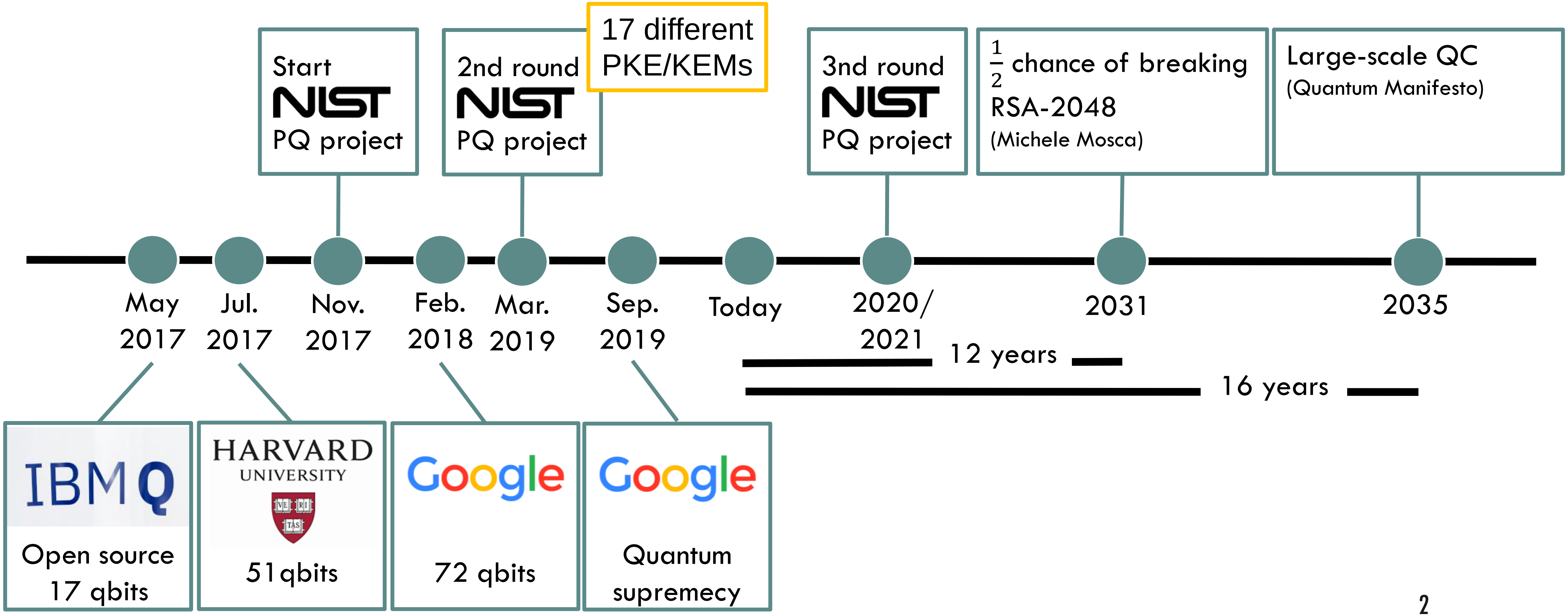
TIGHTER PROOFS OF CCA SECURITY IN THE QUANTUM RANDOM ORACL MODEL

IMACC'19
Oxford, UK
18/12/2019

Nina Bindel
Mike Hamburg
Kathrin Hövelmanns
Andreas Hülsing
Edoardo Persichetti

Quantum computing: State-of-the-art and estimations



Fujisaki-Okamoto transform [FO99,HHK17]

IND-CPA rPKE
rP

$\mathrm{dP} = \mathrm{T}[\mathrm{rP}, \mathrm{G}]$
“De-randomization“

dPKE dP

$\mathrm{K} = \mathrm{U}[\mathrm{dP}, \mathrm{F}]$
“Hashing“

IND-CCA KEM
K

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

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

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

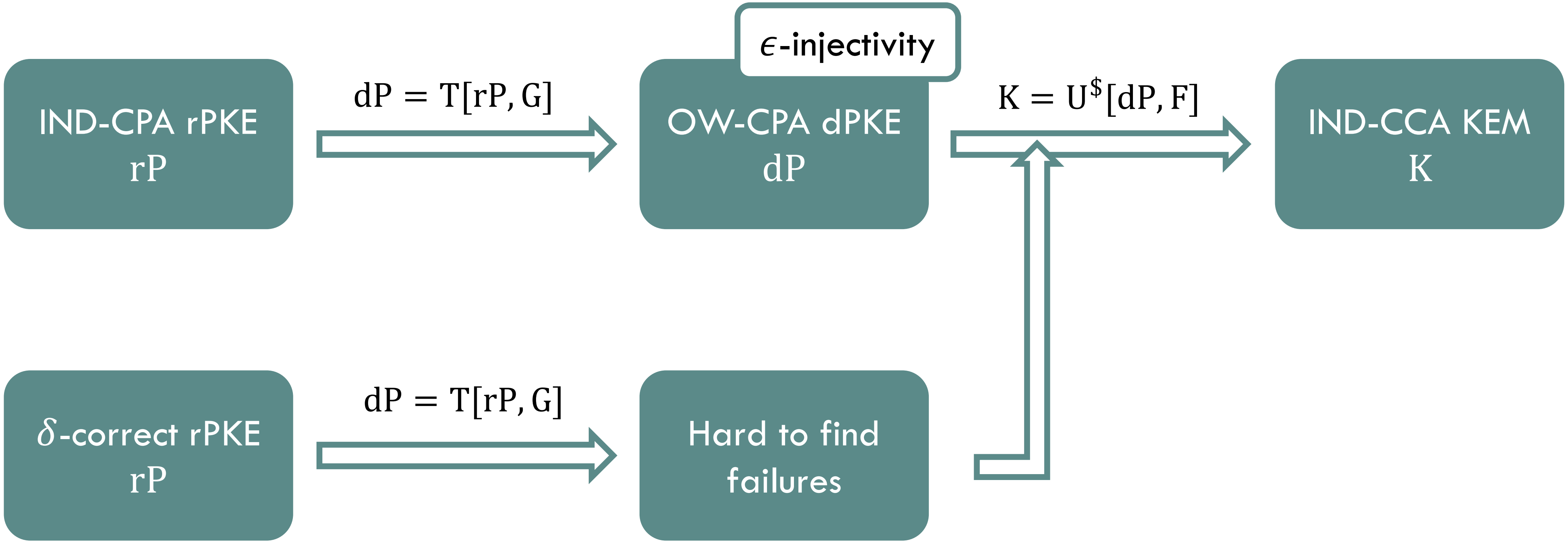
$\mathrm{k} \leftarrow \mathrm{H}(\mathrm{m}, \mathrm{c})$	$\mathrm{k} \leftarrow \mathrm{H}(\mathrm{m})$	Rejection
$\mathrm{U}^{\perp}$	$\mathrm{U}_{\mathrm{m}}^{\perp}$	$\perp$ - ‘’explicit’’
$\mathrm{U}^{\$}$	$\mathrm{U}_{\mathrm{m}}^{\$}$	\$ - ‘’implicit’’

Related work

[HHK17]	$q_G\sqrt{\epsilon_{rP}} \geq \epsilon_{dP}$	$(q_{H'}+q_H)\sqrt{\epsilon_{dP}} \geq \epsilon_K$	$\boldsymbol{\epsilon_{rP} \geq \epsilon_K^4/q_{RO}^6}$	For $K = \$$ or $\perp$
[SXY18, JZCWM18]	$q_G\sqrt{\epsilon_{rP}} \geq \epsilon_{dP}$	$\epsilon_{dP} \geq \epsilon_K$	$\boldsymbol{\epsilon_{rP} \geq \epsilon_K^2/q_{RO}^2}$	For $K = \$$
[JZM19,HKSU18,…]	$\sqrt{q_G\epsilon_{rP}} \geq \epsilon_{dP}$	$\epsilon_{dP} \geq \epsilon_K$	$\boldsymbol{\epsilon_{rP} \geq \epsilon_K^2/q_{RO}}$	For $K = \$$ or $\perp$
This paper	$d\epsilon_{rP} \geq \epsilon_{dP}$	$\sqrt{\epsilon_{dP}} \geq \epsilon_K$	$\boldsymbol{\epsilon_{rP} \geq \epsilon_K^2/d}$	For $K = \$$ or $\perp$

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

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



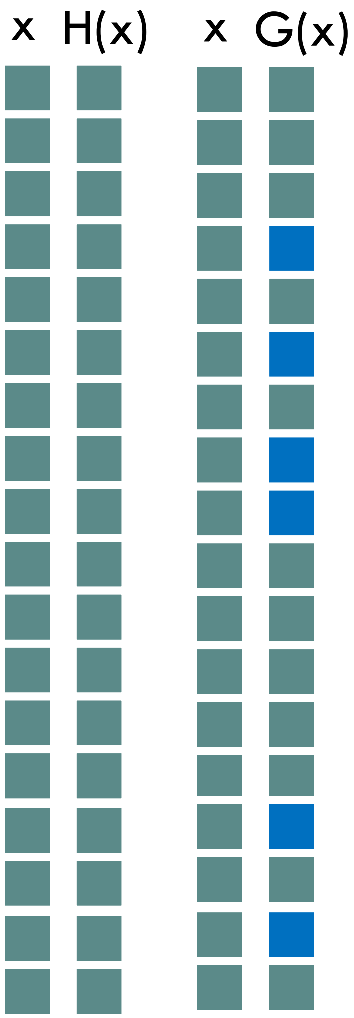
Random oracle vs. quantum random oracle

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

Behavior can be observed by B

$B \rightarrow x$ with probability ϵ

O2H variant	#S	Sim. must know	Bound
Original [Unr15]	Arbitrary	H or G	$\delta \leq 2d\sqrt{\epsilon}$
Semi-classical [AHU19]	Arbitrary	(G or H) and S	$\delta \leq 2\sqrt{d\epsilon}$
Double-sided [this work]	1	H and G	$\delta \leq 2\sqrt{\epsilon}$

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

such that

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

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

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

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

$H \leftarrow \mathcal{H}$

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

$m^* \leftarrow_\$ M$

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

$k_0^* \leftarrow R(c)$

$k_1^* \leftarrow_\$ K$

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

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

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

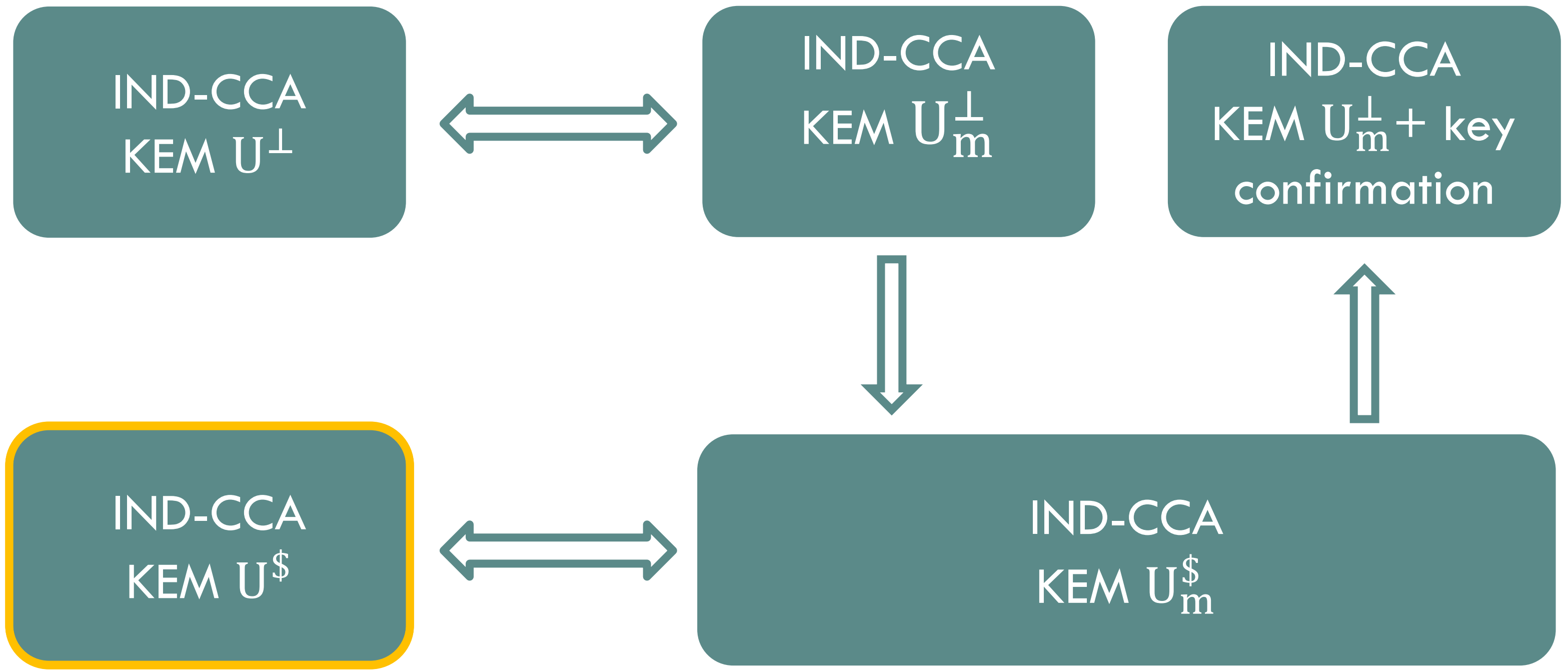
$\mathrm{Adv}_{\mathrm{dP}}^{\mathrm{FFC}}(B_2) + \epsilon$ Re-programm random oracle

- 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:

$\big(c, H(m)\big) \leftarrow \mathrm{Encr}_C(pk, m)$

$\mathrm{Decr}_C\big(sk, (c, t)\big)$:

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

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

$\quad$ return m'

Conclusion

- New **O2H** Lemma
- **Modular proof** showing KEMs almost as secure as PKE in QROM (explicit + implicit)

Full paper:

IACR eprint 2019/590

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 strongly inspired by Mike's talk given at the 2nd NIST post-quantum workshop.

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

THANKS

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.