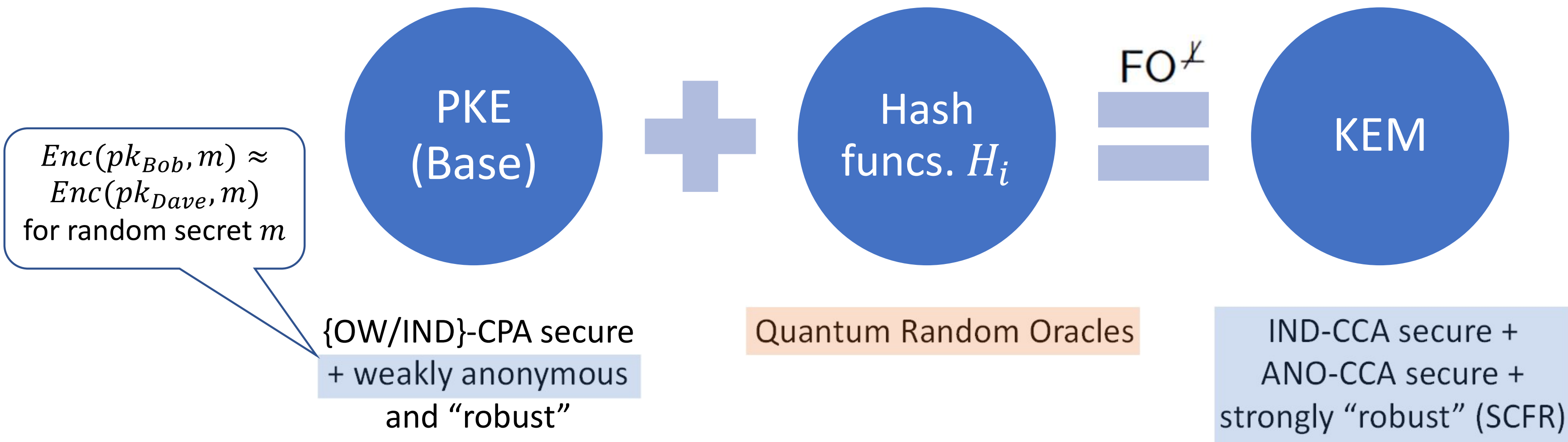
{OW/IND}-CPA secure + weakly anonymous and "robust"

Quantum Random Oracles

IND-CCA secure + ANO-CCA secure + strongly "robust" (SCFR)

Shown in [Grubbs-Maram-Paterson'22]

Anonymity from FO transforms



Shown in [Grubbs-Maram-Paterson'22]

Anonymity from FO transforms

PKE (Base) + Hash funcs. H_i $\overset{\mathrm{FO}^{\not\perp}}{=}$ KEM

$Enc(pk_{Bob}, m) \approx Enc(pk_{Dave}, m)$ for random secret m

{OW/IND}-CPA secure + weakly anonymous and "robust"

"CPA-style" collision-freeness of deterministic version of PKE

Quantum Random Oracles

IND-CCA secure + ANO-CCA secure + strongly "robust" (SCFR)

Shown in [Grubbs-Maram-Paterson'22]

Anonymity from FO transforms

PKE (Base) + Hash funcs. H_i $\overset{\mathsf{FO}^{\not\perp}}{=}$ KEM

$Enc(pk_{Bob}, m) \approx Enc(pk_{Dave}, m)$ for random secret m

{OW/IND}-CPA secure + weakly anonymous and “robust”

“CPA-style” collision-freeness of deterministic version of PKE

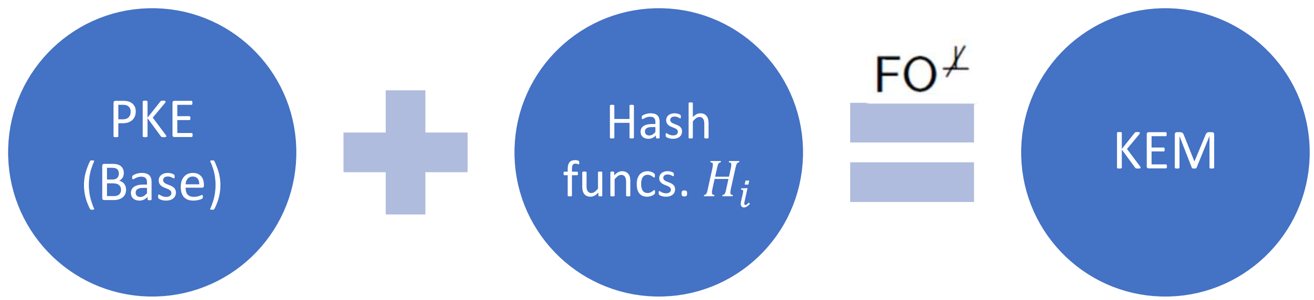
Quantum Random Oracles

IND-CCA secure + ANO-CCA secure + strongly “robust” (SCFR)

reduction

Shown in [Grubbs-Maram-Paterson’22]

Anonymity from FO transforms



$Enc(pk_{Bob}, m) \approx$
$Enc(pk_{Dave}, m)$
for random secret m

{OW/IND}-CPA secure
+ weakly anonymous
and "robust"

"CPA-style" collision-freeness of deterministic version of PKE

Quantum Random Oracles

reduction

IND-CCA secure +
ANO-CCA secure +
strongly "robust" (SCFR)

Shown in [Grubbs-Maram-Paterson'22]

Extended [Jiang et. al.'18]'s proof techniques from a *single-key* setting (IND-CCA) to a *two-key* setting (ANO-CCA).

Anonymity from FO transforms

$\mathrm{IND\text{-}CCA}^{\mathcal{A}}_{\mathsf{KEM}}$

$(\mathsf{pk}, \mathsf{sk}) \leftarrow_{\$} \mathsf{KGen}$

$b \leftarrow_{\$} \{0, 1\}$

$(C, k_0) \leftarrow_{\$} \mathsf{Encap}(\mathsf{pk})$

$k_1 \leftarrow_{\$} \mathcal{K}$

$b' \leftarrow_{\$} \mathcal{A}^{D_{\not C}(\cdot)}(\mathsf{pk}, C, k_b)$

$\mathbf{return}\ b = b'$

$\mathrm{ANO\text{-}CCA}^{\mathcal{A}}_{\mathsf{KEM}}$

$(\mathsf{pk}_0, \mathsf{sk}_0) \leftarrow_{\$} \mathsf{KGen}$

$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow_{\$} \mathsf{KGen}$

$b \leftarrow_{\$} \{0, 1\}$

$(C, k) \leftarrow_{\$} \mathsf{Encap}(\mathsf{pk}_b)$

$b' \leftarrow_{\$} \mathcal{A}^{D(\cdot,\cdot)}(\mathsf{pk}_0, \mathsf{pk}_1, (C, k))$

$\mathbf{return}\ b = b'$

Anonymity from FO transforms

$\mathrm{IND\text{-}CCA}^{\mathcal{A}}_{\mathsf{KEM}}$

$(\mathsf{pk}, \mathsf{sk}) \leftarrow_\$ \mathsf{KGen}$

$b \leftarrow_\$ \{0, 1\}$

$(C, k_0) \leftarrow_\$ \mathsf{Encap}(\mathsf{pk})$

$k_1 \leftarrow_\$ \mathcal{K}$

$b' \leftarrow_\$ \mathcal{A}^{D_{\not C}(\cdot)}(\mathsf{pk}, C, k_b)$

return $b = b'$

$\mathrm{ANO\text{-}CCA}^{\mathcal{A}}_{\mathsf{KEM}}$

$(\mathsf{pk}_0, \mathsf{sk}_0) \leftarrow_\$ \mathsf{KGen}$

$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow_\$ \mathsf{KGen}$

$b \leftarrow_\$ \{0, 1\}$

$(C, k) \leftarrow_\$ \mathsf{Encap}(\mathsf{pk}_b)$

$b' \leftarrow_\$ \mathcal{A}^{D(\cdot,\cdot)}(\mathsf{pk}_0, \mathsf{pk}_1, (C, k))$

return $b = b'$

Anonymity from FO transforms

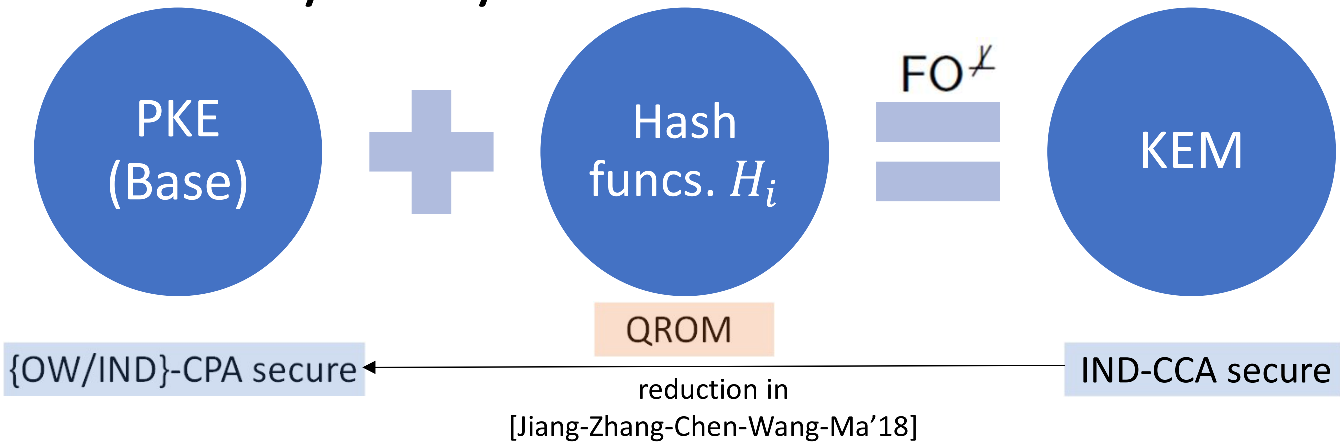
$\mathrm{IND\text{-}CCA}^{\mathcal{A}}_{\mathsf{KEM}}$

$(\mathsf{pk}, \mathsf{sk}) \leftarrow_{\$} \mathsf{KGen}$
$b \leftarrow_{\$} \{0, 1\}$
$(C, k_0) \leftarrow_{\$} \mathsf{Encap}(\mathsf{pk})$
$k_1 \leftarrow_{\$} \mathcal{K}$
$b' \leftarrow_{\$} \mathcal{A}^{D_{\not C}(\cdot)}(\mathsf{pk}, C, k_b)$
$\textbf{return } b = b'$

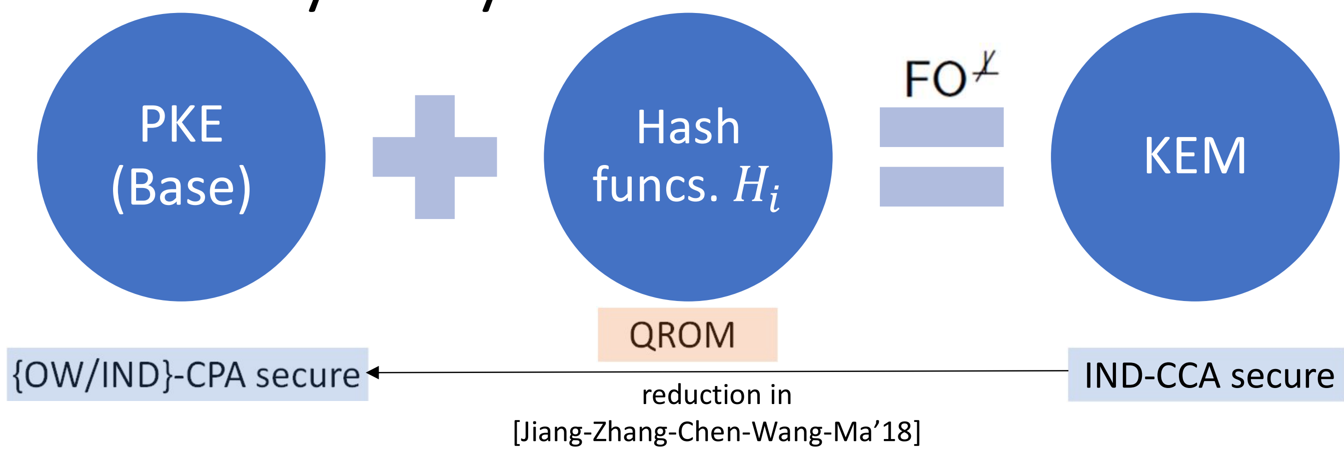
$\mathrm{ANO\text{-}CCA}^{\mathcal{A}}_{\mathsf{KEM}}$

$(\mathsf{pk}_0, \mathsf{sk}_0) \leftarrow_{\$} \mathsf{KGen}$
$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow_{\$} \mathsf{KGen}$
$b \leftarrow_{\$} \{0, 1\}$
$(C, k) \leftarrow_{\$} \mathsf{Encap}(\mathsf{pk}_b)$
$b' \leftarrow_{\$} \mathcal{A}^{D(\cdot,\cdot)}(\mathsf{pk}_0, \mathsf{pk}_1, (C, k))$
$\textbf{return } b = b'$

Anonymity from FO transforms



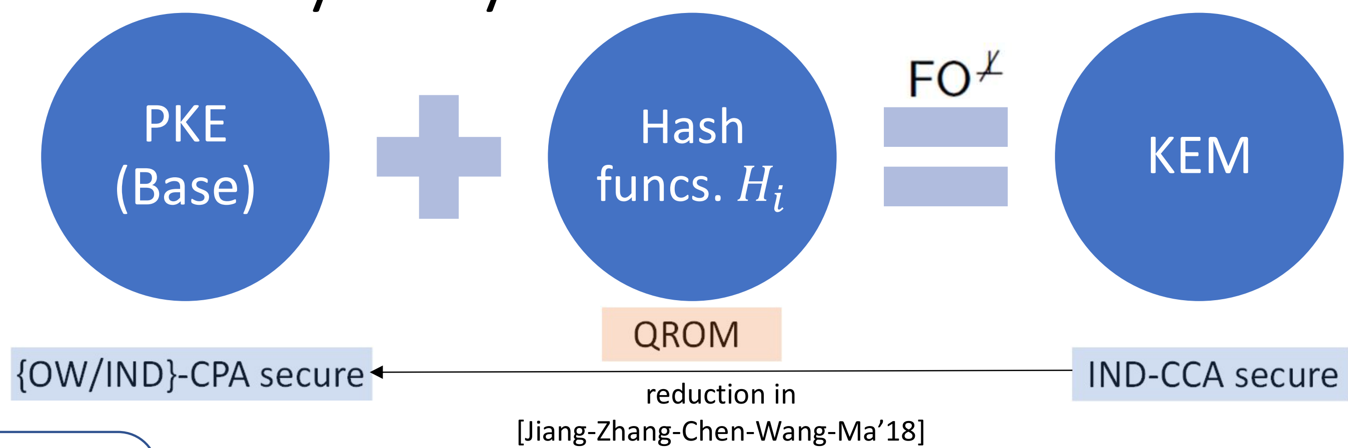
Anonymity from FO transforms



$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$m \leftarrow_\$ \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
return (c, k)	**if** $c' = c$ **then**
	return $H(m', c)$
	else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

Anonymity from FO transforms

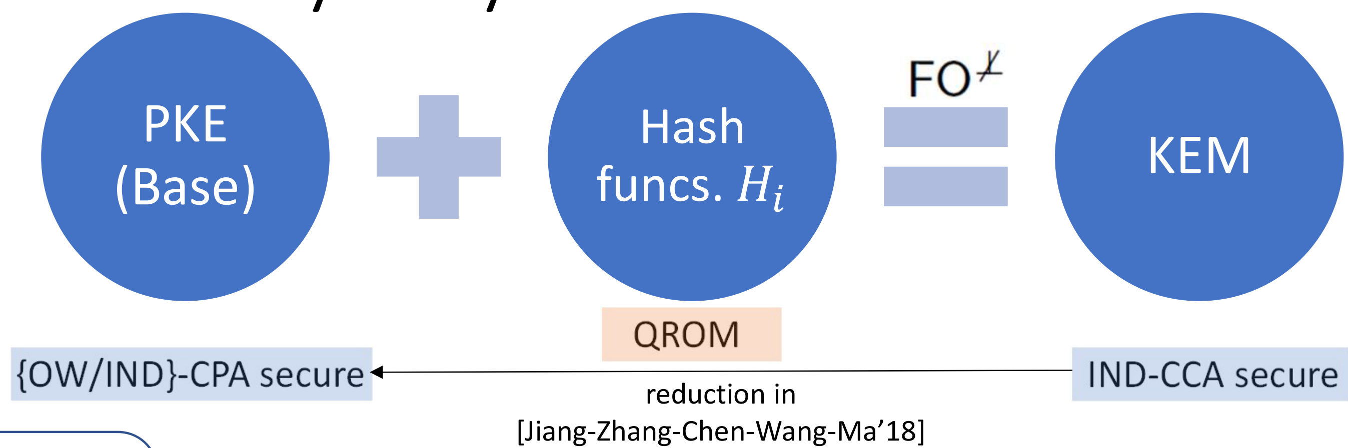


Replace key-derivation step with "$k \leftarrow H'(c)$" …
(for secret QRO H')

$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
1 : $m \leftarrow_{\$} \mathcal{M}$	1 : Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
2 : $c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	2 : $m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
3 : $k \leftarrow H(m, c)$	3 : $c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
4 : **return** (c, k)	4 : **if** $c' = c$ **then**
	5 : **return** $H(m', c)$
	6 : **else return** $H(s, c)$

$\mathsf{FO}^{\not\perp}$

Anonymity from FO transforms



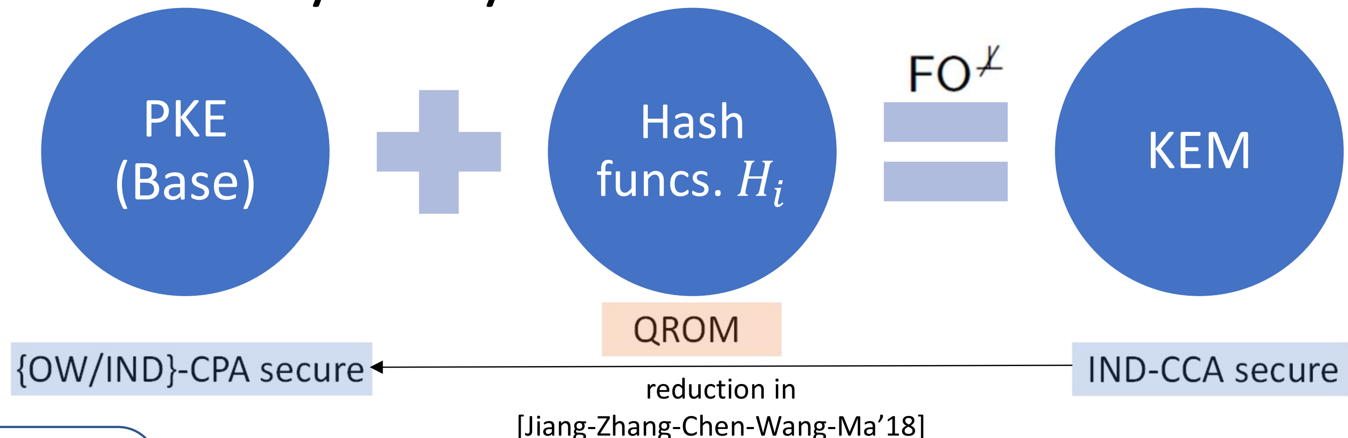
Replace key-derivation step with "$k \leftarrow H'(c)$" ...
(for secret QRO H')

... when (m, c) satisfies.

$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$m \leftarrow_{\$} \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
return (c, k)	**if** $c' = c$ **then**
	return $H(m', c)$
	else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

Anonymity from FO transforms



Replace key-derivation step with "$k \leftarrow H'(c)$" ...
(for secret QRO H')

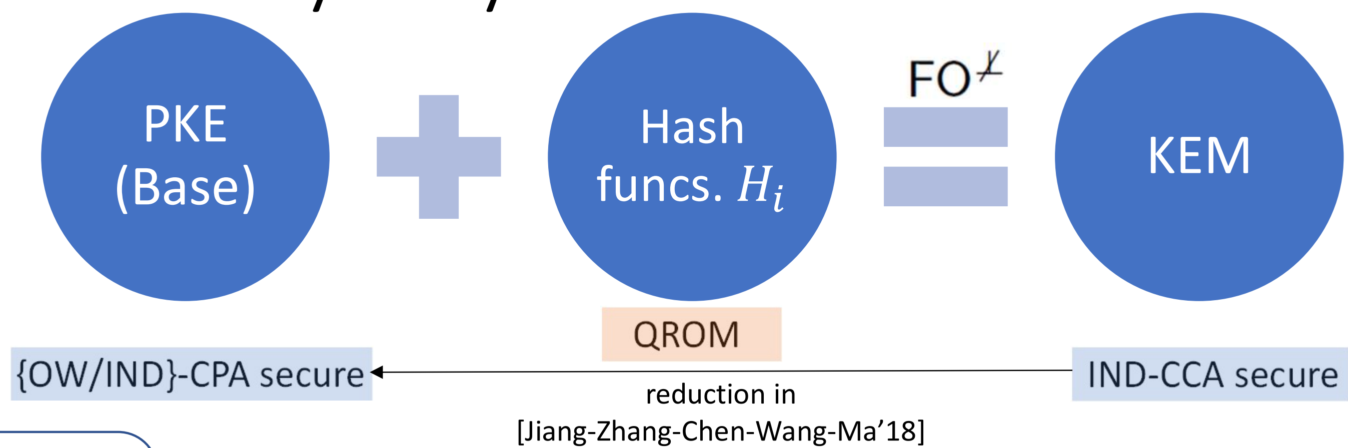
... when (m, c) satisfies.

Replacement is justified if there do not exist pairs (m_1, c) and (m_2, c) ...

$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$m \leftarrow_\$ \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
return (c, k)	**if** $c' = c$ **then**
	return $H(m', c)$
	else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

Anonymity from FO transforms



Replace key-derivation step with "$k \leftarrow H'(c)$" ...
(for secret QRO H')

... when (m, c) satisfies.

Replacement is justified if there do not exist pairs (m_1, c) and (m_2, c) ...

... i.e., PKE correctness.

$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
1 : $m \leftarrow_{\$} \mathcal{M}$	1 : Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
2 : $c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	2 : $m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
3 : $k \leftarrow H(m, c)$	3 : $c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
4 : **return** (c, k)	4 : **if** $c' = c$ **then**
	5 : **return** $H(m', c)$
	6 : **else return** $H(s, c)$

$\mathsf{FO}^{\not\perp}$

Anonymity from FO transforms

PKE (Base) + Hash funcs. H_i $\overset{\mathsf{FO}^{\not\perp}}{=}$ KEM

QROM

{OW/IND}-CPA secure ← IND-CCA secure

reduction in [Jiang-Zhang-Chen-Wang-Ma'18]

Replace key-derivation step with "$k \leftarrow H'(c)$" ...
(for secret QRO H')

... when (m, c) satisfies.

Replacement is justified if there do not exist pairs (m_1, c) and (m_2, c) ...

... i.e., PKE correctness.

$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
1 : $m \leftarrow_{\$} \mathcal{M}$	1 : Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
2 : $c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	2 : $m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
3 : $k \leftarrow H(m, c)$	3 : $c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
4 : **return** (c, k)	4 : **if** $c' = c$ **then**
	5 : **return** $H(m', c)$
	6 : **else return** $H(s, c)$

$\mathsf{FO}^{\not\perp}$

Can now return $H'(c)$ instead ...

Anonymity from FO transforms

PKE (Base) + Hash funcs. H_i $\overset{\mathsf{FO}^{\not\perp}}{=}$ KEM

QROM

{OW/IND}-CPA secure ← IND-CCA secure

reduction in
[Jiang-Zhang-Chen-Wang-Ma'18]

Replace key-derivation step with "$k \leftarrow H'(c)$" ...
(for secret QRO H')

... when (m, c) satisfies.

Replacement is justified if there do not exist pairs (m_1, c) and (m_2, c) ...

... i.e., PKE correctness.

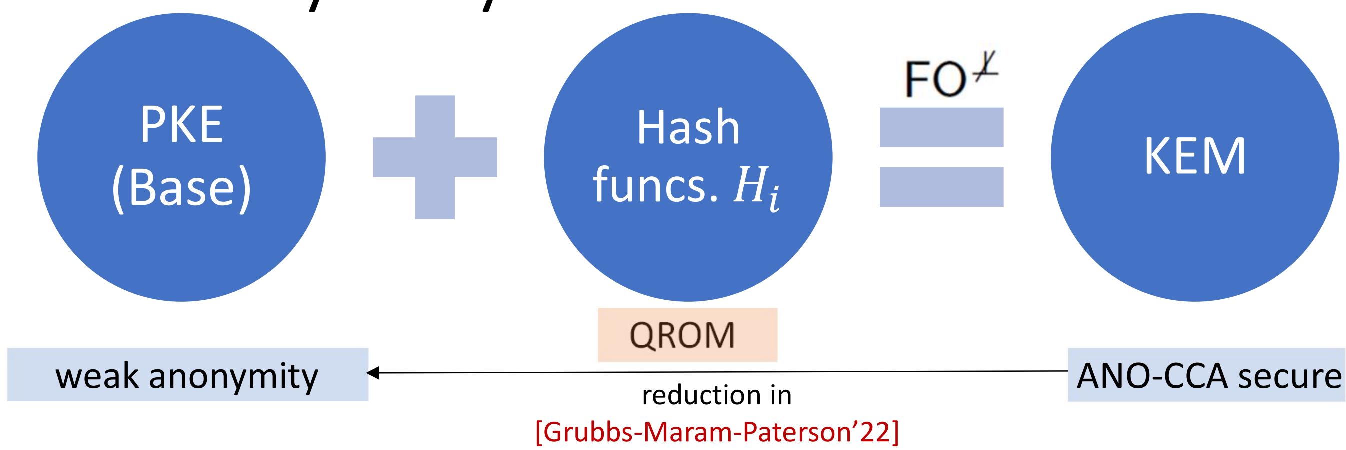
Encap(pk)	Decap(sk$'$, c)
1 : $m \leftarrow_\$ \mathcal{M}$	1 : Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
2 : $c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	2 : $m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
3 : $k \leftarrow H(m, c)$	3 : $c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
4 : **return** (c, k)	4 : **if** $c' = c$ **then**
	5 : **return** $H(m', c)$
	6 : **else return** $H(s, c)$

$\mathsf{FO}^{\not\perp}$

Can now return $H'(c)$ instead ...

... where sk' no longer required!

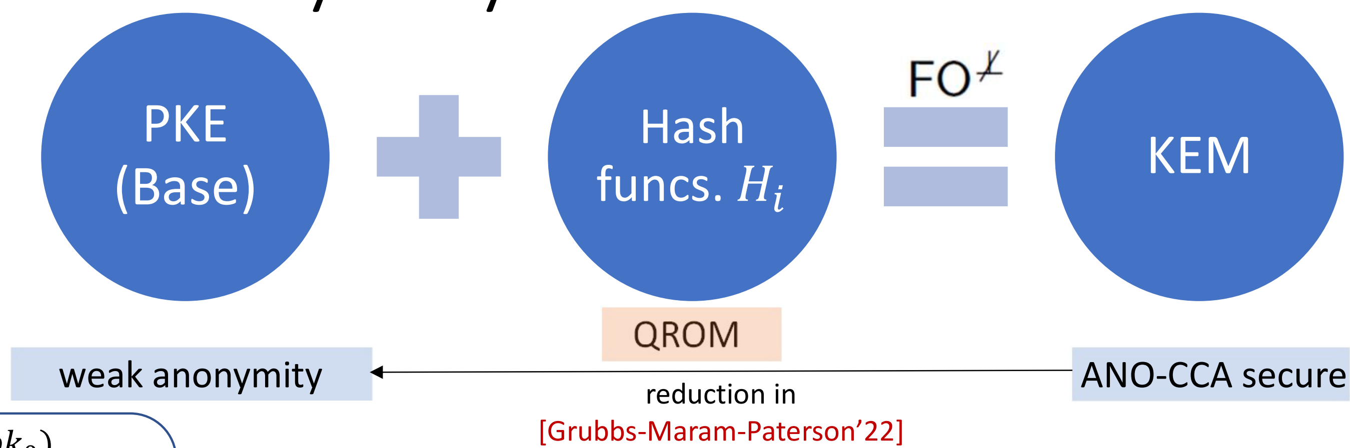
Anonymity from FO transforms

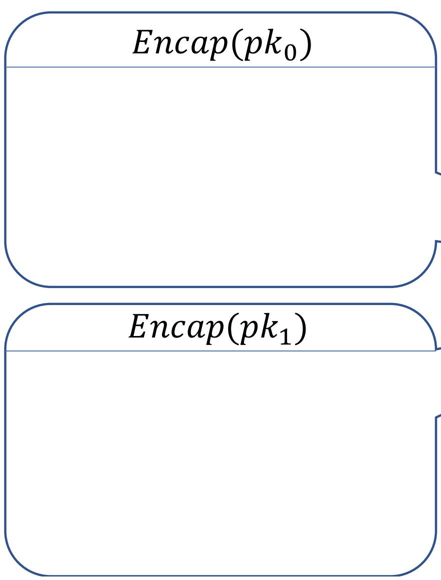


$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$m \leftarrow_{\$} \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
return (c, k)	**if** $c' = c$ **then**
	return $H(m', c)$
	else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

Anonymity from FO transforms

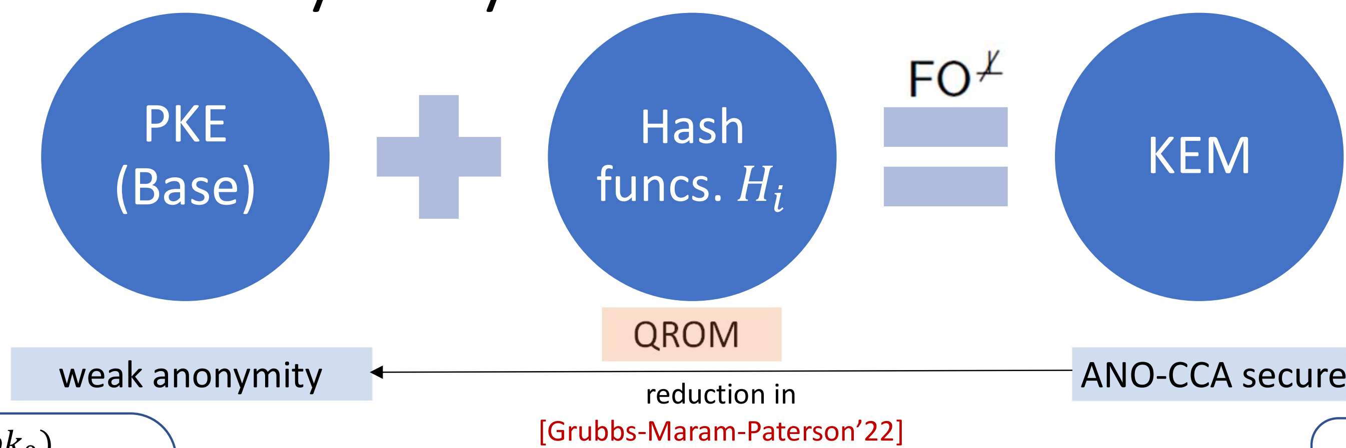




$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$m \leftarrow_{\$} \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
return (c, k)	**if** $c' = c$ **then**
	return $H(m', c)$
	else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

Anonymity from FO transforms



$Encap(pk_0)$

$Encap(pk_1)$

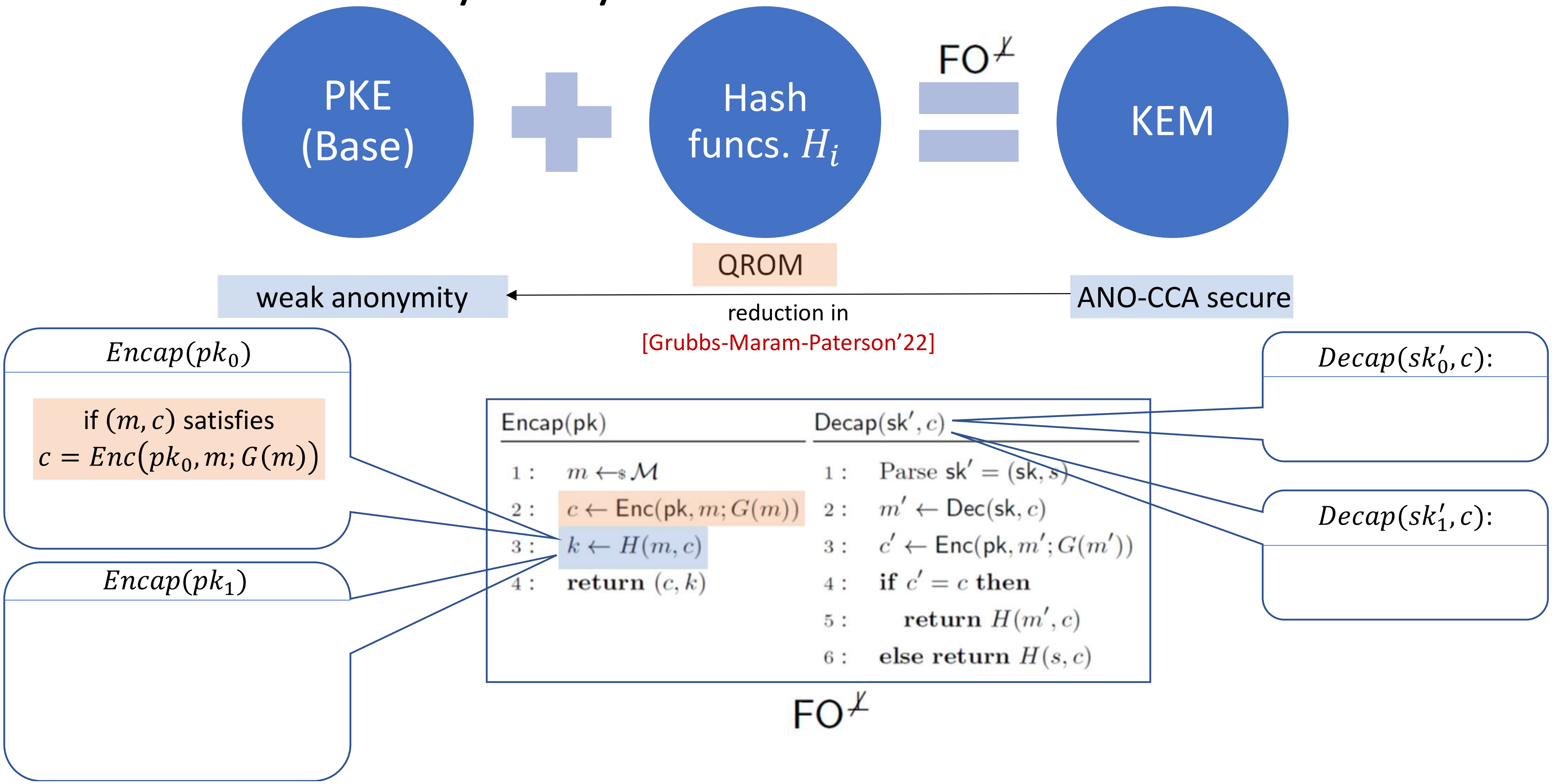
$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
1 : $m \leftarrow_\$ \mathcal{M}$	1 : Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
2 : $c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	2 : $m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
3 : $k \leftarrow H(m, c)$	3 : $c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
4 : **return** (c, k)	4 : **if** $c' = c$ **then**
	5 : **return** $H(m', c)$
	6 : **else return** $H(s, c)$

$\mathsf{FO}^{\not\perp}$

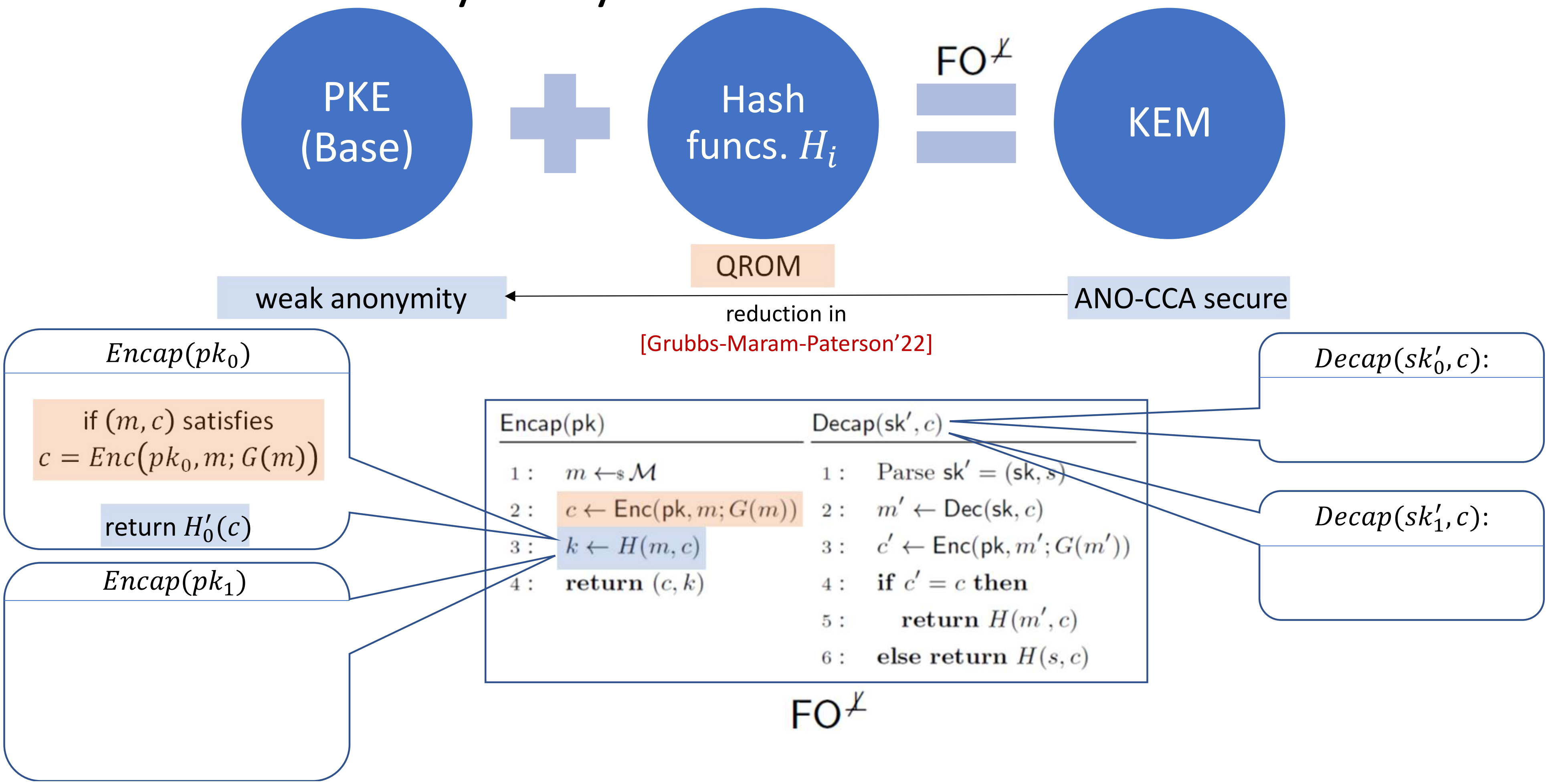
$Decap(sk_0', c)$:

$Decap(sk_1', c)$:

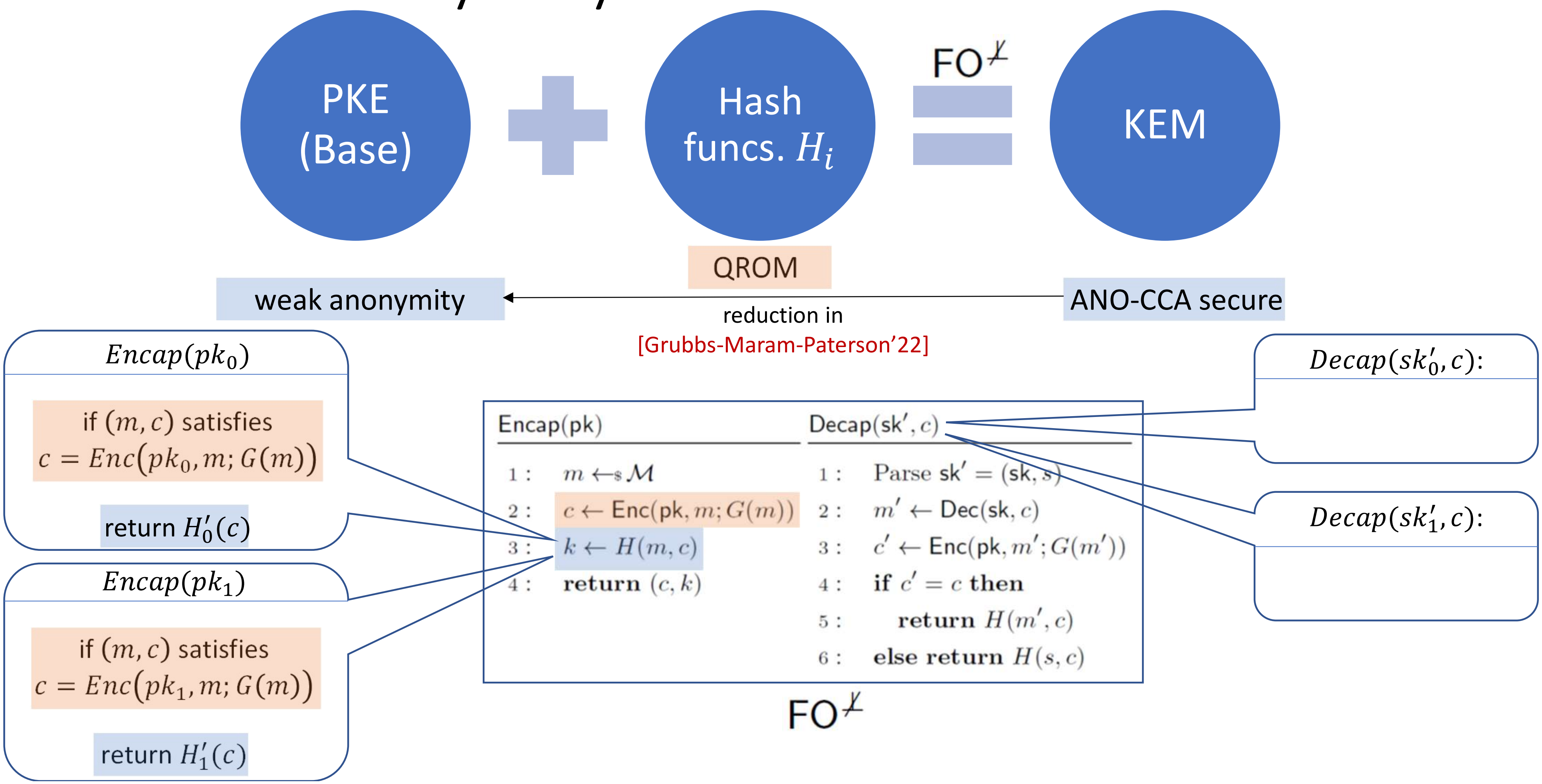
Anonymity from FO transforms



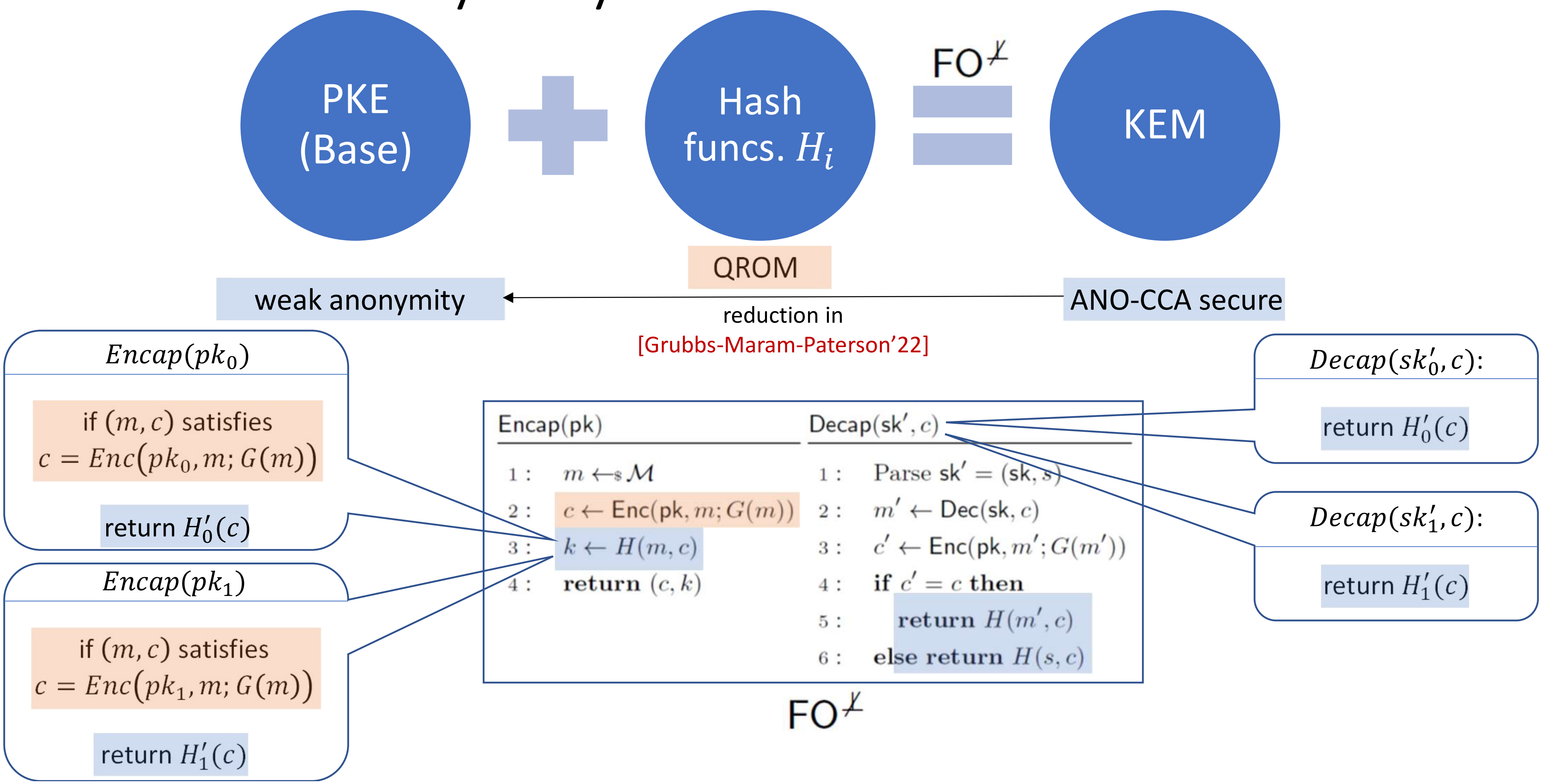
Anonymity from FO transforms



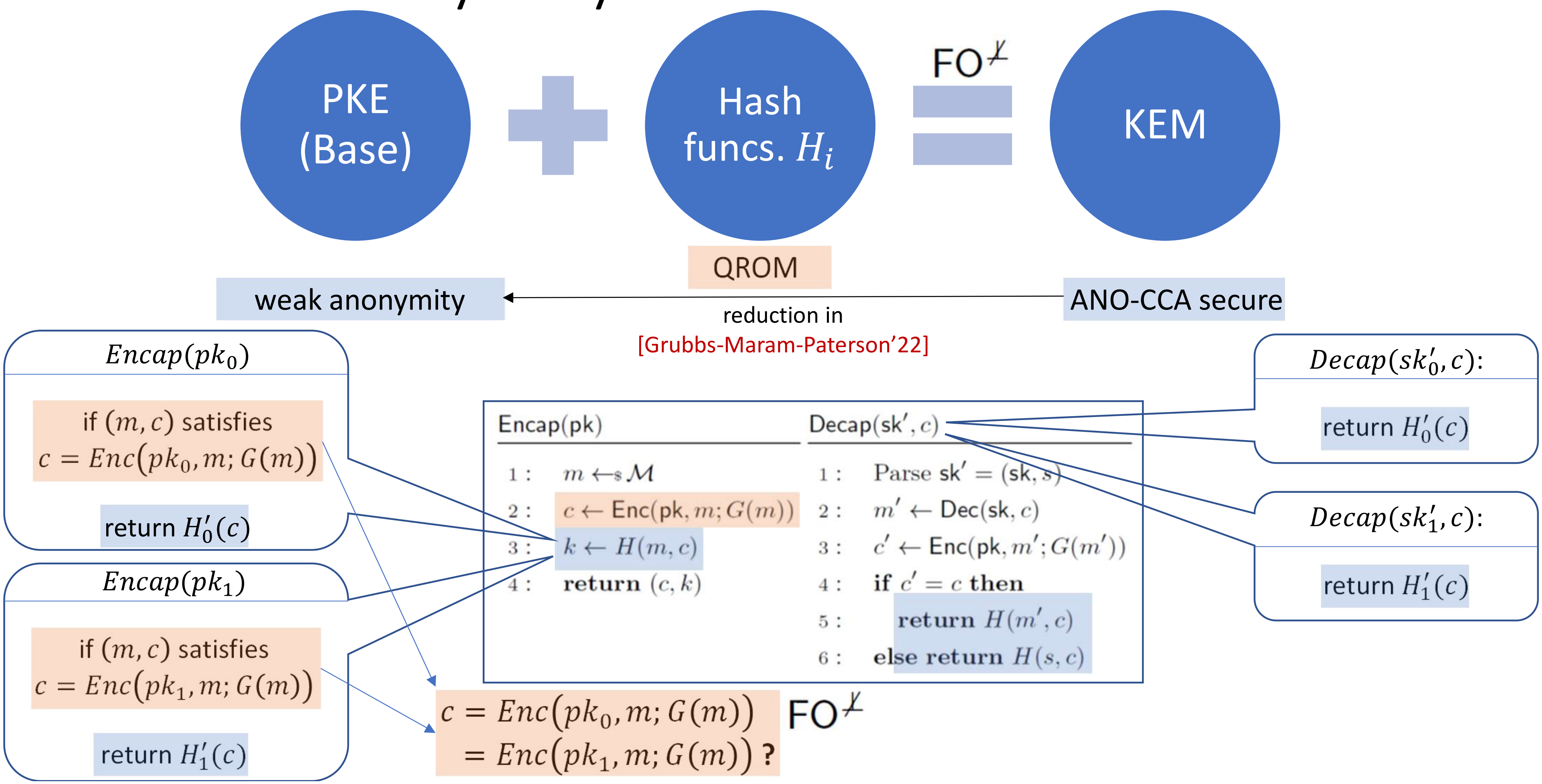
Anonymity from FO transforms



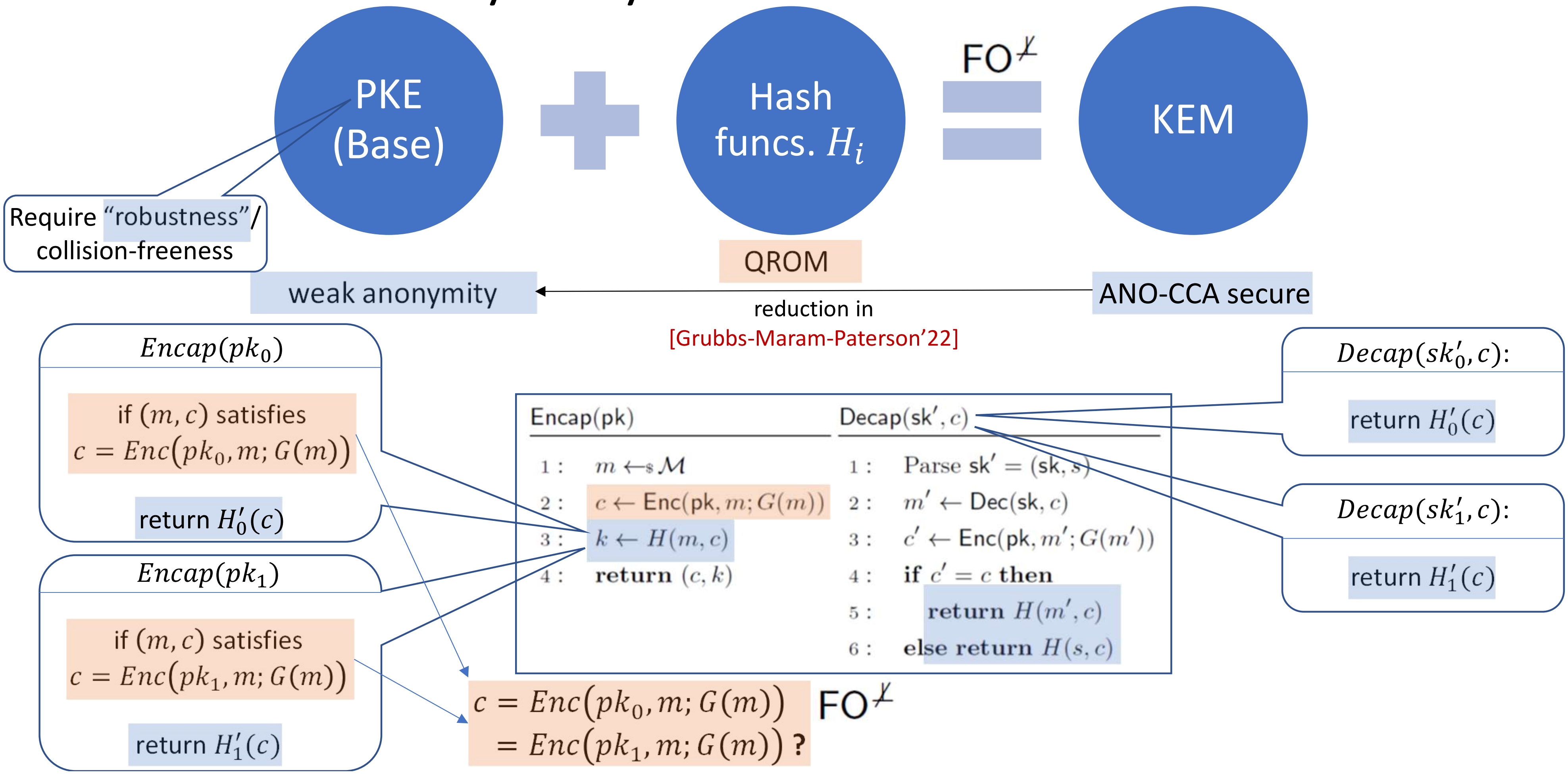
Anonymity from FO transforms



Anonymity from FO transforms



Anonymity from FO transforms



Fujisaki-Okamoto Transformation

- Classic McEliece
- CRYSTALS-KYBER
- SABER
- NTRU

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow\!\!\$\, \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow\!\!\$\, \mathcal{M}$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
return $(\mathsf{pk}, \mathsf{sk}')$	**return** (c, k)	**if** $c' = c$ **then**
		return $H(m', c)$
		else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

Fujisaki-Okamoto Transformation

Classic McEliece

CRYSTALS-KYBER

SABER

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_{\$} \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_{\$} \mathcal{M}$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
return $(\mathsf{pk}, \mathsf{sk}')$	**return** (c, k)	**if** $c' = c$ **then**
		return $H(m', c)$
		else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

NTRU

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_{\$} \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_{\$} \mathcal{M}$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$k \leftarrow H(m)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
return $(\mathsf{pk}, \mathsf{sk}')$	**return** (c, k)	**if** $c' = c$ **then**
		return $H(m')$
		else return $H(s, c)$

$\mathsf{FO}_m^{\not\perp}$

Fujisaki-Okamoto Transformation

Classic McEliece

CRYSTALS-KYBER

SABER

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_{\$} \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_{\$} \mathcal{M}$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
return $(\mathsf{pk}, \mathsf{sk}')$	**return** (c, k)	**if** $c' = c$ **then**
		return $H(m', c)$
		else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

NTRU

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_{\$} \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_{\$} \mathcal{M}$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$k \leftarrow H(m)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
return $(\mathsf{pk}, \mathsf{sk}')$	**return** (c, k)	**if** $c' = c$ **then**
		return $H(m')$
		else return $H(s, c)$

$\mathsf{FO}_m^{\not\perp}$

Fujisaki-Okamoto Transformation

Classic McEliece
CRYSTALS-KYBER
SABER

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_\$ \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_\$ \mathcal{M}$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
return $(\mathsf{pk}, \mathsf{sk}')$	**return** (c, k)	**if** $c' = c$ **then**
		return $H(m', c)$
		else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

Difficult to extend our simulation "trick".

NTRU

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_\$ \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_\$ \mathcal{M}$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$k \leftarrow H(m)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
return $(\mathsf{pk}, \mathsf{sk}')$	**return** (c, k)	**if** $c' = c$ **then**
		return $H(m')$
		else return $H(s, c)$

$\mathsf{FO}^{\not\perp}_m$

Fujisaki-Okamoto Transformation

Classic McEliece

CRYSTALS-KYBER

SABER

NTRU

[Xagawa'22] showed ANO-CCA security (and "robustness") of NTRU!

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_{\$} \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_{\$} \mathcal{M}$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
return $(\mathsf{pk}, \mathsf{sk}')$	**return** (c, k)	**if** $c' = c$ **then**
		return $H(m', c)$
		else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

Difficult to extend our simulation "trick".

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_{\$} \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_{\$} \mathcal{M}$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$k \leftarrow H(m)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
return $(\mathsf{pk}, \mathsf{sk}')$	**return** (c, k)	**if** $c' = c$ **then**
		return $H(m')$
		else return $H(s, c)$

$\mathsf{FO}^{\not\perp}_m$

Fujisaki-Okamoto Transformation

Classic McEliece

CRYSTALS-KYBER

SABER

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_\$ \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_\$ \mathcal{M}$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
return $(\mathsf{pk}, \mathsf{sk}')$	**return** (c, k)	**if** $c' = c$ **then**
		return $H(m', c)$
		else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

Difficult to extend our simulation "trick".

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_\$ \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_\$ \mathcal{M}$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$k \leftarrow H(m)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
return $(\mathsf{pk}, \mathsf{sk}')$	**return** (c, k)	**if** $c' = c$ **then**
		return $H(m')$
		else return $H(s, c)$

$\mathsf{FO}^{\not\perp}_m$

NTRU

[Xagawa'22] showed ANO-CCA security (and "robustness") of NTRU!

Relied on a stronger *single-key* notion, i.e., strong pseudo-randomness.

Anonymity from FO transforms

Public-Key Encryption/KEMs

- Classic McEliece
- CRYSTALS-KYBER
- NTRU
- SABER

"Implicit-rejection" KEMs!

Cannot be even weakly robust.

Public-Key Encryption/KEMs

- BIKE
- FrodoKEM
- HQC
- NTRU Prime
- SIKE

Shown in [Grubbs-Maram-Paterson'22]; generalization of [Mohassel'10].

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

KEM + DEM = PKE (Hybrid)

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + weakly robust (WROB)

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure

Anonymity from FO transforms

Public-Key Encryption/KEMs

Classic McEliece
CRYSTALS-KYBER
NTRU
SABER

"Implicit-rejection" KEMs!

Cannot be even weakly robust.

Public-Key Encryption/KEMs

BIKE
FrodoKEM
HQC
NTRU Prime
SIKE

Shown in [Grubbs-Maram-Paterson'22]; generalization of [Mohassel'10].

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

KEM + DEM ≠ PKE (Hybrid)

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure
+ strongly "robust" (SCFR)

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure
(and XROB)

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure +
ANO-CCA secure

Anonymity from FO transforms

Public-Key Encryption/KEMs

- Classic McEliece
- CRYSTALS-KYBER
- NTRU
- SABER

"Implicit-rejection" KEMs!

Cannot be even weakly robust.

Public-Key Encryption/KEMs

- BIKE
- FrodoKEM
- HQC
- NTRU Prime
- SIKE

Shown in [Grubbs-Maram-Paterson'22]; generalization of [Mohassel'10].

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

$FO^{\pm}$-based KEM + DEM = PKE (Hybrid)

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure ✓

Anonymity from FO transforms

Public-Key Encryption/KEMs

Classic McEliece
CRYSTALS-KYBER
NTRU
SABER

"Implicit-rejection" KEMs!

Cannot be even weakly robust.

Public-Key Encryption/KEMs

BIKE
FrodoKEM
HQC
NTRU Prime
SIKE

Shown in [Grubbs-Maram-Paterson'22]; generalization of [Mohassel'10].

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

$FO^{\pm}$-based KEM + DEM = PKE (Hybrid)

$c \leftarrow Enc^{base}(pk_{Bob}, m)$ should have large enough entropy.

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure ✓

Anonymity from FO transforms

Public-Key Encryption/KEMs

- Classic McEliece
- CRYSTALS-KYBER
- NTRU
- SABER

"Implicit-rejection" KEMs!

Cannot be even weakly robust.

Public-Key Encryption/KEMs

- BIKE
- FrodoKEM
- HQC
- NTRU Prime
- SIKE

Shown in [Grubbs-Maram-Paterson'22]; generalization of [Mohassel'10].

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

Implicitly assumes "robustness" of base PKE

$FO^{\pm}$-based KEM + DEM = PKE (Hybrid)

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

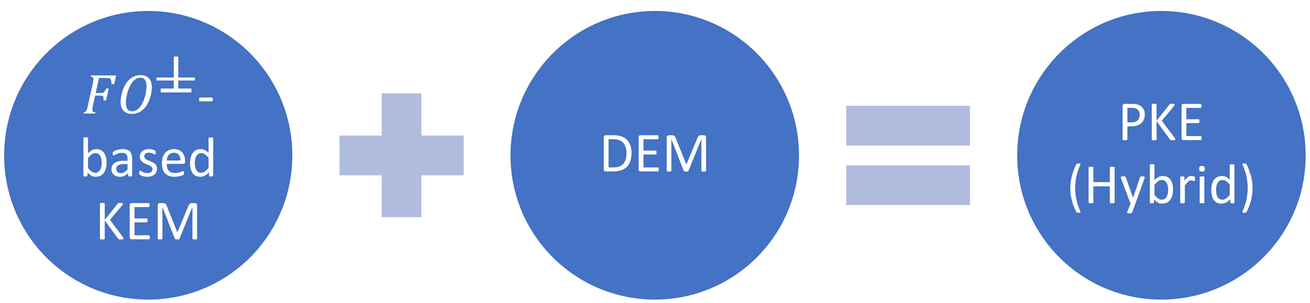
IND-CCA secure + ANO-CCA secure ✓

Classic McEliece (CM)

Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

$c \leftarrow Enc^{base}(pk_{Bob}, m)$ should have large enough entropy.



$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure

Classic McEliece (CM)

Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

CM uses a *deterministic* base PKE scheme.

CM KEM + DEM = PKE (Hybrid)

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

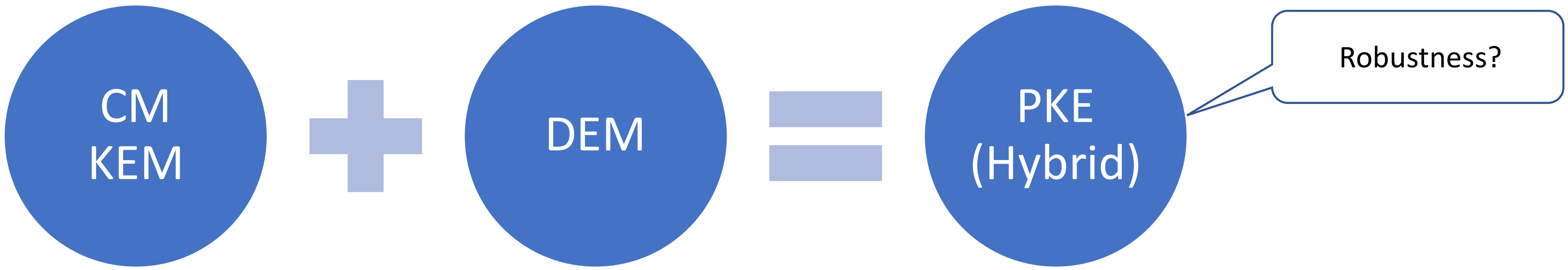
AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure

Classic McEliece (CM)

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$



$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$ $c_{DEM} \leftarrow Enc^{sym}(k, m)$ $(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

Classic McEliece (CM)

2.2.3 Encoding subroutine

The following algorithm ENCODE takes two inputs: a weight-t column vector $e \in \mathbb{F}_2^n$; and a public key T, i.e., an $(n-k) \times k$ matrix over $\mathbb{F}_2$. The algorithm output $\text{ENCODE}(e, T)$ is a vector $C_0 \in \mathbb{F}_2^{n-k}$. Here is the algorithm:

1. Define $H = (I_{n-k} \mid T)$.
2. Compute and return $C_0 = He \in \mathbb{F}_2^{n-k}$.

Classic McEliece (CM)

2.2.3 Encoding subroutine

The following algorithm ENCODE takes two inputs: a weight-t column vector $e \in \mathbb{F}_2^n$; and a public key T, i.e., an $(n-k) \times k$ matrix over $\mathbb{F}_2$. The algorithm output ENCODE(e, T) is a vector $C_0 \in \mathbb{F}_2^{n-k}$. Here is the algorithm:

1. Define $H = (I_{n-k} \mid T)$.
2. Compute and return $C_0 = He \in \mathbb{F}_2^{n-k}$.

Classic McEliece (CM)

2.2.3 Encoding subroutine

The following algorithm ENCODE takes two inputs: a weight-t column vector $e \in \mathbb{F}_2^n$; and a public key T, i.e., an $(n-k) \times k$ matrix over $\mathbb{F}_2$. The algorithm output $\text{ENCODE}(e, T)$ is a vector $C_0 \in \mathbb{F}_2^{n-k}$. Here is the algorithm:

1. Define $H = (I_{n-k} \mid T)$.
2. Compute and return $C_0 = He \in \mathbb{F}_2^{n-k}$.

Classic McEliece (CM)

2.2.3 Encoding subroutine

The following algorithm ENCODE takes two inputs: a weight-t column vector $e \in \mathbb{F}_2^n$; and a public key T, i.e., an $(n-k) \times k$ matrix over $\mathbb{F}_2$. The algorithm output $\text{ENCODE}(e, T)$ is a vector $C_0 \in \mathbb{F}_2^{n-k}$. Here is the algorithm:

1. Define $H = (I_{n-k} \mid T)$.
2. Compute and return $C_0 = He \in \mathbb{F}_2^{n-k}$.

Classic McEliece (CM)

2.2.3 Encoding subroutine

The following algorithm Encode takes two inputs: a weight-t column vector $e \in \mathbb{F}_2^n$; and a public key T, i.e., an $(n-k) \times k$ matrix over $\mathbb{F}_2$. The algorithm output $\text{Encode}(e, T)$ is a vector $C_0 \in \mathbb{F}_2^{n-k}$. Here is the algorithm:

1. Define $H = (I_{n-k} \mid T)$.
2. Compute and return $C_0 = He \in \mathbb{F}_2^{n-k}$.

Classic McEliece (CM)

2.2.3 Encoding subroutine

The following algorithm ENCODE takes two inputs: a weight-t column vector $e \in \mathbb{F}_2^n$; and a public key T, i.e., an $(n-k) \times k$ matrix over $\mathbb{F}_2$. The algorithm output ENCODE(e, T) is a vector $C_0 \in \mathbb{F}_2^{n-k}$. Here is the algorithm:

1. Define $H = (I_{n-k} \mid T)$.
2. Compute and return $C_0 = He \in \mathbb{F}_2^{n-k}$.

Fix any "message" $e = \binom{e_{n-k}}{0^k}$:

Classic McEliece (CM)

2.2.3 Encoding subroutine

The following algorithm ENCODE takes two inputs: a weight-t column vector $e \in \mathbb{F}_2^n$; and a public key T, i.e., an $(n-k) \times k$ matrix over $\mathbb{F}_2$. The algorithm output ENCODE(e, T) is a vector $C_0 \in \mathbb{F}_2^{n-k}$. Here is the algorithm:

1. Define $H = (I_{n-k} \mid T)$.
2. Compute and return $C_0 = He \in \mathbb{F}_2^{n-k}$.

Fix any "message" $e = \binom{e_{n-k}}{0^k}$:

- ($n - k \ \geq t$ in all CM parameters)

Classic McEliece (CM)

2.2.3 Encoding subroutine

The following algorithm ENCODE takes two inputs: a weight-t column vector $e \in \mathbb{F}_2^n$; and a public key T, i.e., an $(n-k) \times k$ matrix over $\mathbb{F}_2$. The algorithm output ENCODE(e, T) is a vector $C_0 \in \mathbb{F}_2^{n-k}$. Here is the algorithm:

1. Define $H = (I_{n-k} \mid T)$.
2. Compute and return $C_0 = He \in \mathbb{F}_2^{n-k}$.

Fix any “message” $e = \binom{e_{n-k}}{0^k}$:

- $(n - k \ \geq t$ in all CM parameters)
- $C_0 = (I_{n-k}|T)\binom{e_{n-k}}{0^k} = e_{n-k}$ – i.e., independent of public-key T.

Classic McEliece (CM)

2.2.3 Encoding subroutine

The following algorithm ENCODE takes two inputs: a weight-t column vector $e \in \mathbb{F}_2^n$; and a public key T, i.e., an $(n-k) \times k$ matrix over $\mathbb{F}_2$. The algorithm output ENCODE(e, T) is a vector $C_0 \in \mathbb{F}_2^{n-k}$. Here is the algorithm:

1. Define $H = (I_{n-k} \mid T)$.
2. Compute and return $C_0 = He \in \mathbb{F}_2^{n-k}$.

Fix any "message" $e = \binom{e_{n-k}}{0^k}$:

- ($n - k \geq t$ in all CM parameters)
- $C_0 = (I_{n-k}|T)\binom{e_{n-k}}{0^k} = e_{n-k}$ – i.e., independent of public-key T.
- Because of perfect correctness, C_0 must decrypt to fixed e under *any private key* of CM's base PKE scheme.

Classic McEliece (CM)

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

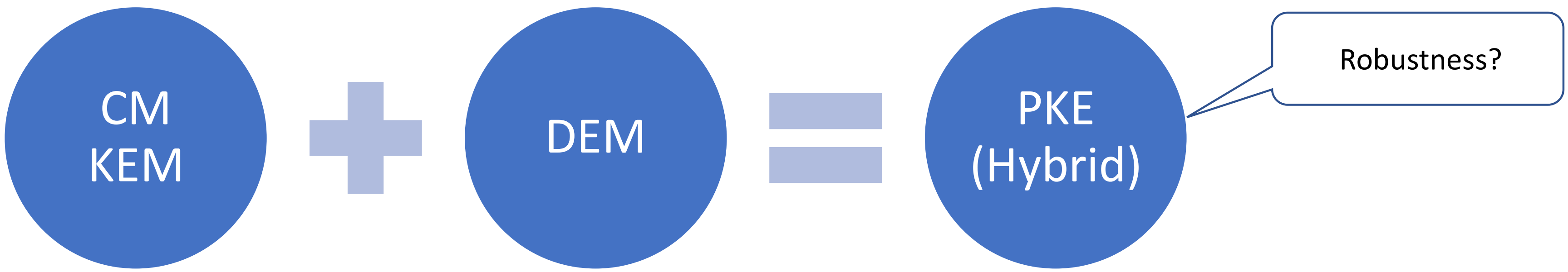
CM KEM + DEM = PKE (Hybrid)

Robustness?

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$ $c_{DEM} \leftarrow Enc^{sym}(k, m)$ $(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

Classic McEliece (CM)

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$



$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$ $c_{DEM} \leftarrow Enc^{sym}(k, m)$ $(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

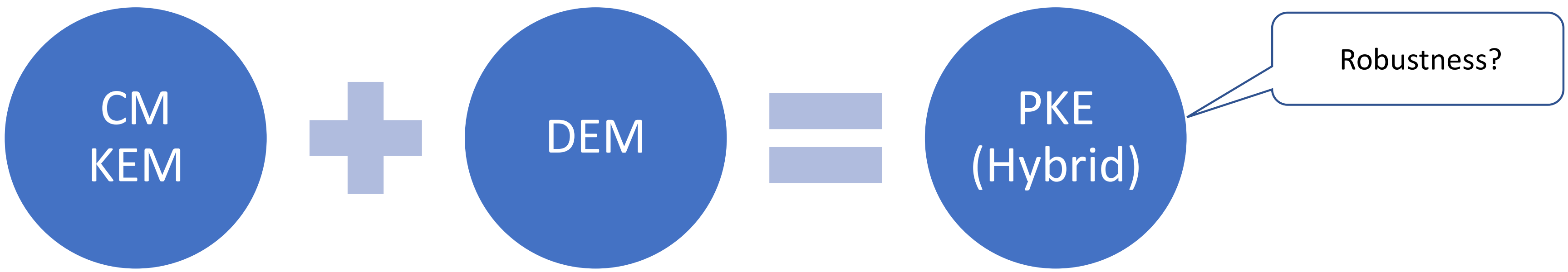
2.4.5 Encapsulation

The following randomized algorithm ENCAP takes as input a public key T. It outputs a ciphertext C and a session key K. Here is the algorithm:

1. Use FIXEDWEIGHT to generate a vector $e \in \mathbb{F}_2^n$ of weight t.
2. Compute $C_0 = \text{ENCODE}(e, T)$.
3. Compute $C_1 = \mathsf{H}(2, e)$; see Section 2.5.2 for H input encodings. Put $C = (C_0, C_1)$.
4. Compute $K = \mathsf{H}(1, e, C)$; see Section 2.5.2 for H input encodings.
5. Output ciphertext C and session key K.

Classic McEliece (CM)

$KEM = (KGen, Encap, Decap)$ $\quad DEM = (Enc^{sym}, Dec^{sym})$ $\quad PKE = (KGen, Enc, Dec)$



$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$ $\quad c_{DEM} \leftarrow Enc^{sym}(k, m)$ $\quad (c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

2.4.5 Encapsulation

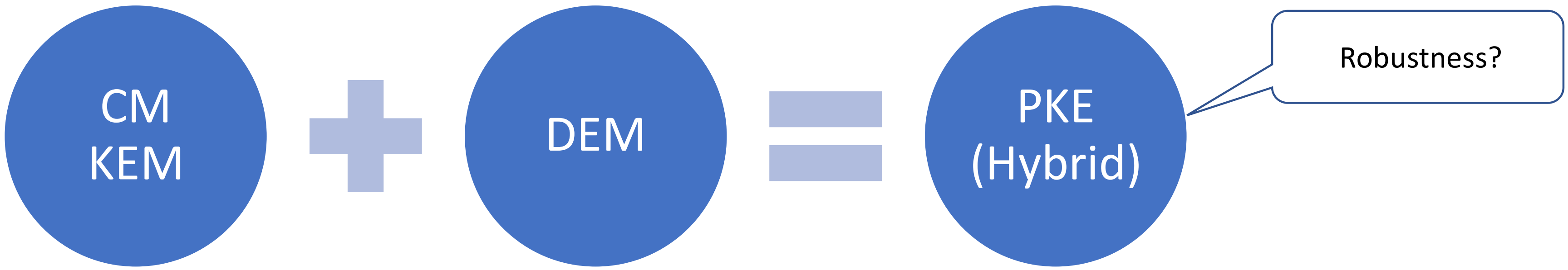
The following randomized algorithm ENCAP takes as input a public key T. It outputs a ciphertext C and a session key K. Here is the algorithm:

1. Use FIXEDWEIGHT to generate a vector $e \in \mathbb{F}_2^n$ of weight t.
2. Compute $C_0 = \text{ENCODE}(e, T)$.
3. Compute $C_1 = \mathsf{H}(2, e)$; see Section 2.5.2 for H input encodings. Put $C = (C_0, C_1)$.
4. Compute $K = \mathsf{H}(1, e, C)$; see Section 2.5.2 for H input encodings.
5. Output ciphertext C and session key K.

For *any* message m:

Classic McEliece (CM)

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$



$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$ $c_{DEM} \leftarrow Enc^{sym}(k, m)$ $(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

2.4.5 Encapsulation

The following randomized algorithm ENCAP takes as input a public key T. It outputs a ciphertext C and a session key K. Here is the algorithm:

1. Use FIXEDWEIGHT to generate a vector $e \in \mathbb{F}_2^n$ of weight t.
2. Compute $C_0 = \text{ENCODE}(e, T)$.
3. Compute $C_1 = \mathsf{H}(2, e)$; see Section 2.5.2 for H input encodings. Put $C = (C_0, C_1)$.
4. Compute $K = \mathsf{H}(1, e, C)$; see Section 2.5.2 for H input encodings.
5. Output ciphertext C and session key K.

For *any* message m:

- Fix vector $e = \binom{e_{n-k}}{0^k}$.

Classic McEliece (CM)

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

CM KEM + DEM = PKE (Hybrid)

Robustness?

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$ $c_{DEM} \leftarrow Enc^{sym}(k, m)$ $(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

2.4.5 Encapsulation

The following randomized algorithm ENCAP takes as input a public key T. It outputs a ciphertext C and a session key K. Here is the algorithm:

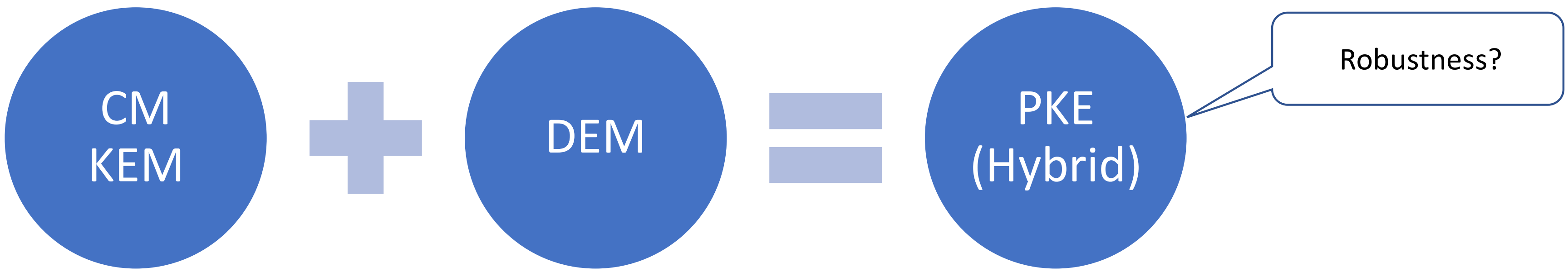
1. Use FIXEDWEIGHT to generate a vector $e \in \mathbb{F}_2^n$ of weight t.
2. Compute $C_0 = \text{ENCODE}(e, T)$.
3. Compute $C_1 = \mathsf{H}(2, e)$; see Section 2.5.2 for H input encodings. Put $C = (C_0, C_1)$.
4. Compute $K = \mathsf{H}(1, e, C)$; see Section 2.5.2 for H input encodings.
5. Output ciphertext C and session key K.

For *any* message m:

- Fix vector $e = \binom{e_{n-k}}{0^k}$.
- Set $C_0 = e_{n-k}, C_1 = \mathsf{H}(2, e)$ and $c_{KEM} \leftarrow (C_0, C_1)$.

Classic McEliece (CM)

$KEM = (KGen, Encap, Decap)$ $\quad DEM = (Enc^{sym}, Dec^{sym})$ $\quad PKE = (KGen, Enc, Dec)$



$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$ $\quad c_{DEM} \leftarrow Enc^{sym}(k, m)$ $\quad (c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

2.4.5 Encapsulation

The following randomized algorithm ENCAP takes as input a public key T. It outputs a ciphertext C and a session key K. Here is the algorithm:

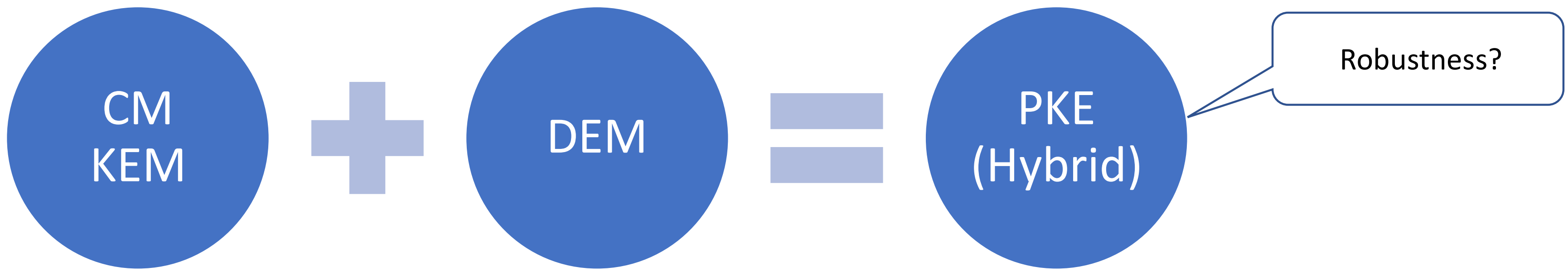
1. Use FIXEDWEIGHT to generate a vector $e \in \mathbb{F}_2^n$ of weight t.
2. Compute $C_0 = \text{ENCODE}(e, T)$.
3. Compute $C_1 = \mathsf{H}(2, e)$; see Section 2.5.2 for H input encodings. Put $C = (C_0, C_1)$.
4. Compute $K = \mathsf{H}(1, e, C)$; see Section 2.5.2 for H input encodings.
5. Output ciphertext C and session key K.

For *any* message m:

- Fix vector $e = \binom{e_{n-k}}{0^k}$.
- Set $C_0 = e_{n-k}, C_1 = \mathrm{H}(2, e)$ and $c_{KEM} \leftarrow (C_0, C_1)$.
- Compute $k = \mathrm{H}(1, e, c_{KEM})$ and $c_{DEM} \leftarrow Enc^{sym}(k, m)$.

Classic McEliece (CM)

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$



$(c_{KEM}, k) \leftarrow \boxed{Encap(pk_{Bob})}$ $c_{DEM} \leftarrow Enc^{sym}(k, m)$ $\boxed{(c_{KEM}, c_{DEM})} \leftarrow Enc(pk_{Bob}, m)$

2.4.5 Encapsulation

The following randomized algorithm ENCAP takes as input a public key T. It outputs a ciphertext C and a session key K. Here is the algorithm:

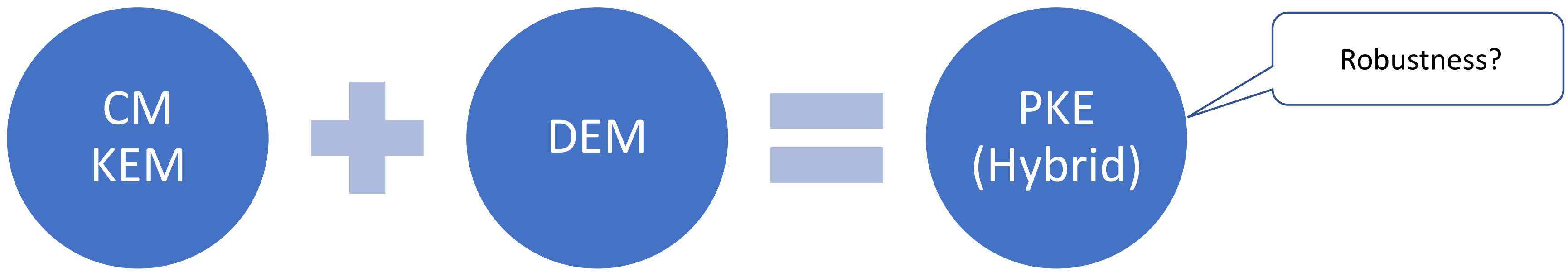
1. Use FIXEDWEIGHT to generate a vector $e \in \mathbb{F}_2^n$ of weight t.
2. Compute $C_0 = \text{ENCODE}(e, T)$.
3. Compute $C_1 = \mathsf{H}(2, e)$; see Section 2.5.2 for H input encodings. Put $C = (C_0, C_1)$.
4. Compute $K = \mathsf{H}(1, e, C)$; see Section 2.5.2 for H input encodings.
5. Output ciphertext C and session key K.

For *any* message m:

- Fix vector $e = \binom{e_{n-k}}{0^k}$.
- Set $C_0 = e_{n-k}, C_1 = \mathsf{H}(2, e)$ and $c_{KEM} \leftarrow (C_0, C_1)$.
- Compute $k = \mathsf{H}(1, e, c_{KEM})$ and $c_{DEM} \leftarrow Enc^{sym}(k, m)$.
- Return $\boxed{c \leftarrow (c_{KEM}, c_{DEM})}$.

Classic McEliece (CM)

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$



$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$ $c_{DEM} \leftarrow Enc^{sym}(k, m)$ $(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

2.4.5 Encapsulation

The following randomized algorithm ENCAP takes as input a public key T. It outputs a ciphertext C and a session key K. Here is the algorithm:

1. Use FIXEDWEIGHT to generate a vector $e \in \mathbb{F}_2^n$ of weight t.
2. Compute $C_0 = \text{ENCODE}(e, T)$.
3. Compute $C_1 = \mathsf{H}(2, e)$; see Section 2.5.2 for H input encodings. Put $C = (C_0, C_1)$.
4. Compute $K = \mathsf{H}(1, e, C)$; see Section 2.5.2 for H input encodings.
5. Output ciphertext C and session key K.

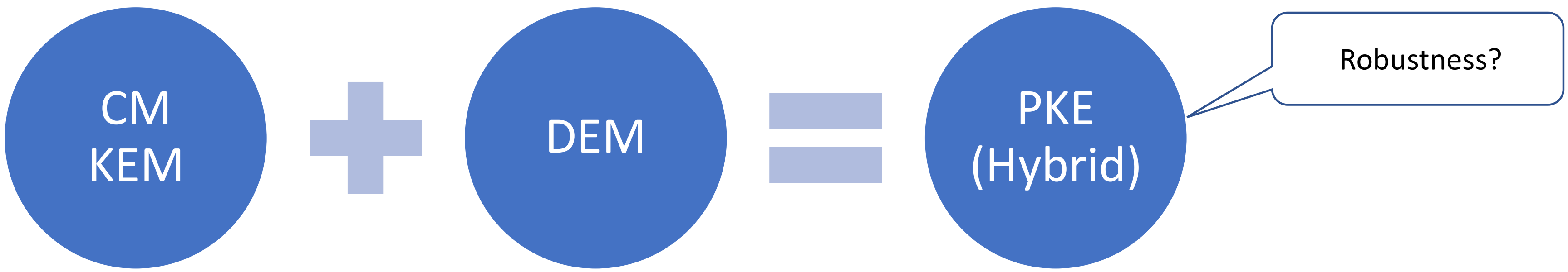
For *any* message m:

- Fix vector $e = \binom{e_{n-k}}{0^k}$.
- Set $C_0 = e_{n-k}, C_1 = \mathsf{H}(2, e)$ and $c_{KEM} \leftarrow (C_0, C_1)$.
- Compute $k = \mathsf{H}(1, e, c_{KEM})$ and $c_{DEM} \leftarrow Enc^{sym}(k, m)$.
- Return $c \leftarrow (c_{KEM}, c_{DEM})$.

For *any* CM private key sk_* ,

Classic McEliece (CM)

$KEM = (KGen, Encap, Decap)$ $\quad DEM = (Enc^{sym}, Dec^{sym})$ $\quad PKE = (KGen, Enc, Dec)$



$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$ $\quad c_{DEM} \leftarrow Enc^{sym}(k, m)$ $\quad (c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

2.4.5 Encapsulation

The following randomized algorithm ENCAP takes as input a public key T. It outputs a ciphertext C and a session key K. Here is the algorithm:

1. Use FIXEDWEIGHT to generate a vector $e \in \mathbb{F}_2^n$ of weight t.
2. Compute $C_0 = \text{ENCODE}(e, T)$.
3. Compute $C_1 = \mathsf{H}(2, e)$; see Section 2.5.2 for H input encodings. Put $C = (C_0, C_1)$.
4. Compute $K = \mathsf{H}(1, e, C)$; see Section 2.5.2 for H input encodings.
5. Output ciphertext C and session key K.

For *any* message m:

- Fix vector $e = \binom{e_{n-k}}{0^k}$.
- Set $C_0 = e_{n-k}, C_1 = \mathsf{H}(2, e)$ and $c_{KEM} \leftarrow (C_0, C_1)$.
- Compute $k = \mathsf{H}(1, e, c_{KEM})$ and $c_{DE} \leftarrow Enc^{sym}(k, m)$.
- Return $c \leftarrow (c_{KEM}, c_{DEM})$.

For *any* CM private key sk_*,

$$Dec(sk_*, c) = m \ (\neq \perp).$$

Classic McEliece (CM)

$KEM = (KGen, Encap, Decap)$ $\quad DEM = (Enc^{sym}, Dec^{sym})$ $\quad PKE = (KGen, Enc, Dec)$

CM KEM + DEM = PKE (Hybrid)

Cannot be (strongly) robust, i.e., SROB-insecure!

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$ $\quad c_{DEM} \leftarrow Enc^{sym}(k, m)$ $\quad (c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

2.4.5 Encapsulation

The following randomized algorithm ENCAP takes as input a public key T. It outputs a ciphertext C and a session key K. Here is the algorithm:

1. Use FIXEDWEIGHT to generate a vector $e \in \mathbb{F}_2^n$ of weight t.
2. Compute $C_0 = \text{ENCODE}(e, T)$.
3. Compute $C_1 = \mathsf{H}(2, e)$; see Section 2.5.2 for H input encodings. Put $C = (C_0, C_1)$.
4. Compute $K = \mathsf{H}(1, e, C)$; see Section 2.5.2 for H input encodings.
5. Output ciphertext C and session key K.

For *any* message m:

- Fix vector $e = \binom{e_{n-k}}{0^k}$.
- Set $C_0 = e_{n-k}, C_1 = \mathsf{H}(2, e)$ and $c_{KEM} \leftarrow (C_0, C_1)$.
- Compute $k = \mathsf{H}(1, e, c_{KEM})$ and $c_{DEM} \leftarrow Enc^{sym}(k, m)$.
- Return $c \leftarrow (c_{KEM}, c_{DEM})$.

For *any* CM private key sk_*,

$$Dec(sk_*, c) = m \ (\neq \perp).$$

Classic McEliece (CM)

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

CM KEM + DEM = PKE (Hybrid)

Cannot be (strongly) robust, i.e., SROB-insecure!

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$ $c_{DEM} \leftarrow Enc^{sym}(k, m)$ $(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

But can be ANO-CCA secure. [Xagawa'22]

2.4.5 Encapsulation

The following randomized algorithm ENCAP takes as input a public key T. It outputs a ciphertext C and a session key K. Here is the algorithm:

1. Use FIXEDWEIGHT to generate a vector $e \in \mathbb{F}_2^n$ of weight t.
2. Compute $C_0 = \text{ENCODE}(e, T)$.
3. Compute $C_1 = \mathsf{H}(2, e)$; see Section 2.5.2 for H input encodings. Put $C = (C_0, C_1)$.
4. Compute $K = \mathsf{H}(1, e, C)$; see Section 2.5.2 for H input encodings.
5. Output ciphertext C and session key K.

For *any* message m:

- Fix vector $e = \begin{pmatrix} e_{n-k} \\ 0^k \end{pmatrix}$.
- Set $C_0 = e_{n-k}, C_1 = \mathsf{H}(2, e)$ and $c_{KEM} \leftarrow (C_0, C_1)$.
- Compute $k = \mathsf{H}(1, e, c_{KEM})$ and $c_{DEM} \leftarrow Enc^{sym}(k, m)$.
- Return $c \leftarrow (c_{KEM}, c_{DEM})$.

Relied on a stronger *single-key* notion, i.e., strong pseudo-randomness.

For *any* CM private key sk_*,

$Dec(sk_*, c) = m \ (\neq \perp)$.

CRYSTALS-KYBER and SABER

<u>Public-Key Encryption/KEMs</u>

Classic McEliece
CRYSTALS-KYBER
NTRU
SABER

<u>Public-Key Encryption/KEMs</u>

BIKE
FrodoKEM
HQC
NTRU Prime
SIKE

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

$FO^{\pm}$-based KEM + DEM = PKE (Hybrid)

$c \leftarrow Enc^{base}(pk_{Bob}, m)$ should have large enough entropy.

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure

CRYSTALS-KYBER and SABER

<u>Public-Key Encryption/KEMs</u>	<u>Public-Key Encryption/KEMs</u>
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

$KEM = (KGen, Encap, Decap)$ $\quad DEM = (Enc^{sym}, Dec^{sym})$ $\quad PKE = (KGen, Enc, Dec)$

KYBER/ SABER KEM + DEM = PKE (Hybrid)

$c \leftarrow Enc^{base}(pk_{Bob}, m)$ should have large enough entropy.

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure

CRYSTALS-KYBER and SABER

Public-Key Encryption/KEMs
- Classic McEliece
- CRYSTALS-KYBER
- NTRU
- SABER

Public-Key Encryption/KEMs
- BIKE
- FrodoKEM
- HQC
- NTRU Prime
- SIKE

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

KYBER/ SABER KEM + DEM = PKE (Hybrid)

?

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure

CRYSTALS-KYBER and SABER

<u>Public-Key Encryption/KEMs</u>

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

<u>Public-Key Encryption/KEMs</u>

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_\$ \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_\$ \mathcal{M}$	$r \leftarrow G(m)$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$	$r' \leftarrow G(m')$
return $(\mathsf{pk}, \mathsf{sk}')$	$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; r')$
	return (c, k)	**if** $c' = c$ **then**
		return $H(m', c)$
		else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

CRYSTALS-KYBER and SABER

<u>Public-Key Encryption/KEMs</u>

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

<u>Public-Key Encryption/KEMs</u>

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_\$ \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_\$ \mathcal{M}$	$r \leftarrow G(m)$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$	$r' \leftarrow G(m')$
return $(\mathsf{pk}, \mathsf{sk}')$	$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; r')$
	return (c, k)	**if** $c' = c$ **then**
		return $H(m', c)$
		else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_\$ \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, \mathsf{pk}, F(\mathsf{pk}), s)$
$s \leftarrow_\$ \mathcal{M}$	$m \leftarrow F(m)$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' \leftarrow (\mathsf{sk}, \mathsf{pk}, F(\mathsf{pk}), s)$	$(\hat{k}, r) \leftarrow G(F(pk), m)$	$(\hat{k}', r') \leftarrow G(F(\mathsf{pk}), m')$
return $(\mathsf{pk}, \mathsf{sk}')$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; r')$
	$k \leftarrow \mathsf{KDF}(\hat{k}, F(c))$	**if** $c' = c$ **then**
	return (c, k)	**return** $\mathsf{KDF}(\hat{k}', F(c))$
		else return $\mathsf{KDF}(s, F(c))$

CRYSTALS-KYBER, Saber

CRYSTALS-KYBER and SABER

<u>Public-Key Encryption/KEMs</u>

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

<u>Public-Key Encryption/KEMs</u>

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_\$ \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_\$ \mathcal{M}$	$r \leftarrow G(m)$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$	$r' \leftarrow G(m')$
return $(\mathsf{pk}, \mathsf{sk}')$	$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; r')$
	return (c, k)	**if** $c' = c$ **then**
		return $H(m', c)$
		else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_\$ \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, \mathsf{pk}, F(\mathsf{pk}), s)$
$s \leftarrow_\$ \mathcal{M}$	$m \leftarrow F(m)$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' \leftarrow (\mathsf{sk}, \mathsf{pk}, F(\mathsf{pk}), s)$	$(\hat{k}, r) \leftarrow G(F(pk), m)$	$(\hat{k}', r') \leftarrow G(F(\mathsf{pk}), m')$
return $(\mathsf{pk}, \mathsf{sk}')$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; r')$
	$k \leftarrow \mathsf{KDF}(\hat{k}, F(c))$	**if** $c' = c$ **then**
	return (c, k)	**return** $\mathsf{KDF}(\hat{k}', F(c))$
		else return $\mathsf{KDF}(s, F(c))$

CRYSTALS-KYBER, Saber

CRYSTALS-KYBER and SABER

<u>Public-Key Encryption/KEMs</u>

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

<u>Public-Key Encryption/KEMs</u>

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

"Nested" hashing of both m and c.

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_{\$} \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_{\$} \mathcal{M}$	$r \leftarrow G(m)$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$	$r' \leftarrow G(m')$
return $(\mathsf{pk}, \mathsf{sk}')$	$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; r')$
	return (c, k)	**if** $c' = c$ **then**
		return $H(m', c)$
		else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_{\$} \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, \mathsf{pk}, F(\mathsf{pk}), s)$
$s \leftarrow_{\$} \mathcal{M}$	$m \leftarrow F(m)$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' \leftarrow (\mathsf{sk}, \mathsf{pk}, F(\mathsf{pk}), s)$	$(\hat{k}, r) \leftarrow G(F(pk), m)$	$(\hat{k}', r') \leftarrow G(F(\mathsf{pk}), m')$
return $(\mathsf{pk}, \mathsf{sk}')$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; r')$
	$k \leftarrow \mathsf{KDF}(\hat{k}, F(c))$	**if** $c' = c$ **then**
	return (c, k)	**return** $\mathsf{KDF}(\hat{k}', F(c))$
		else return $\mathsf{KDF}(s, F(c))$

CRYSTALS-KYBER, Saber

CRYSTALS-KYBER and SABER

<u>Public-Key Encryption/KEMs</u>

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

<u>Public-Key Encryption/KEMs</u>

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

KYBER/ SABER KEM + DEM = PKE (Hybrid)

Faced barriers towards proving anonymity.

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure

CRYSTALS-KYBER and SABER

<u>Public-Key Encryption/KEMs</u>

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

<u>Public-Key Encryption/KEMs</u>

BIKE

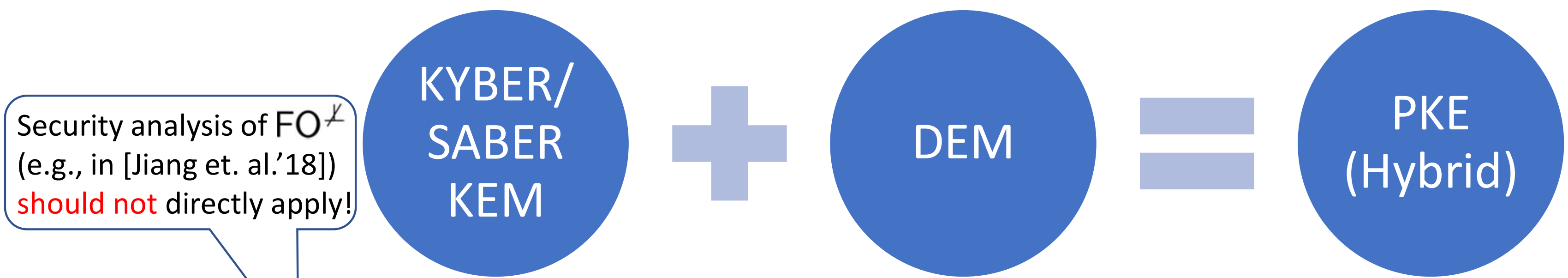
FrodoKEM

HQC

NTRU Prime

SIKE

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$



$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure
+ γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure +
ANO-CCA secure

CRYSTALS-KYBER and SABER

<u>Public-Key Encryption/KEMs</u>

Classic McEliece
CRYSTALS-KYBER
NTRU
SABER

<u>Public-Key Encryption/KEMs</u>

BIKE
FrodoKEM
HQC
NTRU Prime
SIKE

Is strongly "robust", i.e., SCFR-secure. [Grubbs-Maram-Paterson'22]

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

KYBER/ SABER KEM + DEM = PKE (Hybrid)

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure

CRYSTALS-KYBER and SABER

<u>Public-Key Encryption/KEMs</u>

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

<u>Public-Key Encryption/KEMs</u>

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

Is strongly "robust", i.e., SCFR-secure. [Grubbs-Maram-Paterson'22]

By having a "fully" robust DEM, i.e., FROB-secure.

$KEM = (KGen, Encap, Decap)$ $\quad DEM = (Enc^{sym}, Dec^{sym})$ $\quad PKE = (KGen, Enc, Dec)$

KYBER/ SABER KEM + DEM = PKE (Hybrid)

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure

CRYSTALS-KYBER and SABER

Public-Key Encryption/KEMs

- Classic McEliece
- CRYSTALS-KYBER
- NTRU
- SABER

Public-Key Encryption/KEMs

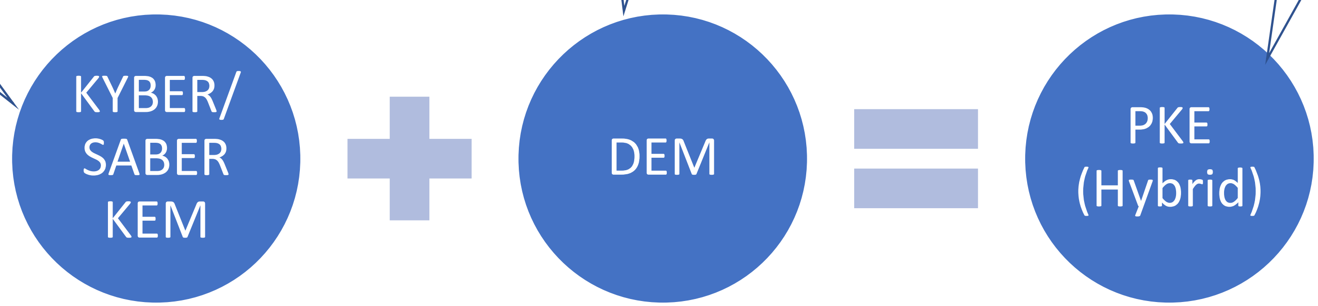
- BIKE
- FrodoKEM
- HQC
- NTRU Prime
- SIKE

Is strongly "robust", i.e., SCFR-secure. [Grubbs-Maram-Paterson'22]

By having a "fully" robust DEM, i.e., FROB-secure.

Can be made strongly robust, i.e., SROB-secure.

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$



$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure

FrodoKEM

Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

$FO^{\pm}$-based KEM + DEM = PKE (Hybrid)

$c \leftarrow Enc^{base}(pk_{Bob}, m)$ should have large enough entropy.

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure

FrodoKEM

Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

Frodo KEM + DEM = PKE (Hybrid)

$c \leftarrow Enc^{base}(pk_{Bob}, m)$ should have large enough entropy.

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure

FrodoKEM

<u>Public-Key Encryption/KEMs</u>

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

<u>Public-Key Encryption/KEMs</u>

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

Frodo KEM + DEM = PKE (Hybrid)

?

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure
+ γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure +
ANO-CCA secure

FrodoKEM

<u>Public-Key Encryption/KEMs</u>

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

<u>Public-Key Encryption/KEMs</u>

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_{\$} \mathcal{M}$	$\text{Parse } \mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_{\$} \mathcal{M}$	$r \leftarrow G(m)$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$	$r' \leftarrow G(m')$
$\textbf{return } (\mathsf{pk}, \mathsf{sk}')$	$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; r')$
	$\textbf{return } (c, k)$	$\textbf{if } c' = c \textbf{ then}$
		$\quad \textbf{return } H(m', c)$
		$\textbf{else return } H(s, c)$

$\mathsf{FO}^{\not\perp}$

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_{\$} \mathcal{M}$	$\text{Parse } \mathsf{sk}' = (\mathsf{sk}, \mathsf{pk}, F(\mathsf{pk}), s)$
$s \leftarrow_{\$} \mathcal{M}$	$(\hat{k}, r) \leftarrow G(F(pk), m)$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' \leftarrow (\mathsf{sk}, \mathsf{pk}, F(\mathsf{pk}), s)$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$	$(\hat{k}', r') \leftarrow G(F(\mathsf{pk}), m')$
$\textbf{return } (\mathsf{pk}, \mathsf{sk}')$	$k \leftarrow H(\hat{k}, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; r')$
	$\textbf{return } (c, k)$	$\textbf{if } c' = c \textbf{ then}$
		$\quad \textbf{return } H(\hat{k}', c)$
		$\textbf{else return } H(s, c)$

FrodoKEM

FrodoKEM

<u>Public-Key Encryption/KEMs</u>	<u>Public-Key Encryption/KEMs</u>
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_{\$} \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_{\$} \mathcal{M}$	$r \leftarrow G(m)$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$	$r' \leftarrow G(m')$
return $(\mathsf{pk}, \mathsf{sk}')$	$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; r')$
	return (c, k)	**if** $c' = c$ **then**
		return $H(m', c)$
		else return $H(s, c)$

FO$^{\not\perp}$

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_{\$} \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, \mathsf{pk}, F(\mathsf{pk}), s)$
$s \leftarrow_{\$} \mathcal{M}$	$(\hat{k}, r) \leftarrow G(F(pk), m)$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' \leftarrow (\mathsf{sk}, \mathsf{pk}, F(\mathsf{pk}), s)$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$	$(\hat{k}', r') \leftarrow G(F(\mathsf{pk}), m')$
return $(\mathsf{pk}, \mathsf{sk}')$	$k \leftarrow H(\hat{k}, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; r')$
	return (c, k)	**if** $c' = c$ **then**
		return $H(\hat{k}', c)$
		else return $H(s, c)$

FrodoKEM

FrodoKEM

<u>Public-Key Encryption/KEMs</u>

Classic McEliece
CRYSTALS-KYBER
NTRU
SABER

<u>Public-Key Encryption/KEMs</u>

BIKE
FrodoKEM
HQC
NTRU Prime
SIKE

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

Frodo KEM + DEM = PKE (Hybrid)

Security analysis of $\mathrm{FO}^{\not\perp}$ should not directly apply.

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure

FrodoKEM

<u>Public-Key Encryption/KEMs</u>	<u>Public-Key Encryption/KEMs</u>
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

Frodo KEM + DEM = PKE (Hybrid)

But (provable) IND-CCA security can be "recovered". [Grubbs-Maram -Paterson'22]

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure

FrodoKEM

<u>Public-Key Encryption/KEMs</u>

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

<u>Public-Key Encryption/KEMs</u>

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

Only nested hashing of m and <u>not</u> c.

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_{\$} \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_{\$} \mathcal{M}$	$r \leftarrow G(m)$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$	$r' \leftarrow G(m')$
return $(\mathsf{pk}, \mathsf{sk}')$	$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; r')$
	return (c, k)	**if** $c' = c$ **then**
		return $H(m', c)$
		else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_{\$} \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, \mathsf{pk}, F(\mathsf{pk}), s)$
$s \leftarrow_{\$} \mathcal{M}$	$(\hat{k}, r) \leftarrow G(F(pk), m)$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' \leftarrow (\mathsf{sk}, \mathsf{pk}, F(\mathsf{pk}), s)$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$	$(\hat{k}', r') \leftarrow G(F(\mathsf{pk}), m')$
return $(\mathsf{pk}, \mathsf{sk}')$	$k \leftarrow H(\hat{k}, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; r')$
	return (c, k)	**if** $c' = c$ **then**
		return $H(\hat{k}', c)$
		else return $H(s, c)$

FrodoKEM

FrodoKEM

<u>Public-Key Encryption/KEMs</u>

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

<u>Public-Key Encryption/KEMs</u>

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

Only nested hashing of m and <u>not</u> c.

Length-preserving hash, i.e., $|m| = |\hat{k}|$ ...

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_{\$} \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_{\$} \mathcal{M}$	$r \leftarrow G(m)$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$	$r' \leftarrow G(m')$
return $(\mathsf{pk}, \mathsf{sk}')$	$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; r')$
	return (c, k)	**if** $c' = c$ **then**
		return $H(m', c)$
		else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_{\$} \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, \mathsf{pk}, F(\mathsf{pk}), s)$
$s \leftarrow_{\$} \mathcal{M}$	$(\hat{k}, r) \leftarrow G(F(pk), m)$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' \leftarrow (\mathsf{sk}, \mathsf{pk}, F(\mathsf{pk}), s)$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$	$(\hat{k}', r') \leftarrow G(F(\mathsf{pk}), m')$
return $(\mathsf{pk}, \mathsf{sk}')$	$k \leftarrow H(\hat{k}, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; r')$
	return (c, k)	**if** $c' = c$ **then**
		return $H(\hat{k}', c)$
		else return $H(s, c)$

FrodoKEM

FrodoKEM

Public-Key Encryption/KEMs

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

Public-Key Encryption/KEMs

BIKE

FrodoKEM

HQC

NTRU Prime

SIKE

Only nested hashing of m and not c.

Length-preserving hash, i.e., $|m| = |\hat{k}|$ …

… which allows to "extract" m given $\hat{k}$ [Targhi-Unruh'16].

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_\$ \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_\$ \mathcal{M}$	$r \leftarrow G(m)$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$	$r' \leftarrow G(m')$
return $(\mathsf{pk}, \mathsf{sk}')$	$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; r')$
	return (c, k)	**if** $c' = c$ **then**
		return $H(m', c)$
		else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_\$ \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, \mathsf{pk}, F(\mathsf{pk}), s)$
$s \leftarrow_\$ \mathcal{M}$	$(\hat{k}, r) \leftarrow G(F(pk), m)$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' \leftarrow (\mathsf{sk}, \mathsf{pk}, F(\mathsf{pk}), s)$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$	$(\hat{k}', r') \leftarrow G(F(\mathsf{pk}), m')$
return $(\mathsf{pk}, \mathsf{sk}')$	$k \leftarrow H(\hat{k}, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; r')$
	return (c, k)	**if** $c' = c$ **then**
		return $H(\hat{k}', c)$
		else return $H(s, c)$

FrodoKEM

FrodoKEM

<u>Public-Key Encryption/KEMs</u>	<u>Public-Key Encryption/KEMs</u>
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

Only nested hashing of m and <u>not</u> c.

Length-preserving hash, i.e., $|m| = |\hat{k}|$ …

… which allows to "extract" m given $\hat{k}$ [Targhi-Unruh'16].

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_\$ \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, s)$
$s \leftarrow_\$ \mathcal{M}$	$r \leftarrow G(m)$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' = (\mathsf{sk}, s)$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$	$r' \leftarrow G(m')$
return $(\mathsf{pk}, \mathsf{sk}')$	$k \leftarrow H(m, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; r')$
	return (c, k)	**if** $c' = c$ **then**
		return $H(m', c)$
		else return $H(s, c)$

$\mathsf{FO}^{\not\perp}$

KGen'	$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}', c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$	$m \leftarrow_\$ \mathcal{M}$	Parse $\mathsf{sk}' = (\mathsf{sk}, \mathsf{pk}, F(\mathsf{pk}), s)$
$s \leftarrow_\$ \mathcal{M}$	$(\hat{k}, r) \leftarrow G(F(pk), m)$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$
$\mathsf{sk}' \leftarrow (\mathsf{sk}, \mathsf{pk}, F(\mathsf{pk}), s)$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$	$(\hat{k}', r') \leftarrow G(F(\mathsf{pk}), m')$
return $(\mathsf{pk}, \mathsf{sk}')$	$k \leftarrow H(\hat{k}, c)$	$c' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; r')$
	return (c, k)	**if** $c' = c$ **then**
		return $H(\hat{k}', c)$
		else return $H(s, c)$

$(\hat{k}, c)$ can be "reduced" to (m, c).

FrodoKEM

FrodoKEM

Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$

Frodo KEM + DEM = PKE (Hybrid)

FrodoKEM is ANO-CCA and SCFR-secure in the QROM. [Grubbs-Maram -Paterson'22]

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure

FrodoKEM

<u>Public-Key Encryption/KEMs</u>

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

<u>Public-Key Encryption/KEMs</u>

BIKE

FrodoKEM

HQC

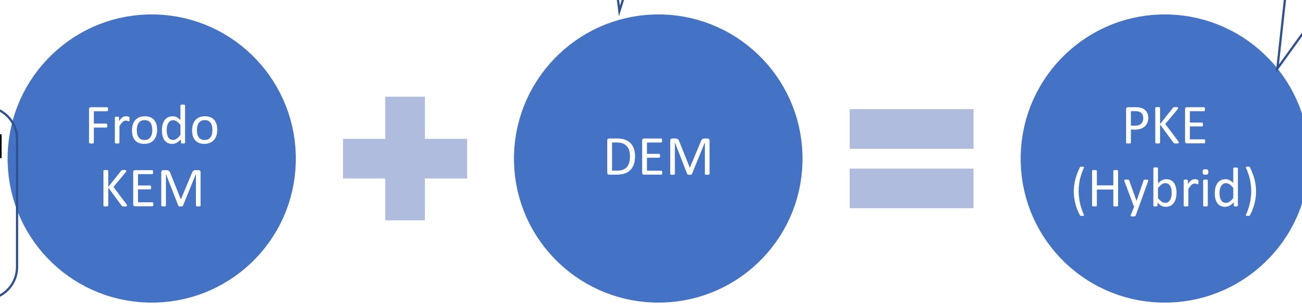
NTRU Prime

SIKE

By having a "fully" robust DEM, i.e., FROB-secure.

FrodoKEM does result in anonymous and robust PKE in a PQ setting.

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$



FrodoKEM is ANO-CCA and SCFR-secure in the QROM. [Grubbs-Maram -Paterson'22]

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA + ANO-CCA secure + γ-spread base PKE

$c_{DEM} \leftarrow Enc^{sym}(k, m)$

AE-secure

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure + ANO-CCA secure

Other Contributions

Other Contributions

$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}, c)$
$m \leftarrow_{\$} \mathcal{M}$	Parse $c = (c_1, c_2)$
$c_1 \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c_1)$
$c_2 \leftarrow H'(m)$	$c_1' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
	if $c_1' = c_1 \wedge H'(m') = c_2$ **then**
$c \leftarrow (c_1, c_2)$	
$k = H(m, c)$	**return** $H(m', c)$
return (c, k)	**else return** $\perp$

$\mathsf{HFO}^{\perp}$

Other Contributions

$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}, c)$
$m \leftarrow_{\$} \mathcal{M}$	Parse $c = (c_1, c_2)$
$c_1 \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c_1)$
$c_2 \leftarrow H'(m)$	$c_1' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
	if $c_1' = c_1 \wedge H'(m') = c_2$ **then**
$c \leftarrow (c_1, c_2)$	
$k = H(m, c)$	**return** $H(m', c)$
return (c, k)	**else return** $\perp$

$\mathsf{HFO}^{\perp}$

Results in IND-CCA secure KEMs in the QROM. [Jiang-Zhang-Ma'19]

Other Contributions

$\mathsf{Encap}(\mathsf{pk})$		$\mathsf{Decap}(\mathsf{sk}, c)$	
1 :	$m \leftarrow_\$ \mathcal{M}$	1 :	Parse $c = (c_1, c_2)$
2 :	$c_1 \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	2 :	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c_1)$
3 :	$c_2 \leftarrow H'(m)$	3 :	$c_1' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
4 :	$\boxed{c_2 \leftarrow H'(m, c_1)}$	4 :	**if** $c_1' = c_1 \wedge H'(m') = c_2$ **then**
5 :	$c \leftarrow (c_1, c_2)$	5 :	$\boxed{\textbf{if } c_1' = c_1 \wedge H'(m', c_1) = c_2 \textbf{ then}}$
6 :	$k = H(m, c)$	6 :	**return** $H(m', c)$
7 :	**return** (c, k)	7 :	**else return** $\perp$

$\mathsf{HFO}^{\perp}$ $\boxed{\mathsf{HFO}^{\perp'}}$

Results in IND-CCA secure KEMs in the QROM. [Jiang-Zhang-Ma'19]

Other Contributions

$\mathsf{Encap}(\mathsf{pk})$	$\mathsf{Decap}(\mathsf{sk}, c)$
$m \leftarrow_{\$} \mathcal{M}$	Parse $c = (c_1, c_2)$
$c_1 \leftarrow \mathsf{Enc}(\mathsf{pk}, m; G(m))$	$m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c_1)$
$c_2 \leftarrow H'(m)$	$c_1' \leftarrow \mathsf{Enc}(\mathsf{pk}, m'; G(m'))$
$\boxed{c_2 \leftarrow H'(m, c_1)}$	**if** $c_1' = c_1 \wedge H'(m') = c_2$ **then**
$c \leftarrow (c_1, c_2)$	$\boxed{\textbf{if } c_1' = c_1 \wedge H'(m', c_1) = c_2 \textbf{ then}}$
$k = H(m, c)$	**return** $H(m', c)$
return (c, k)	**else return** $\perp$

$\mathsf{HFO}^{\perp}$ $\boxed{\mathsf{HFO}^{\perp'}}$

Results in IND-CCA secure KEMs in the QROM. [Jiang-Zhang-Ma'19]

Results in IND-CCA, ANO-CCA and SROB secure KEMs in the QROM. [Grubbs-Maram-Paterson'22]

Conclusions

Conclusions

- We provide insights into obtaining anonymous and robust hybrid PKE schemes – via the KEM-DEM composition – when the KEM is <u>implicitly rejecting</u> (i.e., non-robust).

Conclusions

- We provide insights into obtaining anonymous and robust hybrid PKE schemes – via the KEM-DEM composition – when the KEM is <u>implicitly rejecting</u> (i.e., non-robust).
- We showed that the $\mathsf{FO}^{\not\perp}$ transform does result in ANO-CCA secure and "robust" KEMs in a <u>post-quantum setting</u> (i.e., the QROM).

Conclusions

- We provide insights into obtaining anonymous and robust hybrid PKE schemes – via the KEM-DEM composition – when the KEM is <u>implicitly rejecting</u> (i.e., non-robust).
- We showed that the $\mathsf{FO}^{\not\perp}$ transform does result in ANO-CCA secure and "robust" KEMs in a <u>post-quantum setting</u> (i.e., the QROM).
- Hybrid PKE schemes derived from <u>Classic McEliece</u> cannot be (strongly) robust.

Conclusions

- We provide insights into obtaining anonymous and robust hybrid PKE schemes – via the KEM-DEM composition – when the KEM is implicitly rejecting (i.e., non-robust).
- We showed that the $\mathsf{FO}^{\not\perp}$ transform does result in ANO-CCA secure and "robust" KEMs in a post-quantum setting (i.e., the QROM).
- Hybrid PKE schemes derived from Classic McEliece cannot be (strongly) robust.
  - Though they can be made ANO-CCA secure as shown in [Xagawa'21].

Conclusions

- We provide insights into obtaining anonymous and robust hybrid PKE schemes – via the KEM-DEM composition – when the KEM is implicitly rejecting (i.e., non-robust).
- We showed that the $\mathsf{FO}^{\not\perp}$ transform does result in ANO-CCA secure and "robust" KEMs in a post-quantum setting (i.e., the QROM).
- Hybrid PKE schemes derived from Classic McEliece cannot be (strongly) robust.
  - Though they can be made ANO-CCA secure as shown in [Xagawa'21].
- We identified barriers towards proving IND-CCA and ANO-CCA security of CRYSTALS-KYBER and SABER in the QROM.

Conclusions

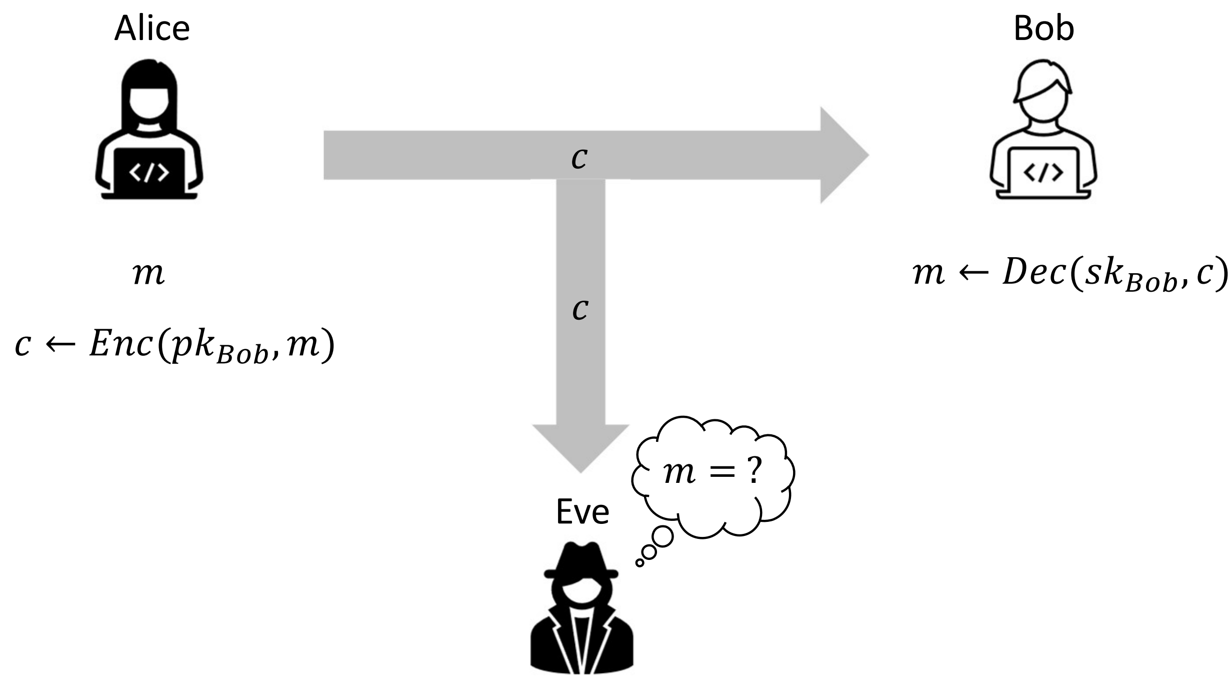
- We provide insights into obtaining anonymous and robust hybrid PKE schemes – via the KEM-DEM composition – when the KEM is implicitly rejecting (i.e., non-robust).
- We showed that the $\mathsf{FO}^{\not\perp}$ transform does result in ANO-CCA secure and "robust" KEMs in a post-quantum setting (i.e., the QROM).
- Hybrid PKE schemes derived from Classic McEliece cannot be (strongly) robust.
  - Though they can be made ANO-CCA secure as shown in [Xagawa'21].
- We identified barriers towards proving IND-CCA and ANO-CCA security of CRYSTALS-KYBER and SABER in the QROM.
  - At the same time, we showed they do result in strongly robust hybrid PKE schemes.

Conclusions

- We provide insights into obtaining anonymous and robust hybrid PKE schemes – via the KEM-DEM composition – when the KEM is implicitly rejecting (i.e., non-robust).
- We showed that the $\mathsf{FO}^{\not\perp}$ transform does result in ANO-CCA secure and "robust" KEMs in a post-quantum setting (i.e., the QROM).
- Hybrid PKE schemes derived from Classic McEliece cannot be (strongly) robust.
  - Though they can be made ANO-CCA secure as shown in [Xagawa'21].
- We identified barriers towards proving IND-CCA and ANO-CCA security of CRYSTALS-KYBER and SABER in the QROM.
  - At the same time, we showed they do result in strongly robust hybrid PKE schemes.
- Finally, we showed that FrodoKEM does result in ANO-CCA secure and strongly robust hybrid PKE schemes in the QROM.

IND-CCA Security

$PKE = (KGen, Enc, Dec)$



KEM-DEM Paradigm

Public-Key Encryption/KEMs

Classic McEliece

CRYSTALS-KYBER

NTRU

SABER

Public-Key Encryption/KEMs

BIKE

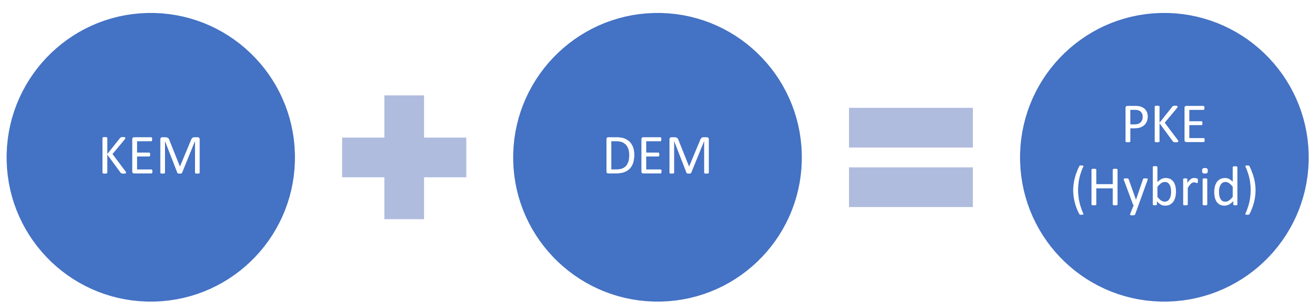
FrodoKEM

HQC

NTRU Prime

SIKE

$KEM = (KGen, Encap, Decap)$ $DEM = (Enc^{sym}, Dec^{sym})$ $PKE = (KGen, Enc, Dec)$



IND-CCA secure

(one-time) authenticated encryption

IND-CCA secure

KEM-DEM Paradigm

Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

$KEM = (KGen, Encap, Decap)$ $\quad DEM = (Enc^{sym}, Dec^{sym})$ $\quad PKE = (KGen, Enc, Dec)$

KEM + DEM = PKE (Hybrid)

Indistinguishable from a uniformly random DEM key k'

$(c_{KEM}, k) \leftarrow Encap(pk_{Bob})$

IND-CCA secure

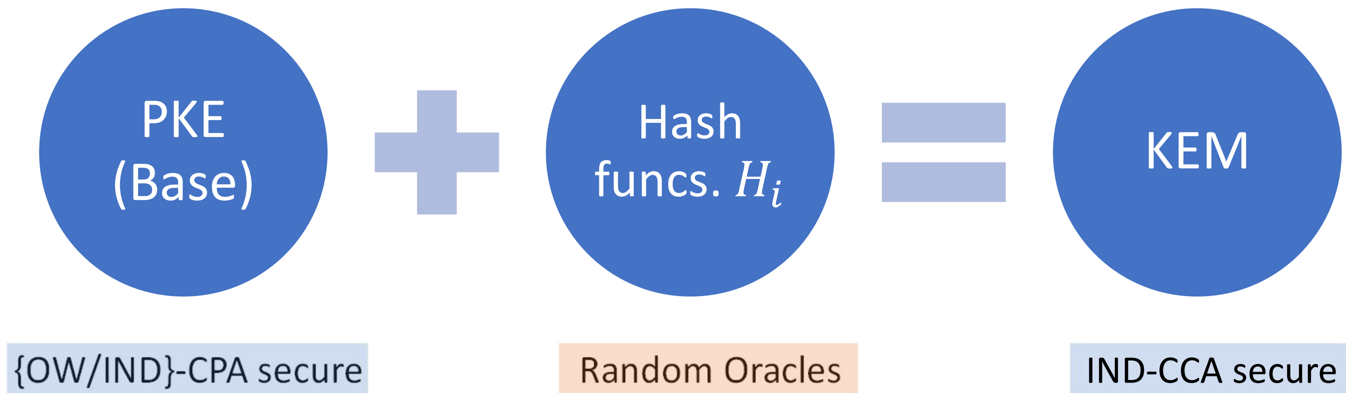
$c_{DEM} \leftarrow Enc^{sym}(k, m)$

(one-time) authenticated encryption

$(c_{KEM}, c_{DEM}) \leftarrow Enc(pk_{Bob}, m)$

IND-CCA secure

Fujisaki-Okamoto Transformation



Anonymity from FO transforms

$Enc(pk_{Bob}, m) \approx Enc(pk_{Dave}, m)$, for random secret m

PKE (Base) + Hash funcs. H_i $\overset{\text{FO}^{\not\perp}}{=}$ KEM

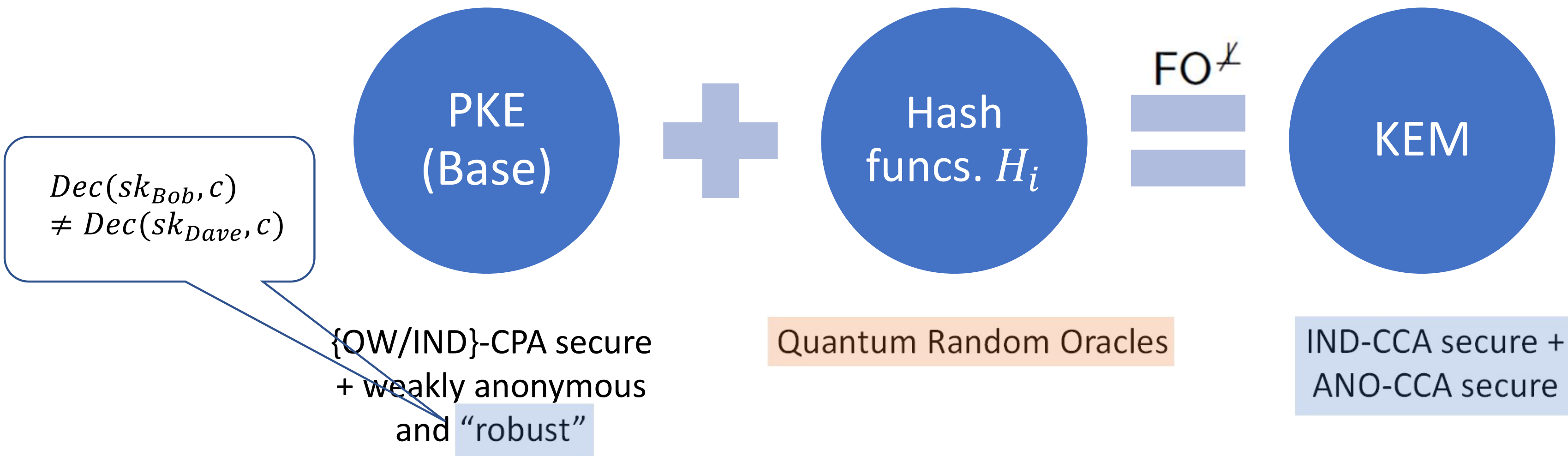
{OW/IND}-CPA secure + weakly anonymous and “robust”

Quantum Random Oracles

IND-CCA secure + ANO-CCA secure

Shown in [Grubbs-Maram-Paterson’22]

Anonymity from FO transforms



Shown in [Grubbs-Maram-Paterson'22]