Post-Quantum

Cryptography Conference

Post-quantum crypto integration for enterprise applications

Anselme Tueno
Cryptography Researcher at SAP

ENTRUST HID PKI Consortium

Post-Quantum Crypto Integration For Enterprise Applications

Anselme Tueno, SAP

November 7, 2023

Public

THE BEST RUN SAP

Agenda

Standardization and Regulations

Implementation

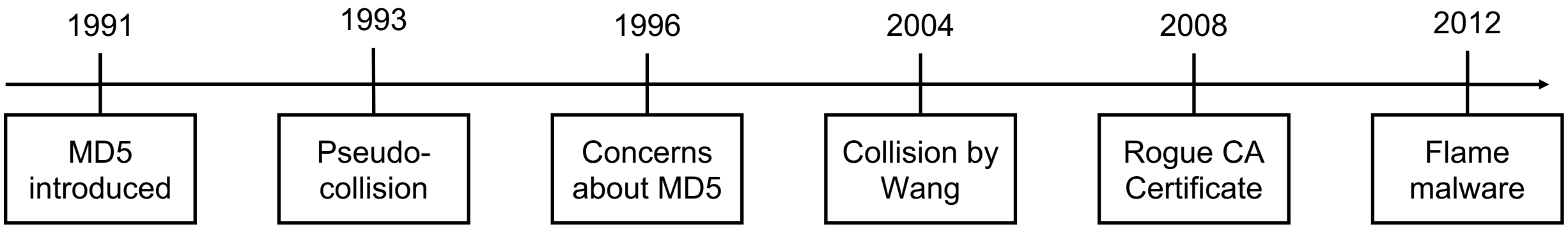
Internet Protocols

Integration and Migration

„Cryptography Is Harder Than It Looks“ ~ (Bruce Schneier)

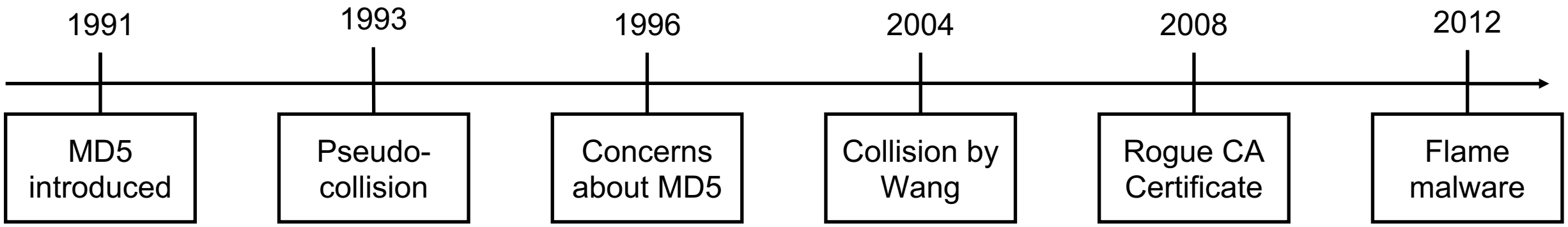
Schneier on Security: https://www.schneier.com/

„Cryptography Is Harder Than It Looks“ ~ (Bruce Schneier)



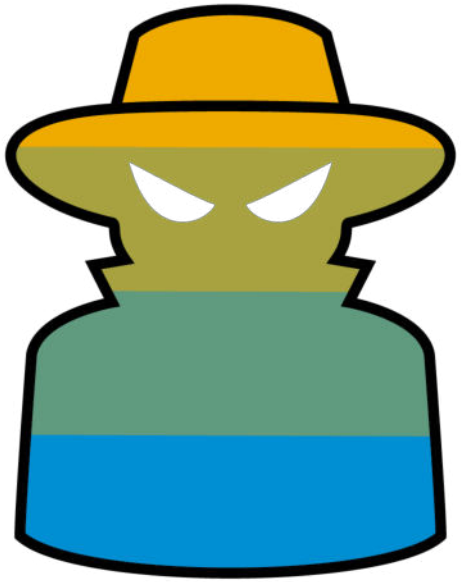
Schneier on Security: https://www.schneier.com/

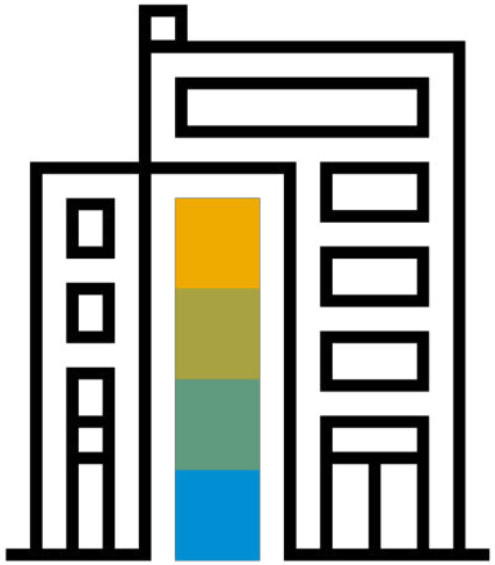
„Cryptography Is Harder Than It Looks“ ~ (Bruce Schneier)



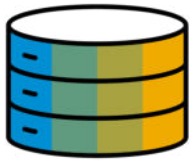
Schneier on Security: https://www.schneier.com/

Quantum Threat



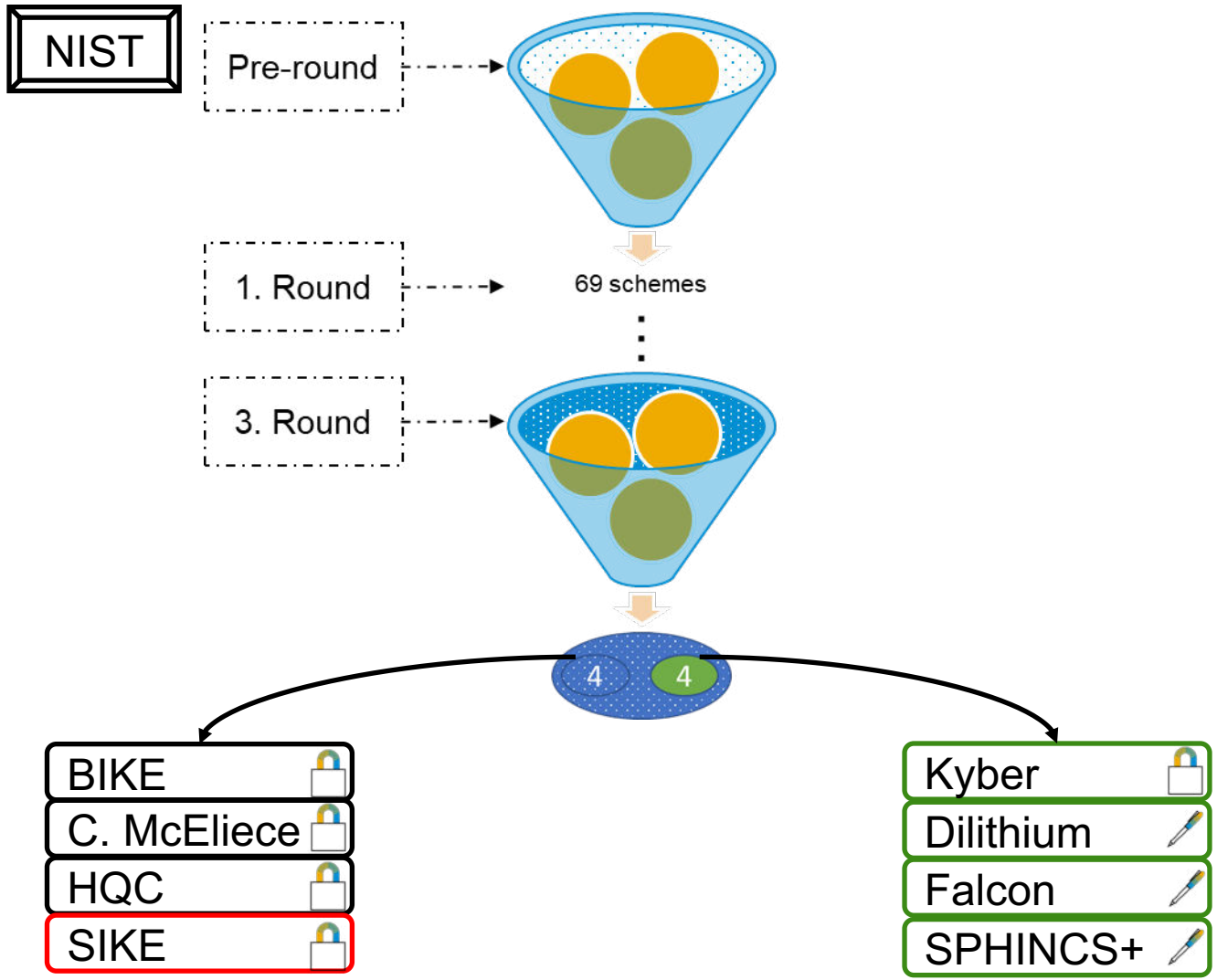


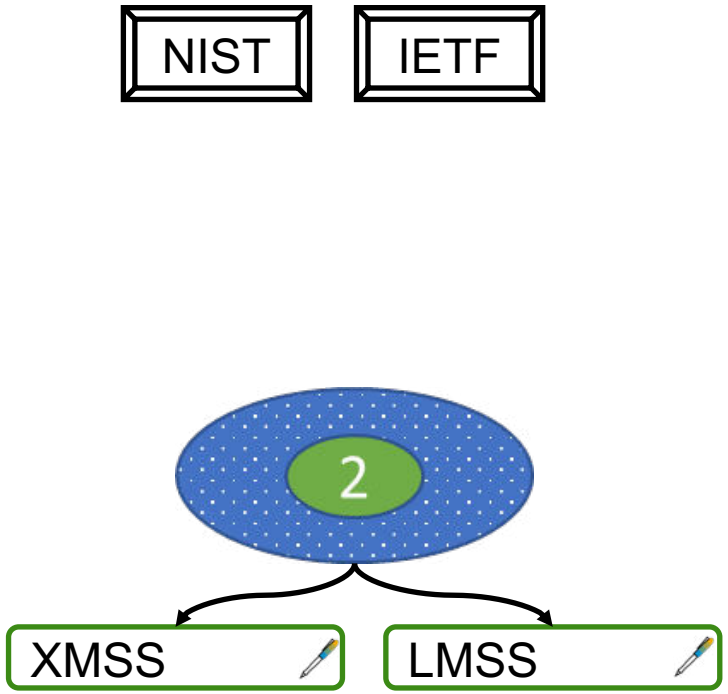
VPN



Standardization and Regulations

PQC Standardization



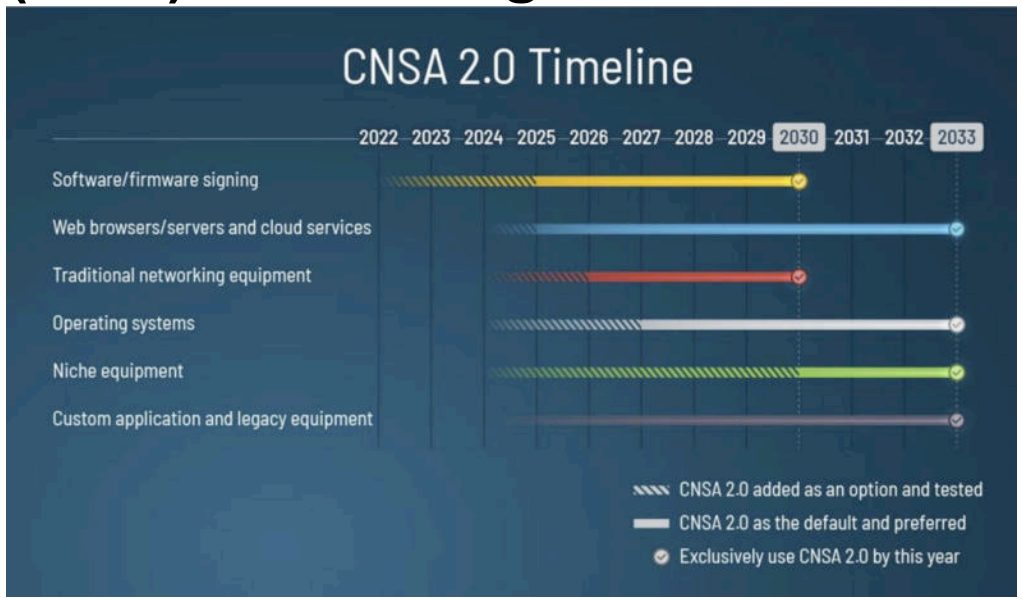


NIST Call for Additional Digital Signature

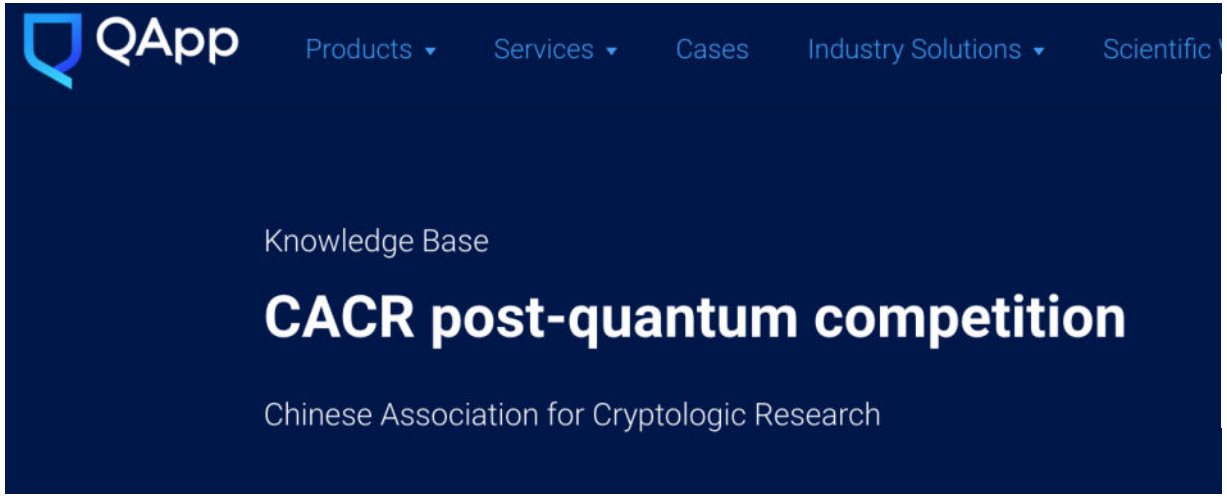
3WISE ⚠	On-ramp	Multivariate	cubic degree
ALTEQ ⚠	On-ramp	Other	alternating trilinear form equivalence problem
Biscuit ⚠	On-ramp	Multivariate	multivariate: solving generic sctructured algebraic equations
CROSS	On-ramp	MPC-in-the-Head	Restricted syndrome decoding
DME-Sign ⚠	On-ramp	Multivariate	deterministic trapdoor permutation
EagleSign ⚠	On-ramp	Lattices	MNTRU/MLWE
EHTv3 / EHTv4 ⚠	On-ramp	Lattices	Lattices?
eMLE-Sig 2.0 ⚠	On-ramp	Other	Embedded Multilayer Equations
Enhanced pqsigRM	On-ramp	Code-based	Reed Muller codes
FuLeeca ⚠	On-ramp	Code-based	Code-based Lee Metric
HAETAE	On-ramp	Lattices	MLWE/MSIS
HAWK	On-ramp	Lattices	Lattice Isomorphism Problem
HPPC ⚠	On-ramp	Multivariate	HFE
HuFu ⚠	On-ramp	Lattices	LWE/SIS
KAZ-Sign ⚠	On-ramp	Other	Second-order Discrete Logarithm Problem
LESS ⚠	On-ramp	Code-based	Linear Equivalence Problem
MAYO	On-ramp	Multivariate	Multivariate quadratic
MEDS ⚠	On-ramp	Code-based	Matrix Code Equivalence
MIRA	On-ramp	MPC-in-the-Head	MinRank
MiRitH	On-ramp	MPC-in-the-Head	MinRank
MQOM	On-ramp	MPC-in-the-Head	Multivariate Quadratic
PERK	On-ramp	MPC-in-the-Head	Permuted Kernel
PREON	On-ramp	Other	zk-SNARK
PROV	On-ramp	Multivariate	Multivariate
QR-UOV	On-ramp	Multivariate	Multivariate
Raccoon	On-ramp	Lattices	MLWE/MSIS
RYDE	On-ramp	MPC-in-the-Head	Rank Syndrome Decoding
SDitH ⚠	On-ramp	MPC-in-the-Head	Syndrome Decoding
SNOVA	On-ramp	Multivariate	Non-commutative ring UOV
SQIsign	On-ramp	Isogenies	Isogenies
Squirrels	On-ramp	Lattices	SIS
TUOV	On-ramp	Multivariate	UOV
UOV	On-ramp	Multivariate	Multivariate
VOX	On-ramp	Multivariate	Multivariate
Wave	On-ramp	Code-based	Coding theory
Xifrat1-Sign.I ⚠	On-ramp	Other	randomized abelian quasigroups

https://pqshield.github.io/nist-sigs-zoo/

(Inter)National Agencies



Bundesamt
für Sicherheit in der
Informationstechnik



Articles / Analysis

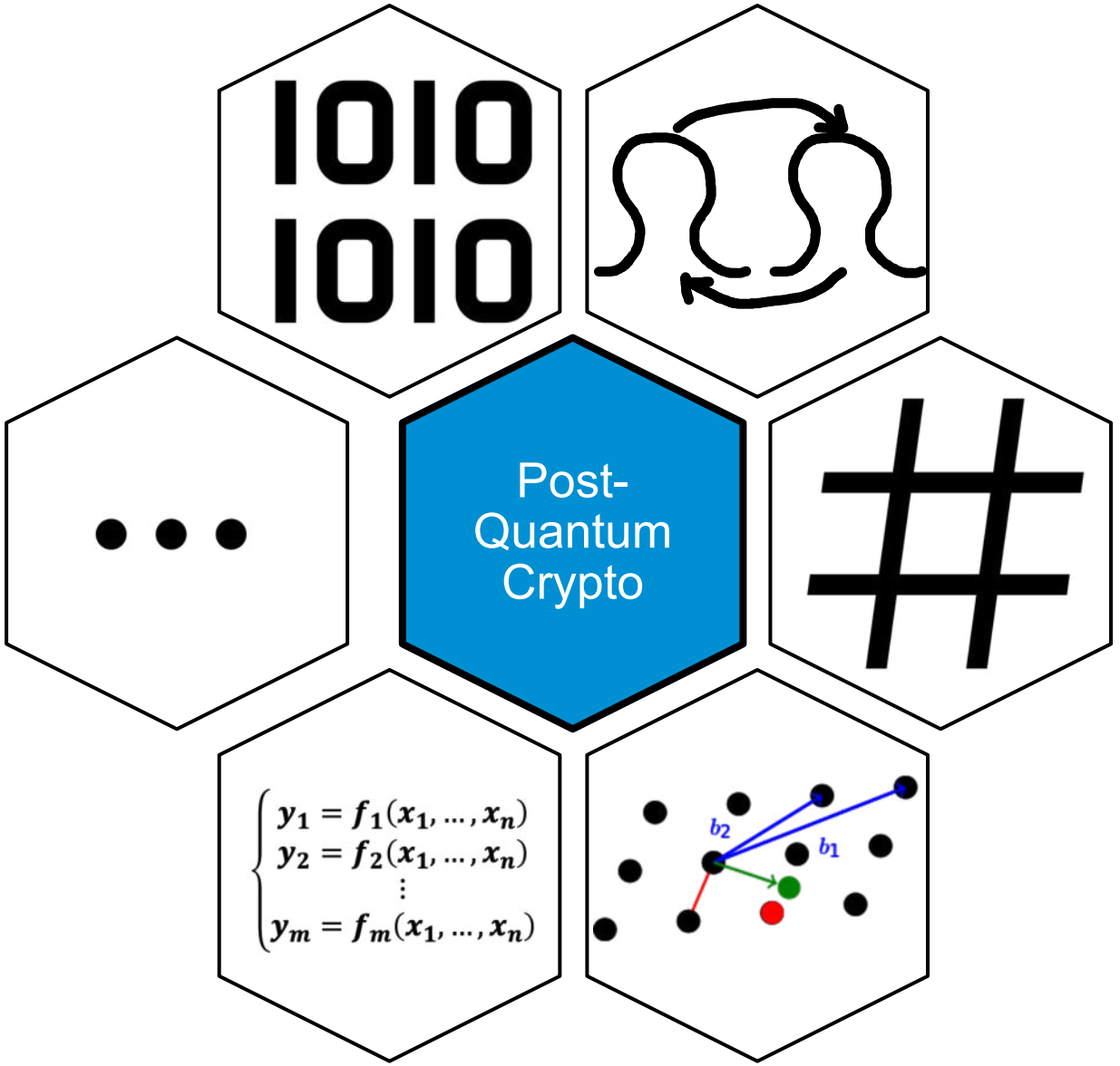
China, Russia to Adopt 'Slightly Different' PQC Standards From US

Nancy Liu | Editor
October 19, 2022 6:00 PM

Share this article:

Implementation

PQC Families



Parameters

RSA

- Key length e.g.: 2048, 3072

DSA

- Key length e.g.: 2048, 3072
- Hash function e.g.: SHA-1, SHA-2

Parameters

RSA

- Key length e.g.: 2048, 3072

DSA

- Key length e.g.: 2048, 3072
- Hash function e.g.: SHA-1, SHA-2

Table 1. ML-DSA Parameter sets

Parameters (see sections 5 and 6 of this document)	Values assigned by each parameter set ML-DSA-44	ML-DSA-65	ML-DSA-87
q - modulus [see §5]	8380417	8380417	8380417
d - # of dropped bits from $\mathbf{t}$ [see §5]	13	13	13
τ - # of ± 1's in polynomial c [see §6]	39	49	60
λ - collision strength of $\tilde{c}$ [see §6]	128	192	256
γ_1 - coefficient range of $\mathbf{y}$ [see §6]	2^{17}	2^{19}	2^{19}
γ_2 - low-order rounding range [see §6]	$(q-1)/88$	$(q-1)/32$	$(q-1)/32$
(k, ℓ) - dimensions of $\mathbf{A}$ [see §5]	(4,4)	(6,5)	(8,7)
η - private key range [see §5]	2	4	2
$\beta = \tau \cdot \eta$ [see §6]	78	196	120
ω - max # of 1's in the hint $\mathbf{h}$ [see §6]	80	55	75
Challenge entropy $\log \binom{256}{\tau} + \tau$ [see §6]	192	225	257
Repetitions (see explanation below)	4.25	5.1	3.85
Claimed security strength	Category 2	Category 3	Category 5

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.ipd.pdf

Complexity

RSA

- Choose prime P and Q
- Compute $N = PQ,\ \varphi(N) = (P-1)(Q-1)$
- Choose public key e: $2 < e < \varphi(N)$
- Compute secret key d: $d = e^{-1} \, mod \, \varphi(N)$

DSA

- Choose Prime P and Q: Q divides $P-1$
- Choose h: $2 < h < P-2$
- Choose secret key x: $1 < x < Q-1$
- Compute $g = h^{(P-1)/Q}$
- Compute public key $y = g^x \, mod \, P$

Complexity

RSA

- Choose prime P and Q
- Compute $N = PQ,\ \varphi(N) = (P-1)(Q-1)$
- Choose public key e: $2 < e < \varphi(N)$
- Compute secret key d: $d = e^{-1} \bmod \varphi(N)$

DSA

- Choose Prime P and Q: Q divides $P-1$
- Choose h: $2 < h < P-2$
- Choose secret key x: $1 < x < Q-1$
- Compute $g = h^{(P-1)/Q}$
- Compute public key $y = g^x \bmod P$

Algorithm 1 ML-DSA.KeyGen()

Generates a public-private key pair.

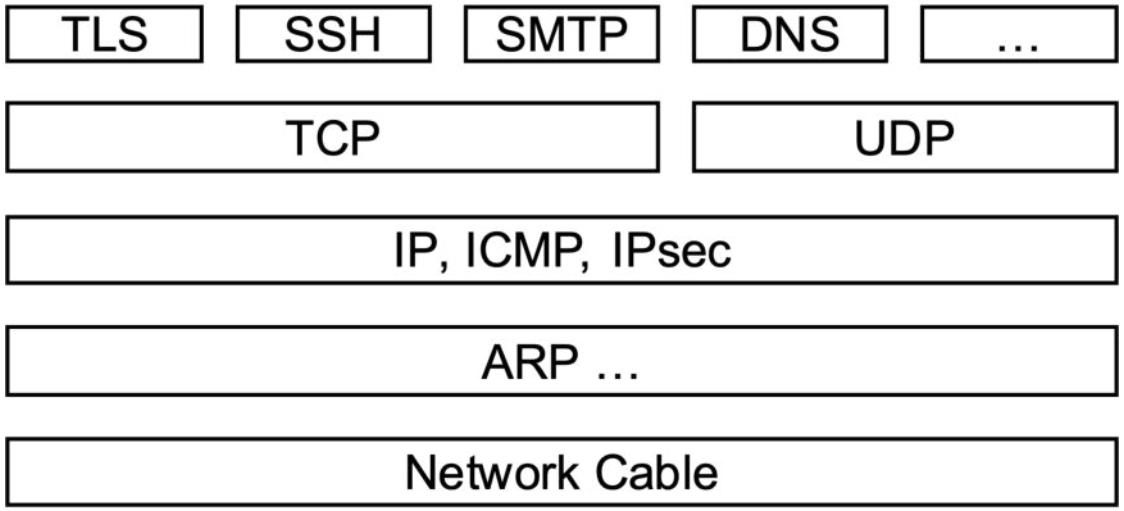
Output: Public key, $pk \in \mathbb{B}^{32+32k(\text{bitlen }(q-1)-d)}$,
and private key, $sk \in \mathbb{B}^{32+32+64+32\cdot((\ell+k)\cdot\text{bitlen }(2\eta)+dk)}$.

1: $\xi \leftarrow \{0,1\}^{256}$ ▷ Choose random seed
2: $(\rho,\rho',K) \in \{0,1\}^{256} \times \{0,1\}^{512} \times \{0,1\}^{256} \leftarrow \text{H}(\xi,1024)$ ▷ Expand seed
3: $\hat{\mathbf{A}} \leftarrow \text{ExpandA}(\rho)$ ▷ $\mathbf{A}$ is generated and stored in NTT representation as $\hat{\mathbf{A}}$
4: $(\mathbf{s}_1,\mathbf{s}_2) \leftarrow \text{ExpandS}(\rho')$
5: $\mathbf{t} \leftarrow \text{NTT}^{-1}(\hat{\mathbf{A}} \circ \text{NTT}(\mathbf{s}_1)) + \mathbf{s}_2$ ▷ Compute $\mathbf{t} = \mathbf{A}\mathbf{s}_1 + \mathbf{s}_2$
6: $(\mathbf{t}_1,\mathbf{t}_0) \leftarrow \text{Power2Round}(\mathbf{t},d)$ ▷ Compress $\mathbf{t}$
7: $pk \leftarrow \text{pkEncode}(\rho,\mathbf{t}_1)$
8: $tr \leftarrow \text{H}(\text{BytesToBits}(pk),512)$
9: $sk \leftarrow \text{skEncode}(\rho,K,tr,\mathbf{s}_1,\mathbf{s}_2,\mathbf{t}_0)$ ▷ K and tr are for use in signing
10: **return** (pk,sk)

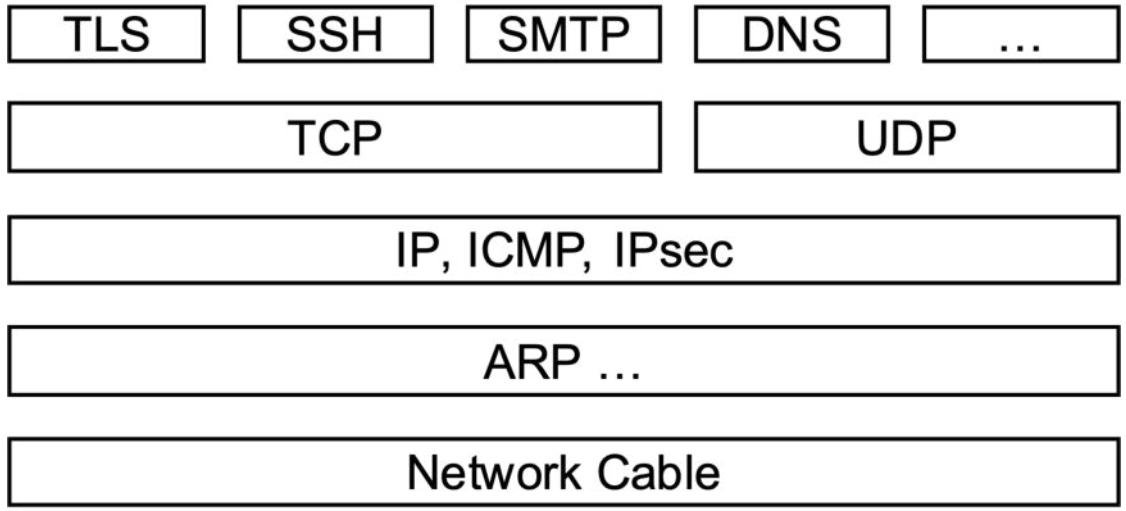
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.ipd.pdf

Protocols

Internet Protocols Stack

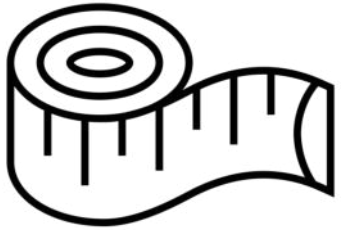


Internet Protocols Stack



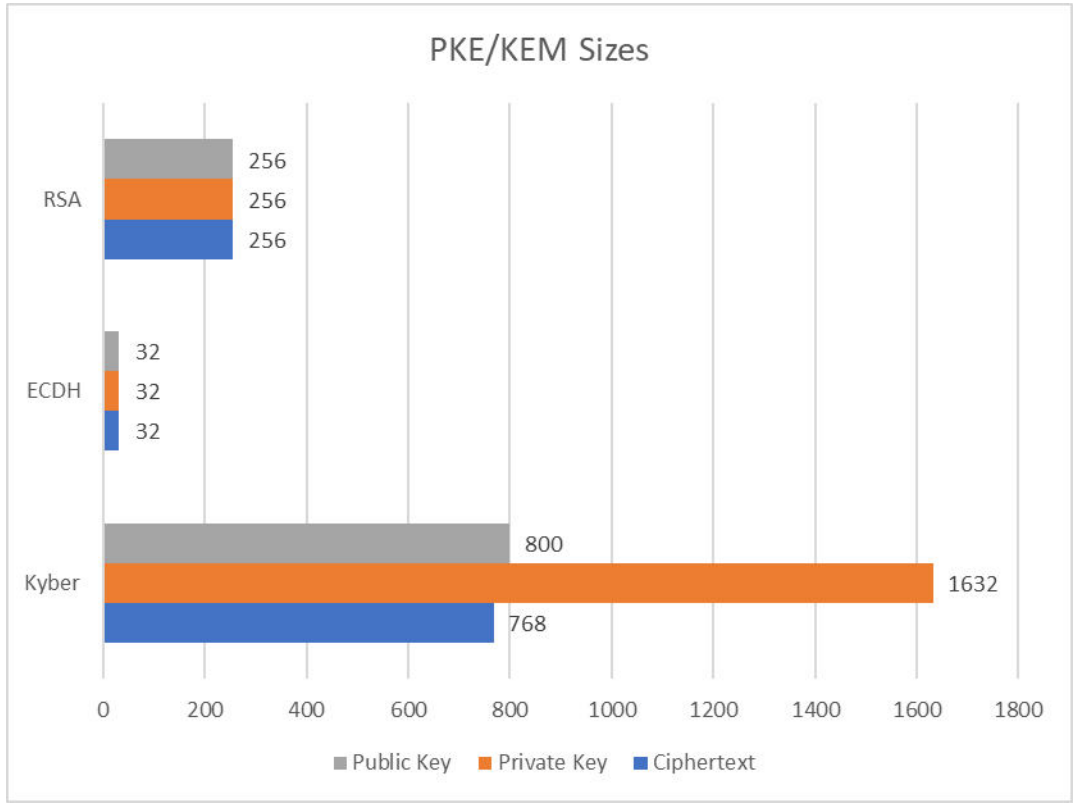
Requirements

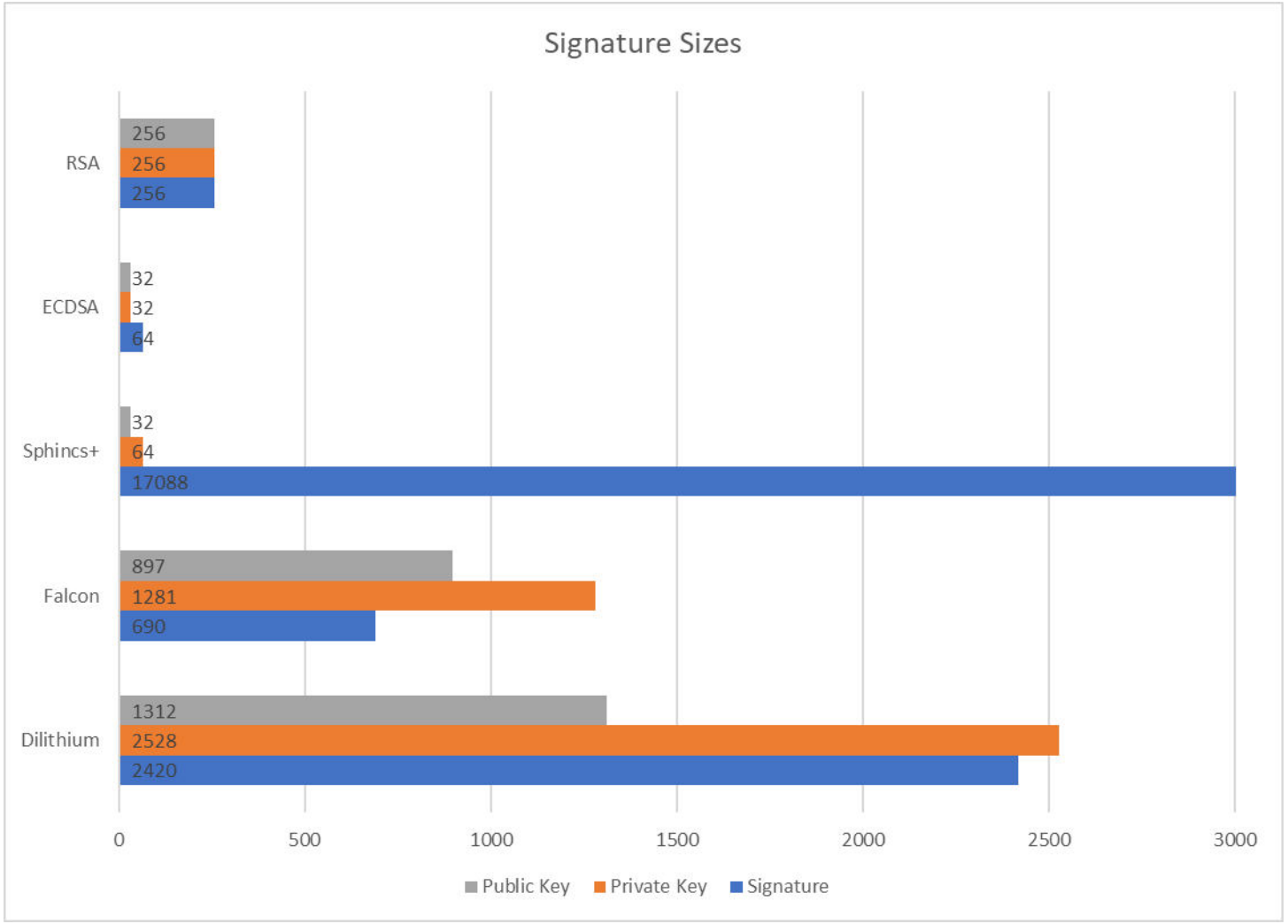
TIME



SIZE

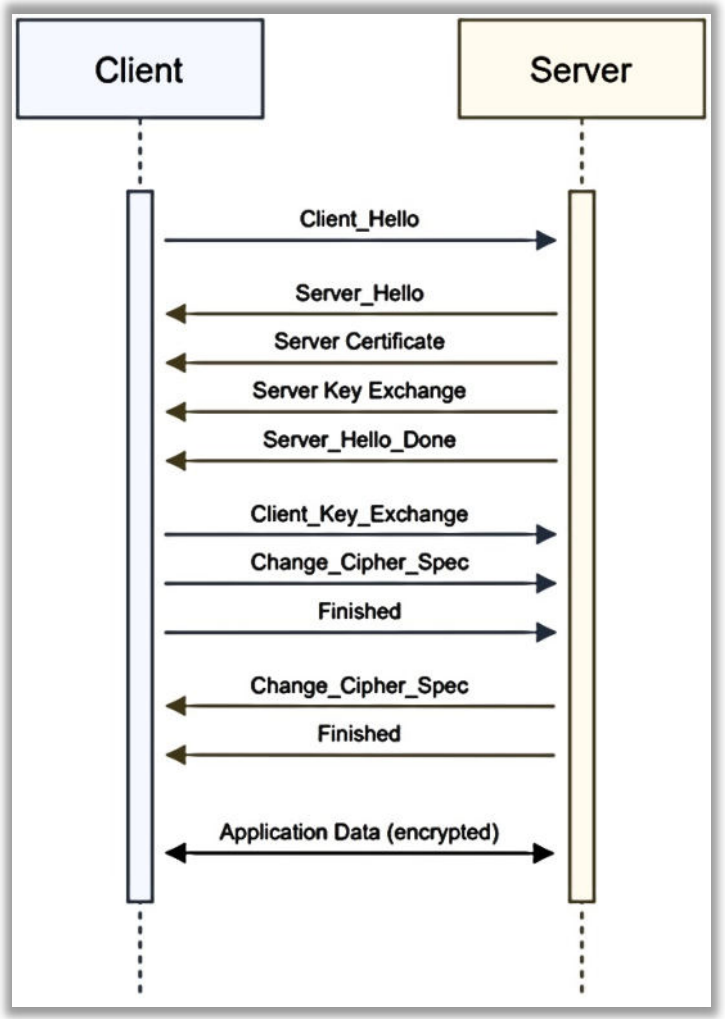
Sizes


PKE/KEM Sizes
RSA
256
256
256
ECDH
32
32
32
Kyber
800
1632
768
0
200
400
600
800
1000
1200
1400
1600
1800
Public Key
Private Key
Ciphertext


Signature Sizes
RSA
256
256
256
ECDSA
32
32
64
Sphincs+
32
64
17088
Falcon
897
1281
690
Dilithium
1312
2528
2420
0
500
1000
1500
2000
2500
3000
Public Key
Private Key
Signature

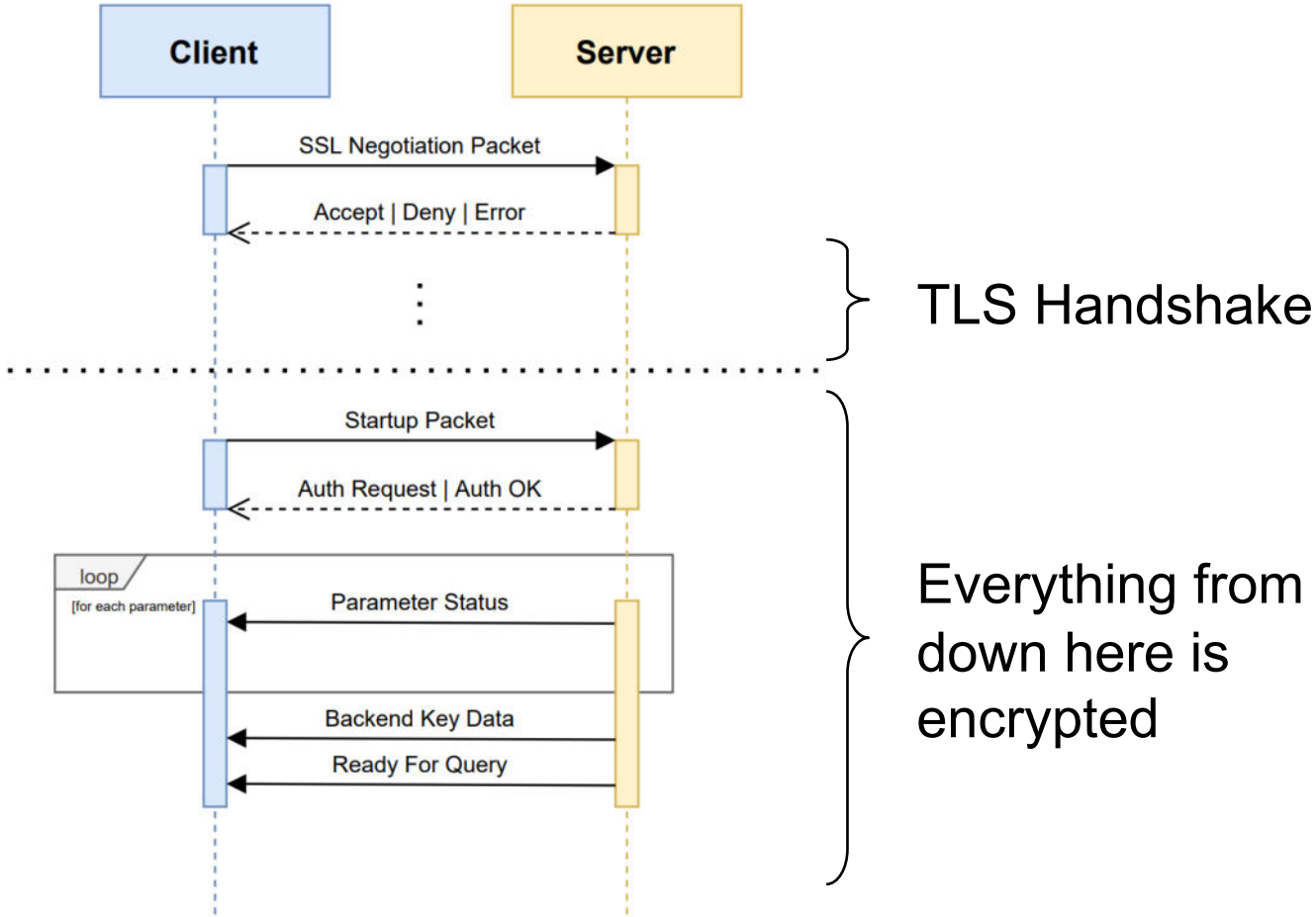
TLS

- Client and Server communicate through public channel
  - Exchanged data must be encrypted
- Handshake Protocol
  - Negotiation of encryption parameters (cipher suite, compression, …)
  - Authentication of server (mutual authentication possible) → requires digital signature
  - Secure exchange of session keys → requires key exchange/key encapsulation mechanism

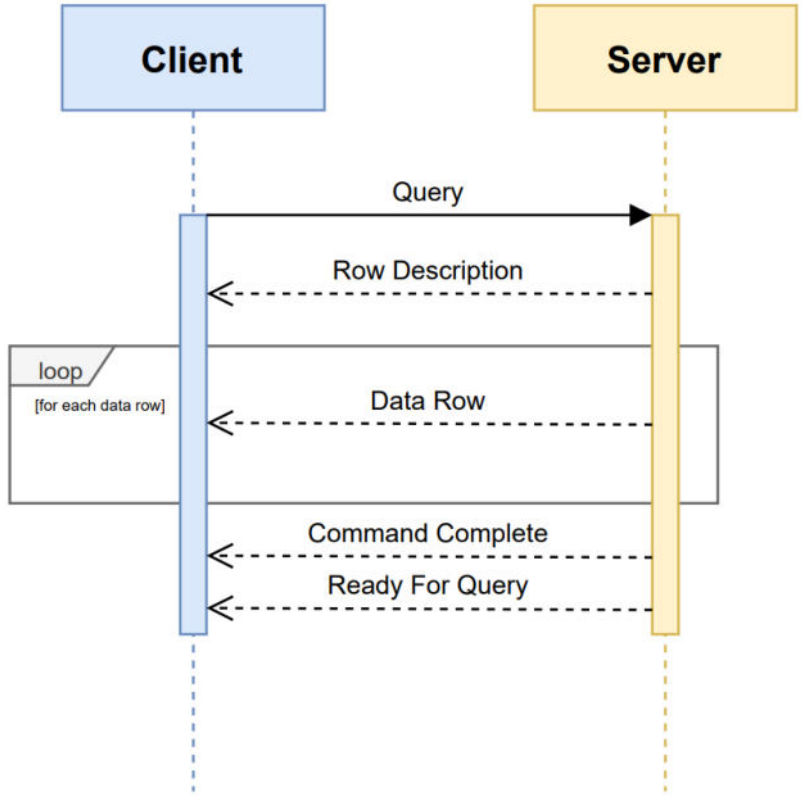


PostgreSQL: Frontend-Backend Protocol

Connection with TLS:



Retrieving data:

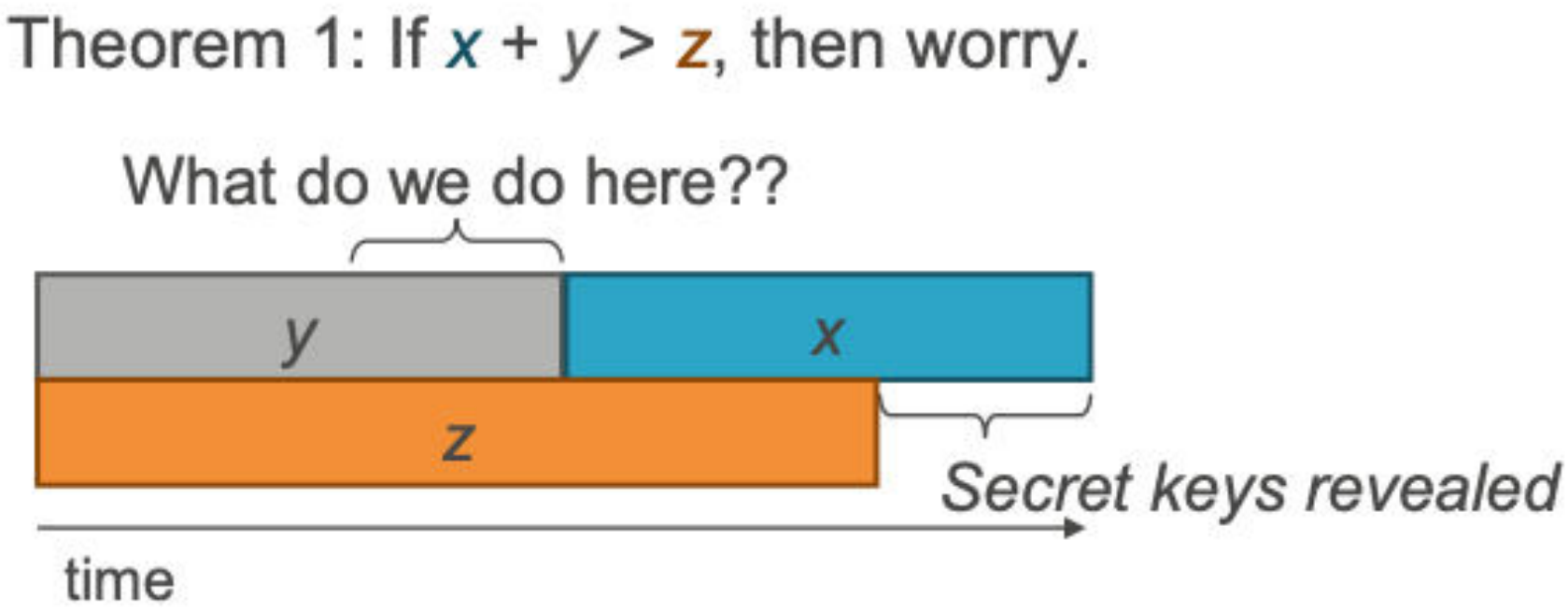


https://link.springer.com/chapter/10.1007/978-3-031-10684-2_15

https://www.postgresql.org/docs/

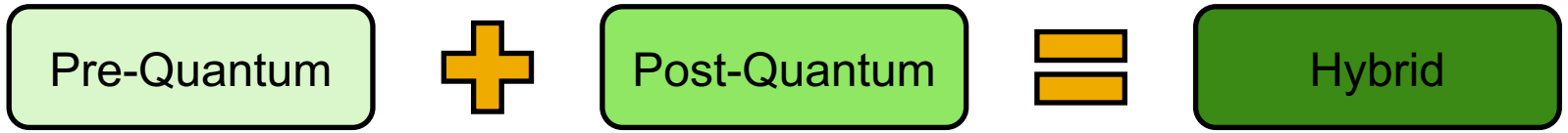
Integration and Migration

Quantum Uncertainty

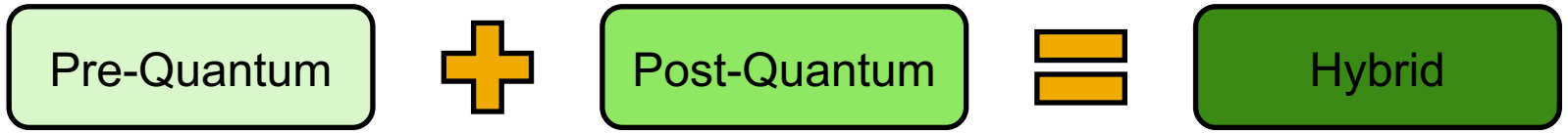


Source: https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf

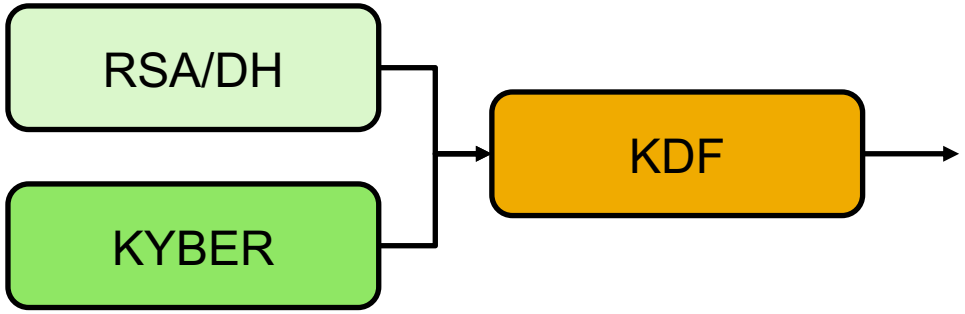
Hybrids



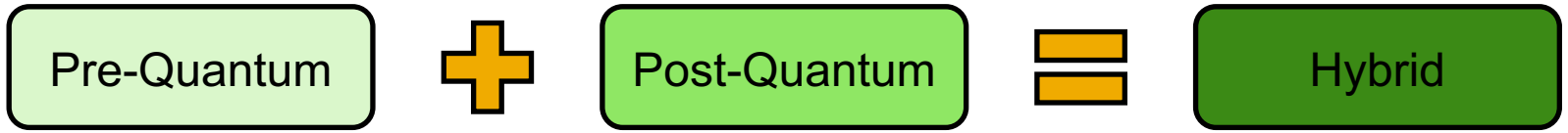
Hybrids



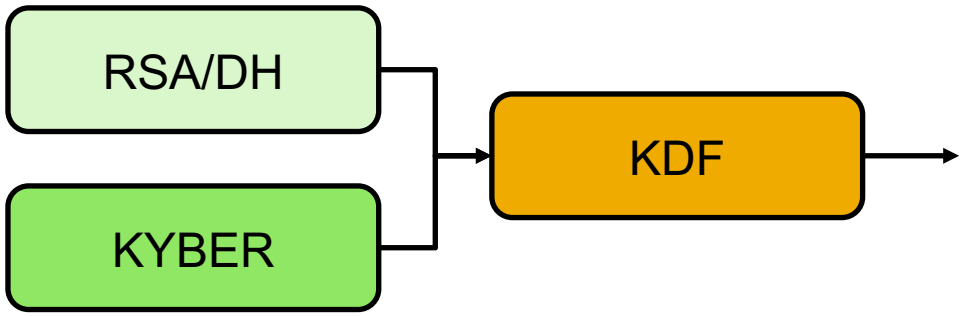
Hybrid Key Encapsulation Mechanism



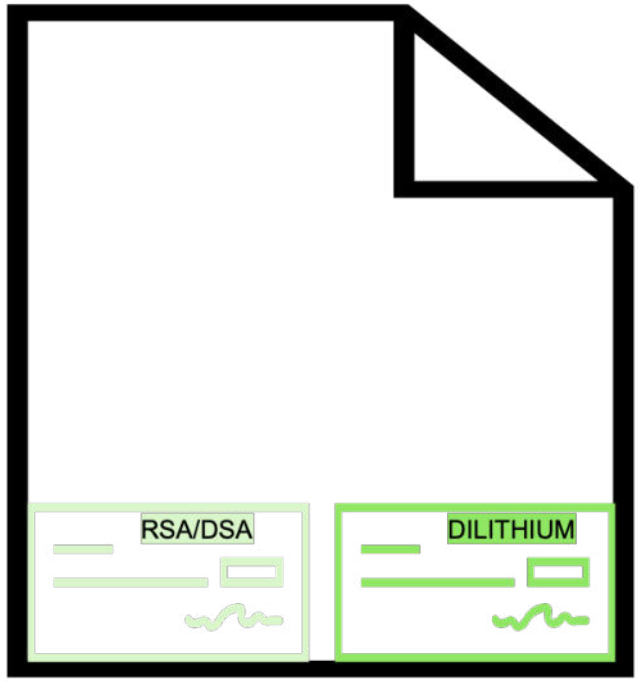
Hybrids



Hybrid Key Encapsulation Mechanism



Hybrid Digital Signature



More Challenges

Crypto-(non)agility

- Hardcoded crypto parameters

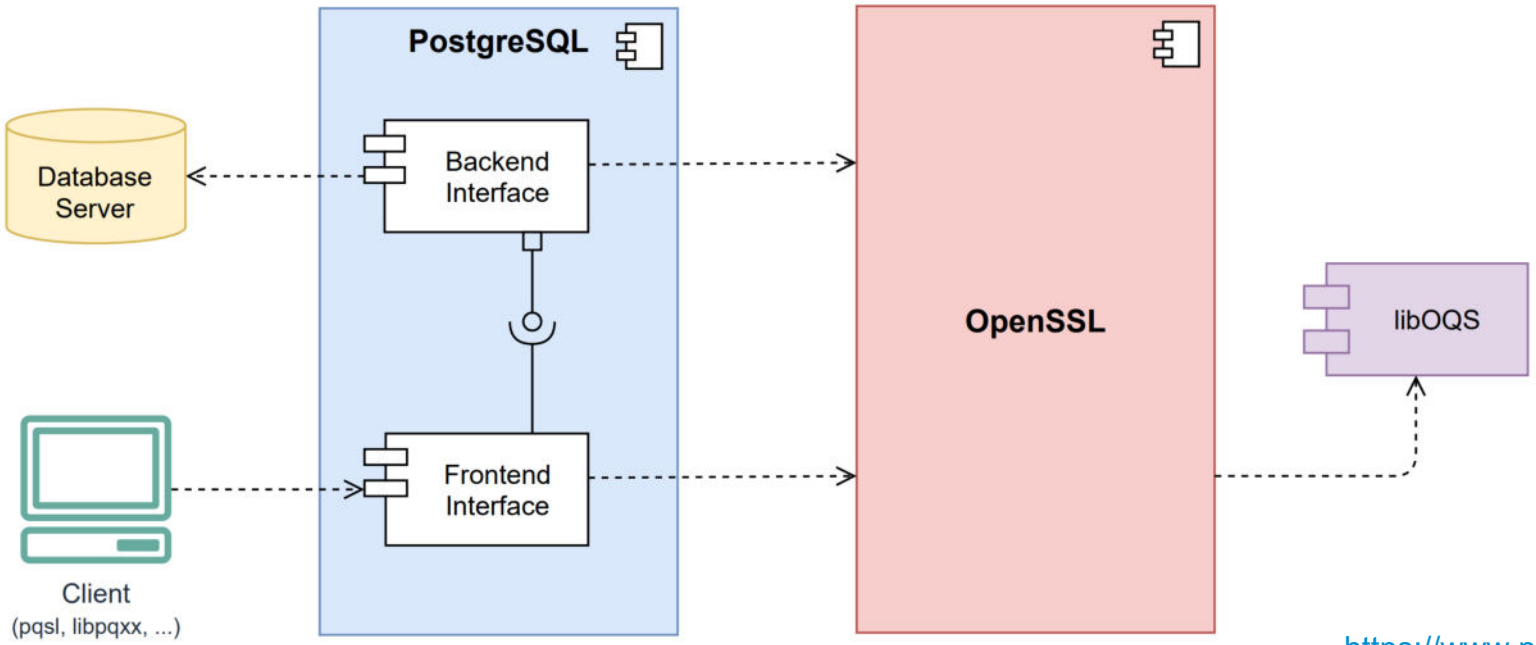
Crypto-inventory

- Which crypto is used where in code/protocols/etc.?

New requirements

- Decryption failure, state, size, etc.

Quantum-Safe TLS in PostgreSQL



https://link.springer.com/chapter/10.1007/978-3-031-10684-2_15

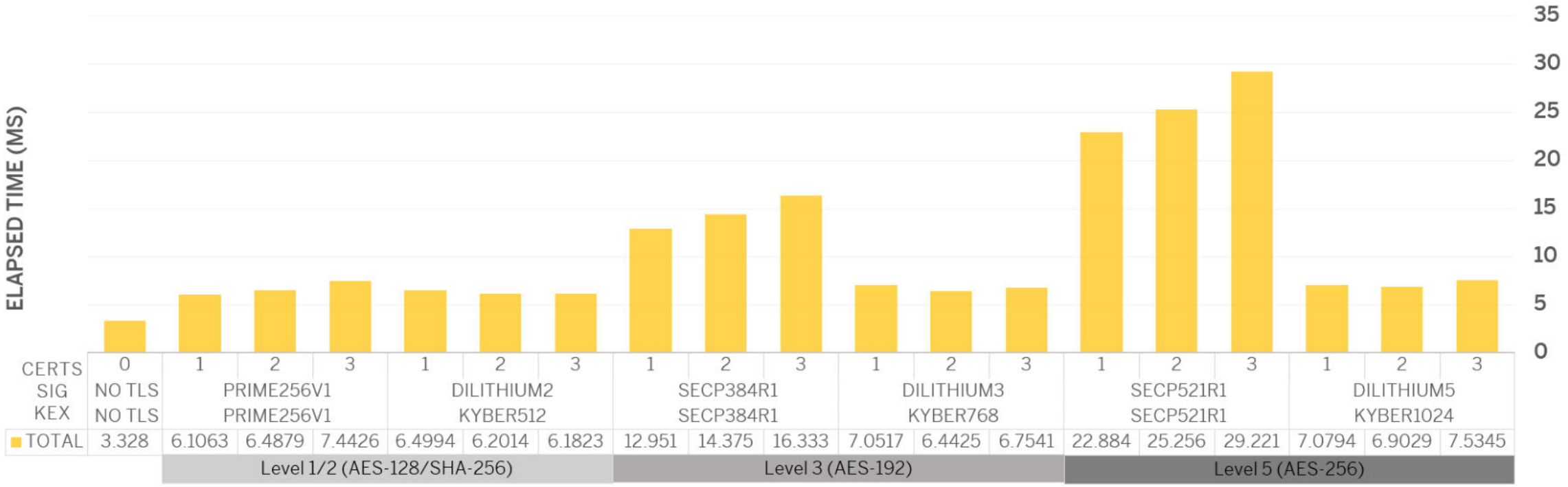
https://www.postgresql.org/docs/

https://github.com/postgres/postgres

https://www.openssl.org/

https://openquantumsafe.org/

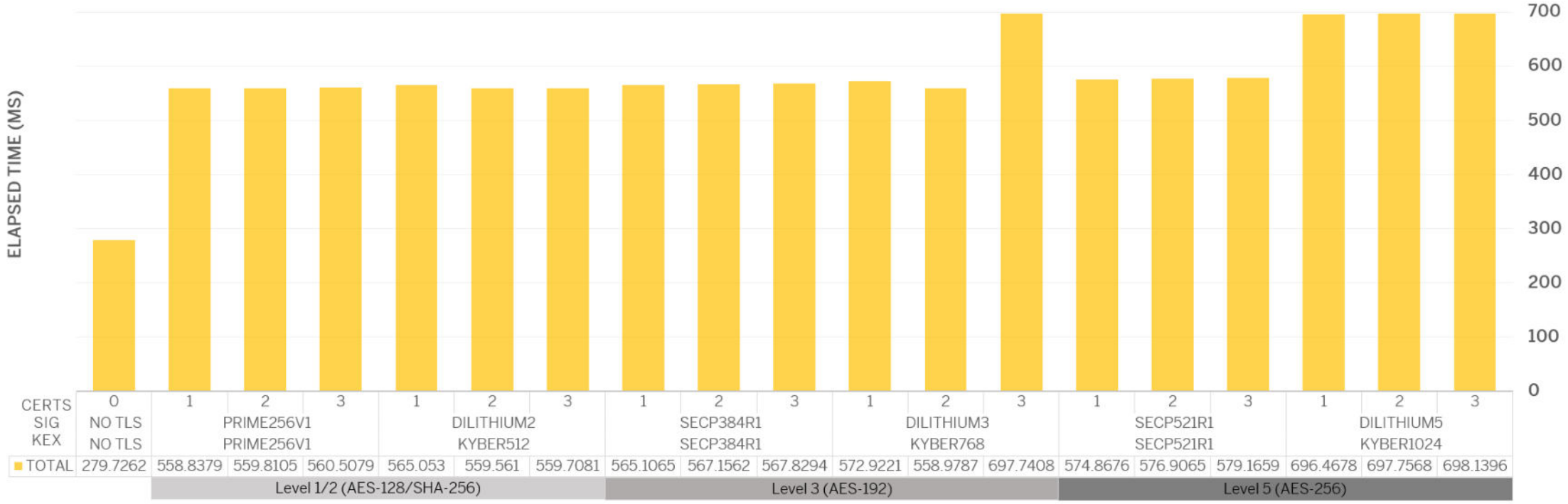
PostgreSQL TLS-Handshake on LAN: ECC vs. Quantum-safe



https://link.springer.com/chapter/10.1007/978-3-031-10684-2_15

Latency: 0.98 ms

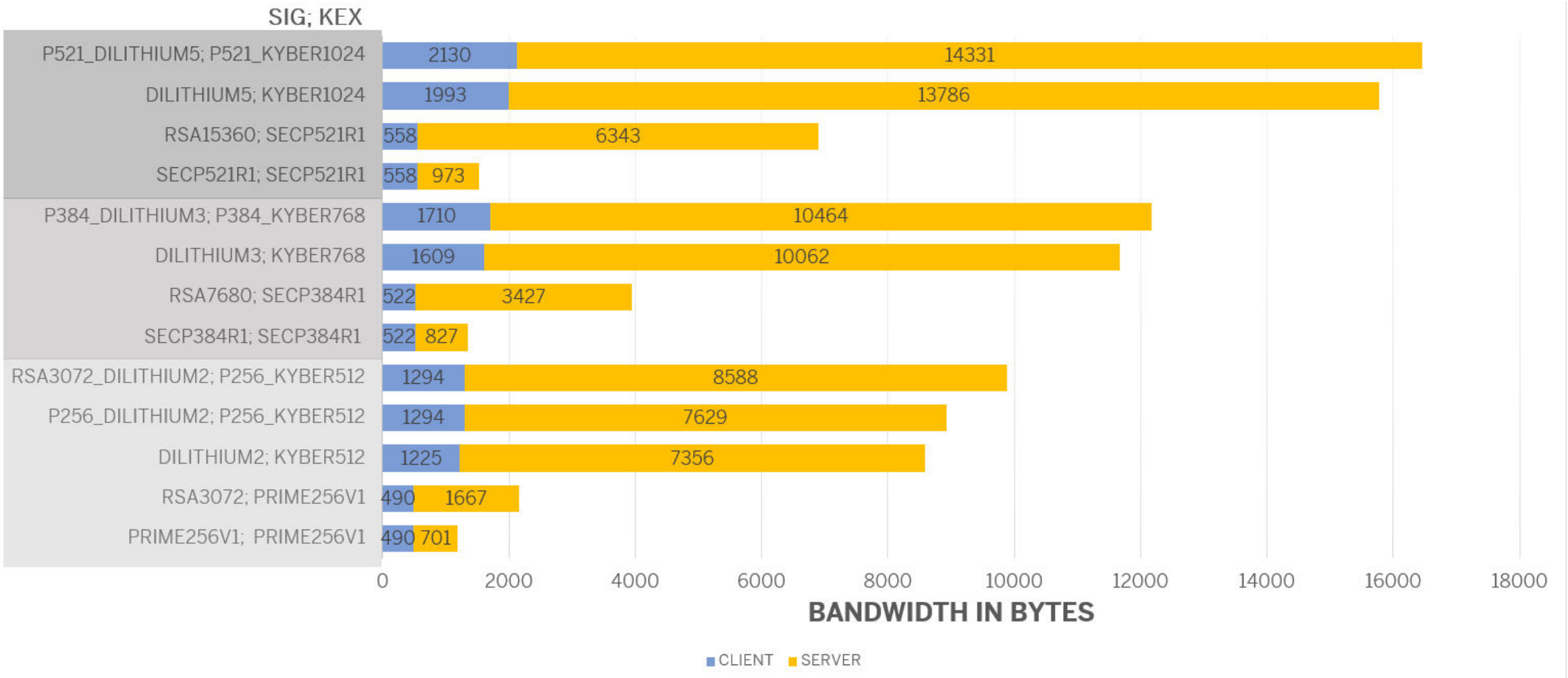
PostgreSQL TLS-Handshake on WAN: ECC vs. Quantum-safe



https://link.springer.com/chapter/10.1007/978-3-031-10684-2_15

Latency: 140 ms

PostgresSQL TLS-Handshake Bandwidth



https://link.springer.com/chapter/10.1007/978-3-031-10684-2_15

Stateful Hash-based Signature

Implementation challenges

- The State
  - Part of private key – must be updated
- State Management
  - Read → Sign → Update → Save
- Hardcoding
  - Hardcoded verification algorithms

```
//Private Key and Input have been initialized before...
Signature signature = Signature.getInstance("SHA256WITHXMSSMT");
signature.initSign(xmssPrivate);
signature.update(input);
byte[] sig = signature.sign();
```

Other Issues

- Serialization
  - Invalid signature after updating and storing

Takeaways

Summary

Standardization and Regulations

- Different players → several standards/recommendations → Interoperatbility
- PQC Immaturity

Implementation

- PQC Complexity → too many parameters, complex algorithms
- PQC Diversity

Internet Protocols

- Requirement on runtime
- Requirement on packet size

Integration and Migration

- PQC uncertainty
- Hybrids, crypto-(non)agility, crypto inventory, new requirements

Recommendations

Stay tuned

- Visit: NIST PQC Website, NCCoE Migration Website
- Attend PQC events: Like this one, NIST PQC events etc.

Start preparing now

- Various APIs: Open Quantum Safe (OQS) library and other APIs
- Crypto-Inventory
- Crypto-agility for new software version
- Migration plan → See NIST, BSI, ANSSI, NCCoE, etc.

Thank you.

Contact information:

Anselme Tueno
anselme.tueno@sap.com

“It is critical to begin planning for replacement of hardware, software, and services that use public-key algorithms now so that the information is protected from future attacks.”

~ NIST NCCoE

https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

THE BEST RUN SAP

Post-Quantum Cryptography Conference

PKI Consortium

ENTRUST

HID

PQ SHIELD

Fortanix

KEYFACTOR

NOREG

QRL

THALES

d-trust.

amsterdam convention bureau

ascertia

亞洲誠信 TRUSTAsia