Quantum CCA-Secure PKE, Revisited

Varun Maram
Quantum Security Group
SandboxAQ

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

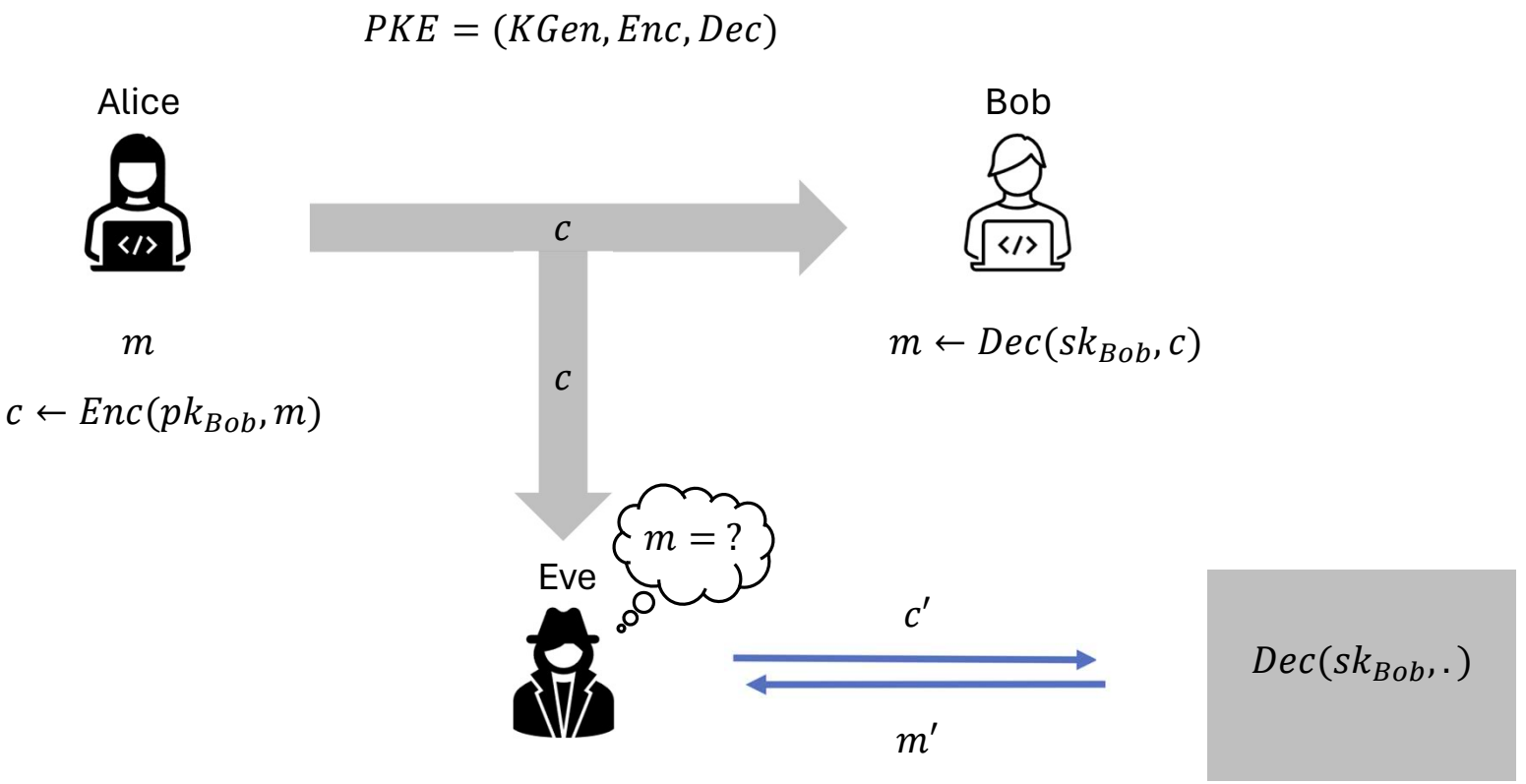
: varun-maram-pqc

Joint work with Navid Alamati

Quantum CCA-Secure PKE, Revisited

Quantum CCA-Secure PKE, Revisited

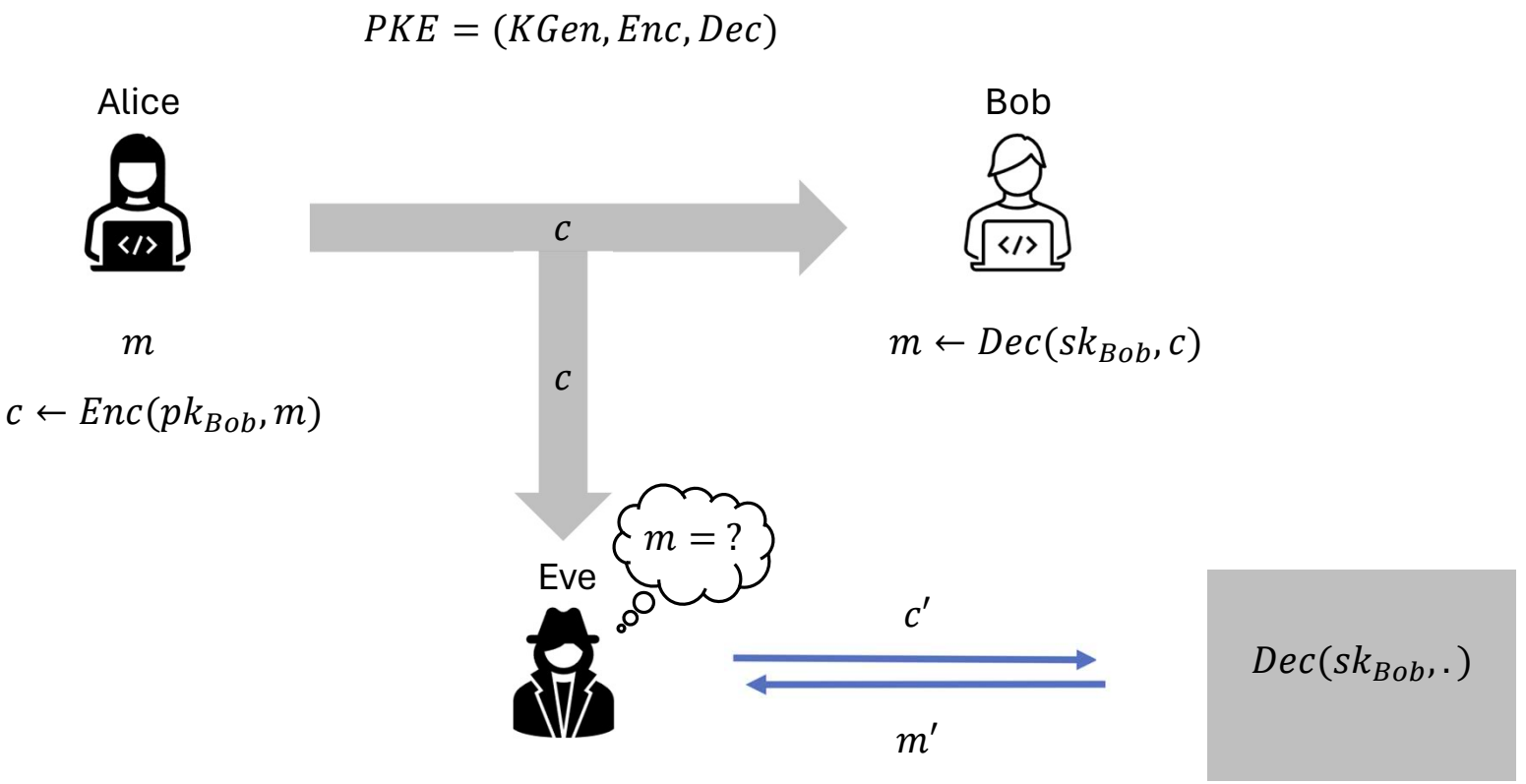
IND-CCA Security



Quantum CCA-Secure PKE, Revisited

Quantum CCA-Secure PKE, Revisited

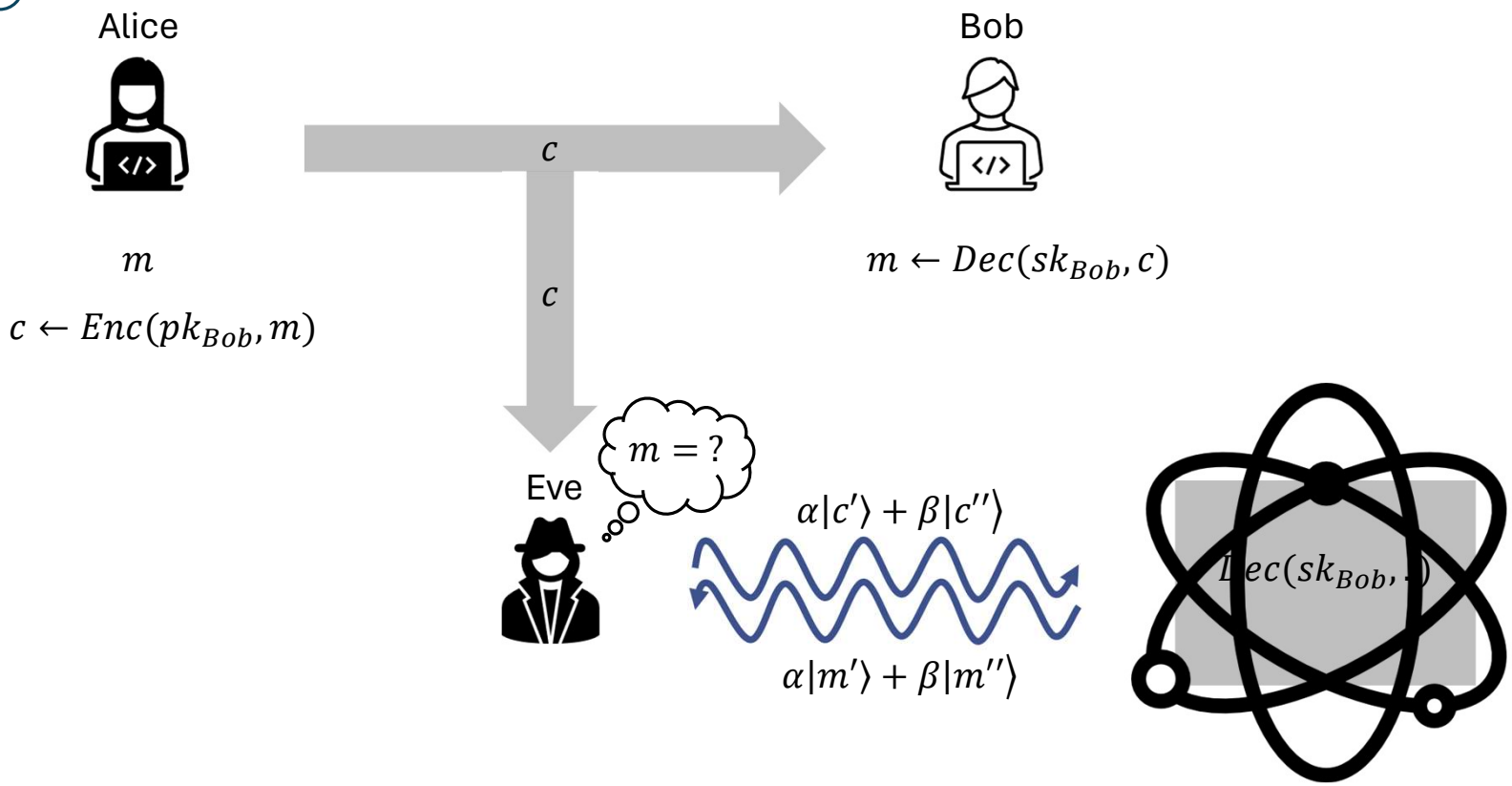
IND-CCA Security



IND-qCCA Security

Introduced by [Boneh-Zhandry'13].

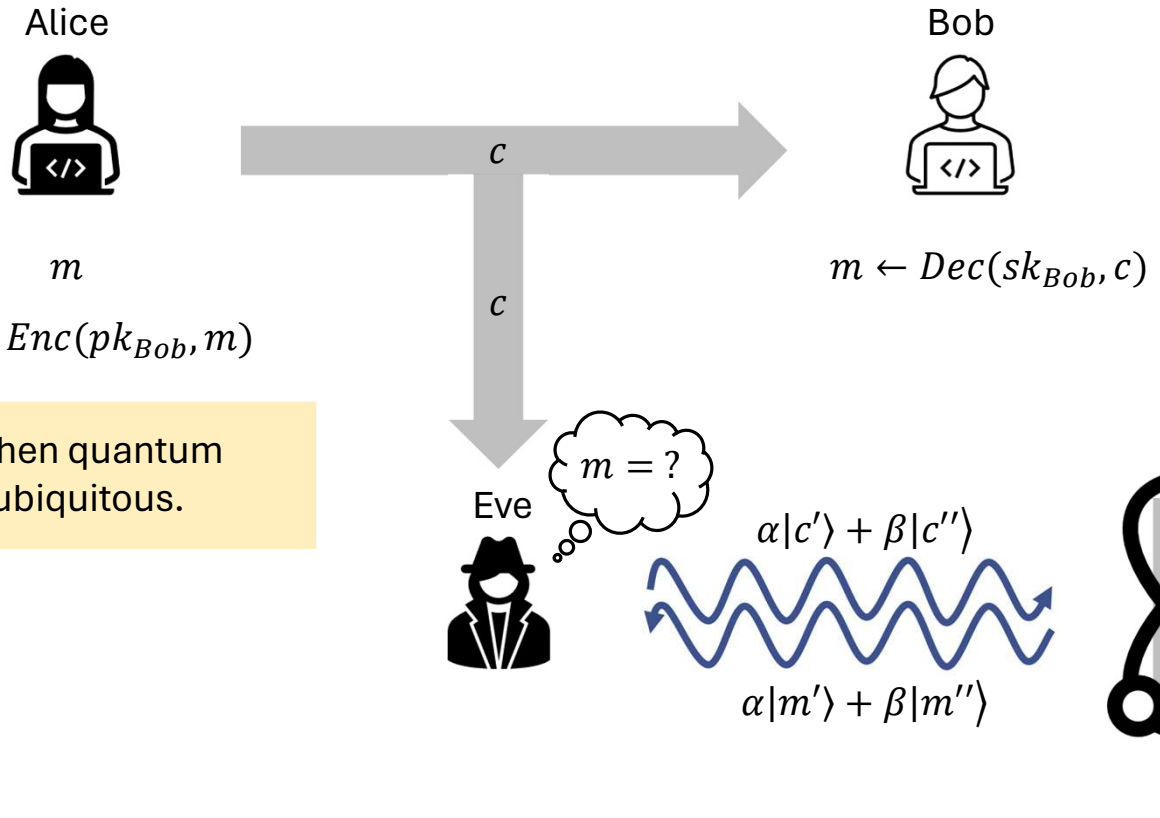
$PKE = (KGen, Enc, Dec)$



IND-qCCA Security

Introduced by [Boneh-Zhandry'13].

$PKE = (KGen, Enc, Dec)$

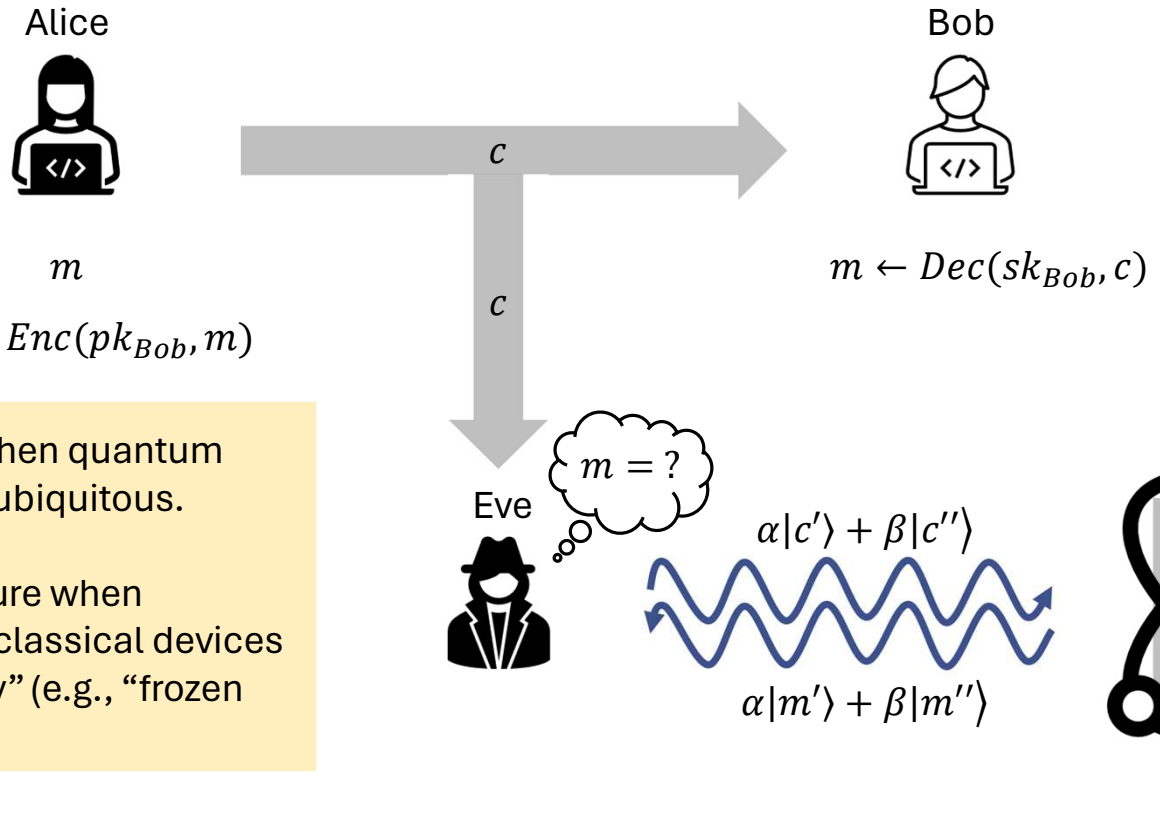


- Relevance in future when quantum computing becomes ubiquitous.

IND-qCCA Security

Introduced by [Boneh-Zhandry'13].

$PKE = (KGen, Enc, Dec)$



- 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").

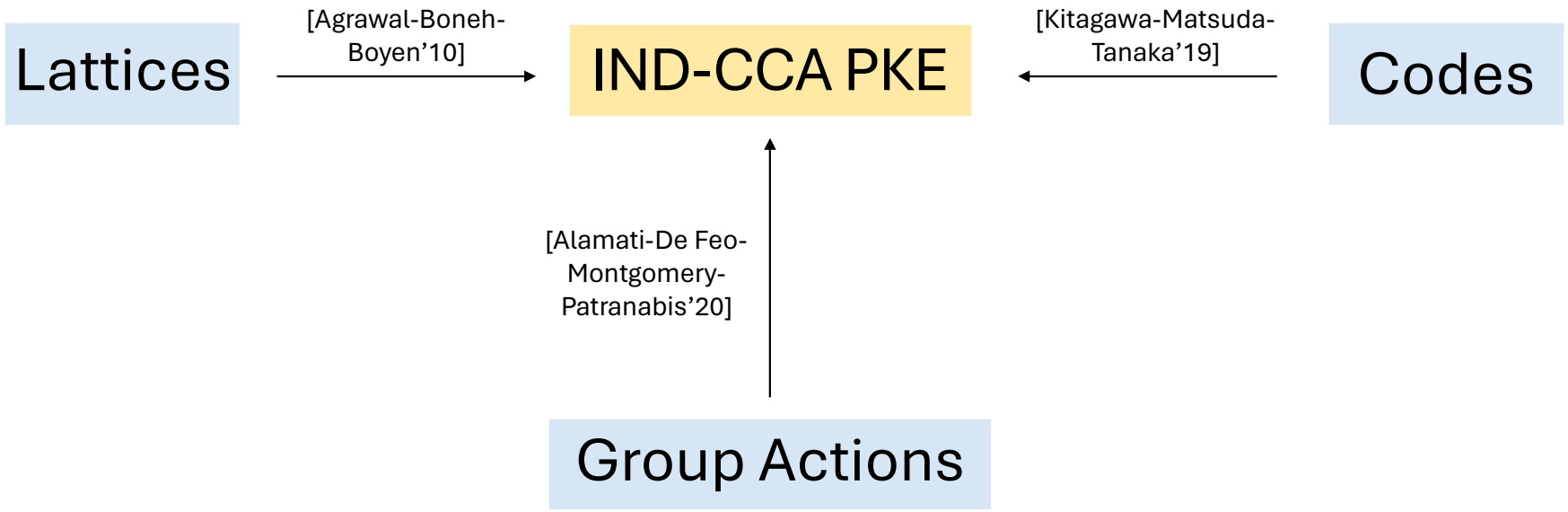
Quantum CCA-Secure PKE, Revisited

Quantum CCA-Secure PKE, Revisited

Motivation

IND-CCA PKE

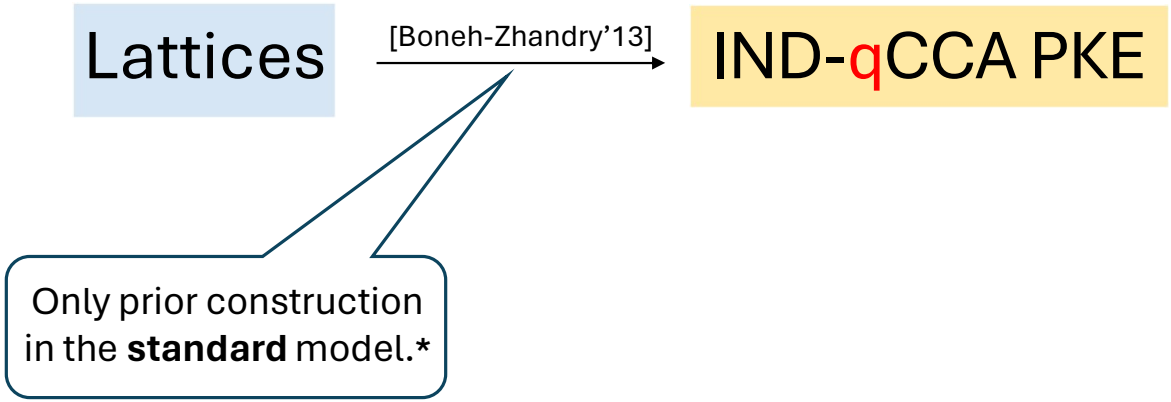
Motivation


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

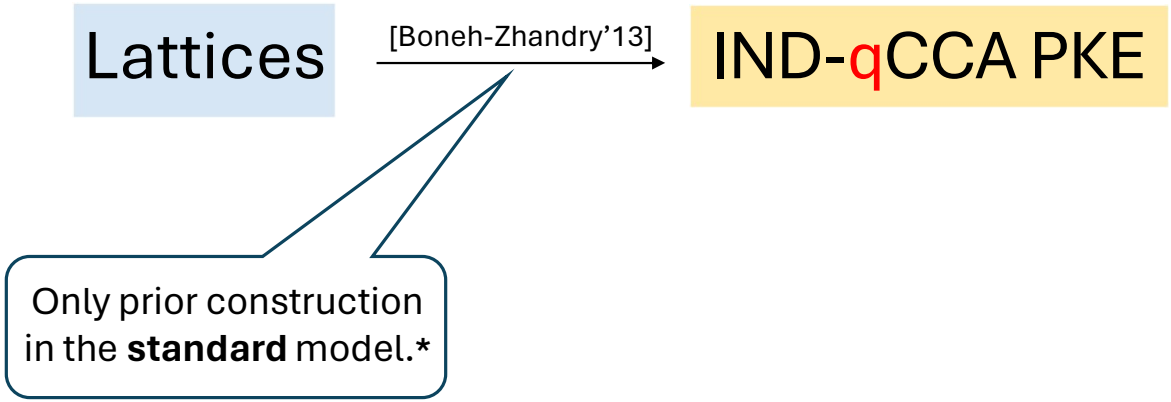
Motivation

IND-qCCA PKE

Motivation

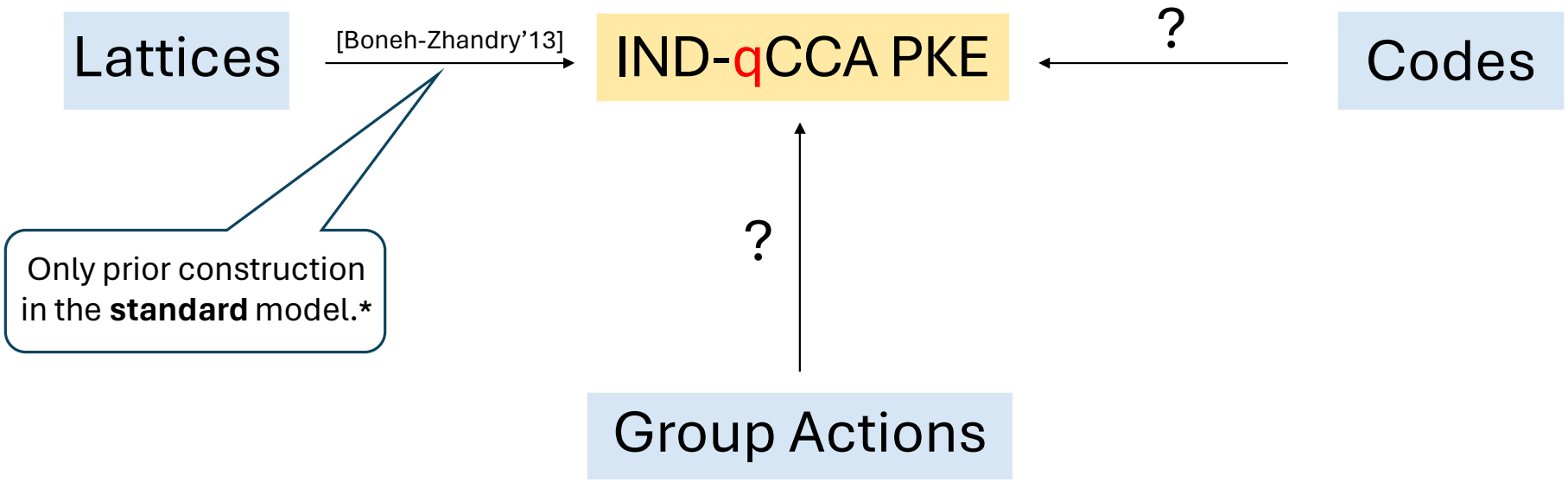

Lattices
[Boneh-Zhandry'13]
IND-qCCA PKE
Only prior construction in the **standard** model.*

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

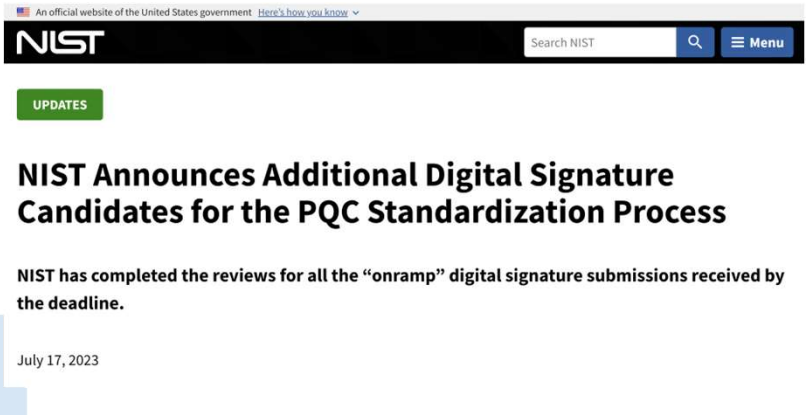
?

Codes

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

?

Group Actions



Motivation

Quantum Algorithms for Lattice Problems

Yilei Chen*

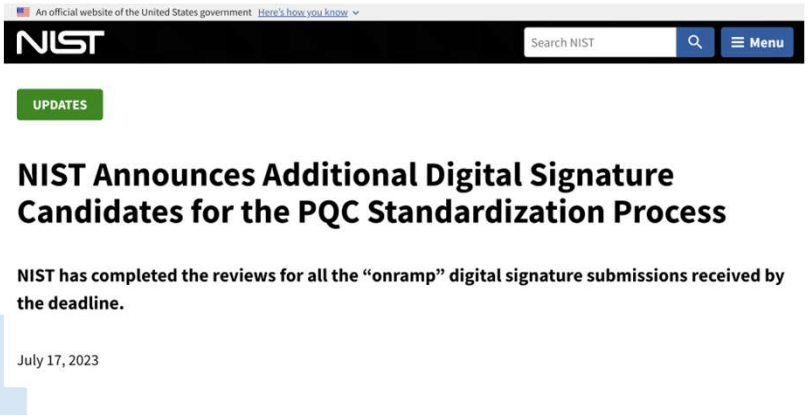
April 10, 2024

Lattices —[Boneh-Zhandry'13]→ IND-qCCA PKE ← ? — Codes

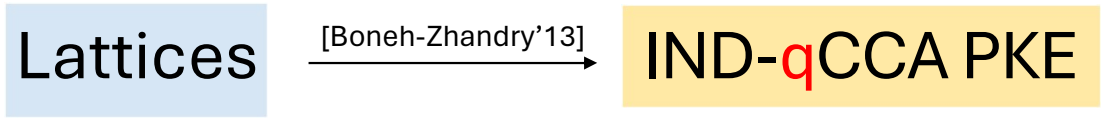
Only prior construction in the **standard** model.*

? ↑

Group Actions



Motivation



Motivation

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

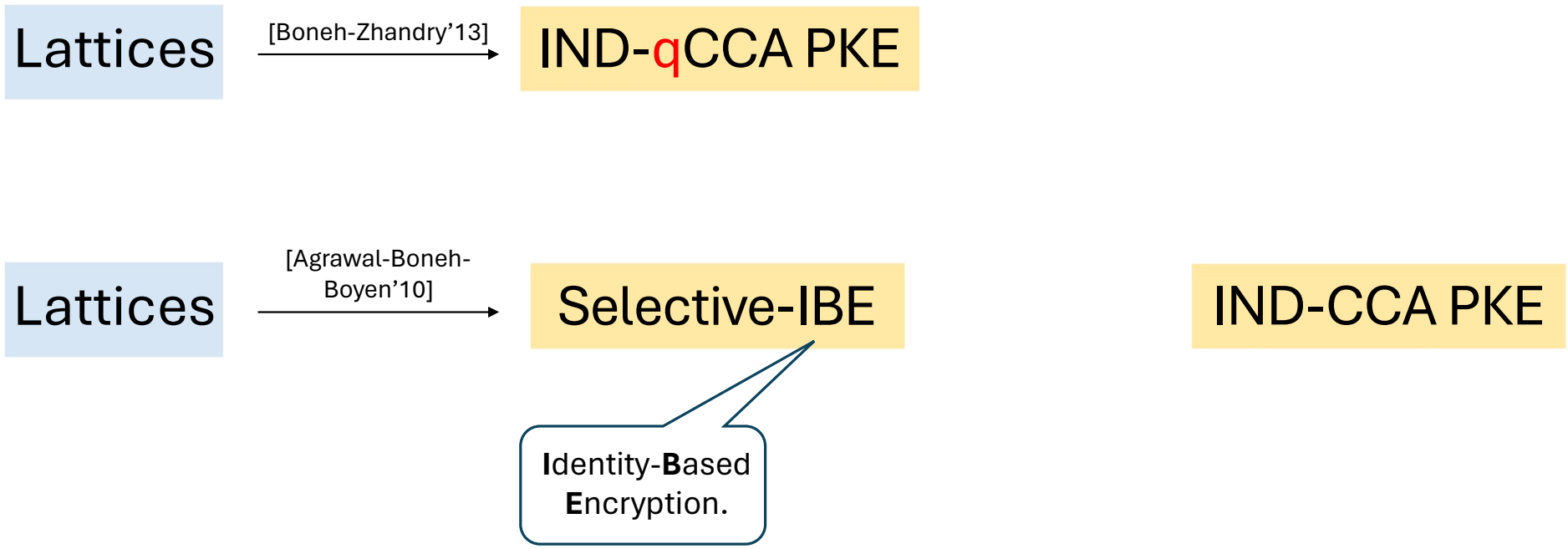
Lattices —[Agrawal-Boneh-Boyen'10]→ IND-CCA PKE

Motivation

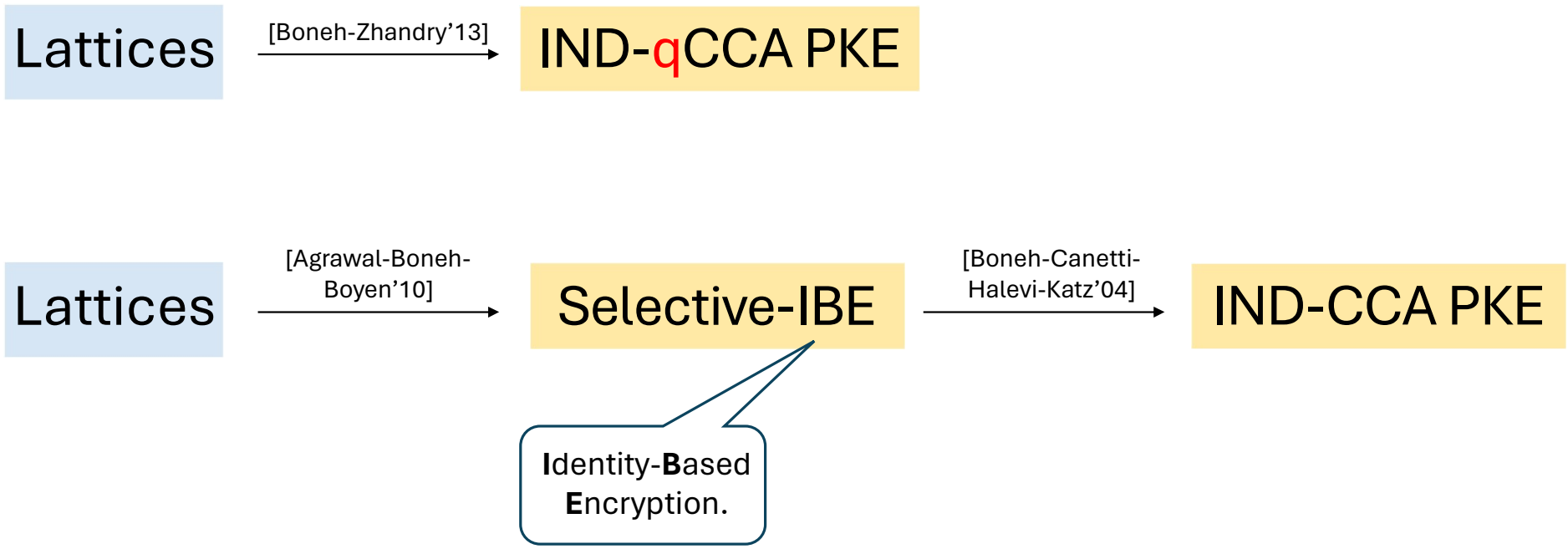
Lattices —[Boneh-Zhandry'13]→ IND-qCCA PKE

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

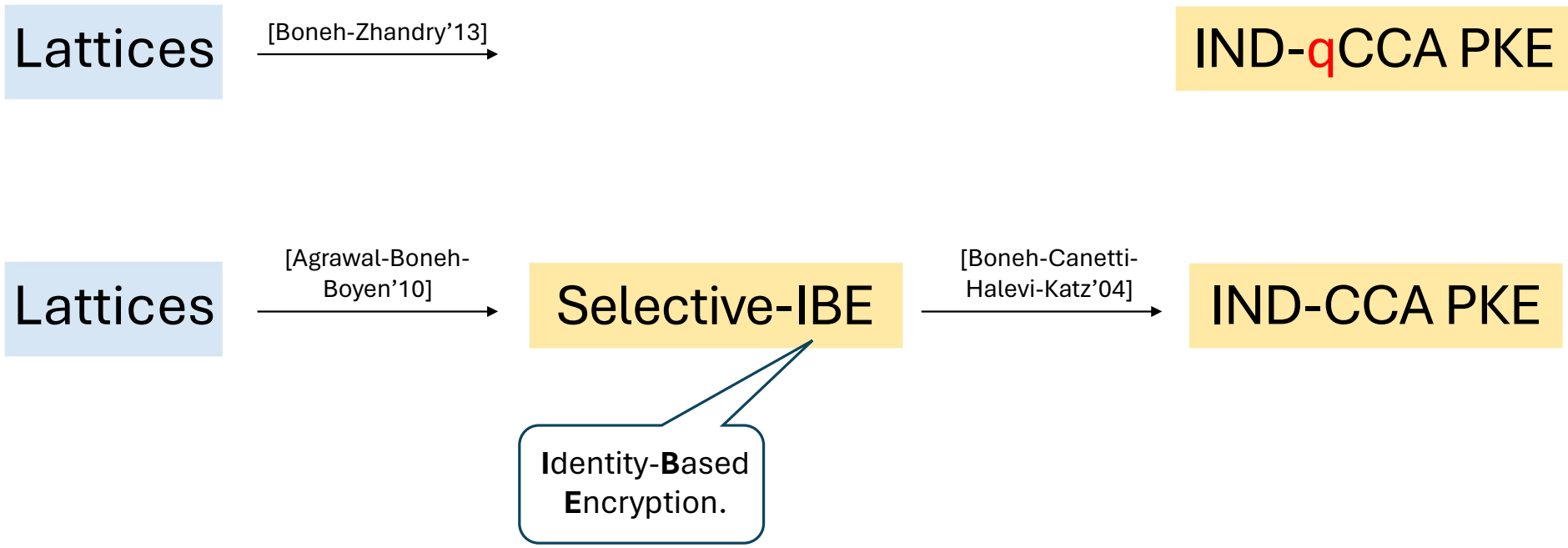
Motivation


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

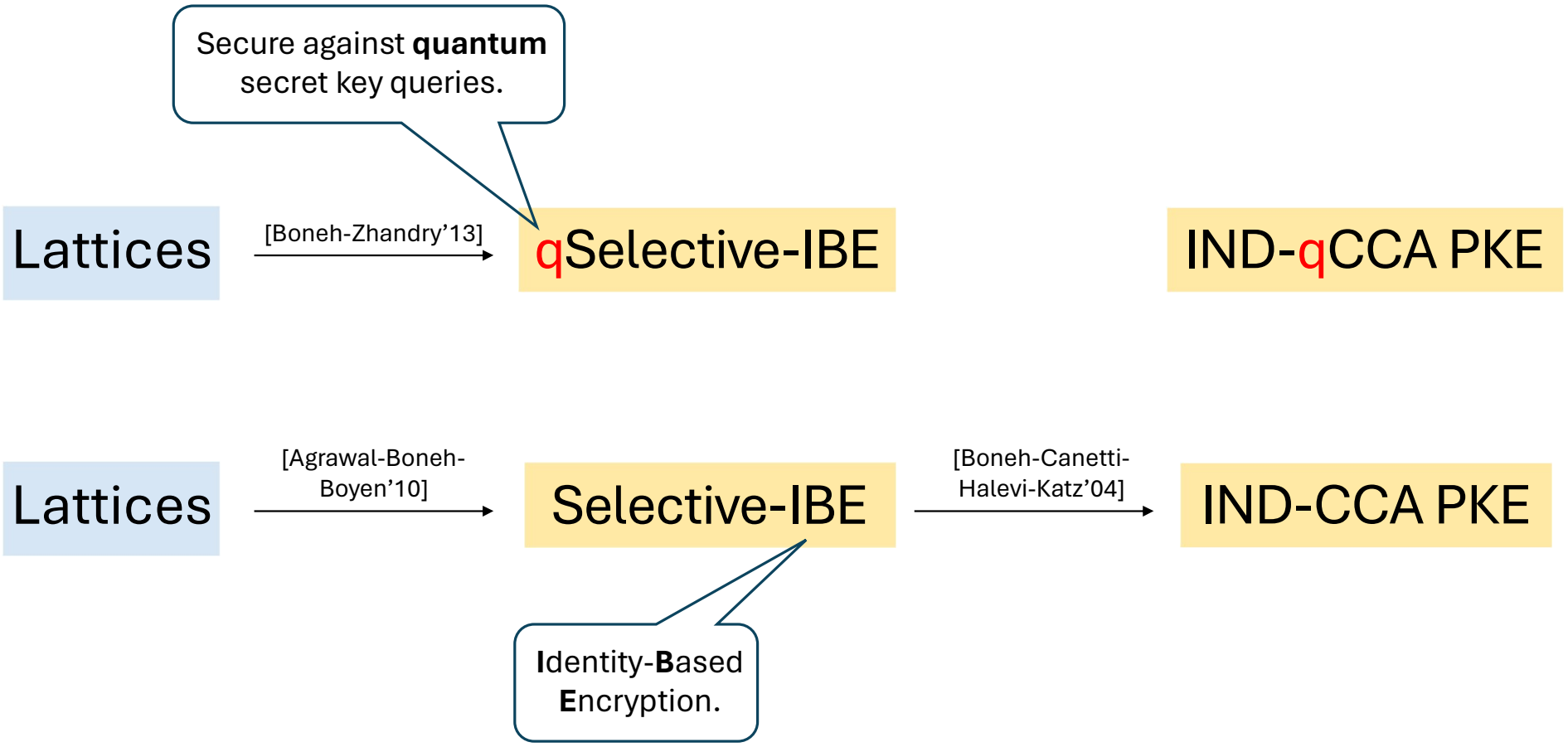
Motivation


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.

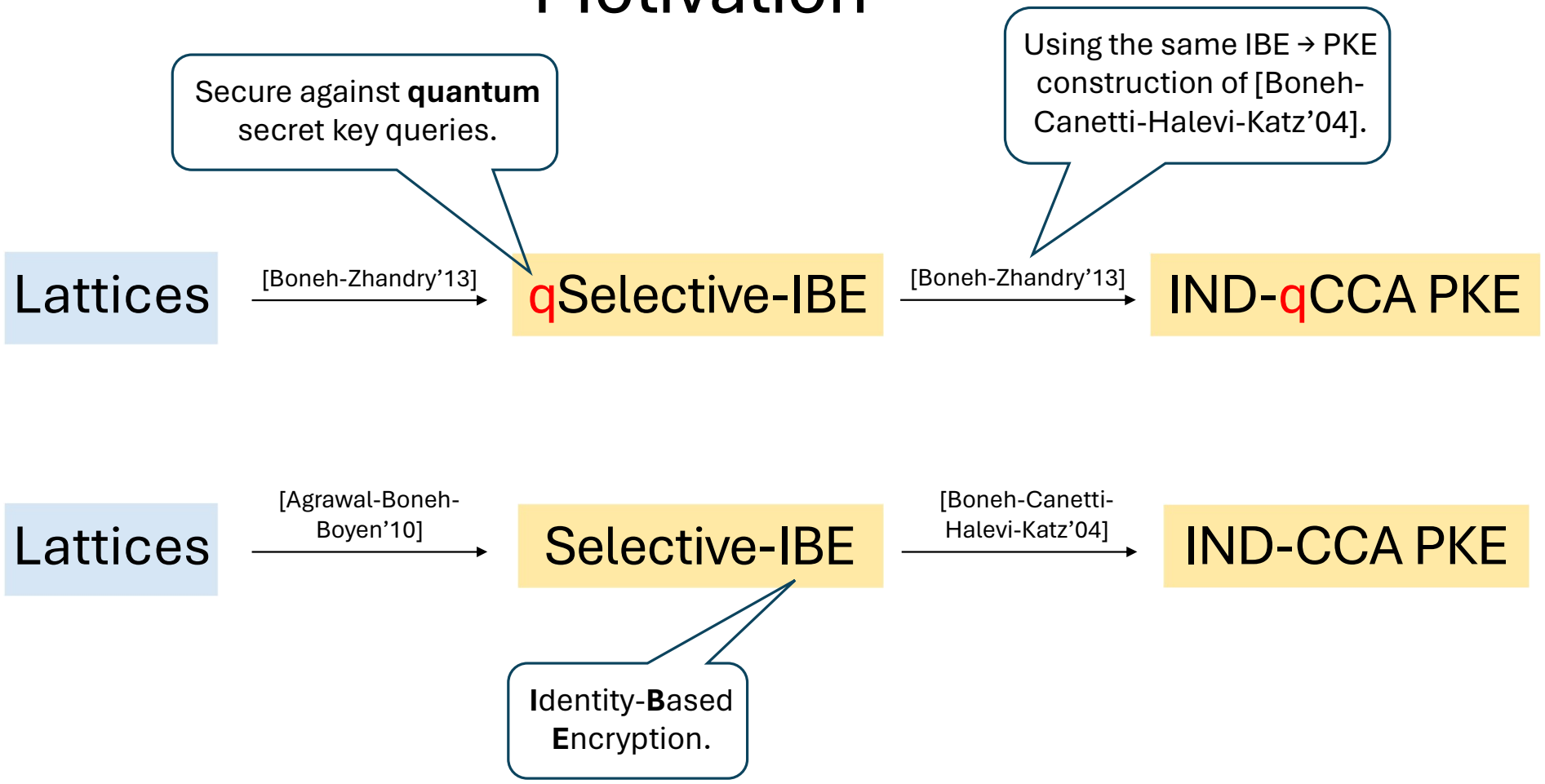
Motivation


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.

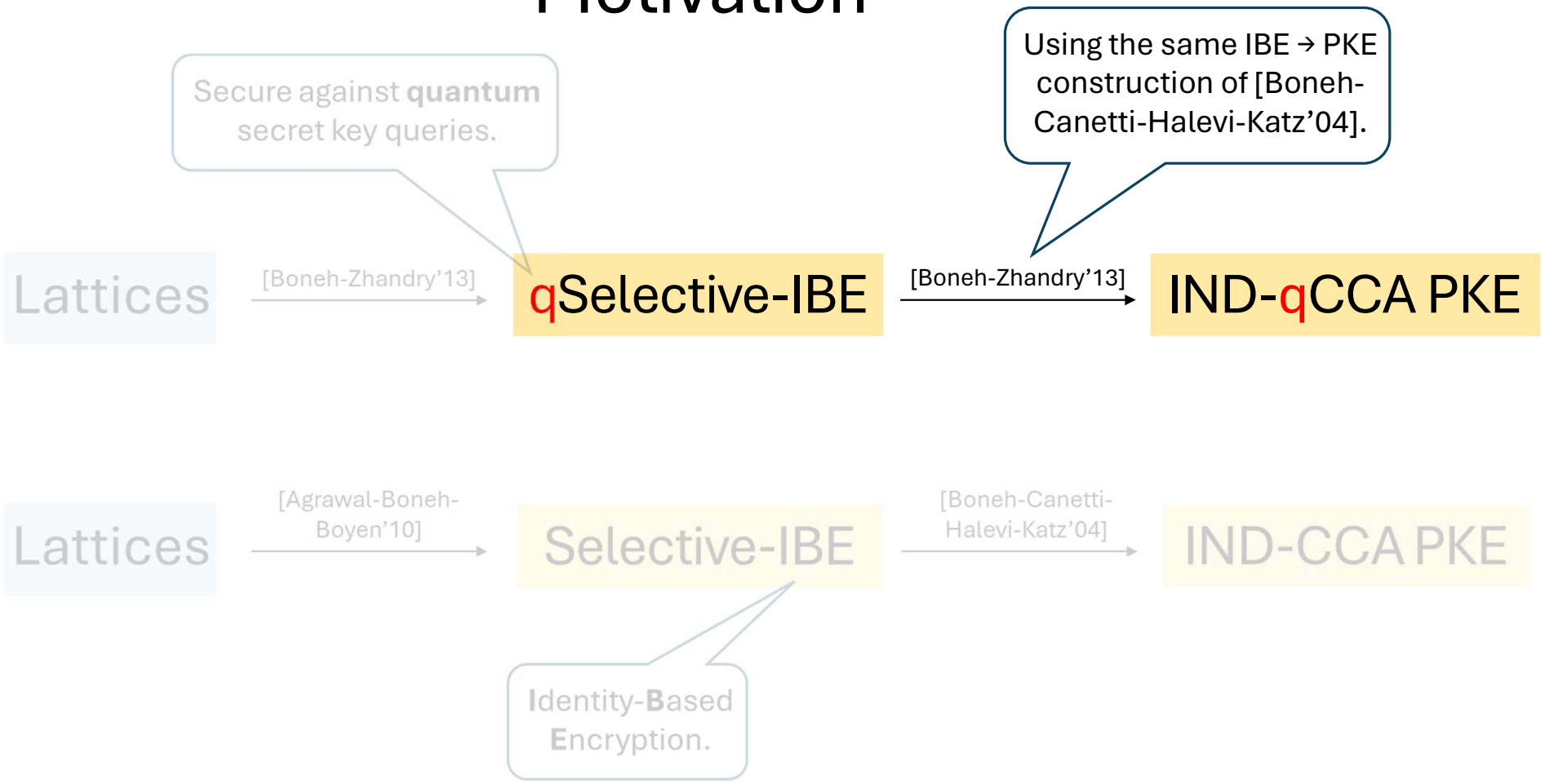
Motivation


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.

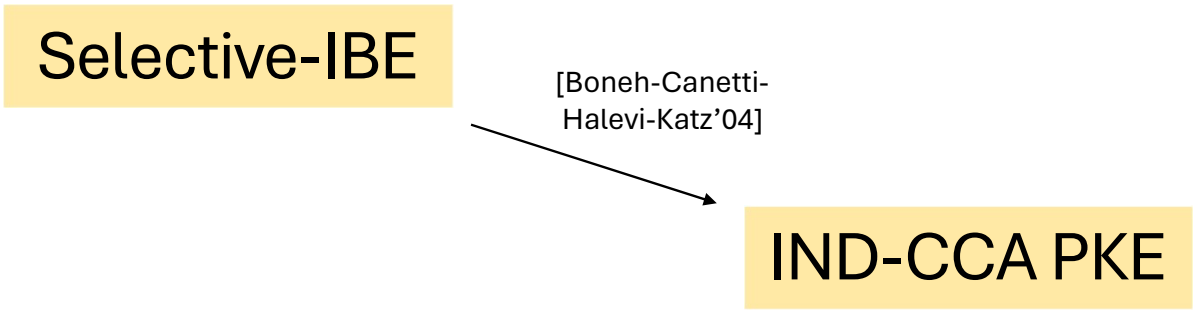
Motivation


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.

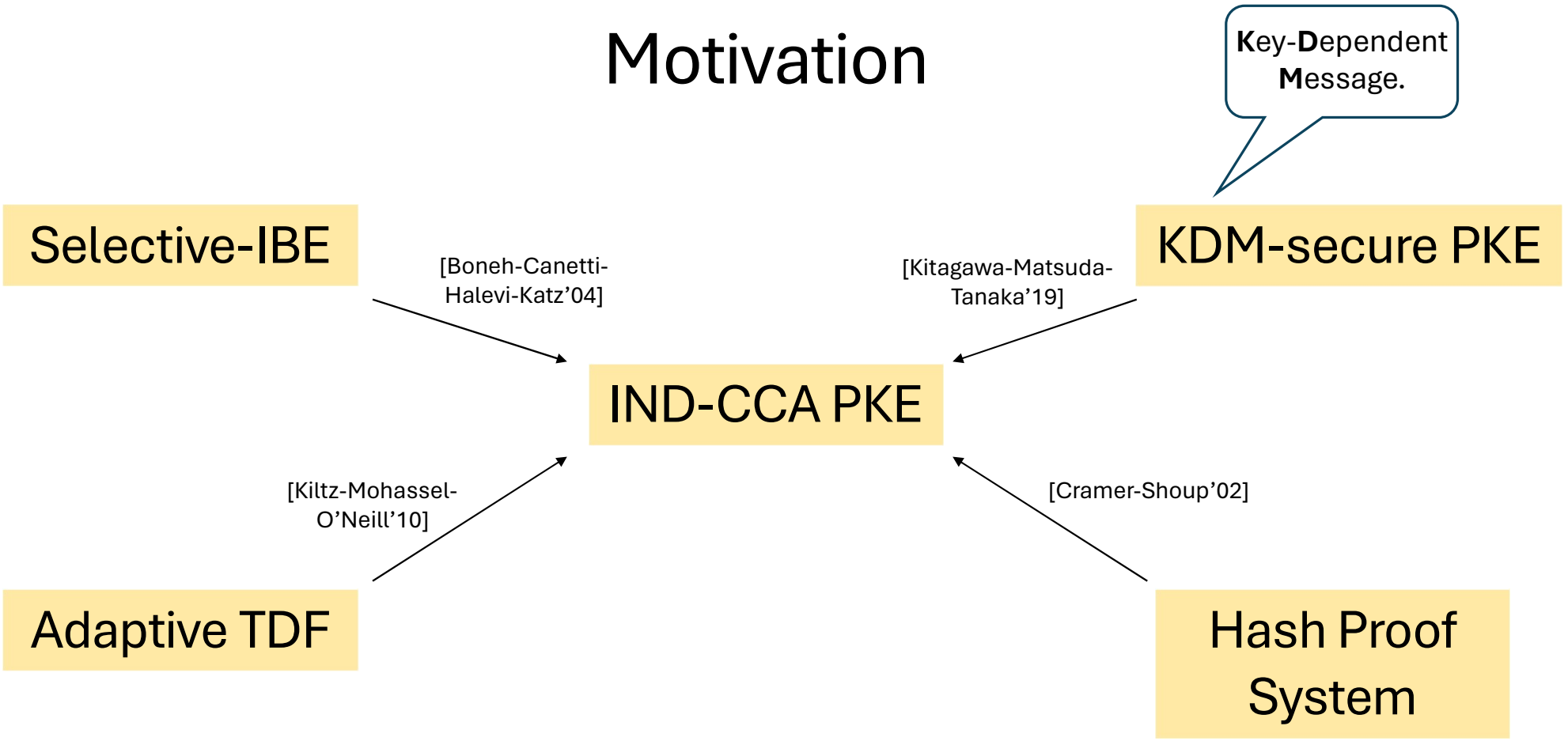
Motivation


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-Based Encryption.

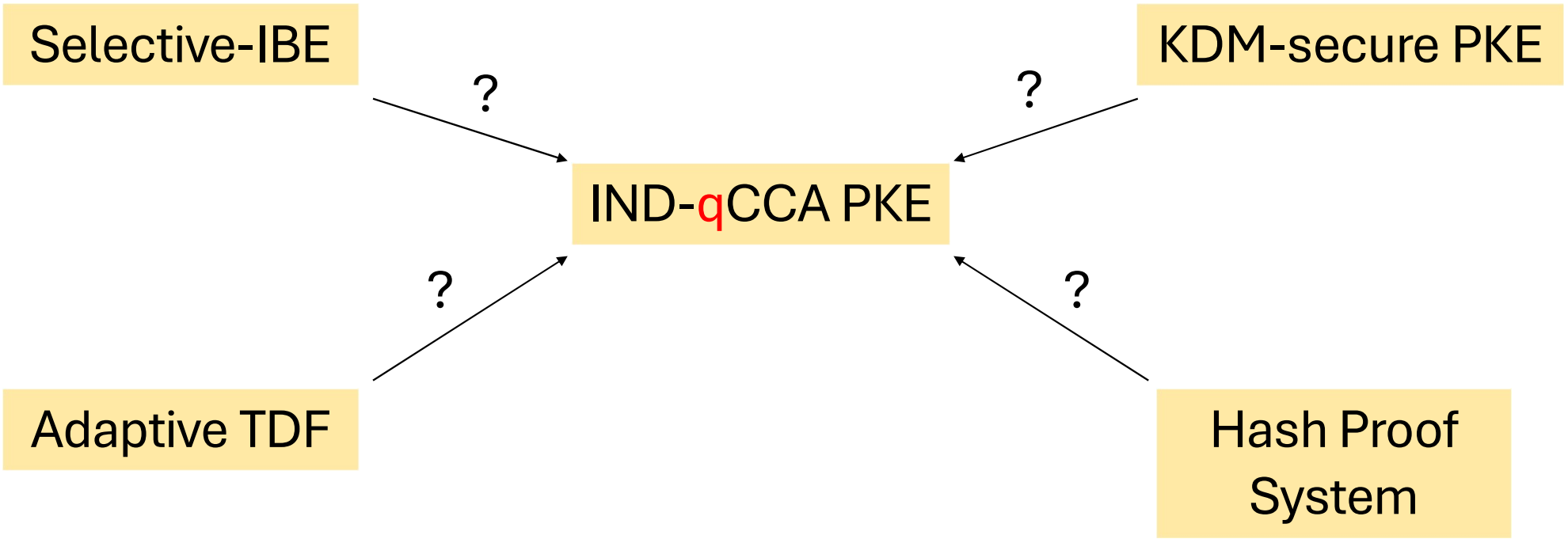
Motivation



Motivation

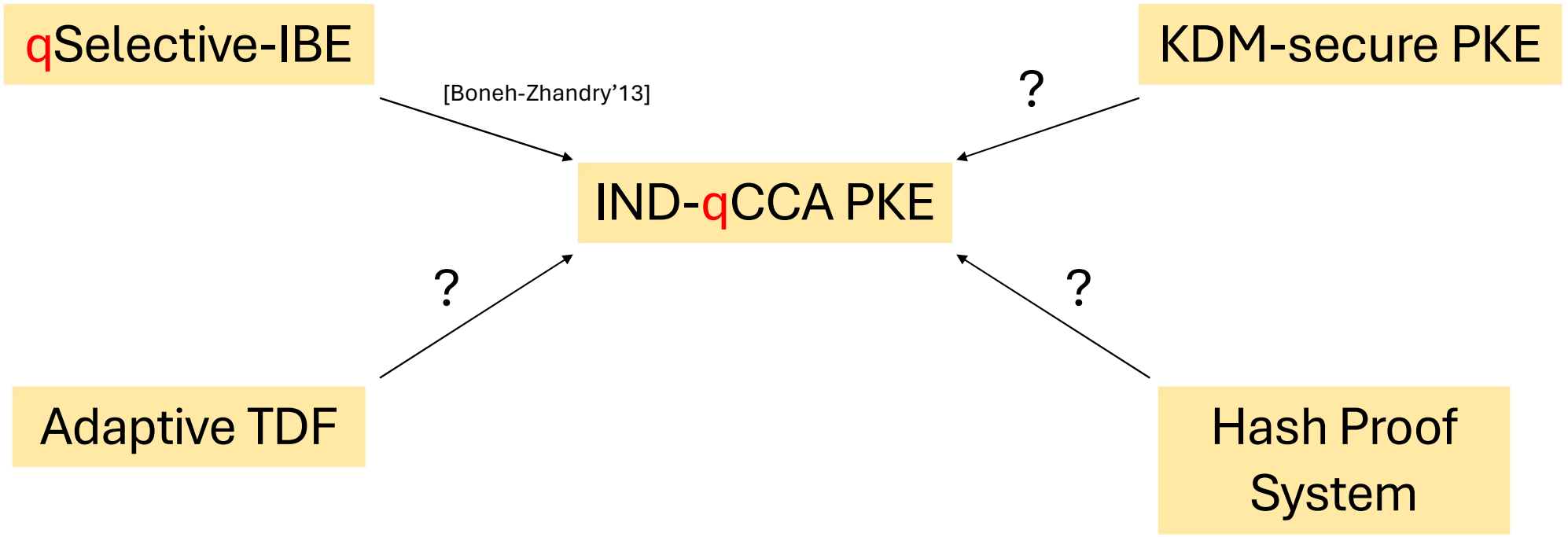

Key-Dependent Message.
Selective-IBE
[Boneh-Canetti-Halevi-Katz'04]
KDM-secure PKE
[Kitagawa-Matsuda-Tanaka'19]
IND-CCA PKE
[Kiltz-Mohassel-O'Neill'10]
[Cramer-Shoup'02]
Adaptive TDF
Hash Proof System

Motivation


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

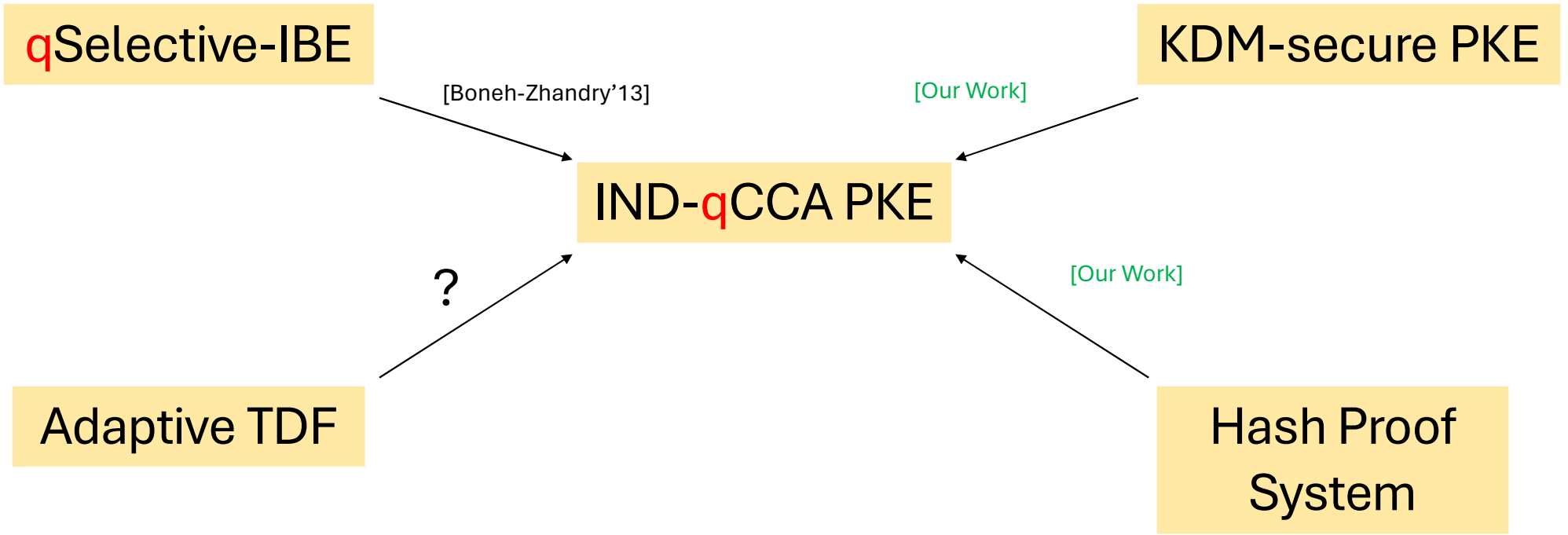
Motivation

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

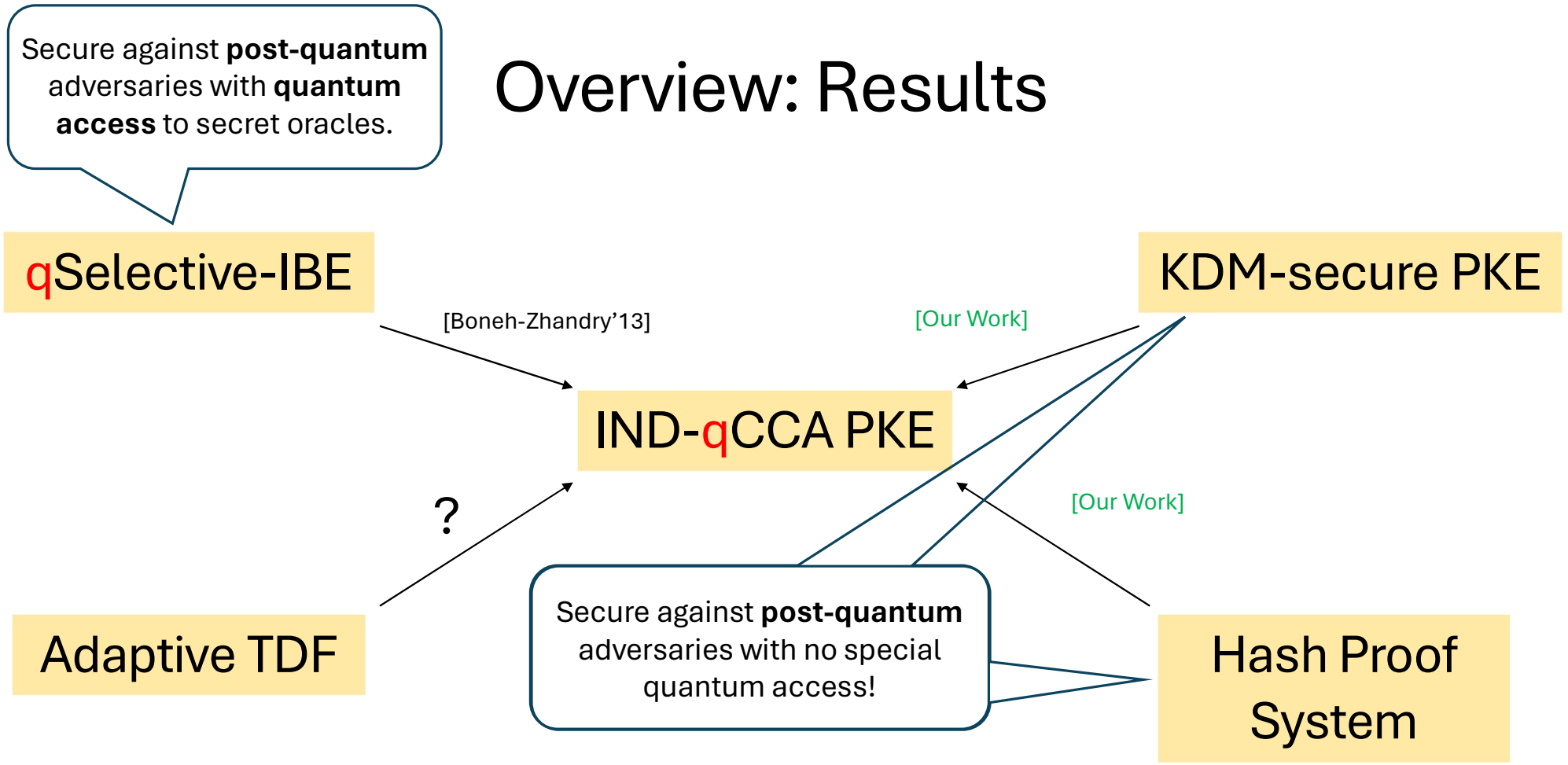


Overview: Results

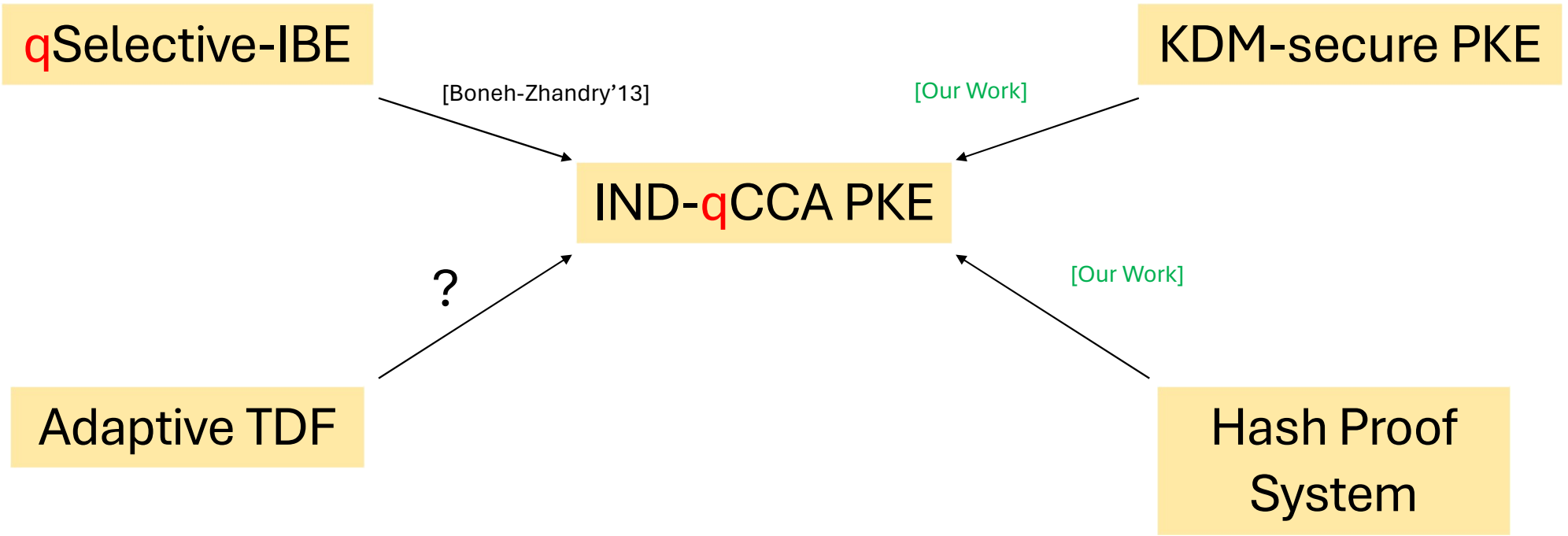
Secure against **post-quantum** adversaries with **quantum access** to secret oracles.



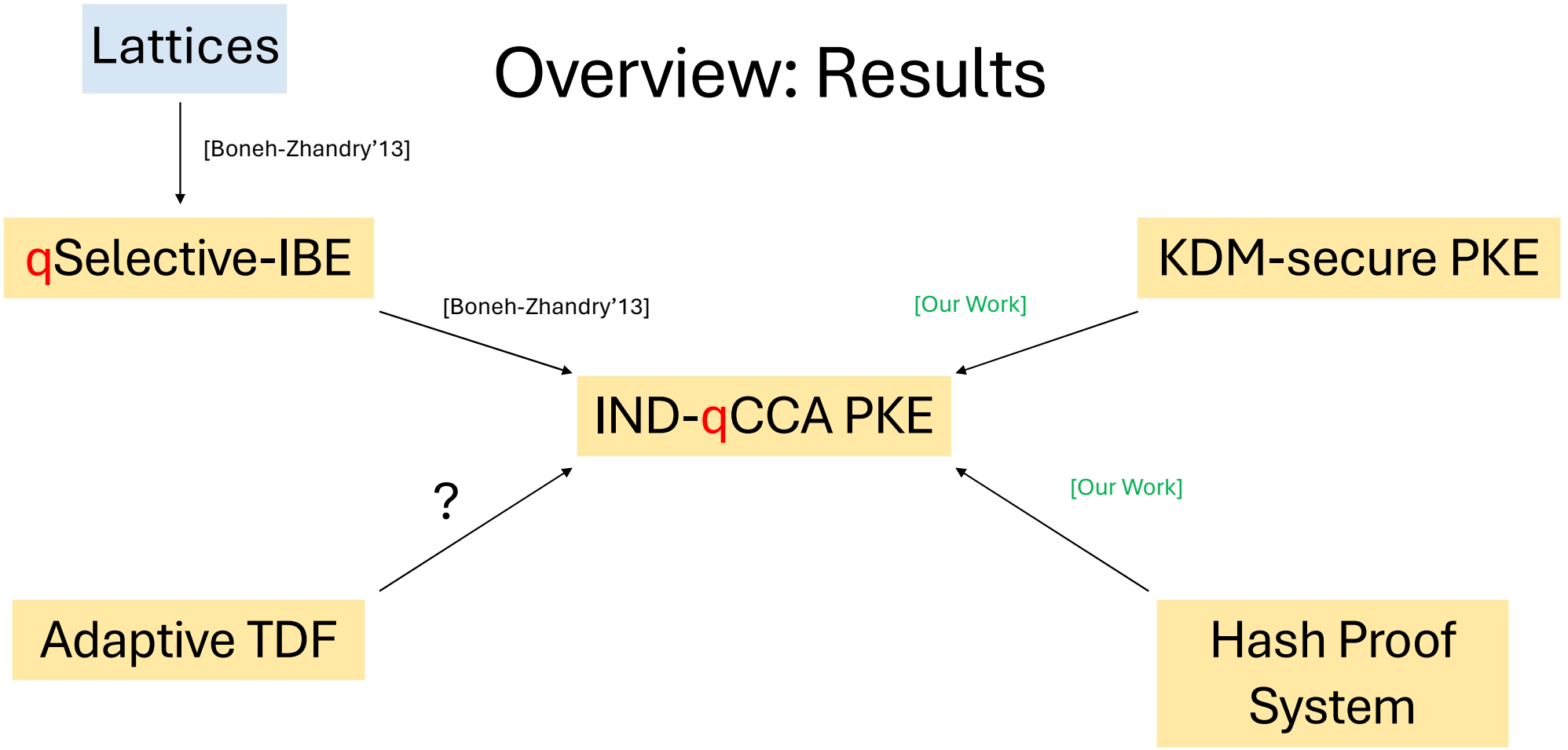
Overview: Results



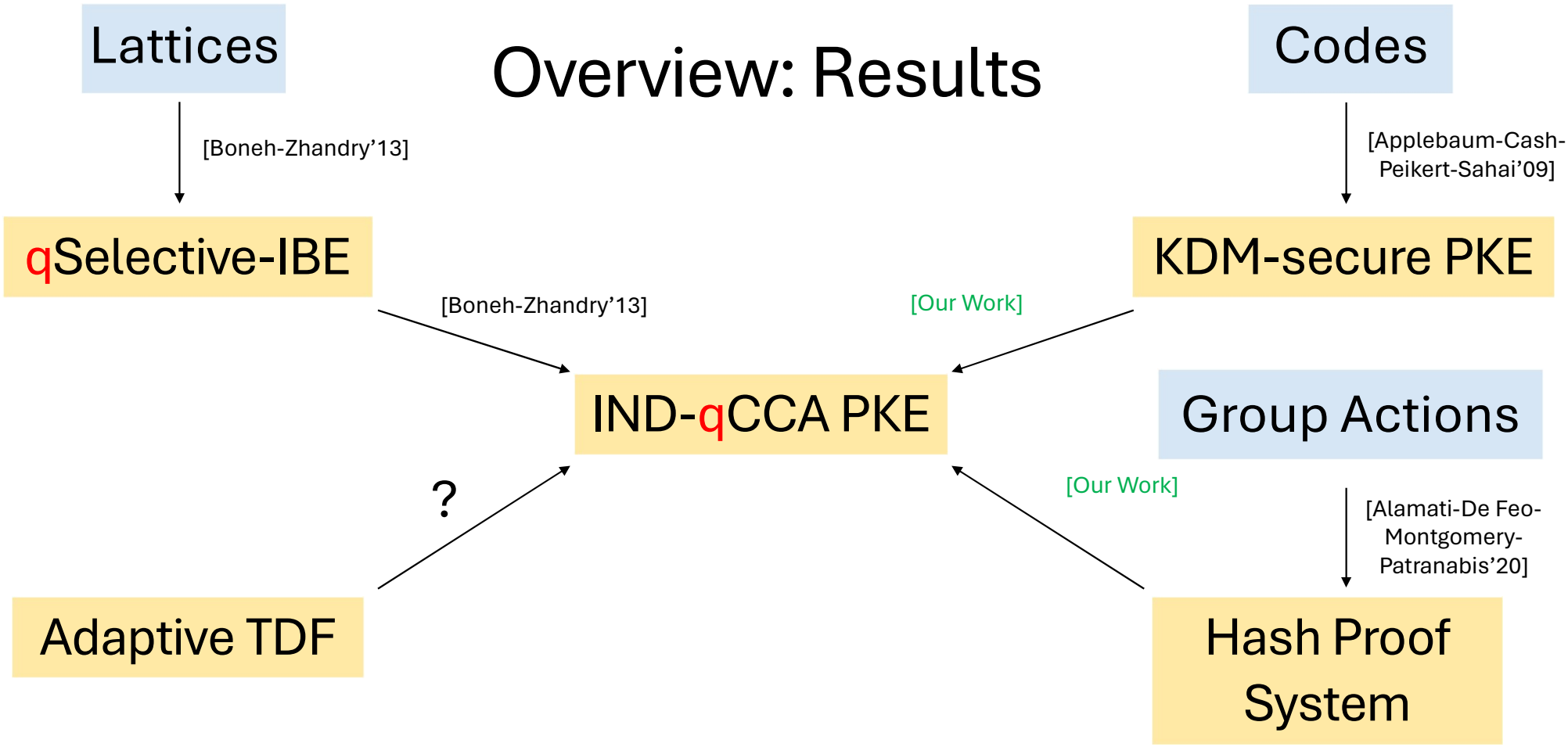
Overview: Results



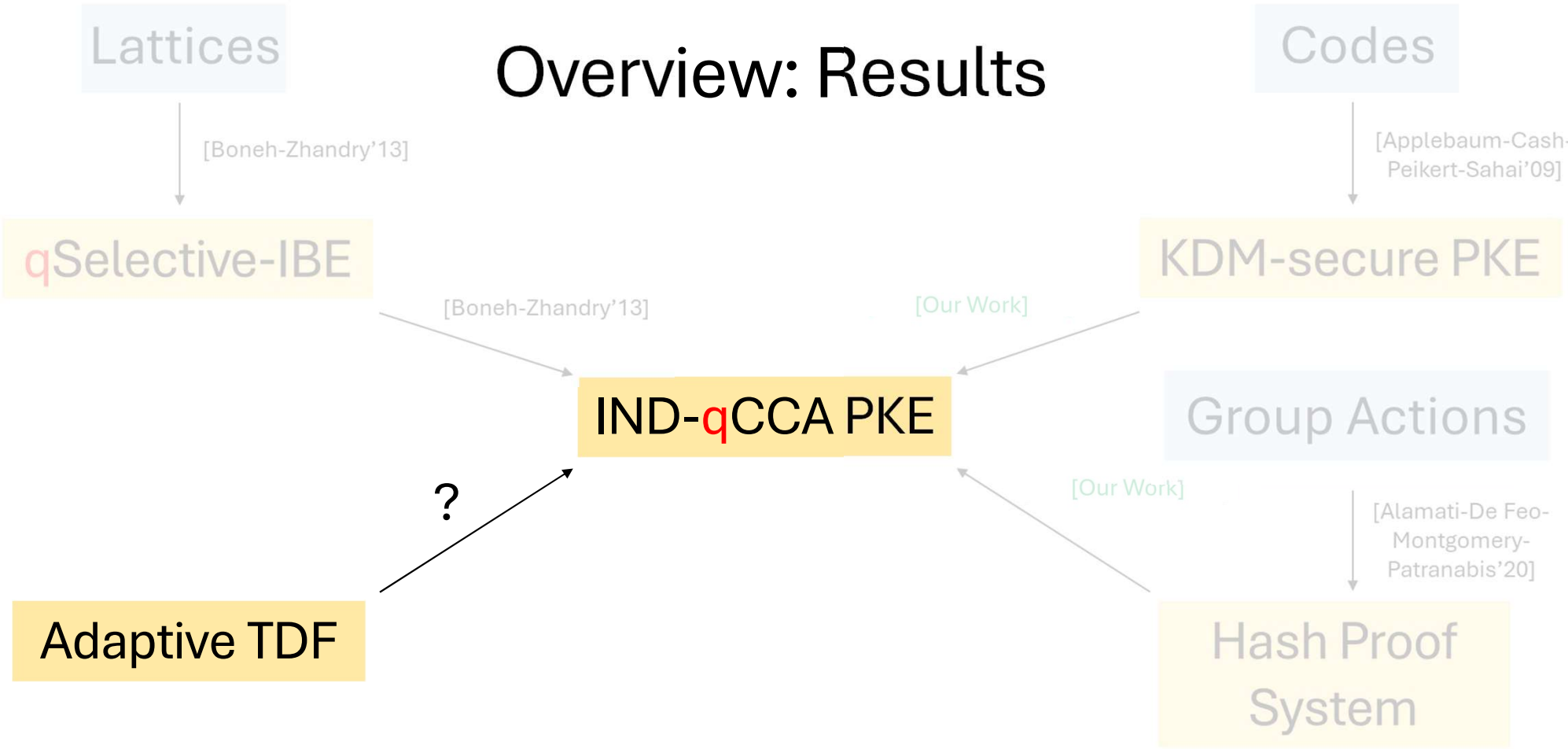
Overview: Results



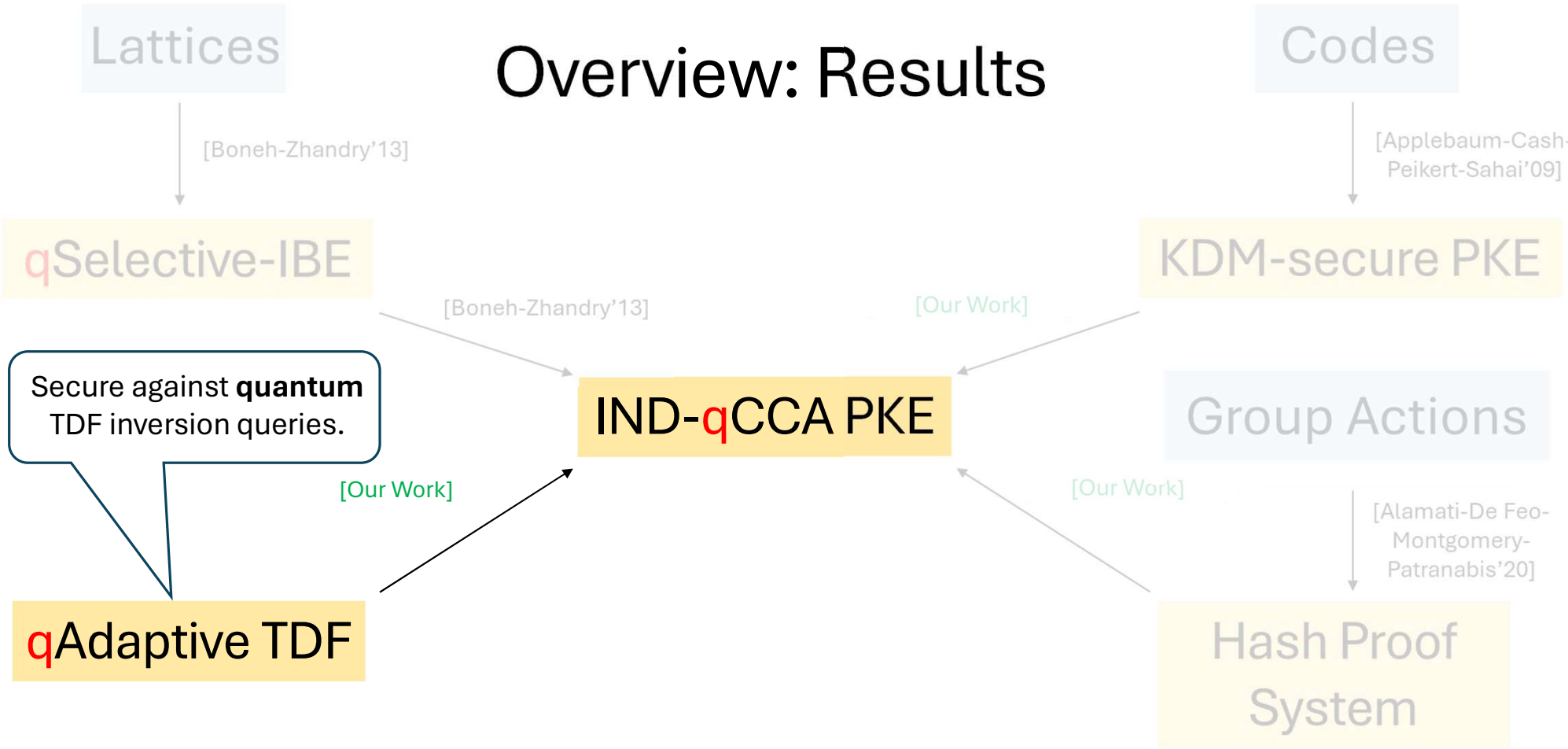
Overview: Results



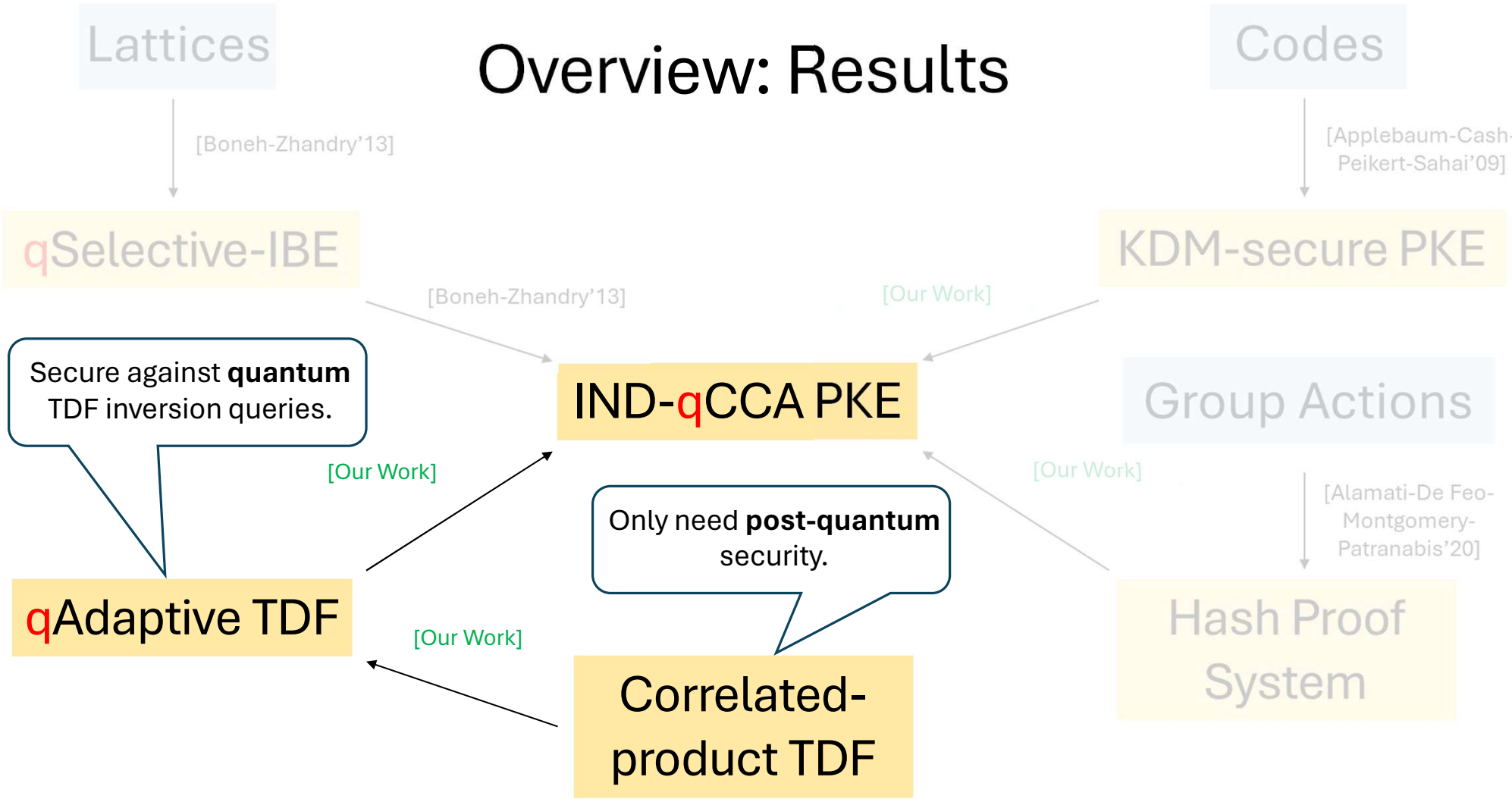
Overview: Results



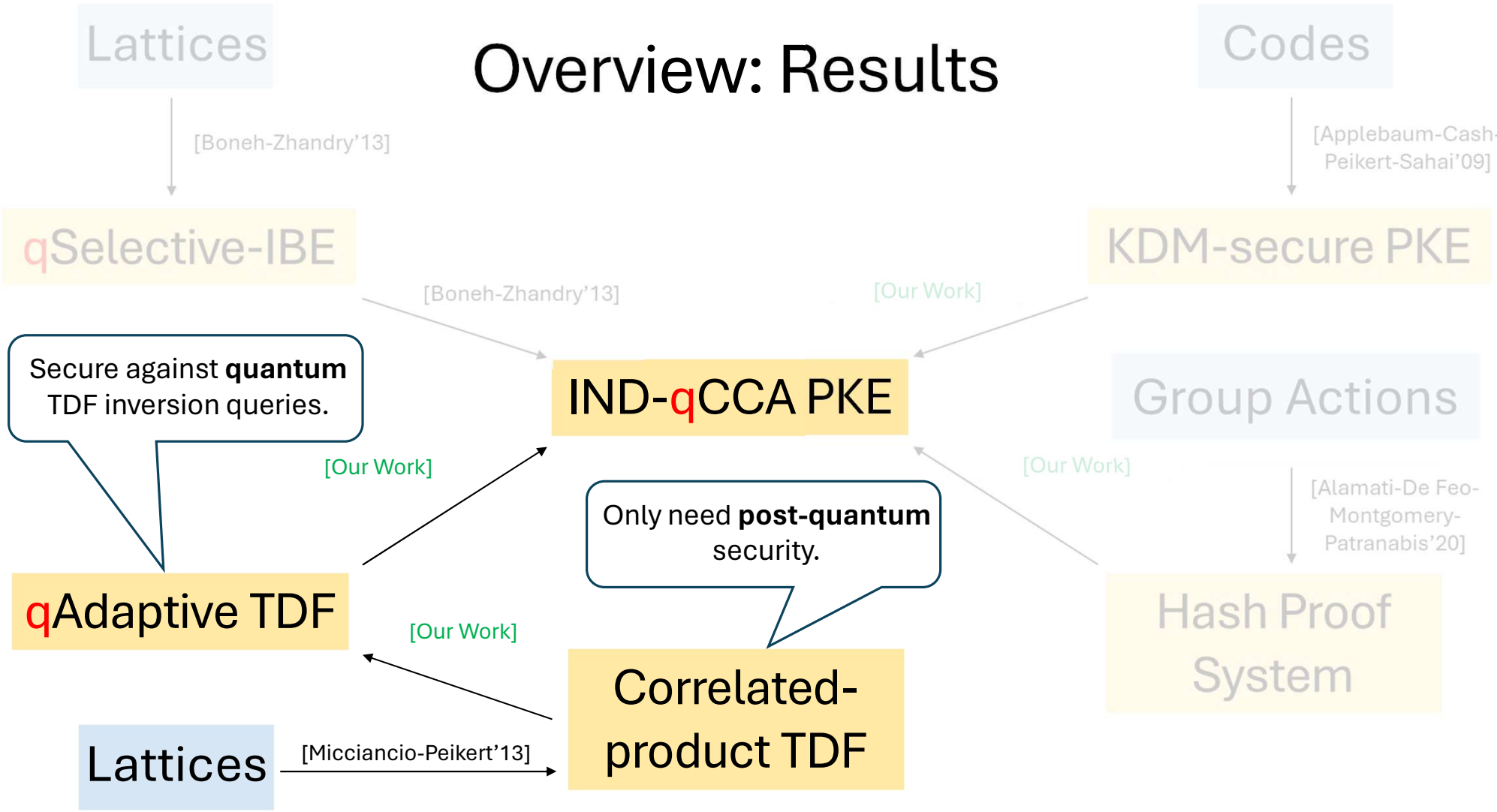
Overview: Results



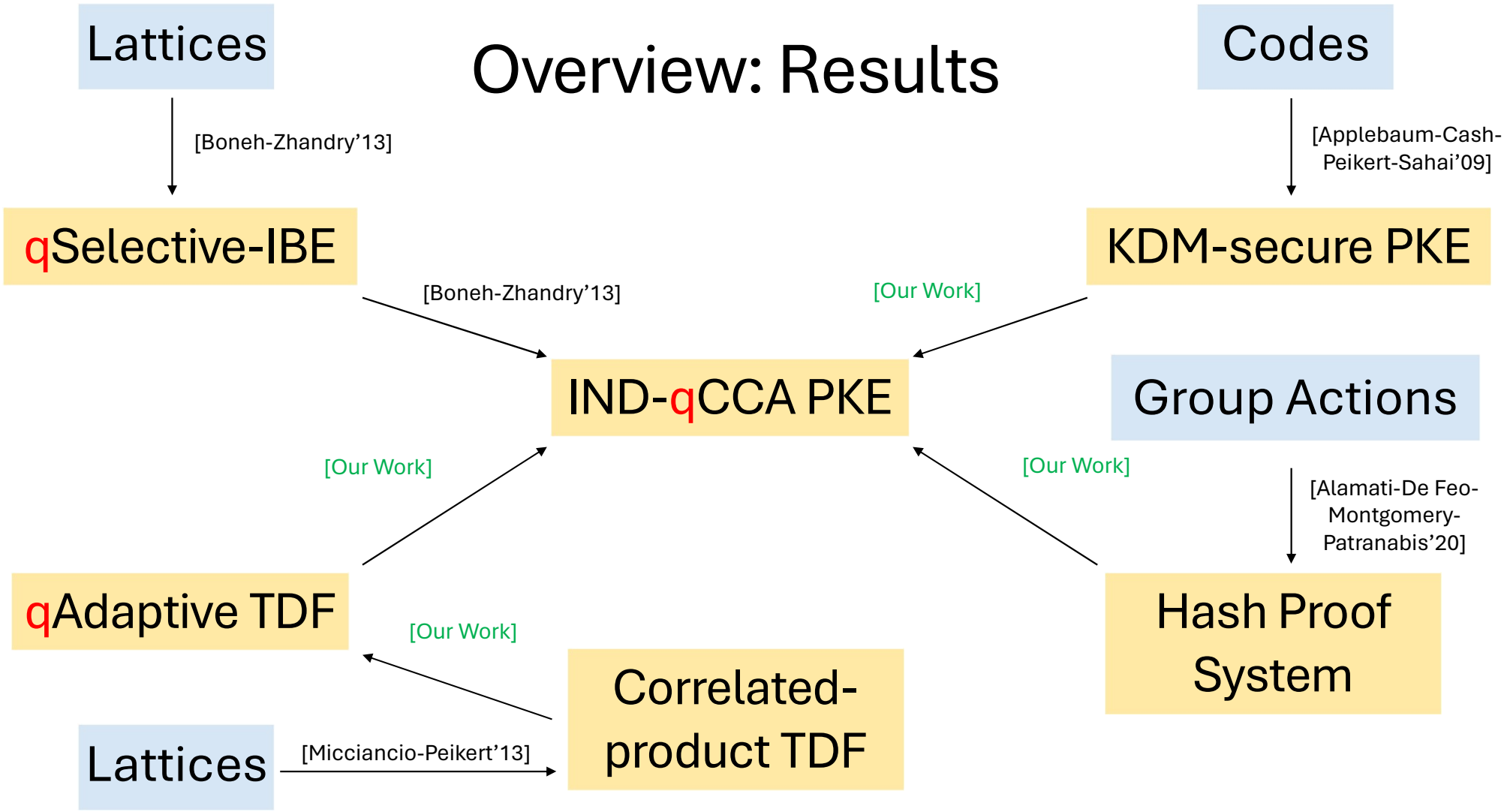
Overview: Results



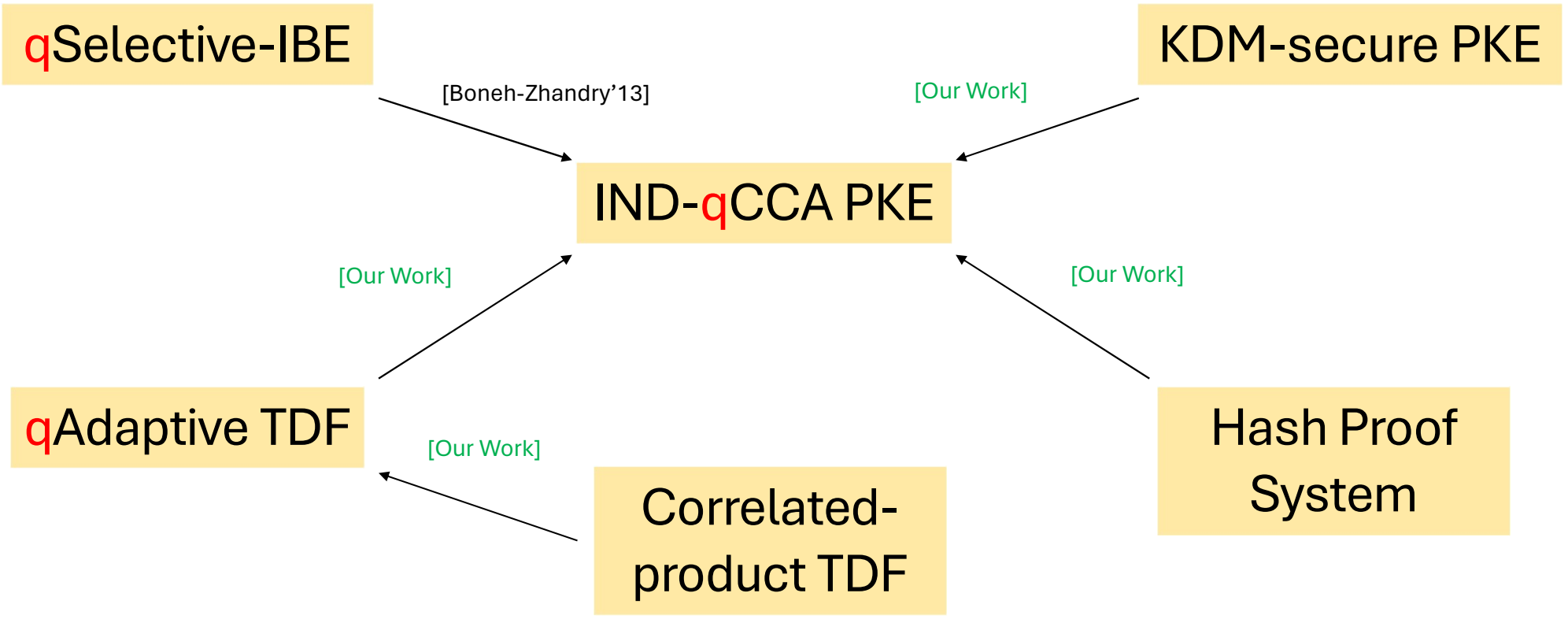
Overview: Results



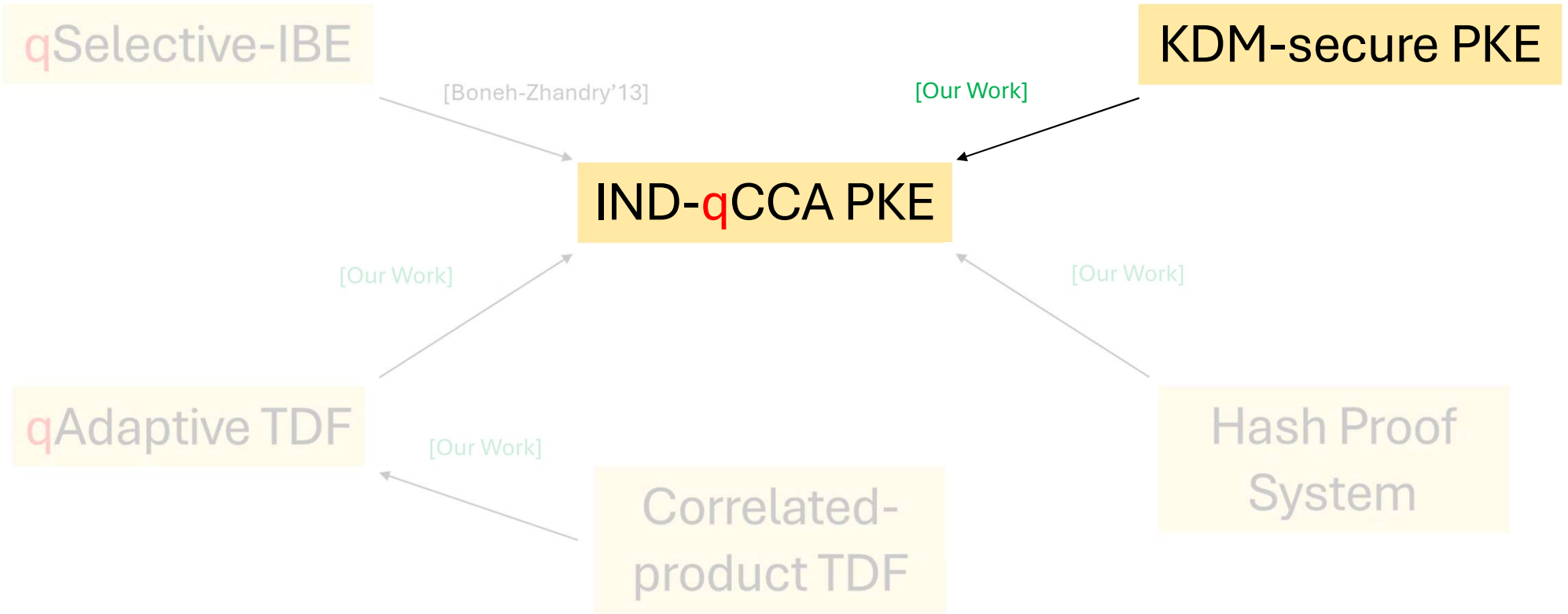
Overview: Results



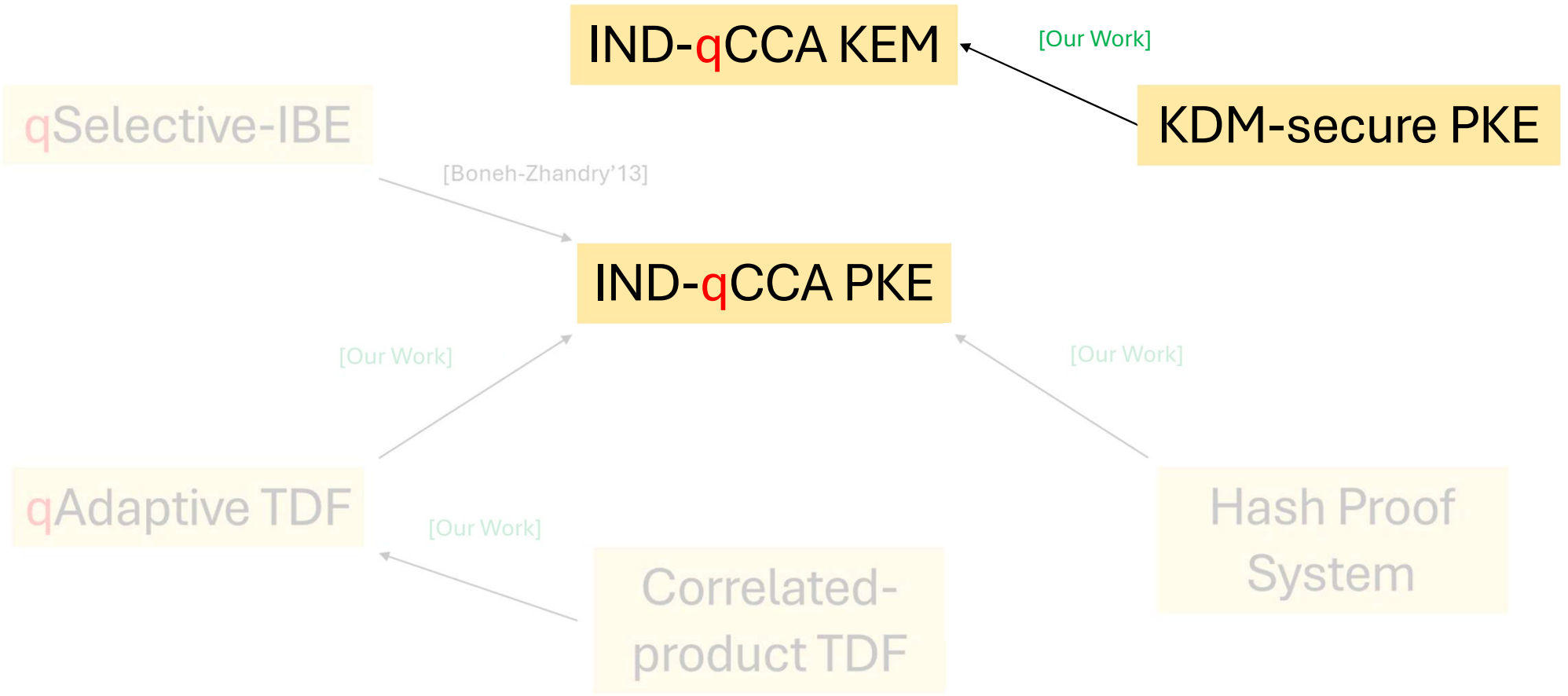
Overview: Results



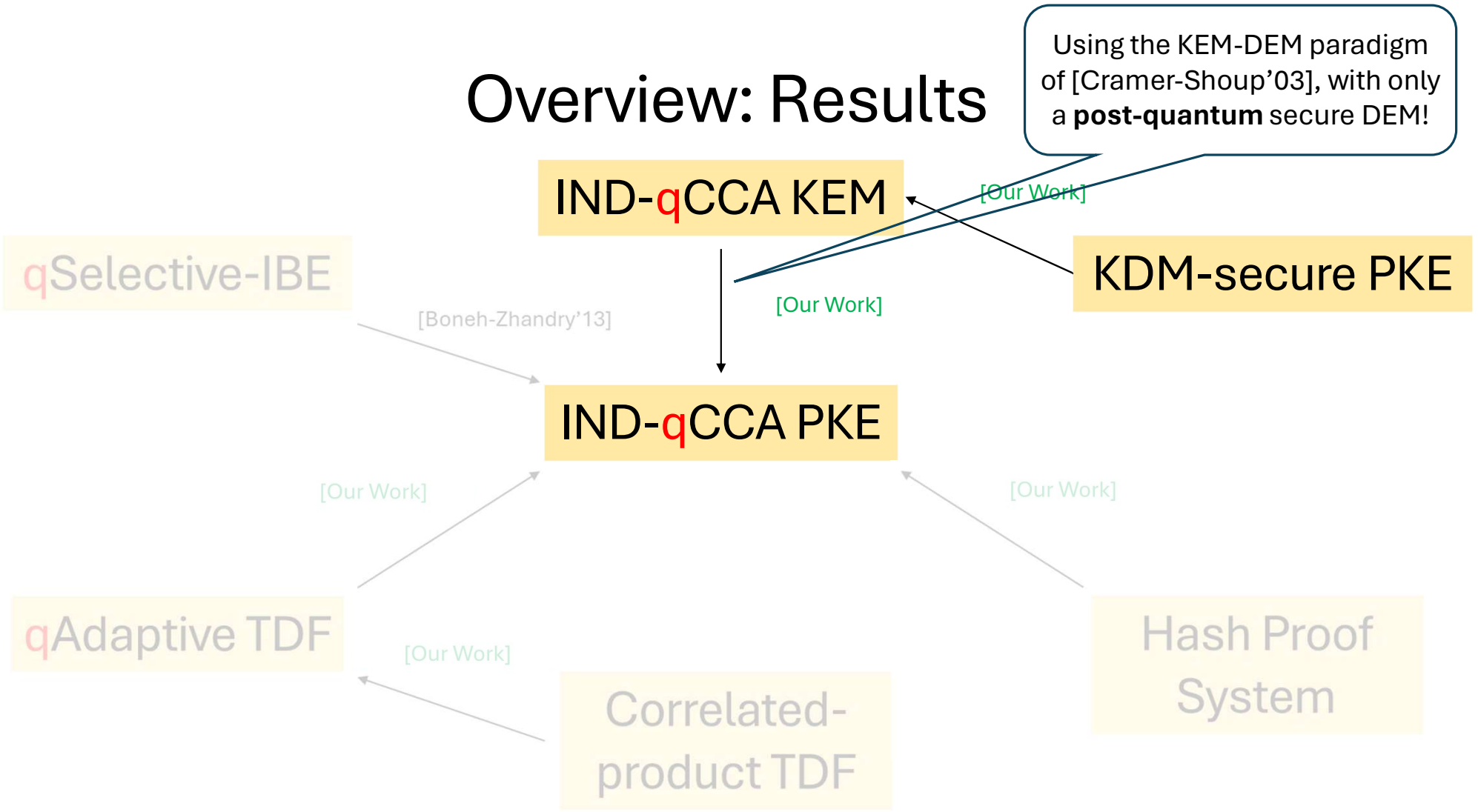
Overview: Results



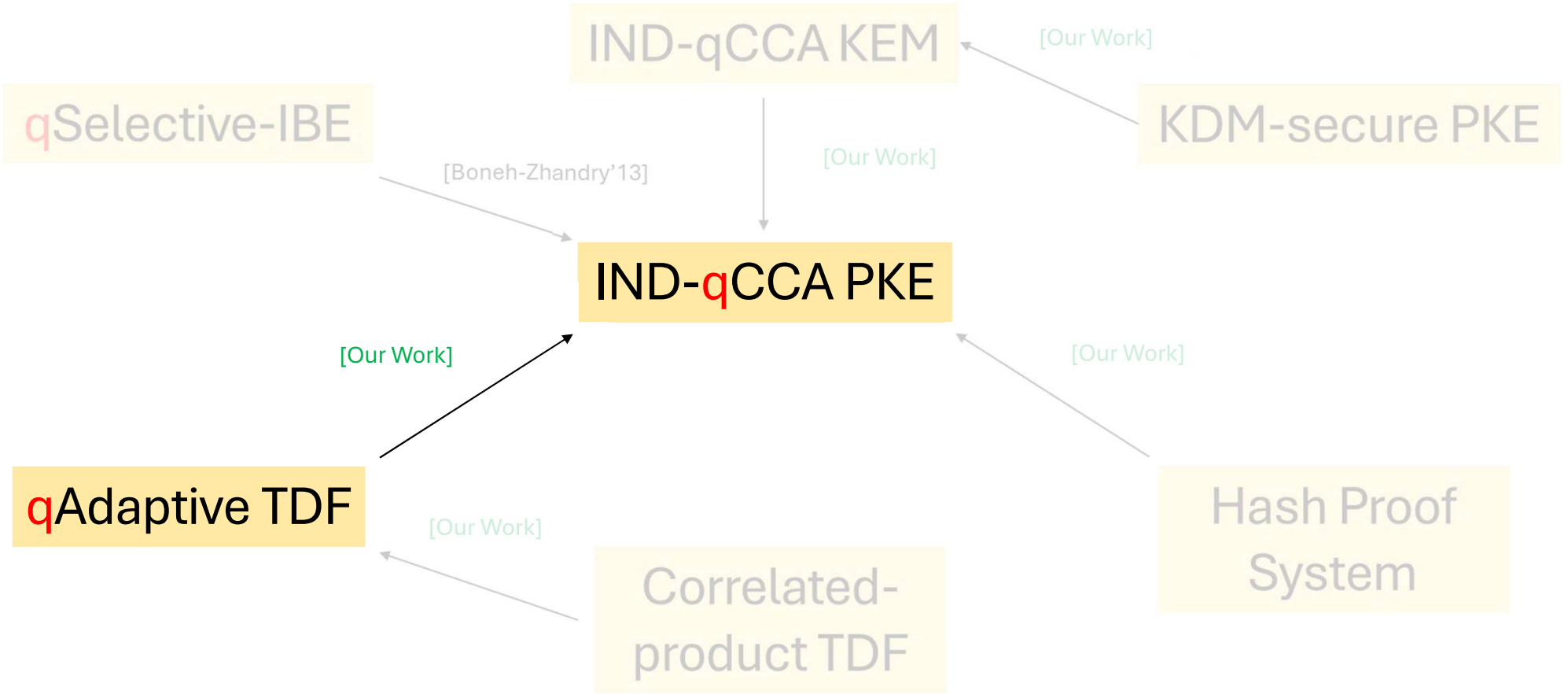
Overview: Results



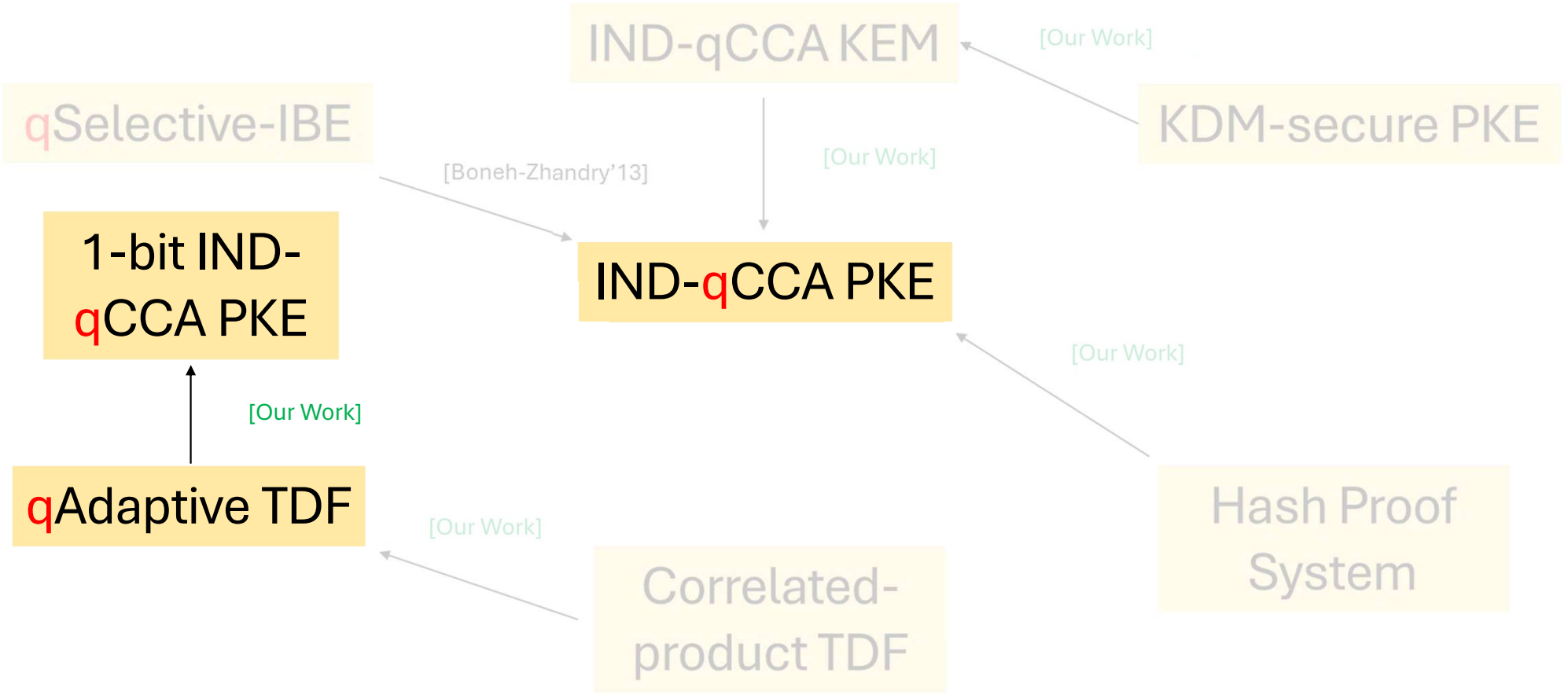
Overview: Results



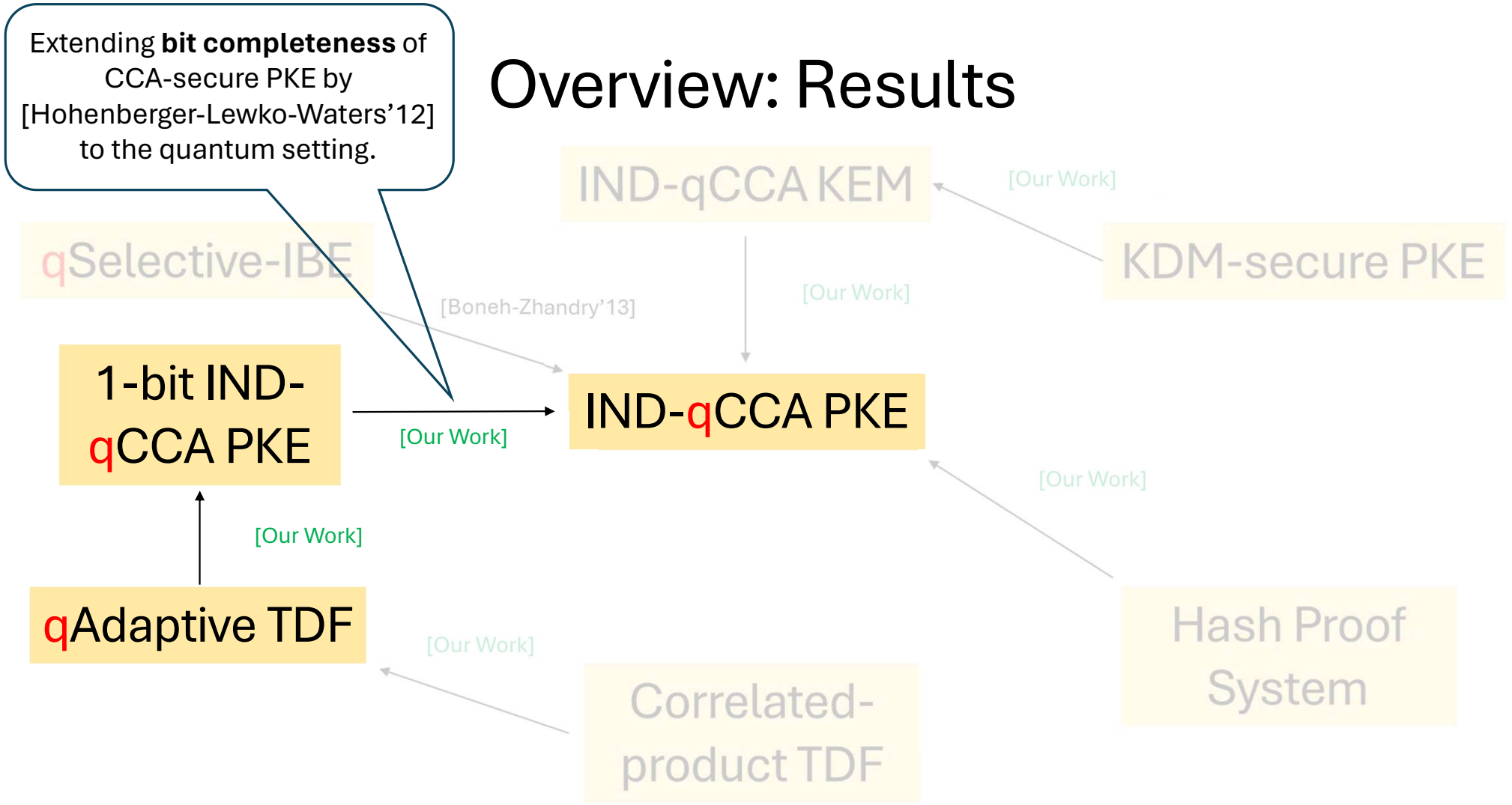
Overview: Results



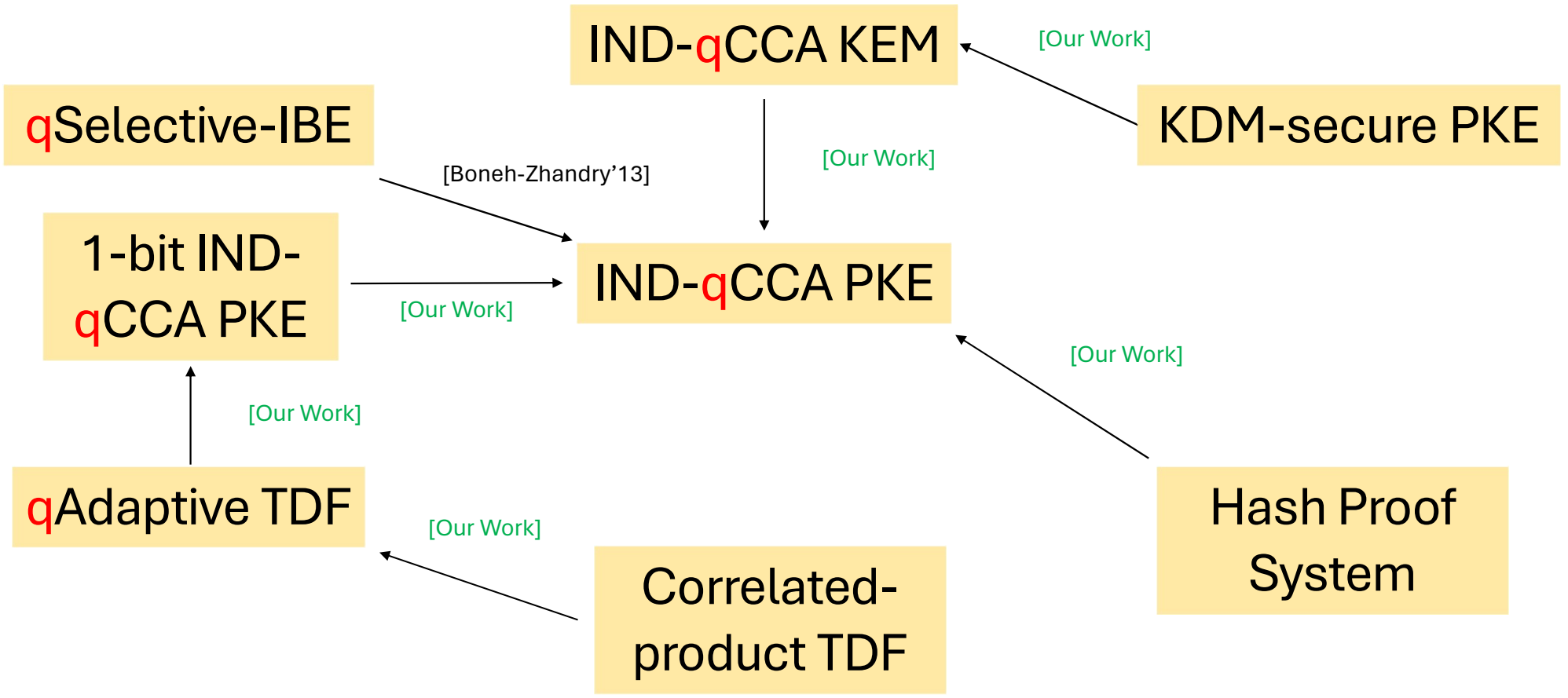
Overview: Results



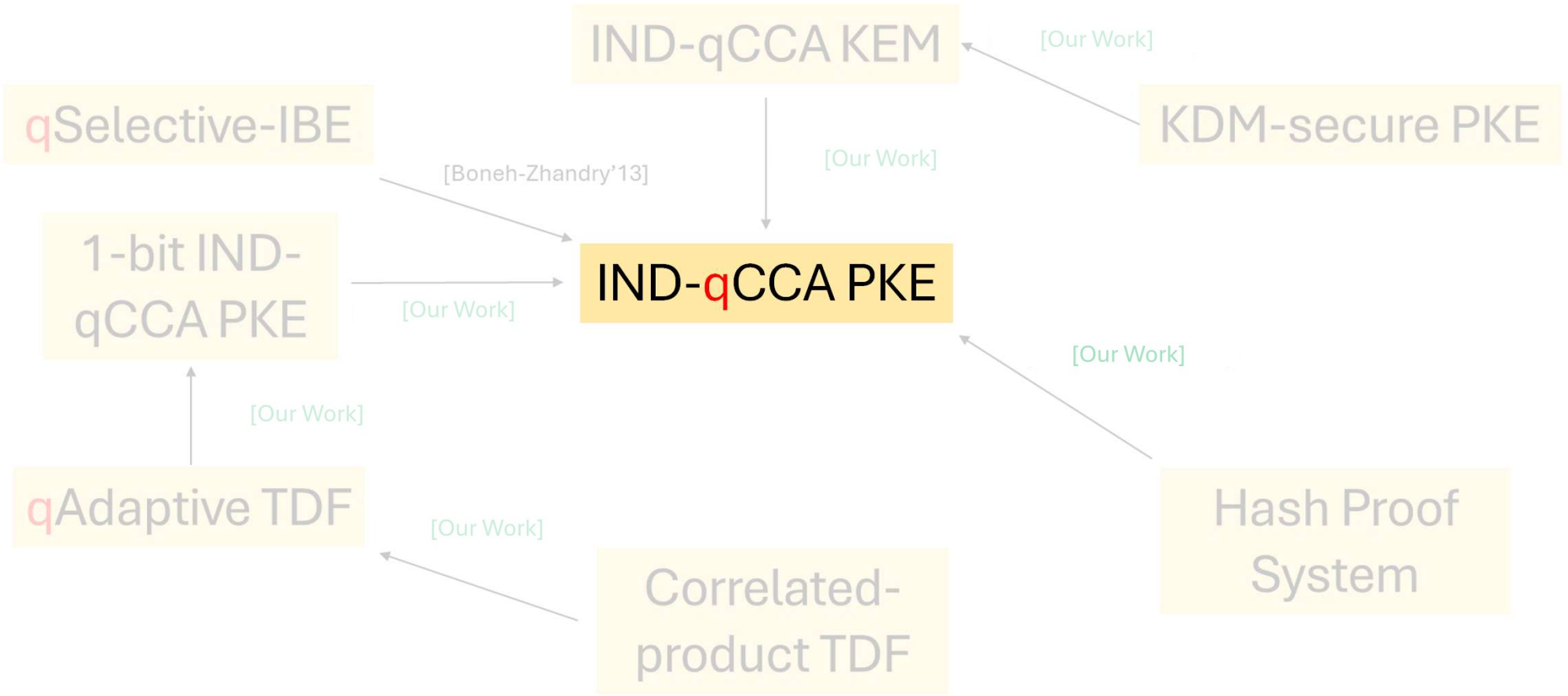
Overview: Results



Overview: Results



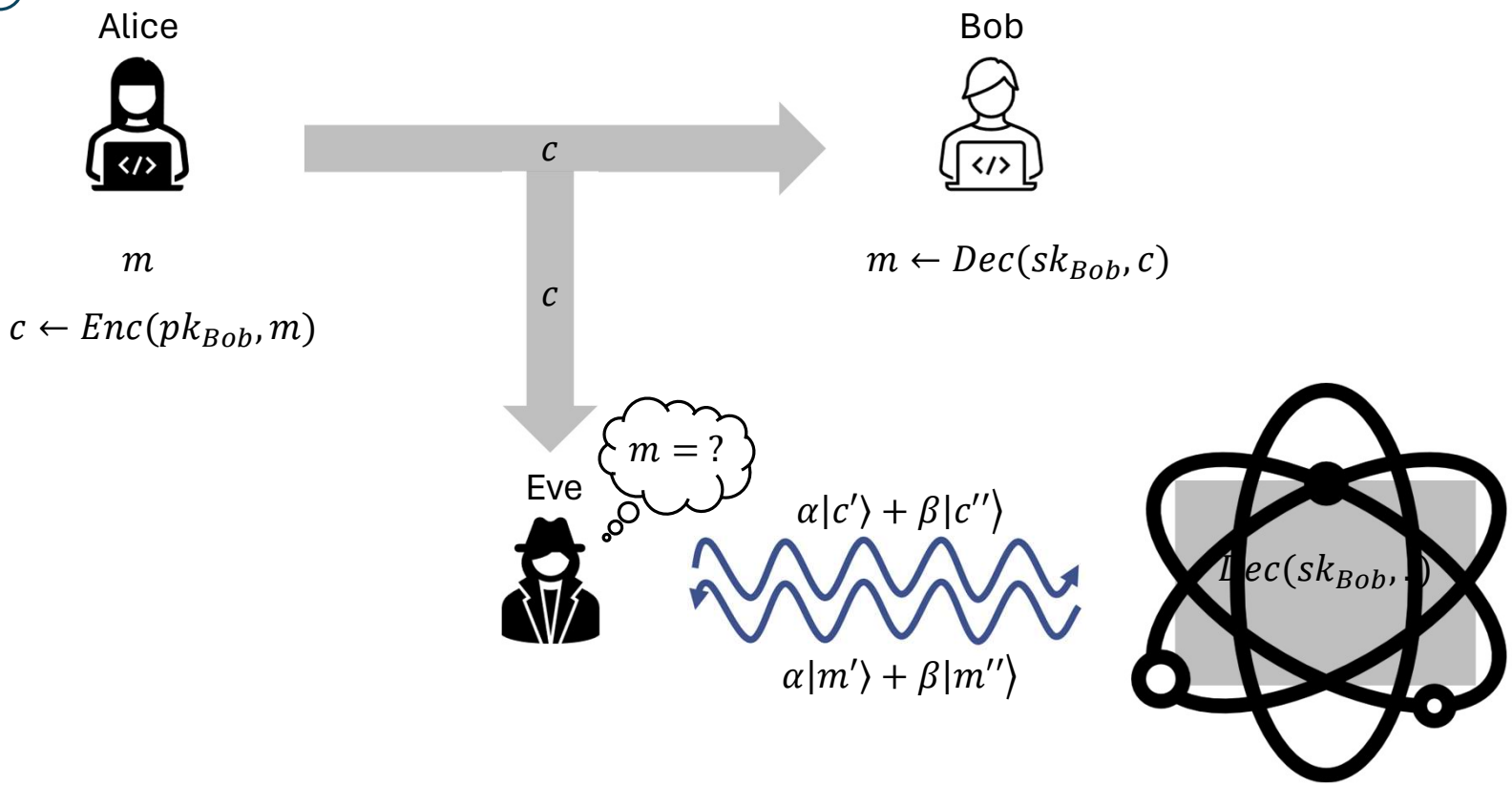
Overview: Results



IND-qCCA Security

Introduced by [Boneh-Zhandry'13].

$PKE = (KGen, Enc, Dec)$



IND-qCCA Security

Introduced by [Boneh-Zhandry'13].

$PKE = (KGen, Enc, Dec)$

Alice

m

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

c

Bob

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

c

Notion restricted to **classical** challenge messages.

$m = ?$

Eve

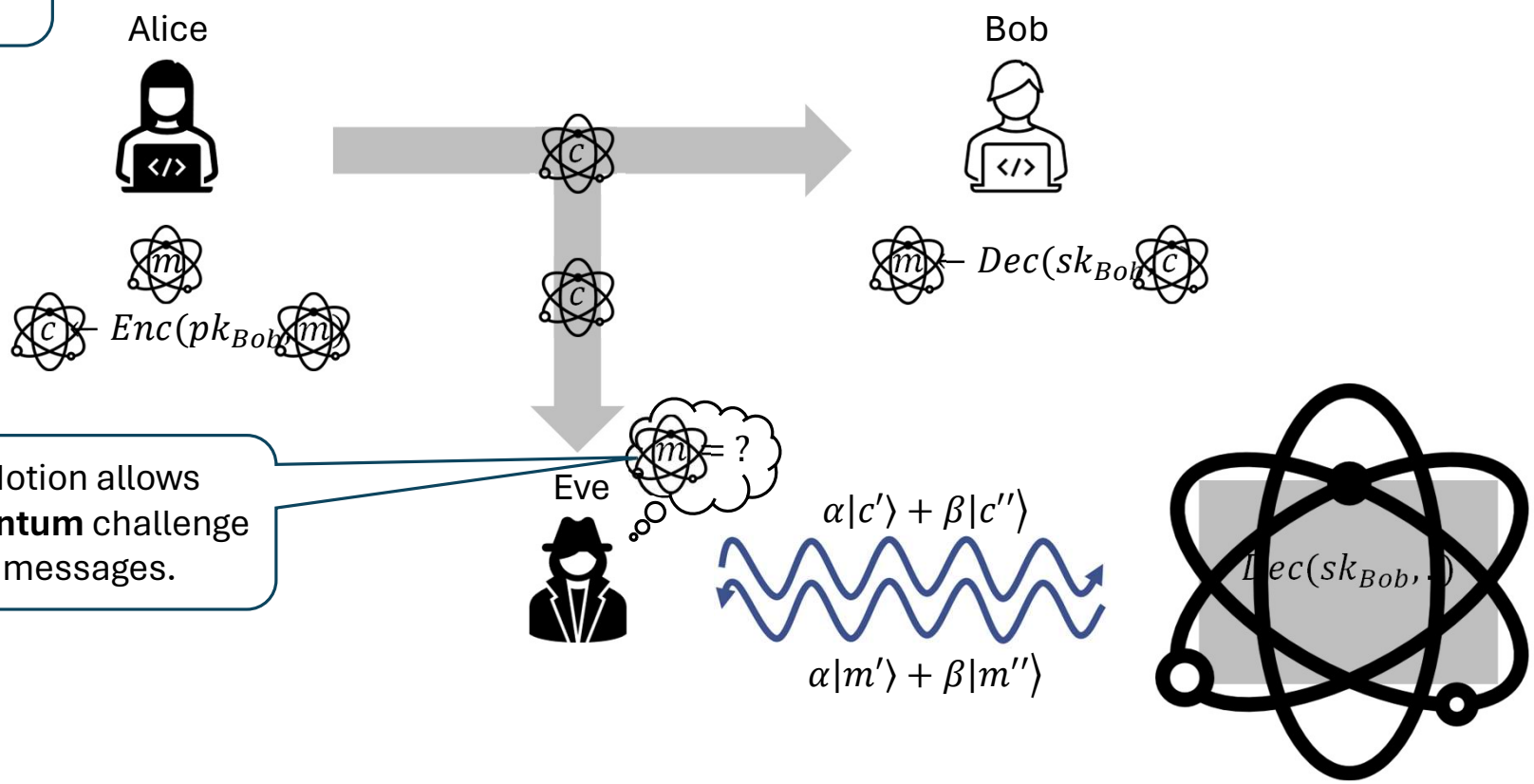
$\alpha|c'\rangle + \beta|c''\rangle$

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

qIND-qCCA Security

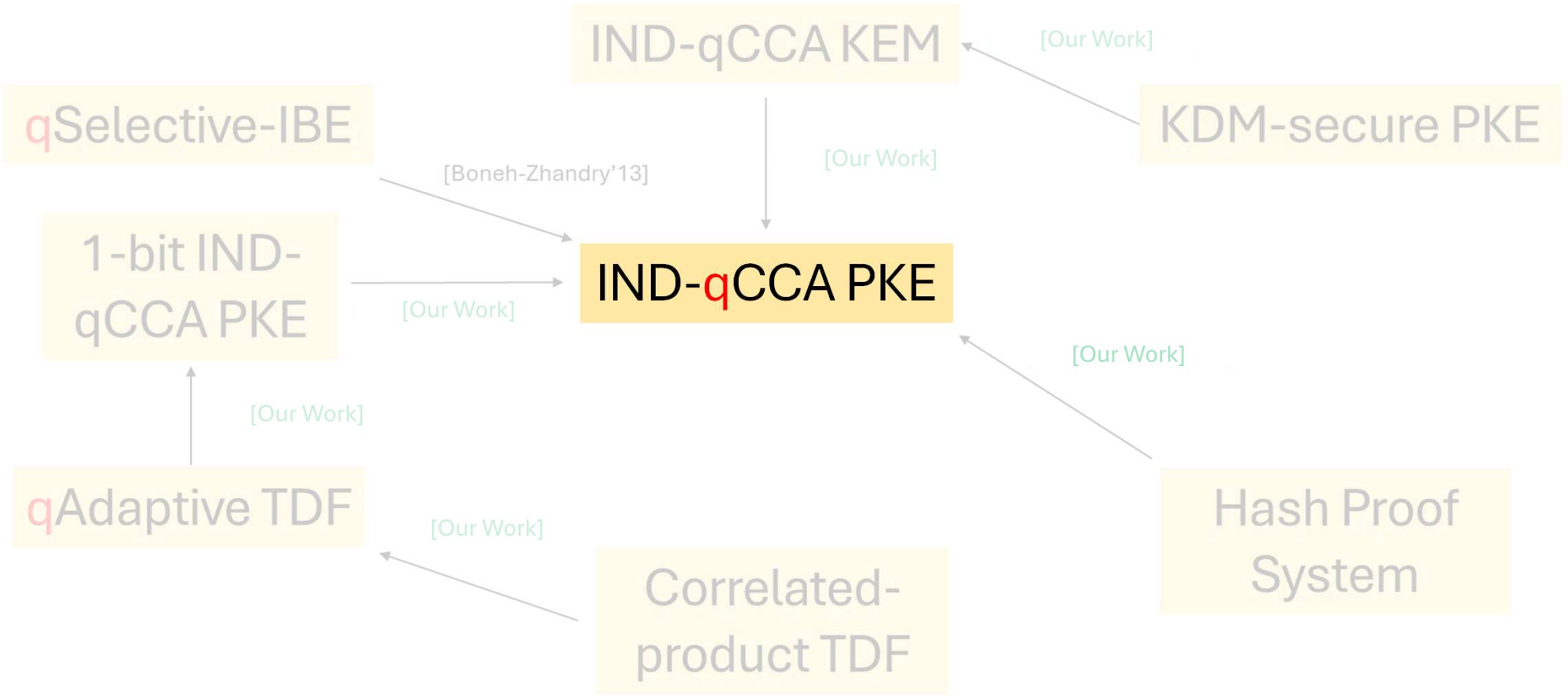
Introduced by [Chevalier-Ebrahimi-Vu'22].

$PKE = (KGen, Enc, Dec)$

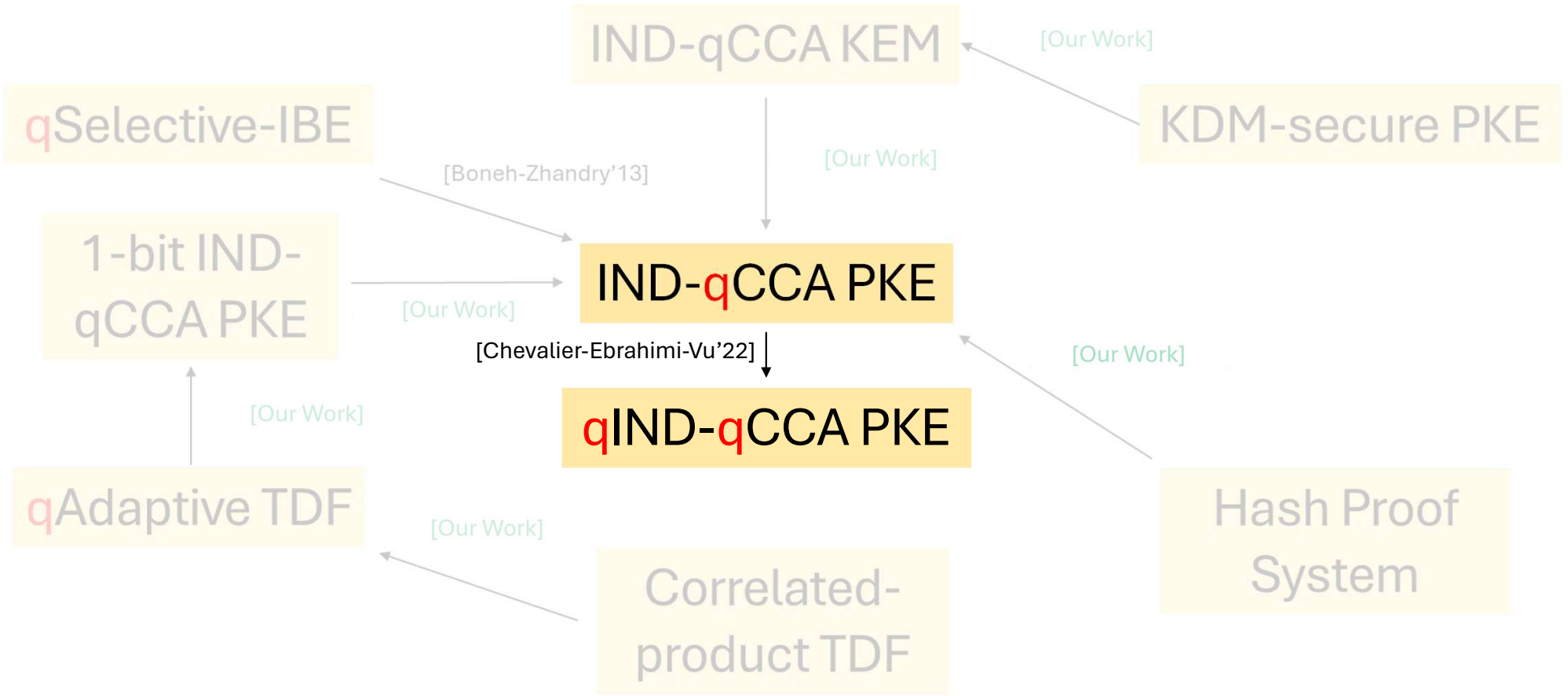


Notion allows **quantum** challenge messages.

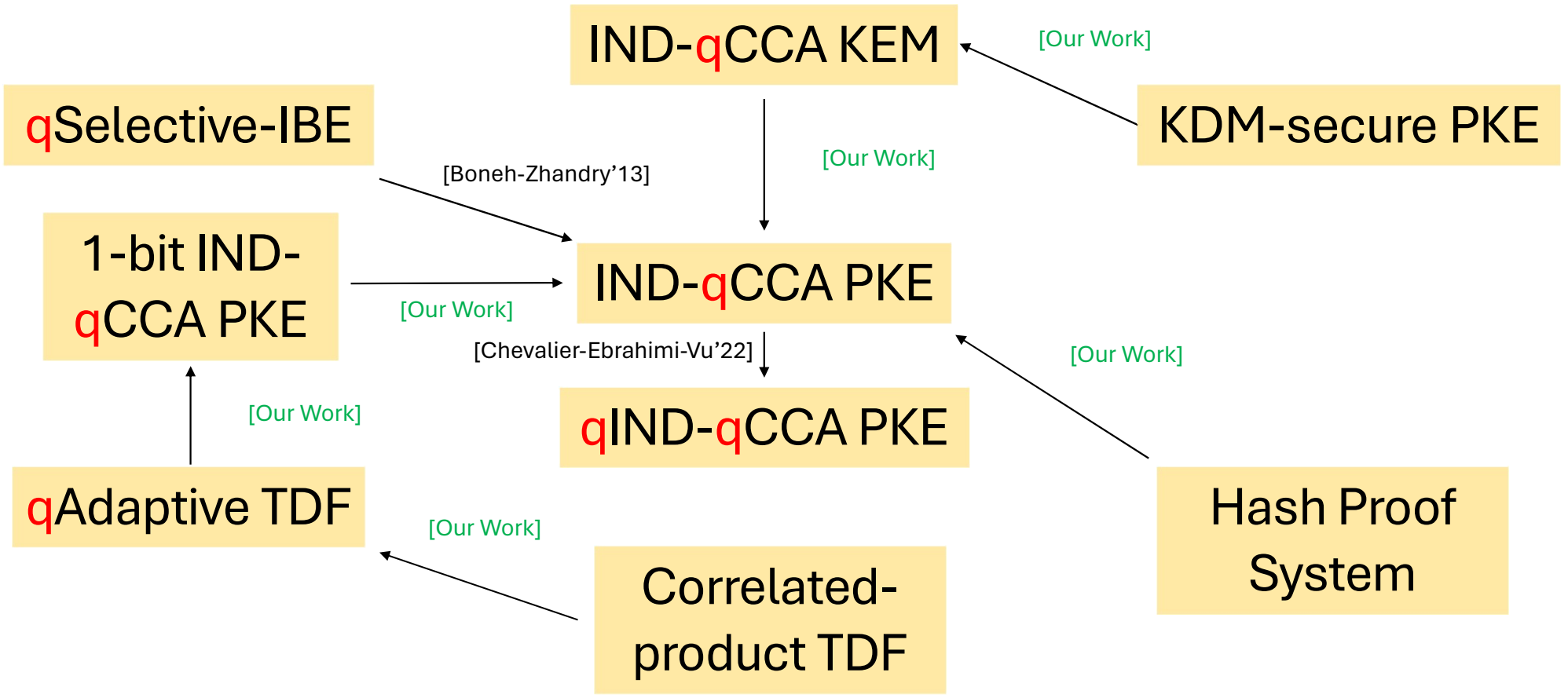
Overview: Results

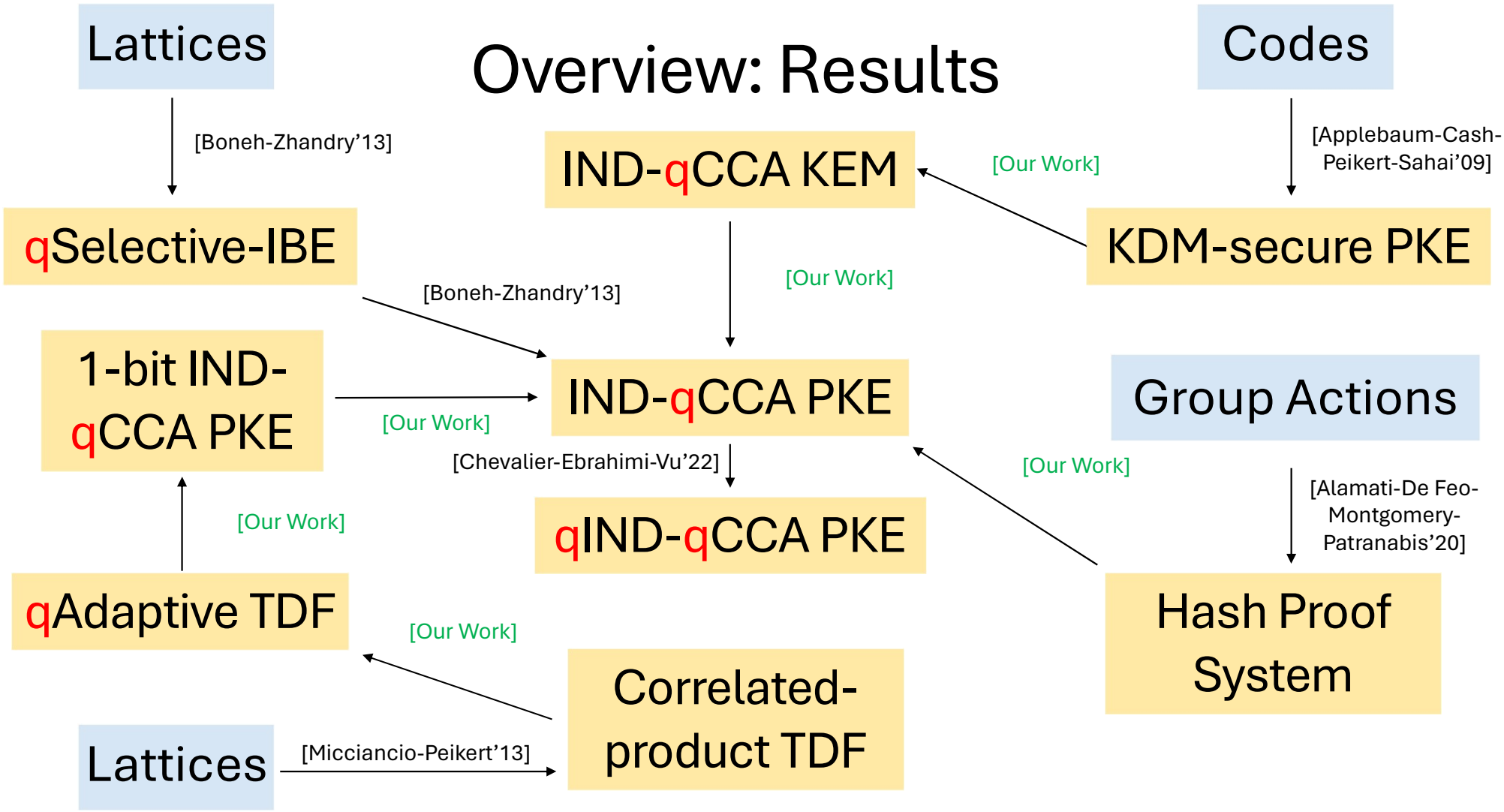


Overview: Results



Overview: Results




Overview: Results
Lattices
[Boneh-Zhandry'13]
qSelective-IBE
Codes
[Applebaum-Cash-Peikert-Sahai'09]
IND-qCCA KEM
[Our Work]
KDM-secure PKE
[Our Work]
[Boneh-Zhandry'13]
1-bit IND-qCCA PKE
[Our Work]
IND-qCCA PKE
Group Actions
[Chevalier-Ebrahimi-Vu'22]
qIND-qCCA PKE
[Our Work]
[Alamati-De Feo-Montgomery-Patranabis'20]
[Our Work]
qAdaptive TDF
Hash Proof System
[Our Work]
Correlated-product TDF
Lattices
[Micciancio-Peikert'13]

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**.

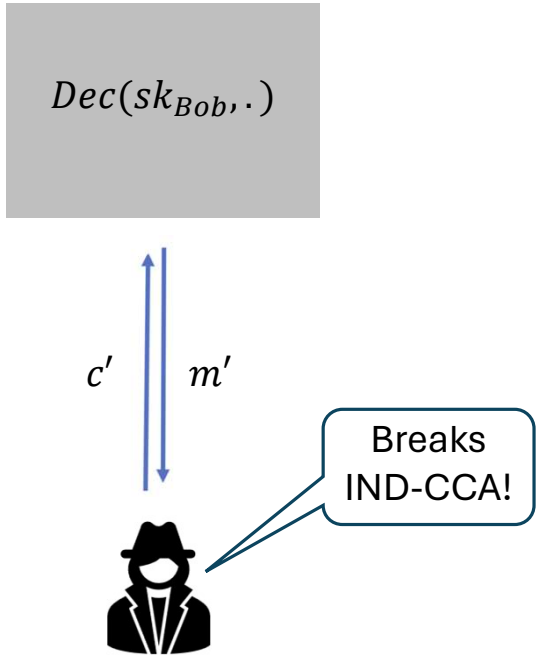
- They can be implemented on **classical computers**.
- As opposed to **quantum PKE schemes** (e.g., in [Barooti-Grilo-Huguenin(-)Dumittan-Malavolta-Sattath-Vu-Walter'23]) which need inherent quantum components, such as **quantum public keys**.

Overview: Techniques

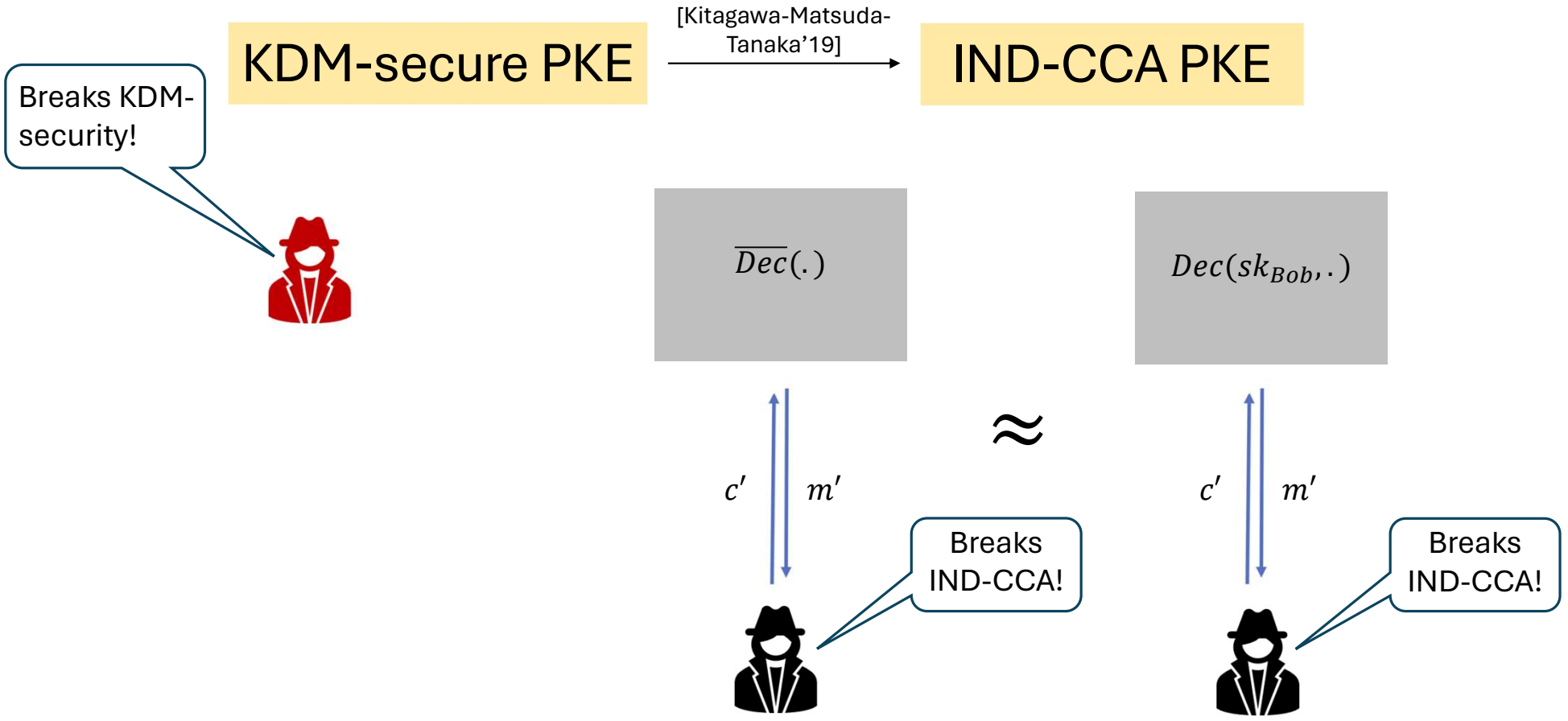
KDM-secure PKE → [Kitagawa-Matsuda-Tanaka'19] → IND-CCA PKE

Overview: Techniques

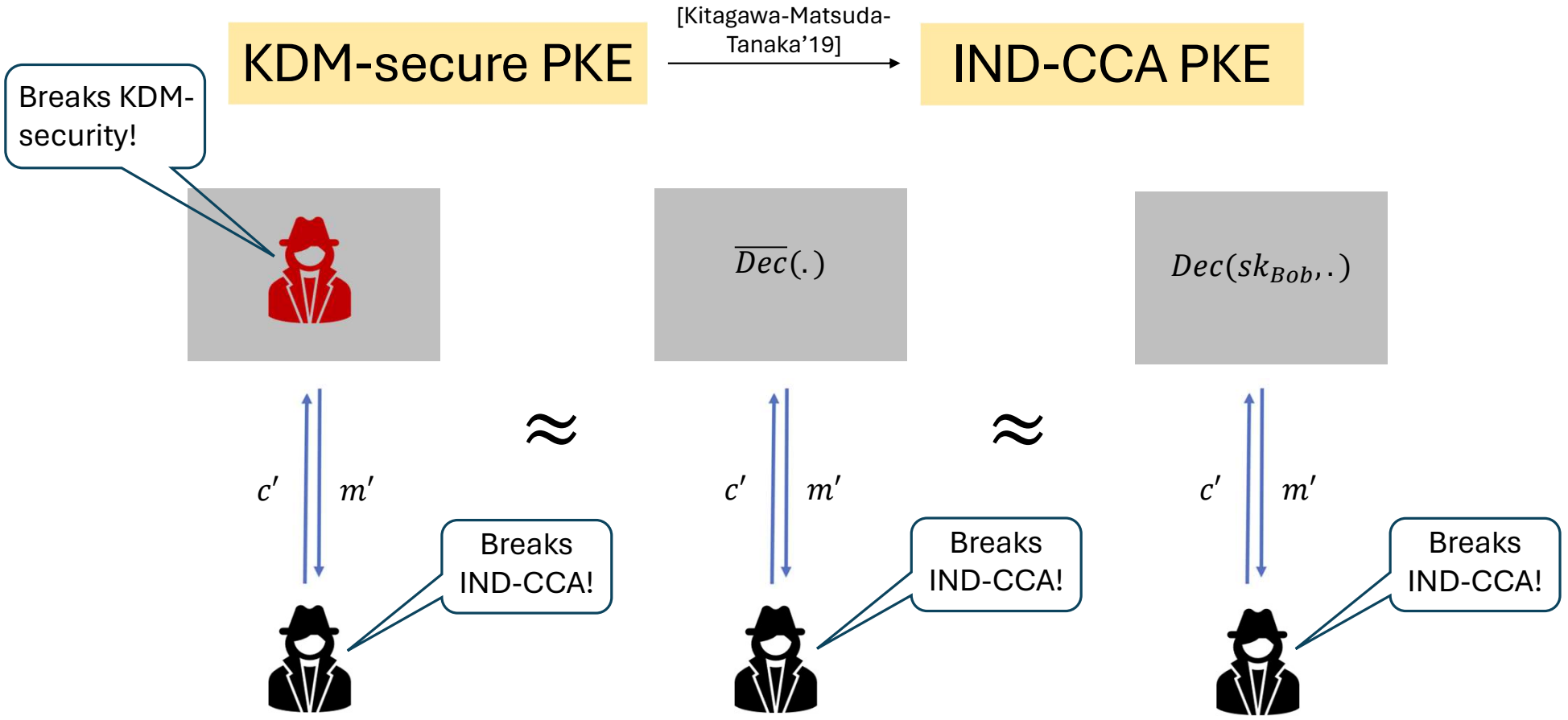
KDM-secure PKE → [Kitagawa-Matsuda-Tanaka'19] → IND-CCA PKE



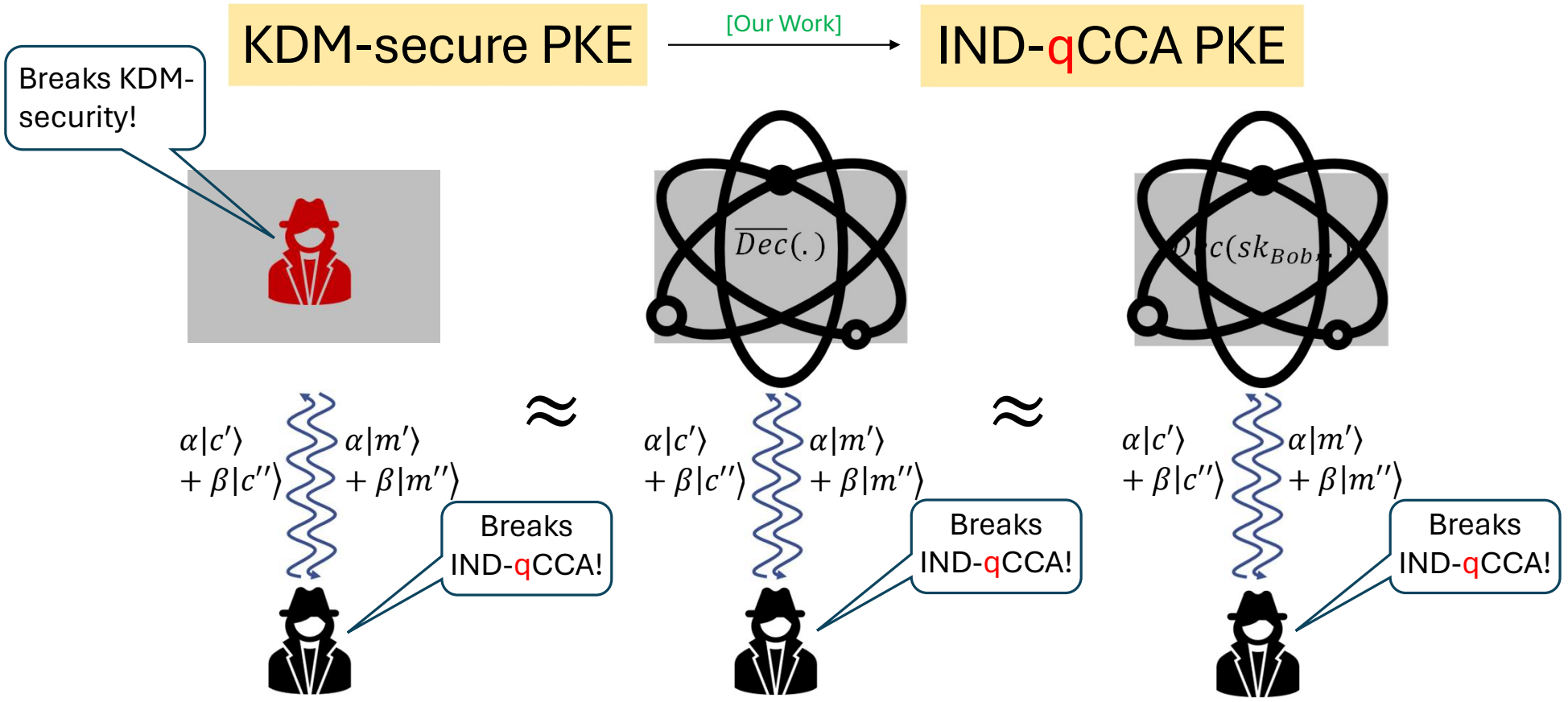
Overview: Techniques



Overview: Techniques



Overview: Techniques



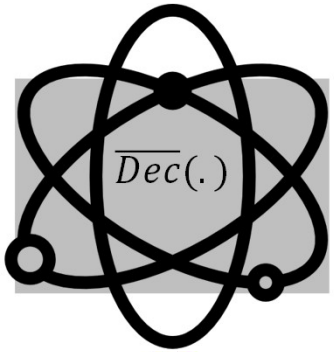
Overview: Techniques

KDM-secure PKE → [Our Work] → IND-qCCA PKE

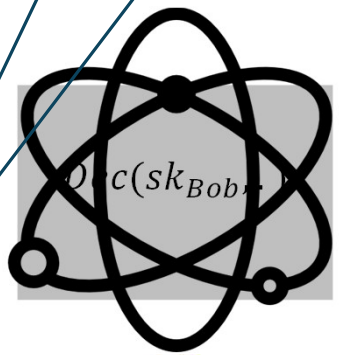
Showed using the **generalized OW2H lemma** of [Ambainis-Hamburg-Unruh'19].

Breaks KDM-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**.

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**.

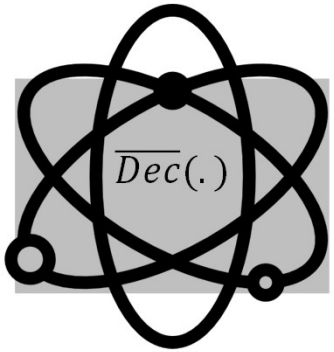
Overview: Techniques

KDM-secure PKE → [Our Work] → IND-qCCA PKE

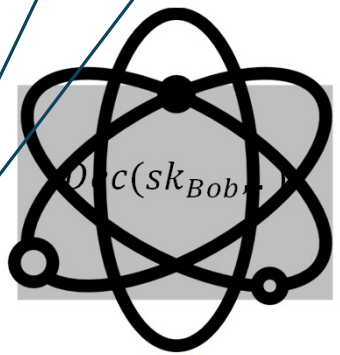
Showed using the **generalized OW2H lemma** of [Ambainis-Hamburg-Unruh'19].

Breaks KDM-security!

$\approx$



$\approx$



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

Breaks IND-qCCA!

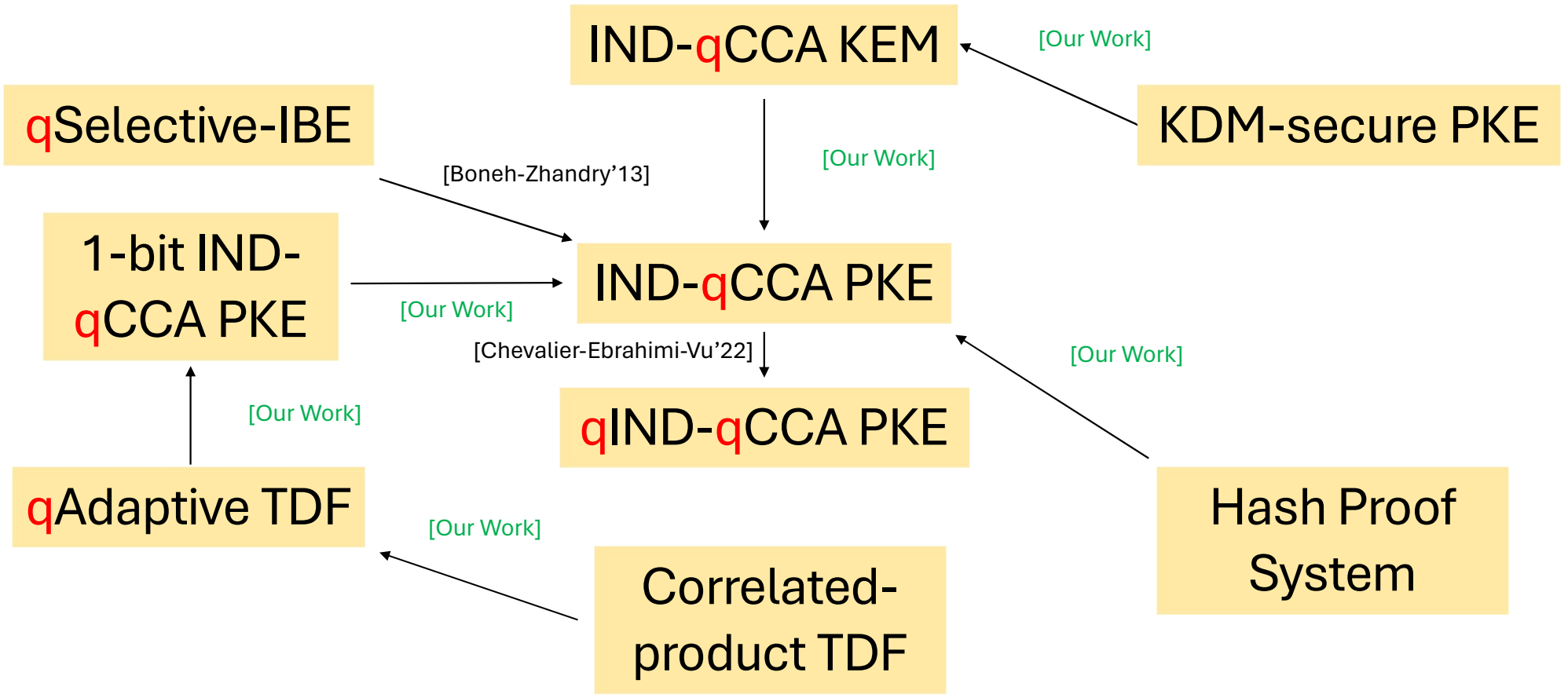
$\alpha|c'\rangle + \beta|c''\rangle$ $\alpha|m'\rangle + \beta|m''\rangle$

Breaks IND-qCCA!

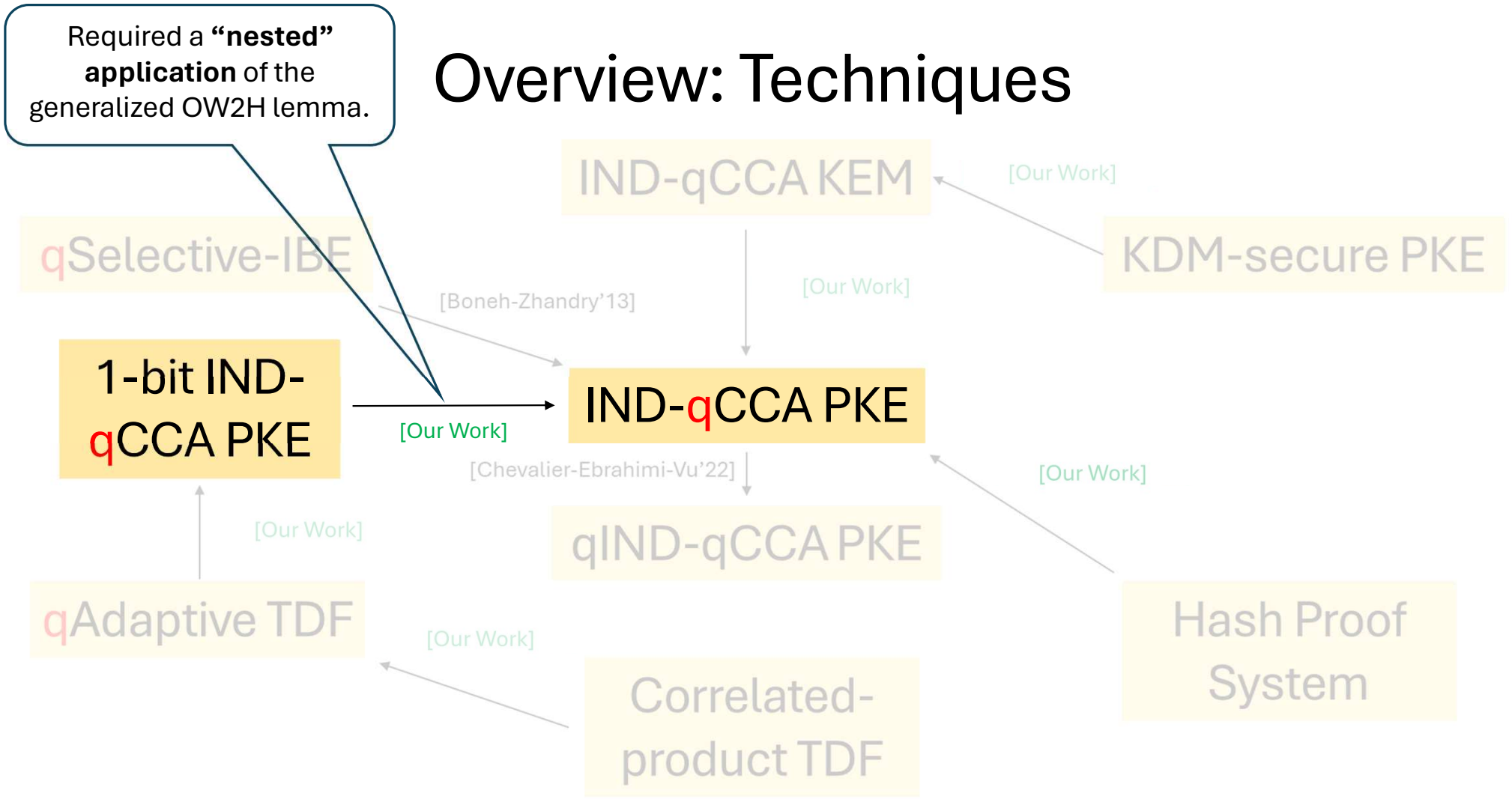
$\alpha|c'\rangle + \beta|c''\rangle$ $\alpha|m'\rangle + \beta|m''\rangle$

Breaks IND-qCCA!

Overview: Techniques

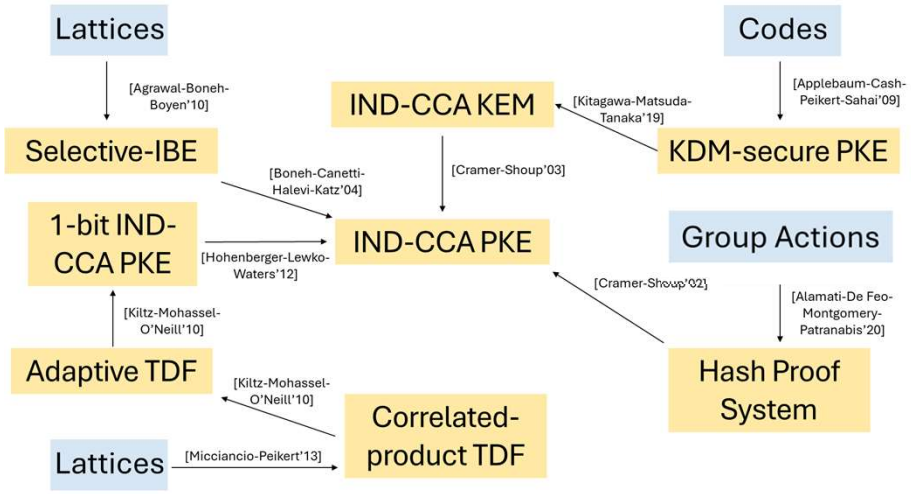


Overview: Techniques



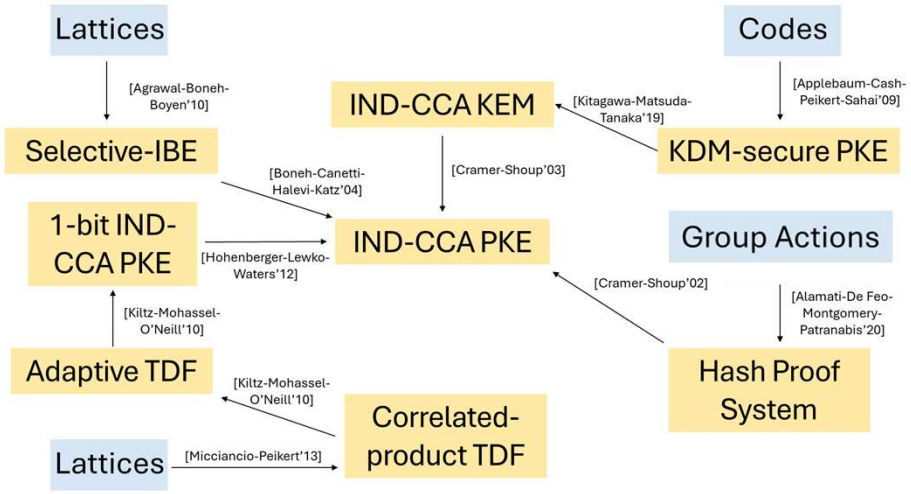
Conclusion

Conclusion

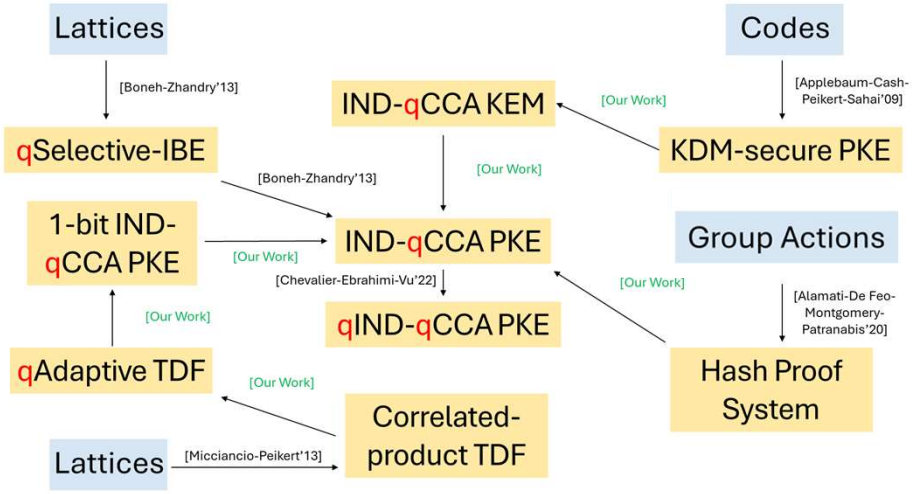


IND-CCA PKE

Conclusion

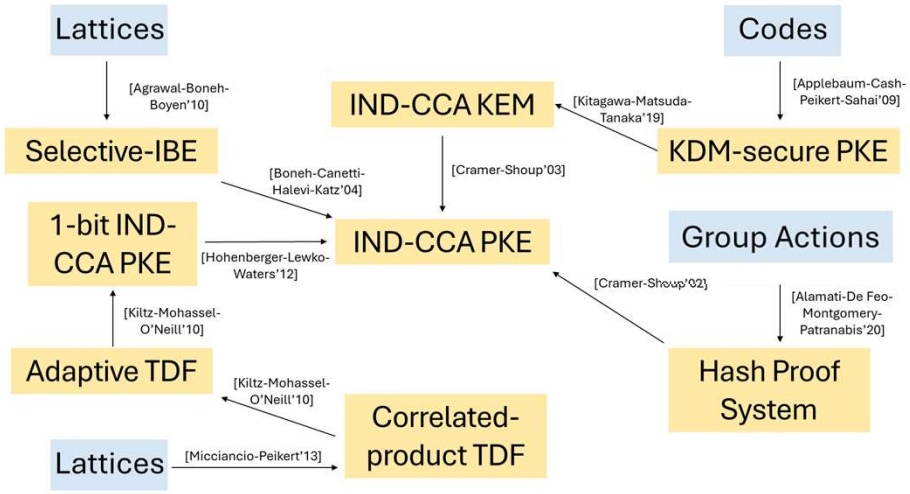


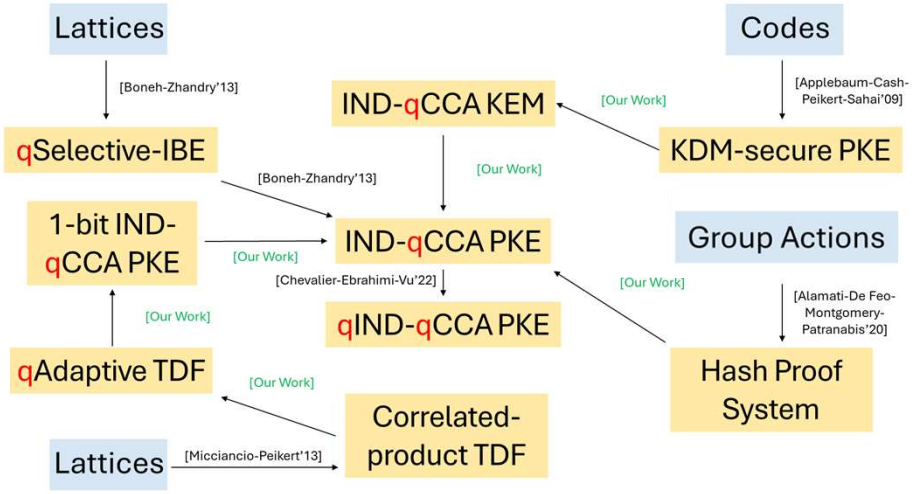
IND-CCA PKE



IND-qCCA PKE

Conclusion





IND-CCA PKE → ?? → IND-qCCA PKE