TIGHTER PROOFS OF CCA SECURITY IN THE QUANTUM RANDOM ORACL MODEL

Nina Bindel

Mike Hamburg

Kathrin Hövelmanns

Andreas Hülsing

Edoardo Persichetti

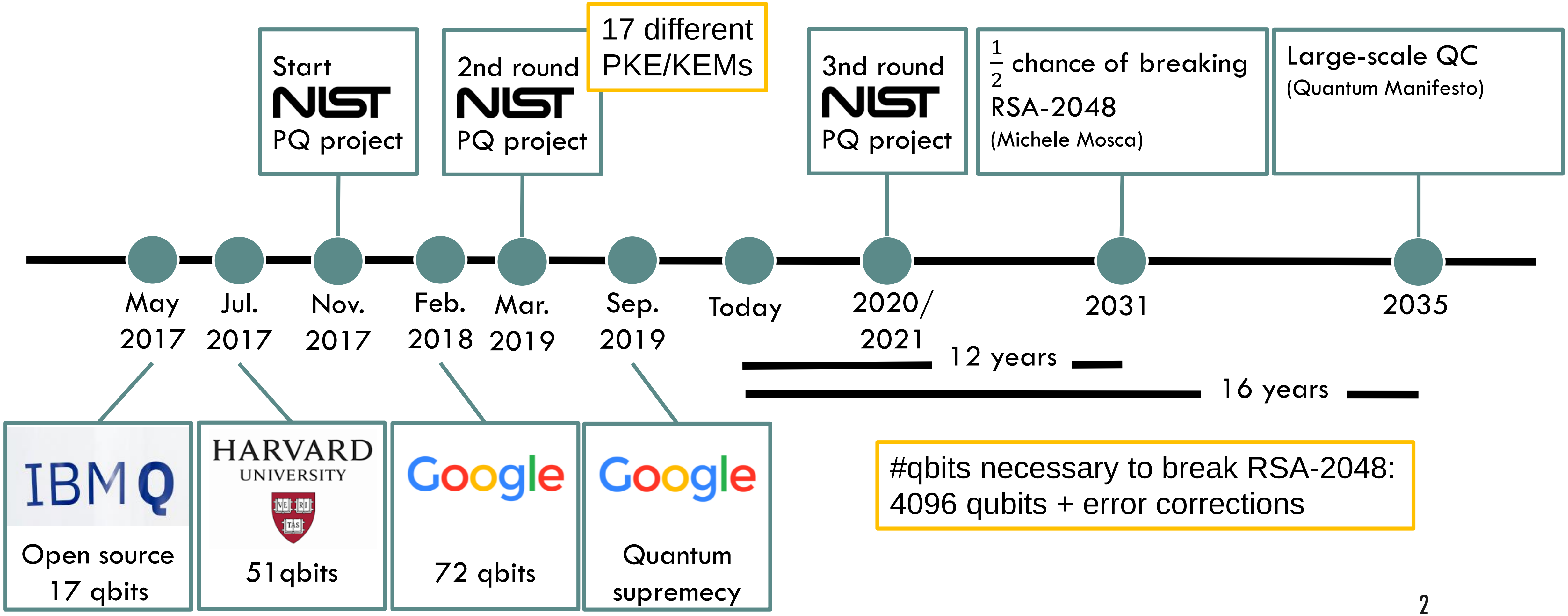
UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

TCC'19

Nurmberg, Germany

03/12/2019

QUANTUM COMPUTING
– STATE OF THE ART AND ESTIMATIONS



May 2017
IBM Q
Open source
17 qbits

Jul. 2017
HARVARD
UNIVERSITY
VE RI TAS
51qbits

Nov. 2017
Start
NIST
PQ project

Feb. 2018
Google
72 qbits

Mar. 2019
2nd round
NIST
PQ project
17 different PKE/KEMs

Sep. 2019
Google
Quantum supremecy

Today

2020/ 2021
3nd round
NIST
PQ project

2031
$\frac{1}{2}$ chance of breaking RSA-2048
(Michele Mosca)

2035
Large-scale QC
(Quantum Manifesto)

12 years

16 years

#qbits necessary to break RSA-2048:
4096 qubits + error corrections

FUJISAKI-OKAMOTO TRANSFORM

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

$$\mathrm{Enc_d}(\mathrm{pk}, \mathrm{m}) = \mathrm{Enc_r}\big(\mathrm{pk}, \mathrm{m}; \mathbf{G}(\mathbf{m})\big)$$

$\mathrm{c} \leftarrow \mathrm{Enc_d}(\mathrm{pk}, \mathrm{m})$		+ Re-encryption return
$\mathrm{k} \leftarrow \mathrm{H}(\mathrm{m}, \mathrm{c}')$	$\mathrm{k} \leftarrow \mathrm{H}(\mathrm{m})$	
$\mathrm{U}^{\perp}$	$\mathrm{U}_{\mathrm{m}}^{\perp}$	$\perp$ - ‘’explicit’’
$\mathrm{U}^{\$}$	$\mathrm{U}_{\mathrm{m}}^{\$}$	$\$$ - ‘’implicit’’

FORMER BOUNDS IN QROM

IND-CPA rPKE
rP

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

non-tight

OW-CPA dPKE
dP

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

Tight ??

IND-CCA KEM
K

[HHK17]: original modular proofs in QROM; very non-tight

[SXY18]: tighter bounds using implicit rejection

[JZCWM18,JZM19]: further improvements

RELATED WORK

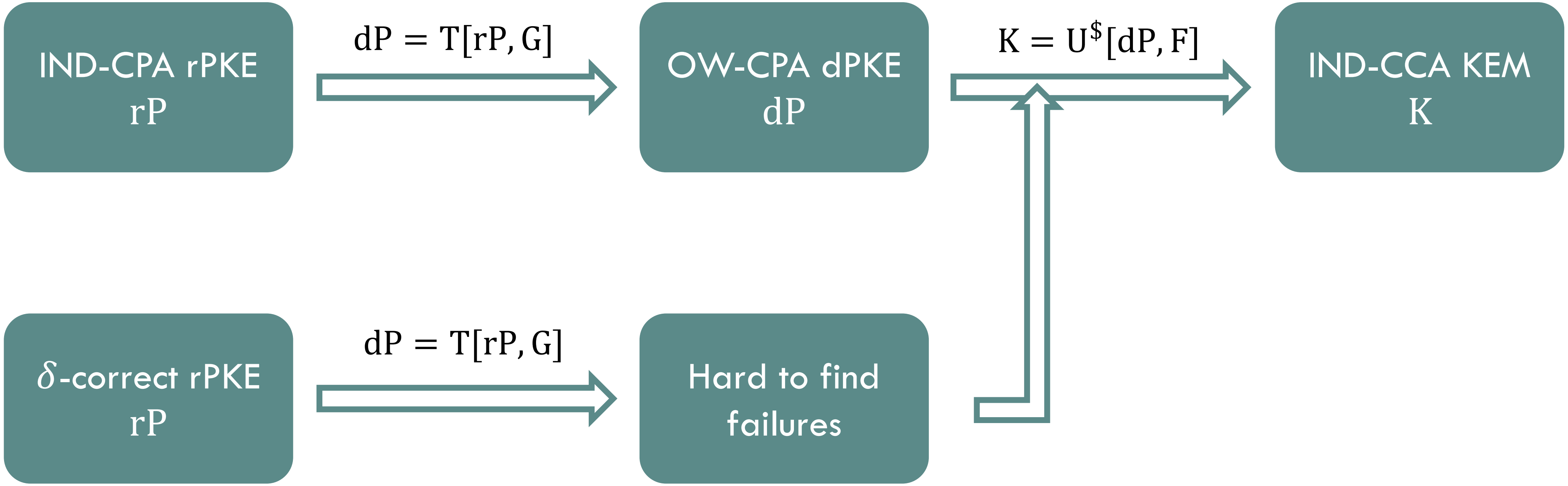
δ-correct IND-CPA rPKE rP $\xrightarrow{\mathrm{dP} = \mathrm{T}[\mathrm{rP}, \mathrm{G}]}$ dPKE dP $\xrightarrow{\mathrm{K} = \mathrm{U}[\mathrm{dP}, \mathrm{F}]}$ IND-CCA KEM K

[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 $\mathrm{K} = \$$ 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 $\mathrm{K} = \$$
[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 $\mathrm{K} =$????
This paper:	$d\epsilon_{rP} \geq \epsilon_{dP}$	$\sqrt{\epsilon_{dP}} \geq \epsilon_K$	$\boldsymbol{\epsilon_{rP} \geq \epsilon_K^2/d^2}$	For $\mathrm{K} = \$$ or $\perp$

d = the max number of sequential invocations of the oracle

$d \leq q$

CONTRIBUTION – IND-CCA SECURITY OF $\mathrm{U}^{\$}$ IN QROM



IND-CPA rPKE
rP

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

OW-CPA dPKE
dP

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

IND-CCA KEM
K

δ-correct rPKE
rP

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

Hard to find failures

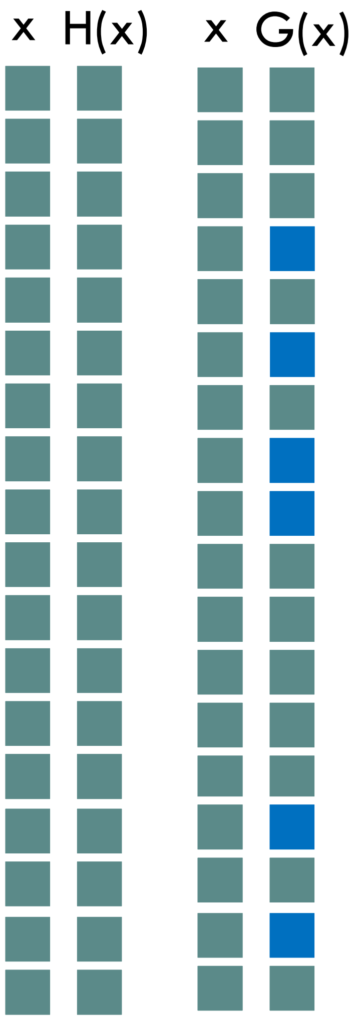
RANDOM ORACLE VS. QUANTUM RANDOM ORACLE

- 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



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

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

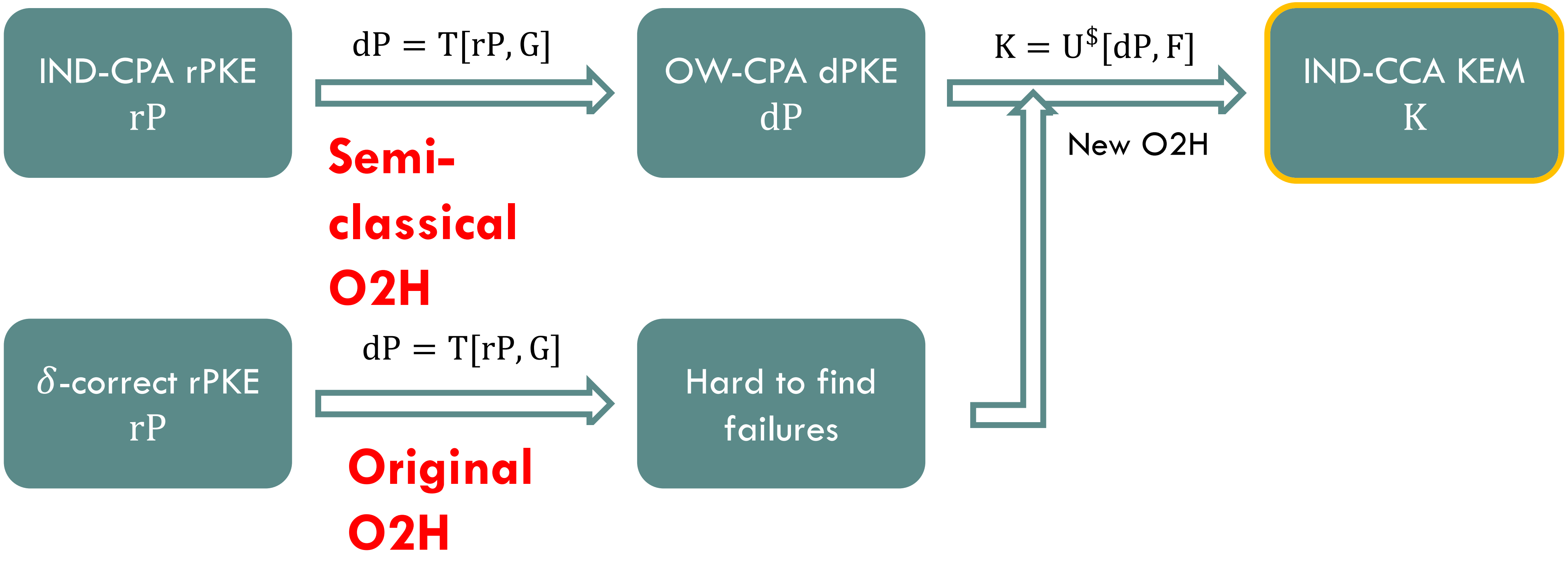
Behavior can be observed by B

$B \rightarrow x$ 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 DETERMINISTIC PKE TO OW-CCA KEM

CONTRIBUTION – IND-CCA SECURITY OF $\mathrm{U}^{\$}$



IND-CPA rPKE

rP

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

Semi-classical O2H

OW-CPA dPKE

dP

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

New O2H

IND-CCA KEM

K

δ-correct rPKE

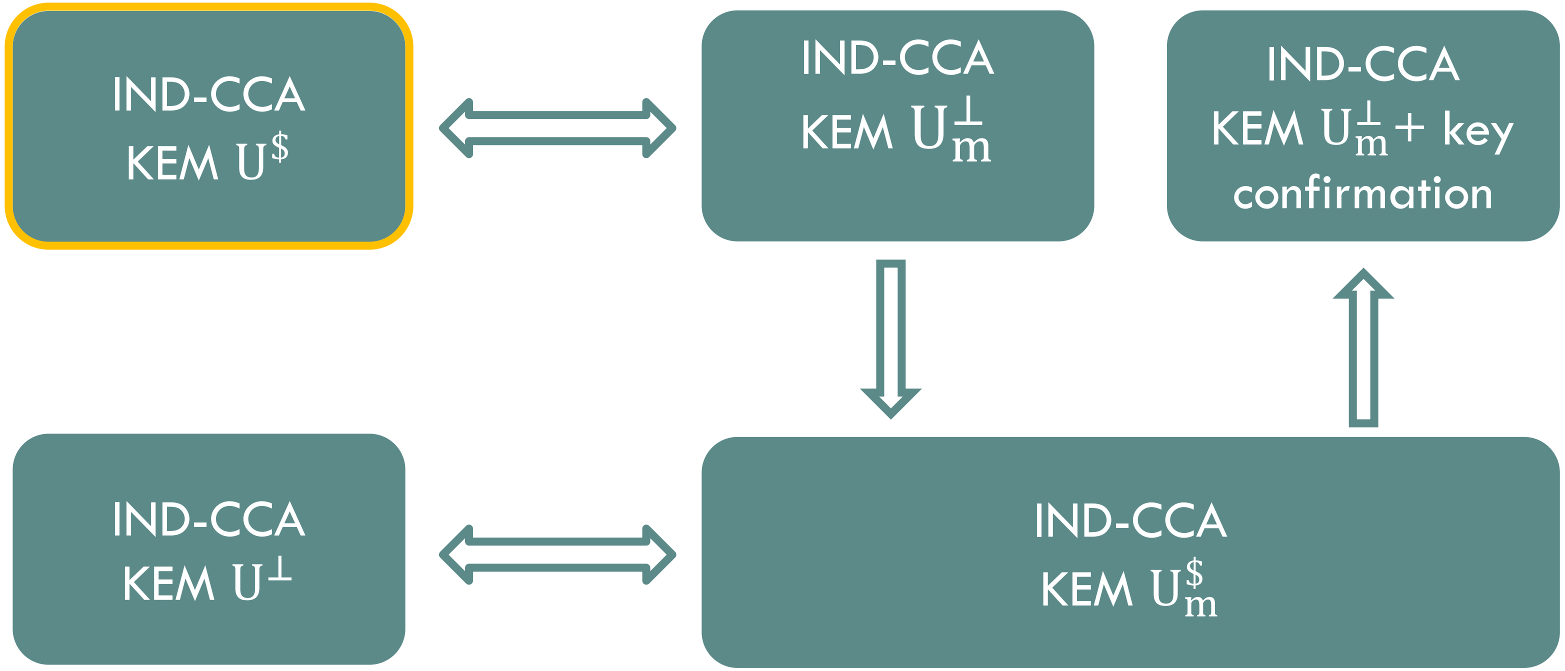
rP

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

Original O2H

Hard to find failures

CONTRIBUTION – RELATION OF U CONSTRUCTIONS



IND-CCA KEM $U^{\$}$

IND-CCA KEM $U_m^{\perp}$

IND-CCA KEM $U_m^{\perp}$ + key confirmation

IND-CCA KEM $U^{\perp}$

IND-CCA KEM $U_m^{\$}$

Key confirmation:

$(c, H(m)) \leftarrow \mathrm{Encr_C}(pk, m)$

```
$\mathrm{Decr_C}(sk, (c, t))$:
    $m' \leftarrow \mathrm{Decr}(sk, c)$
    if $H(m') \neq t$: return $\perp$
    return $m'$
```

FUTURE WORK

CONCLUSION

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

ACKNOWLEDGMENTS

- This work comes from Oxford 2019 PQC workshop
- Thanks to **Dan Bernstein, Edward Eaton, and Mark Zhandry** for helpful discussions and feedback.

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

THANKS

REFERENCES

FUJISAKI-OKAMOTO TRANSFORM

- def
- in ROM
- to be quantum: in QROM

IND-CPA rPKE

rP

$dP = T[rP, G]$

"De-randomization"

OW-CPA dPKE

dP

$K = U[dP, F]$

"Hashing"

IND-CCA KEM

K

$rP = (Gen_r, Enc_r, Dec_r)$

$dP = (Gen_d, Enc_d, Dec_d)$
$\mathrm{Gen_d}(\,) = \mathrm{Gen_r}(\,)$
$\mathrm{Enc_d}(\mathrm{pk}, \mathrm{m}) = \mathrm{Enc_r}\big(\mathrm{pk}, \mathrm{m}; \mathbf{G}(\mathbf{m})\big)$
$\mathrm{Dec_d}(\mathrm{sk}, \mathrm{c}) = \mathrm{Dec_r}(\mathrm{sk}, \mathrm{c})$