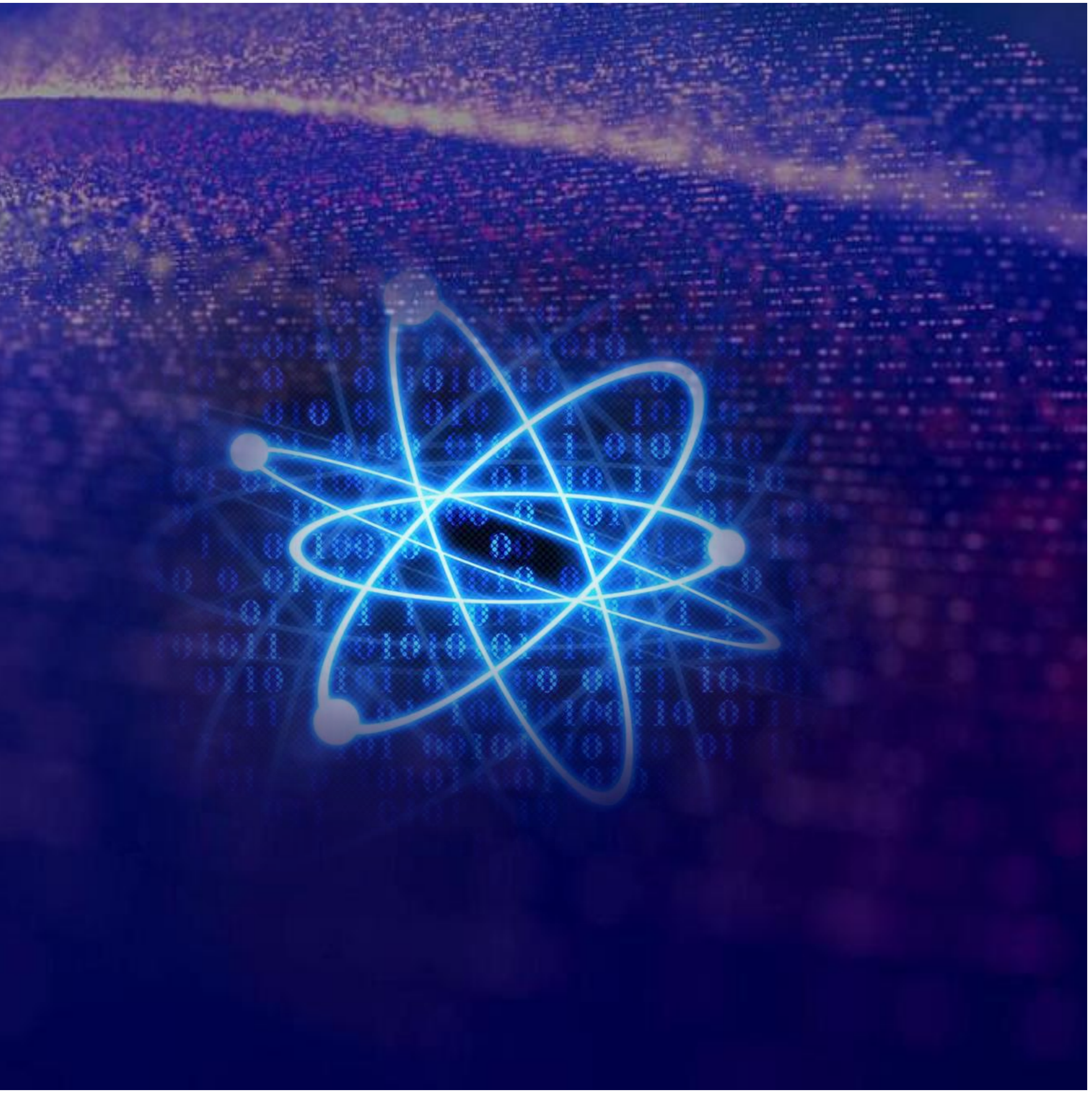
Post-Quantum Direct Anonymous Attestation (PQ-DAA)

Nada El Kassem

University of Surrey

www.project-assured.eu



ASSURED

Quantum Computing (Q-bits)

> A classical binary bit is physically realized with a state equal to 0 or 1.

> In quantum computing, a qubit or quantum bit is the basic unit of quantum information.

> A qubit is a two-state quantum-mechanical system, qubits can achieve a mixed state, called a "superposition" where they are both 1 and 0 at the same time.

This allows quantum computers to store exponentially more data than binary machines, and to work much faster!

A real Thread!

- Currently standardized signature schemes have their security based on the factoring and the discrete logarithm problems and are therefore insecure against quantum attackers as a result of Shor's quantum algorithm.

- In 1994 Peter Shor showed that a quantum computer could be used to factor a number n in polynomial time, thus effectively breaking RSA.

Overview

- There are two kinds of cryptosystems; symmetric and asymmetric. Symmetric cryptography can also be affected by specific quantum algorithms; however, its security can be increased with the use of larger key spaces.

- Quantum algorithms can break the present asymmetric crypto-schemes whose security is based on the difficulty of factorizing large prime numbers and the discrete logarithm.

- Even the elliptic curve cryptography which is considered presently the most secure and efficient scheme is broken against quantum computers.

Consequently, a need for quantum-attacks-resistant cryptography.

Current Cryptography

ASSURED

Asymmetric
PK ≠ SK (encryption\digital signatures)

RSA
Factorization of large numbers

DSA
Calculation of discrete logarithms

Elliptic curve crypto
ECDSA, ECDH

Post Quantum crypto

- Lattice-based
- Code-based
- Multi-Variate
- Symmetric

Symmetric
SK share

Advanced Encryption Standards (AES)

Double the Key sizes

AES of Key sizes 192 and 256 are still post-quantum secure

Hash functions

At least triple the out-put size

SHA-2 and SHA-3 remain quantum resistant

COMPARISON OF THE SECURITY LEVELS

ASSURED

TABLE III. COMPARISON OF CLASSICAL AND QUANTUM SECURITY LEVELS FOR THE MOST USED CRYPTOGRAPHIC SCHEMES

Crypto Scheme	Key Size	Effective Key Strength/Security Level (in bits)	
		Classical Computing	Quantum Computing
RSA-1024	1024	80	0
RSA-2048	2048	112	0
ECC-256	256	128	0
ECC-384	384	256	0
AES-128	**128**	**128**	**64**
AES-256	**256**	**256**	**128**

*** https://arxiv.org/pdf/1804.00200.pdf**

NIST PQC Candidates

ASSURED

	Signatures		KEM /Encryption		Overall	
	First Round	Second Round	First Round	Second Round	First Round	Second Round
Lattice-based	5	3	21	9	26	12
Code-based	2	0	17	7	19	7
Multi-Variate	7	4	2	0	9	4
Symmetric	3	2			3	2

Digital Signature to be Standardized

CRYSTALS-Dilithium (Lattice-based)

FALCON (Lattice-based)

SPHINCS$^+$ (hash-based)

Dilithium

ASSURED

- The lattice-based signature scheme. Dilithium is one of the strong candidates submitted for the NIST standardization process of post-quantum cryptography.

- The Dilithium signature scheme is based on the Fiat-Shamir paradigm.

- The design is simple to securely implement everywhere – uses only uniform sampling.

Falcon

- Uses Hash and signs signatures over NTRU.
- Having compact keys.
- Implementation is quite heavy.

SPHINCS+

- Hash-based signatures are attractive as they can be proven secure in the standard model under well-known properties of hash functions such as collision resistance.
- SPHINCS+ beats the performance of other symmetric crypto-based signatures for comparable parameters.
- SPHINCS+ has a tight security reduction to the security of its building blocks, i.e., hash functions
- At the 128-bit post-quantum security level, signatures are about 41 kB in size, and keys are of size of about 1 kB each.

SPHINCS+

- A SPHINCS tree needs to be considerably large

- To verify this chain of paths and signatures, the verifier iteratively reconstructs the public keys and root nodes until the root node at the top of the SPHINCS+ hypertree is reached.

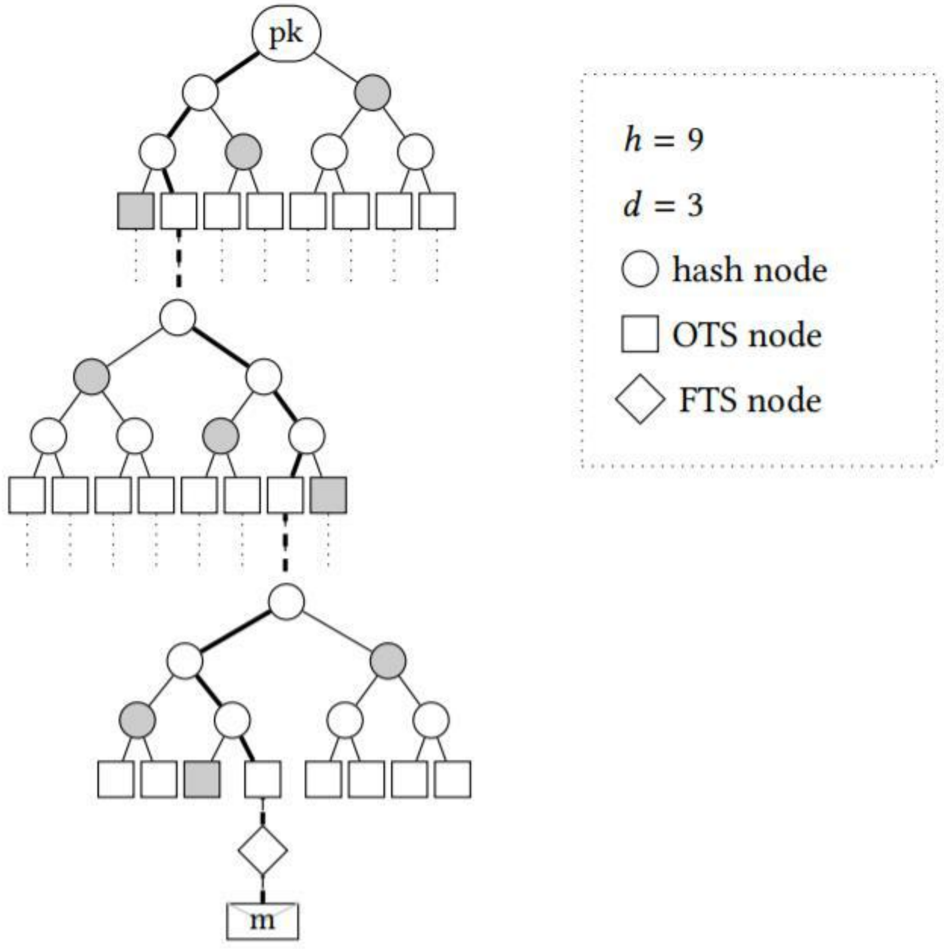
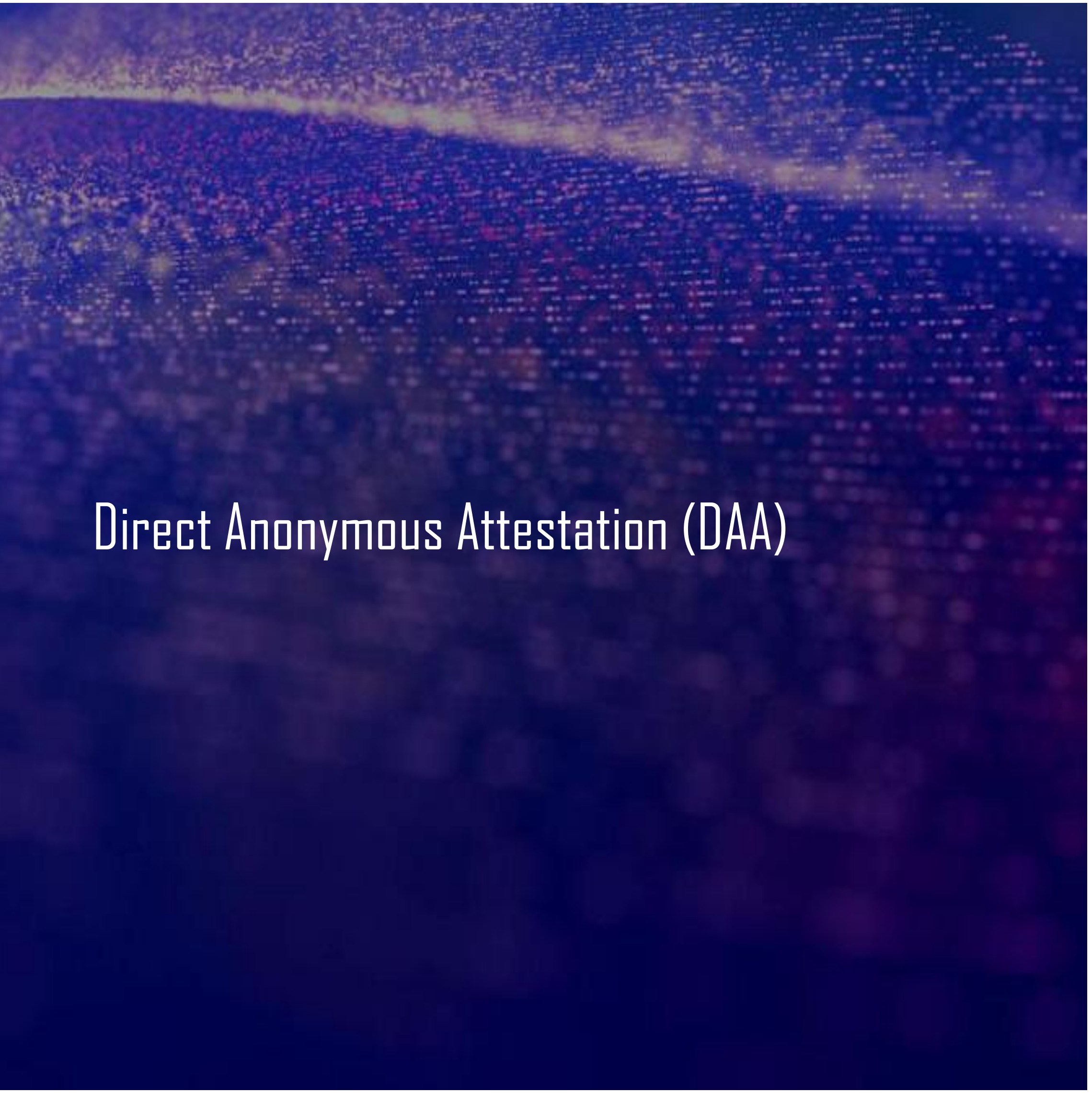


Figure 1: An illustration of a (small) SPHINCS structure.

Comparison with Current Crypto

	Signature size (Bytes)	PK size (bytes)	SK size (bytes)
RSA-2048	250	250	250
RSA-4096	500	500	500
ECDSA-256	62.5	31.25	31.25
SPHINCS+	**30552**	48	96
Dilithium	2701	1472	-
Falcon	625	897	-

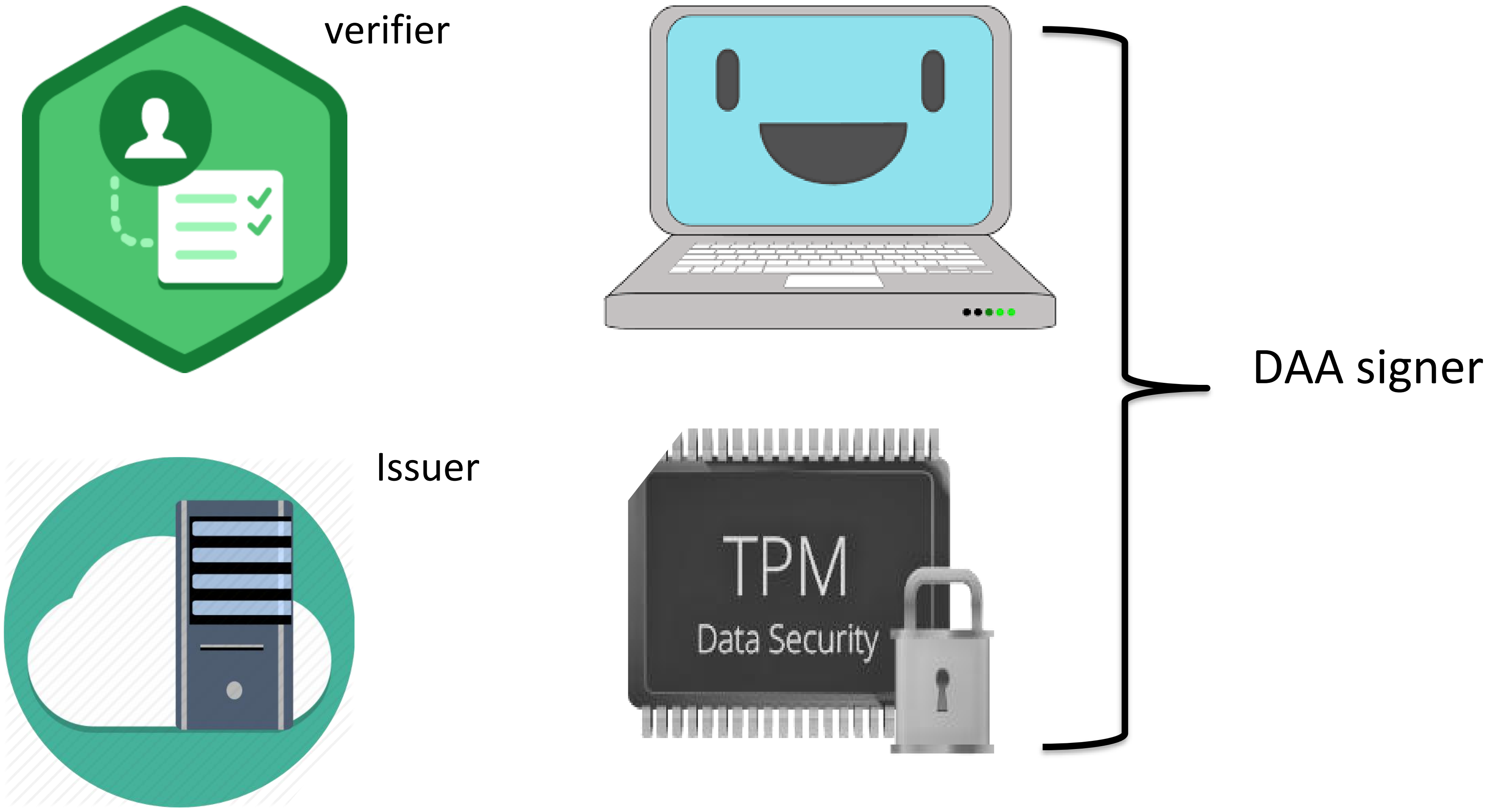
Direct Anonymous Attestation (DAA)



- 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 the linkability of signatures via link tokens.
- TPM can be revoked if its private key is extracted.

Direct Anonymous Attestation (DAA)

ASSURED

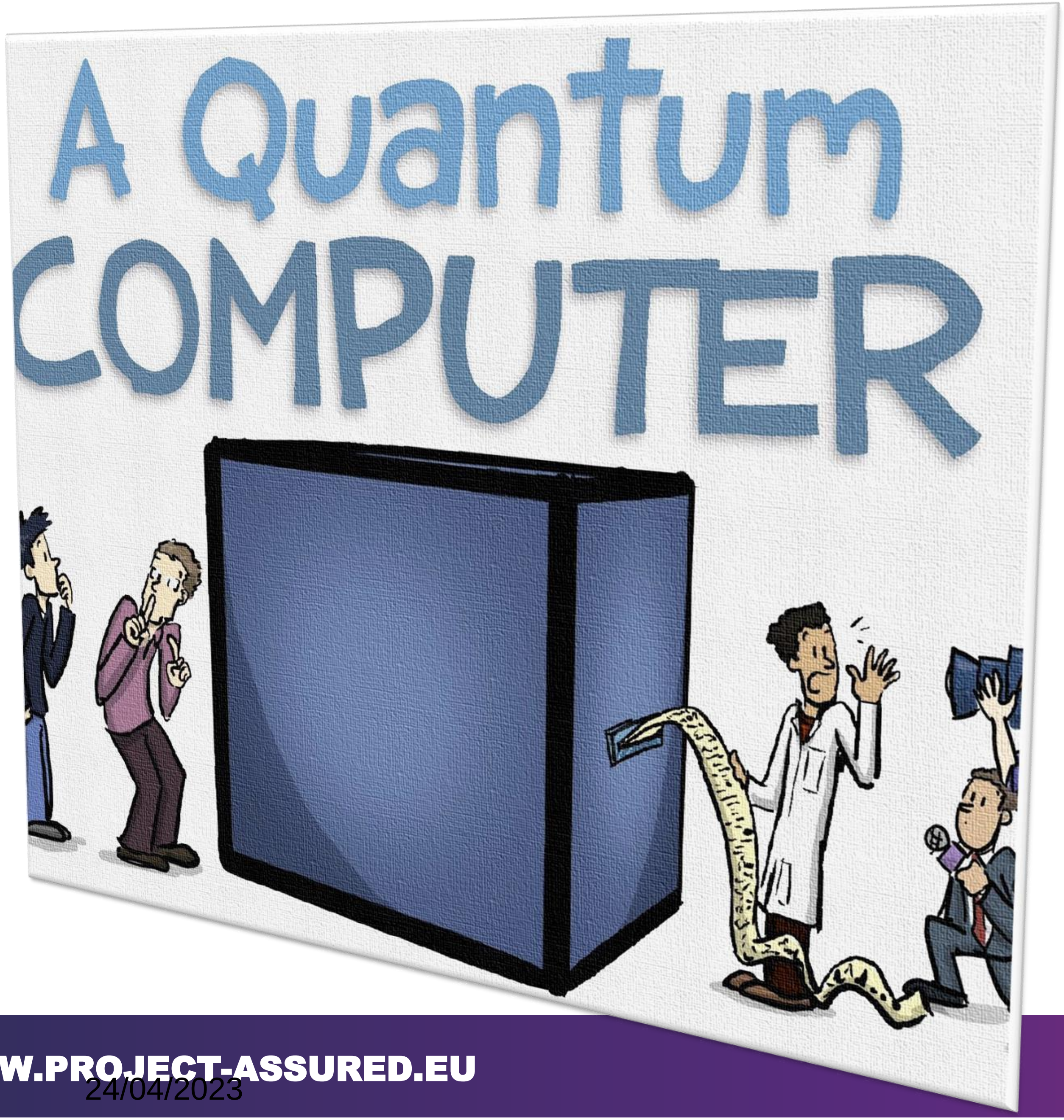


DAA Security Requirements

Unforgeability: No adversary without knowing the signing key can output a signature.

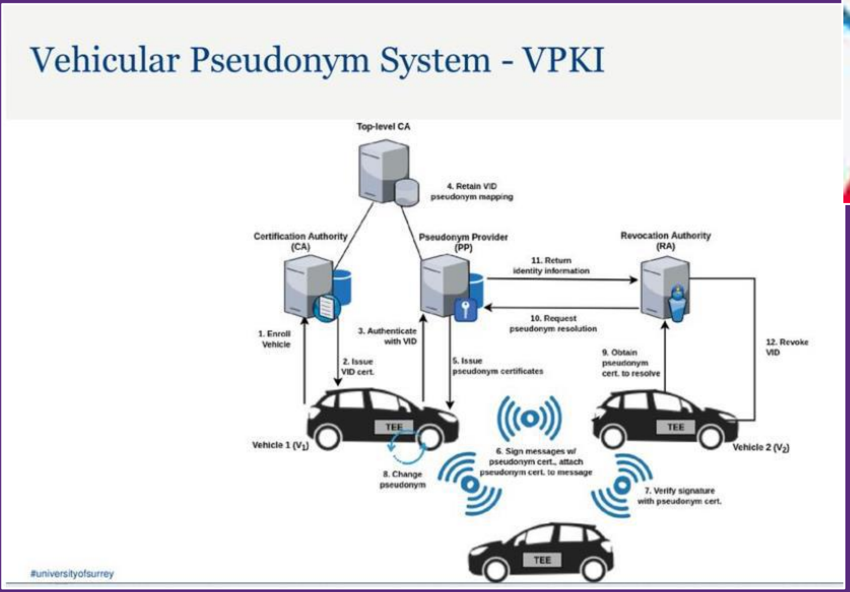
Anonymity: Starting from two valid signatures with respect to two different base-names, the adversary can't tell whether these signatures were produced by one or two different honest platforms.

Non-frameability: No adversary can produce a signature that links to signatures generated by an honest platform.



Currently standardised Direct Anonymous Attestation (DAA)schemes have their security based on the factoring and the discrete logarithm problems and are therefore insecure against quantum attackers as a result of Shor's quantum algorithm.

Some DAA Applications



Pictures taken from: https://slideplayer.com/slide/16147464/
https://abouttmc.com/wp-content/uploads/2017/11/Microsoft-TMC-Azure-cloud-secur.jpg

Lattice-based Enhanced Privacy ID (EPID)

- EPID is a more general scheme than DAA and thus does not split signers into TPMs and hosts, but also targets the creation of anonymous signatures.

- Like with DAA, one can check whether a certain signature was generated by a corrupt private key.

- Nonetheless, the ability to link signatures with the same base name is removed. Instead, whenever a signer is corrupted, they may be revoked by including one of their signatures as part of the signature revocation list SRL.
- EPID is capable of revoking corrupted signers from the system, even when their private key is kept hidden, whilst providing maximum privacy for the platforms.

- We designed two Lattice-based DAA schemes

(More Efficient, Provably-Secure Direct Anonymous Attestation (DAA) from Lattices, A Framework for Efficient Lattice-Based DAA) and an EPID (A Lattice-based Enhanced Privacy ID)

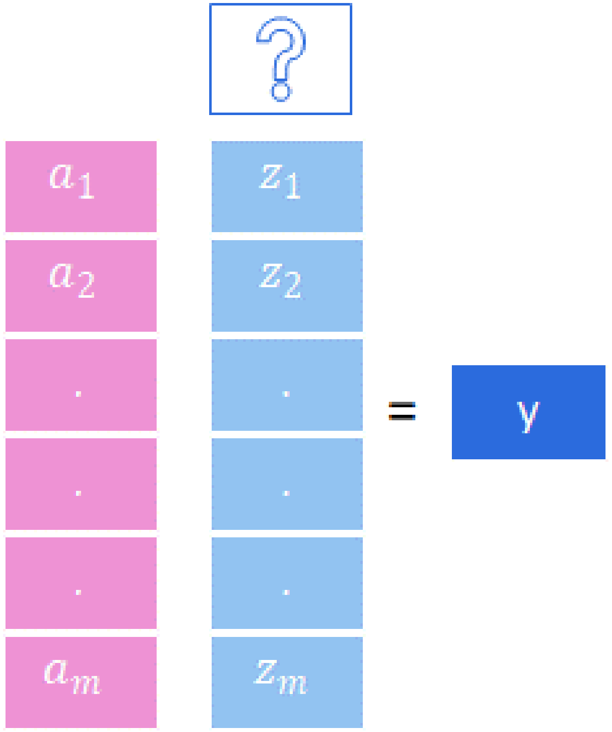
- The latest one is based on the Dilithium signature scheme.
- Another Hash-based DAA scheme based on the SPHINCS+ scheme is designed and submitted.

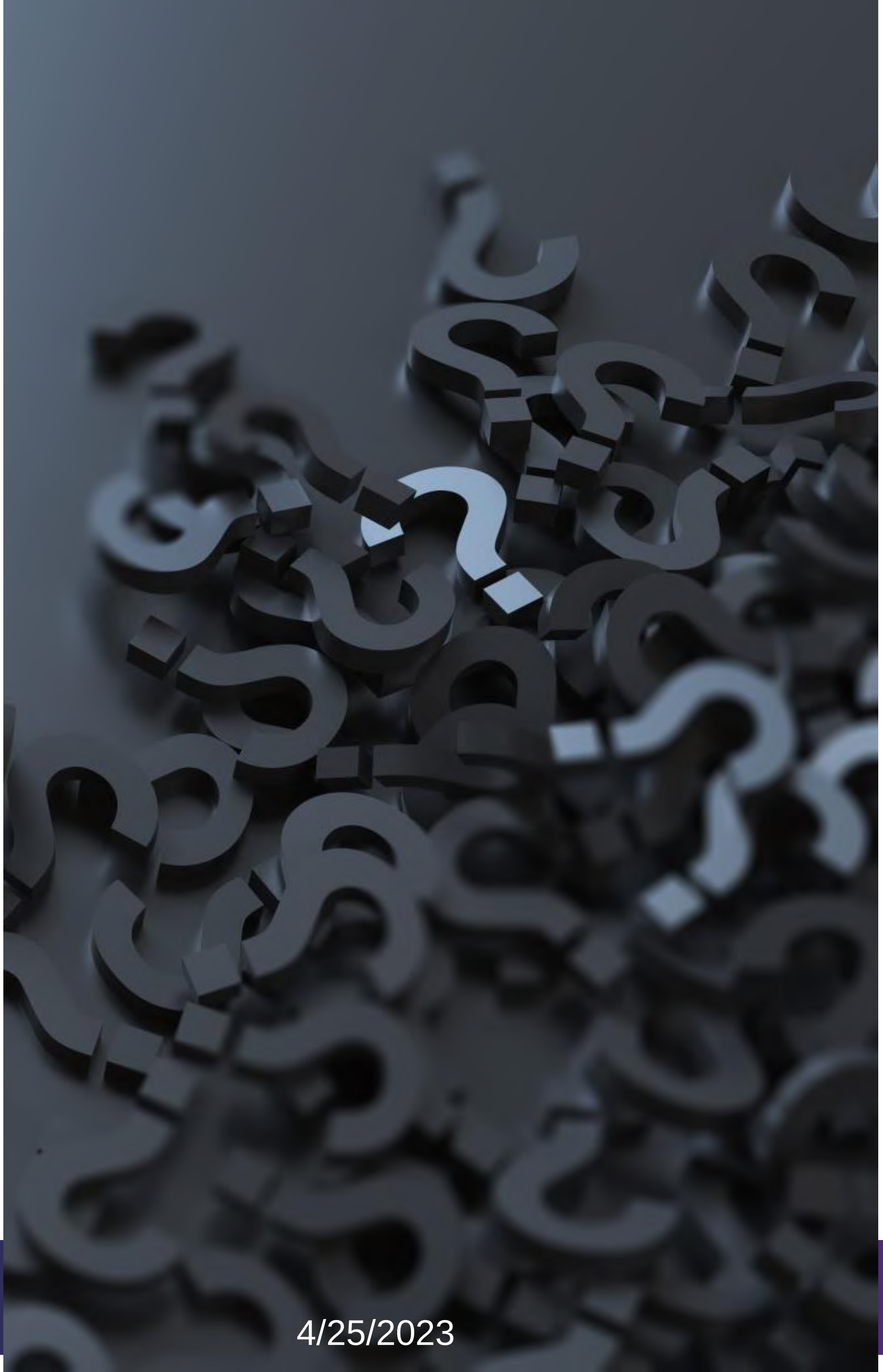
Hard Problems over Lattices

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

Given m uniformly random element **a**=(a_1, a_2,..., a_m), where ai in **R**q. The Ring Short Integer Solution problem asks to find **z**=(z_1, z_2,..., z_m)with |**z**| < β and such that: **a z** = 0.

- The Ring Inhomogeneous Short Integer Solution problem R-ISISn,m,q,β problem asks to find **z**=(z_1. z_2,..., z_m) with |**z**| < β and such that: **a z** = y, for some uniform random polynomial y.





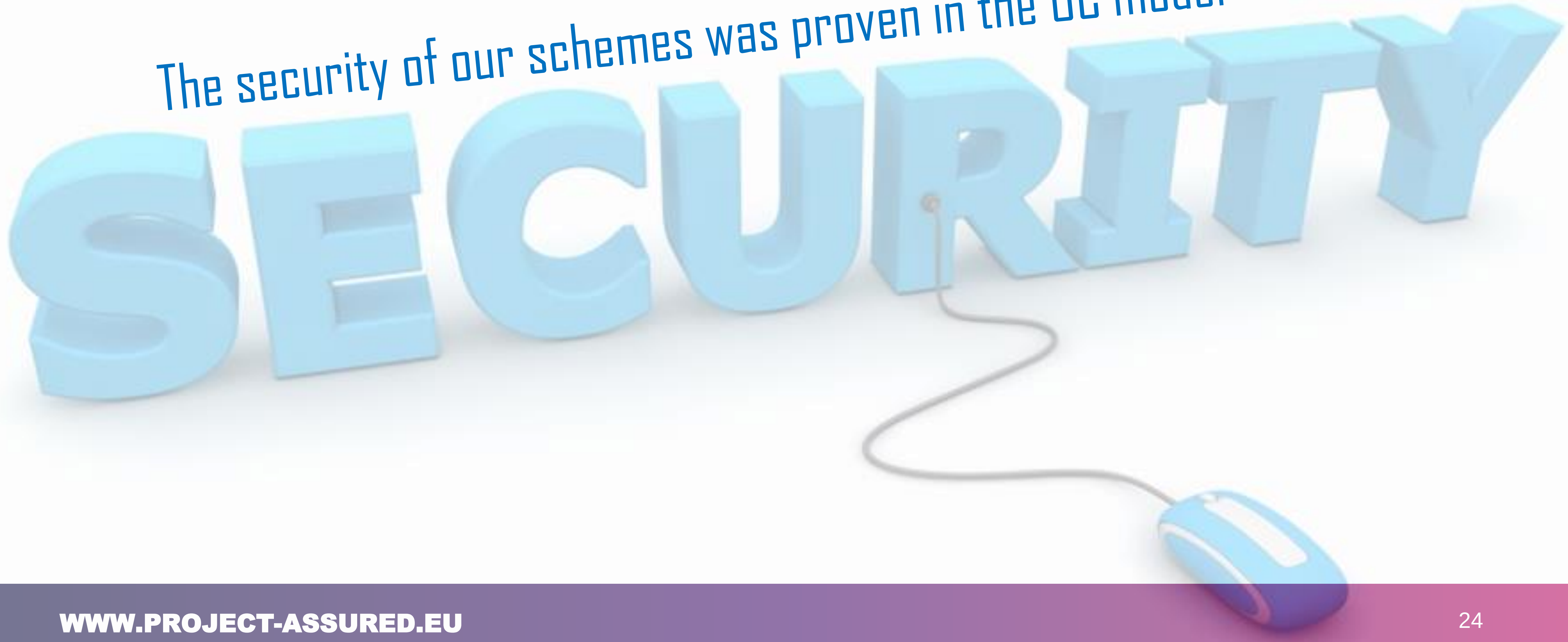
The RING Learning with errors (LWE) Problem

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

a s + e ? = b

ASSURED

The security of our schemes was proven in the UC model



Future Work

- To design a new lattice-based DAA based on the recent lattice-based Zero-Knowledge proofs.
- To work on shifting more complex designed protocols that have DAA as their main ingredients such as ASSURED SWARM attestation and Verifiable credentials (VC) to be PQ secure.
- Designing a QR-TPM that can manage PQ-DAA execution.

PARTNERS

ASSURED

UBITECH ubiquitous solutions

MARTEL innovate

Suite5 We Deliver Intelligence

netcompany intrasoft

SPACE

United Technologies Research Center

uni.systems

BIBA Bremer Institut für Produktion und Logistik

CITY OF ATHENS ΔΑΕΜ

TECHNISCHE UNIVERSITÄT DARMSTADT

TU Delft

DTU

UNIVERSITY OF SURREY

NVIDIA

THANKS

PROJECT-ASSURED.EU

@Project_Assured

ASSURED project is funded by the EU's Horizon2020
programme under Grant Agreement number 952697