Quantum CCA-Secure PKE, Revisited

Varun Maram

Cybersecurity Group

SandboxAQ

: https://varun-maram.github.io/

: varun-maram-pqc

Joint work with Navid Alamati

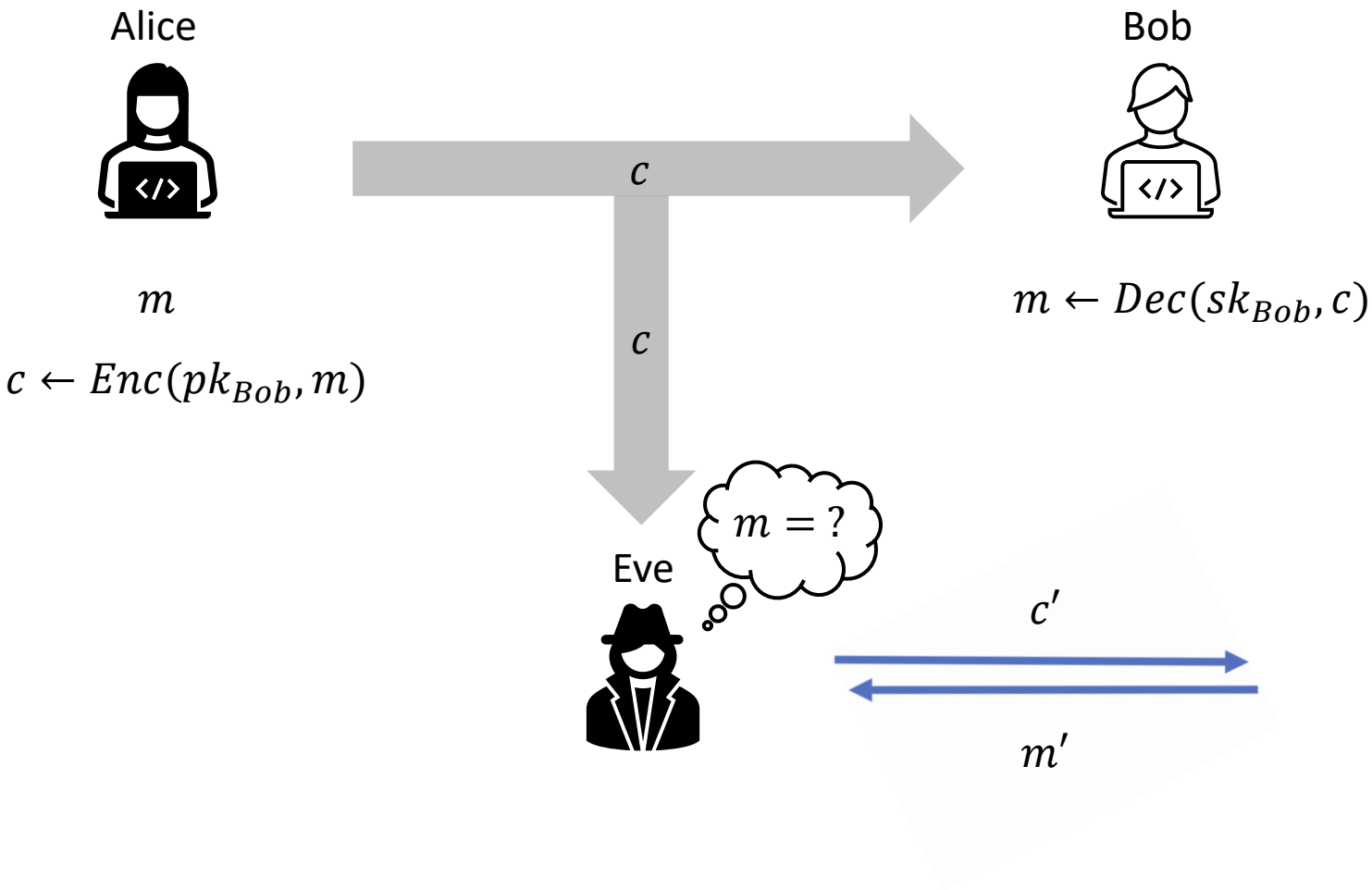
ETH zürich SANDBOXAQ VISA

Quantum CCA-Secure PKE, Revisited

Quantum CCA-Secure PKE, Revisited

IND-CCA Security

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

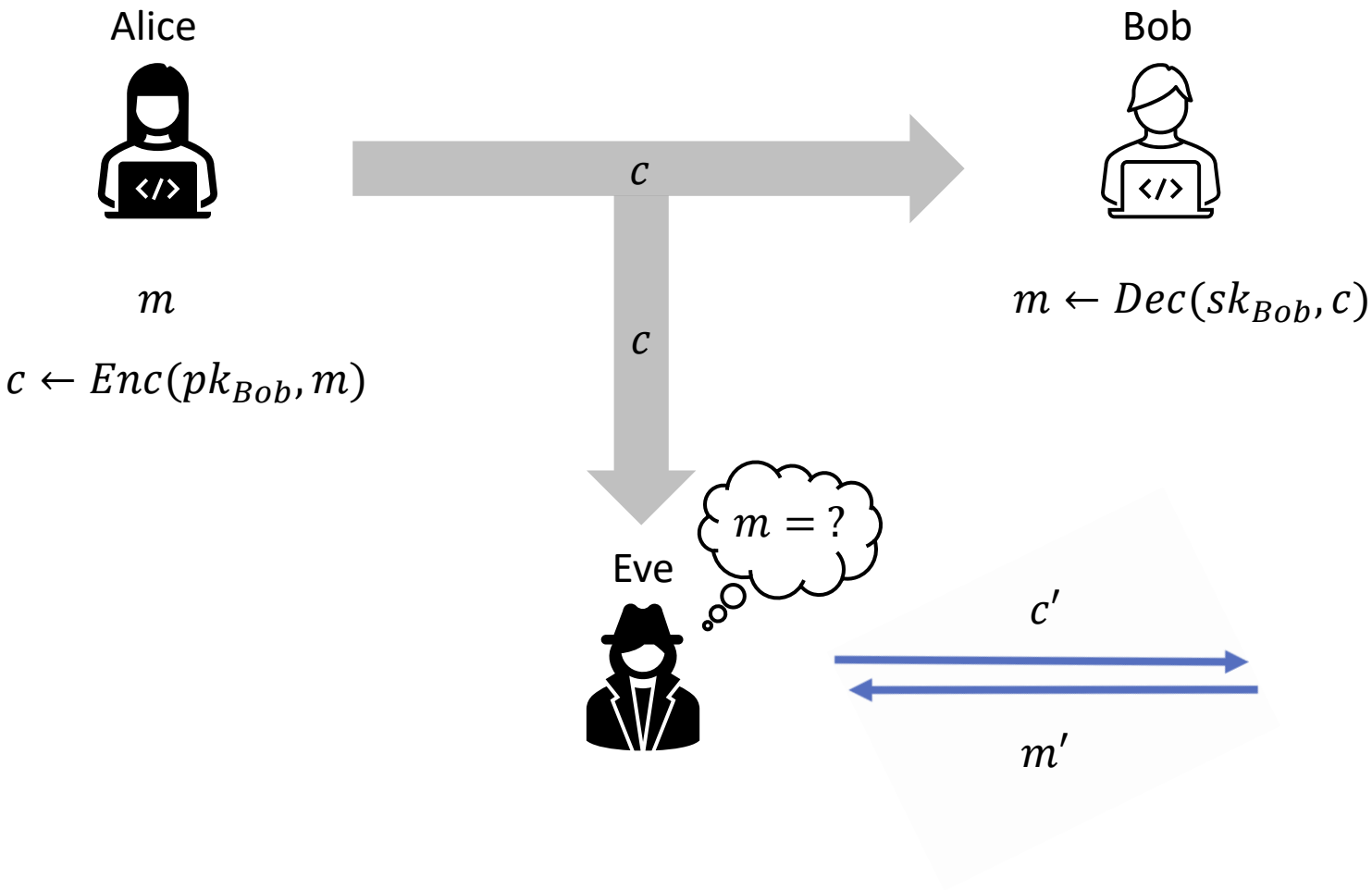


Quantum CCA-Secure PKE, Revisited

Quantum CCA-Secure PKE, Revisited

IND-CCA Security

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



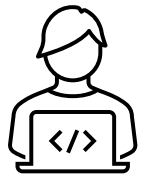
IND-qCCA Security

Introduced by [Boneh-Zhandry'13].

$PKE = (KGen, Enc, Dec)$

Alice

Bob



c

m

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

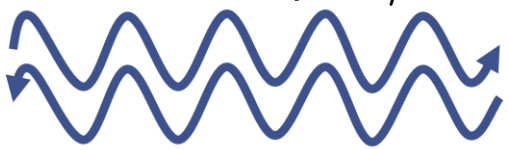
c

$m \leftarrow Dec(sk_{Bob}, c)$

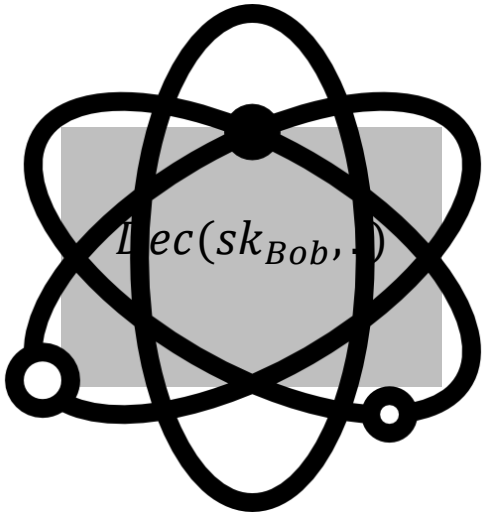
Eve

$m = ?$

$\alpha|c'\rangle + \beta|c''\rangle$



$\alpha|m'\rangle + \beta|m''\rangle$



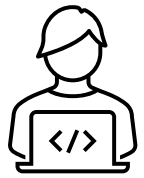
IND-qCCA Security

Introduced by [Boneh-Zhandry'13].

$PKE = (KGen, Enc, Dec)$

Alice

Bob



c

m

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

c

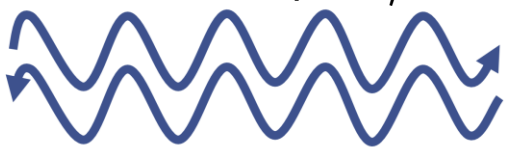
$m \leftarrow Dec(sk_{Bob}, c)$

- Relevance in future when quantum computing becomes ubiquitous.

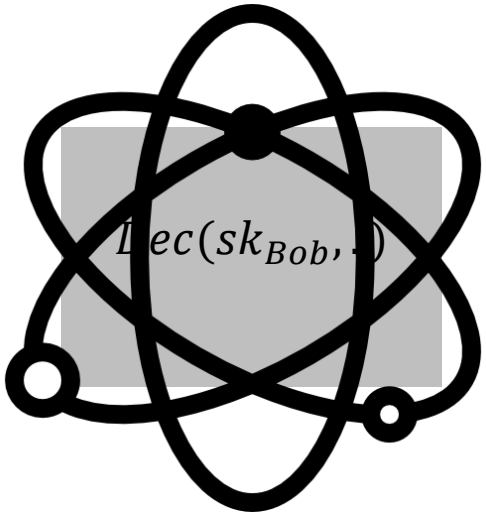
Eve

$m = ?$

$\alpha|c'\rangle + \beta|c''\rangle$



$\alpha|m'\rangle + \beta|m''\rangle$



IND-qCCA Security

Introduced by [Boneh-Zhandry'13].

$PKE = (KGen, Enc, Dec)$

Alice

Bob

m

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

c

c

$m \leftarrow Dec(sk_{Bob}, c)$

Eve

$m = ?$

$\alpha|c'\rangle + \beta|c''\rangle$

$\alpha|m'\rangle + \beta|m''\rangle$

$Dec(sk_{Bob}, \cdot)$

- Relevance in future when quantum computing becomes ubiquitous.
- Also, in not-so-far future when adversaries can trick classical devices to behave "quantumly" (e.g., "frozen smart-card attacks").

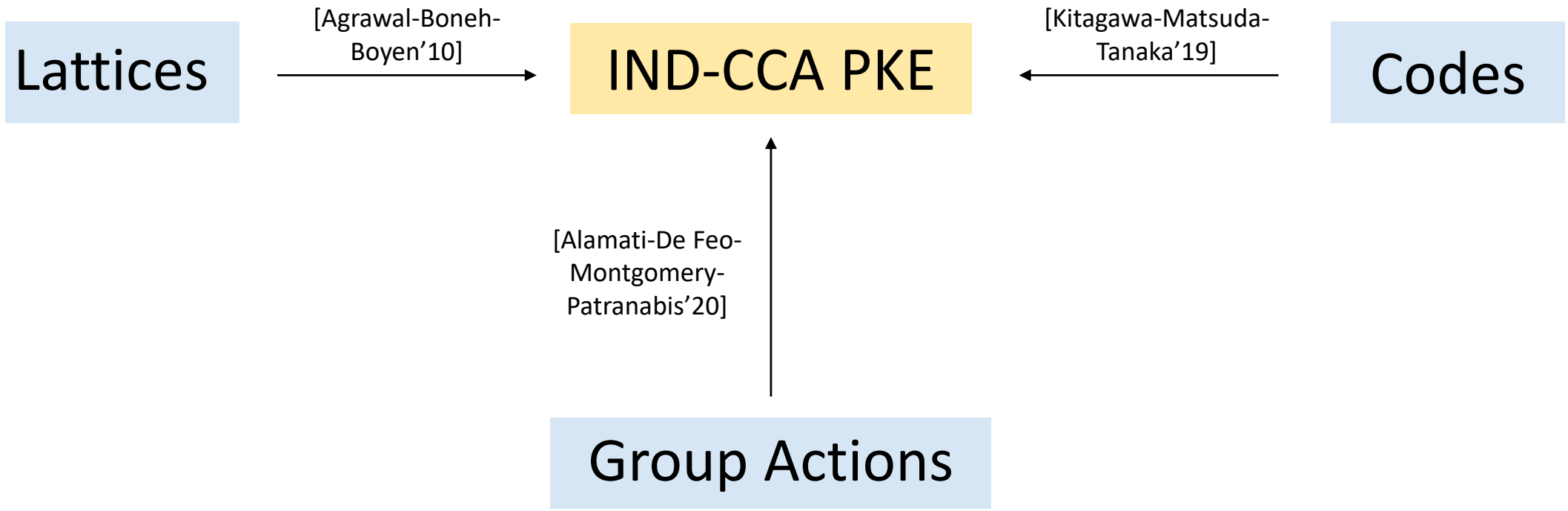
Quantum CCA-Secure PKE, Revisited

Quantum CCA-Secure PKE, Revisited

Motivation

IND-CCA PKE

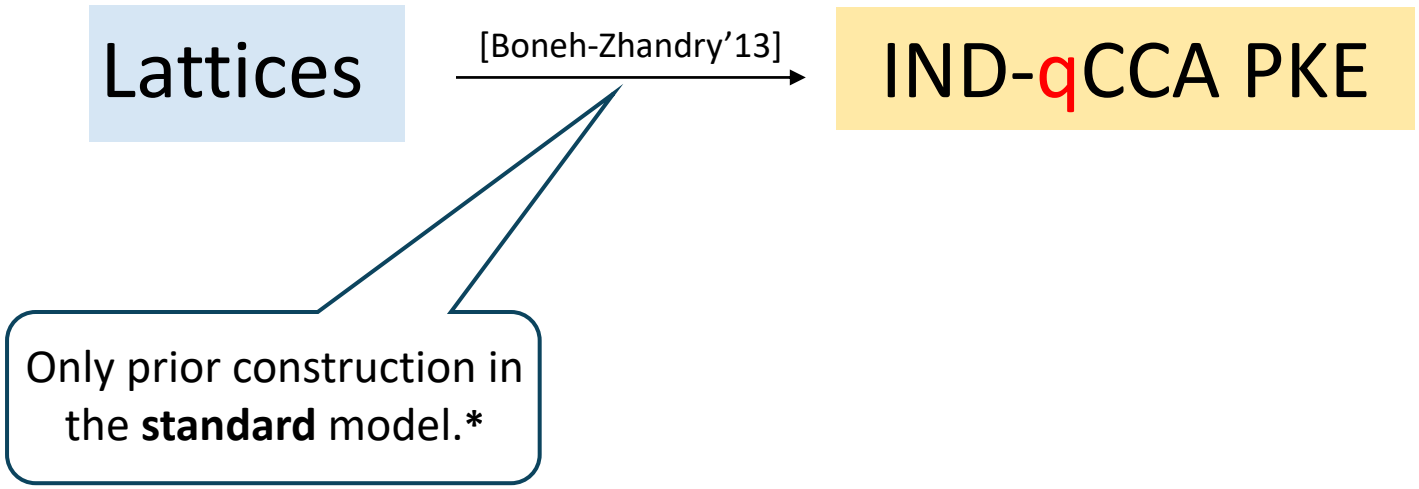
Motivation


Lattices
[Agrawal-Boneh-Boyen'10]
IND-CCA PKE
[Kitagawa-Matsuda-Tanaka'19]
Codes
[Alamati-De Feo-Montgomery-Patranabis'20]
Group Actions

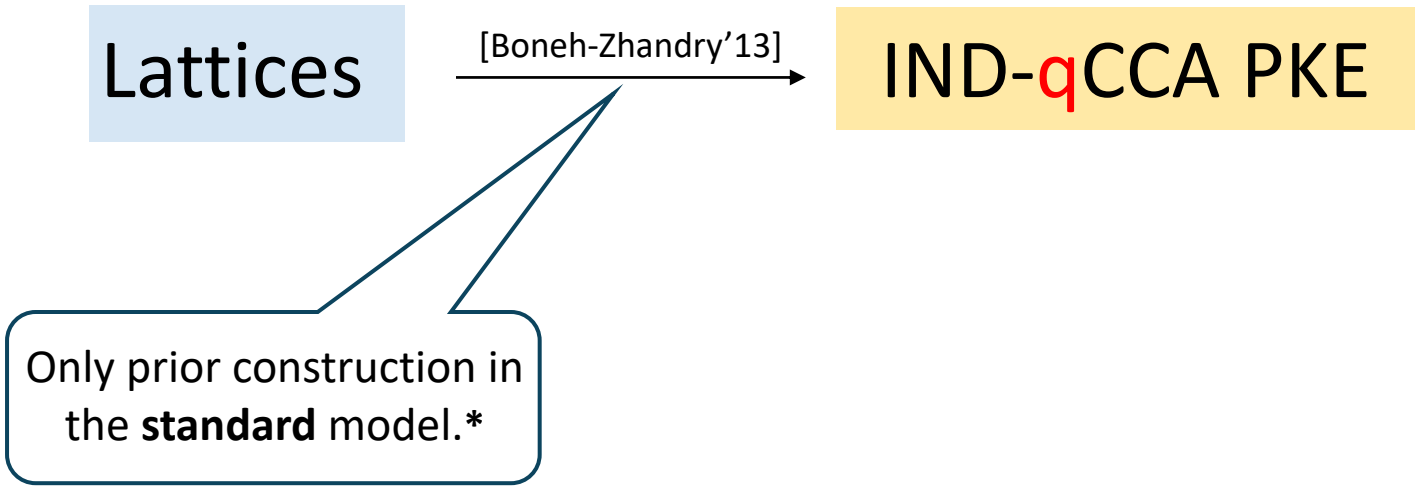
Motivation

IND-qCCA PKE

Motivation

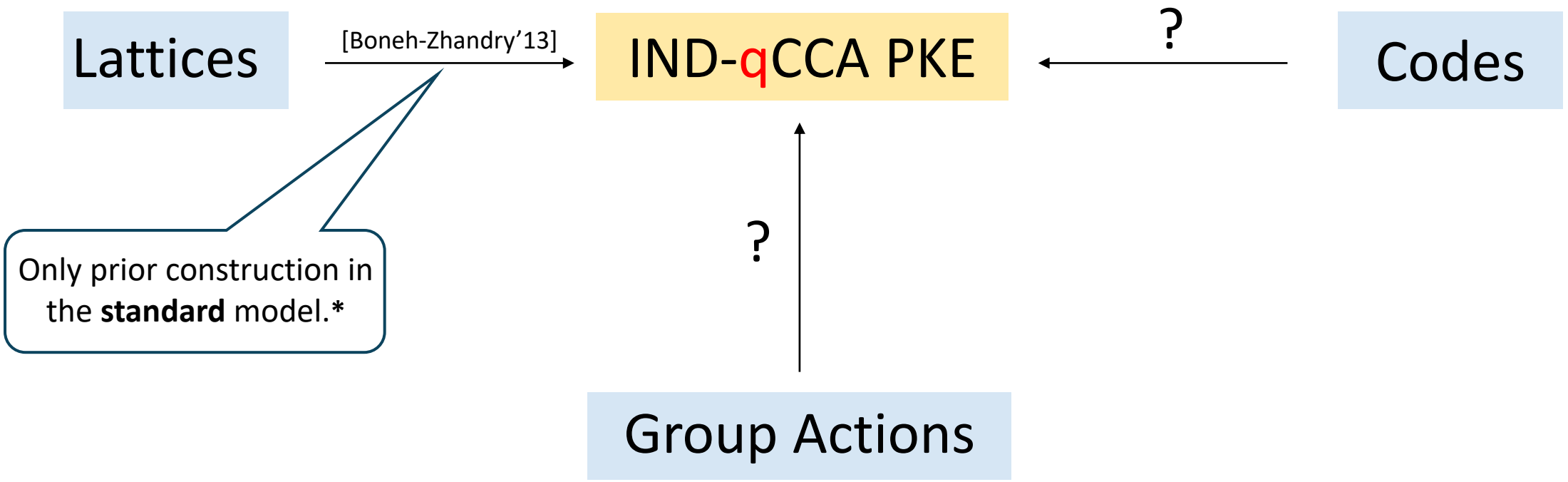

Lattices
[Boneh-Zhandry'13]
IND-qCCA PKE
Only prior construction in the **standard** model.*

Motivation



*There exist richer constructions of qCCA-secure PKE in the idealized **quantum ROM** – e.g., by [Xagawa-Yamakawa'19].

Motivation


Lattices
[Boneh-Zhandry'13]
IND-qCCA PKE
?
Codes
Only prior construction in the **standard** model.*
?
Group Actions

Motivation

Lattices

[Boneh-Zhandry'13]

IND-qCCA PKE

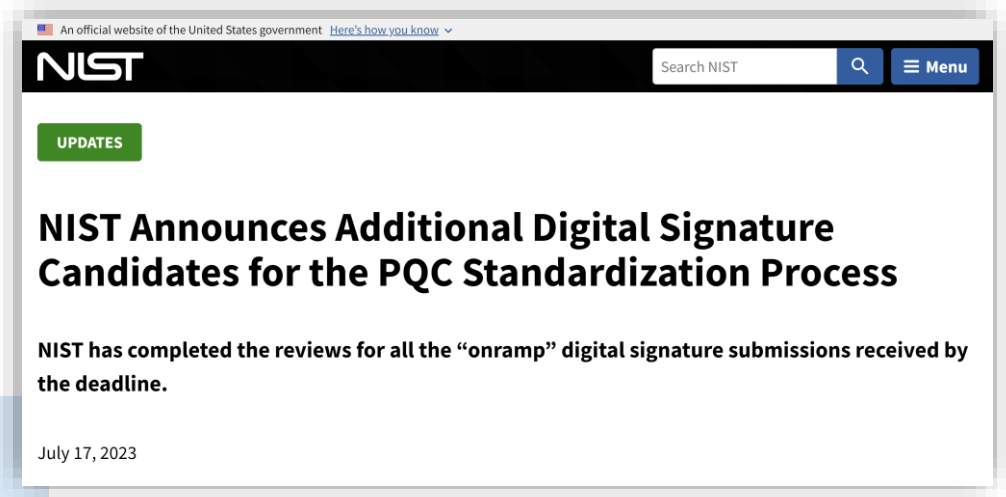
?

Codes

Only prior construction in the **standard** model.*

?

Group Actions



Motivation

Quantum Algorithms for Lattice Problems

Yilei Chen*

April 10, 2024

Lattices

[Boneh-Zhandry'13]

IND-qCCA PKE

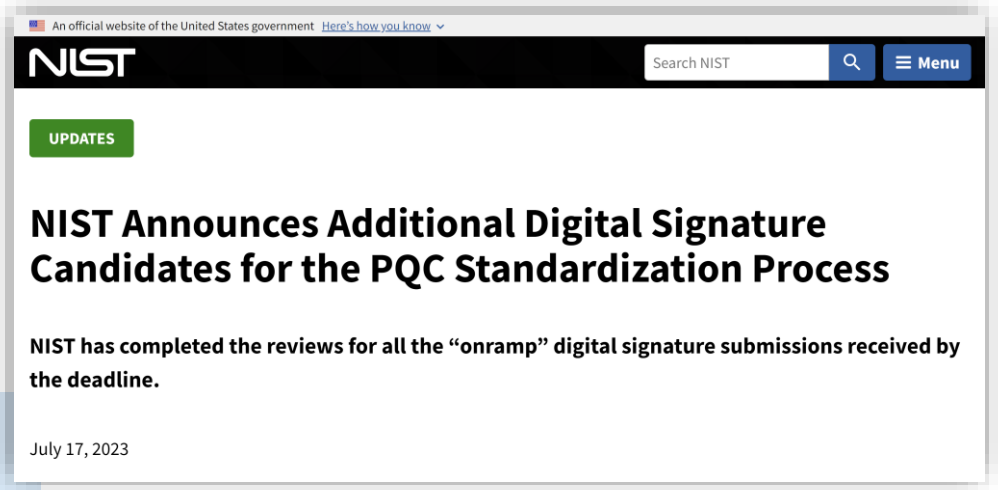
?

Codes

Only prior construction in the **standard** model.*

?

Group Actions



Motivation

Lattices → [Boneh-Zhandry'13] → IND-qCCA PKE

Motivation

Lattices → [Boneh-Zhandry'13] → IND-qCCA PKE

Lattices → [Agrawal-Boneh-Boyen'10] → IND-CCA PKE

Motivation

Lattices → [Boneh-Zhandry'13] → IND-qCCA PKE

Lattices → [Agrawal-Boneh-Boyen'10] → IND-CCA PKE

Motivation

Lattices → [Boneh-Zhandry'13] → IND-qCCA PKE

Lattices → [Agrawal-Boneh-Boyen'10] → Selective-IBE → IND-CCA PKE

Identity-**B**ased **E**ncryption.

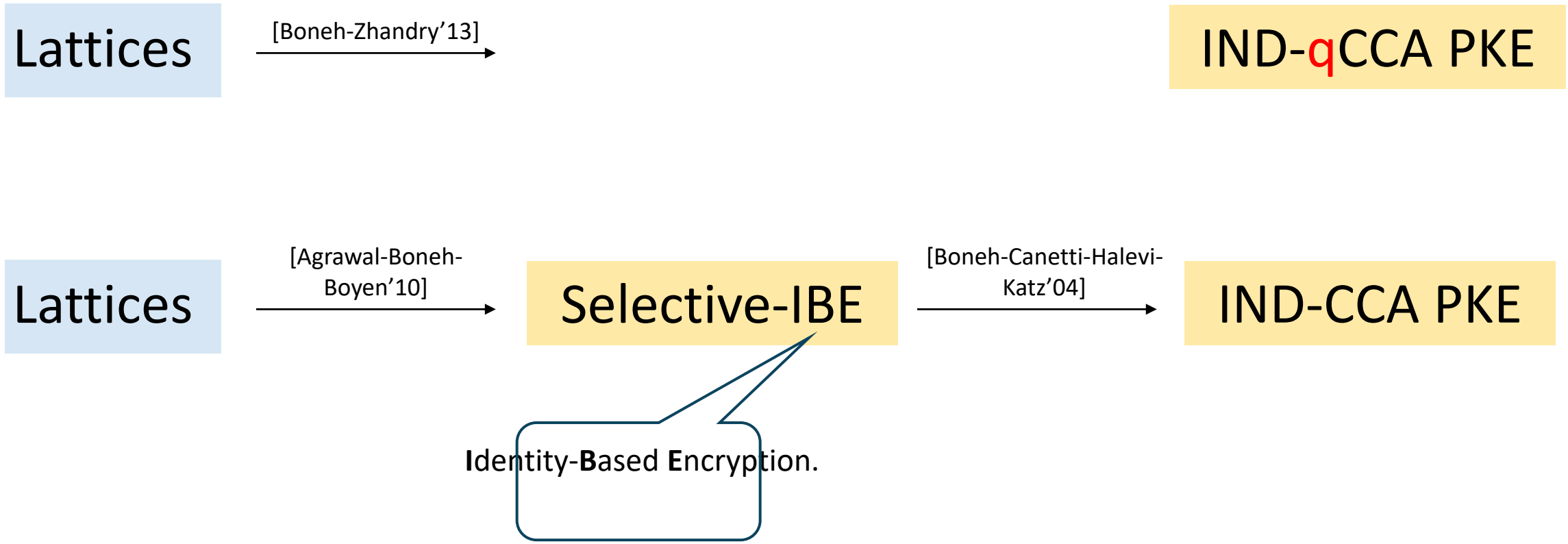
Motivation

Lattices → [Boneh-Zhandry'13] → IND-qCCA PKE

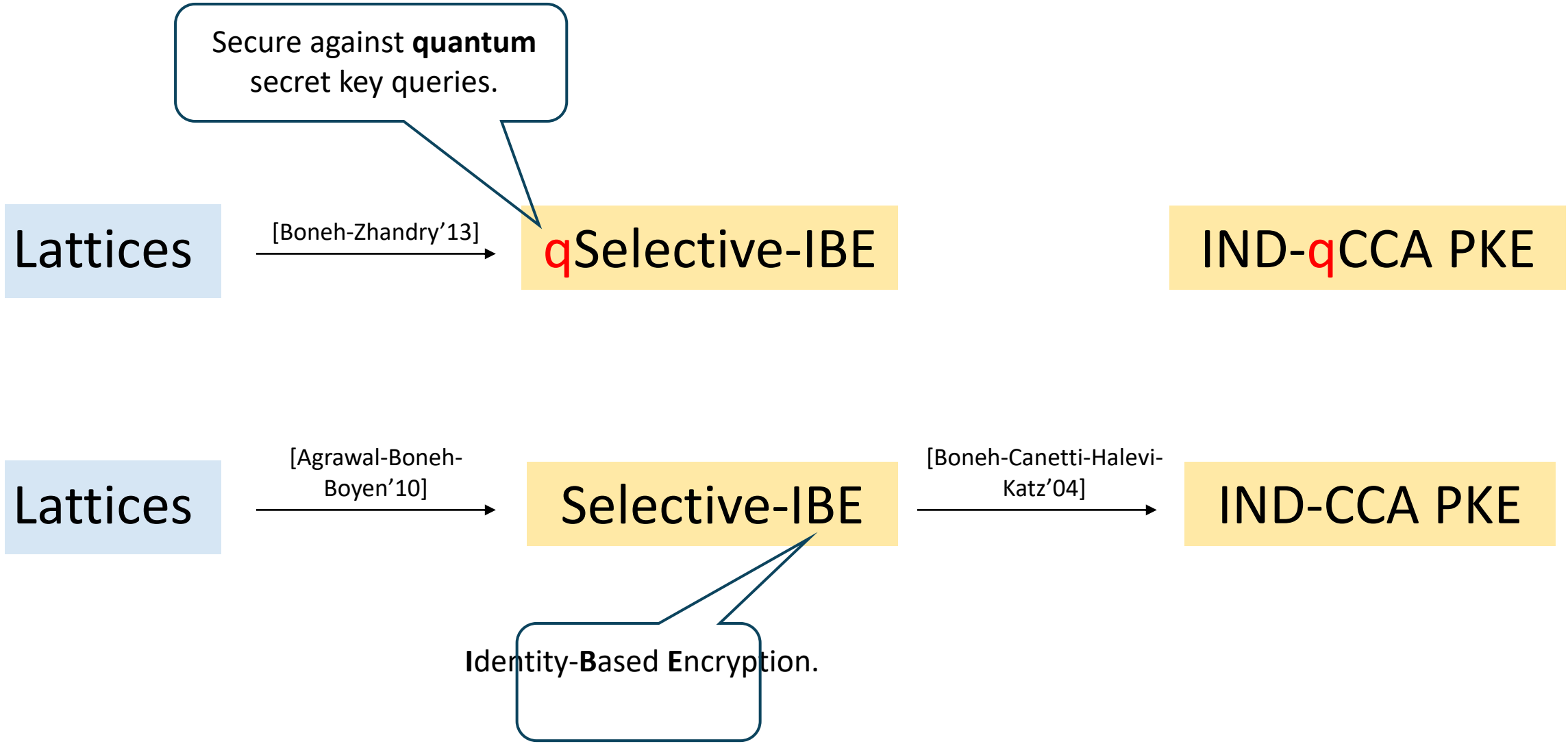
Lattices → [Agrawal-Boneh-Boyen'10] → Selective-IBE → [Boneh-Canetti-Halevi-Katz'04] → IND-CCA PKE

Identity-**B**ased **E**ncryption.

Motivation


Lattices
[Boneh-Zhandry'13]
IND-qCCA PKE
Lattices
[Agrawal-Boneh-Boyen'10]
Selective-IBE
[Boneh-Canetti-Halevi-Katz'04]
IND-CCA PKE
Identity-Based Encryption.

Motivation


Secure against **quantum** secret key queries.
Lattices
[Boneh-Zhandry'13]
qSelective-IBE
IND-qCCA PKE
Lattices
[Agrawal-Boneh-Boyen'10]
Selective-IBE
[Boneh-Canetti-Halevi-Katz'04]
IND-CCA PKE
Identity-**B**ased **E**ncryption.

Motivation

Secure against **quantum** secret key queries.

Using the same IBE → PKE construction of [Boneh-Canetti-Halevi-Katz'04].

Lattices → [Boneh-Zhandry'13] → qSelective-IBE → [Boneh-Zhandry'13] → IND-qCCA PKE

Lattices → [Agrawal-Boneh-Boyen'10] → Selective-IBE → [Boneh-Canetti-Halevi-Katz'04] → IND-CCA PKE

Identity-**B**ased **E**ncryption.

Motivation

Secure against **quantum** secret key queries.

Using the same IBE → PKE construction of [Boneh-Canetti-Halevi-Katz'04].

Lattices → [Boneh-Zhandry'13] → qSelective-IBE → [Boneh-Zhandry'13] → IND-qCCA PKE

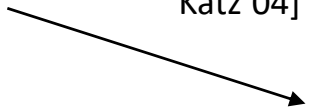
Lattices → [Agrawal-Boneh-Boyen'10] → Selective-IBE → [Boneh-Canetti-Halevi-Katz'04] → IND-CCA PKE

Identity-**B**ased **E**ncryption.

Motivation

Selective-IBE

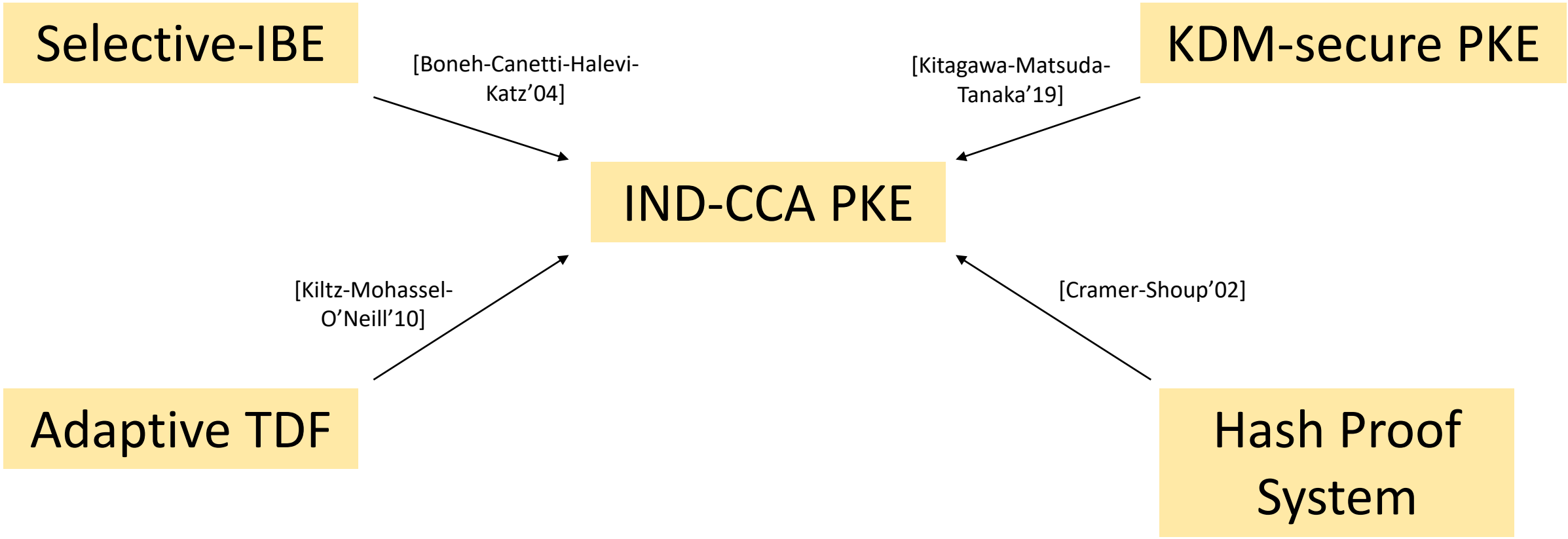
[Boneh-Canetti-Halevi-Katz'04]



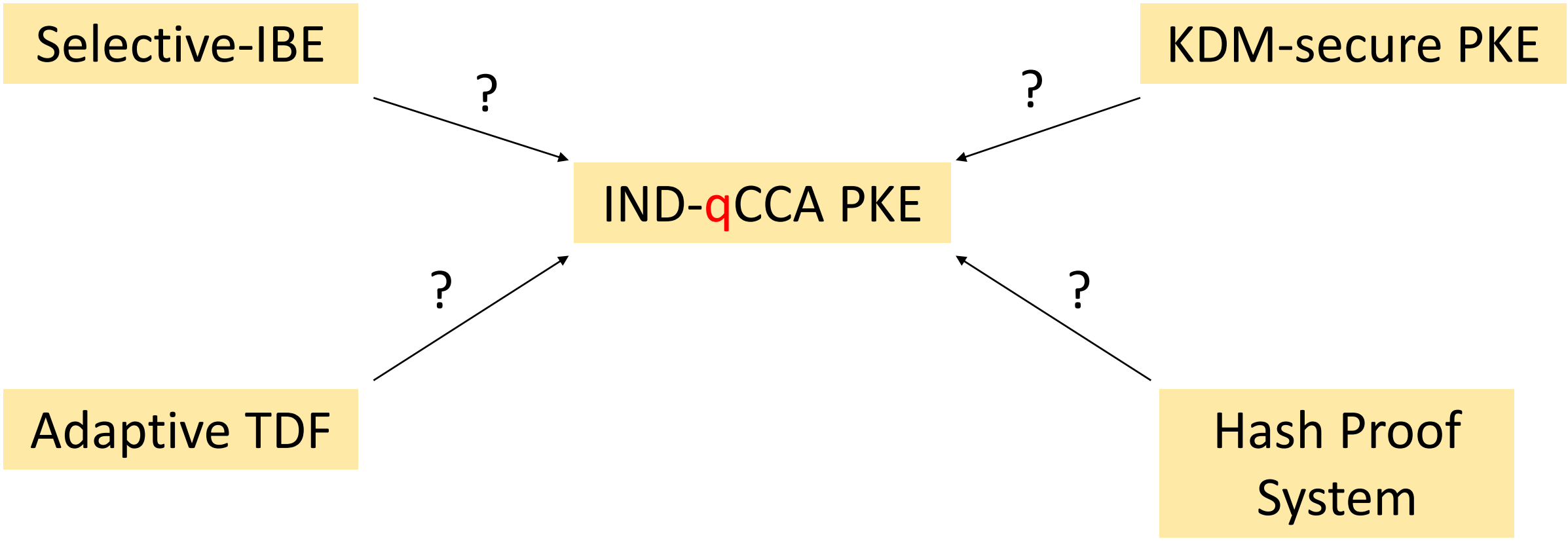
IND-CCA PKE

Motivation

Key-**D**ependent **M**essage.

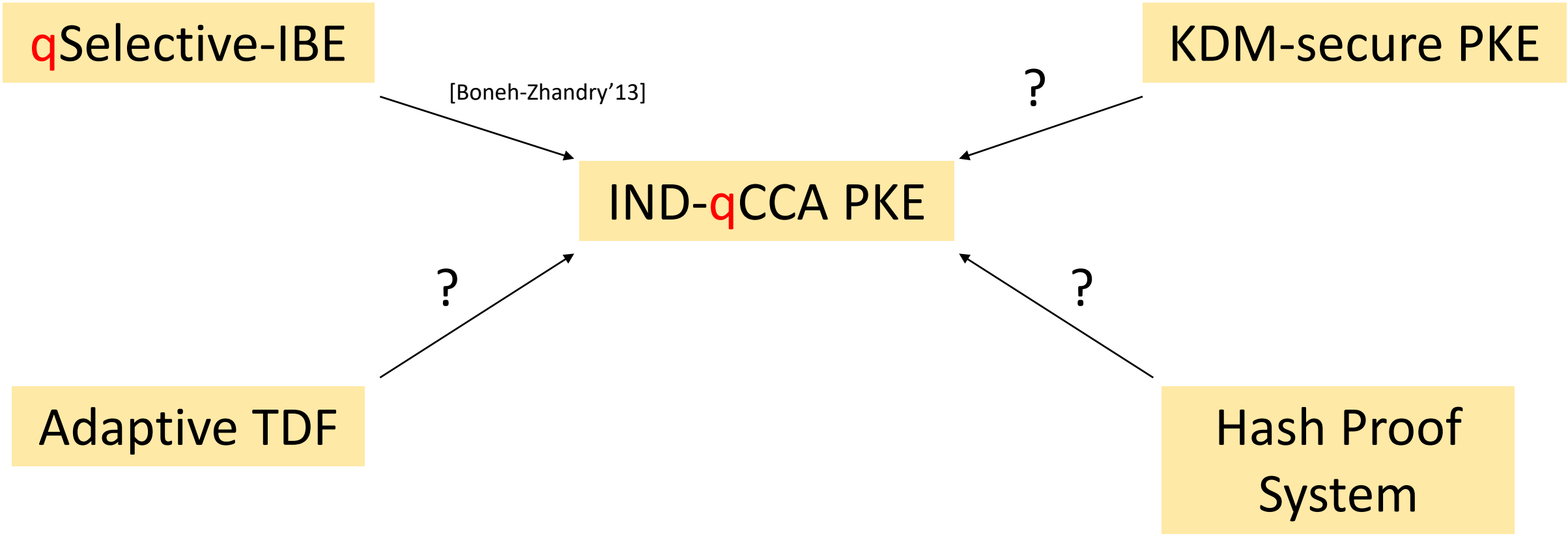


Motivation


Selective-IBE
KDM-secure PKE
?
?
IND-qCCA PKE
?
?
Adaptive TDF
Hash Proof System

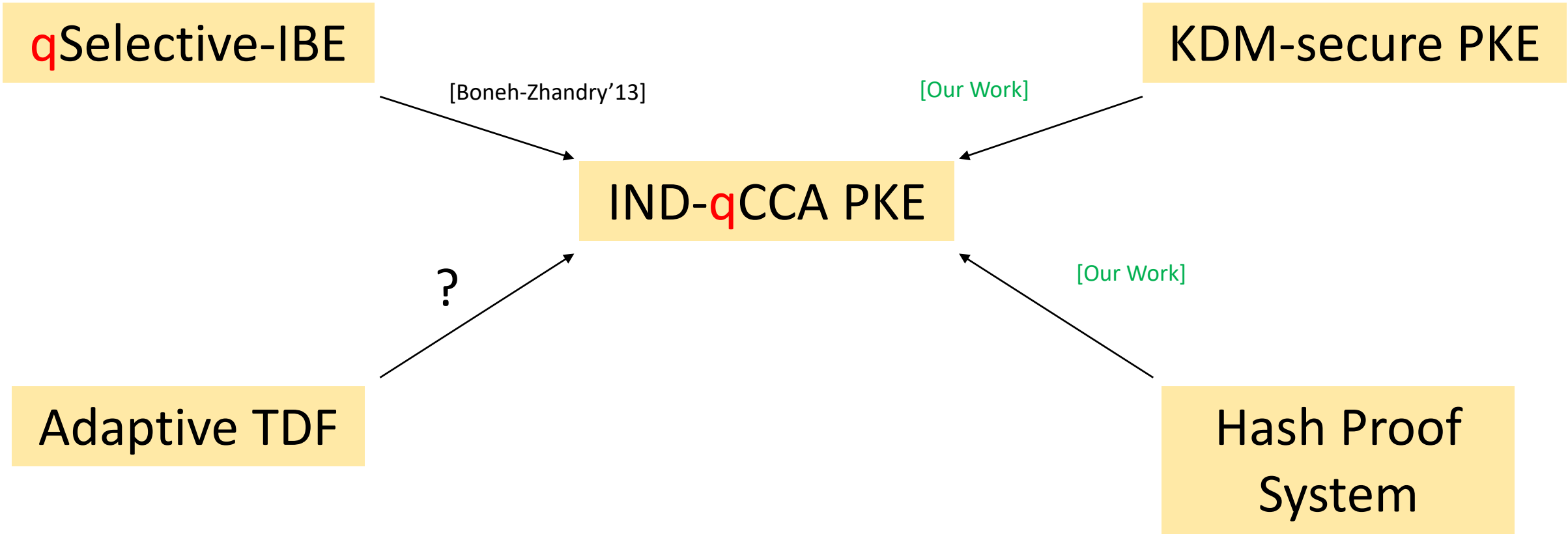
Motivation

Secure against **post-quantum** adversaries with **quantum access** to secret oracles.

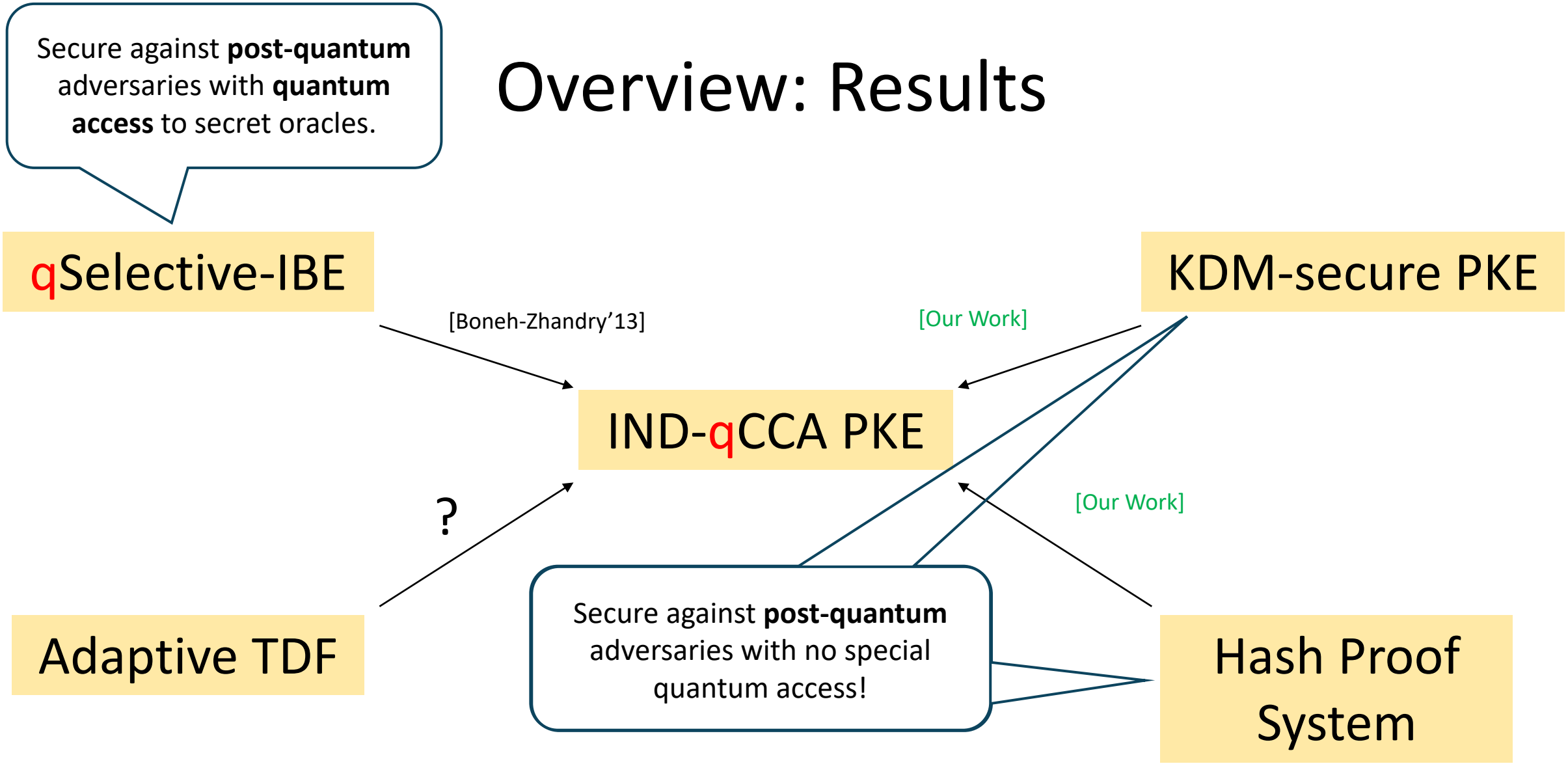


Secure against **post-quantum** adversaries with **quantum access** to secret oracles.

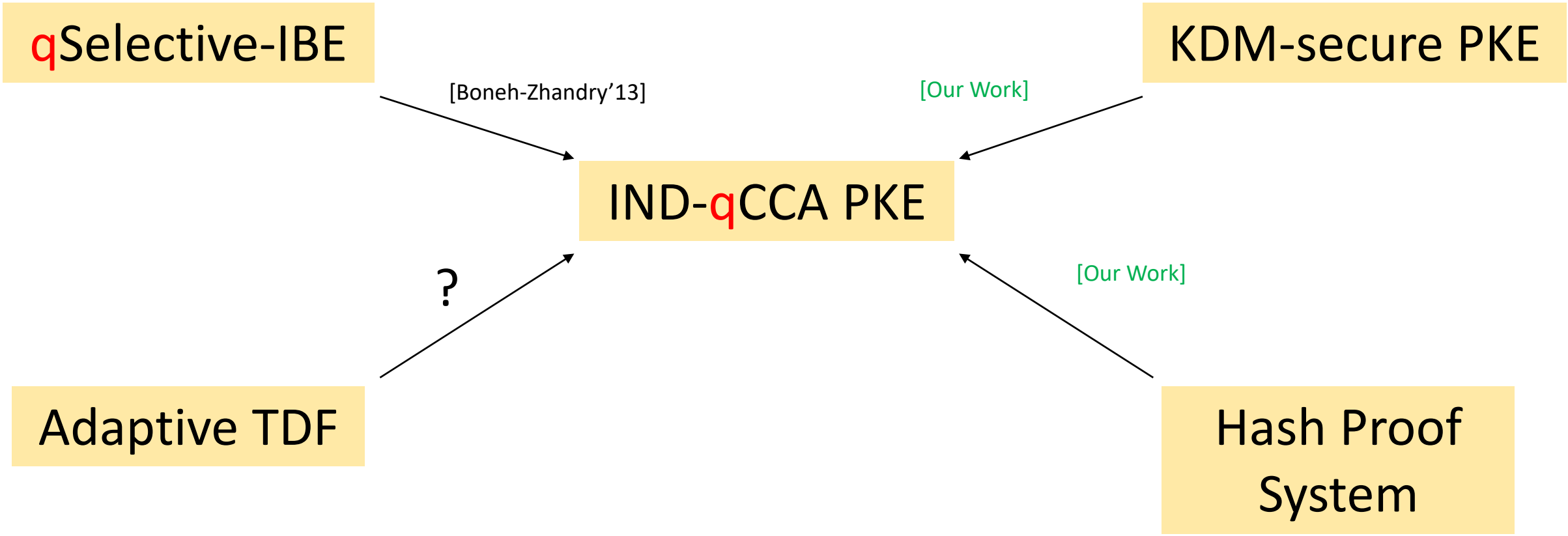
Overview: Results



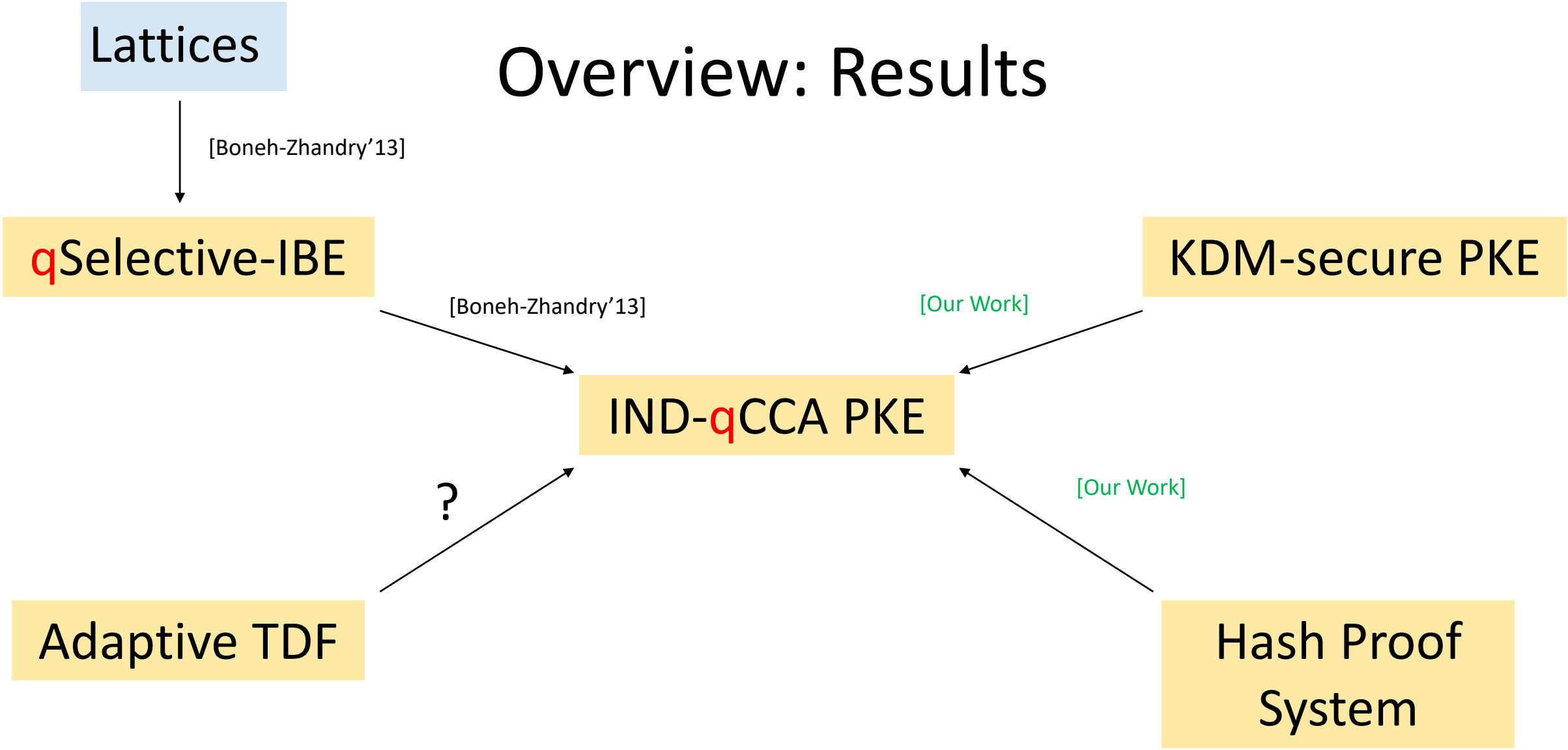
Overview: Results



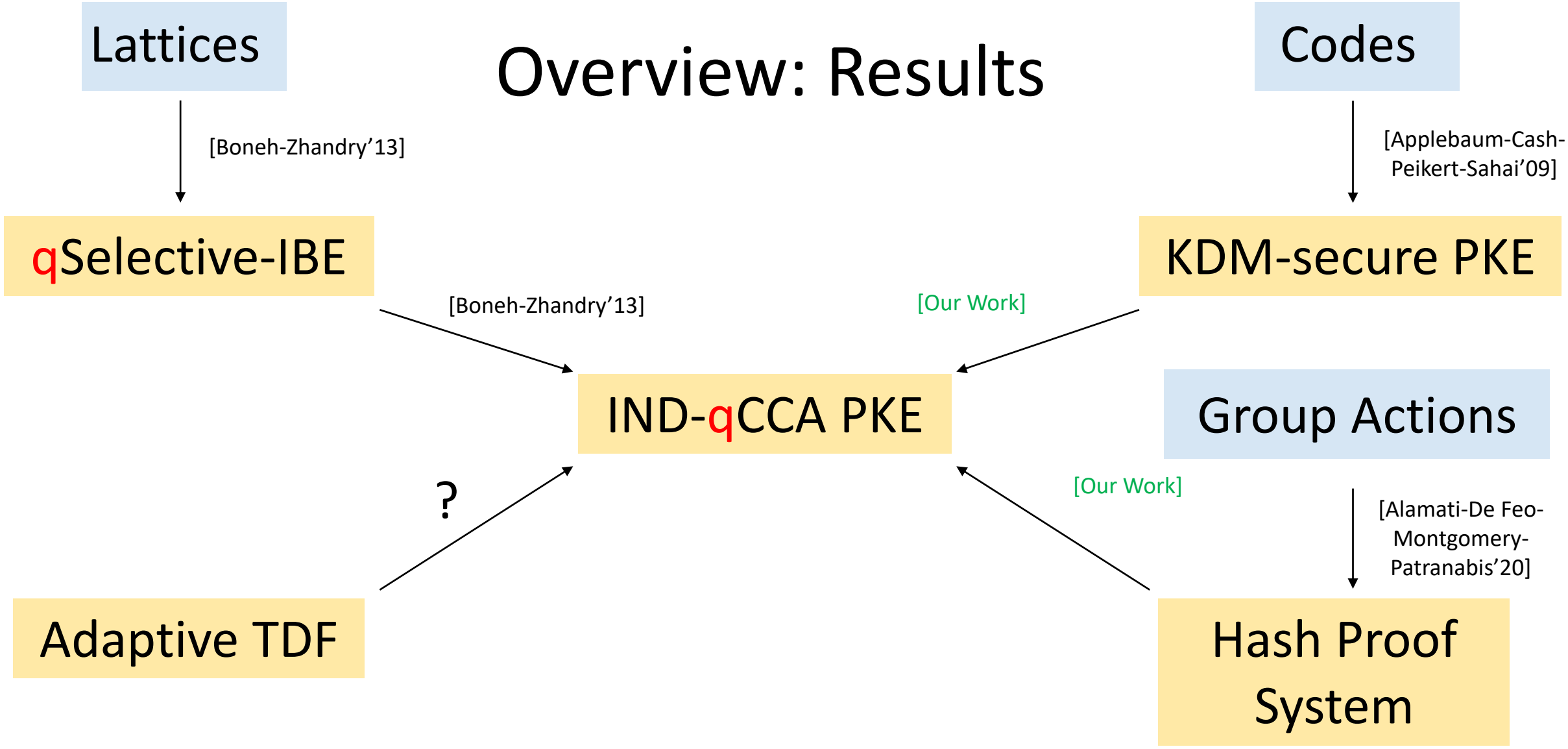
Overview: Results



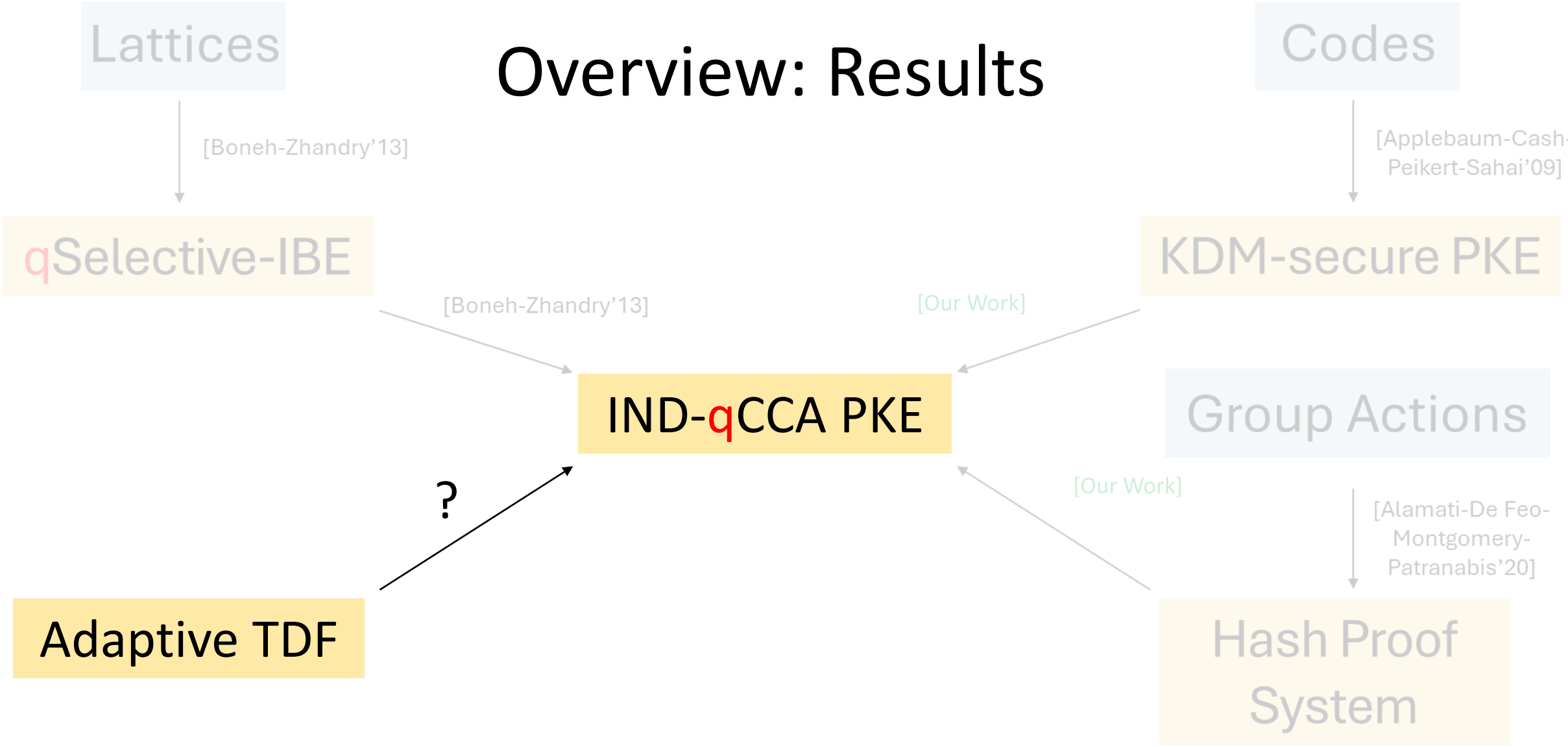
Overview: Results



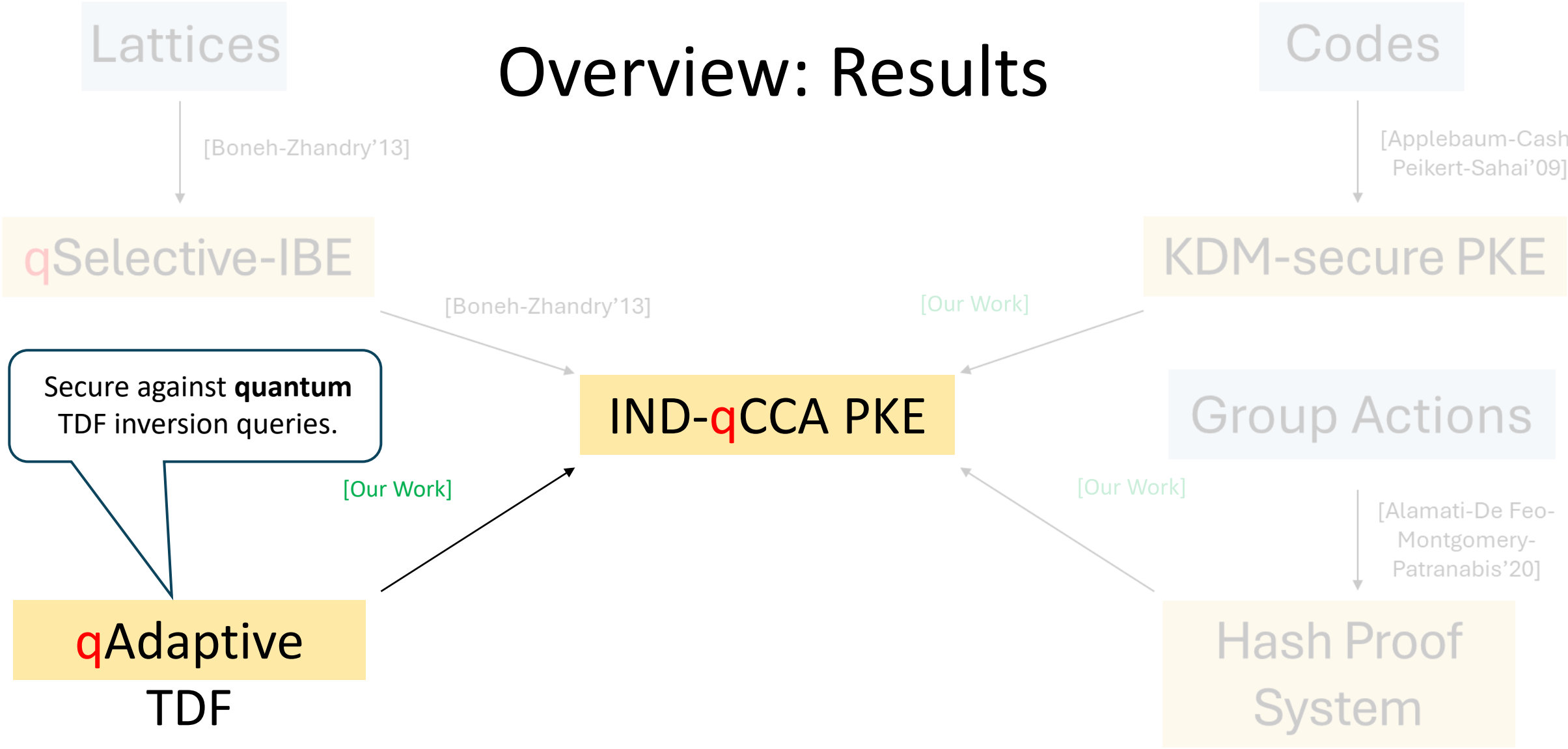
Overview: Results



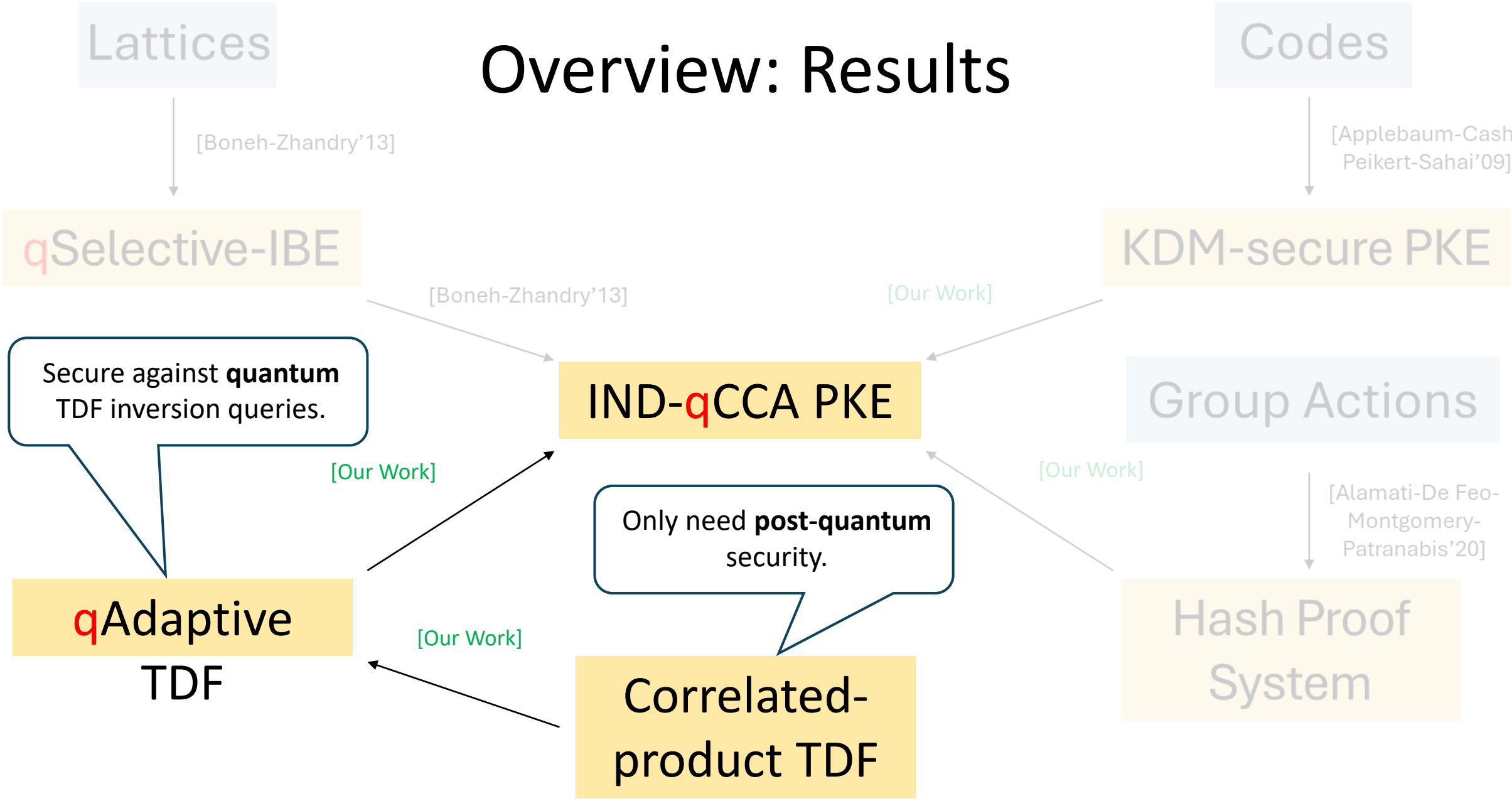
Overview: Results



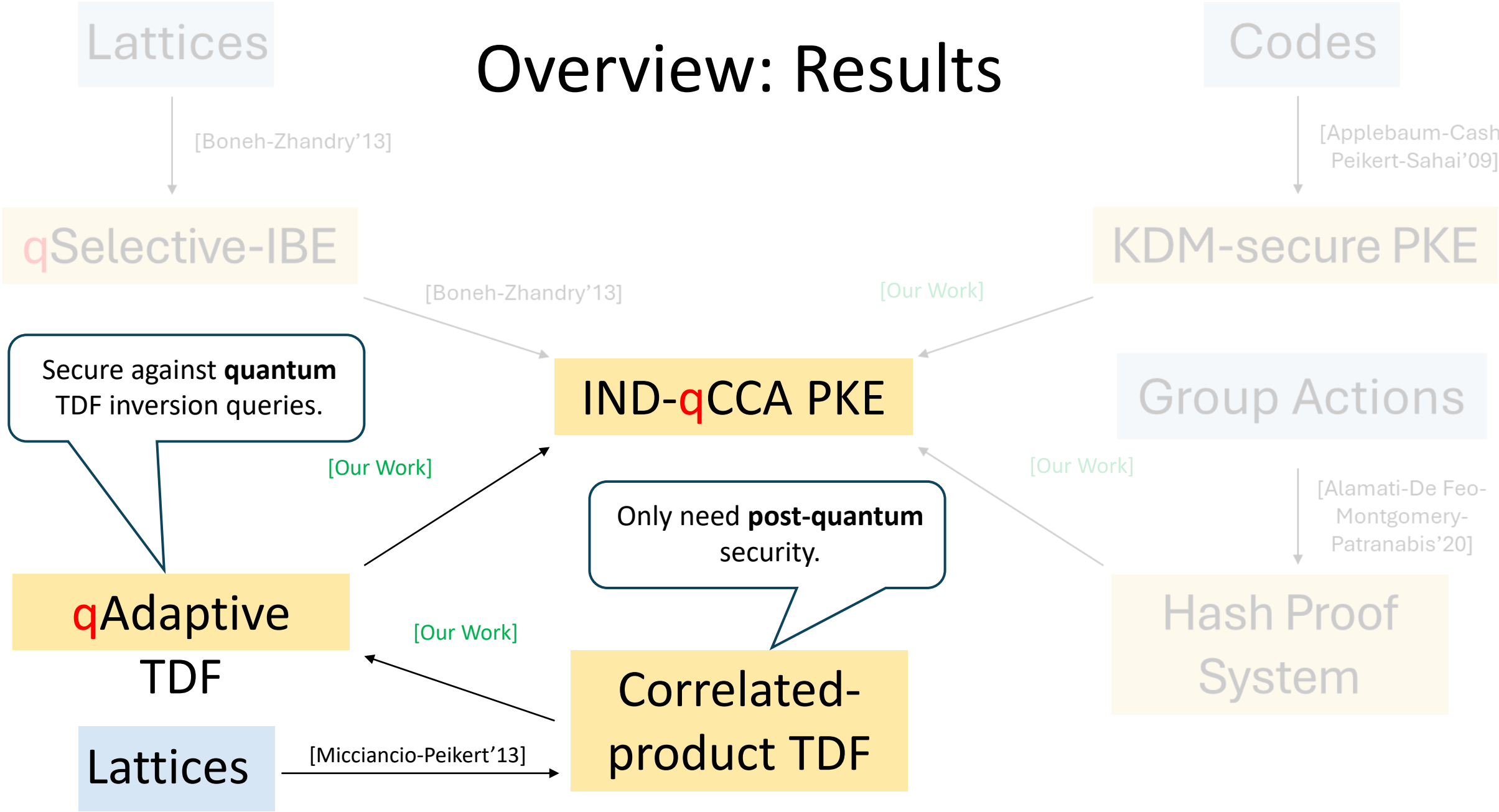
Overview: Results



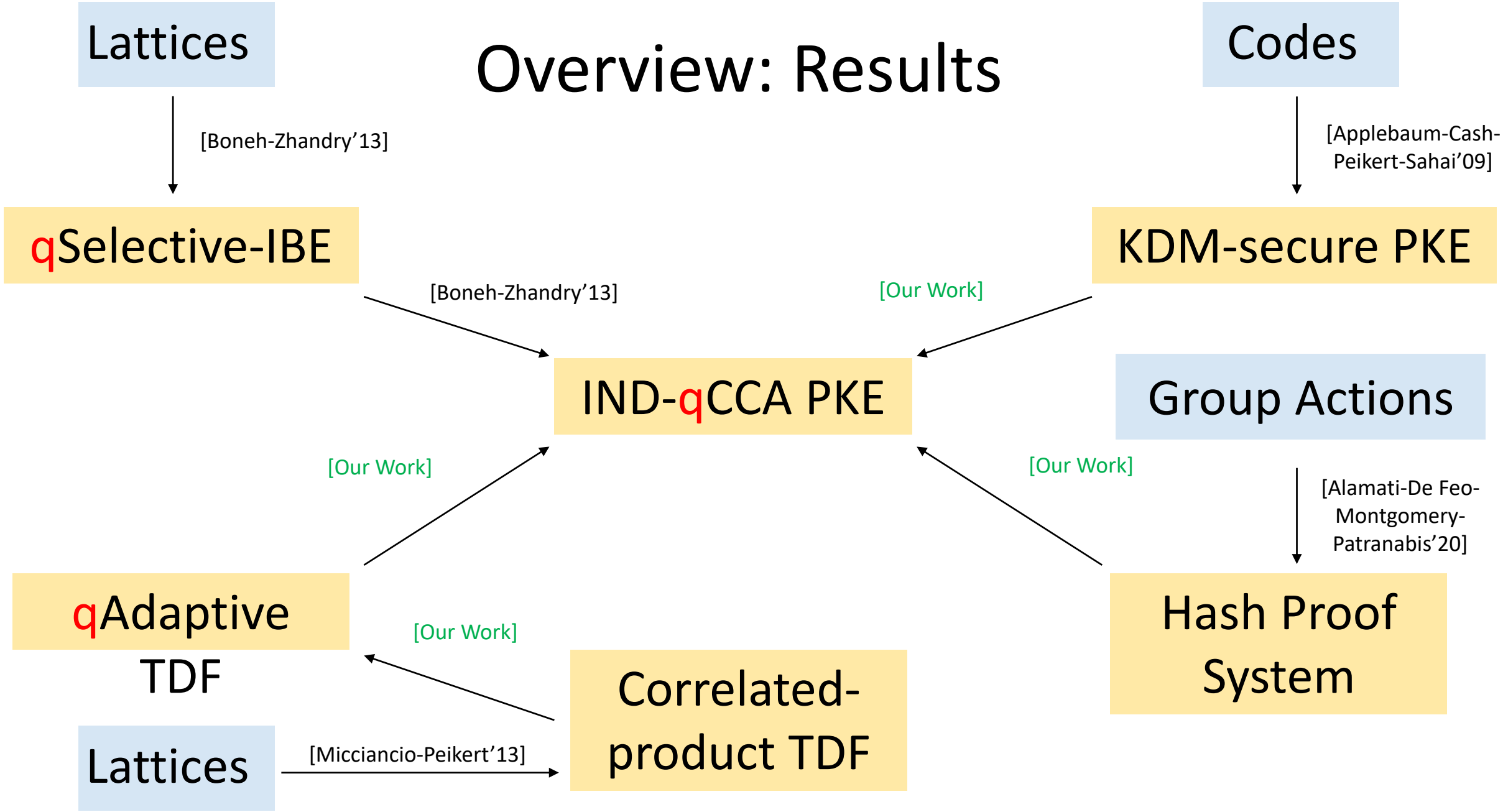
Overview: Results



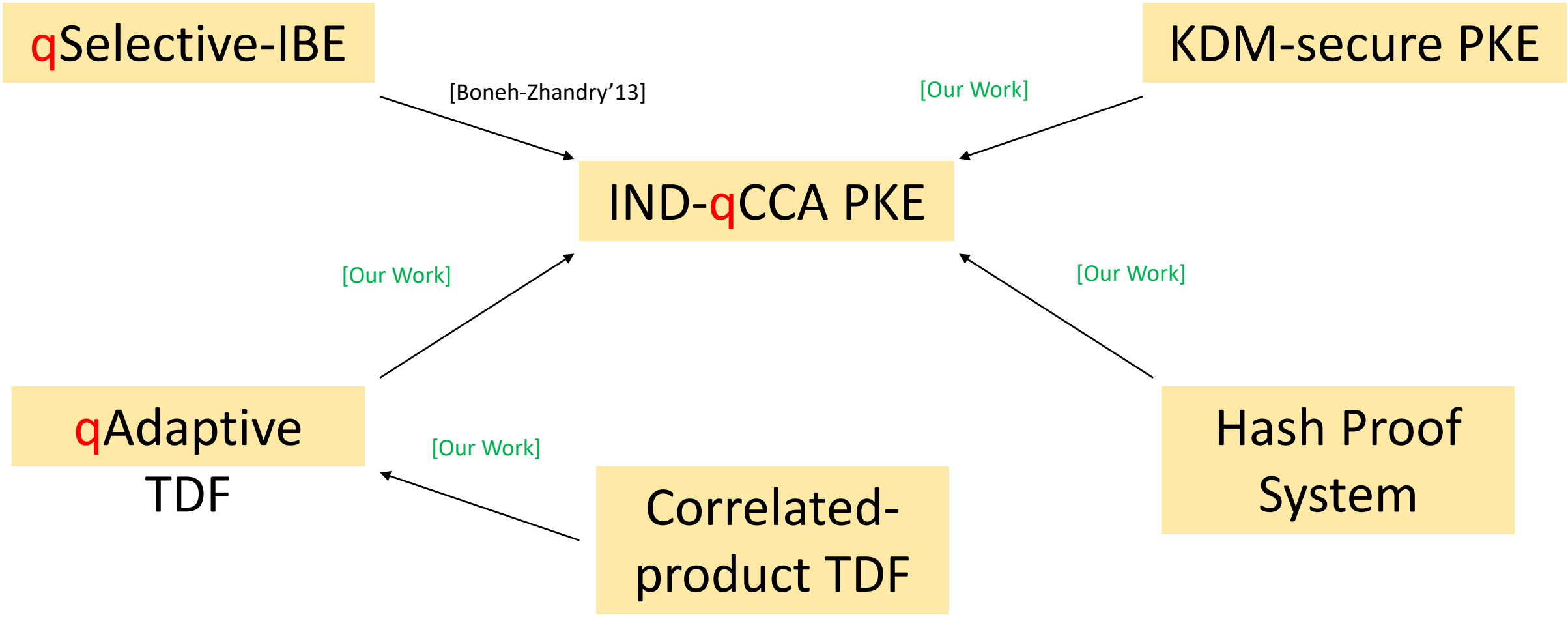
Overview: Results



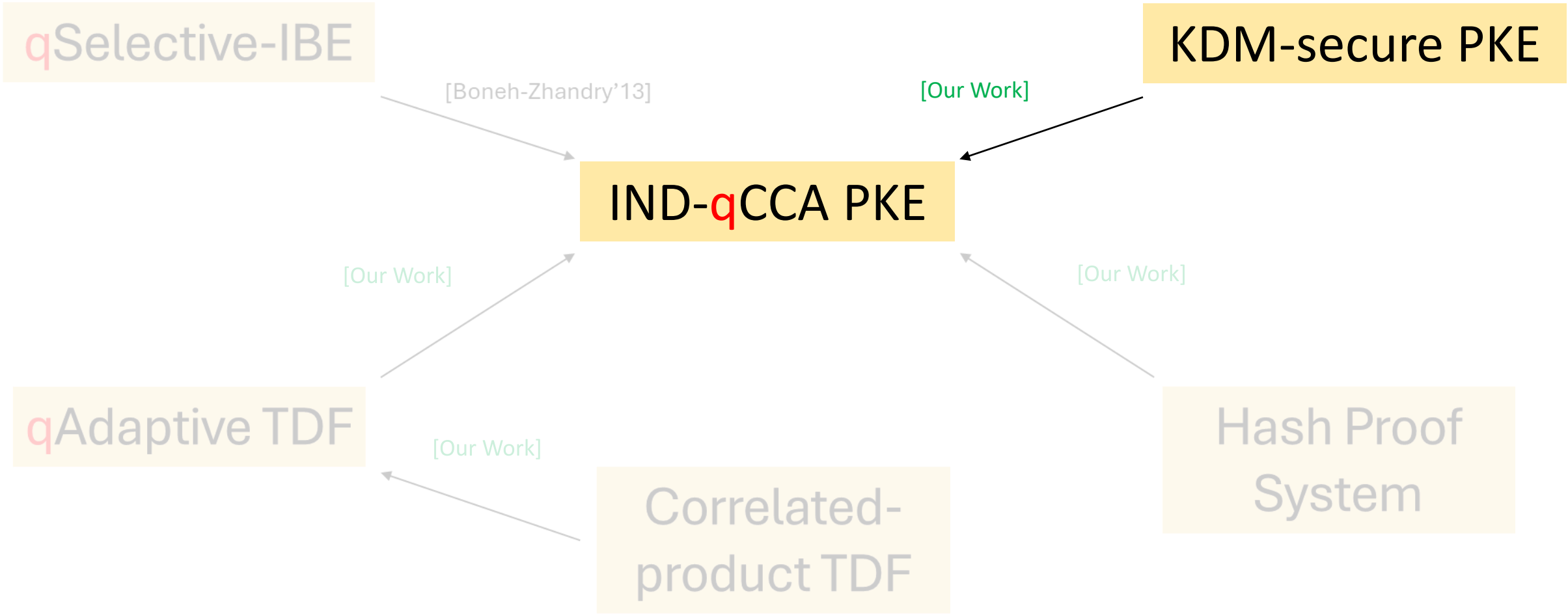
Overview: Results



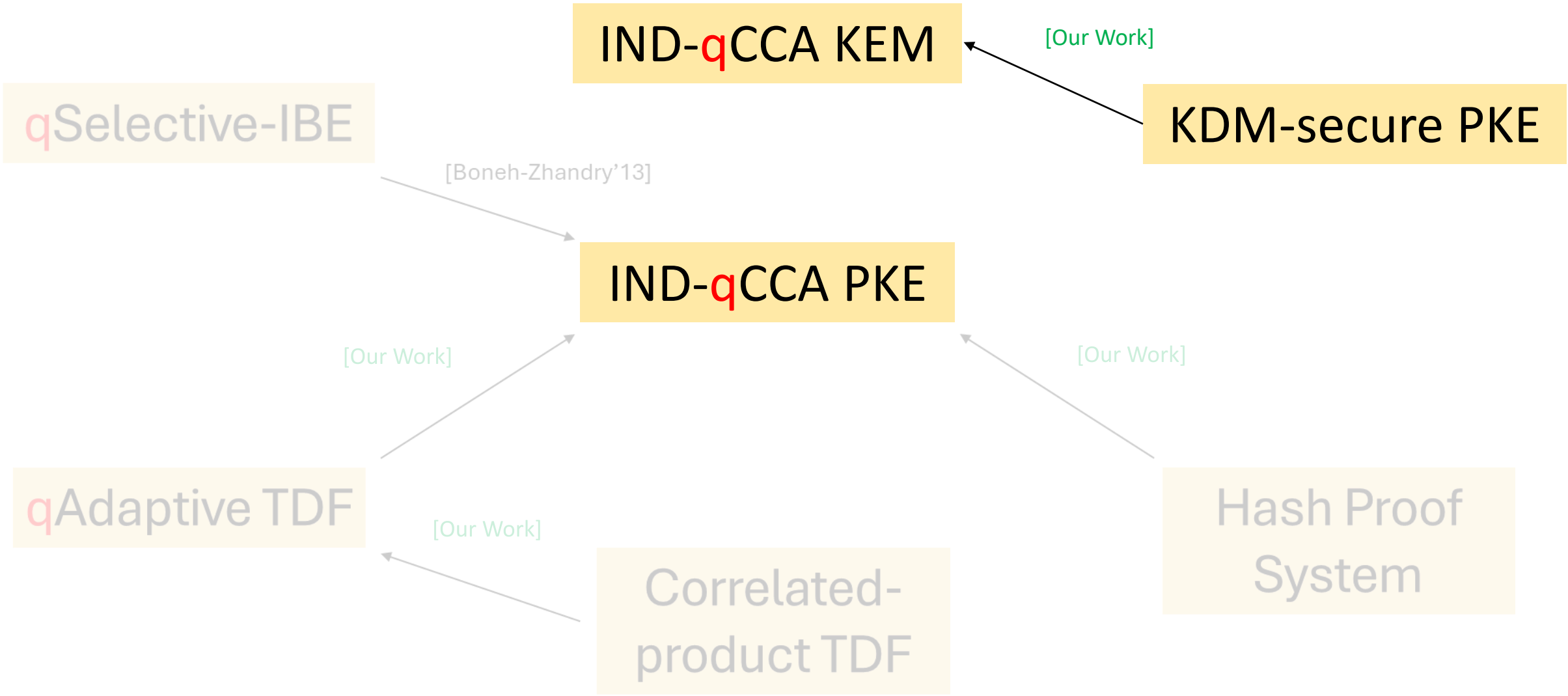
Overview: Results



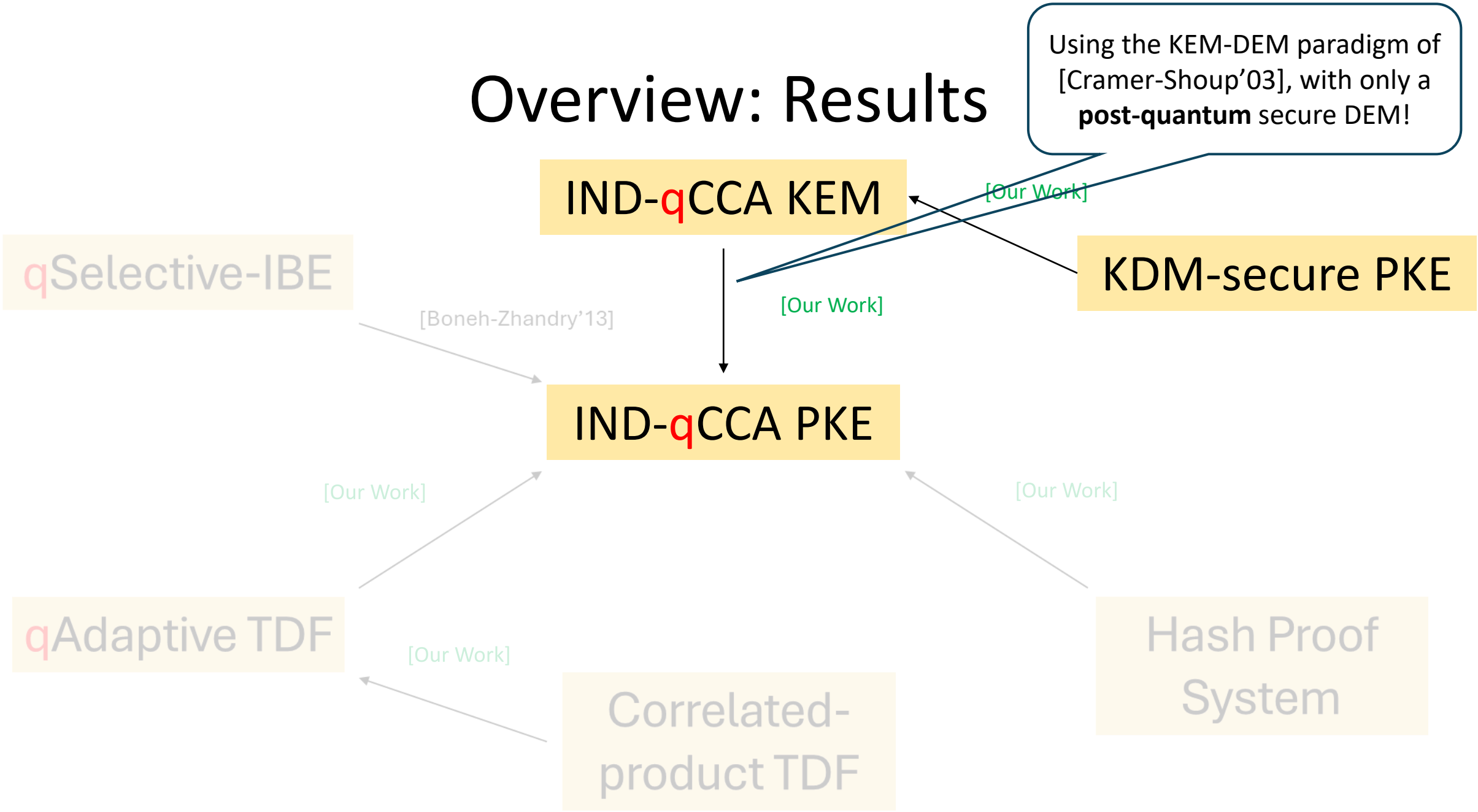
Overview: Results



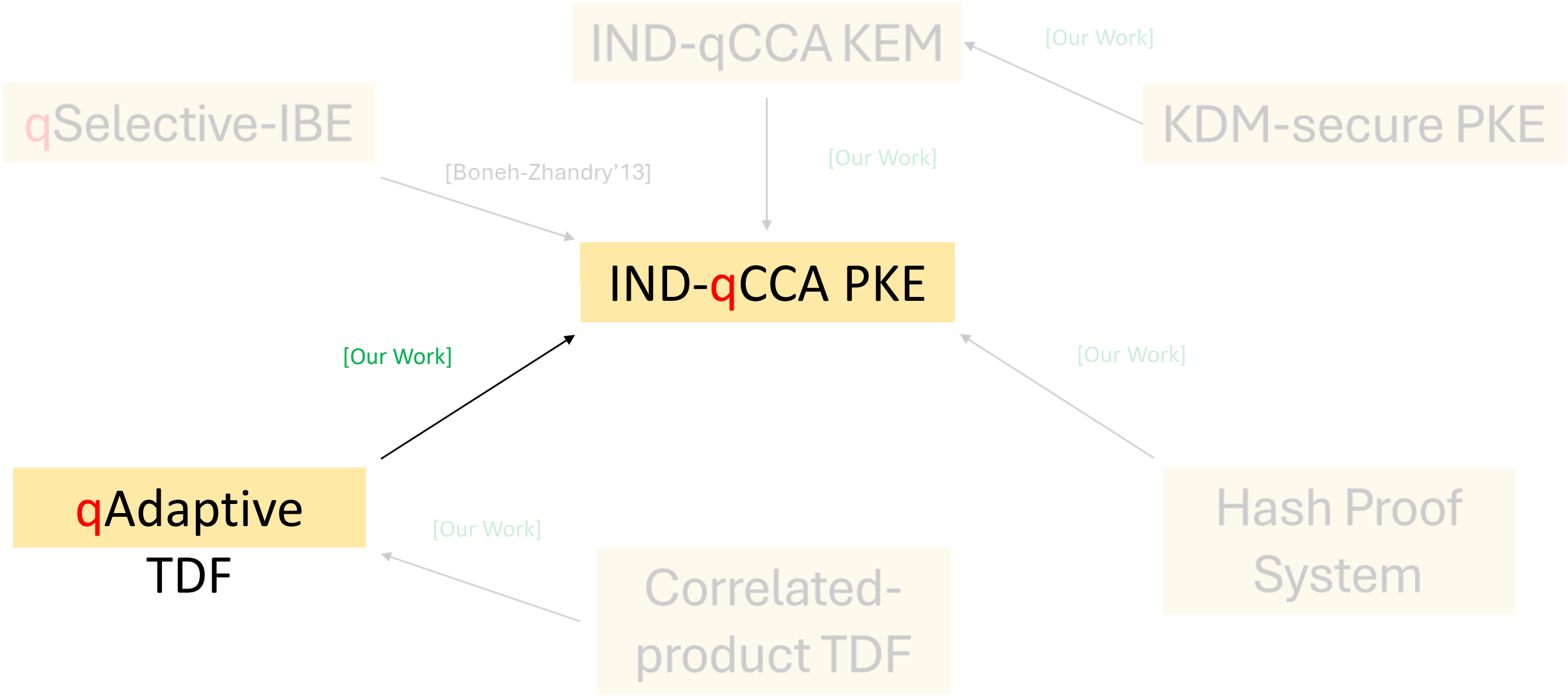
Overview: Results



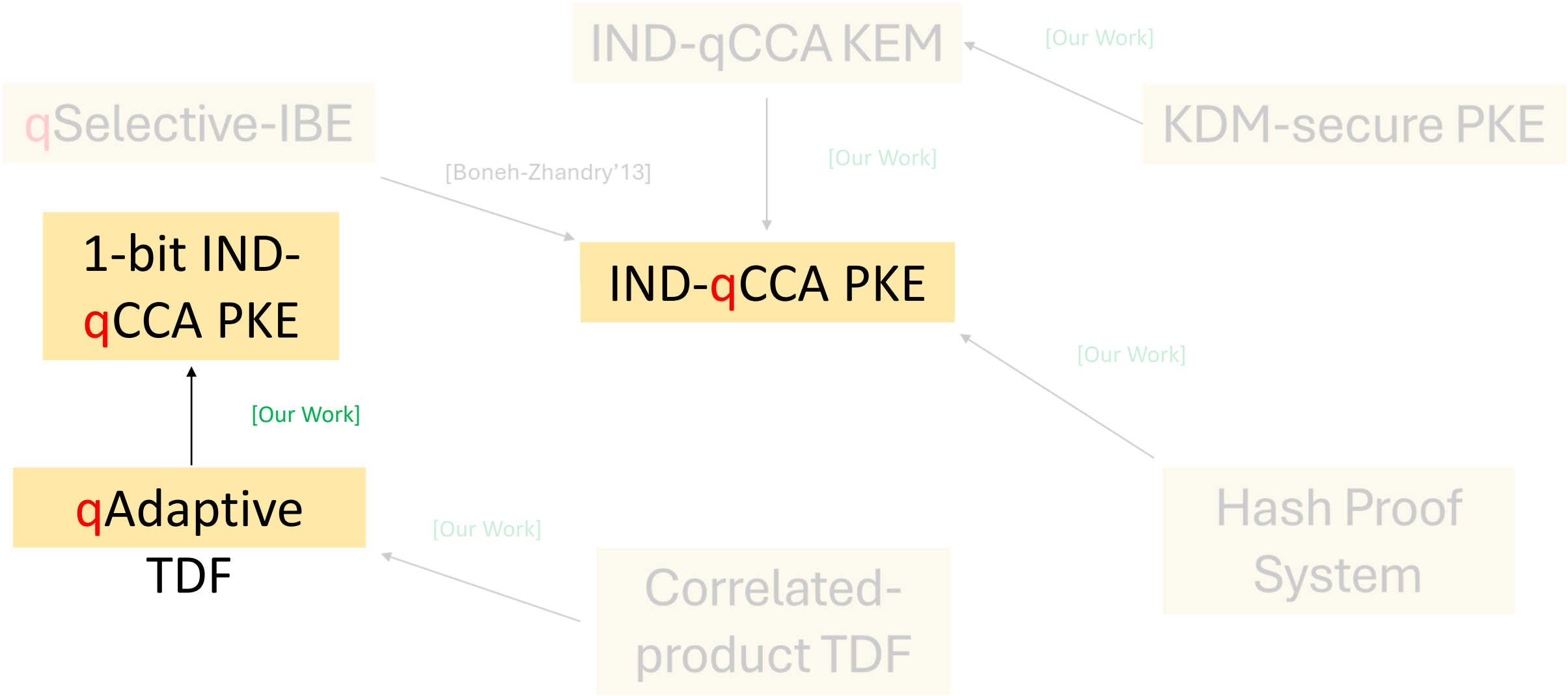
Overview: Results



Overview: Results

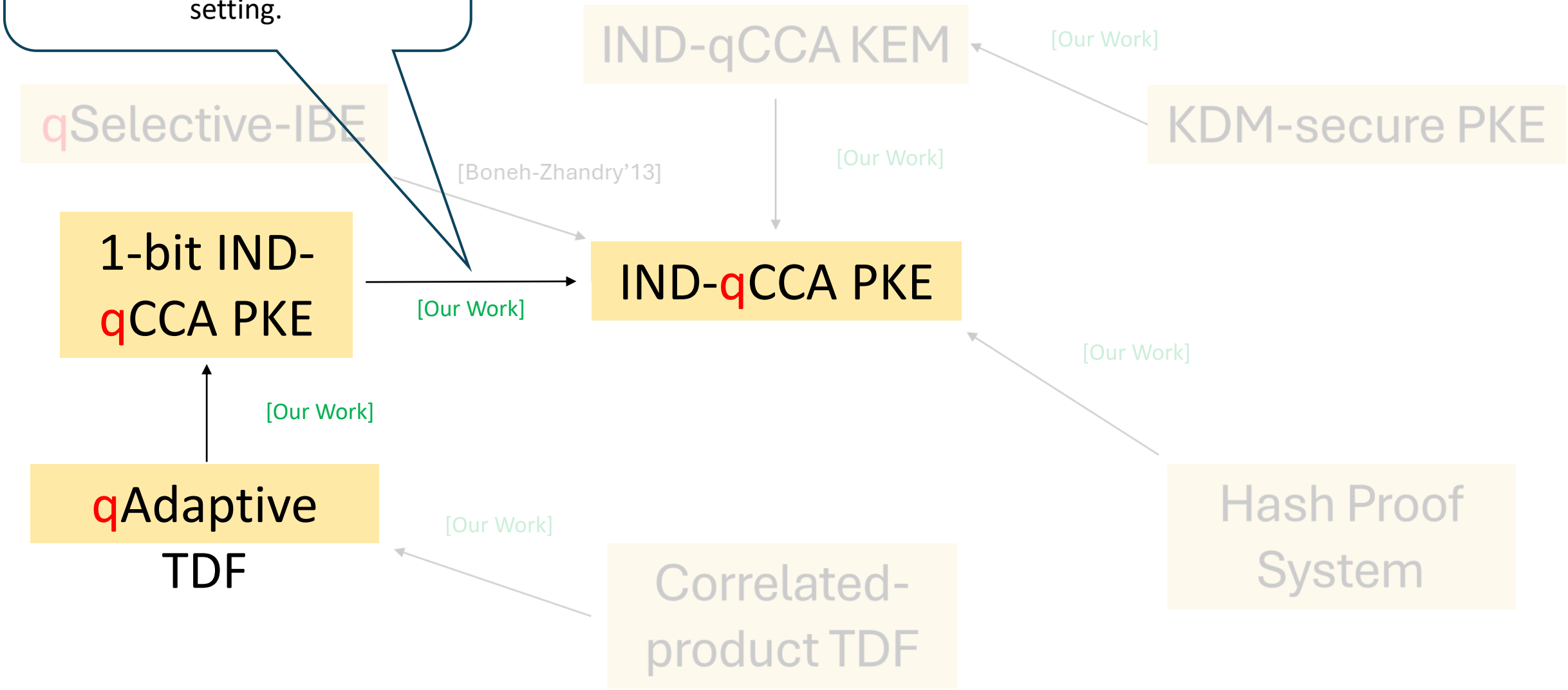


Overview: Results

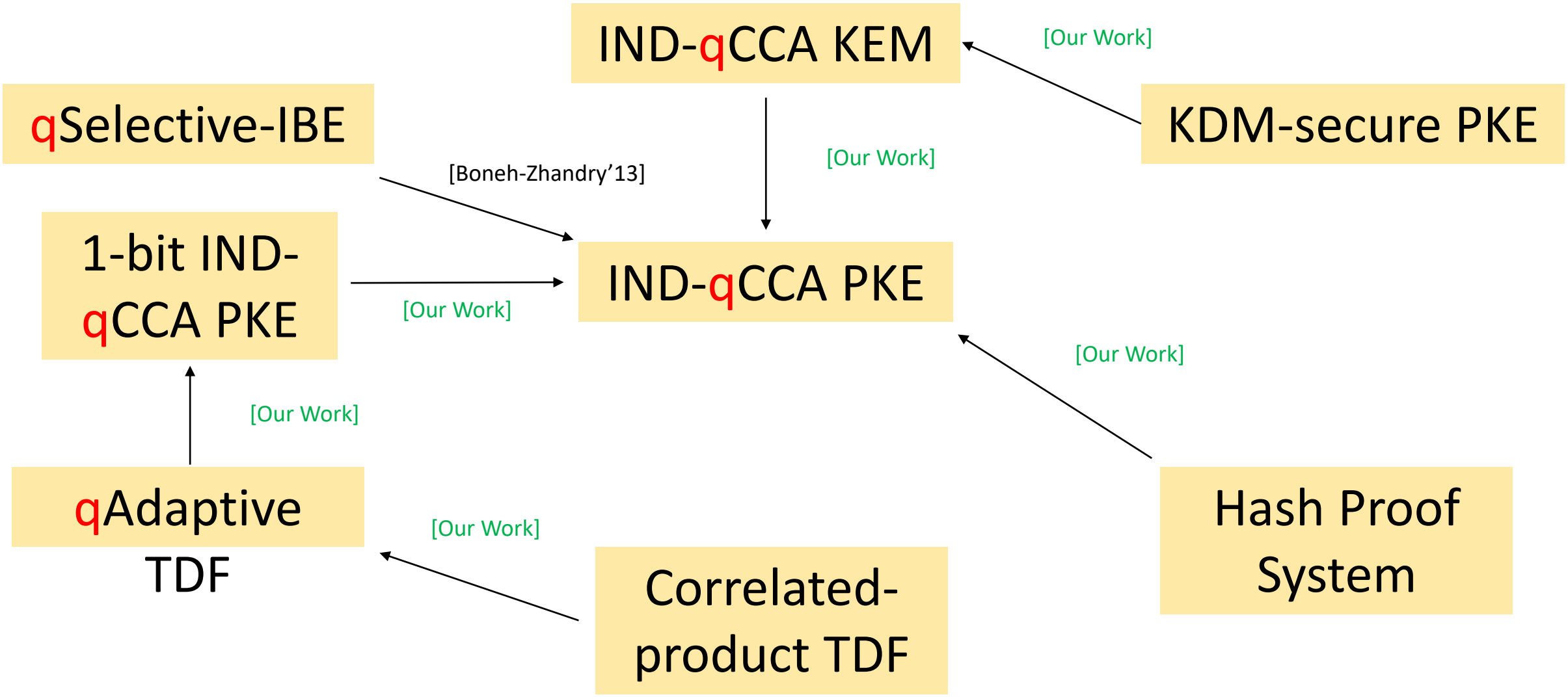


Overview: Results

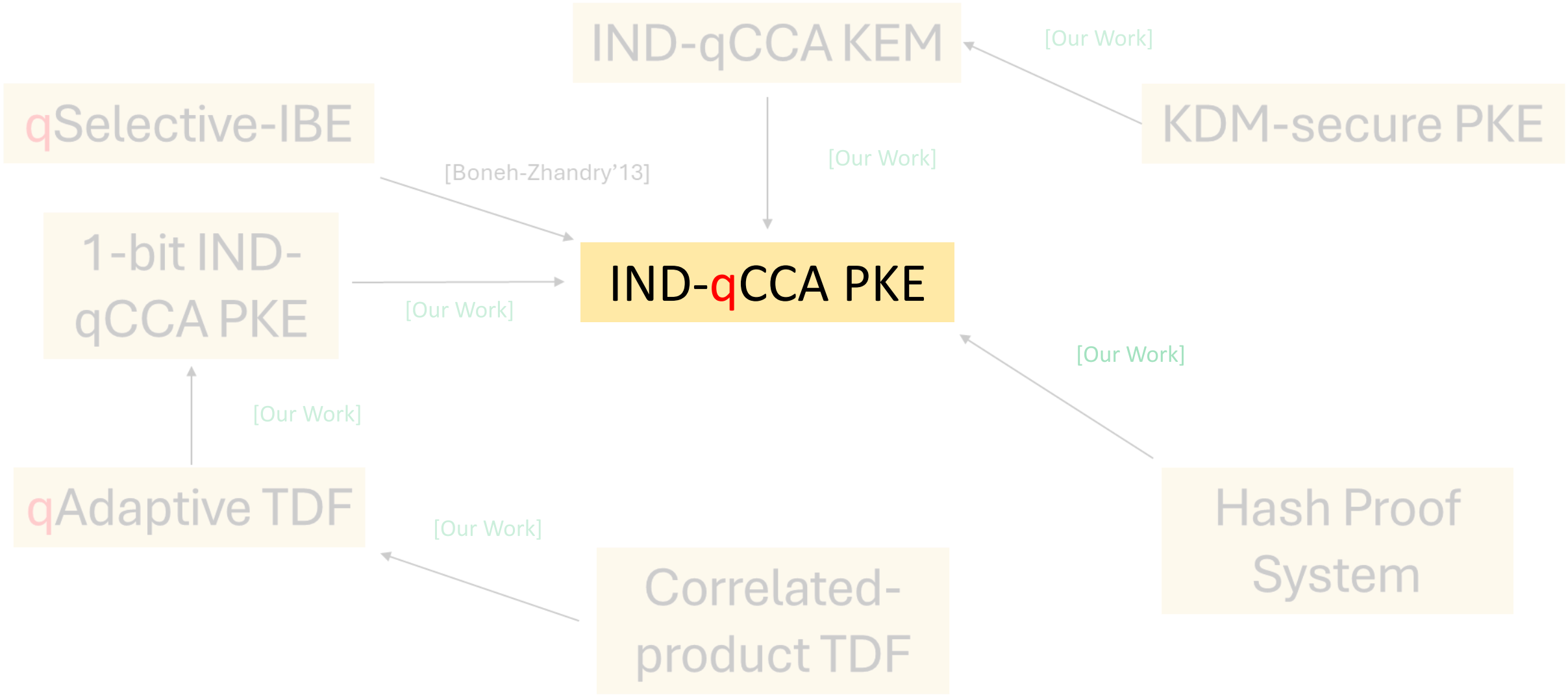
Extending **bit completeness** of CCA-secure PKE by [Hohenberger-Lewko-Waters'12] to the quantum setting.



Overview: Results



Overview: Results



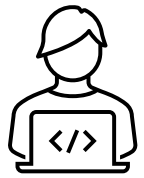
IND-qCCA Security

Introduced by [Boneh-Zhandry'13].

$PKE = (KGen, Enc, Dec)$

Alice

Bob



c

m

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

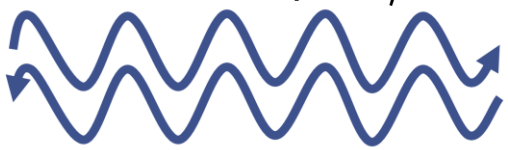
c

$m \leftarrow Dec(sk_{Bob}, c)$

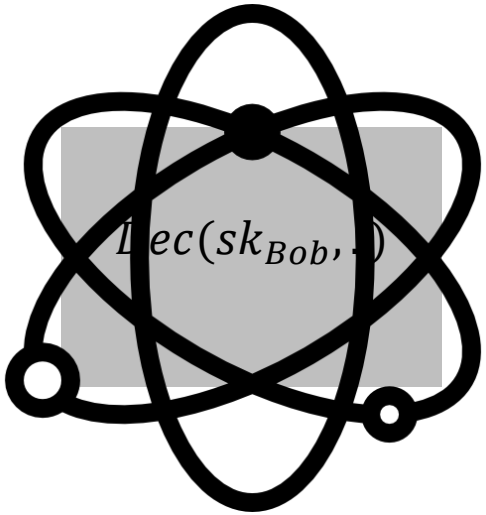
Eve

$m = ?$

$\alpha|c'\rangle + \beta|c''\rangle$



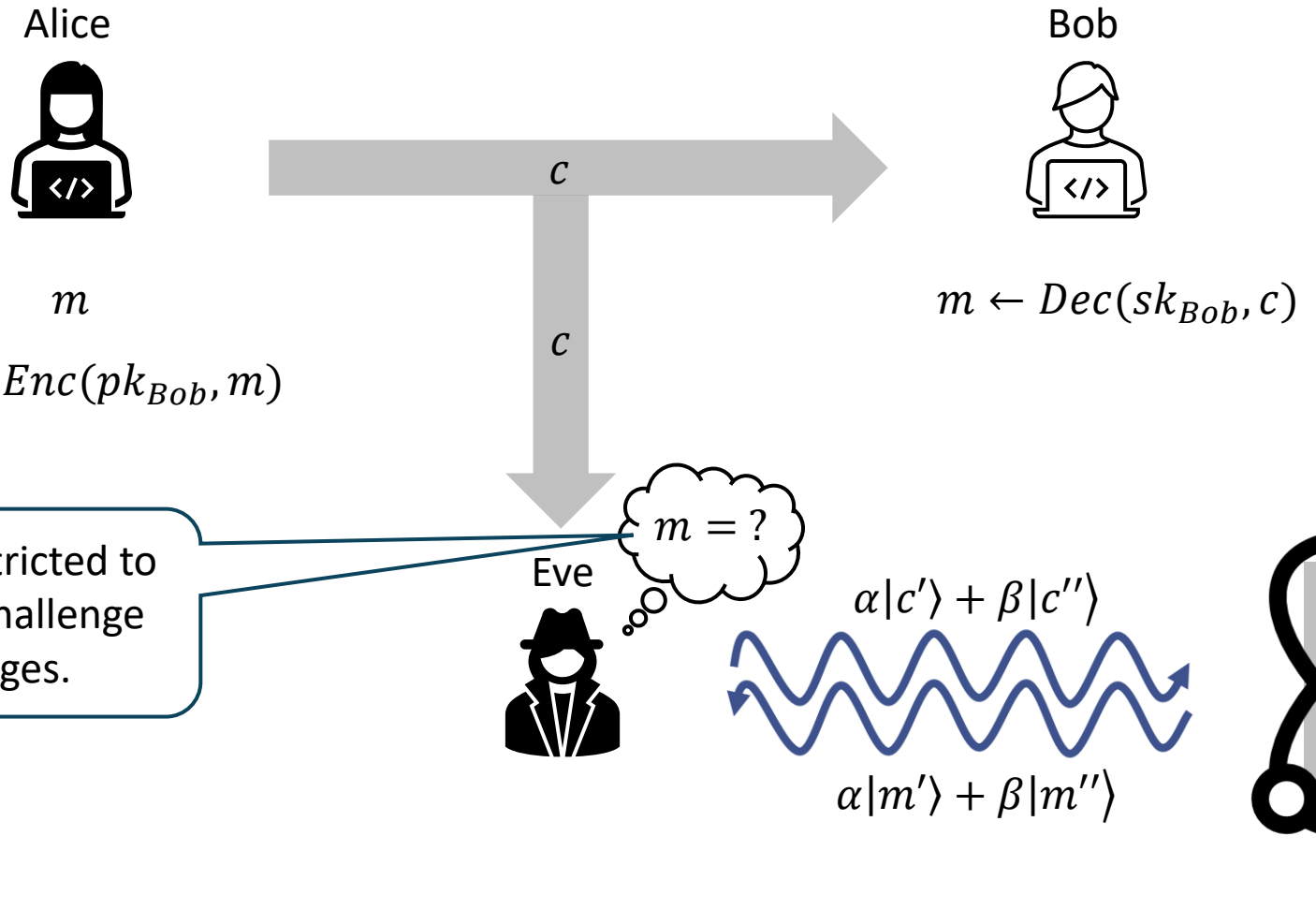
$\alpha|m'\rangle + \beta|m''\rangle$



IND-qCCA Security

Introduced by [Boneh-Zhandry'13].

$PKE = (KGen, Enc, Dec)$

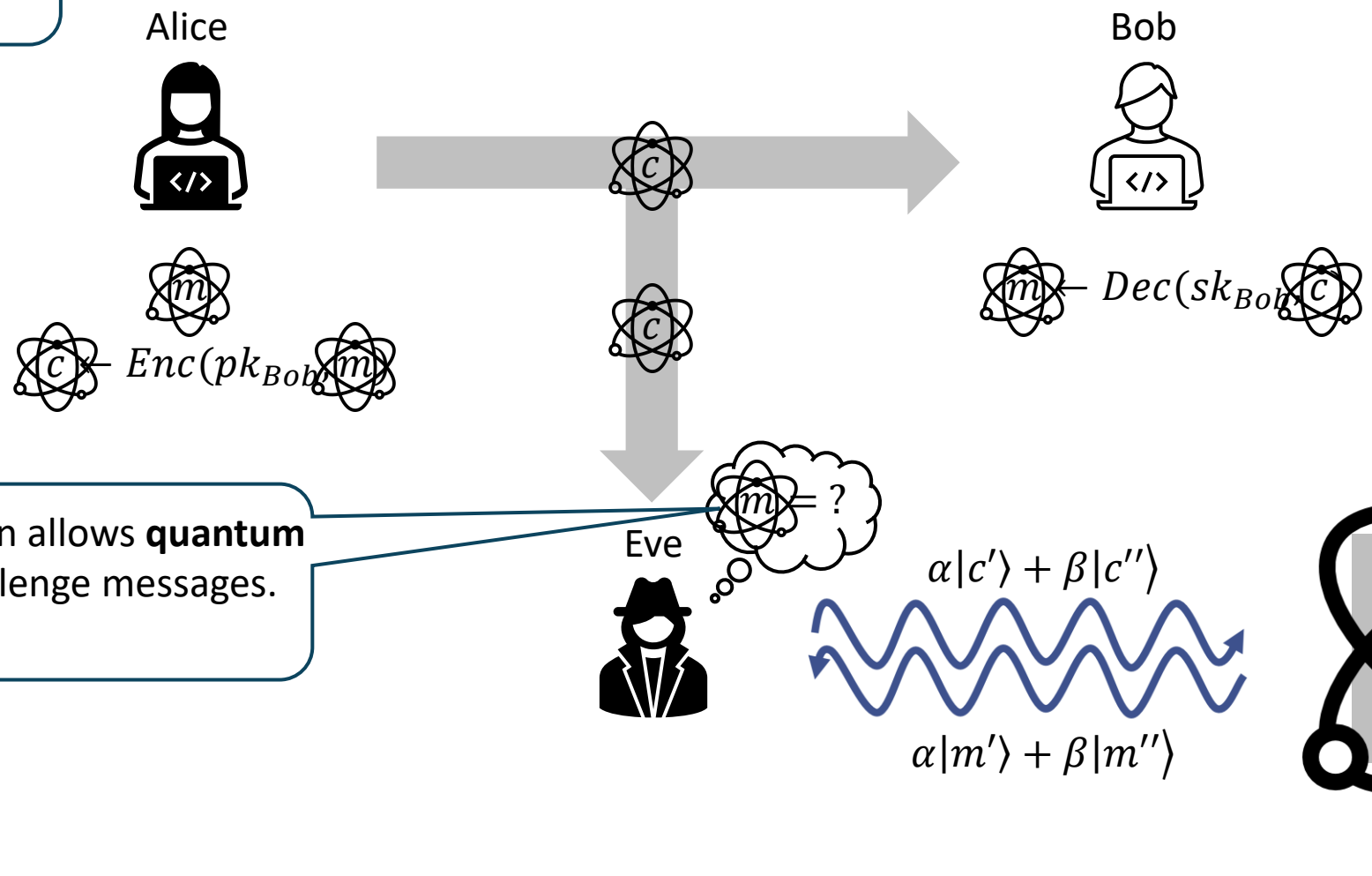


Notion restricted to **classical** challenge messages.

qIND-qCCA Security

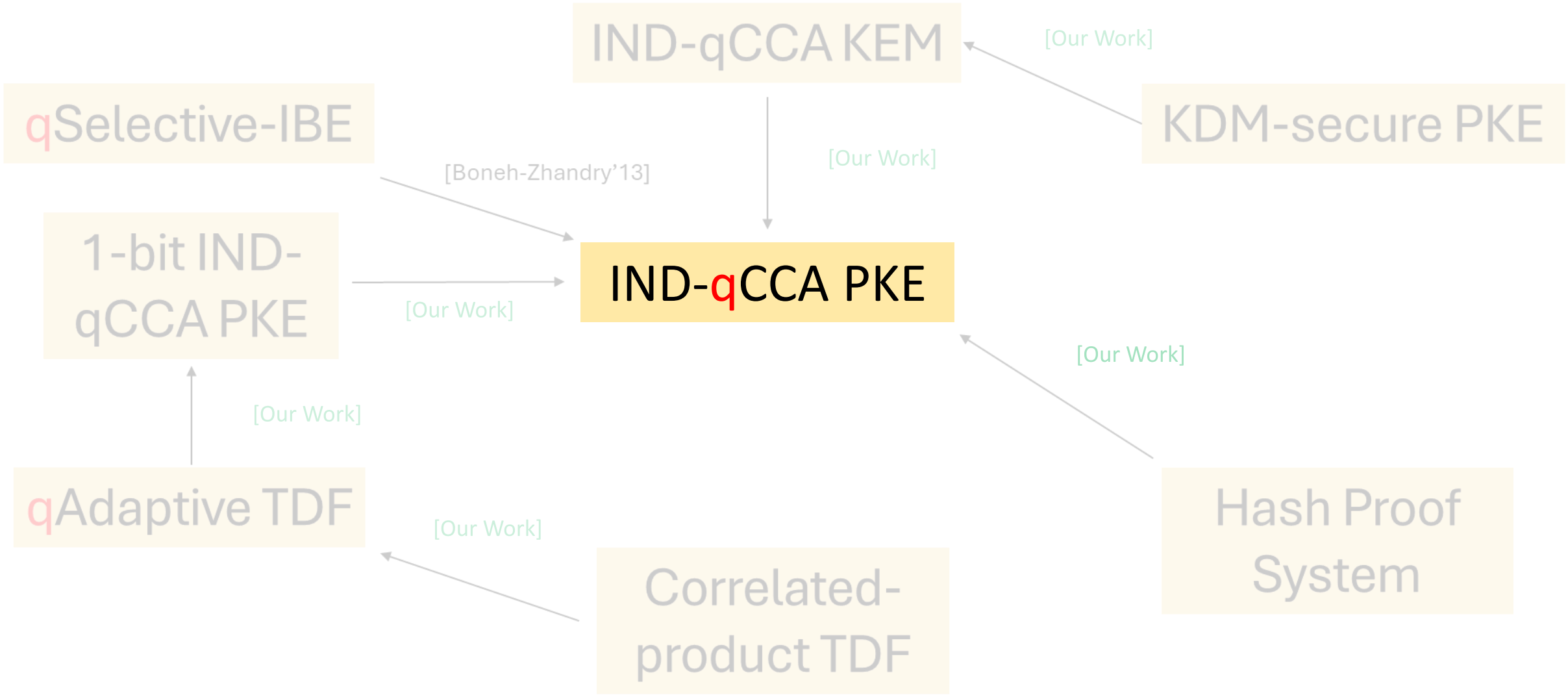
Introduced by [Chevalier-Ebrahimi-Vu'22].

$PKE = (KGen, Enc, Dec)$

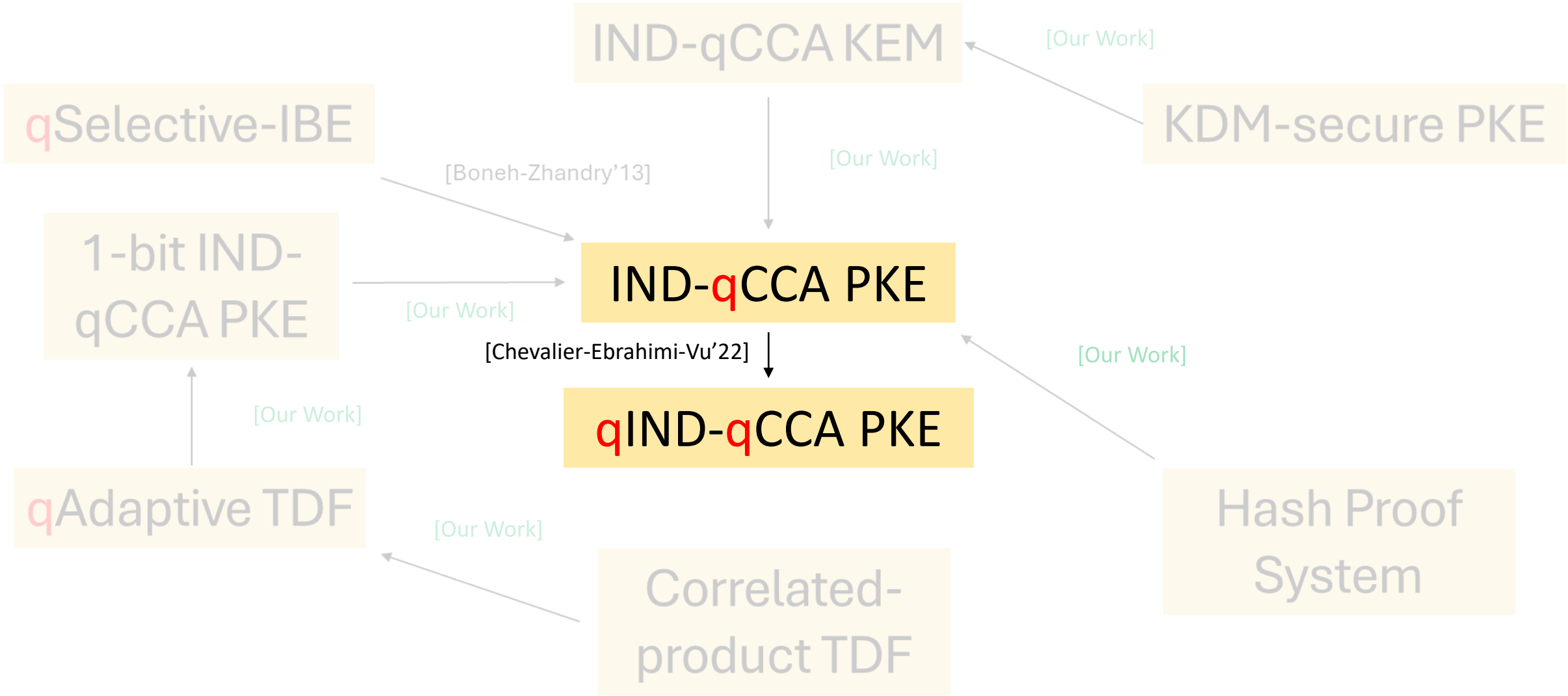


Notion allows **quantum** challenge messages.

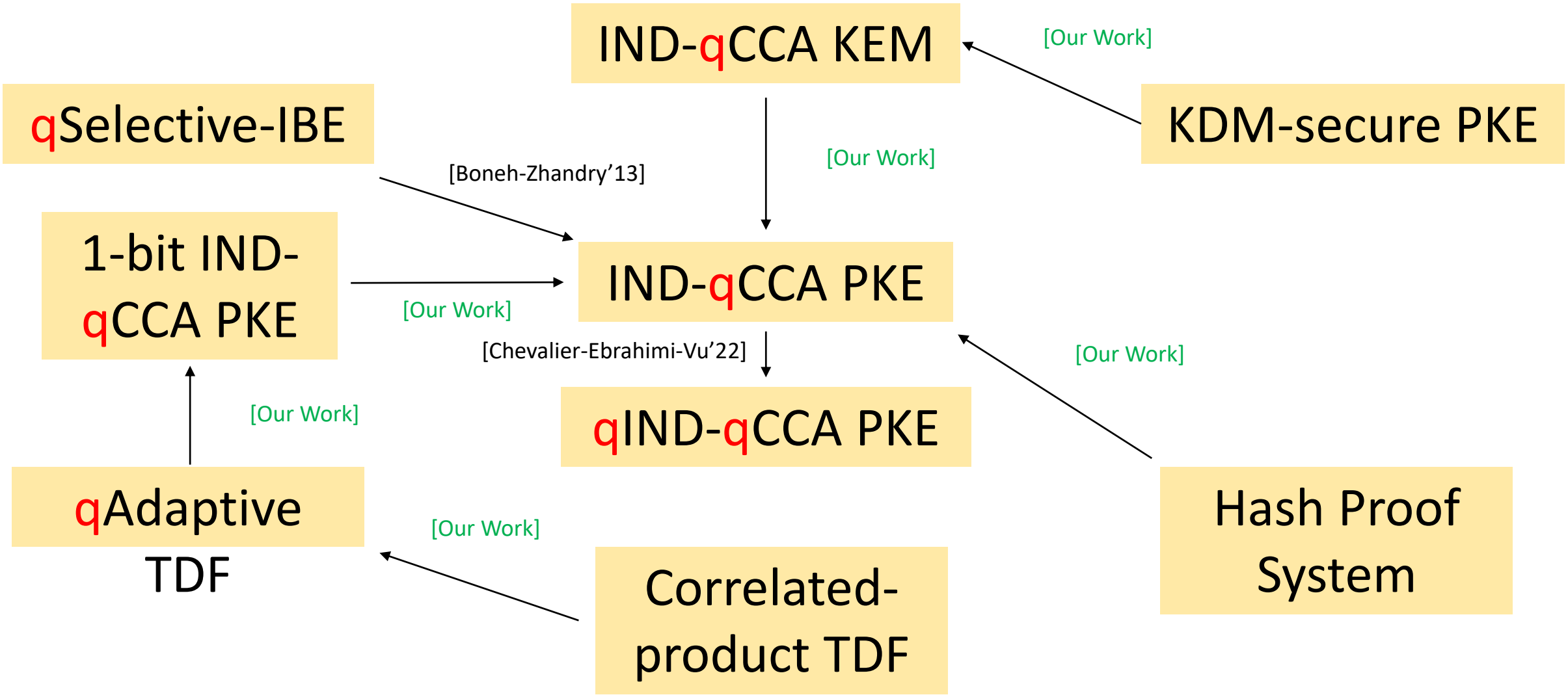
Overview: Results



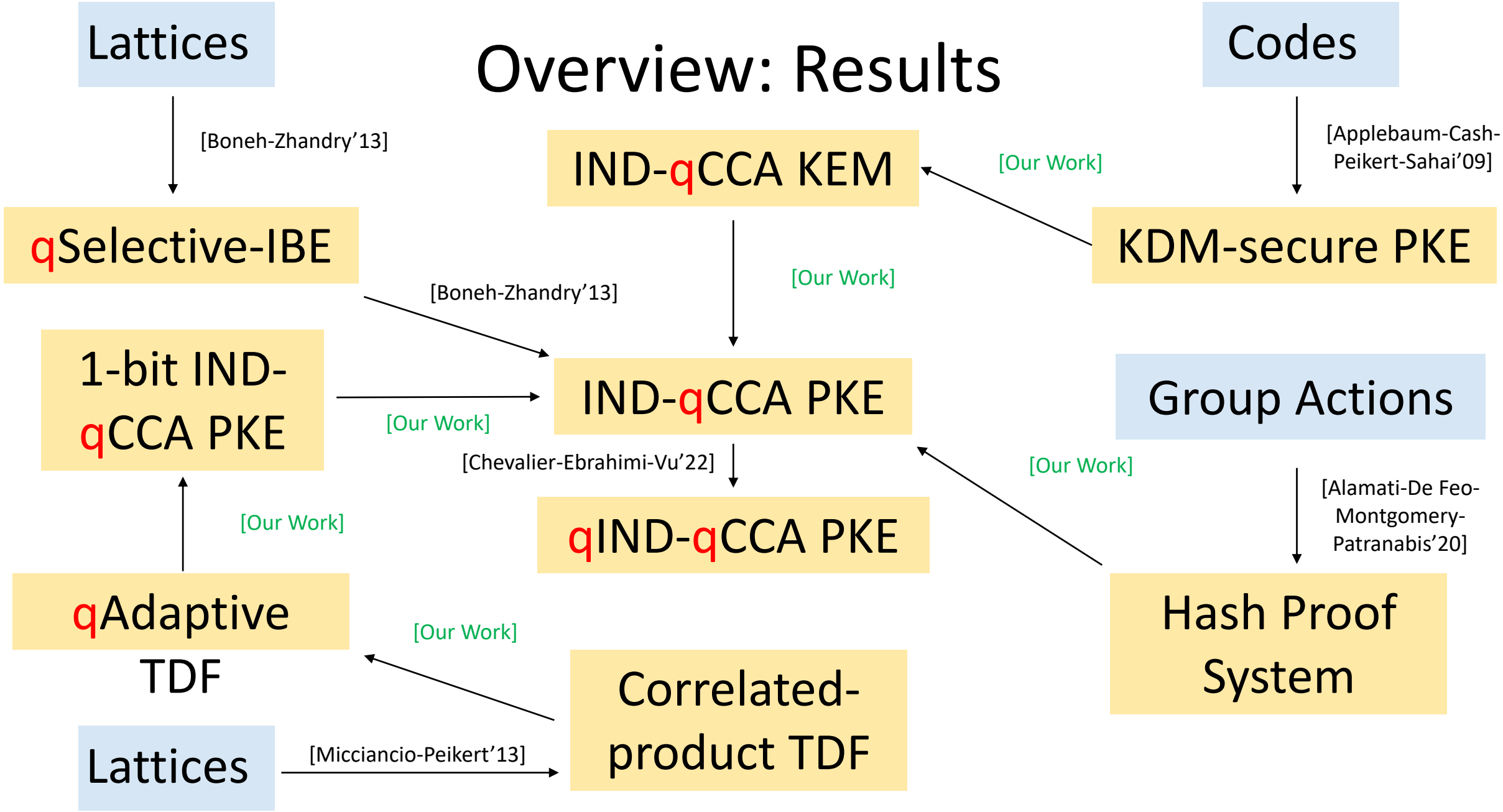
Overview: Results



Overview: Results



Overview: Results



Overview: Results

All our analyzed PKE constructions are **classical**.

Overview: Results

All our analyzed PKE constructions are **classical**.

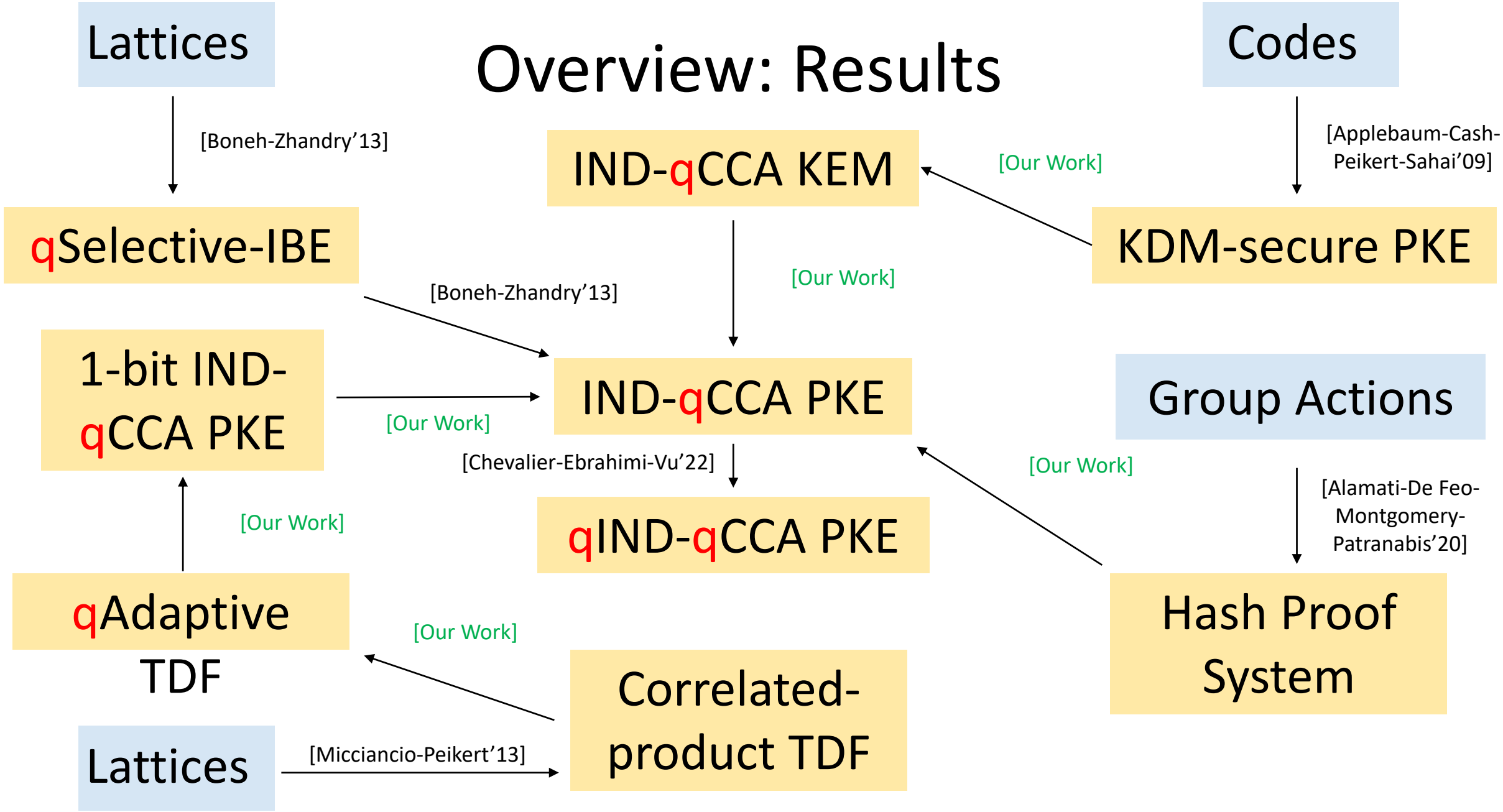
- They can be implemented on **classical computers**.

Overview: Results

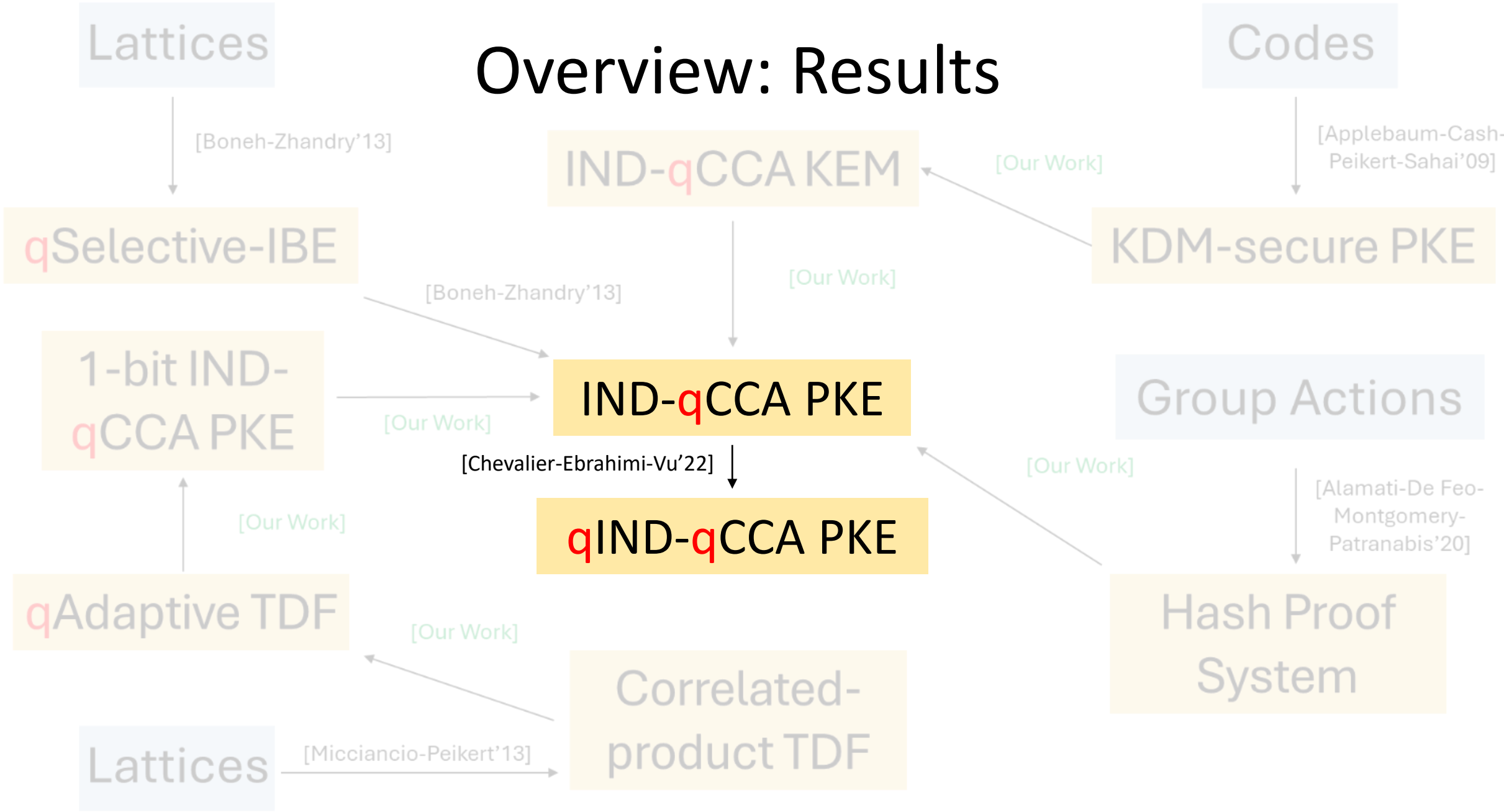
All our analyzed PKE constructions are **classical**.

- They can be implemented on **classical computers**.
- As opposed to **quantum PKE schemes** (e.g., in [Barooti-Grilo-Huguenin(-)Dumittan-Malavolta-Sattath-Vu-Walter'23]) which need inherent quantum components, such as **quantum public keys**.

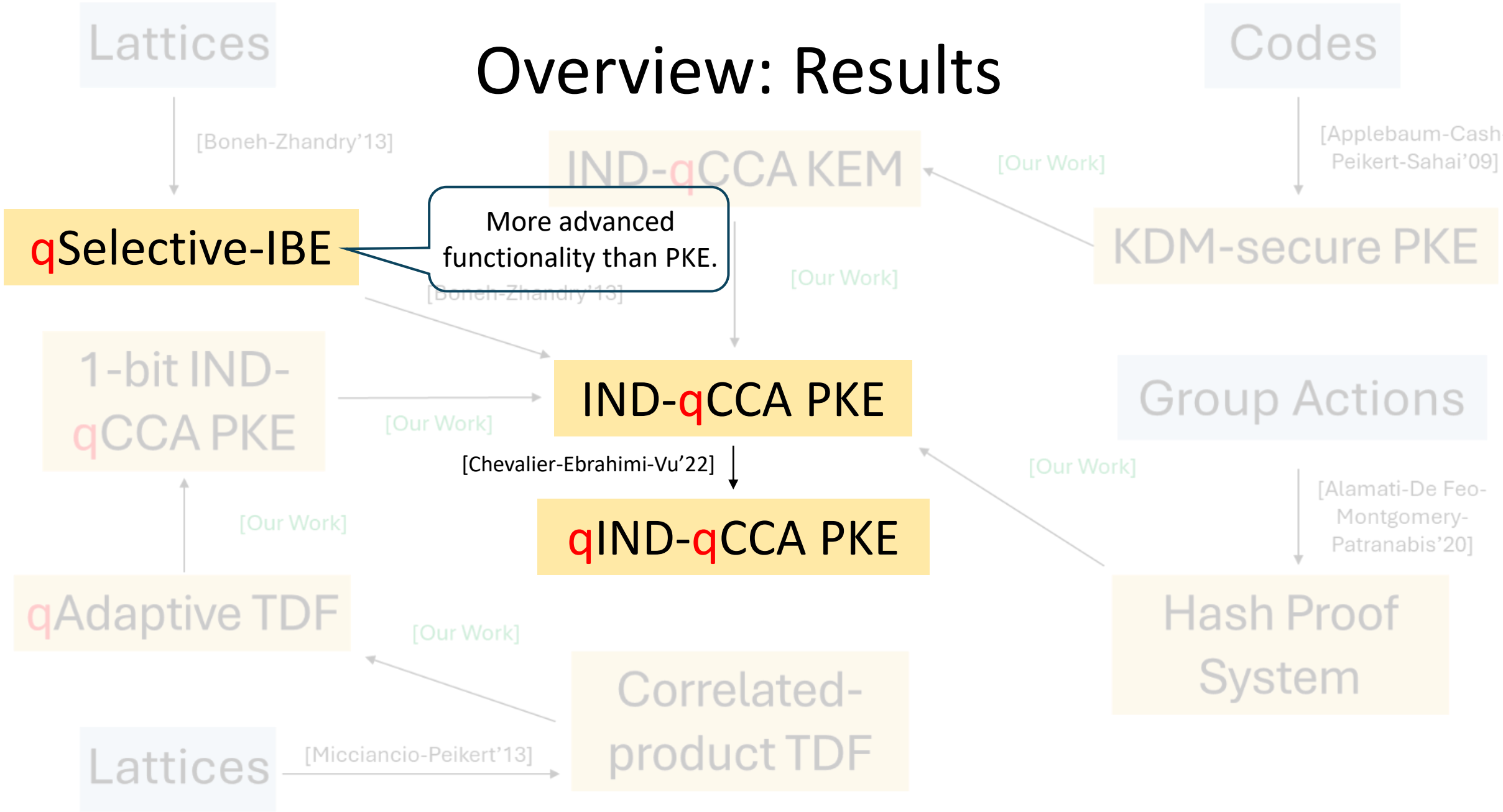
Overview: Results



Overview: Results



Overview: Results



PKE

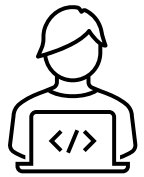
$PKE = (KGen, Enc, Dec)$

Alice

(pk_{Bob}, sk_{Bob})

c

Bob



m

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

$m \leftarrow Dec(sk_{Bob}, c)$

ABE

Attribute-**B**ased **E**ncryption.

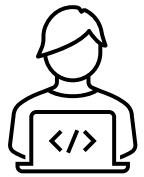
$ABE = (KGen, Enc, Dec, SKGen)$

Alice

(mpk, msk)

c

Bob



$m, attr$

$c \leftarrow Enc(mpk, m, attr)$

ABE

Attribute-**B**ased **E**ncryption.

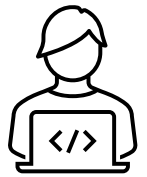
$ABE = (KGen, Enc, Dec, SKGen)$

Alice

(mpk, msk)

c

Bob



msk

$m, attr$

$c \leftarrow Enc(mpk, m, attr)$

ABE

Attribute-**B**ased **E**ncryption.

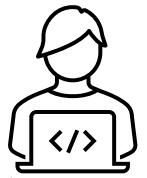
$ABE = (KGen, Enc, Dec, SKGen)$

Alice

(mpk, msk)

Bob

c



$m, attr$

$c \leftarrow Enc(mpk, m, attr)$

msk

$sk \leftarrow SKGen(msk, pred)$

"predicate"

ABE

Attribute-**B**ased **E**ncryption.

$ABE = (KGen, Enc, Dec, SKGen)$

(mpk, msk)

Alice

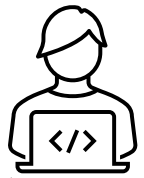
$m, attr$

$c \leftarrow Enc(mpk, m, attr)$

c

msk

Bob



$sk \leftarrow SKGen(msk, pred)$

"predicate"

$m \leftarrow Dec(sk, c)$ *if* $pred(attr) = 1$

ABE

Attribute-**B**ased **E**ncryption.

$ABE = (KGen, Enc, Dec, SKGen)$

(mpk, msk)

Alice

$m, attr$

$c \leftarrow Enc(mpk, m, attr)$

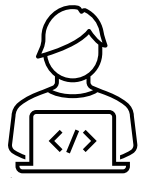
c

msk

$sk \leftarrow SKGen(msk, pred)$

"predicate"

Bob



$m \leftarrow Dec(sk, c)$ if $pred(attr) = 1$

$\perp \leftarrow Dec(sk, c)$ if $pred(attr) = 0$

ABE

Attribute-**B**ased **E**ncryption.

$ABE = (KGen, Enc, Dec, SKGen)$

(mpk, msk)

Alice

Bob

c

$m, attr$

$c \leftarrow Enc(mpk, m, attr)$

"Bob"

msk

$sk \leftarrow SKGen(msk, pred)$

$m \leftarrow Dec(sk, c)$ *if* $pred(attr) = 1$

$\perp \leftarrow Dec(sk, c)$ *if* $pred(attr) = 0$

$pred(\text{"Bob"}) = 1$

$pred(\cdot) = 0, otherwise$

ABE

Attribute-**B**ased **E**ncryption.

$ABE = (KGen, Enc, Dec, SKGen)$

(mpk, msk)

Alice

Bob

c

$m, attr$

$c \leftarrow Enc(mpk, m, attr)$

"Dave"

msk

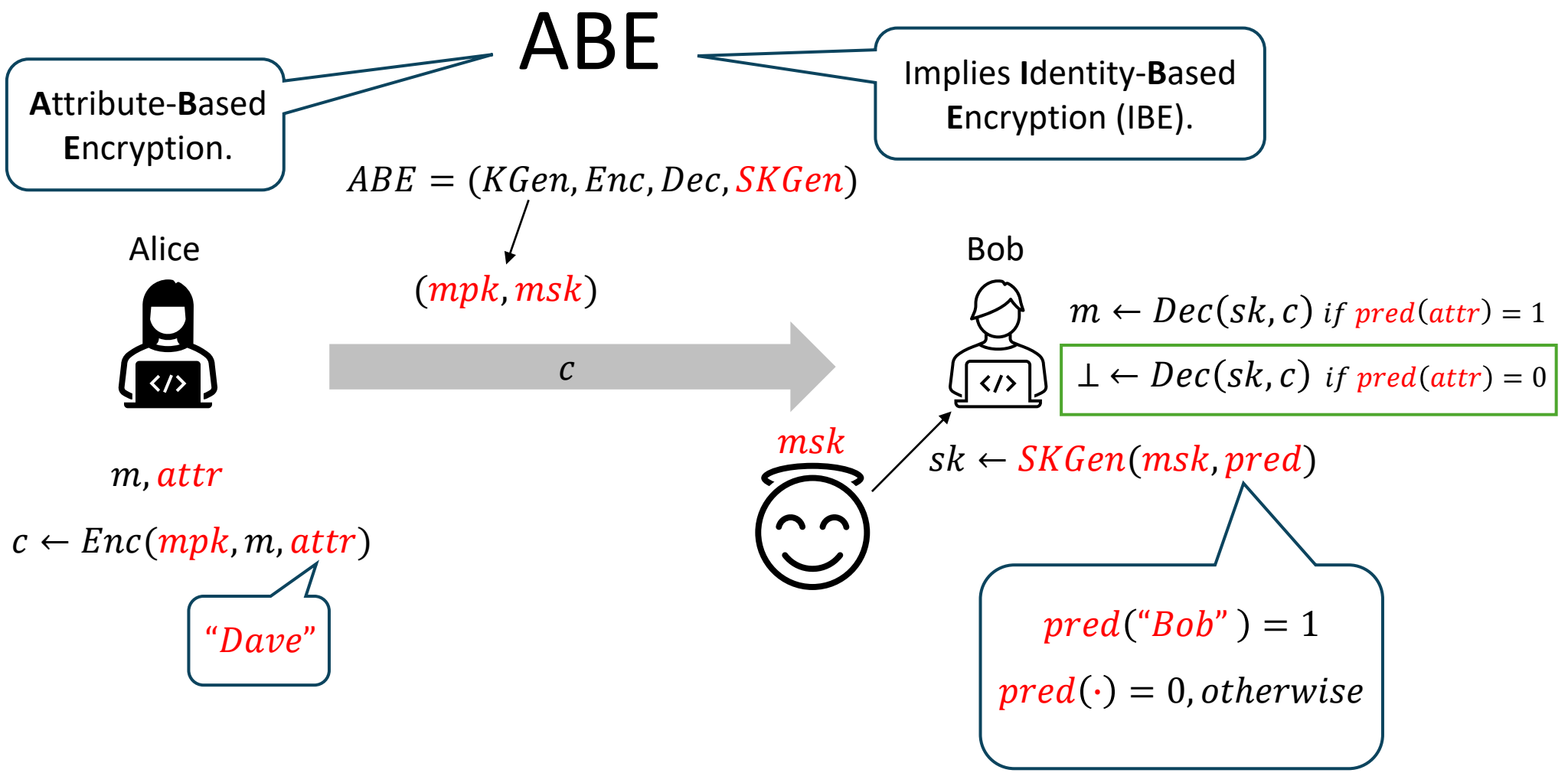
$sk \leftarrow SKGen(msk, pred)$

$m \leftarrow Dec(sk, c)$ *if* $pred(attr) = 1$

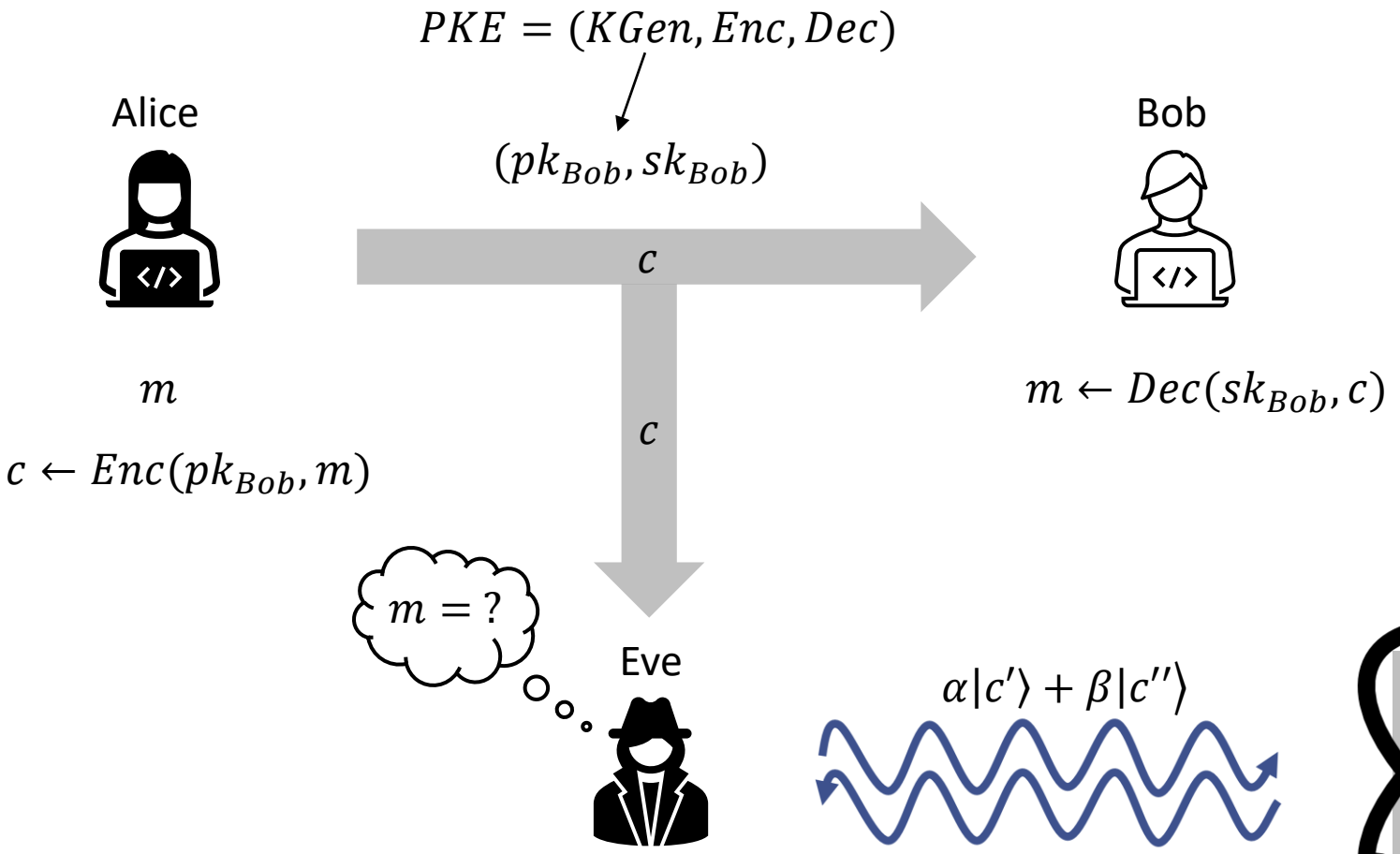
$\perp \leftarrow Dec(sk, c)$ *if* $pred(attr) = 0$

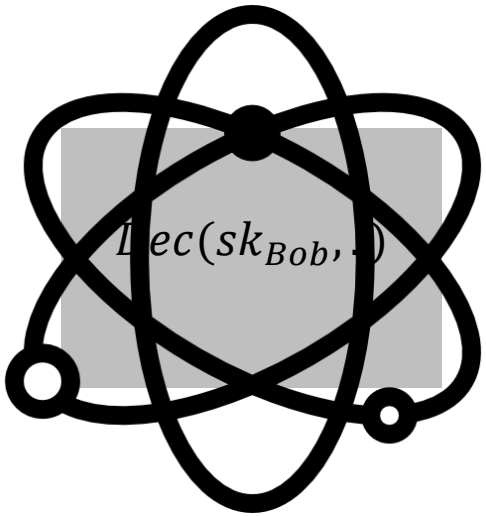
$pred(\text{“}Bob\text{”}) = 1$

$pred(\cdot) = 0, otherwise$

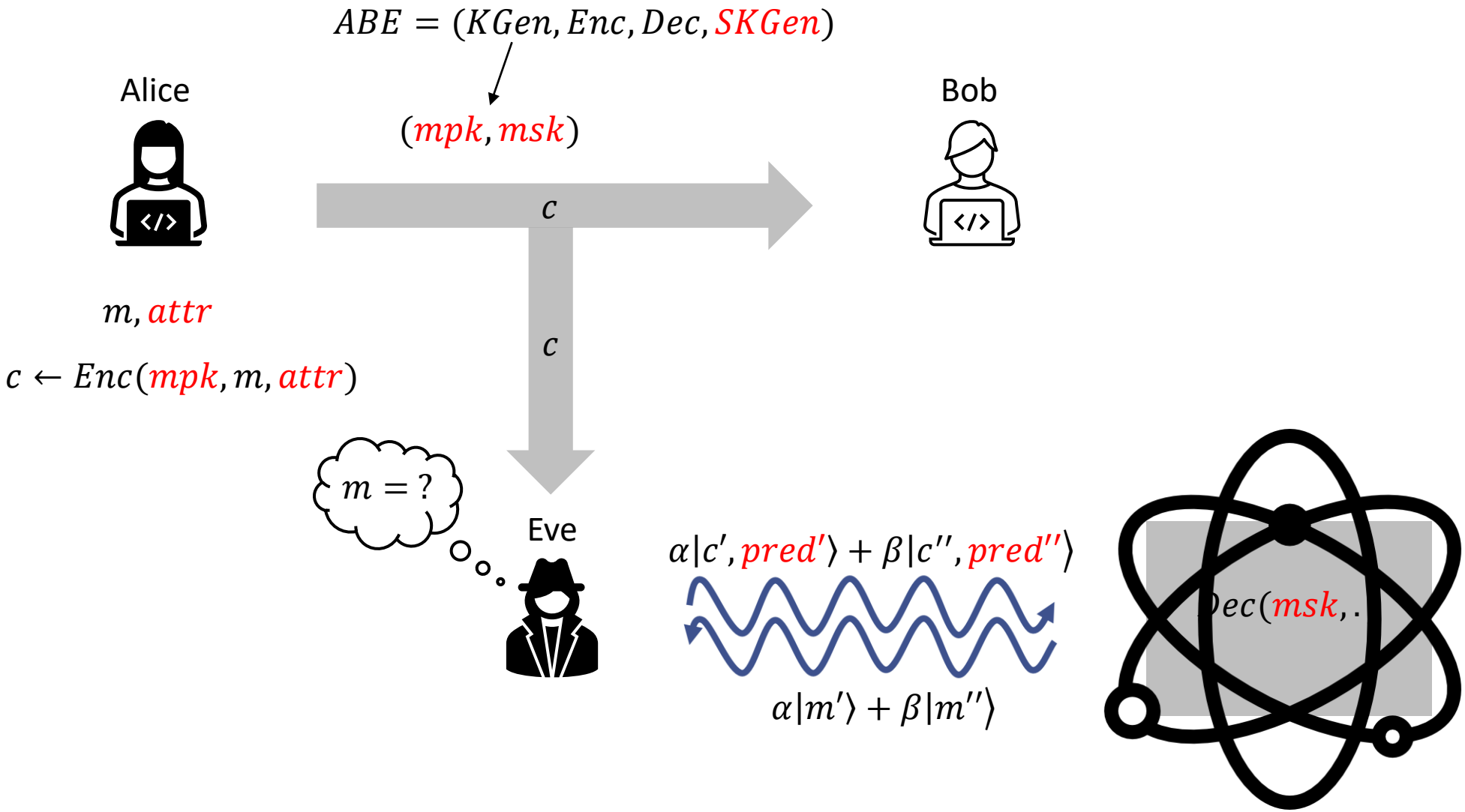

ABE
Attribute-Based Encryption.
Implies Identity-Based Encryption (IBE).
$ABE = (KGen, Enc, Dec, SKGen)$
(mpk, msk)
Alice
Bob
c
$m \leftarrow Dec(sk, c)$ if $pred(attr) = 1$
$\perp \leftarrow Dec(sk, c)$ if $pred(attr) = 0$
msk
$sk \leftarrow SKGen(msk, pred)$
$m, attr$
$c \leftarrow Enc(mpk, m, attr)$
"Dave"
$pred("Bob") = 1$
$pred(\cdot) = 0, otherwise$

IND-qCCA Secure PKE

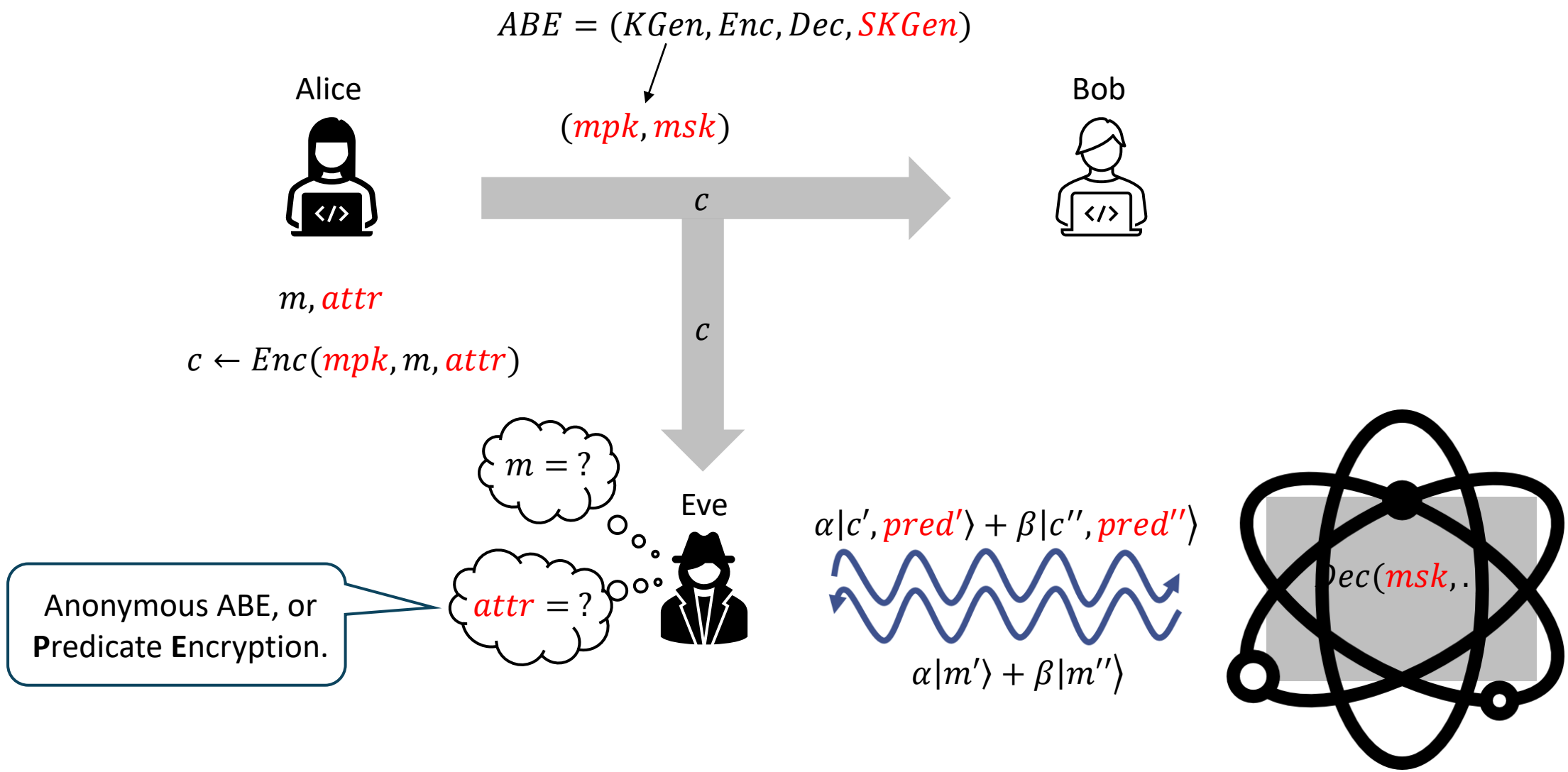




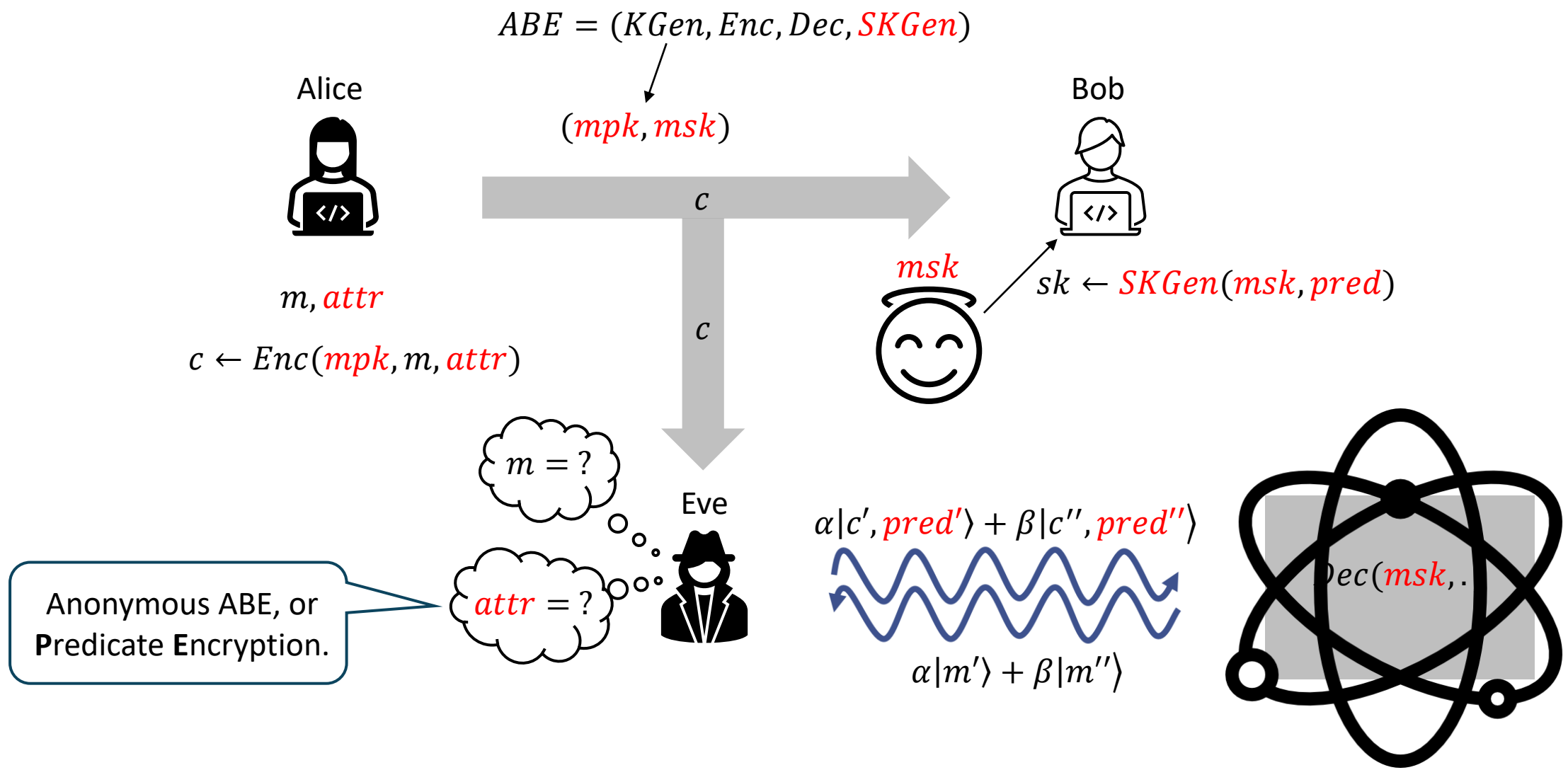
IND-qCCA Secure ABE



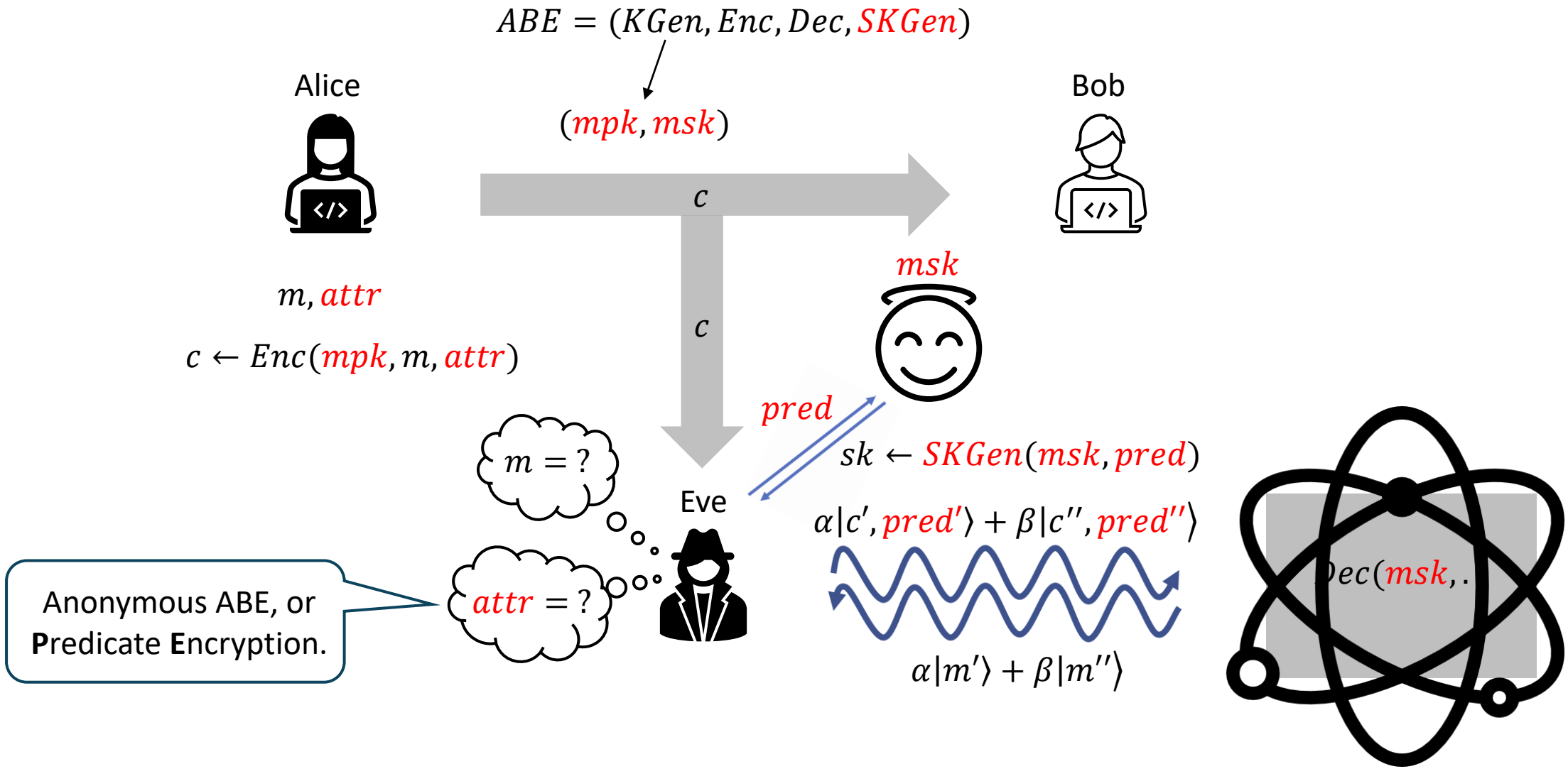
IND-qCCA Secure ABE



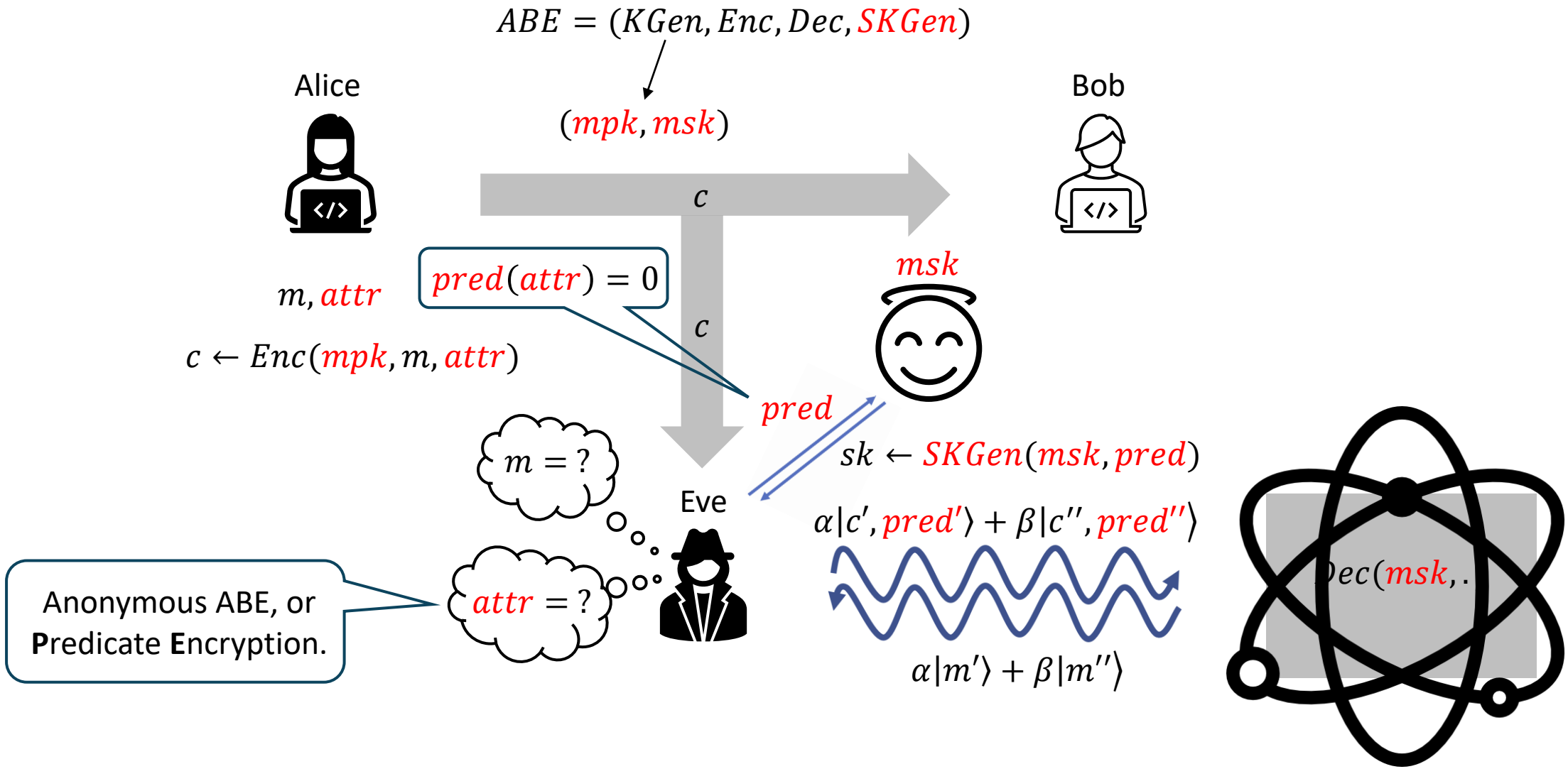
IND-qCCA Secure ABE



IND-qCCA Secure ABE



IND-qCCA Secure ABE



IND-qCCA-cKG Secure ABE

Adversary can only make "classical" $SKGen$ queries.

$ABE = (KGen, Enc, Dec, SKGen)$

(mpk, msk)

Alice

Bob

c

$m, attr$

$pred(attr) = 0$

msk

$c \leftarrow Enc(mpk, m, attr)$

$pred$

$sk \leftarrow SKGen(msk, pred)$

$m = ?$

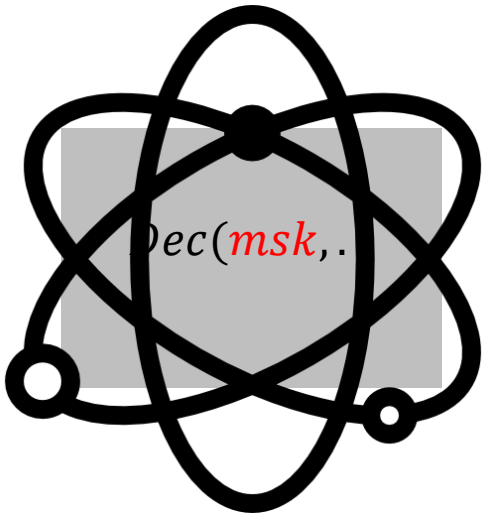
Eve

$attr = ?$

$\alpha|c', pred'\rangle + \beta|c'', pred''\rangle$

$\alpha|m'\rangle + \beta|m''\rangle$

Anonymous ABE, or **P**redicate **E**ncryption.



IND-qCCA-cKG Secure ABE

Adversary can only make "classical" $SKGen$ queries.

"Quantum" $SKGen$ queries come with definitional issues…

$ABE = (KGen, Enc, Dec, SKGen)$

(mpk, msk)

Alice

Bob

c

$m, attr$

$pred(attr) = 0$

msk

$c \leftarrow Enc(mpk, m, attr)$

c

$pred$

$sk \leftarrow SKGen(msk, pred)$

$m = ?$

Eve

$attr = ?$

$\alpha|c', pred'\rangle + \beta|c'', pred''\rangle$

$\alpha|m'\rangle + \beta|m''\rangle$

$Dec(msk, .$

Anonymous ABE, or **P**redicate **E**ncryption.

IND-qCCA-cKG Secure ABE

Adversary can only make "classical" $SKGen$ queries.

"Quantum" $SKGen$ queries come with definitional issues…

… but can be salvaged in a "semi-adaptive" setting.

$ABE = (KGen, Enc, Dec, SKGen)$

(mpk, msk)

Alice

Bob

c

$m, attr$

$pred(attr) = 0$

$c \leftarrow Enc(mpk, m, attr)$

msk

$pred$

$sk \leftarrow SKGen(msk, pred)$

$m = ?$

$attr = ?$

Eve

$\alpha|c', pred'\rangle + \beta|c'', pred''\rangle$

$\alpha|m'\rangle + \beta|m''\rangle$

$Dec(msk, .$

Anonymous ABE, or **P**redicate **E**ncryption.

IND-qCCA-cKG Secure ABE

IND-CPA(-cKG) ABE

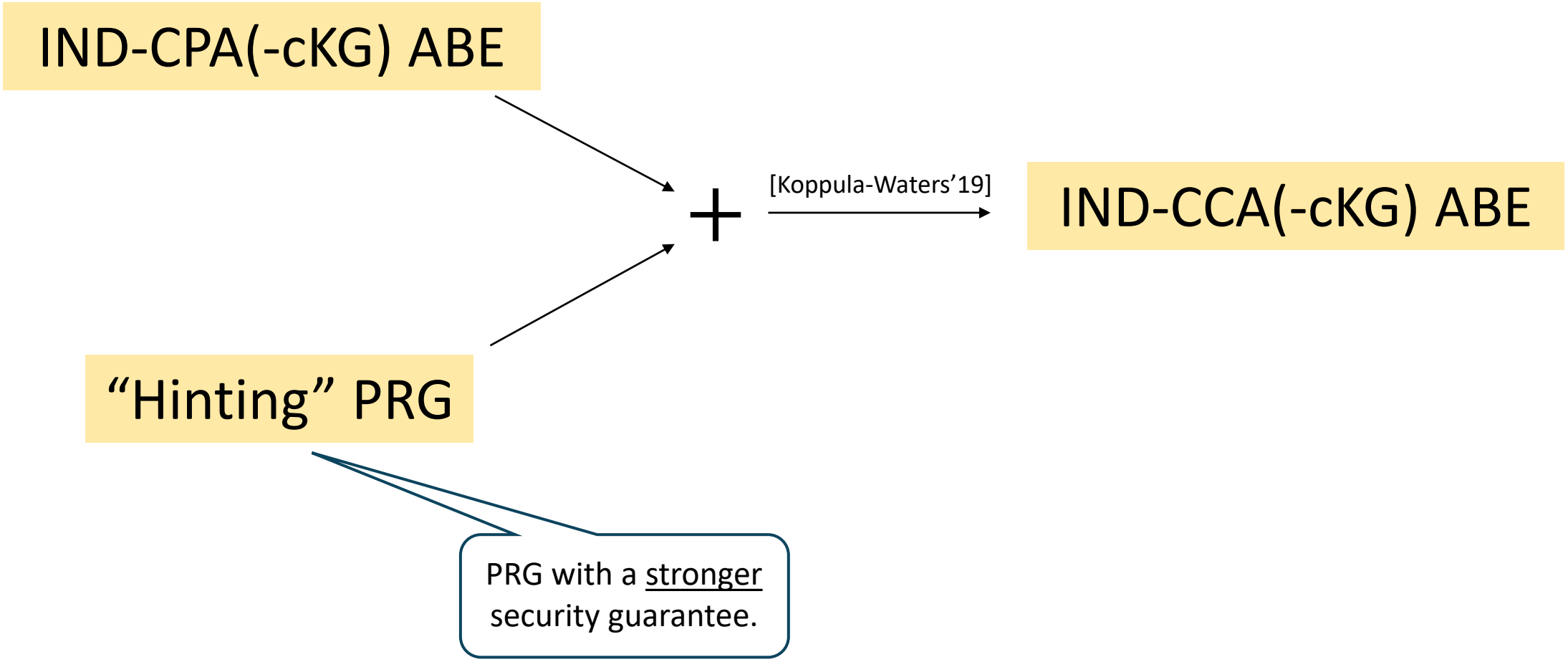
IND-qCCA-cKG Secure ABE

IND-CPA(-cKG) ABE

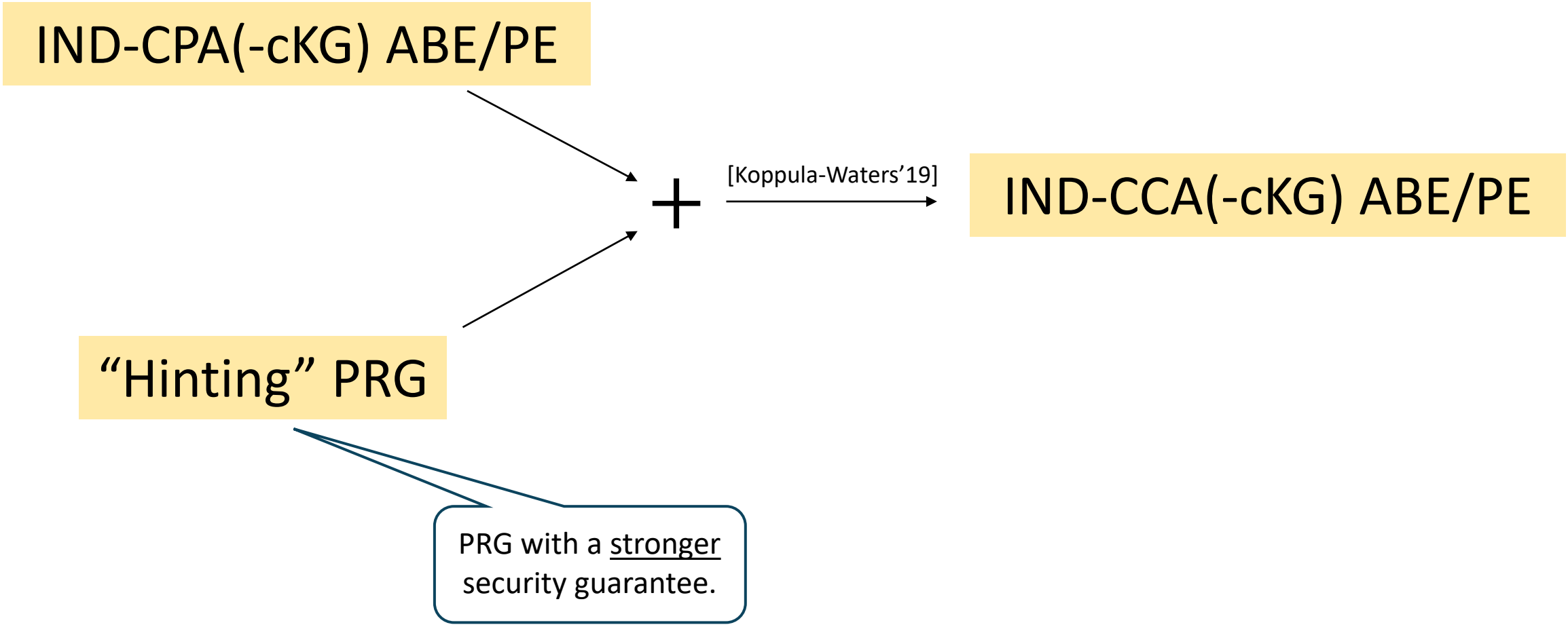
"Hinting" PRG

PRG with a stronger security guarantee.

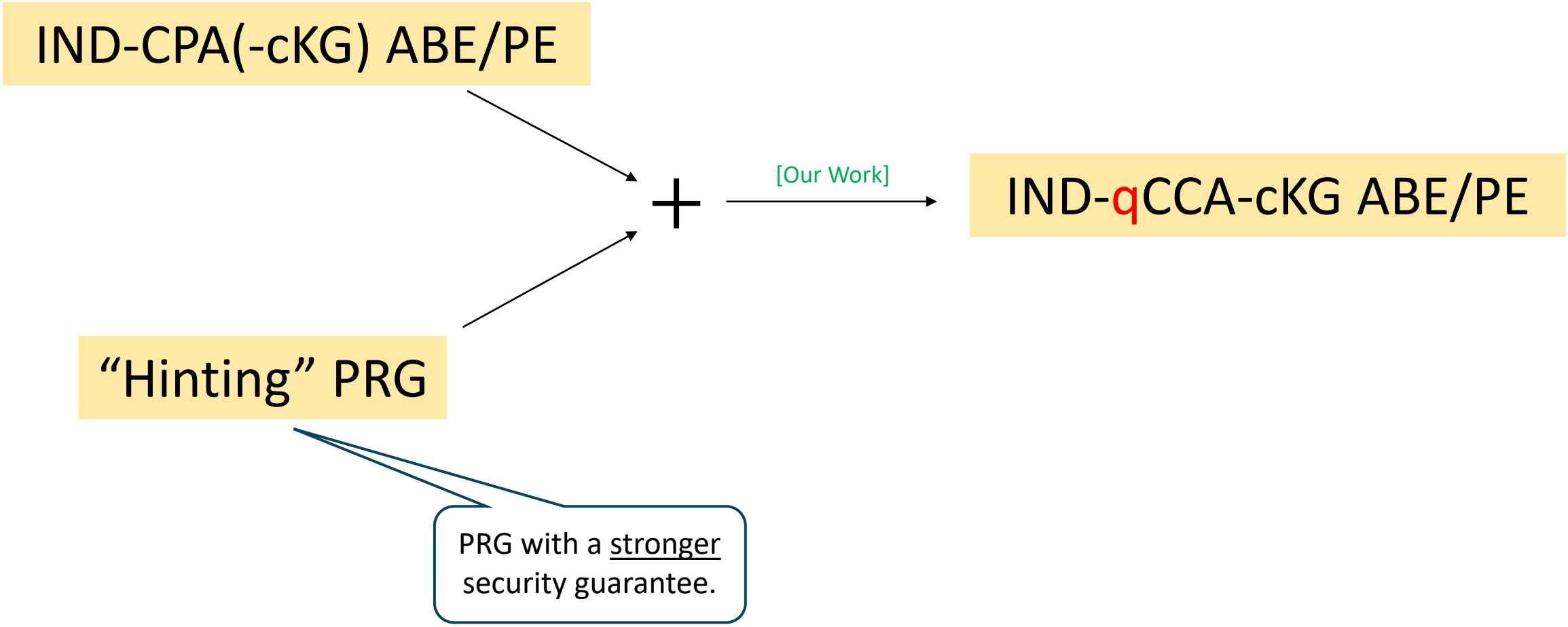
IND-qCCA-cKG Secure ABE



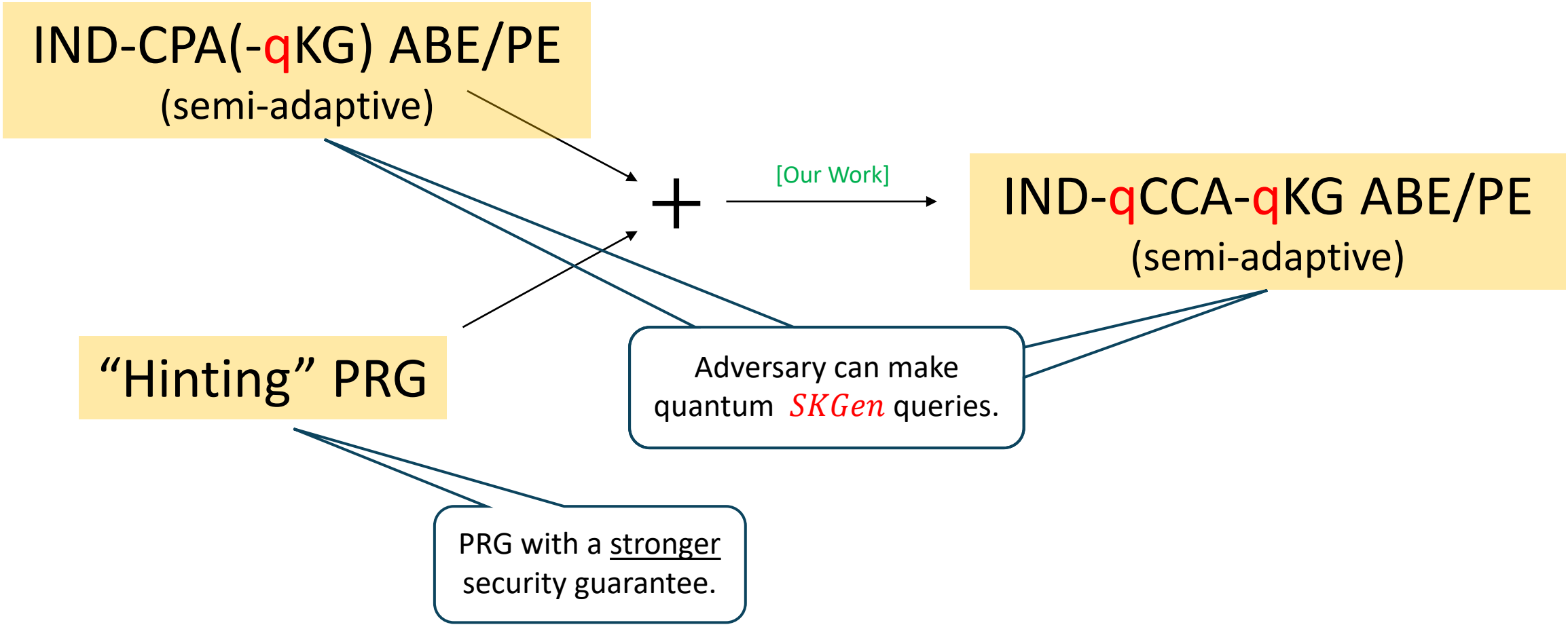
IND-qCCA-cKG Secure ABE



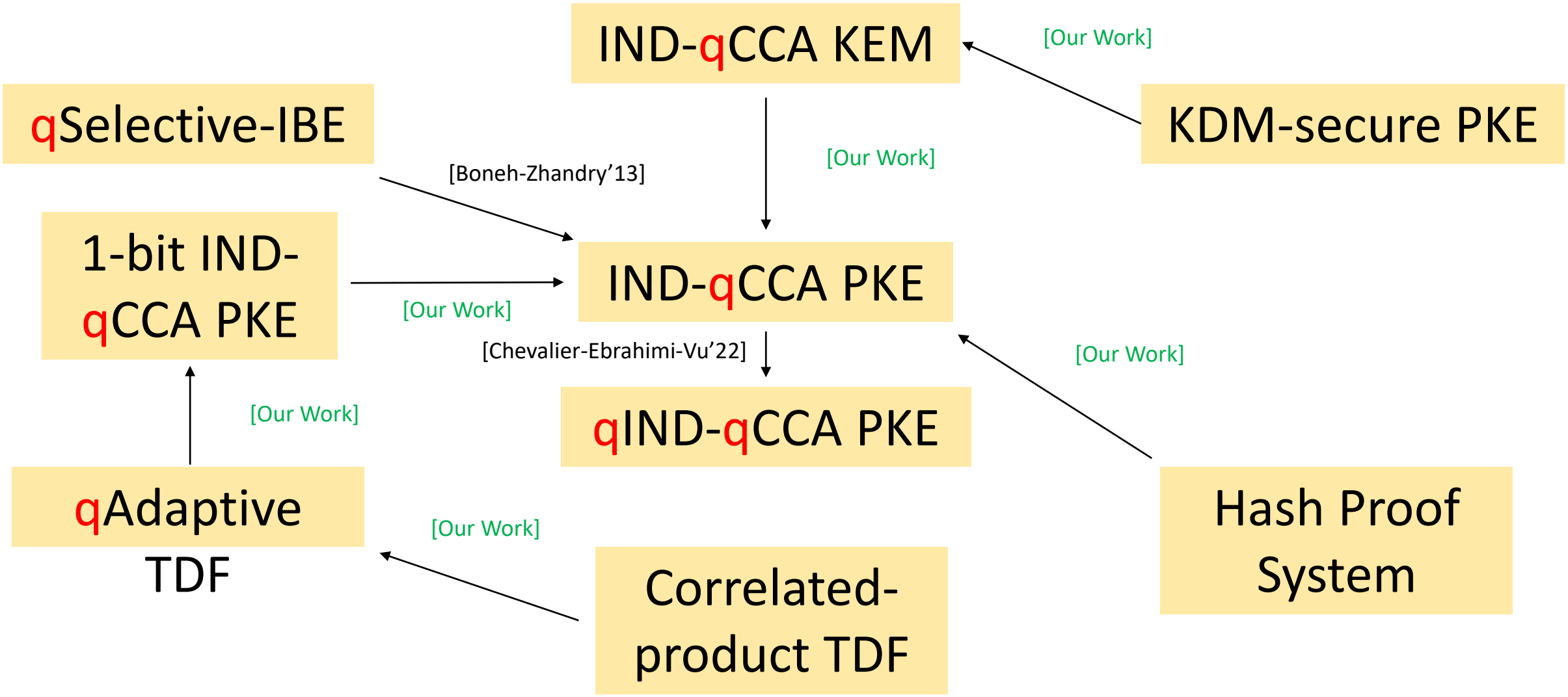
IND-qCCA-cKG Secure ABE



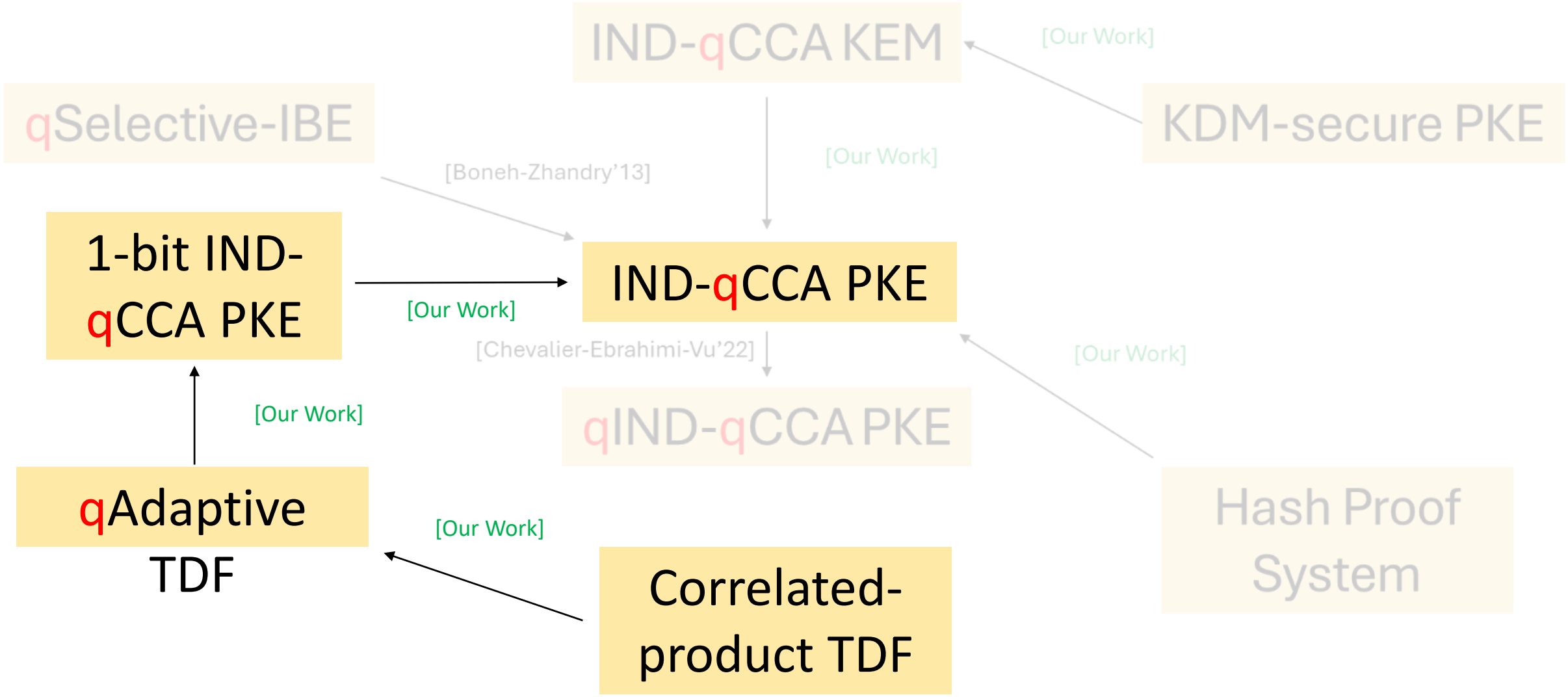
IND-qCCA-cKG Secure ABE



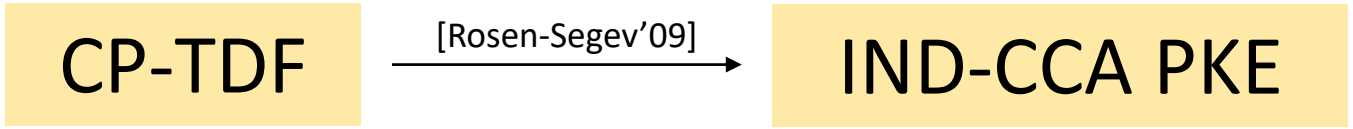
Overview: Techniques



Overview: Techniques

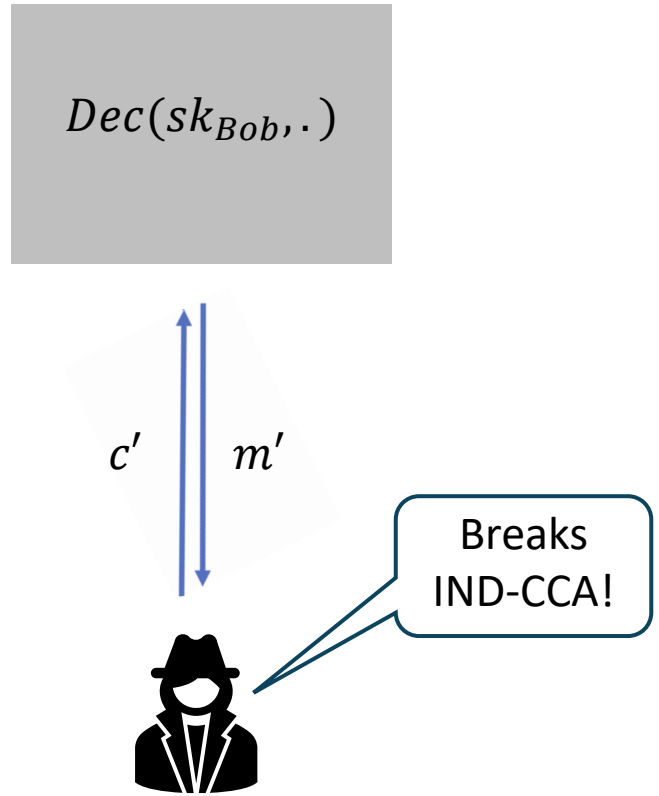


Overview: Techniques

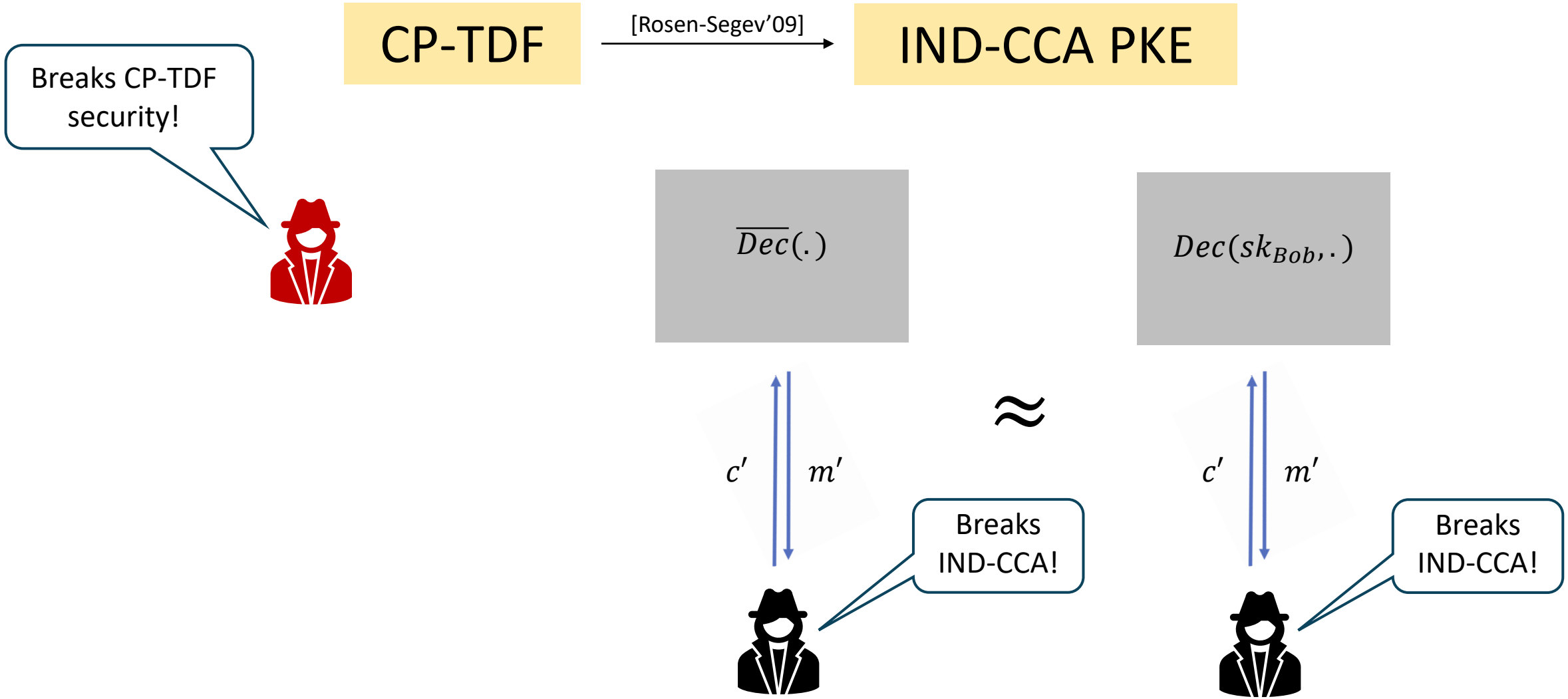


Overview: Techniques

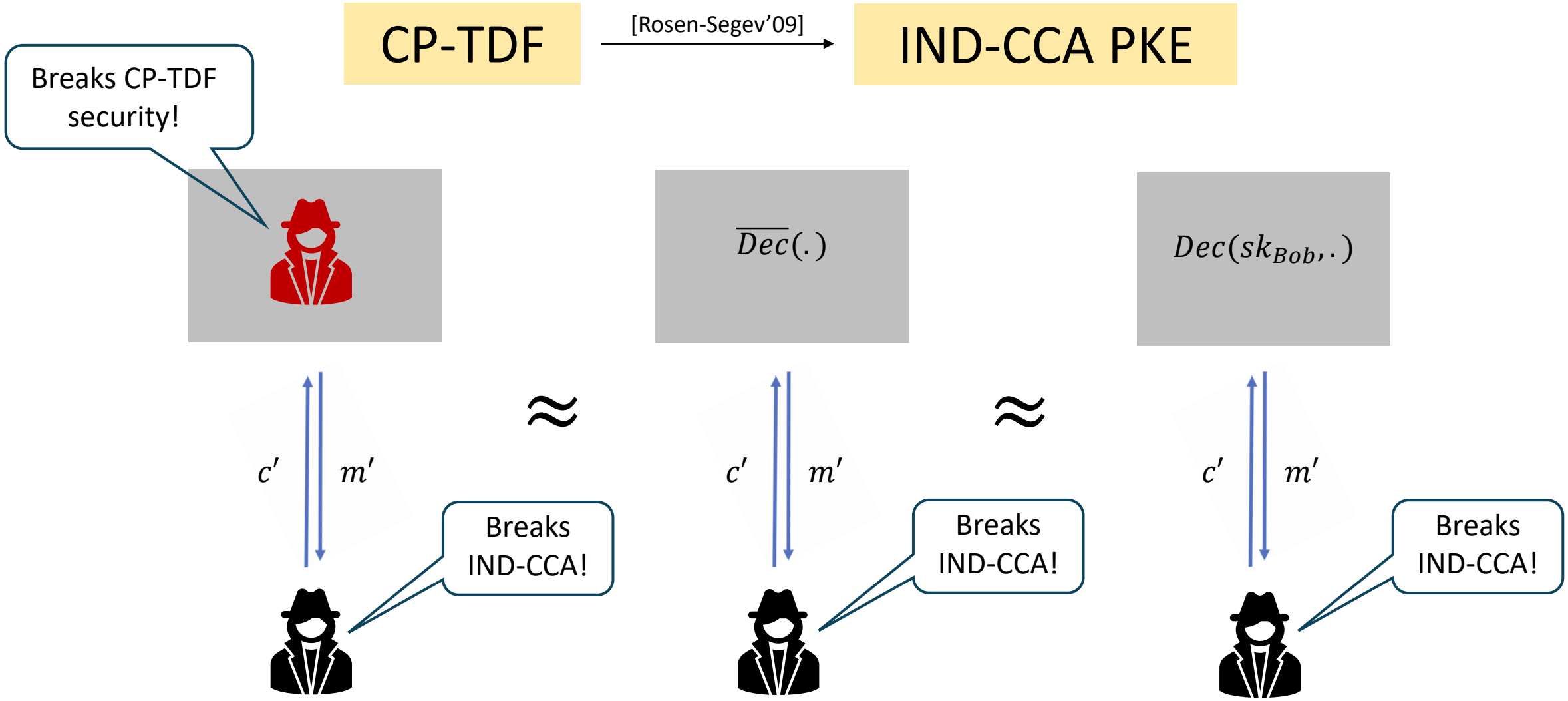
CP-TDF → [Rosen-Segev'09] → IND-CCA PKE



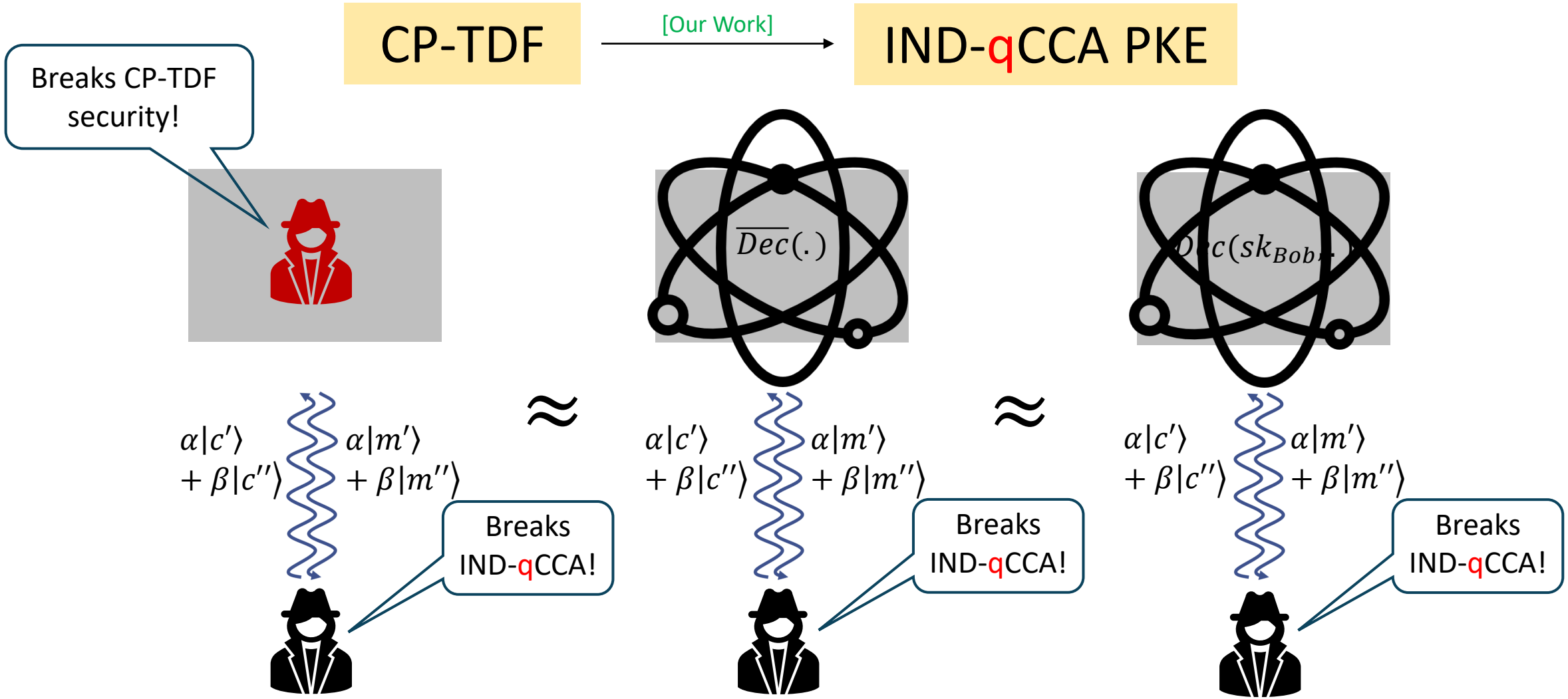
Overview: Techniques



Overview: Techniques



Overview: Techniques



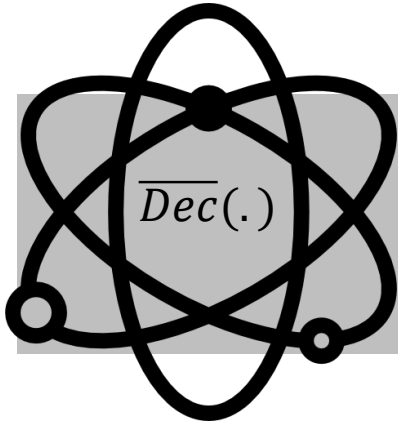
Overview: Techniques

Showed using the **generalized OW2H lemma** of [Ambainis-Hamburg-Unruh'19].

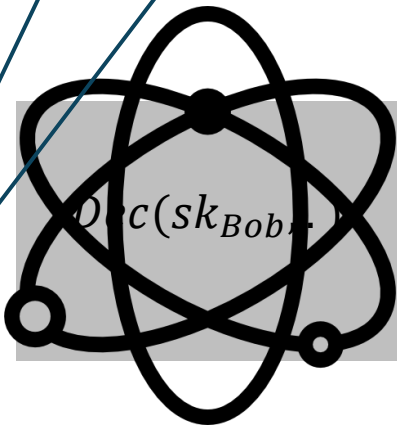
CP-TDF → [Our Work] → IND-qCCA PKE

Breaks CP-TDF security!

$\approx$



$\approx$



$\alpha|c'\rangle + \beta|c''\rangle$ $\alpha|m'\rangle + \beta|m''\rangle$

Breaks IND-qCCA!

$\alpha|c'\rangle + \beta|c''\rangle$ $\alpha|m'\rangle + \beta|m''\rangle$

Breaks IND-qCCA!

$\alpha|c'\rangle + \beta|c''\rangle$ $\alpha|m'\rangle + \beta|m''\rangle$

Breaks IND-qCCA!

Overview: Techniques

- The original "**O**ne-**W**ay **T**o **H**iding" (**OW2H**) lemma of [Unruh'14] was used to argue indistinguishability of **quantum (uniformly) random oracles**.

Overview: Techniques

- The original "**O**ne-**W**ay **T**o **H**iding" (**OW2H**) lemma of [Unruh'14] was used to argue indistinguishability of **quantum (uniformly) random oracles**.
- The lemma was later generalized by [Ambainis-Hamburg-Unruh'19] to handle quantum oracles with **arbitrary output distributions**.
- Our work involves the first application of the (generalized) OW2H

Overview: Techniques

- The original "**O**ne-**W**ay **T**o **H**iding" (**OW2H**) lemma of [Unruh'14] was used to argue indistinguishability of **quantum (uniformly) random oracles**.
- The lemma was later generalized by [Ambainis-Hamburg-Unruh'19] to handle quantum oracles with **arbitrary output distributions**.
- Our work involves the first application of the generalized OW2H lemma w.r.t. qCCA decryption oracles in the **standard model** – as opposed to the **QROM**.

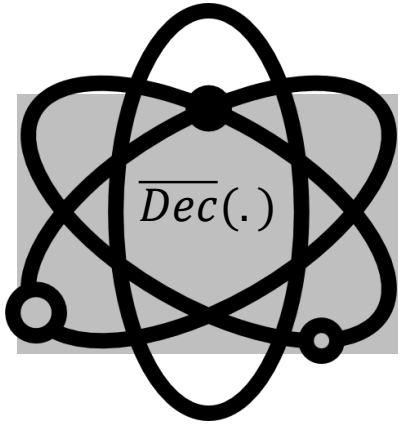
Overview: Techniques

Showed using the **generalized OW2H lemma** of [Ambainis-Hamburg-Unruh'19].

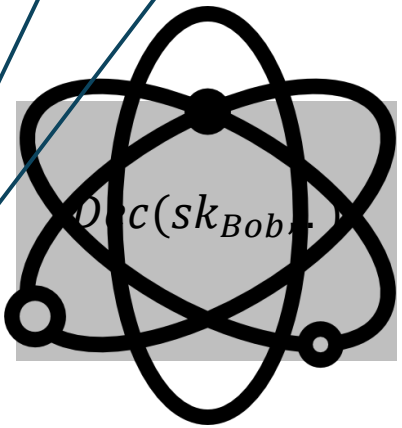
CP-TDF → [Our Work] → IND-qCCA PKE

Breaks CP-TDF security!

$\approx$



$\approx$



$\alpha|c'\rangle + \beta|c''\rangle$ $\alpha|m'\rangle + \beta|m''\rangle$

Breaks IND-qCCA!

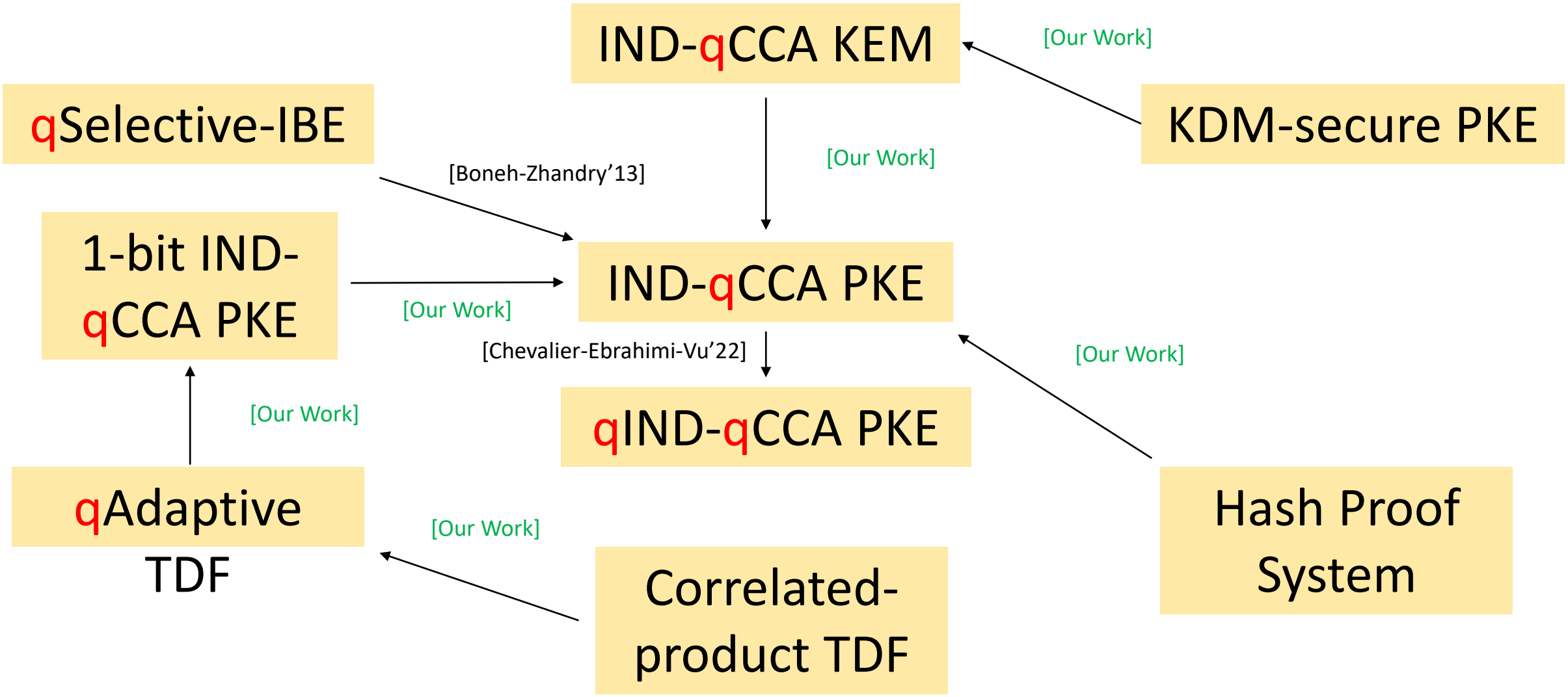
$\alpha|c'\rangle + \beta|c''\rangle$ $\alpha|m'\rangle + \beta|m''\rangle$

Breaks IND-qCCA!

$\alpha|c'\rangle + \beta|c''\rangle$ $\alpha|m'\rangle + \beta|m''\rangle$

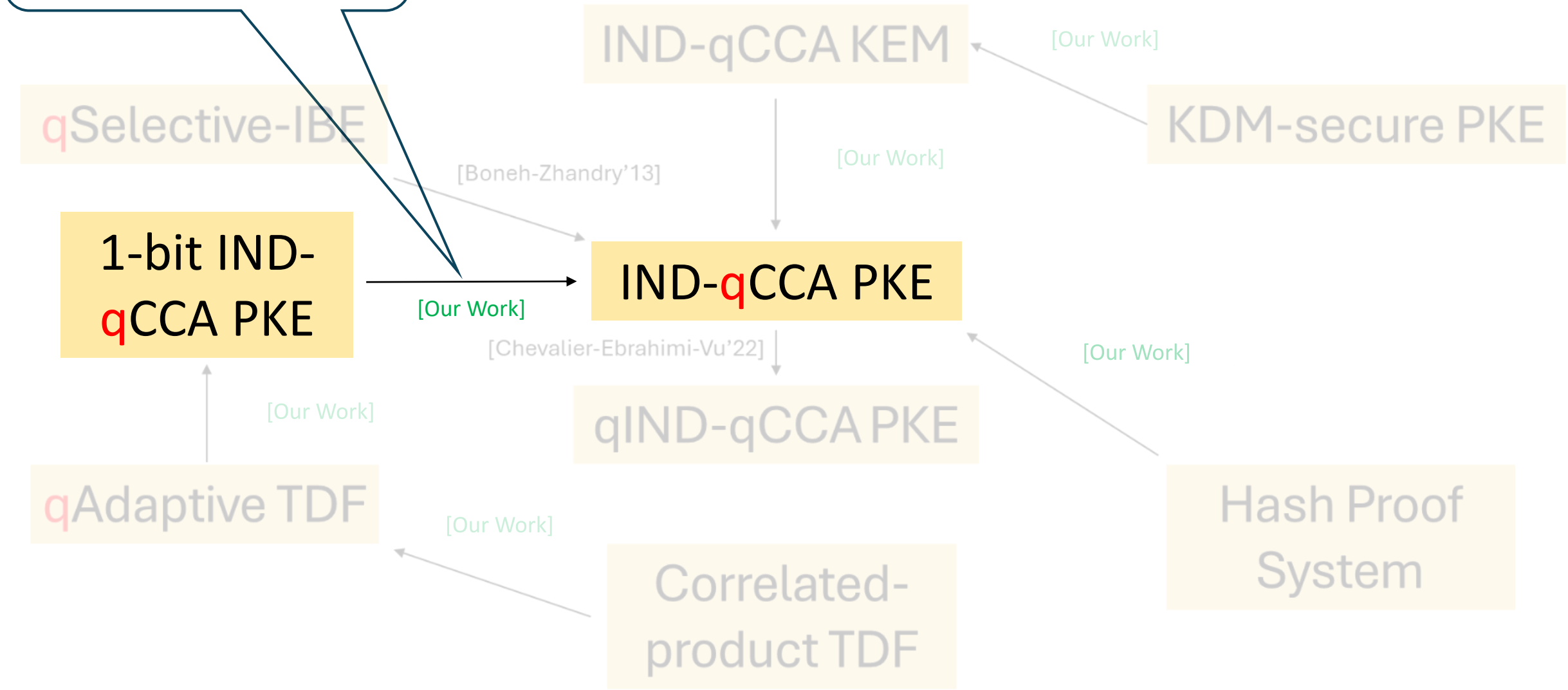
Breaks IND-qCCA!

Overview: Techniques



Overview: Techniques

Required a **"nested" application** of the generalized OW2H lemma.



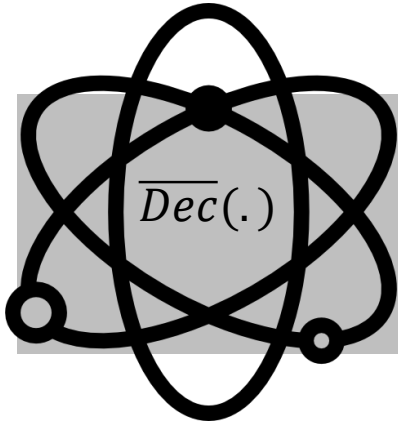
Overview: Techniques

Showed using the **generalized OW2H lemma** of [Ambainis-Hamburg-Unruh'19].

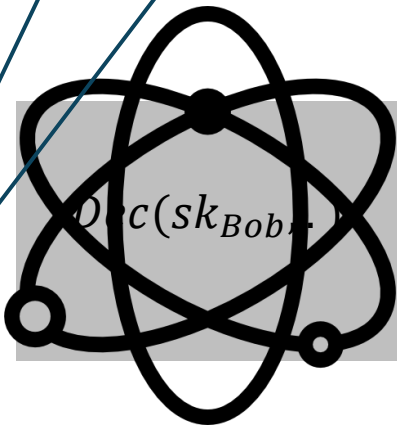
CP-TDF → [Our Work] → IND-qCCA PKE

Breaks CP-TDF security!

$\approx$



$\approx$



$\alpha|c'\rangle + \beta|c''\rangle$ $\alpha|m'\rangle + \beta|m''\rangle$

Breaks IND-qCCA!

$\alpha|c'\rangle + \beta|c''\rangle$ $\alpha|m'\rangle + \beta|m''\rangle$

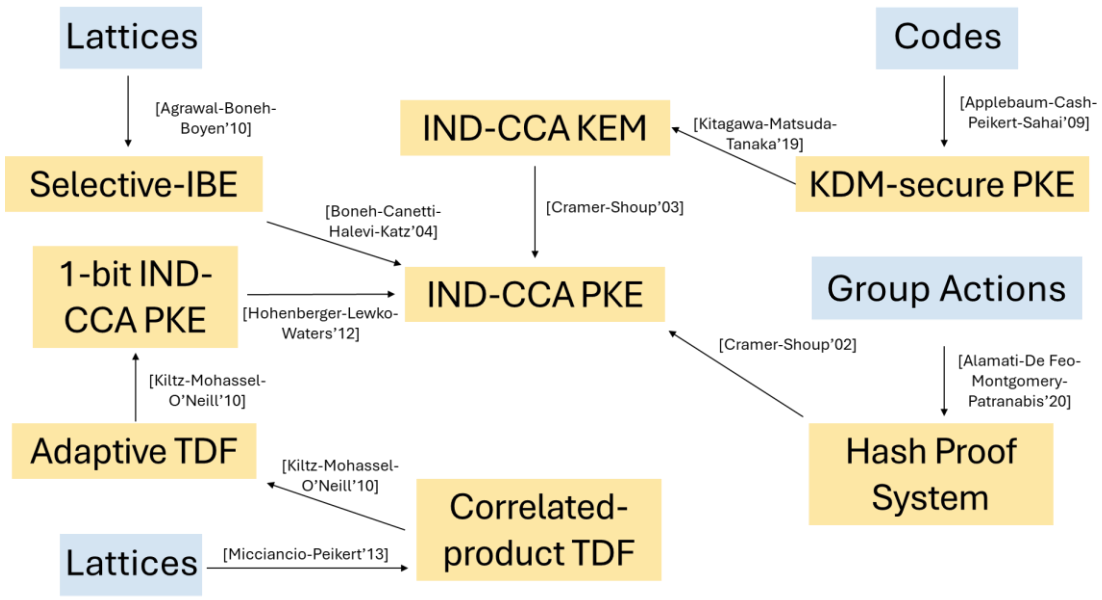
Breaks IND-qCCA!

$\alpha|c'\rangle + \beta|c''\rangle$ $\alpha|m'\rangle + \beta|m''\rangle$

Breaks IND-qCCA!

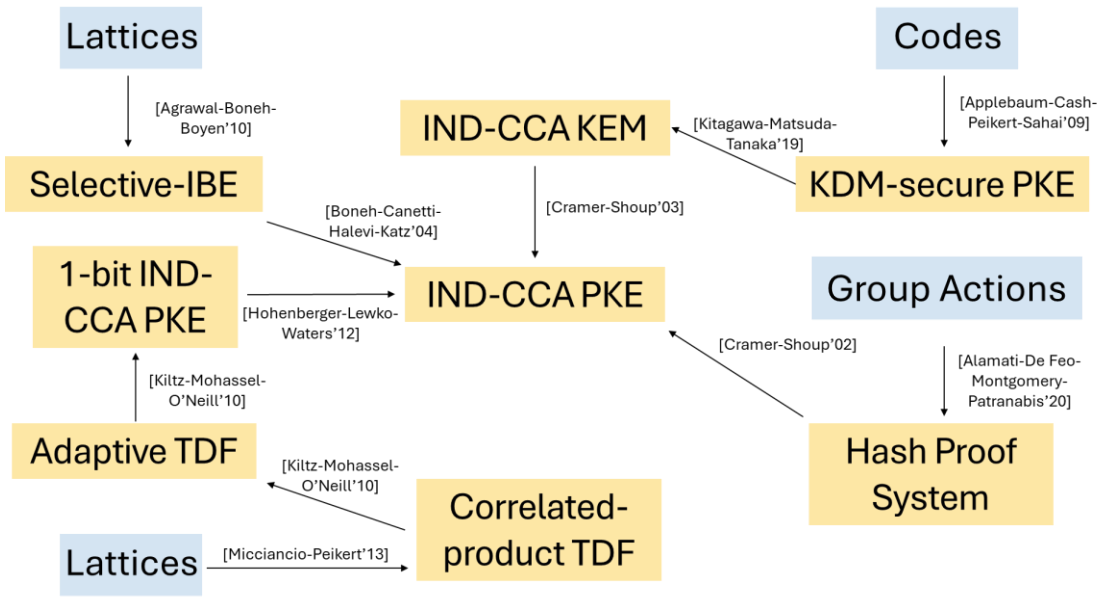
Conclusion

Conclusion

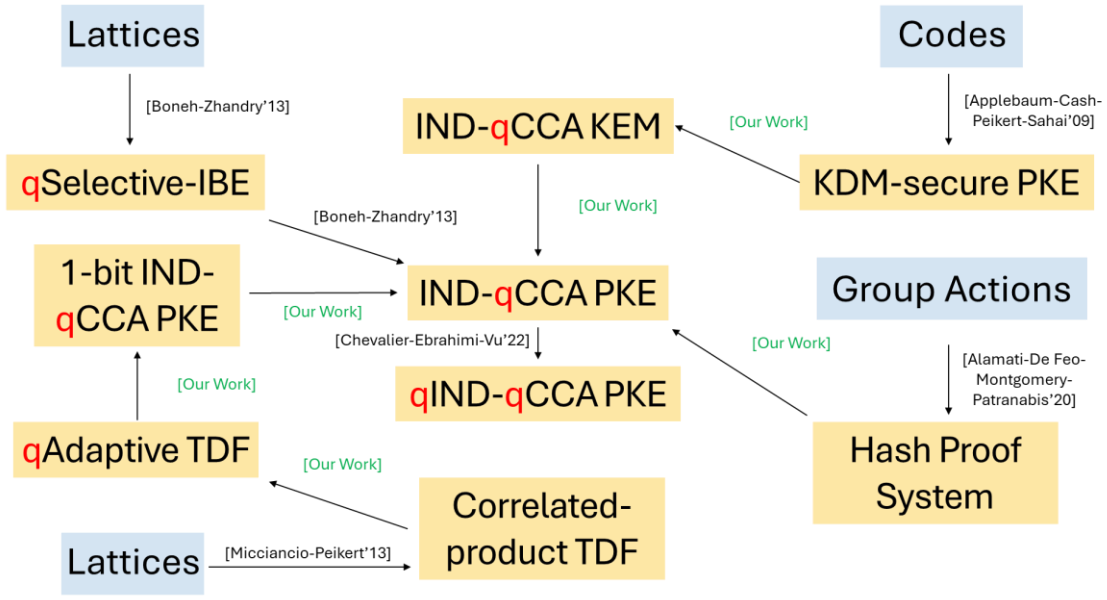


IND-CCA PKE

Conclusion

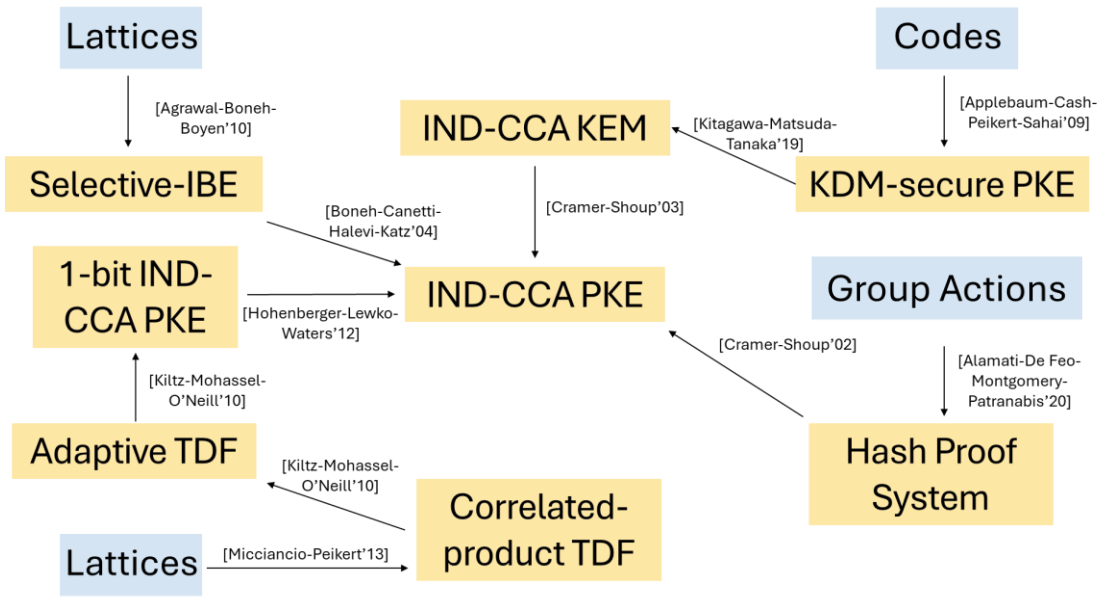


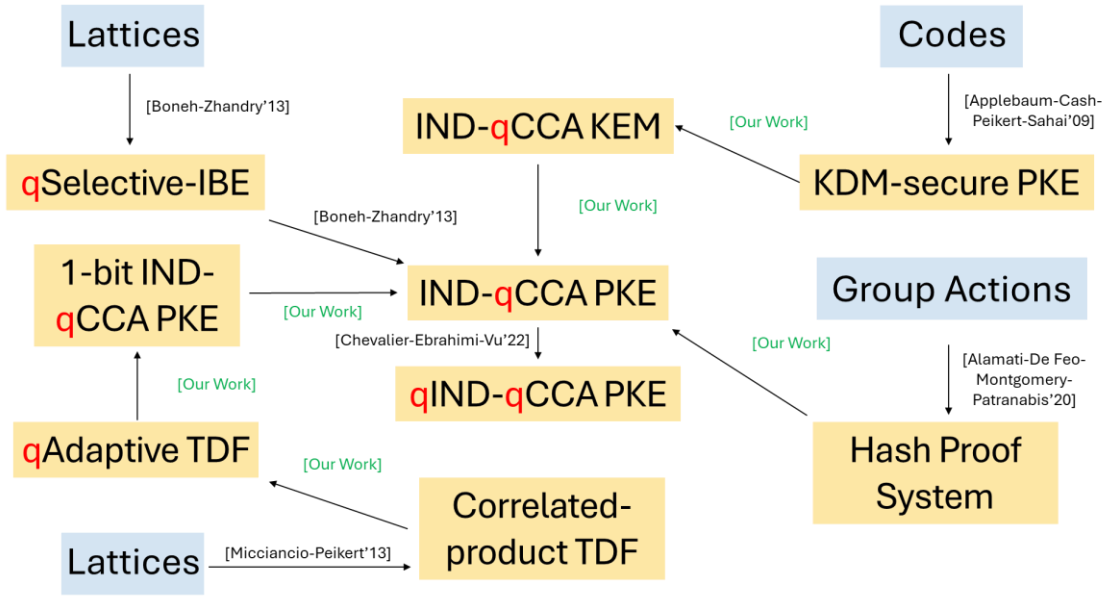
IND-CCA PKE



IND-qCCA PKE

Conclusion





IND-CCA PKE → ?? → IND-qCCA PKE