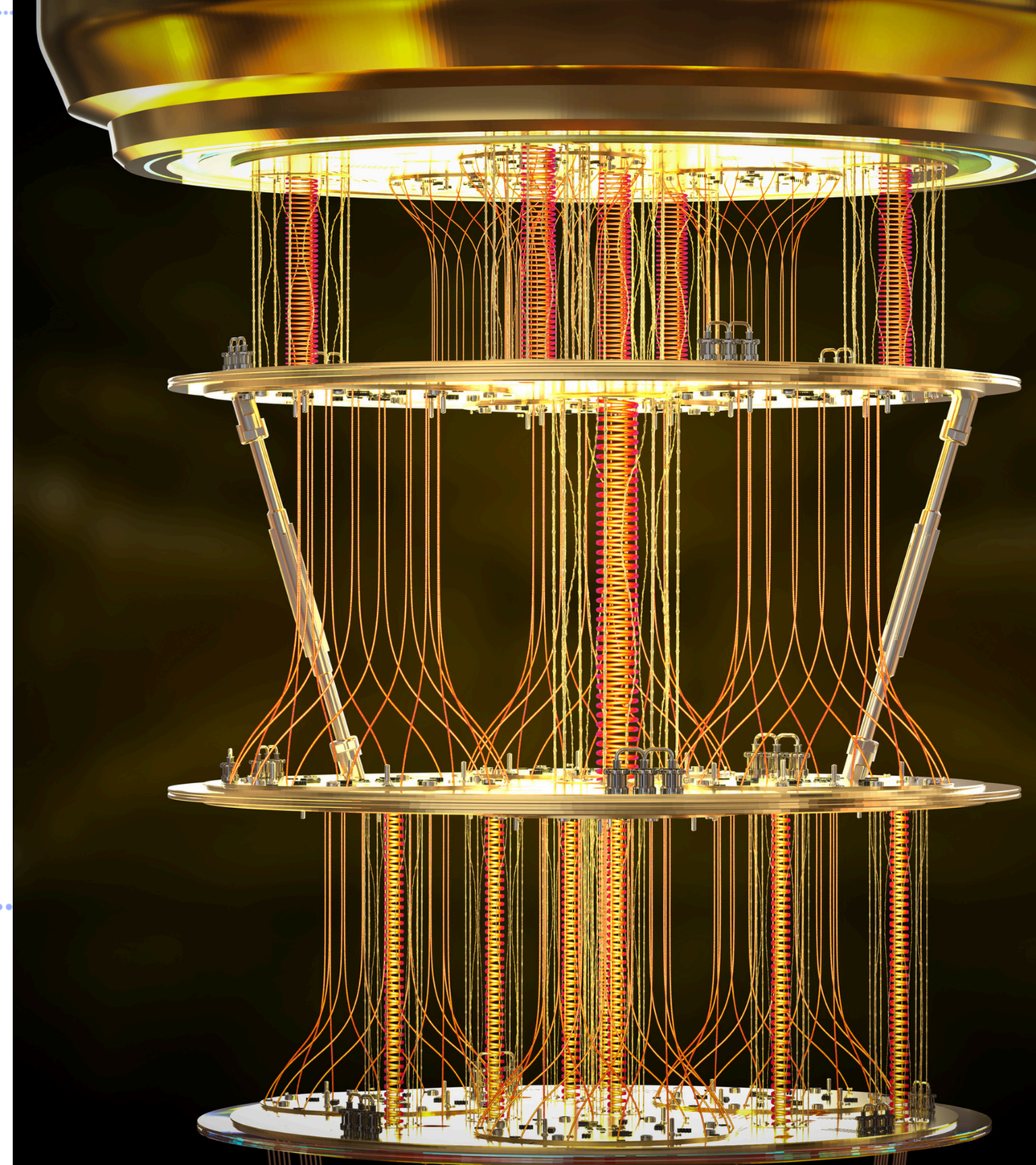
VNNIC
Internet for all

DNSSEC & RPKI IN THE POST-QUANTUM ERA

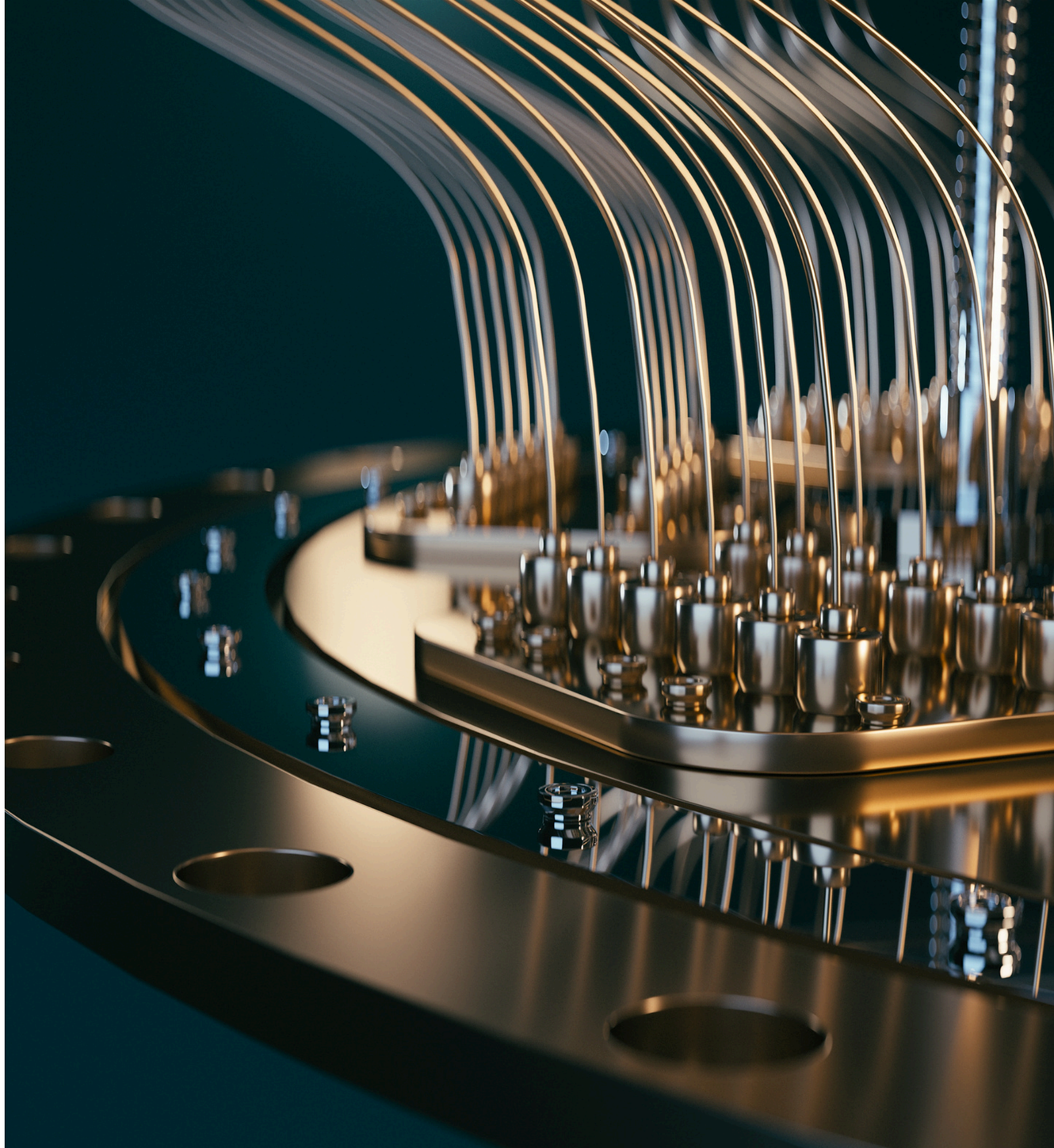
Nha Trang, 16-17 Oct

Tri Nguyen, VNNIC



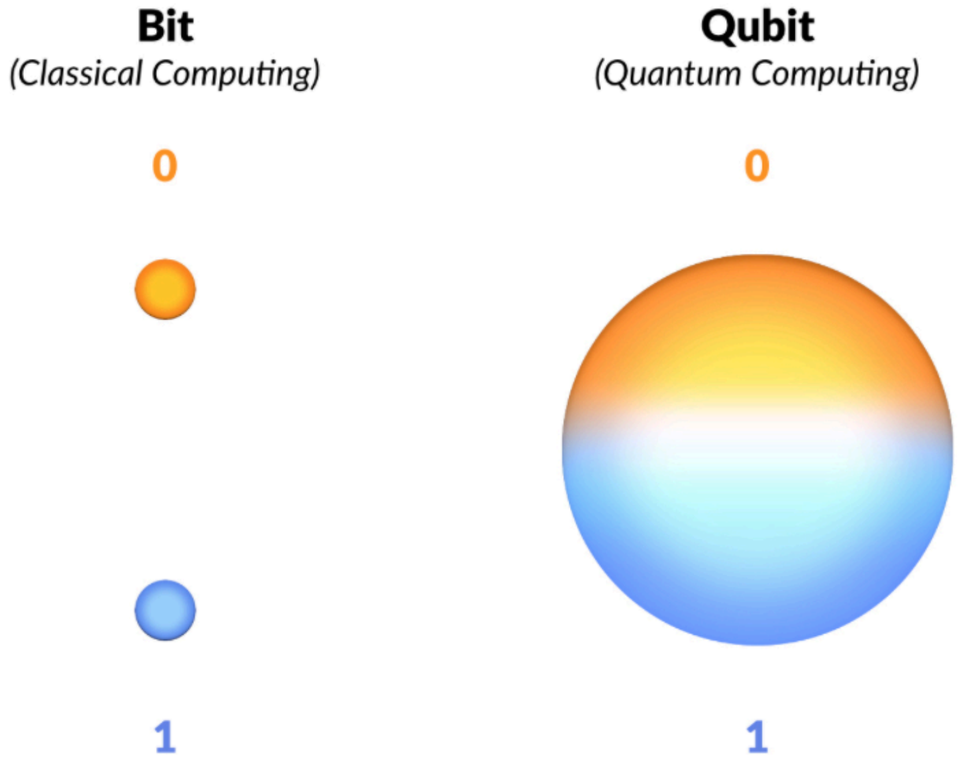
INTRODUCTION

- What is Quantum Computing & its impact on DNSSEC/RPKI
- Why Post-Quantum Cryptography (PQC) is needed
- Standardization and Support Overview PQC for DNSSEC & RPKI
- Conclusion



QUANTUM COMPUTERS

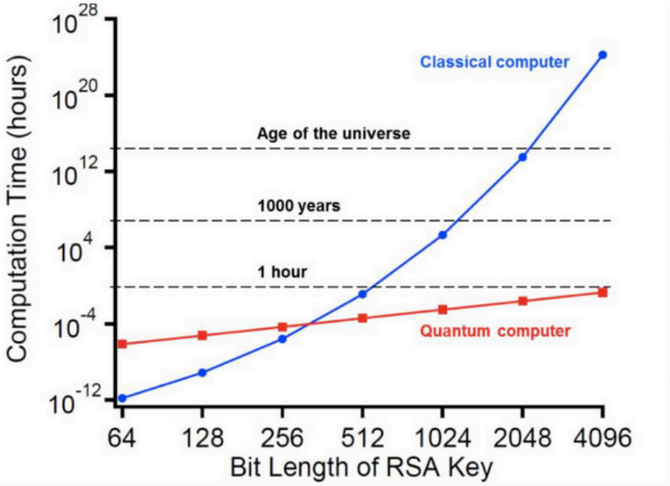
- Not at all like any of today's common computers
- Made up of quantum bits (**qubits**), which hold quantum state
- **Qubits** are extremely susceptible to environmental noise, and thus need to be kept at near-zero Kelvin during computation
- To be useful, quantum computers must be better than classical computers, but we have no idea when those quantum computers can be built
- **CRQCs*** are particularly large, and thus harder to build

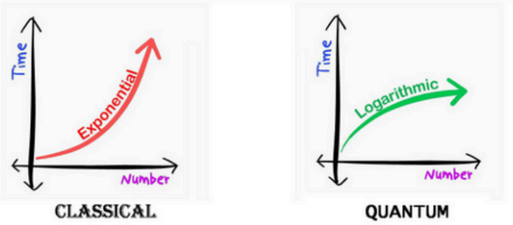


CRQC – *Cryptographically Relevant Quantum Computers*

RISKS AS QUANTUM COMPUTERS EMERGE

- Common public-key algorithms (RSA/ECDSA/DSA/ECDH) could be broken/decoded.
- Risk of forged DNSSEC signatures → domain spoofing and redirection.
- Possibility of forged certificates/ROAs → route hijacking or leaks, loss of routing control.

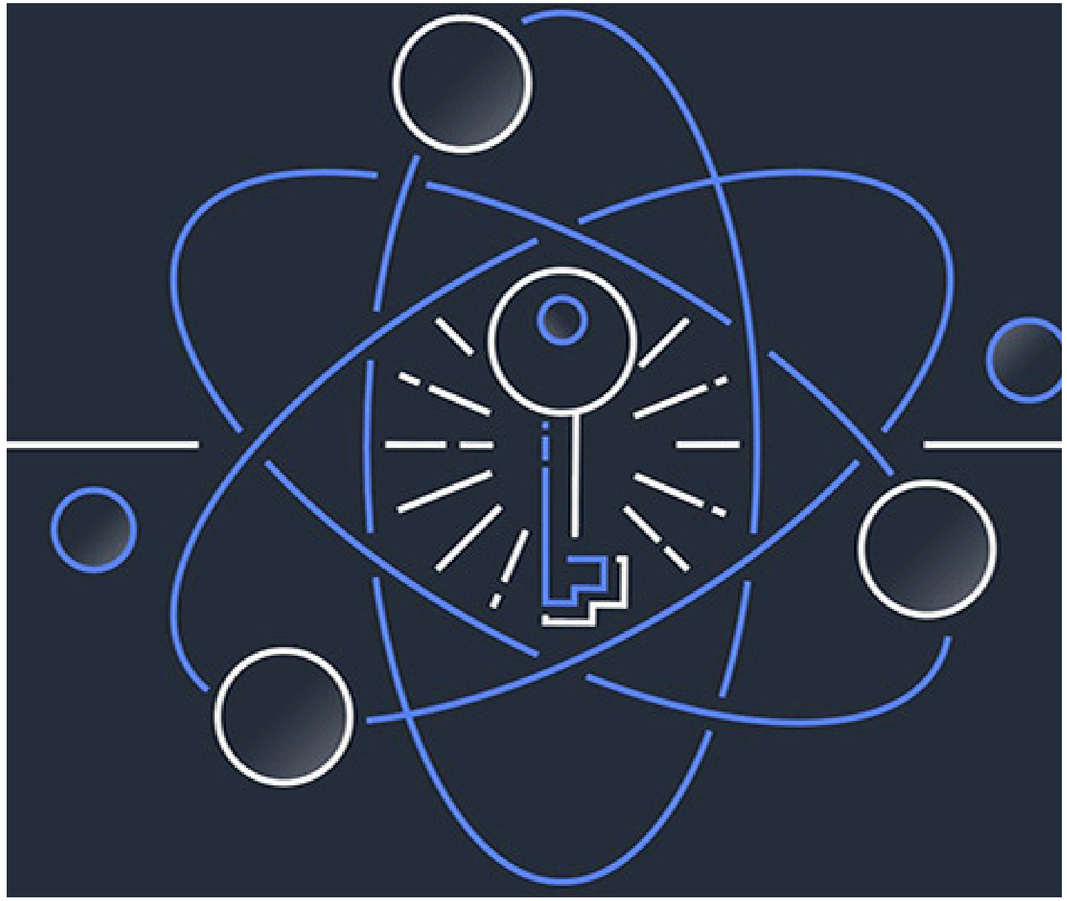




Algorithm	Key size	Security	Logical qubits	Physical qubits	Time to break
RSA	1024 bits	80 bits	2.290	~ 2.560.000 bits	3.5 hours
RSA	**2048 bits**	**112 bits**	**4.338**	**~ 6.200.000 bits**	**29 hours**
RSA	4096 bits	128 bits	8.434	~ 14.700.000 bits	10 days
ECC	256 bits	128 bits	2.330	~ 3.210.000 bits	11 hours

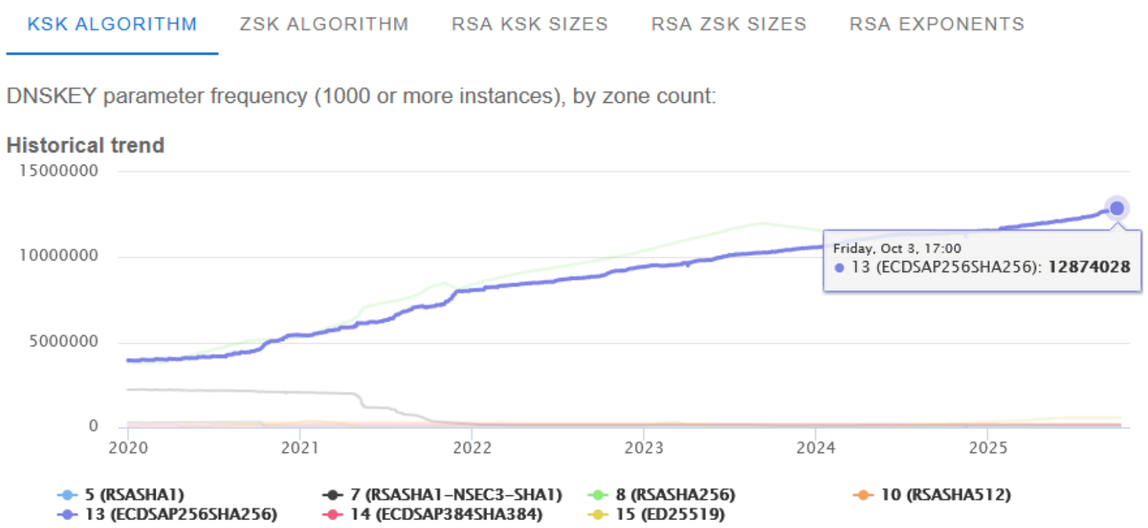
WHY POST-QUANTUM CRYPTOGRAPHY (PQC)

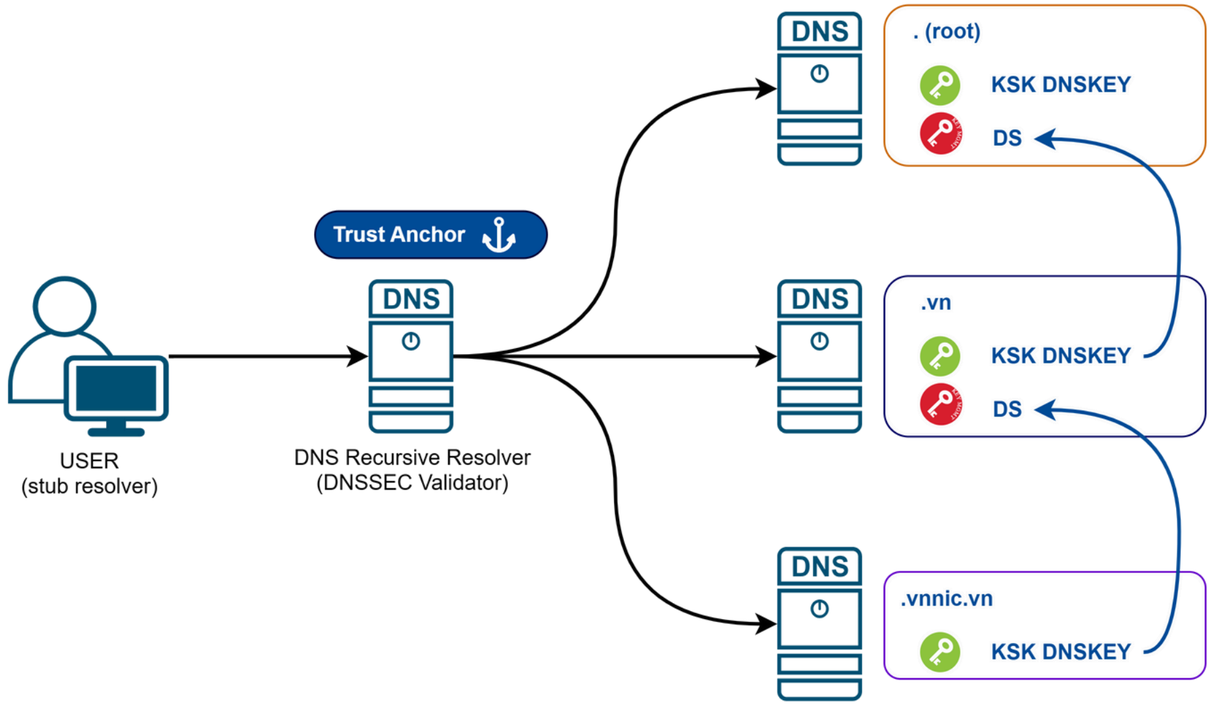
- PQC refers to new cryptographic algorithms designed to remain secure even against quantum computers.
- Unlike traditional systems (RSA, ECDSA, DH) that rely on the difficulty of factoring or discrete logarithms, PQC is based on mathematical problems believed to be hard for both classical and quantum computers (e.g., lattice, hash-based, code-based, multivariate equations).
- Quantum computers will break today's RSA and ECC security.
- Stored data can be decrypted later once quantum power grows.
- Core Internet systems (DNSSEC, RPKI, TLS) must adopt quantum-resistant algorithms early.



DNSSEC DEPLOYMENT OVERVIEW

- **Algorithm**: **RSASHA256** is widely used; there is a trend toward **ECDSAP256SHA256** (RFC 8624).

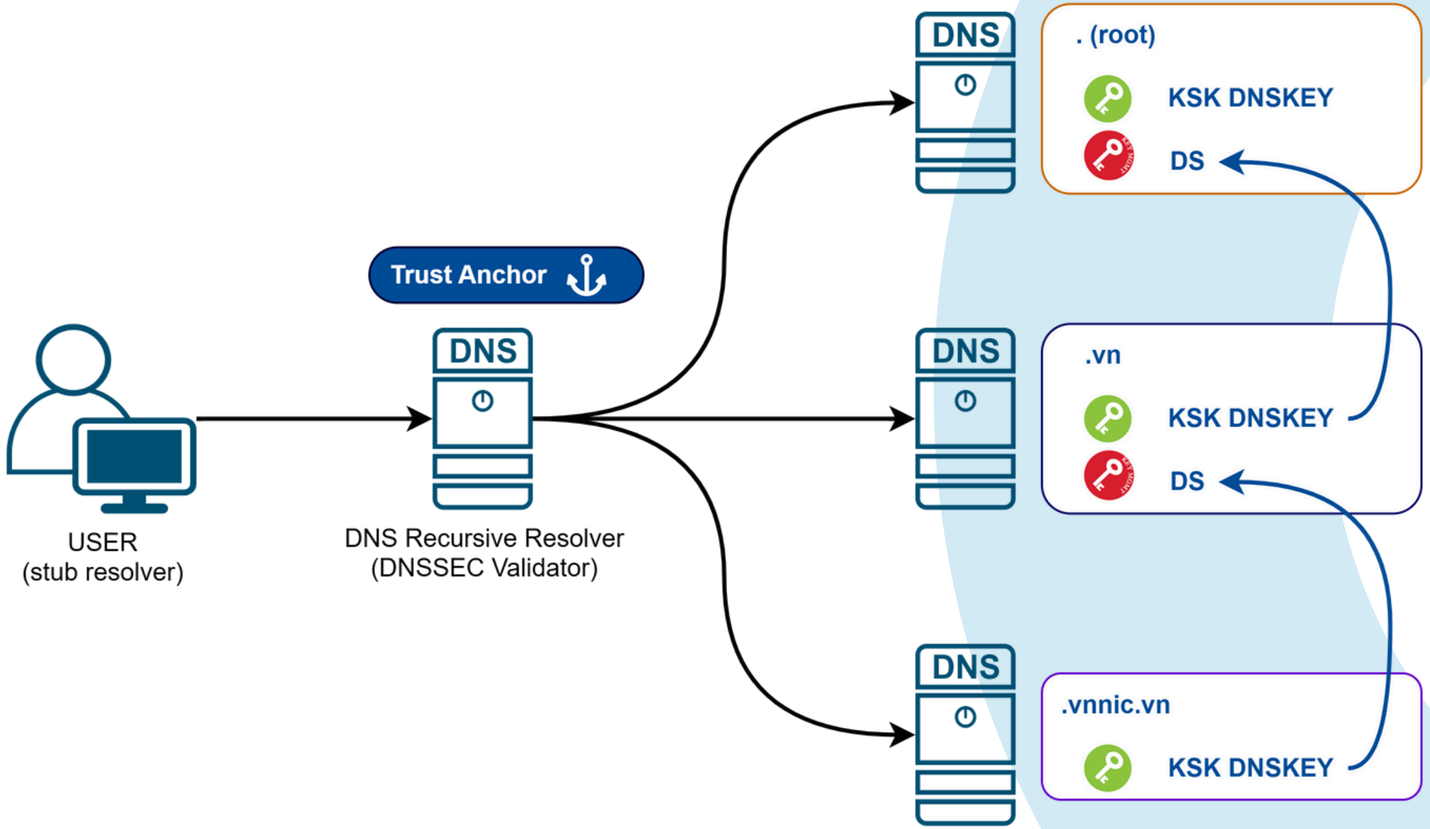




DNSSEC (VN)

- DNSSEC deployment for .VN: 2016
- Key Rollover: 2023

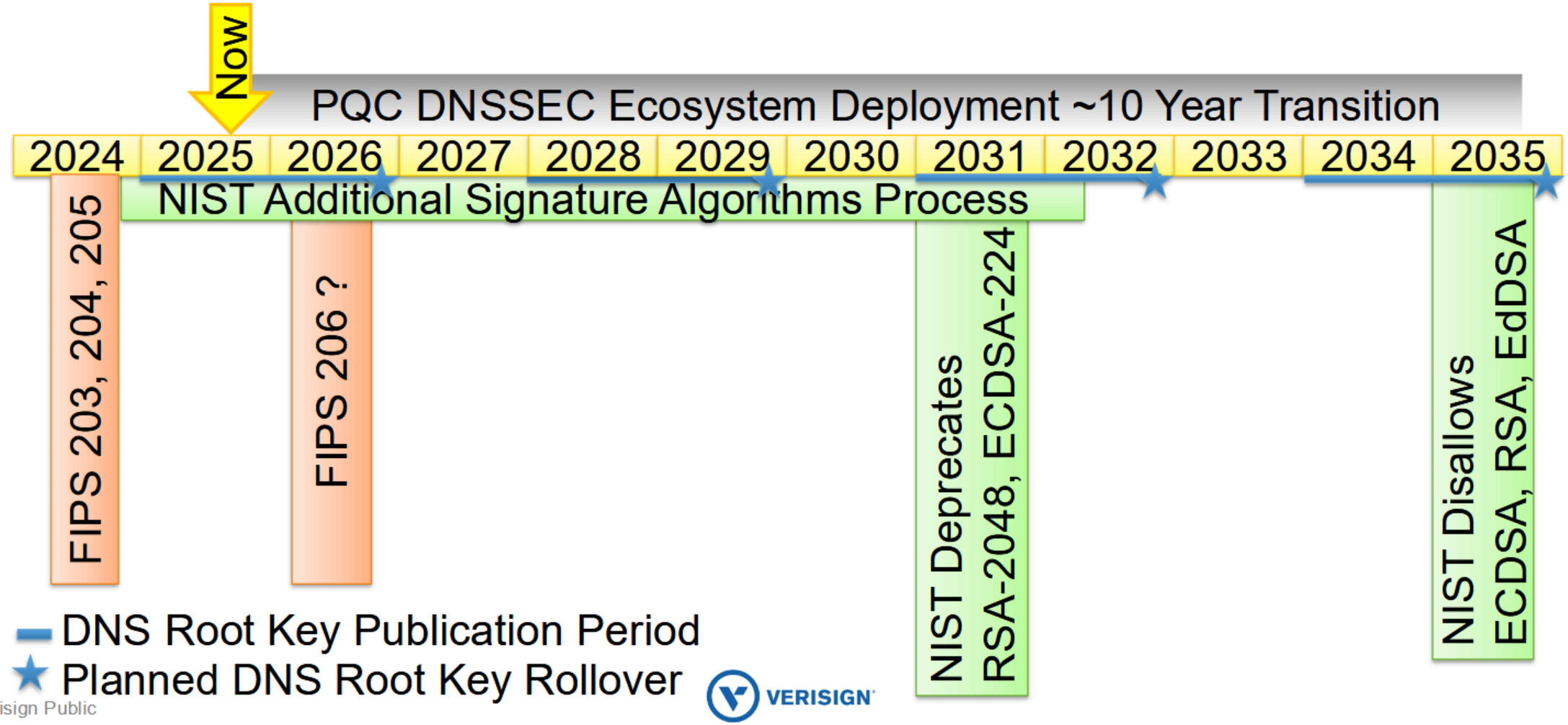
- **13,000+** domains ".vn" signed with DNSSEC (as of Sep 2025)



PQ DNSSEC CONTEXT

- DNSSEC currently relies on digital signature algorithms that could be broken by quantum computers.
- Existing PQC signature algorithms (like ML-DSA in FIPS 204 and SLH-DSA in FIPS 205) have very large signatures, making them difficult to use within DNSSEC's size limits.
- NIST's new "onramp" program aims to standardize smaller PQC signature algorithms, but these will likely depend on newer and less-tested cryptographic assumptions.

TIMELINE CONSIDERATIONS



PQC FOR DNSSEC

- Root Zone Signing and Validation

SIGNING (ROOT, 1 KSK, 1 ZSK, RAW)

ALGORITHM	MEAN	σ	SIGNATURE S/S	RAW SIZE
FALCON-512	4881.9 ms	26.8 ms	589	2891700
HAWK-256	195.5 ms	4.9 ms	62001	1727793
HAWK-512	261.0 ms	9.6 ms	49821	2582375
SQIsign	*54528.1 ms*	67.9 ms	51	1445334
MAYO	1086.6 ms	48.7 ms	2746	2301478
ANTRAG-512+	5339.6 ms	111.2 ms	546	2685056
RSA 2048	845.7 ms	3.0 ms	3980	1746936
ECDSAP256	218.1 ms	10.2 ms	44286	1211056
ED25519	240.6 ms	6.3 ms	47288	1210992
MTL	1501.6 ms	15.4 ms	5314	1604362

VALIDATION (ROOT, 1 KSK, 1 ZSK, RAW)

ALGORITHM	MEAN	σ
FALCON-512	403.7 ms	1.1 ms
HAWK-256	232.5 ms	1.4 ms
HAWK-512	359.4 ms	66.0 ms
SQIsign	22338.5 ms	35.0 ms
MAYO	995.8 ms	26.8 ms
ANTRAG-512	548.6 ms	1.4 ms
RSA 2048	250.2 ms	18.9 ms
ECDSAP256	610.0 ms	4.5 ms
ED25519	819.4 ms	4.5 ms

PQC FOR DNSSEC

- DNS Message Sizes

ALGORITHM	SOA	DNSKEY	NXDOMAIN	NODATA	Delegation
FALCON-512	797	3244	1520	1518	1023
HAWK-256	380	1237	686	684	606
HAWK-512	686	2691	1298	1296	912
SQIsign	279	366	484	482	505
MAYO	1108	3382	1096	1094	811
ANTRAG-512	723	2216	1372	1370	949
RSA 2048	387	864	700	698	613
ECDSAP256	195	280	316	314	421
ED25519	195	216	316	314	421

Doesn't fit into 1232 bytes

Doesn't fit into 1452 bytes

PQC FOR DNSSEC

- Large Public Keys are OK(ish)
- Large Signature affects performance

- FALCON-512 – slow due to signature size, DNS switches to TCP
- HAWK-256 – promising, but cryptographically weaker algorithm
- HAWK-512 – usable algorithm
- SQIsign – small keys, small signatures, very slow due to computational complexity
- MAYO – larger public key, but usable thanks to small signatures
- ANTRAG-512 – usable algorithm (outside NIST)

KEY CHALLENGES

Large Signature Size:

- PQC signatures (Dilithium, Falcon, SPHINCS+) are much larger → risk of exceeding DNS UDP limits (~1232 B).

Performance Overhead:

- Higher CPU/HSM cost for signing and validation; impacts large zones (TLDs, root).

Key Management Complexity:

- Bigger DNSKEY/DS records; complex rollovers and multi-signer coordination.

Software & Protocol Support:

- PQC DNSSEC drafts still evolving; resolvers/ authoritatives not yet fully compatible.

Operational Synchronization:

- Requires all DNS layers (root → TLD → child zones) to migrate consistently.

Algorithm Maturity:

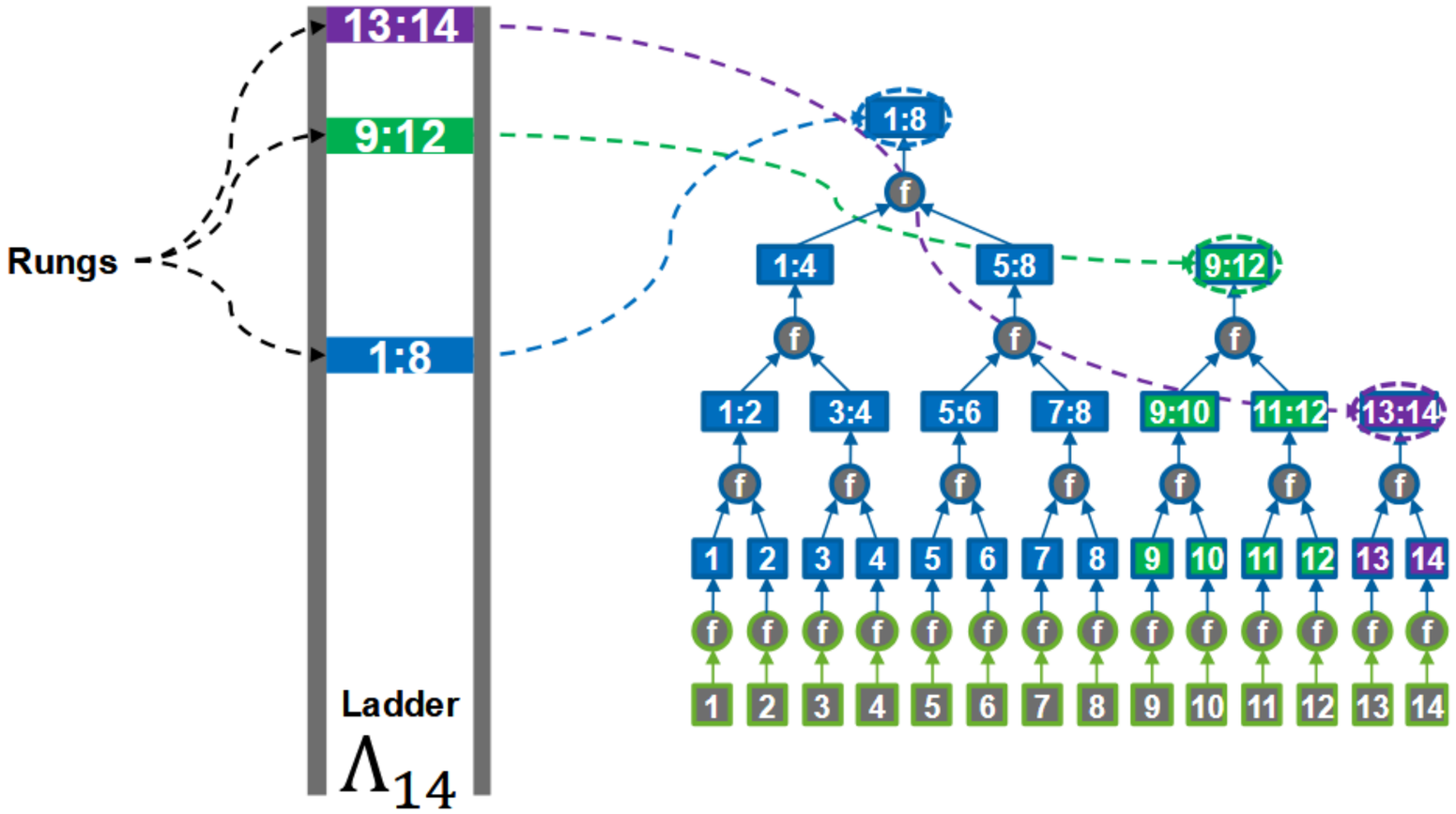
- New PQC algorithms lack long-term field validation; potential performance and security trade-offs.

PQC ADOPTION & TEST STRATEGY

- **Algorithms**
  - ML-DSA (Dilithium)
  - SLH-DSA (SPHINCS+)
  - FN-DSA (Falcon)
- **Modes of operation**
  - MTL Mode (Merkle
- **Hybrid signatures**
  - PQC + RSA/ECDSA
- **Software & testbed**
  - SIDN Labs “PATAD” testbed
  - Open-source MTL of Verisign

PQC FOR DNSSEC: MODES OF OPERATION

- MTL mode is a method for reducing a signature scheme's operational impact on an expanding message series.



- Rather than signing individual messages, MTL mode signs Merkle Tree Ladders
- Messages are authenticated with Merkle proofs relative to ladders
- Ladders provide backward compatibility since they can verify Merkle proofs constructed relative to future ladders too
- Useful for signature series that sign multiple things at one time. (DNSSEC, OCSP, etc.)

IMPACT OF MTL MODE SIGNATURES ON DNSSEC

- **Signature and Key Sizes**

Table I

Size of the algorithms' public key and signature in bytes.

Algorithm	Public Key	Signature Size
ECDSAP256SHA256	64	64
SLH-DSA-MTL-SHA2-128s	32	40–500†
SLH-DSA-MTL-SHAKE-128s	32	40–500†
SLH-DSA-SHA2-128s	32	7856
SLH-DSA-SHAKE-128s	32	7856

† **Condensed** signature for a zone with 1 000 000 000 RRsets: max 504B

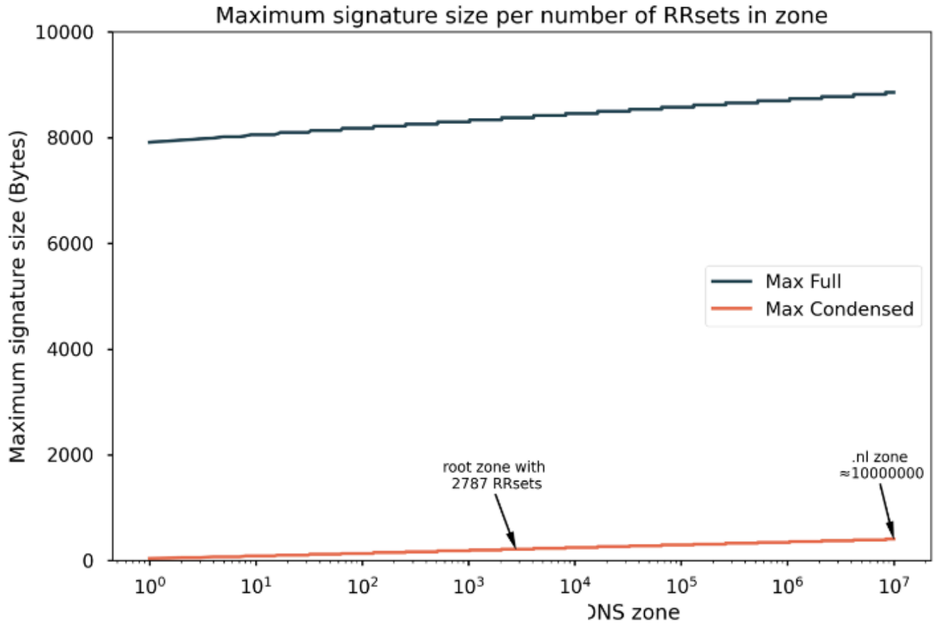


Table II

DNS Message Size (root zone with 1 KSK and 1 ZSK)

Algorithm	SOA	DNSKEY	NXDOMAIN	NODATA	Delegation
ECDSAP256SHA256	197	280	319	316	333
SLH-DSA-MTL-SHA2-128s	8366	8089	8641	8638	486
SLH-DSA-MTL-SHAKE-128s	8366	8089	8641	8638	486
SLH-DSA-SHA2-128s†	7989	8072	15903	15900	8125
SLH-DSA-SHAKE-128s†	7989	8072	15903	15900	8125

† Estimated message sizes, calculated by hand.

IMPACT OF MTL MODE SIGNATURES ON DNSSEC

- **Signing & Verification Performance**

Table III
Signing time in milliseconds.

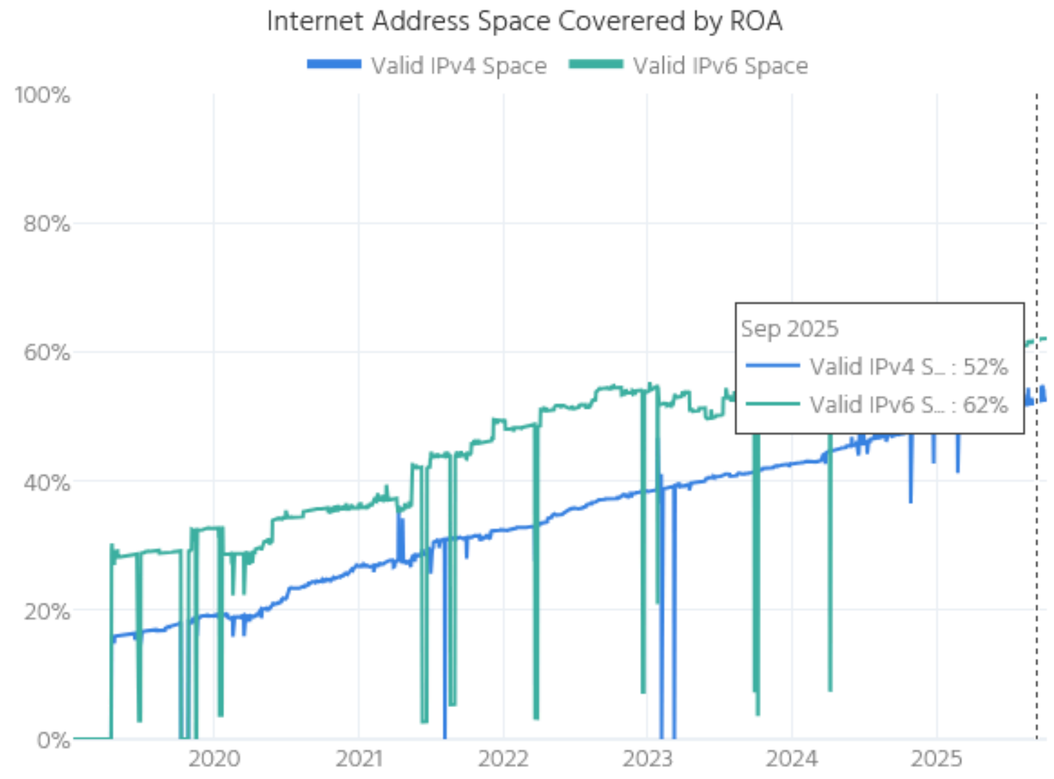
Algorithm	Mean	σ
ECDSAP256SHA256	358.17	8.64
SLH-DSA-MTL-SHA2-128s	598.52	10.03
SLH-DSA-MTL-SHAKE-128s	902.96	5.79
SLH-DSA-SHA2-128s	398793.40	776.08
SLH-DSA-SHAKE-128s	807239.86	762.97

Table IV
Verification time in milliseconds.

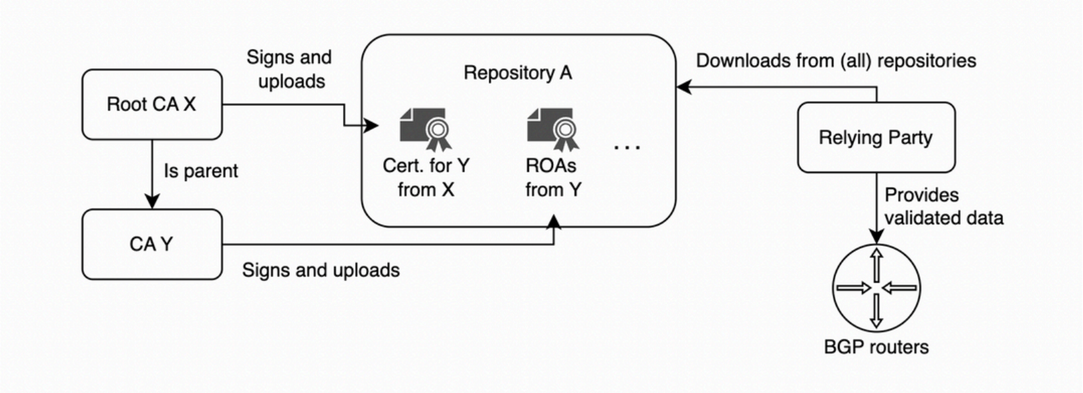
Algorithm	Mean	σ
ECDSAP256SHA256	550.19	4.52
SLH-DSA-MTL-SHA2-128s	598.06	8.40
SLH-DSA-MTL-SHAKE-128s	600.89	7.63
SLH-DSA-SHA2-128s	2968.52	54.94
SLH-DSA-SHAKE-128s	3476.51	22.02

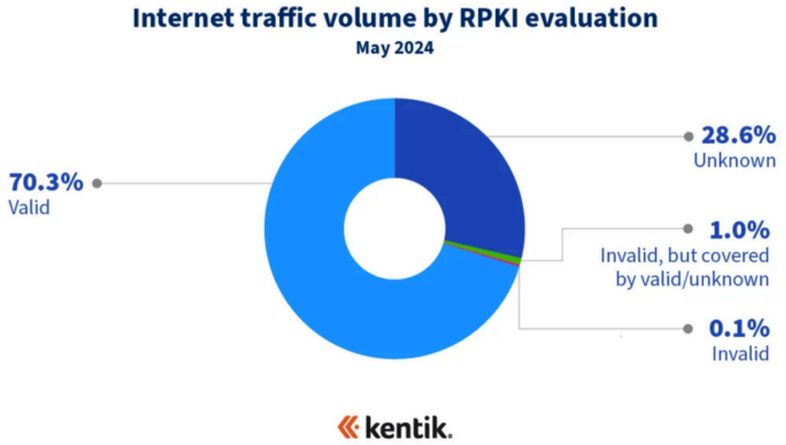
RPKI DEPLOYMENT OVERVIEW

- Most of active RPKI certificates and ROAs globally are signed with 2048-bit RSA keys (with SHA-256 hashes).



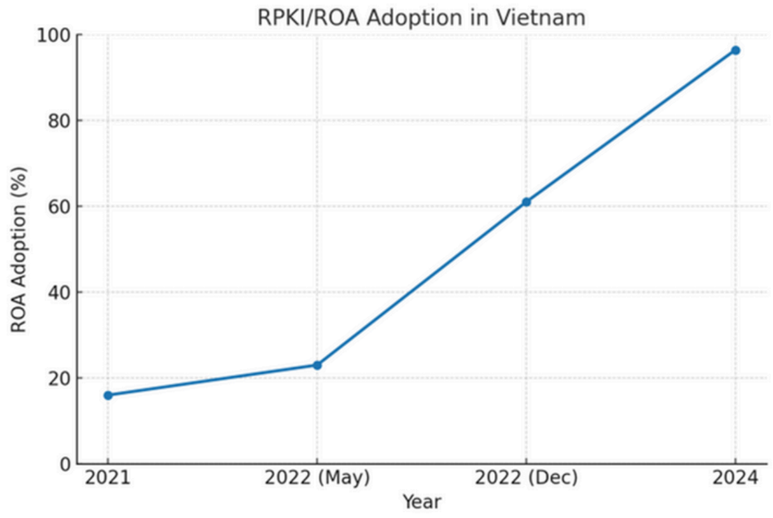
Percentage of address space covered by ROA (data source: APNIC)



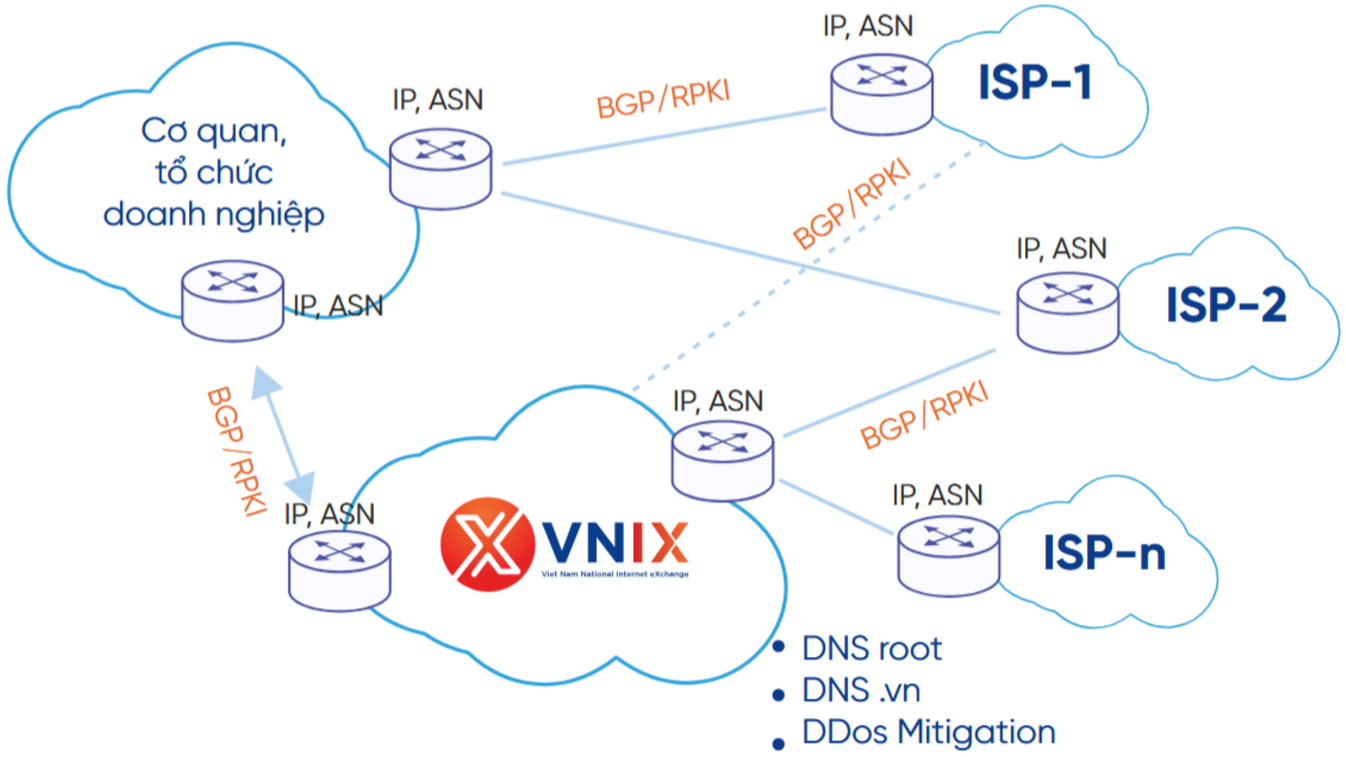


RPKI (VN)

- ROA/RPKI in Vietnam (2021–2024)



- 2021: RPKI coverage was ~16%, with FPT pioneering ROV trials;
- 2025: reached 98% IPv4 and 72% IPv6 signed.
- Challenges with ROV: Adoption remains low due to operational hesitation, routing policy complexity, and lack of strong industry consensus.



PQC FOR RPKI

- **Falcon-512** currently offers the best overall performance among PQC signature schemes and has been selected by NIST for standardization (first public draft expected in late 2024).
- Other candidates (except ML-DSA) may be eliminated, meaning Falcon-512 will become widely available sooner in standards, software, and hardware (HSMs).

Scheme	Parameters	NIST level	Pk. Size (B)	Sig. Size (B)	RPKI size	Est. download time (s)	Est. verification CPU time (s)
RSA	2,048	⚠	272	256	838MB	14.5	13
EdDSA	Ed25519	⚠	32	64	592MB	10.2	37.6
ML-DSA	44	2	1,312	2,420	3.0GB	51.1	34.2
Falcon	512	1	897	666	1.4GB	24.4	23.4
SLH-DSA	SHAKE-128s	1	32	7,856	6.7GB	116.6	1,376.30
	SHAKE-128f	1	32	17,088	14.0GB	242.6	3,729.50
SQIsign	I	1	65	148	671MB	11.6	1,473.30
MAYO	1	1	1,420	454	1.4GB	25	44.3
	2	1	4,912	186	2.6GB	45.1	16.3
HAWK	512	1	1,024	555	1.4GB	23.7	42.8
FAEST	128s	1	32	4,506	4.1GB	70.9	2,826.20
	128f	1	32	5,924	5.2GB	90.2	408.2
SNOVA	(24, 5, 4)	1	1,016	248	1.1GB	19.5	47.3
	(25, 8, 3)	1	2,320	165	1.6GB	27.2	63.2

PQC FOR RPKI (HYBRID)

- A traditional algorithm to be combined with a post-quantum signature in a hybrid model
  - RSA-2048
  - RSA-3072
  - Ed25519).

Scheme	Pk. Size (B)	Sig. Size (B)	RPKI size	Est. download time (s)	Est. verification CPU time (s)
Falcon-512	897	666	1.4GB	24.4	23.4
Falcon-512 + RSA-2048	1,169	922	1.7GB	29.7	36.4
Falcon-512 + RSA-3072	1,297	1,050	1.9GB	32.3	52
Falcon-512 + Ed25519	929	730	1.5GB	25.4	61

Table 2 — Estimated downloading and verification times for hybrid schemes.

PQC FOR RPKI: NULL SCHEME

- The signature is always the empty string.
- The public key is a hash of the message to be signed.
- Verification is done by comparing the public key to the hash of the message.

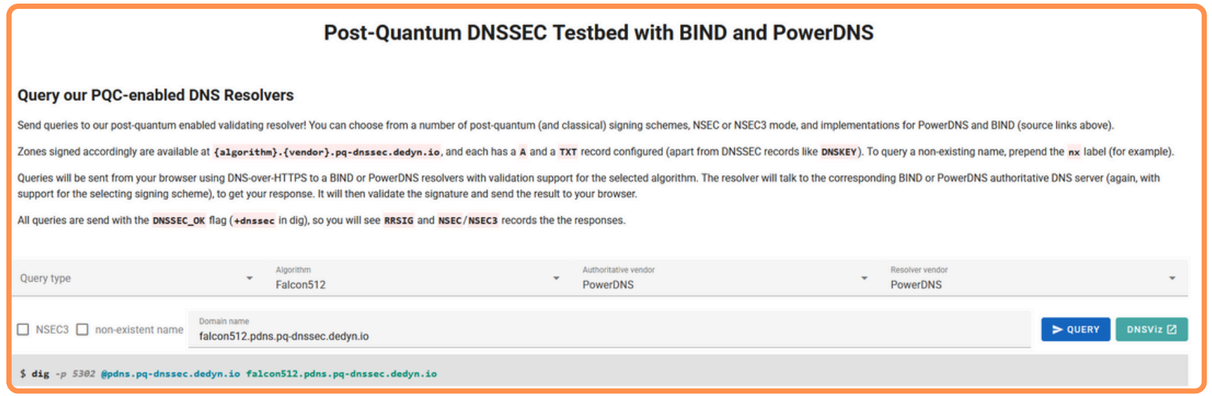
- The **Null Scheme** has some big advantages:
  - **Size:** When using RSA signatures and SHA-256 (the current situation), that saves 496 bytes per object. For the median-size ROA, that is a reduction from 2125 bytes to 1629 bytes, and on the whole 838 MB RPKI, that can save 172 MB of overhead.
  - **Verification time:** That saves 35% of the verification time in the whole RPKI.

STANDARDIZATION AND SUPPORT OVERVIEW

Document	Scope / Description	Status
FIPS 203	ML-KEM (Kyber) – Post-quantum key encapsulation mechanism	Final (Aug 2024) - NIST
FIPS 204	ML-DSA (Dilithium) – Post-quantum digital signature	Final (Aug 2024) - NIST
FIPS 205	SLH-DSA (SPHINCS+) – Hash-based PQ signature	Final (Aug 2024) - NIST
FIPS 206	FN-DSA (Falcon) – Post-quantum digital signature	Draft (expected 2025) - NIST
RFC 9794	Terminology for Post-Quantum / Hybrid Schemes	Published (2025)
I-Draft: PQC Migration	Guidelines for migrating Internet protocols to PQC	In progress
I-Draft: PQC Guidance	Overview of PQC algorithms and parameter sets	In progress
I-Draft: PQC for Engineers	Practical guidance for implementing PQC systems	In progress

STANDARDIZATION AND SUPPORT OVERVIEW

- **IETF:** Active work on PQC and crypto agility across multiple groups — PQUIP (transition guidance), DNSOP (e.g., SLH-DSA-MTL for DNSSEC), LAMPS/UTA (PQC X.509 and TLS usage), and SIDROPS (RPKI validation/algorithm agility).
- **NIST:** PQC standards published (FIPS 203 ML-KEM/Kyber, FIPS 204 ML-DSA/Dilithium, FIPS 205 SLH-DSA/SPHINCS+); FALCON draft planned as FIPS 206; HQC selected as an additional KEM (draft in 2026). These choices strongly influence global algorithm selection.
- **ICANN / Verisign / TLD Operators:** Planning and studies for root/TLD algorithm rollovers and PQC impact; community prototypes include MTL mode code and measurements from IETF hackathons and reports (e.g., IETF 122/123).
- **APNIC / Regional Operators (e.g., SIDN Labs, JPNIC):** Public PQC DNSSEC testbeds and experiments (PATAD testbed; field and lab evaluations of Falcon/MAYO/SLH-DSA/MTL; hands-on training).



Post-quantum Algorithms Testing and Analysis for the DNS

IMPACT & RECOMMENDATIONS

Regulators

- Develop policies recommending PQC-ready solutions for critical infrastructure.
- Deploy DNSSEC/RPKI PQC testbeds and pilots.

ISP/Enterprise

- Identify services that depend on DNSSEC / RPKI.
- Deploy validators/adapters that support hybrid signatures.
- Test in staging environments; monitor fragmentation, latency, and resolver errors.

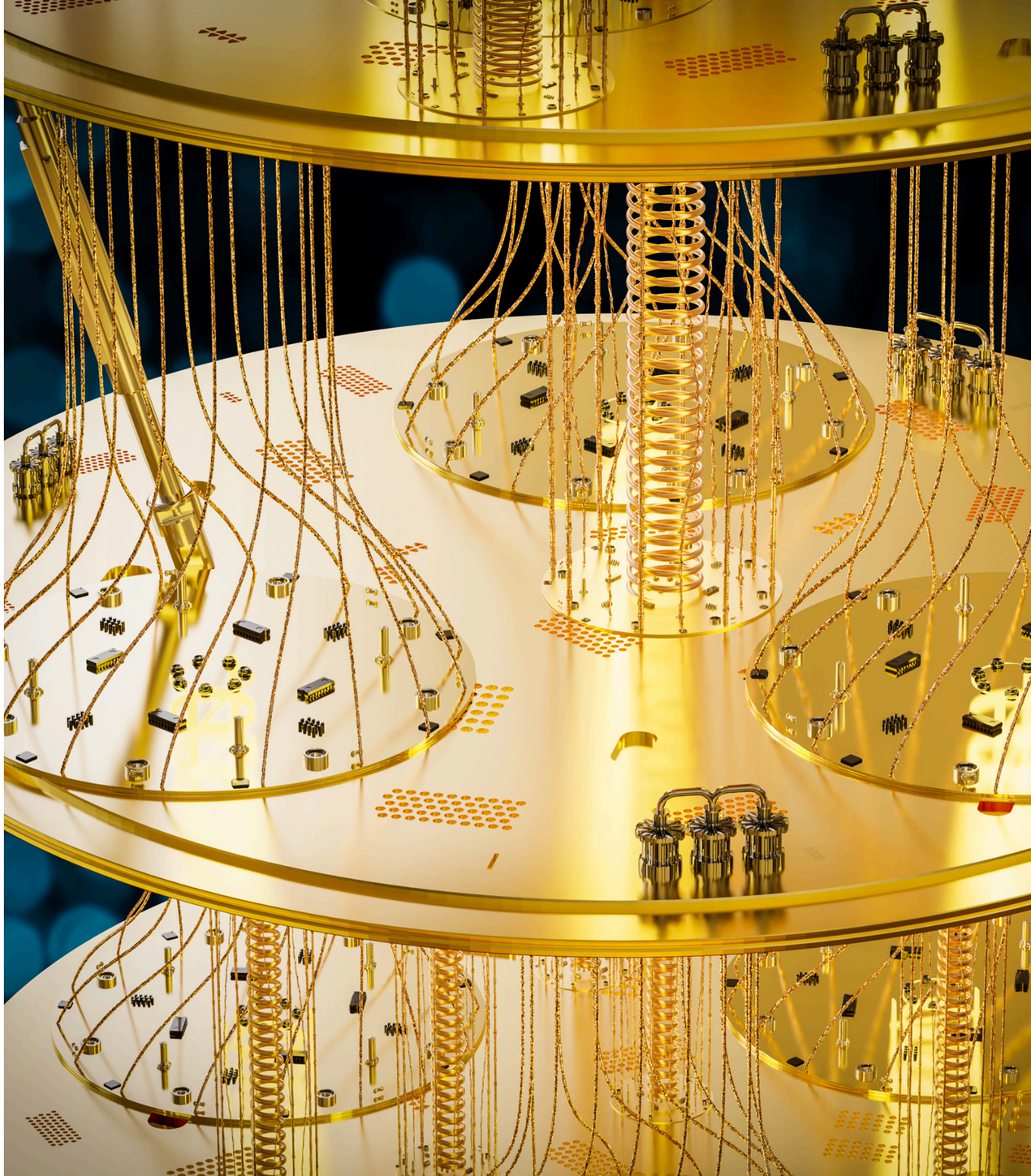
Users & Community

- Raise awareness of “harvest now, decrypt later”; encourage using DANE/TLSA where applicable.
- Urge domain hosting providers to offer PQC-ready DNSSEC options

VN NIC
Internet for all

CONCLUSION

- **PQC** adoption is inevitable — prepare early for the quantum era.
- **DNSSEC:** use MTL mode and packet optimization; choose algorithms balancing size and speed.
- **RPKI:** Falcon-512 is practical; mixed-tree and Null-Signature reduce overhead and add flexibility.
- Keep pace with **NIST/IETF** standards, test implementations, and always have a rollback plan.



THANK YOU !