A FRAMEWORK FOR EFFICIENT LATTICE-BASED DAA

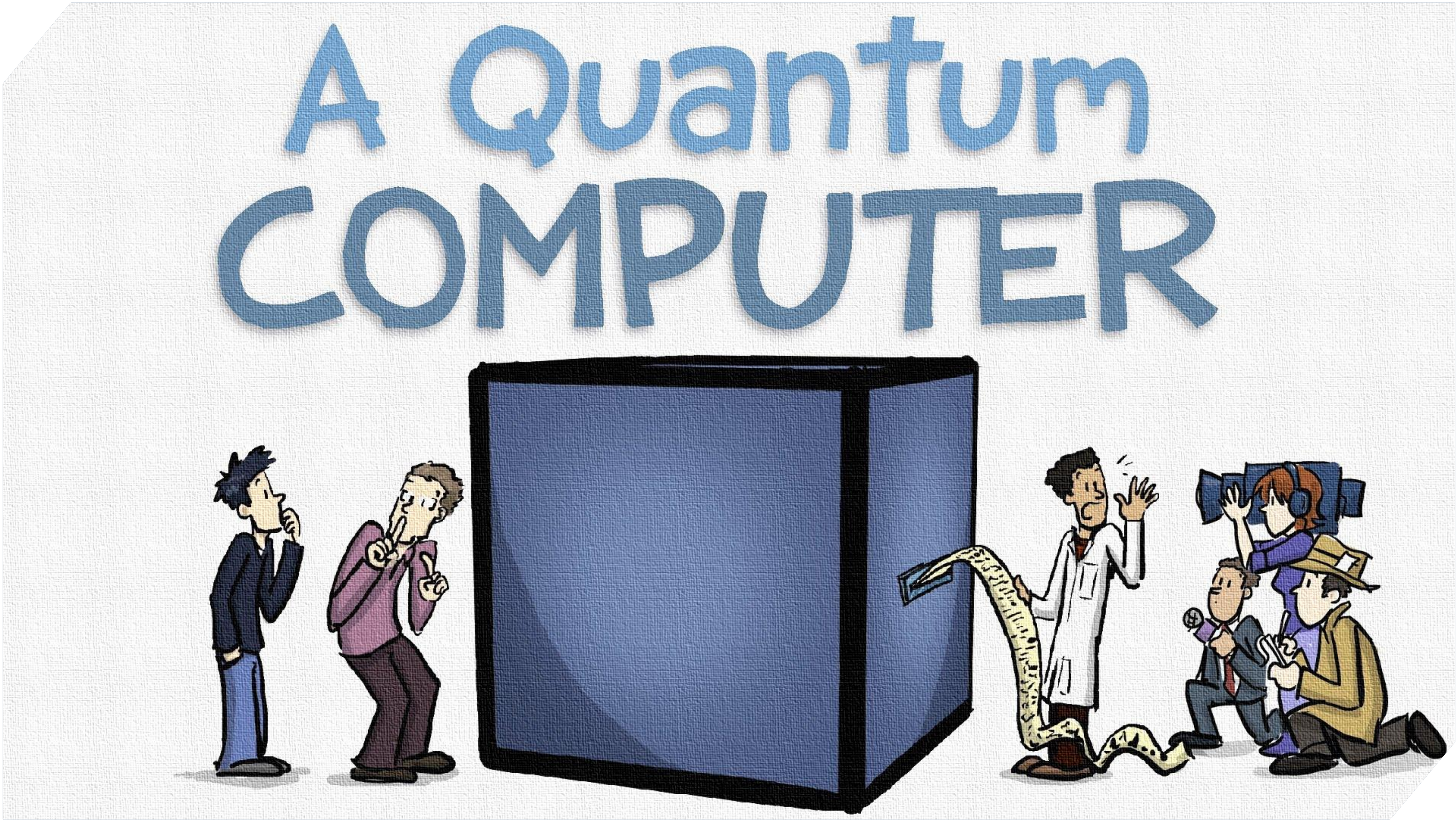
Liqun Chen

Nada El Kassem

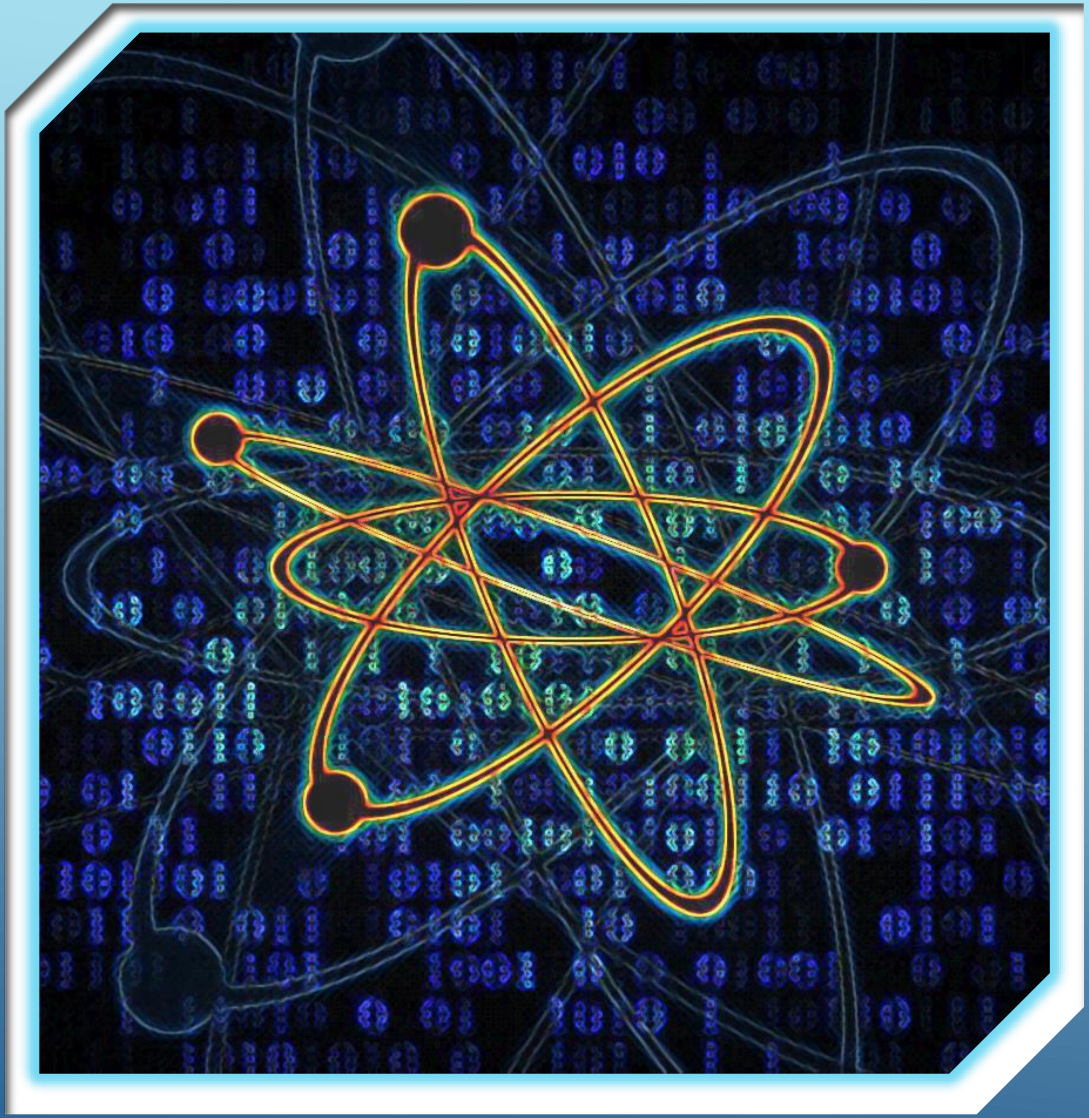
Anja Lehmann

Vadim Lyubashevsky

CYSARM 2019
15/11/2019


A Quantum
COMPUTER

EFFICIENCY OF QUANTUM COMPUTERS



- A quantum computer uses qubits that can be one and zero at the same time(This is called superposition).

- Superposition allows quantum computers to store exponentially more data than binary machines, and to work much faster.

HOW SECURE WILL OUR CURRENT CRYPTOGRAPHY BE WHEN FULL SCALE QUANTUM COMPUTER ARRIVES?

Most current public key crypto-systems rely on the difficulty of two specific problems:

- Integer factorization
- Discrete logarithm in a prime field or an elliptic curve
- Unfortunately, Shor's Algorithm for a quantum computer is effective against precisely these problems.

LATTICE BASED CRYPTOGRAPHY

- **Lattice-based Cryptography is conjectured to be post-quantum secure.**

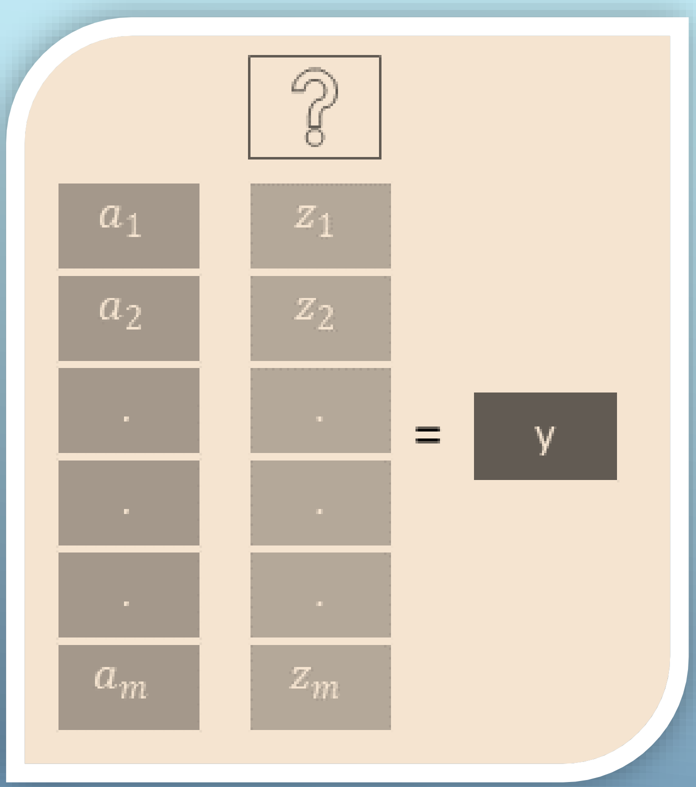
***There is no polynomial-time (even quantum) algorithm that approximates lattice problems to within polynomial factors**

HARD PROBLEMS OVER LATTICES

The Ring Short Integer Solution Problem (R-SIS$_{n,m,q,\beta}$)

- Given m uniformly random element $\mathbf{a}=(a_1, a_2,\ldots, a_m)$, where $a_i \in$ $\mathbf{R}_q$. The Ring Short Integer Solution problem asks to find $\mathbf{z}=(z_1, z_2,\ldots, z_m)$with $|\mathbf{z}| < \beta$ and such that: $\mathbf{a}\ \mathbf{z} = 0$.

- The Ring Inhomogeneous Short Integer Solution problem R-ISIS$_{n,m,q,\beta}$ problem asks to find $\mathbf{z}=(z_1. z_2,\ldots, z_m)$ with $|\mathbf{z}| < \beta$ and such that: $\mathbf{a}\ \mathbf{z} = y$, for some uniform random polynomial y.



THE RING LEARNING WITH ERRORS (LWE) PROBLEM

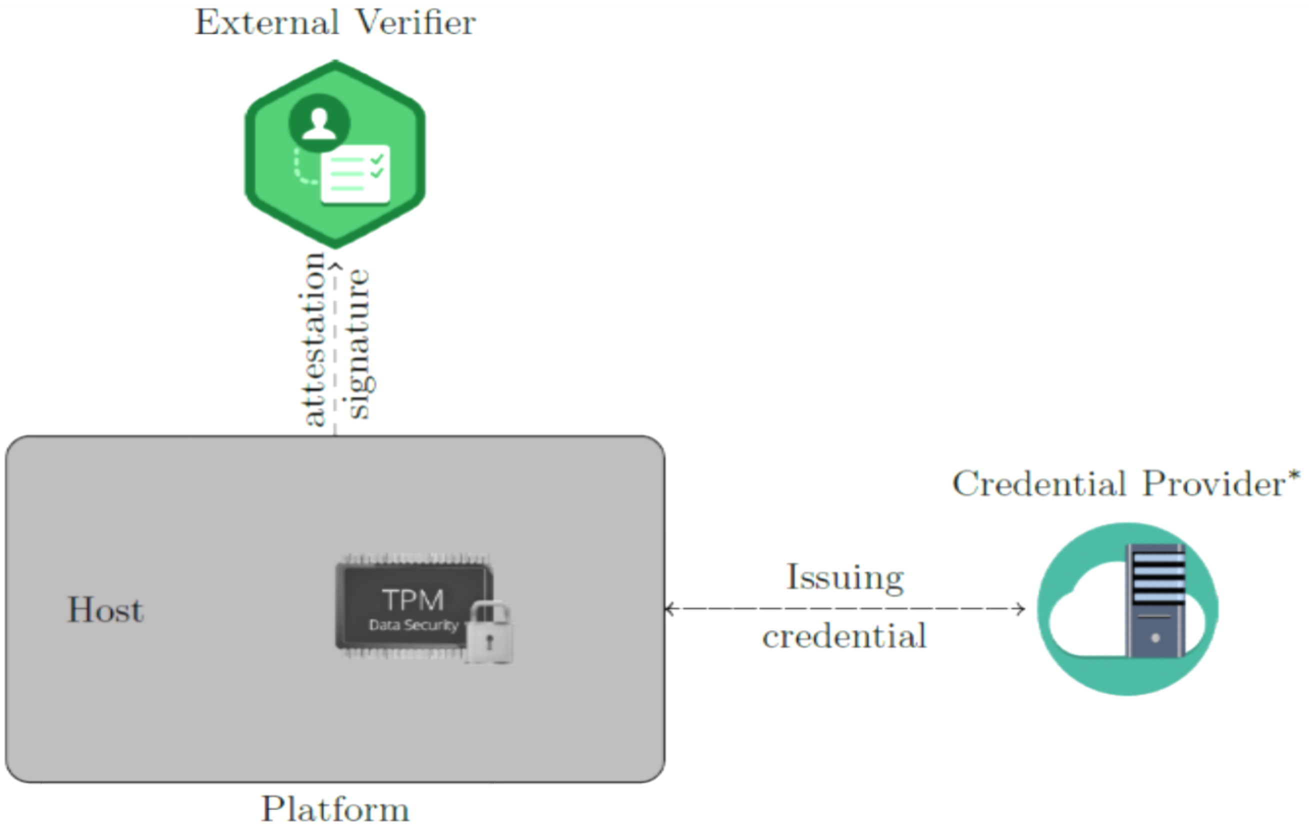
The search Ring LWE problem asks to return a secret short polynomial $s \in R_q$ given a Ring LWE sample $(a, b=as+e)$ from an LWE distribution $\mathcal{D}$, for a uniformly sampled secret s from R_q .

$$\boxed{a}\;\boxed{s} + \boxed{e} \overset{\boxed{?}}{=} \boxed{b}$$

DAA OVERVIEW

- Direct Anonymous Attestation (DAA) is an anonymous digital signature that aims to provide both signer authentication and privacy.
- This primitive was designed for the attestation service of the Trusted Platform Module (TPM).
- DAA signer consists of the TPM and an assistant signer called the host.
- DAA allows linkability of signatures via link tokens.
- TPM can be revoked if its private key is extracted.

DAA PROTOCOL



DAA INTERFACES

Setup

- The issuer sets the system parameters and it's public and secret keys.

Join

- TPM and a host together form a platform which performs the join protocol, while the issuer decides if the platform is allowed to become a member.

Sign

- Once being a member, the TPM and host together can sign a message m with respect to some input parameter called the base name (bsn)

Verify

- Any verifier can check that a signature on message m stems from a certified platform via a deterministic verify algorithm.

Link

- Only when the platform signs repeatedly with the same base name bsn, it will be clear that the resulting signatures were created by the same platform

AN EFFICIENT LATTICE-BASED DAA PROTOCOL (SETUP / JOIN)

❑ Let $R_q = Z_q[X]/\langle X^d + 1\rangle$. The issuer secret key is a matrix $Q \leftarrow R^{2\times 2}$, and his public key is a uniformly-random polynomial $h \leftarrow R_q$ and a vector $b = [h \ 1] \cdot Q$.

❑ Our DAA credential a modification of the [ABB10] lattice-based signature scheme but with an additional term ‘ae’ on the right side of (1)

❑ The credential s was a small-norm polynomial satisfying

$$[h \mid b + iG]s = u + ae \qquad (1)$$

where A, B,G is the gadget matrix $(1 \quad \sqrt{q} \;)$,u and a=(a1,a2) are public parameters over the polynomial Ring R_q, and e=(e1,e2) represents a short TPM’s secret key.

- **[ABB10] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In EUROCRYPT, pages 553–572, 2010.**

AN EFFICIENT LATTICE-BASED DAA PROTOCOL (SIGN)

❑ To construct a signature on a message μ with respect to a base-name bsn,

- The TPM creates a link token nym = H(bsn)e_1 + e ′ for some short polynomial error e', with a non-interactive ZKPoK π_1 about the construction of 2nym.

- The TPM and the host make a joint non-interactive ZKPoK π_2 to prove knowledge of the secrets $\overline{S}$ and $\overline{e}$ satisfying

$P\overline{S}$ - a $\overline{e}$ = $\overline{c}$ u with P is a matrix that contains h, b and the commitments of the identity i.

$\overline{S}$, $\overline{e}$ are slightly larger than s and e respectively, $\overline{c}$ ϵ $\overline{C}$ for some challenge space C.

- The signature is σ=(nym, bsn, π=(π_1 , π_2))

AN EFFICIENT LATTICE-BASED DAA PROTOCOL (VERIFY)

- To verify a signature σ=(nym, bsn, π=(π_1 , π_2)) on a message μ, the verifier verifies π. Thus, for every e1 ∈ RL,
- For all e_1 in the Revocation List that contains all the rogue TPM's secret keys, the verifier checks that $\|2(nym - H(bsn)e_1)\|$ is not small.
- If all checks pass, it outputs 1 and 0 otherwise.

AN EFFICIENT LATTICE-BASED DAA PROTOCOL (LINK)

- On input two signatures (nym_1, bsn, σ_1)and (nym_2, bsn, σ_2) for the same base-name bsn, the verifier checks whether both pseudonyms nym_1, nym_2 match to the same TPM.
- Given pseudonyms nym_1 and nym_2 for the same base-name bsn, signatures are linked to the same TPM if $2(nym_1 - nym_2)$ is a polynomial in R_q with small norm.

CYCARM 2019, 15/11/2019.

SECURITY OF THE SCHEME

The security of our proposed scheme is proved in the Universally Composable UC model under the assumptions of the hardness of the Ring LWE and the Ring-SIS problems, and the unforgeability of the ABB signature scheme.

EFFICIENCY OF THE SCHEME

- Our scheme should be faster than the other lattice based DAA schemes, [KCB+19] and [BK17], in terms of the TPM’s computation costs in the join and sign interfaces, and have smaller TPM keys and signature sizes.

- The signature size of our proposed DAA scheme is around 2MB, which is (at least) two orders of magnitude smaller compared to existing post-quantum DAA schemes.

- A future work is implementing the scheme to check if it is suitable for inclusion in the future TPM, this work is in collaboration with the European H2020 Future TPM project.

[KCB+19] Nada Kassem, Liqun Chen, Rachid El Bansarkhani, Jan Camenisch Ali El Kaafarani,Patrick Hough, Paulo S´ergio Alves Martins, , and Leonel Sous. More efficient, provably secure direct anonymous attestation from lattices. In Future Generation Computer Systems.

[BK17] RE Bansarkhani and AE Kaafarani. Direct anonymous attestation from lattices. 2017

QUESTIONS?

THANK YOU!