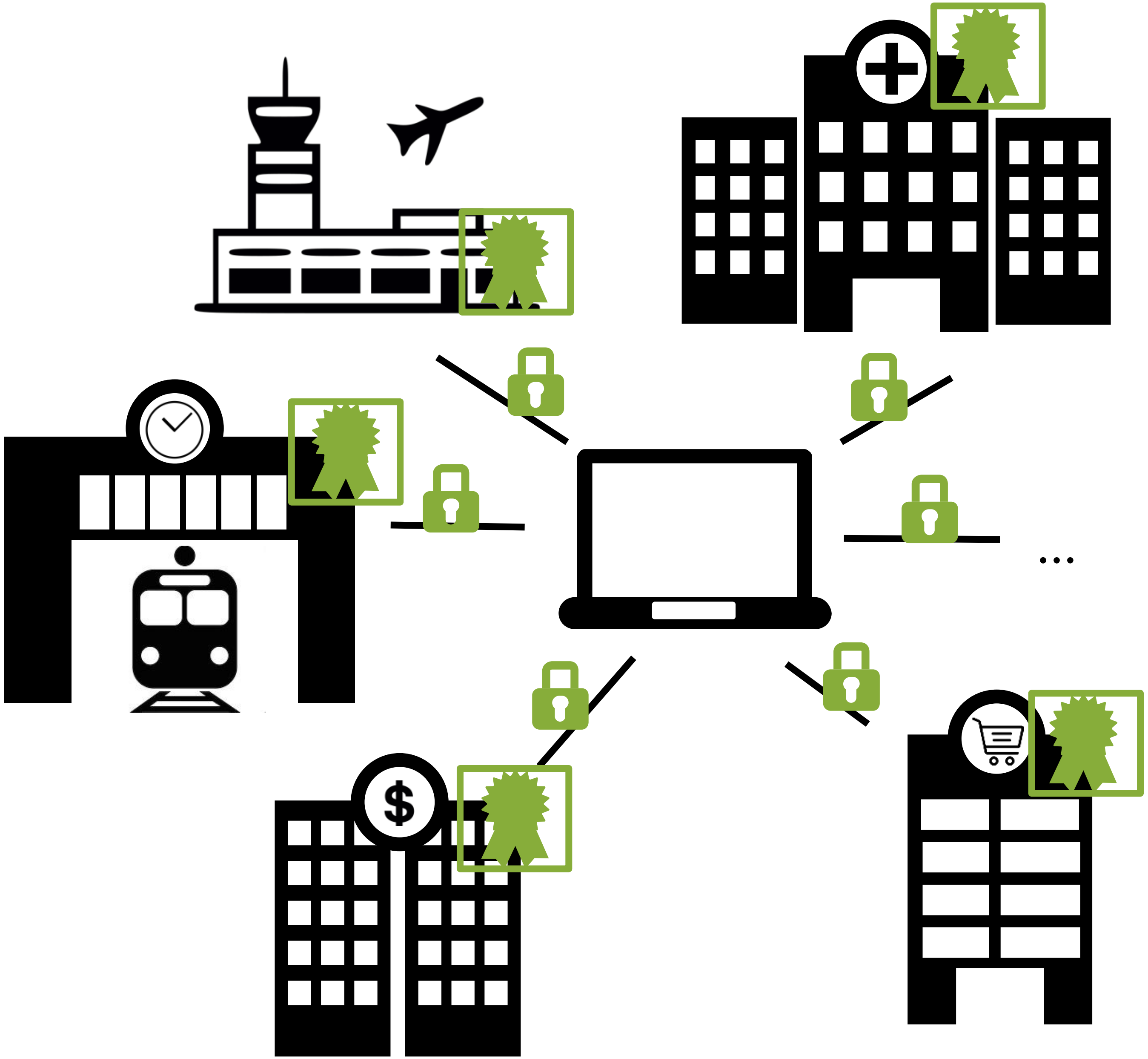
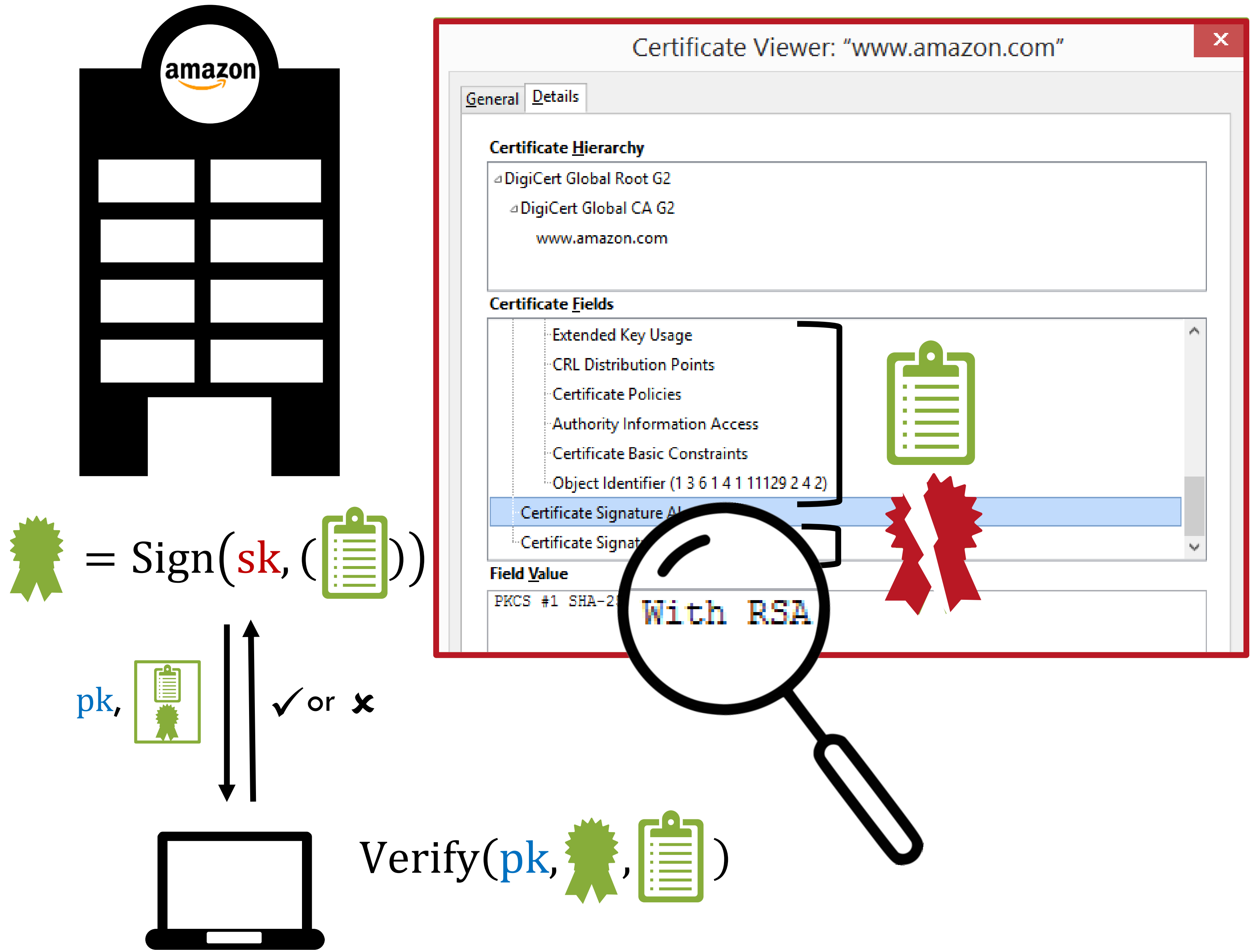
THE LATTICE-BASED DIGITAL SIGNATURE SCHEME QTESLA

Erdem Alkim
Paulo S. L. M. Barreto
Nina Bindel
Juliane Krämer
Patrick Longa
Jefferson E. Ricardini

ACNS 2020
October 2020

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing





Shor's quantum algorithm [Shor97]:

⇒ Recover sk

⇒ Generate RSA- for any

⇒ Need for - secure digital signature schemes

CONTRIBUTION

- **Description of the lattice-based digital signature scheme qTESLA**
- **Sketch of a security reduction from the hardness of the decisional LWE problem**
- **Instantiation with provable secure parameters**
- Constant-time reference implementation
- AVX2-optimized implementation
- **Comparison**

DESIGN OF QTESLA

QTESLA'S SECURITY ASSUMPTION

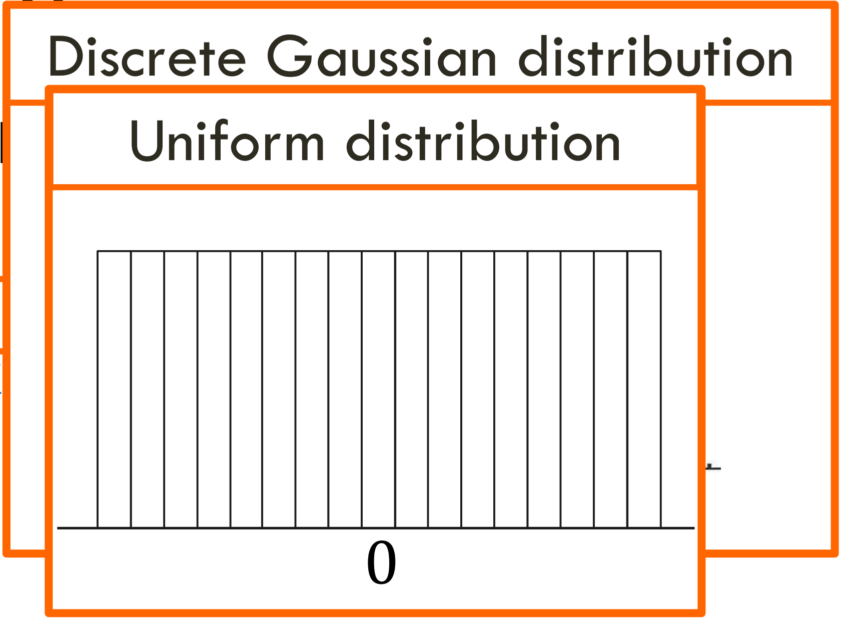
RLWE distribution:

Sample	$s, e_1, \ldots, e_k \leftarrow_\sigma R_n$
	$a_1, \ldots, a_k \leftarrow_\$ R_{n,q}$
Compute	$b_i = a_i s + e_i \bmod q, i = 1, \ldots, k$
Return	$(a_i, b_i), i = 1, \ldots, k$

qT

sk

pk



D-RLWE problem [Regev05,LPR12]

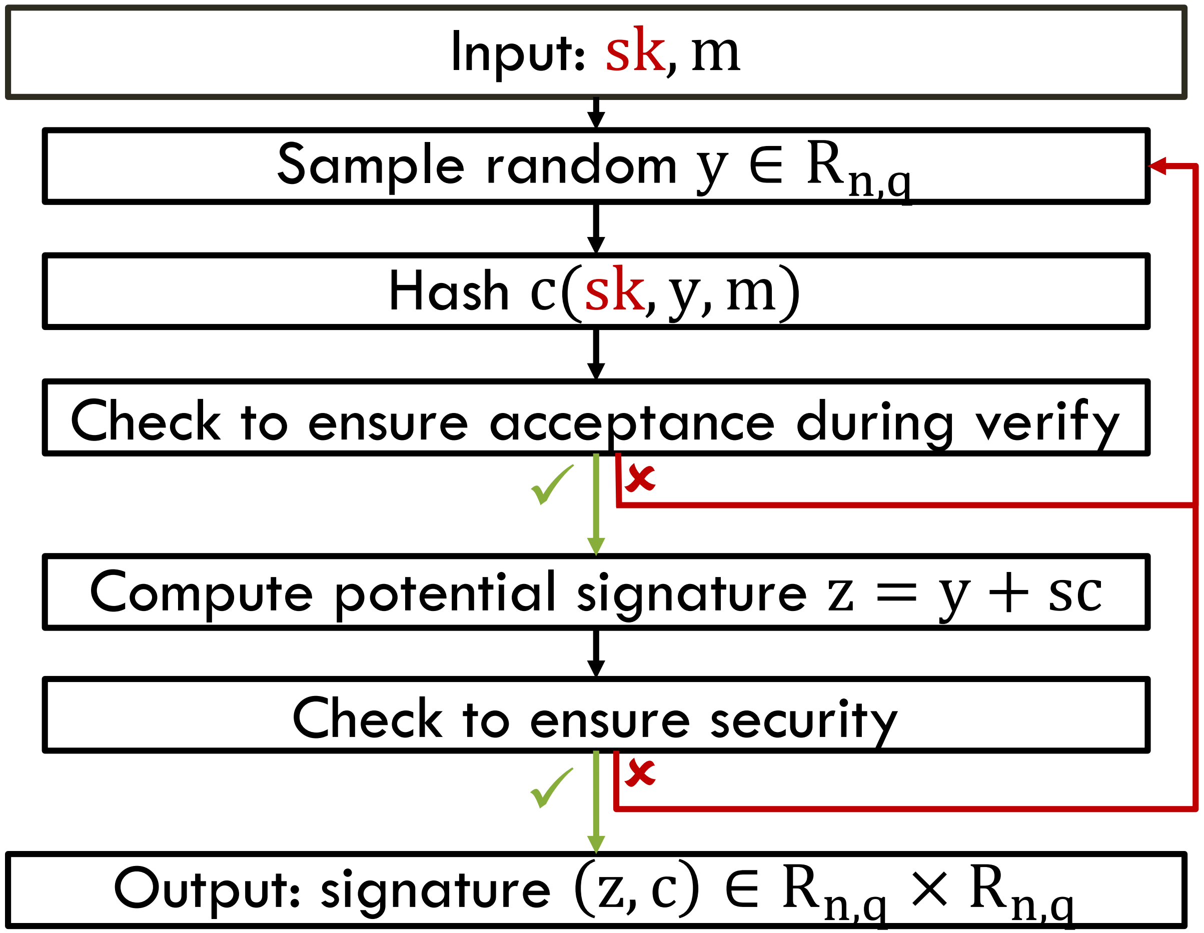
$(a_i, b_i)_{i=1,\ldots,k}$ → **?** →

$(a_i, b_i) \leftarrow_{RLWE} R_{n,q} \times R_{n,q}$

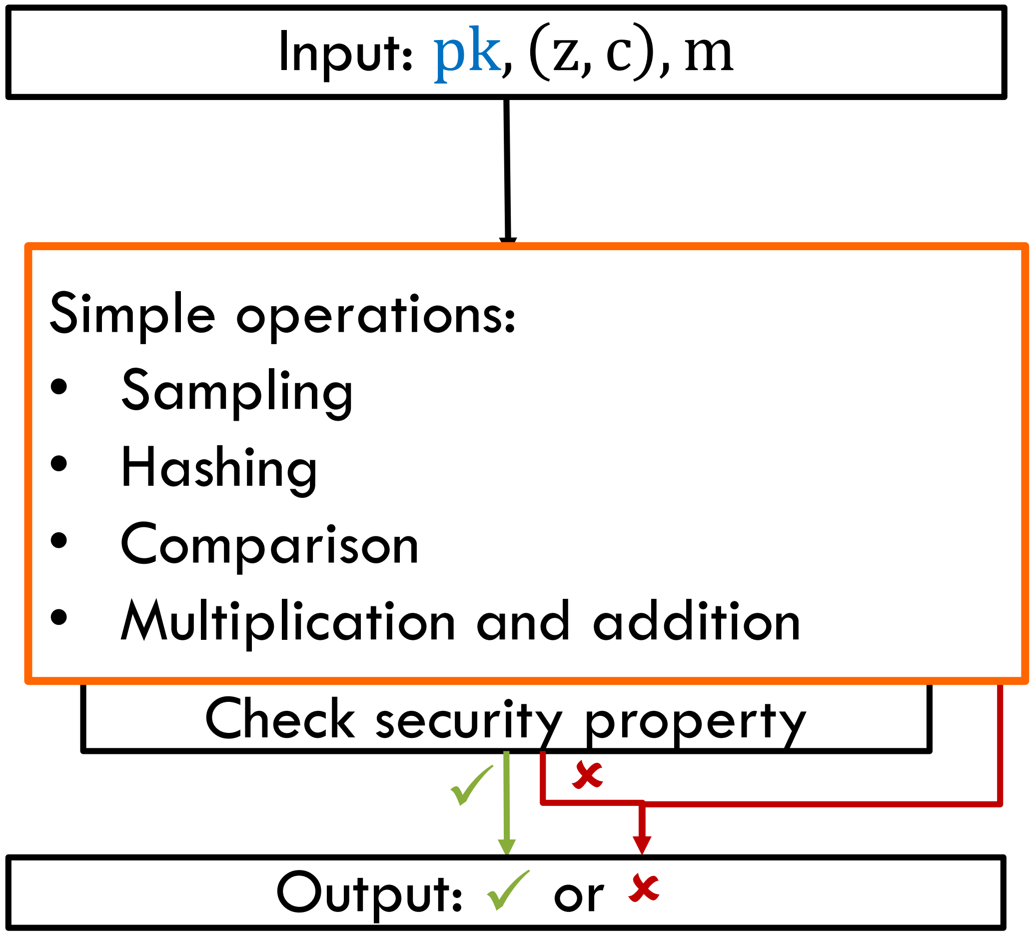
$(a_i, b_i) \leftarrow_\$ R_{n,q} \times R_{n,q}$

QTESLA SIGN AND VERIFY

Signature generation



Signature verification



SECURITY OF QTESLA

SECURITY OF QTESLA

qTESLA is secure against quantum adversaries
as long as D-RLWE is quantum hard.

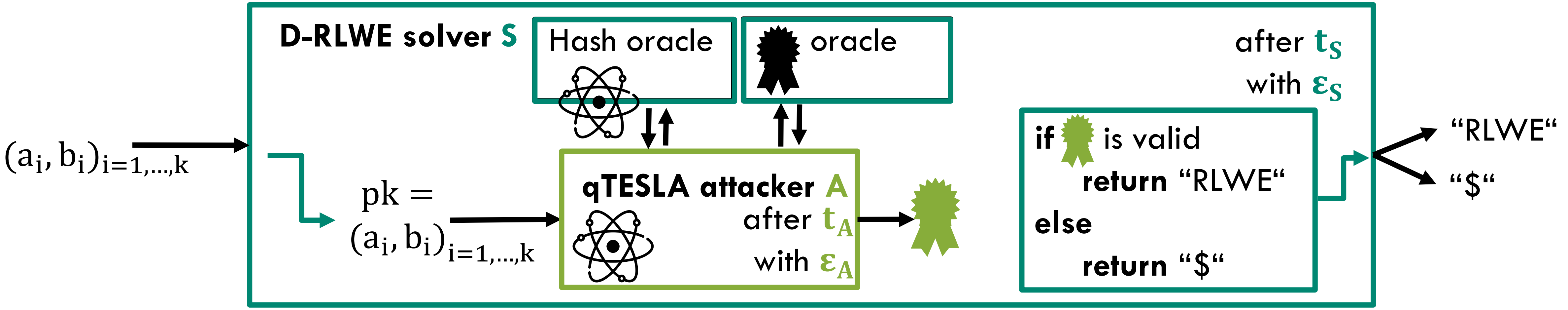
↑

Security reduction:

If there exists a polynomial-time quantum adversary A that breaks the security of qTESLA then there exists an algorithm S that solves D-RLWE in polynomial time.

SECURITY REDUCTION

If there exists a quantum adversary A that breaks qTESLA
then there exists an algorithm S that solves D-RLWE.



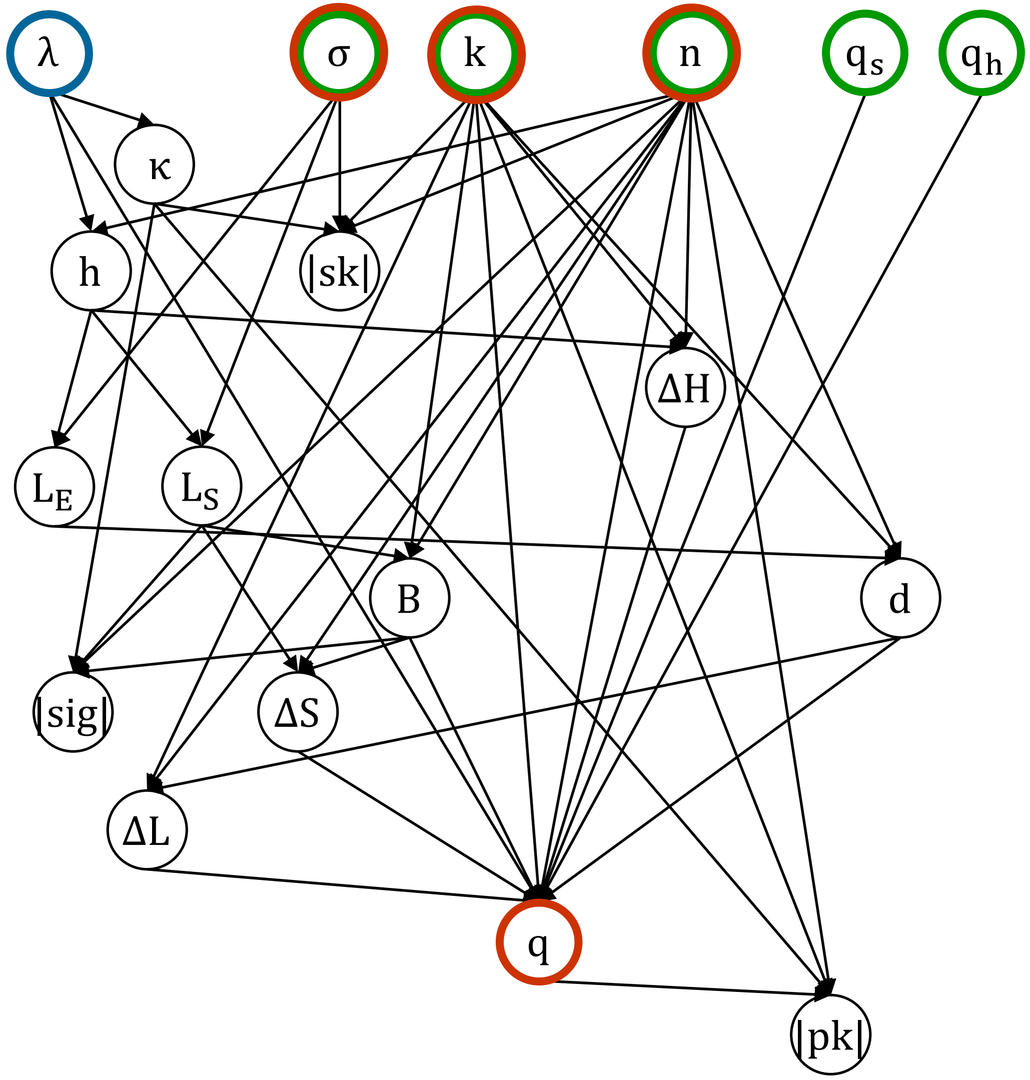
… #ops to solve/break instance

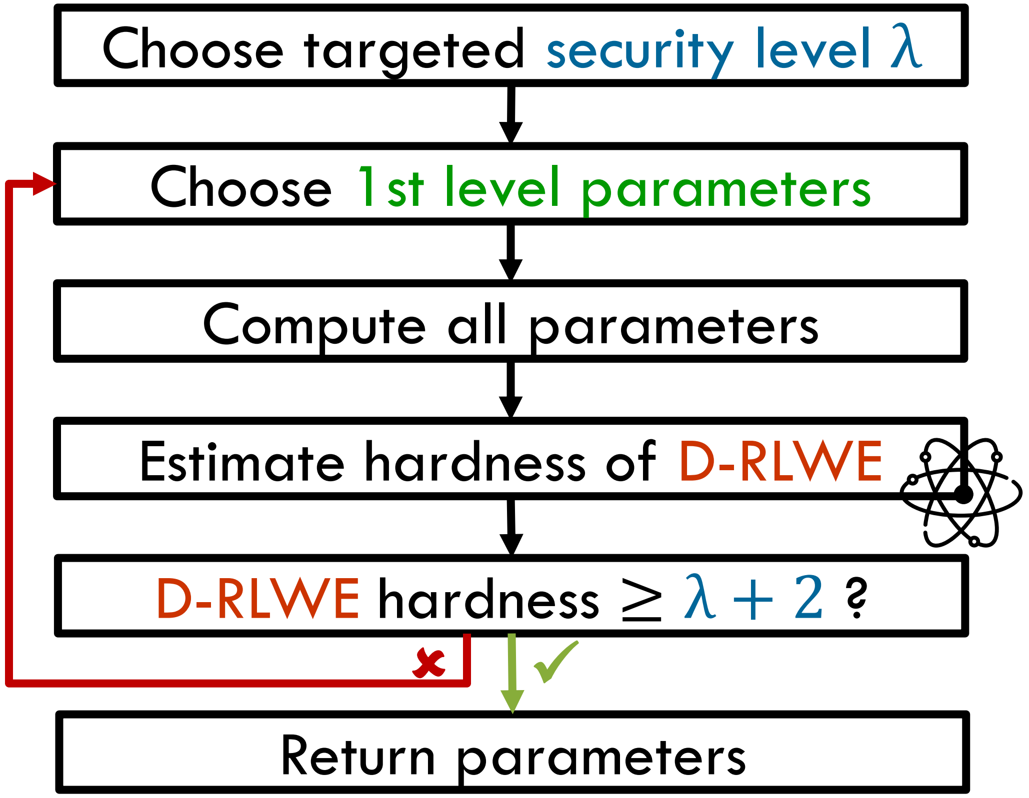
$$\varepsilon_A \leq \varepsilon_S + \varepsilon(q_s, q_h, \lambda, m, d)$$

$$t_A \geq t_S - t(q_h, q_s, d, B, q, h, L_S, L_E)$$

Tight reduction ⟹ Bit hardness η of D-RLWE $\approx$ Bit security $\lambda(\eta)$ of qTESLA

QUANTUM SECURE PARAMETERS





QTESLA'S PARAMETERS

	λ	κ	n	k	q	σ	h	$E = S$	B	d	b_{GenA}
qTESLA-p-I	95	256	1024	4	343, 576, 577	8.5	25	554	$2^{19} - 1$	22	108
qTESLA-p-III	160	256	2048	5	856, 145, 921	8.5	40	901	$2^{21} - 1$	24	180

EXPERIMENTAL EVALUATION OF QTESLA

COMPARISON (REFERENCE IMPLEMENTATION)

Scheme	Security [bit]	const. time	Sizes [B]		Cycle counts [k-cycles]		
						Reference	AVX2
qTESLA-p-I [a] (this paper)	95[b]	✓	pk:	14,880	sign:	3,089.9	1,759.0
			sig:	2,592	verify:	814.3	678.5
qTESLA-p-III [a] (this paper)	160[b]	✓	pk:	38,432	sign:	7,122.6	4,029.5
			sig:	5,664	verify:	2,102.3	1,746.4

Lattice

Symmetric

Multivariate

Speed-up 1.5x (mainly due to polynomial multiplication)

SUMMARY

- ★ Simple arithmetic operations
- ★ Tight quantum reduction from D-RLWE
- ★ Provably-secure parameters
- ★ Implementation security

ACKNOWLEDGMENTS

Special thanks to
Edward Eaton, Vadim Lyubashevsky,
Greg Zaverucha, Joo Woo,
Fernando Virdia, Martin Albrecht
and Shi Bai.

Round 2 submission in PQ standardization

NIST

Reference C implementation

qTESLA on FPGA-based CPU

liboqs library

OQS

CogniCrypt

BouncyCastle library

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

qtesla.org

IACR eprint 2019/085

THANKS.