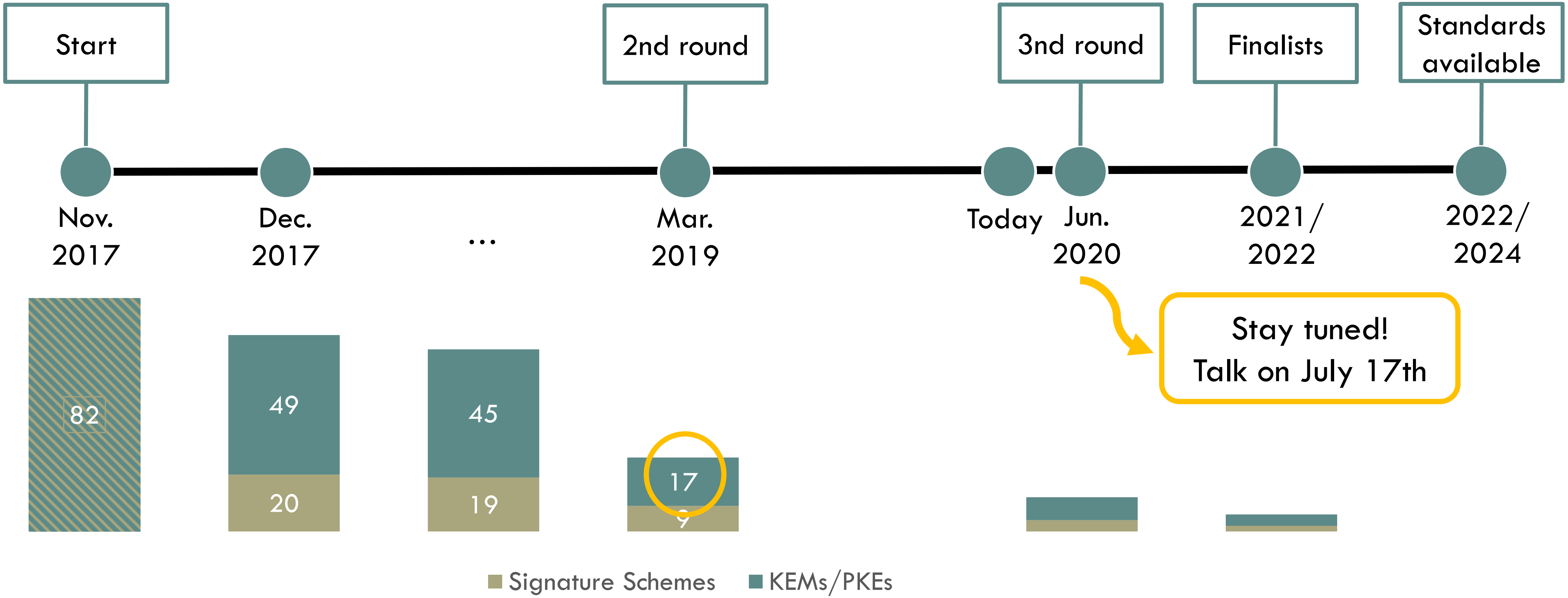
TIGHTER PROOFS OF CCA SECURITY IN THE QUANTUM RANDOM ORACLE MODEL

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

Nina Bindel
Mike Hamburg
Kathrin Hövelmanns
Andreas Hülsing
Edoardo Persichetti

Ottawa, ON, Canada
26/06/2020

NIST PQ Standardization Effort - Timeline



TODAY'S TALK

IND-CPA
&
IND-CCA

IND-CPA
⇩
IND-CCA

IND-CPA
⇩
IND-CCA

ONE-
WAY-TO-
HIDING
LEMMA

PROOF IN
QROM

INDISTINGUISHABILITY UNDER CHOSEN-PLAINTEXT ATTACKS (IND-CPA)

sk, pk $\leftarrow$ KeyGen

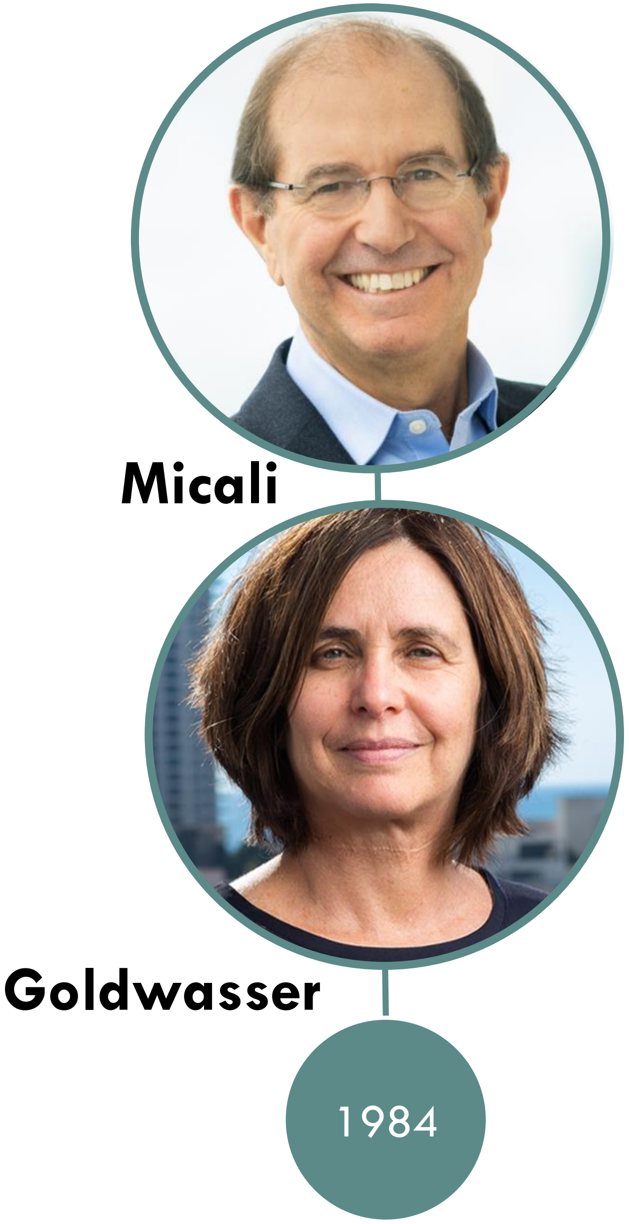
m_0, m_1 $\leftarrow$  (pk)

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

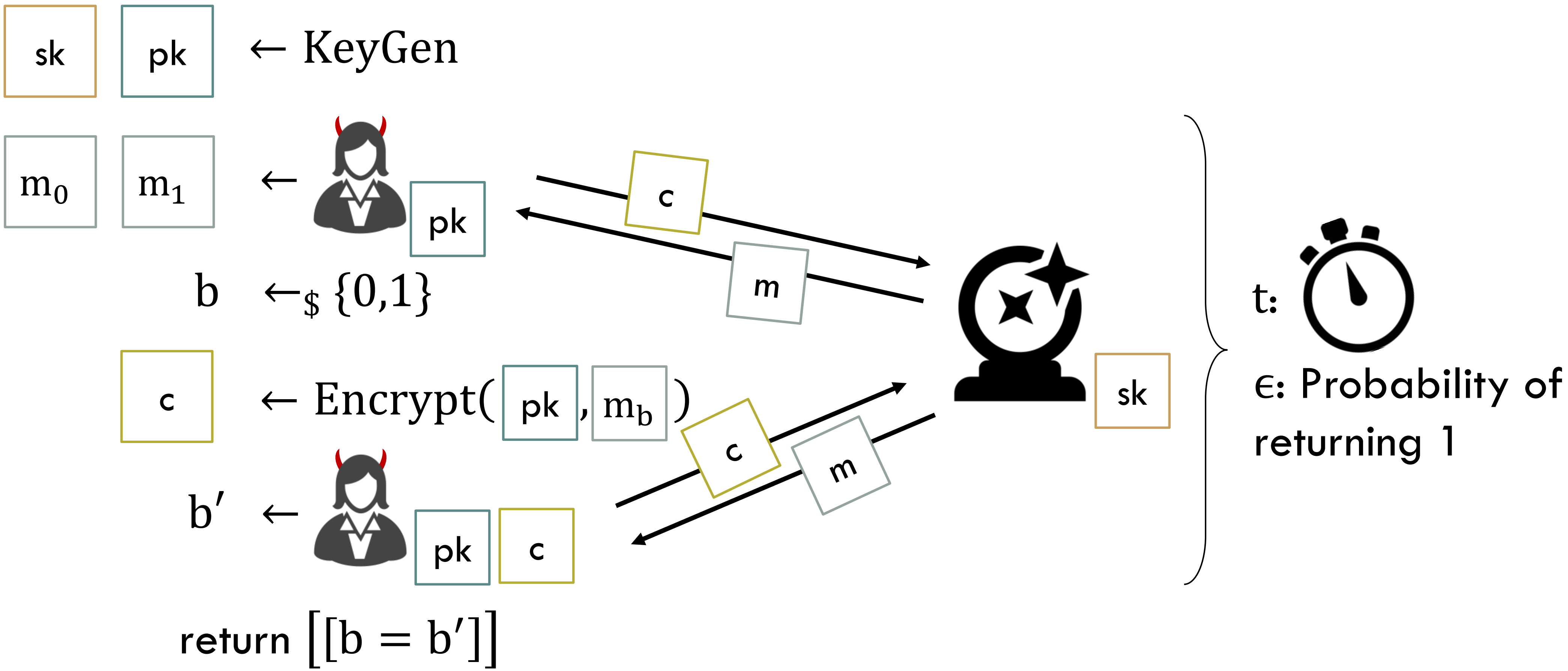
c $\leftarrow$ Encrypt(pk, m_b)

b' $\leftarrow$  (pk, c)

return $[[b = b']]$



INDISTINGUISHABILITY UNDER CHOSEN-CIPHERTEXT ATTACKS (IND-CCA)



TODAY'S TALK

IND-CPA
&
IND-CCA

IND-CPA
⇩
IND-CCA

IND-CPA
⇩
IND-CCA

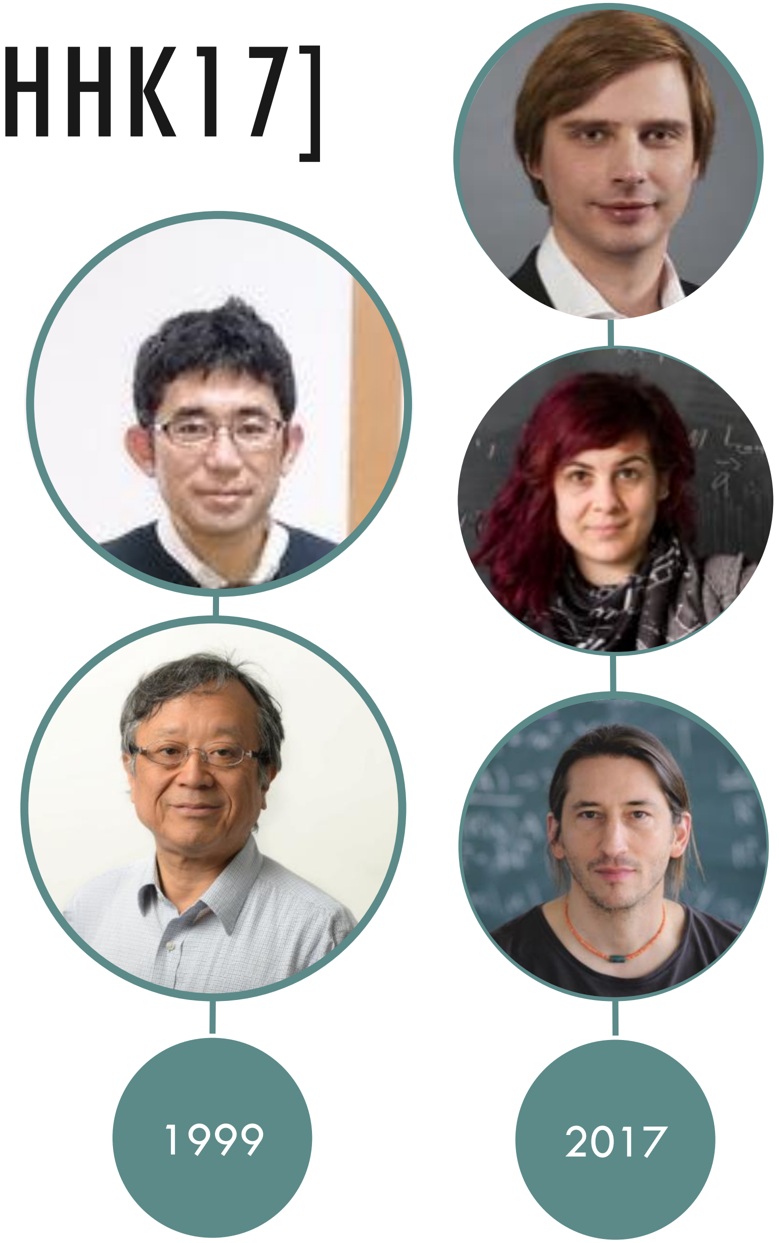
ONE-
WAY-TO-
HIDING
LEMMA

PROOF IN
QROM

Fujisaki-Okamoto transform [FO99,HHK17]

IND-CPA rPKE
rP

IND-CCA KEM
K



Fujisaki-Okamoto transform [FO99,HHK17]

IND-CPA rPKE
rP

$\mathrm{dP} = \mathrm{T}[\mathrm{rP}, \mathrm{G}]$

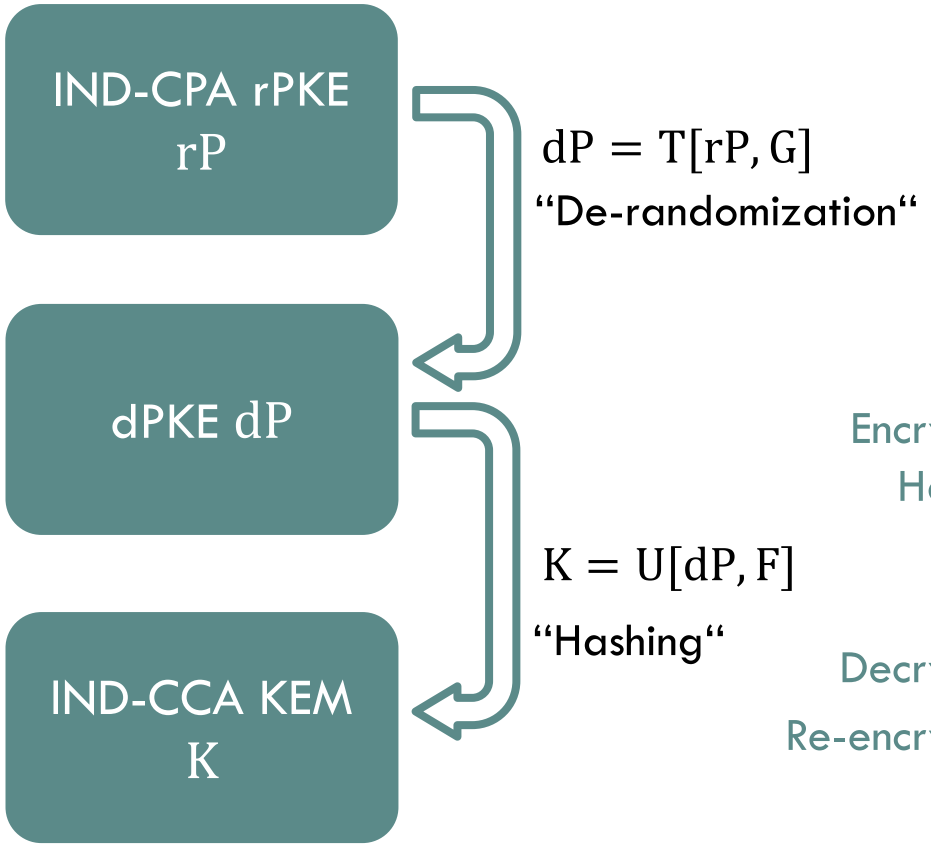
“De-randomization“

$$\mathbf{Encr_{dP}(pk, m)} = \mathrm{Encr_{rP}}\big(\mathrm{pk}, \mathrm{m}; \mathrm{G}(\mathrm{m})\big)$$

dPKE dP

IND-CCA KEM
K

Fujisaki-Okamoto transform [FO99,HHK17]



$\mathbf{Encr_{dP}(pk, m)} = \mathrm{Encr_{rP}}(pk, m; G(m))$

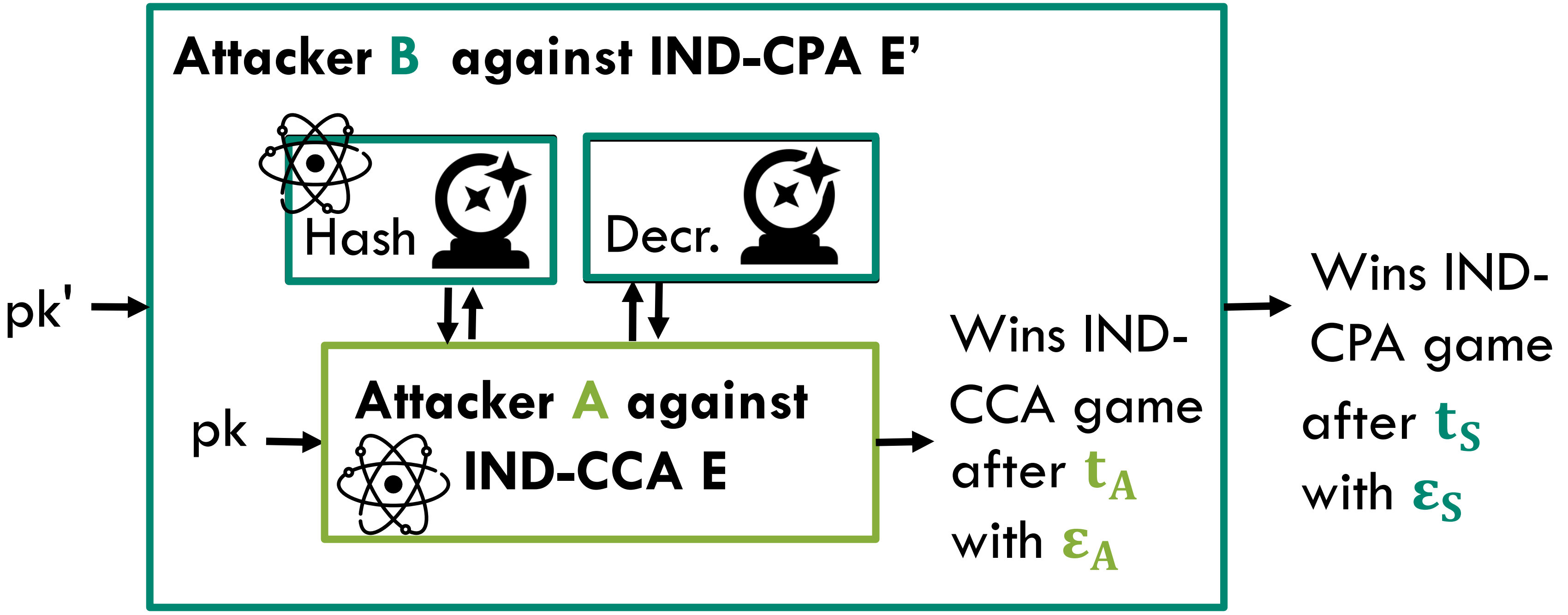
Encaps(pk):
$m \leftarrow_{\$} M$
Encryption: $c \leftarrow \mathrm{Encr_{dP}}(pk, m)$
Hashing: $k \leftarrow H(m, c)$
return (k, c)

Decaps(sk, prfk, c):
Decryption: $m' \leftarrow \mathrm{Decr_{dP}}(sk, c)$
if $m' = \perp$: return $\mathrm{PRF}(prfk, c)$
Re-encryption: if $\mathrm{Encr_{dP}}(pk, m') \neq c$: return $\mathrm{PRF}(prfk, c)$
return $H(m', c)$

$k \leftarrow H(m, c)$	$k \leftarrow H(m)$	Rejection
$U^{\perp}$	$U^{\perp}_{m}$	$\perp$ - "explicit"
$U^{\$}$	$U^{\$}_{m}$	$ - "implicit"

SECURITY REDUCTION

If there exists a quantum adversary A that breaks the IND-CCA security of the PKE E= FO[E‘]
then there exists an algorithm B that breaks the IND-CPA security of the PKE E‘.



Tight reduction:

$\varepsilon_A \approx \varepsilon_B$

$t_A \approx t_B$

TODAY'S TALK

IND-CPA
&
IND-CCA

IND-CPA
IND-CCA

IND-CPA
IND-CCA

ONE-
WAY-TO-
HIDING
LEMMA

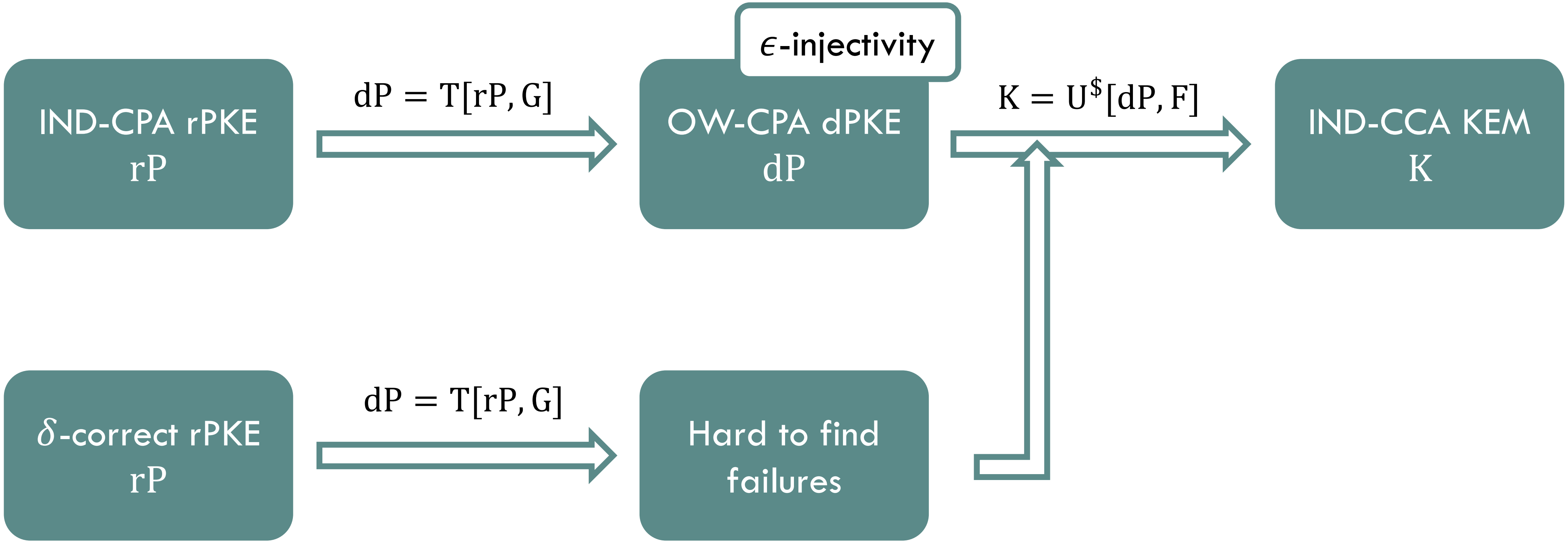
PROOF IN
QROM

Related work in the QROM

[HHK17]	$q_G\sqrt{\epsilon_{rP}} \geq \epsilon_{dP}$	$(q_{H'}+q_H)\sqrt{\epsilon_{dP}} \geq \epsilon_K$	$\epsilon_{rP} \geq \epsilon_K^4/q_{RO}^6$	\$ or ⊥
[SXY18, JZCWM18]	$q_G\sqrt{\epsilon_{rP}} \geq \epsilon_{dP}$	$\epsilon_{dP} \geq \epsilon_K$	$\epsilon_{rP} \geq \epsilon_K^2/q_{RO}^2$	\$
[JZM19,HKSU18]	$\sqrt{q_G\epsilon_{rP}} \geq \epsilon_{dP}$	$\epsilon_{dP} \geq \epsilon_K$	$\epsilon_{rP} \geq \epsilon_K^2/q_{RO}$	\$ or ⊥
[**B**HHHP19]	$d\epsilon_{rP} \geq \epsilon_{dP}$	$\sqrt{\epsilon_{dP}} \geq \epsilon_K$	$\epsilon_{rP} \geq \epsilon_K^2/d$	\$ or ⊥
[KSSSS20]			$\epsilon_{rP} \geq \epsilon_K/4d$	\$ or ⊥

d = the max number of sequential invocations of the oracle, $d \leq q_{RO}$

Contribution – IND-CCA security of $\mathrm{U}^{\$}$ in the QROM



OW-CPA PKE

sk pk ← KeyGen

m ← Message space

c ← Encrypt(pk , m)

m' ←  pk c

return $[\![m = m']\!]$

δ-correct PKE

A PKE $\mathsf{P} = (\mathrm{Keygen}, \mathrm{Encr}, \mathrm{Decr})$ *is δ-correct if*

$$\mathrm{E}\left[\max_{\mathrm{m}\in\mathcal{M}} \Pr[\mathrm{Decr}(\mathrm{sk}, \mathrm{Encr}(\mathrm{pk}, \mathrm{m})) \neq \mathrm{m}]] : (\mathrm{pk}, \mathrm{sk}) \leftarrow \mathrm{Keygen}()\right] \leq \delta.$$

We call δ *the decryption failure probability of* P. *We say* P *is correct if* $\delta = 0$.

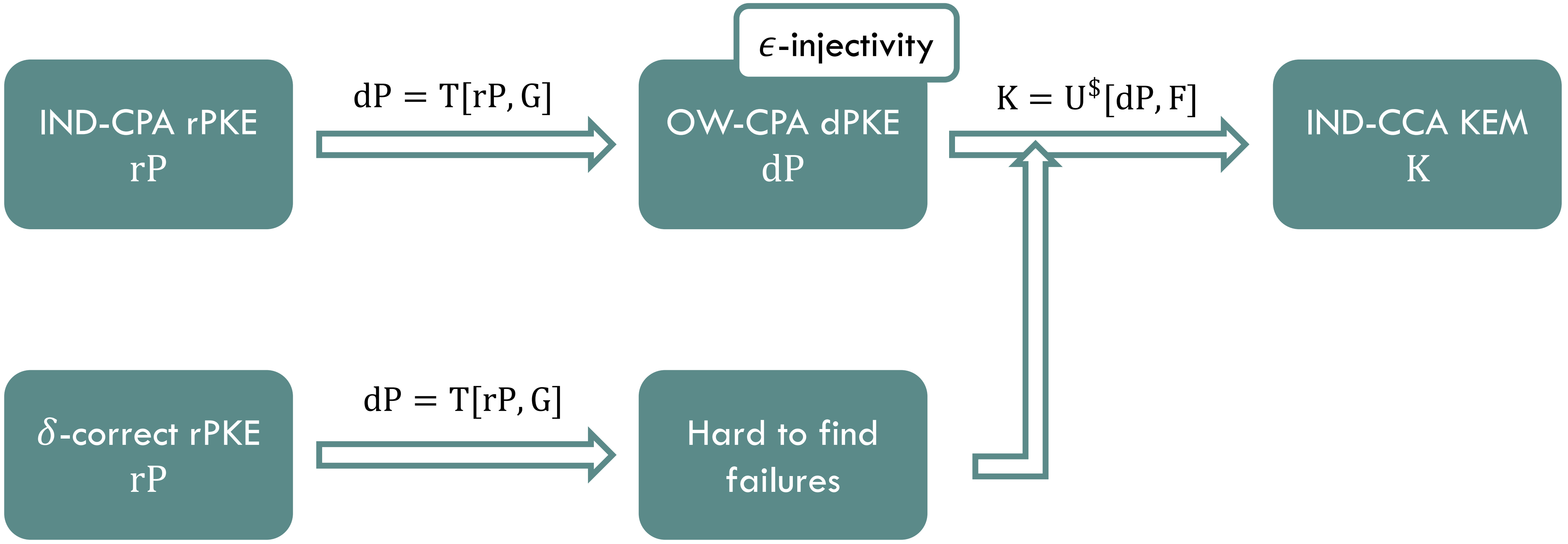
ϵ-injective PKE

A dPKE $\mathsf{P} = (\mathrm{Keygen}, \mathrm{Encr}, \mathrm{Decr})$ *is* ϵ*-injective if*

$$\Pr\left[\mathrm{Encr}(\mathrm{pk}, m) \text{ is not injective} : (\mathrm{pk}, \mathrm{sk}) \leftarrow \mathrm{Keygen}(), H \xleftarrow{\$} \mathcal{H}\right] \leq \epsilon.$$

We say P *is injective if* $\epsilon = 0$. *We say that an rPKE is injective if for all public keys* pk, *all* $m \neq m'$ *and all coins* r, r', *we have* $\mathrm{Encr}(\mathrm{pk}, m, r) \neq \mathrm{Encr}(\mathrm{pk}, m', r')$.

Contribution – IND-CCA security of $U^{\$}$ in the QROM



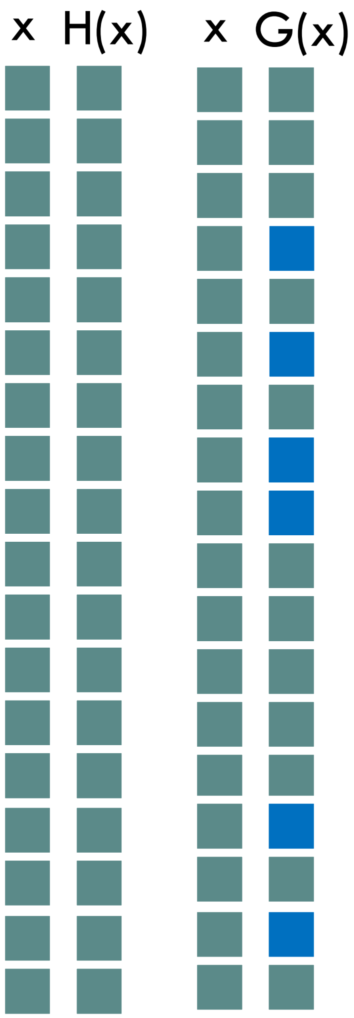
Random oracle vs. quantum random oracle

- Classical queries
- Queries and responses can be easily recorded
- Random oracle can be reprogrammed

- Queries in superposition
- Queries and responses are much harder to record [Zha19]
- Much harder to respond adaptevely/reprogramm oracle

↳ Possible but leads to less tight bounds

Unruh's one-way to hiding (O2H) lemma



$S = G^{-1}(\blacksquare)$, A^H quantum oracle algorithm, q queries of depth $d \leq q$

If $|\Pr[Ev: A^H(z)] - \Pr[Ev: A^G(z)]| = \delta > 0$, A asked some $x \in S$

Behavior can be observed by B

$B \to x$ with probability ϵ

O2H variant	Restriction	Bound
Original [Unr15]	✗	$\delta \leq 2d\sqrt{\epsilon}$
Semi-classical [AHU19]	✓	$\delta \leq 2\sqrt{d\epsilon}$
Double-sided [**B**HHHP19]	✓	$\delta \leq 2\sqrt{\epsilon}$
[KSSSS20]	✓	$\delta \leq 4q\epsilon$

Unruh

2015

IMPOSSIBILITY RESULT [JZM19]

- Adversary $A^{|O>}$ modeled as $A_N \circ U_0 \circ A_{N-1} \circ U_1 \circ \cdots \circ U_0 \circ A_1$
  (*i*-th random oracle query $\triangleq$ output of A_i)
- Square-root loss unavoidable in O2H with **query-based** secret extraction

  Extract preimage from oracle queries $\triangleq$ output register of A_i
  ⟹ only considers input/output behavior of A

- **No** square-root loss in O2H with **measurement-based** secret extraction

  A has to measure to recognize the difference between oracles
  ⟹ consider A's internal workings

Kathrin Hövelmanns' talk: https://simons.berkeley.edu/talks/cca-encryption-qrom-i
Ron Steinfeld's talk: https://simons.berkeley.edu/talks/cca-encryption-qrom-ii

OW-CPA dPKE to IND-CCA KEM

Pr[$Encr(pk, m)$ is not injective: $(\mathrm{pk}, \mathrm{sk}) \leftarrow$ KeyGen()] $\leq \epsilon$

Theorem

$H: M \times C \to K$ Hash function, $F: K_F \times C \to K$ PRF, P ϵ-injective dPKE

If $\exists$ A IND-CCA adversary against KEM $U^{\$}(P, F)$, q_{dec} decryption queries, then $\exists$

- OW-CPA adversary B_1 against P
- PRF adversary B_3 against F
- FFC adversary B_2 against P

"Finding failing ciphertext"
$B_2 \to L$, B_2 wins if $\exists$ $c \in L: Enc(pk, m) = c \ \wedge Dec(sk, c) \neq m$

such that

$$\mathrm{Adv}_{U^{\$}(P,F)}^{\hat{I}ND-CCA}(A) \leq \underbrace{2\sqrt{\mathrm{Adv}_P^{OW-CPA}(B_1)}}_{\text{small}} + \underbrace{2\mathrm{Adv}_F^{PRF}(B_3)}_{\text{small}} + \underbrace{\mathrm{Adv}_P^{FFC}(B_2)}_{\text{small}} + \epsilon.$$

if P' δ-correct pPKE and
$\mathrm{P} = \mathrm{T}[\mathrm{P}', \mathrm{G}]$ ϵ-injective dPKE

Proof: IND-CCA $U^{\$}$ to OW-CPA dP

$\text{Exp}_{\text{KEM}}^{\text{IND-CCA}}(A)$

$H \leftarrow \mathcal{H}$
$(sk, pk) \leftarrow \text{KeyGen}()$
$m^* \leftarrow_{\$} M$
$c^* \leftarrow \text{Encrypt}(pk, m^*)$
$k_0^* \leftarrow H(m^*, c^*)$
$k_1^* \leftarrow_{\$} K$
$b \leftarrow_{\$} \{0,1\}$
$b' \leftarrow A^{H,\text{Dec}}(pk, c^*, k_b^*)$
return $[[b = b']]$

Oracle $\text{Dec}((sk, pk, prfk), c)$:

if $c = c^*$: return $\perp$
$m' \leftarrow \text{Decrypt}(sk, c)$
if $\text{Encrypt}(pk, m') = c$: return $k' \leftarrow H(m, c)$
return $k' \leftarrow \text{PRF}(prfk, c)$

Proof: IND-CCA $U^{\$}$ to OW-CPA dP

$\mathrm{Exp}_{\mathrm{KEM}}^{\mathrm{IND-CCA}}(A)$

$H \leftarrow \mathcal{H}$
$(sk, pk) \leftarrow \mathrm{KeyGen}()$
$m^* \leftarrow_{\$} M$
$c^* \leftarrow \mathrm{Encrypt}(pk, m^*)$
$k_0^* \leftarrow H(m^*, c^*)$
$k_1^* \leftarrow_{\$} K$
$b \leftarrow_{\$} \{0,1\}$
$b' \leftarrow A^{H,\mathrm{Dec}}(pk, c^*, k_b^*)$
return $[[b = b']]$

Oracle $\mathrm{Dec}((sk, pk, prfk), c)$:

if $c = c^*$: return $\perp$
$m' \leftarrow \mathrm{Decrypt}(sk, c)$
if $\mathrm{Encrypt}(pk, m') = c$: return $k' \leftarrow H(m, c)$
return $k' \leftarrow R(c)$

$\mathrm{Adv}_F^{PRF}(B_3)$ PRF is random

Proof: IND-CCA $U^{\$}$ to OW-CPA dP

$\mathrm{Exp}_{\mathrm{KEM}}^{\mathrm{IND-CCA}}(A)$

$H \leftarrow \mathcal{H}$

$(sk, pk) \leftarrow \mathrm{KeyGen}()$

$m^* \leftarrow_\$ M$

$c^* \leftarrow \mathrm{Encrypt}(pk, m^*)$

$k_0^* \leftarrow R(c)$

$k_1^* \leftarrow_\$ K$

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

$b' \leftarrow A^{H,\mathrm{Dec}}(pk, c^*, k_b^*)$

return $[[b = b']]$

Oracle $\mathrm{Dec}((sk, pk, prfk), c)$:

if $c = c^*$: return $\perp$

$m' \leftarrow \mathrm{Decrypt}(sk, c)$

if $\mathrm{Encrypt}(pk, m') = c$: return $k' \leftarrow R(c)$

return $k' \leftarrow R(c)$

$\mathrm{Adv}_F^{PRF}(B_3)$ PRF is random

$\mathrm{Adv}_{\mathrm{dP}}^{\mathrm{FFC}}(B_2) + \epsilon$ Re-programm random oracle

- Injectivity needed
- Independent of PRF change

Proof: IND-CCA $U^{\$}$ to OW-CPA dP

$\mathrm{Exp}_{\mathrm{KEM}}^{\mathrm{IND-CCA}}(A)$

$H \leftarrow \mathcal{H}$

$(sk, pk) \leftarrow \mathrm{KeyGen}()$

$m^* \leftarrow_\$ M$

$c^* \leftarrow \mathrm{Encrypt}(pk, m^*)$

$k_0^* \leftarrow R(c)$

$k_1^* \leftarrow_\$ K$

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

$b' \leftarrow A^{H,\mathrm{Dec}}(pk, c^*, k_b^*)$

return $[[b = b']]$

Oracle $\mathrm{Dec}((sk, pk, prfk), c)$:

if $c = c^*$: return $\perp$

$m' \leftarrow \mathrm{Decrypt}(sk, c)$

if $\mathrm{Encrypt}(pk, m') = c$: return $k' \leftarrow R(c)$

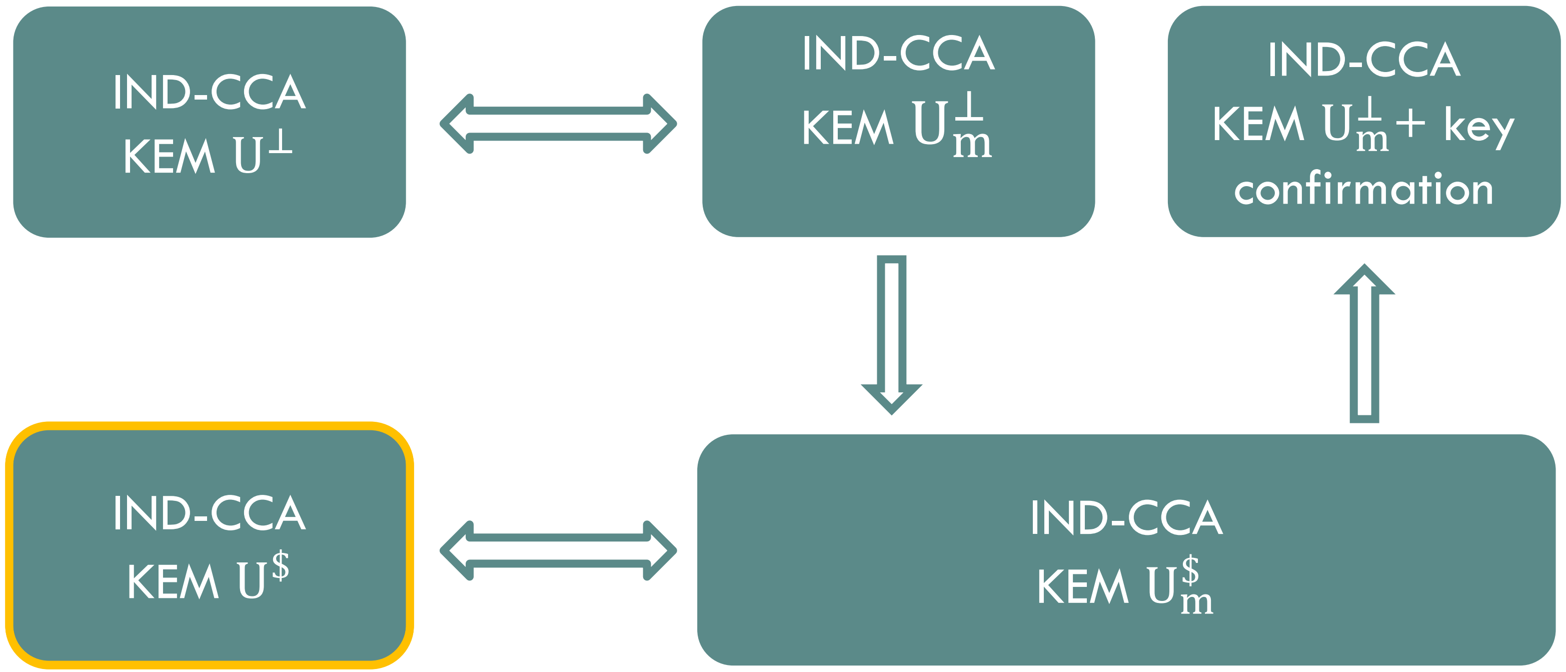
return $k' \leftarrow R(c)$

$\mathrm{Adv}_F^{PRF}(B_3)$ PRF is random

$\mathrm{Adv}_{\mathrm{dP}}^{\mathrm{FFC}}(B_2) + \epsilon$ Re-programm random oracle
- Injectivity needed
- Independent of PRF change

$\sqrt{\mathrm{Adv}_{dP}^{OW-CPA}(B_1)}$ Same as distinguishing $(c^*, k^*, H[m^* \to r])$ and (c^*, k^*, H)
- Apply double-sided O2H to recover m^*

Contribution – Relation of U constructions



Key confirmation:

$(c, H(m)) \leftarrow Encr_C(pk, m)$

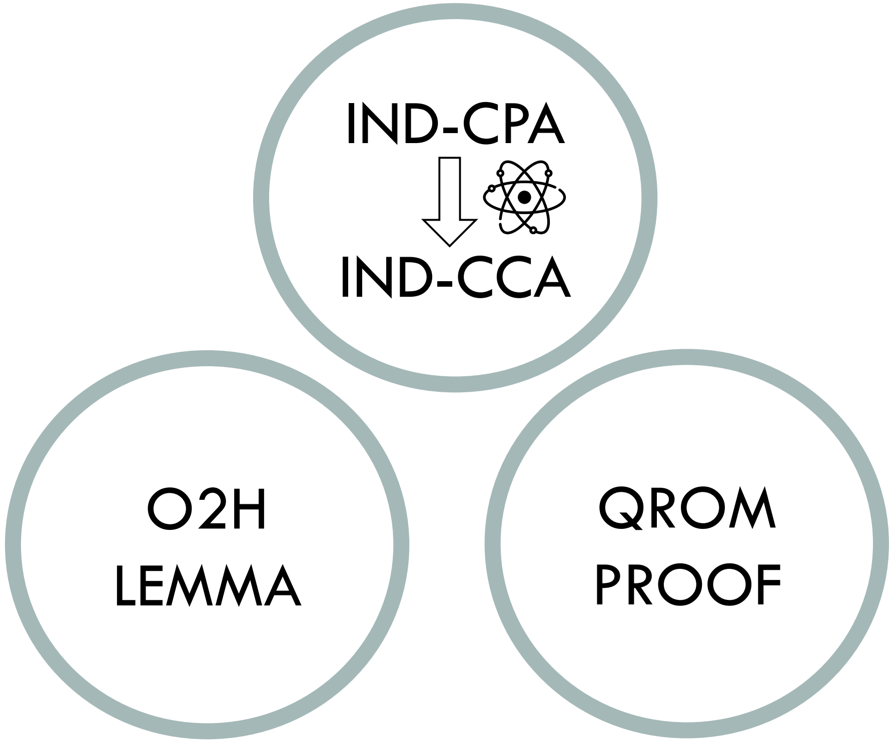
$Decr_C(sk, (c, t))$:

$\quad m' \leftarrow Decr(sk, c)$

$\quad$ if $H(m') \neq t$: return $\perp$

$\quad$ return m'

Conclusion



Acknowledgments

- This results were achieved during the Oxford 2019 PQC workshop.
- Thanks to **Dan Bernstein, Edward Eaton,** and **Mark Zhandry** for helpful discussions and feedback.
- My slides are inspired by **Mike Hamburg**'s talk given at the 2nd NIST post-quantum workshop and **Kathrin Hövelmanns**' and **Ron Steinfeld**'s talks at "Lattices: From Theory to Practice" – Simons Institute Workshop.

Full paper:

IACR eprint 2019/590

THANKS

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

References

[FO99] E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. Crypto 1999.

[HHK17] D. Hofheinz, K. Hövelmanns, and E. Kiltz. A Modular Analysis of the Fujisaki-Okamoto Transformation. TCC 2017.

[SXY18] T. Saito, K. Xagawa and T. Yamakawa. Tightly-secure key-encapsulation mechanism in the quantum random oracle model. Eurocrypt2018.

[JZCWM18] H. Jiang and Z. Zhang and L. Chen and H. Wang and Z. Ma. IND-CCA-secure Key Encapsulation Mechanism in the Quantum Random Oracle Model, Revisited. Crypto 2018.

[JZM19] H. Jiang and Z. Zhang and Z. Ma. Tighter security proofs for generic key encapsulation mechanism in the quantum random oracle model.

[HKSU18] K. Hövelmanns, E. Kiltz, S. Schäge, and D. Unruh. Generic Authenticated Key Exchange in the Quantum Random Oracle Model.

[Zha19] M. Zhandry. How to Record Quantum Queries, and Applications to Quantum Indifferentiability. Crypto 2019.

[AHU19] A. Ambainis, M. Hamburg, and D. Unruh. Quantum security proofs using semi-classical oracles. Crypto 2019.

[Unr15] D. Unruh. Revocable quantum timed-release encryption. JACM 2015.