Post-Quantum
Cryptography Conference

Crunching the Numbers: Post Quantum Algorithm Performance

Tomas Gustavsson
Chief PKI Officer at Keyfactor

KEYFACTOR

KEYFACTOR

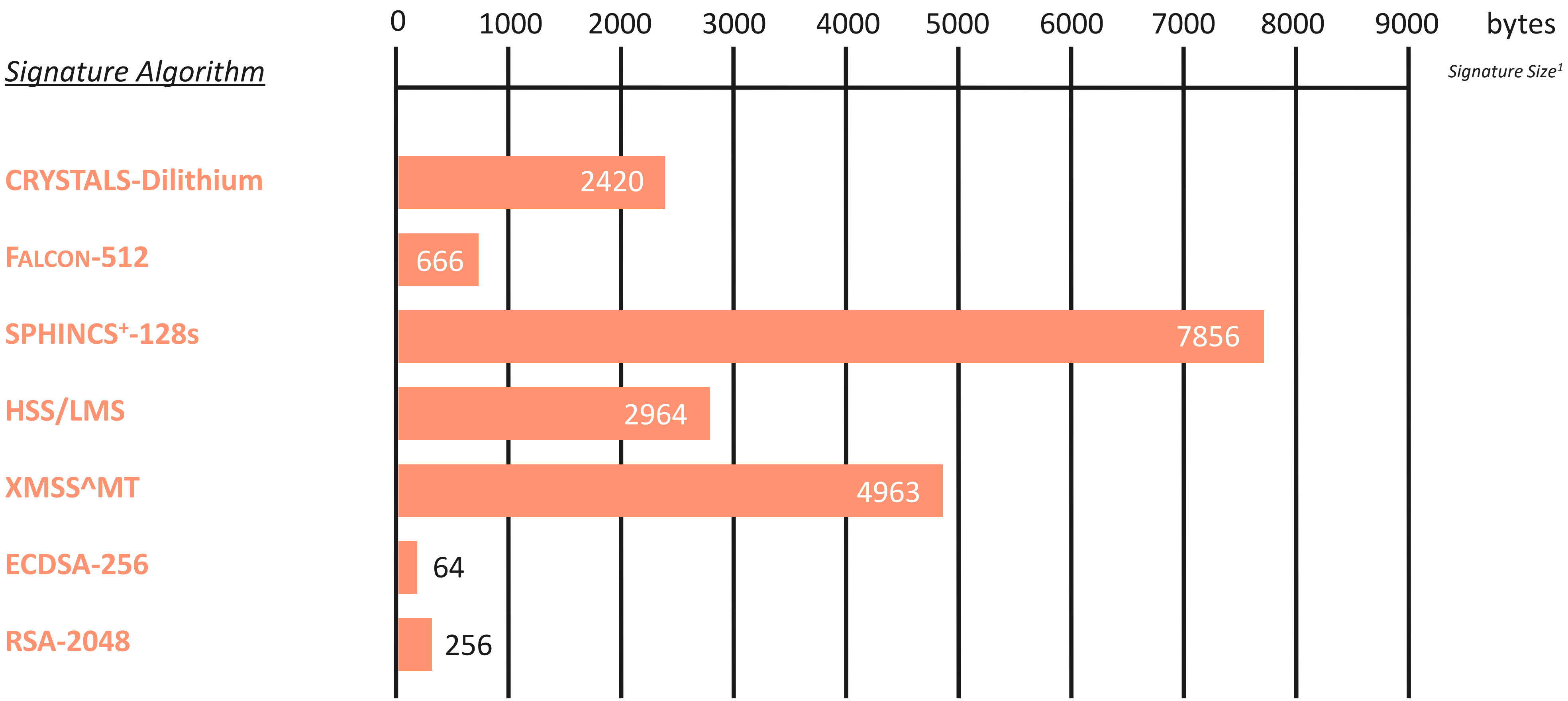
Crunching the Numbers:
The Reality of Quantum Algorithm Performance and Security

Tomas Gustavsson, Chief PKI Officer

Post-Quantum Algorithm Metrics

How does it compare
to todays world?

Signature Size



Thanks to Verisign for the graph

[1]*with example parameters*

KEYFACTOR

Compare Apples with Apples

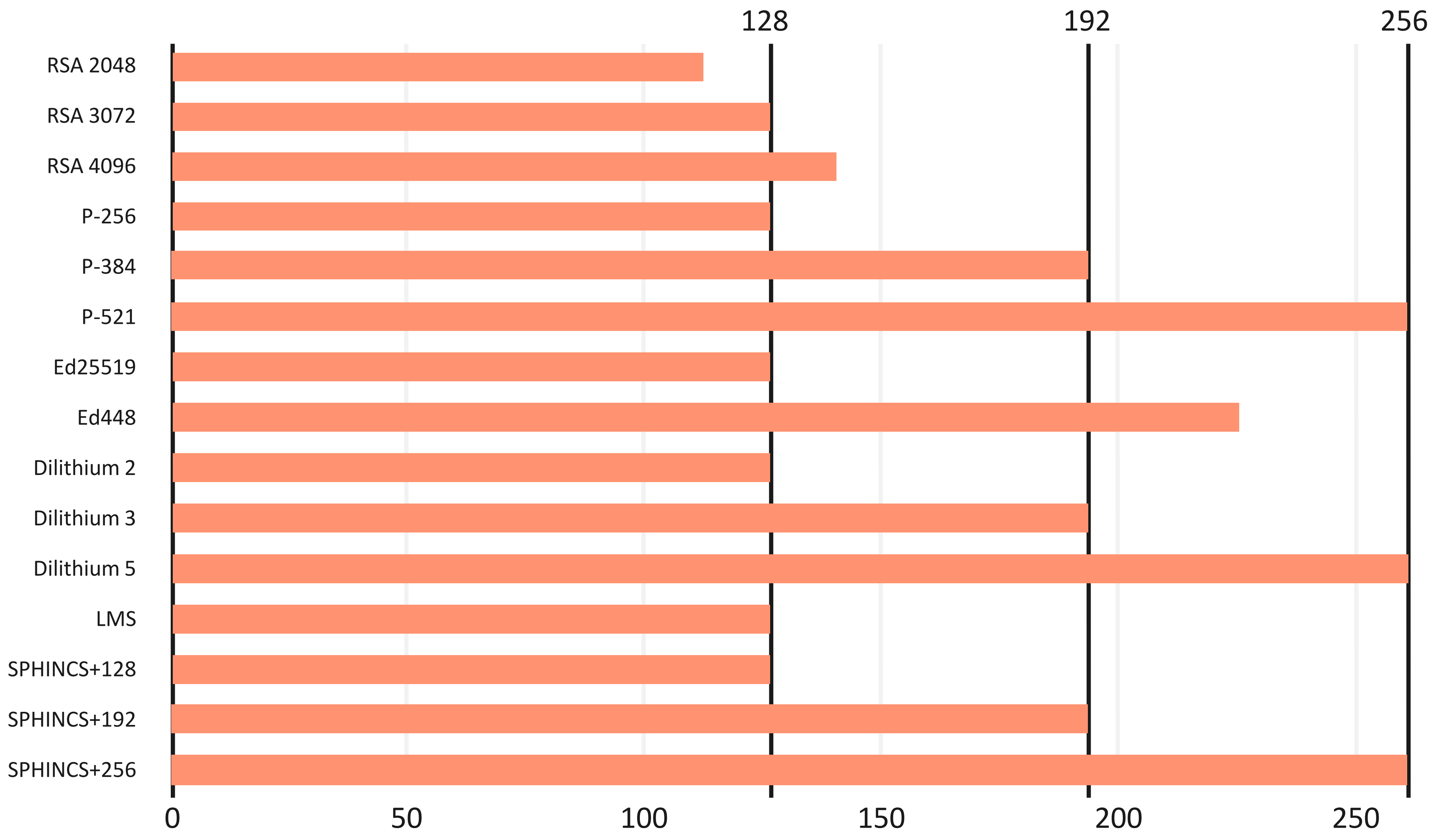
Level	Definition, as least as hard to break as...
1	To recover the key of AES-128 by exhaustive search
2	To find collision in SHA256 by exhaustive search
3	To recover the key of AES-192 by exhaustive search
4	To find collision in SHA384 by exhaustive search
5	To recover the key of AES-258 by exhaustive search

Security Strength	Symmetric Key Algorithms	FFC (DSA, DH, MQV)	IFC* (RSA)	ECC* (ECDSA, EdDSA, DH, MQV)
128	AES-128	L = 3072 N = 256	K = 3072	f = 256-383
192	AES-192	L = 7680 N = 384	K = 7680	f = 384-511
256	AES-256	L = 15360 N = 512	K = 15360	f = 512+

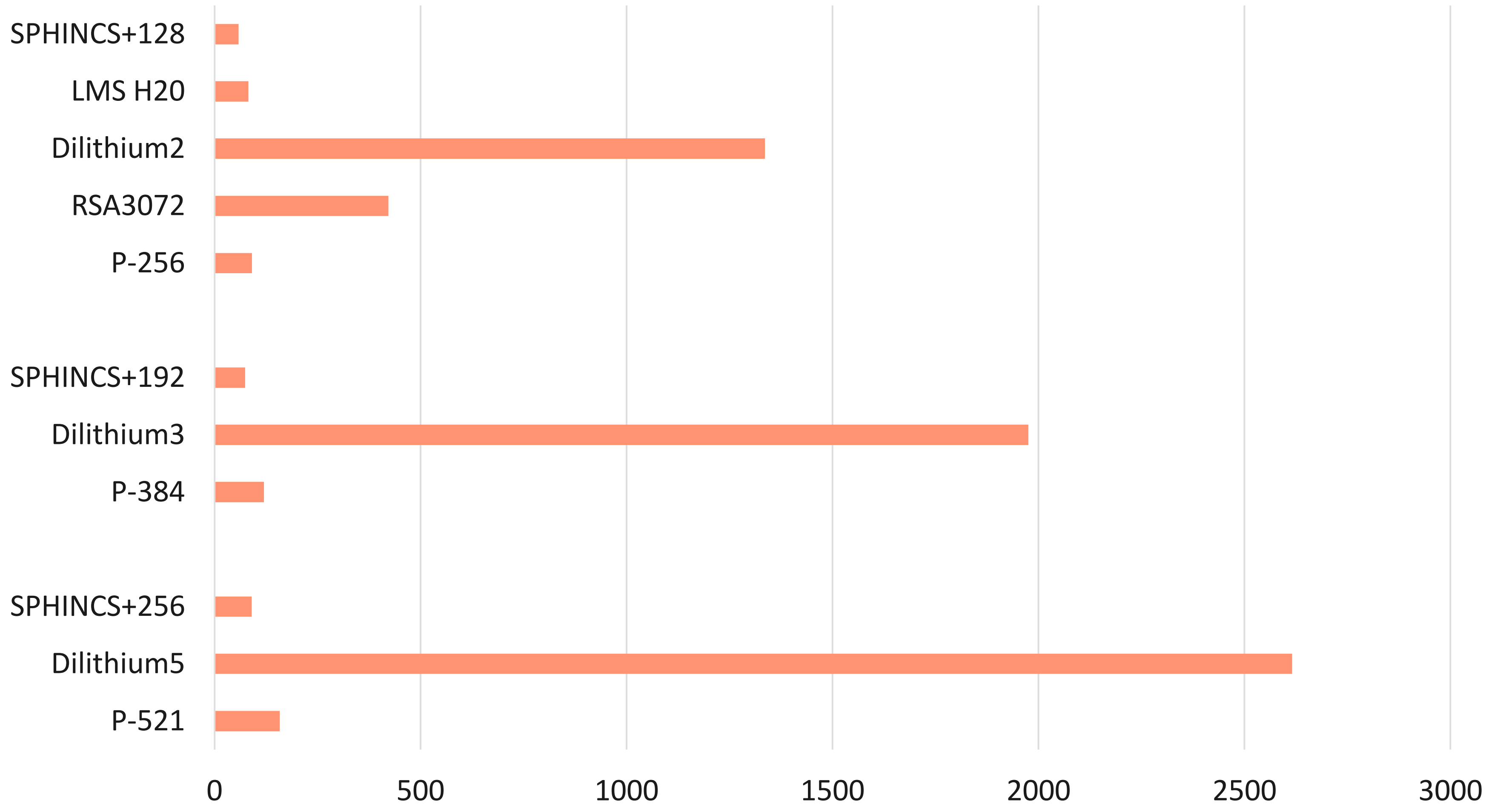
Key sizes

- Not obvious with PQC
- "security strength"; FIPS 800-57
- Solution "security level"

Security Levels

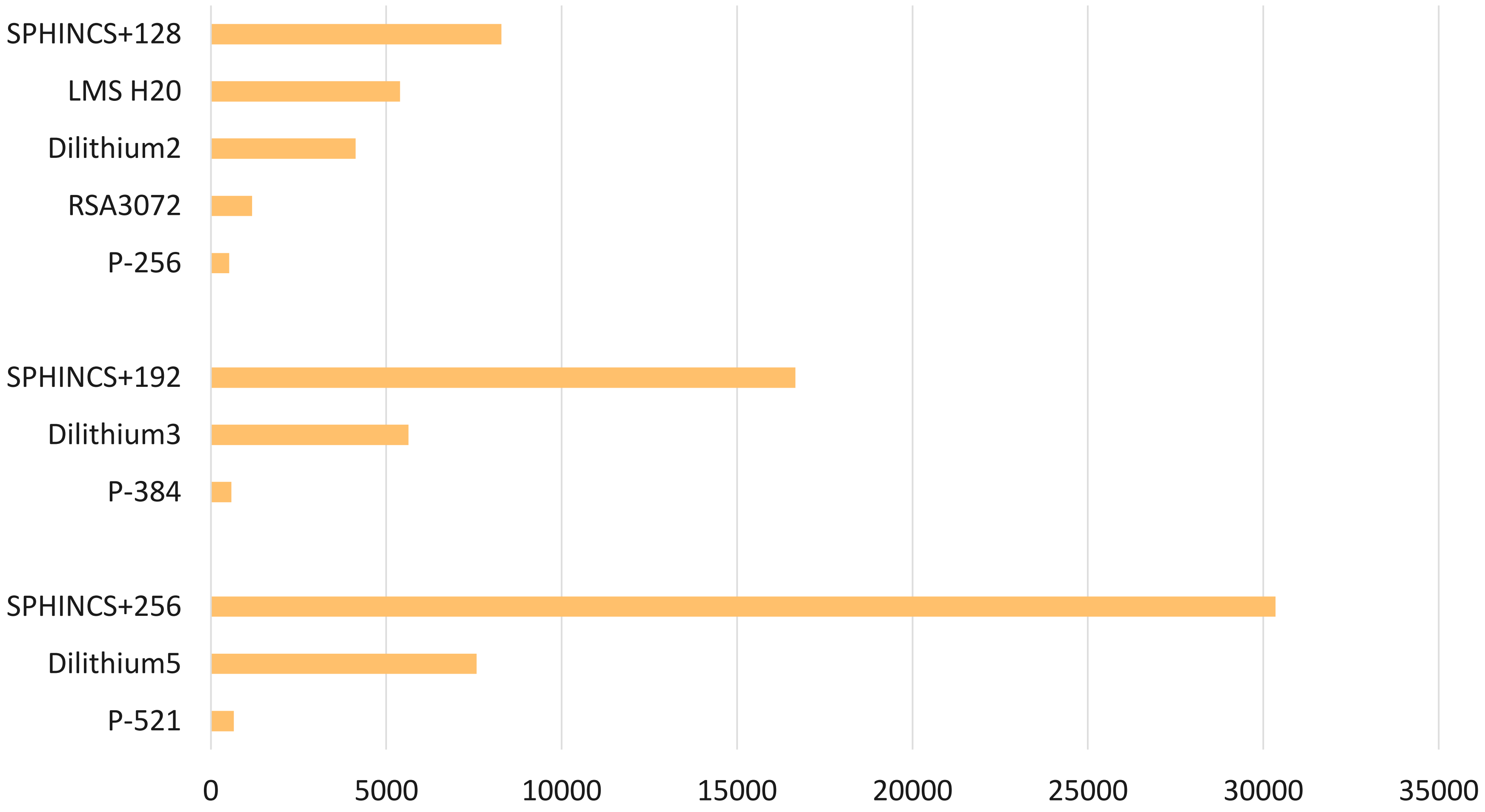


Public Key Size



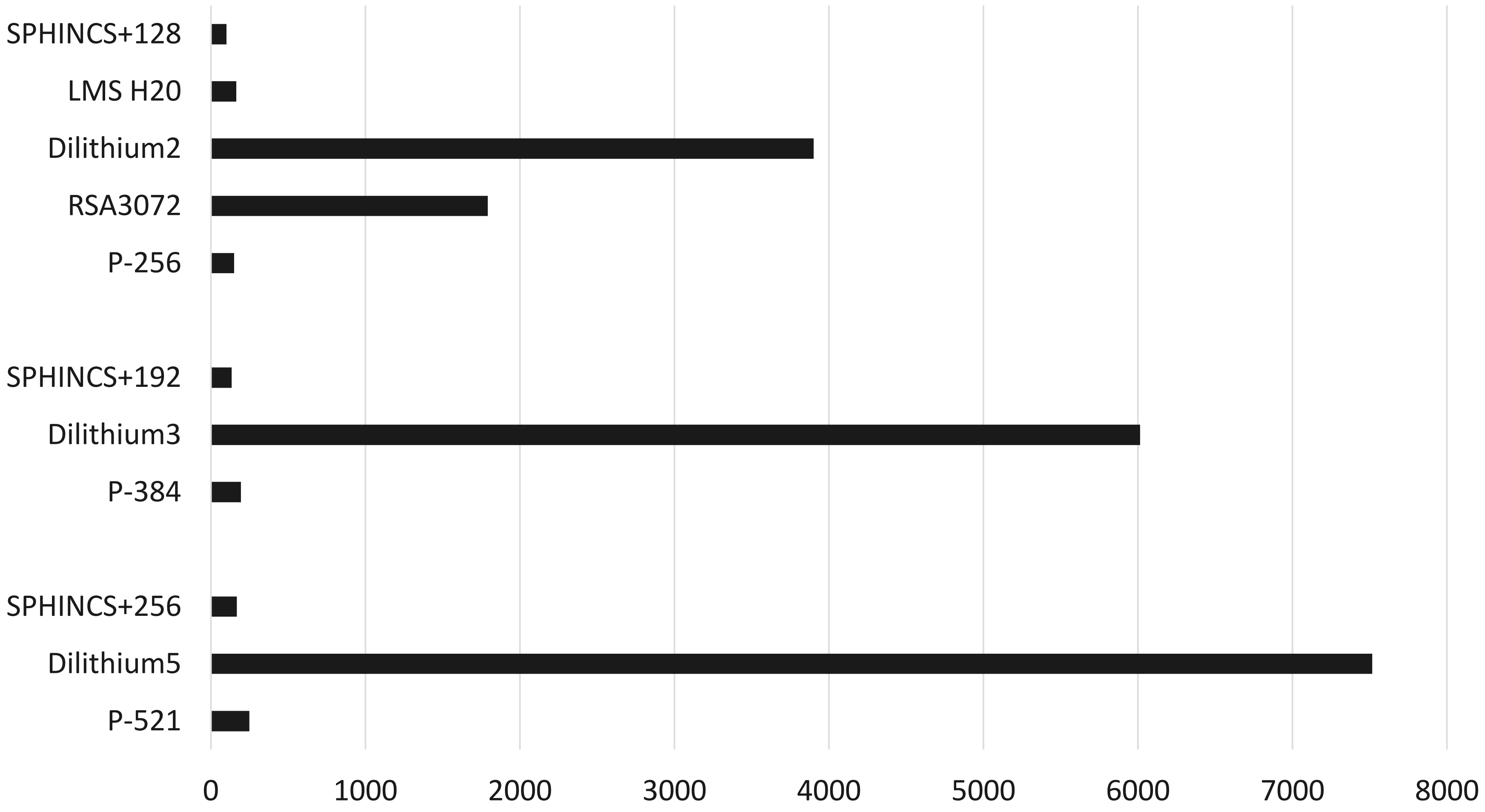
KEYFACTOR

Certificate Size



KEYFACTOR

Private Key Size



KEYFACTOR

Size Table

ALGORITHM	PUBLIC	PRIVATE	CERTIFICATE
SHA256WithRSA 3072	294	1217	1173
SHA256WithECDSA P-256	191	150	522
Dilithium2	1336	3902	4123
SPHINCS+ 128	58	101	8279
LMS_SHA256_M32_H20	82	164	5389

KEYFACTOR

Speed!

KEYFACTOR

HSM Status

5 HSMs tested with Dilithium

- 3 on Round3 version ✓
- 2 still on Round2 version ✗

(none on FIPS Draft specs)

KEYFACTOR

Certificate Issuance

<sample command>

KEYFACTOR

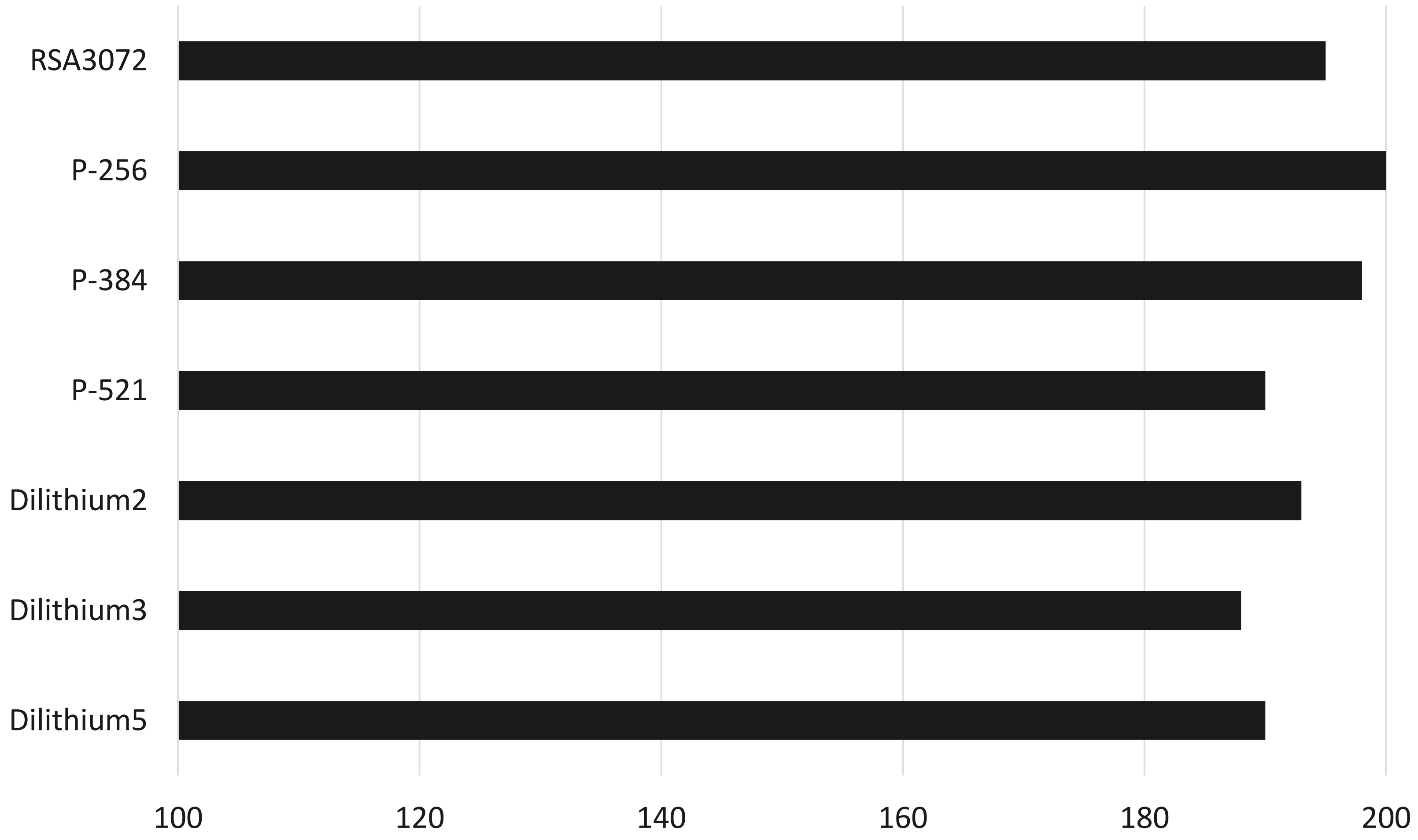
Software Crypto

BC 1.75

Test

- 10 threads
- 1 minute per CA
- 2 rounds
- Intel Corei7, 1TB SSD, 64GB RAM

Certificate Issuance - Software



KEYFACTOR

Certificate Issuance

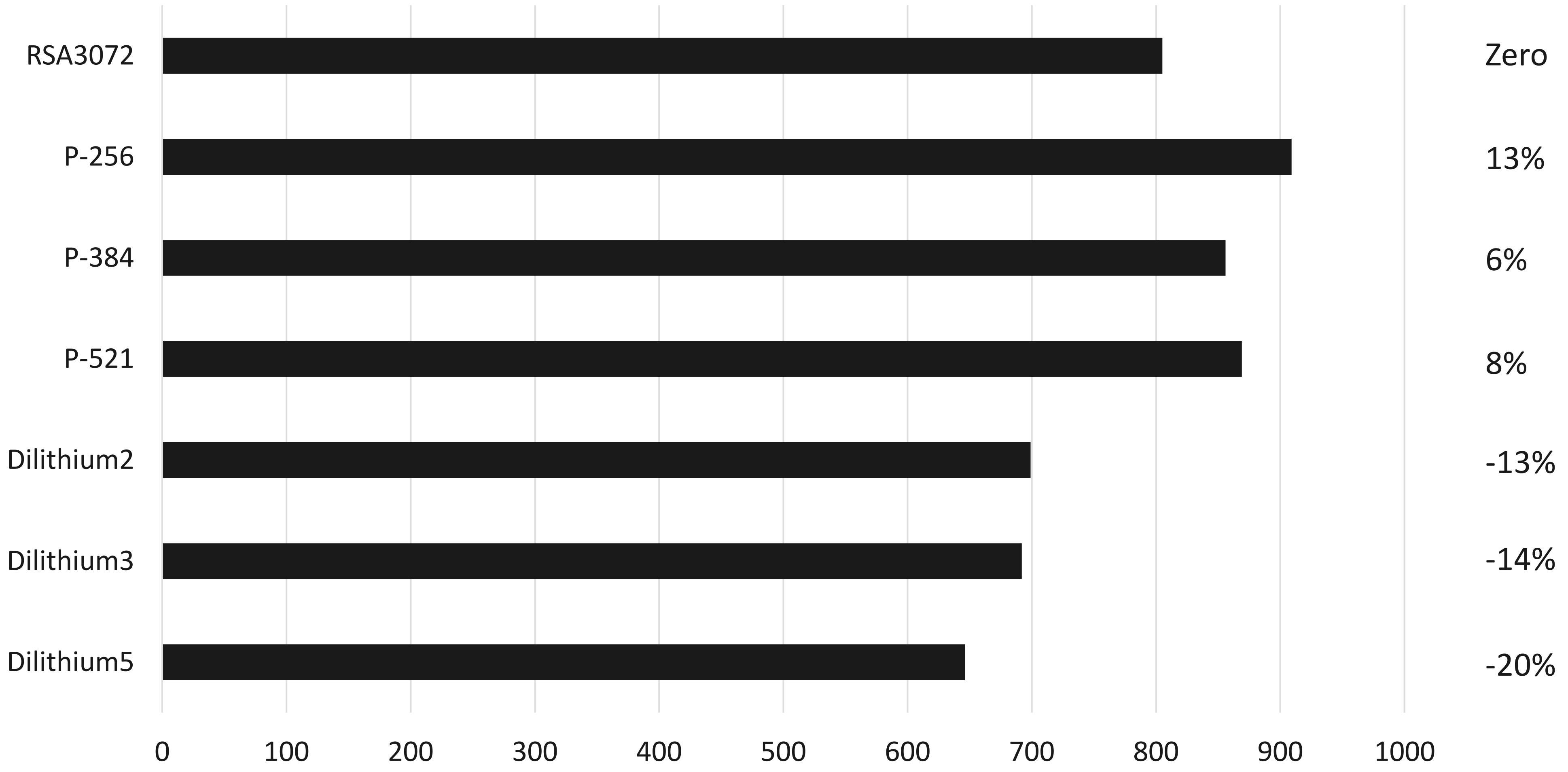
<sample command>

KEYFACTOR

50 threads

10 000 certificates

Certificate Issuance - Software



KEYFACTOR

HSM Signatures

<sample command>

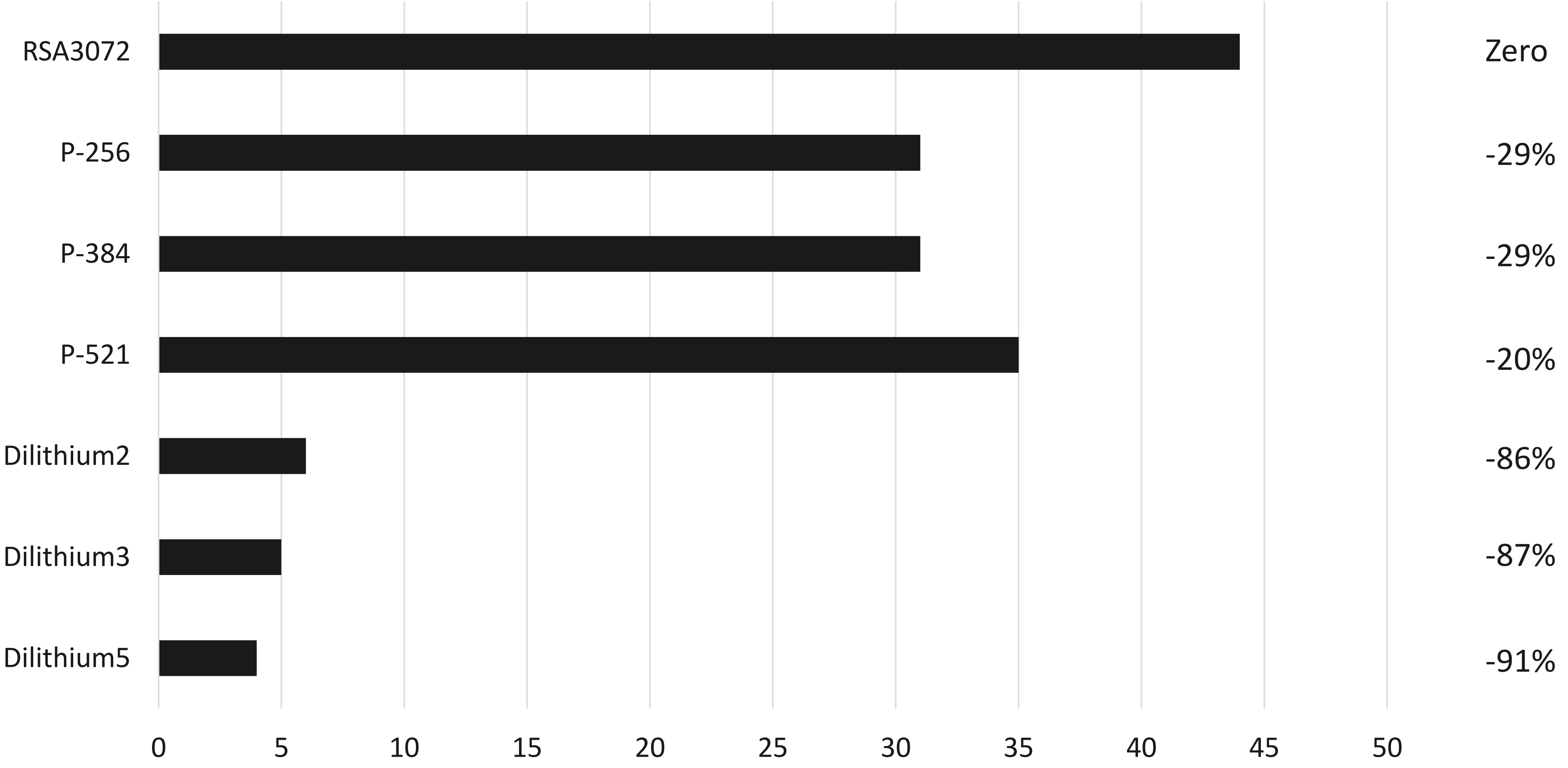
KEYFACTOR

15 threads

60 seconds

Network over cloud – high latency: +-10%

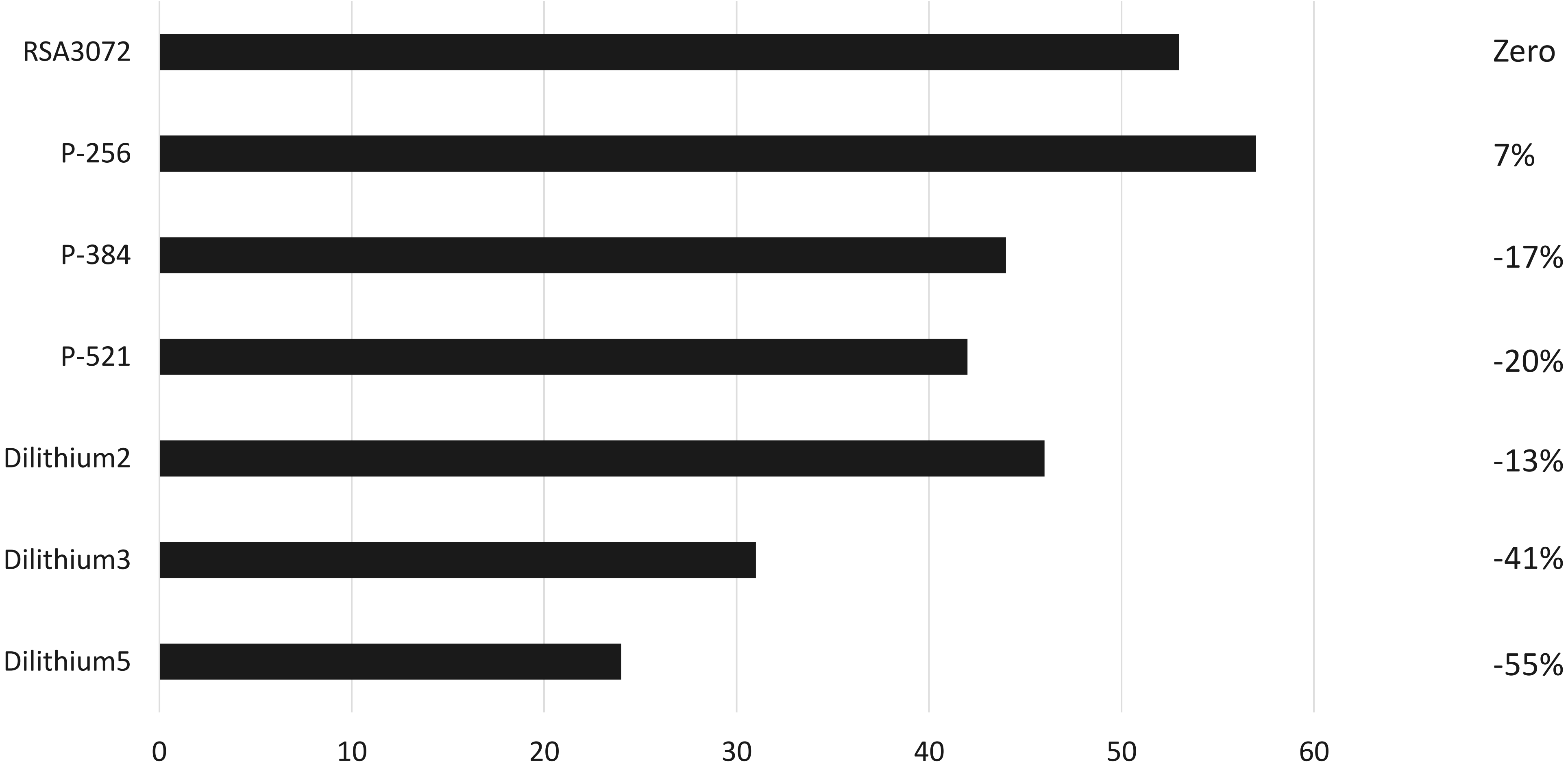
Signing Speed – HSM 1



KEYFACTOR

Network over cloud – high latency: +-10%

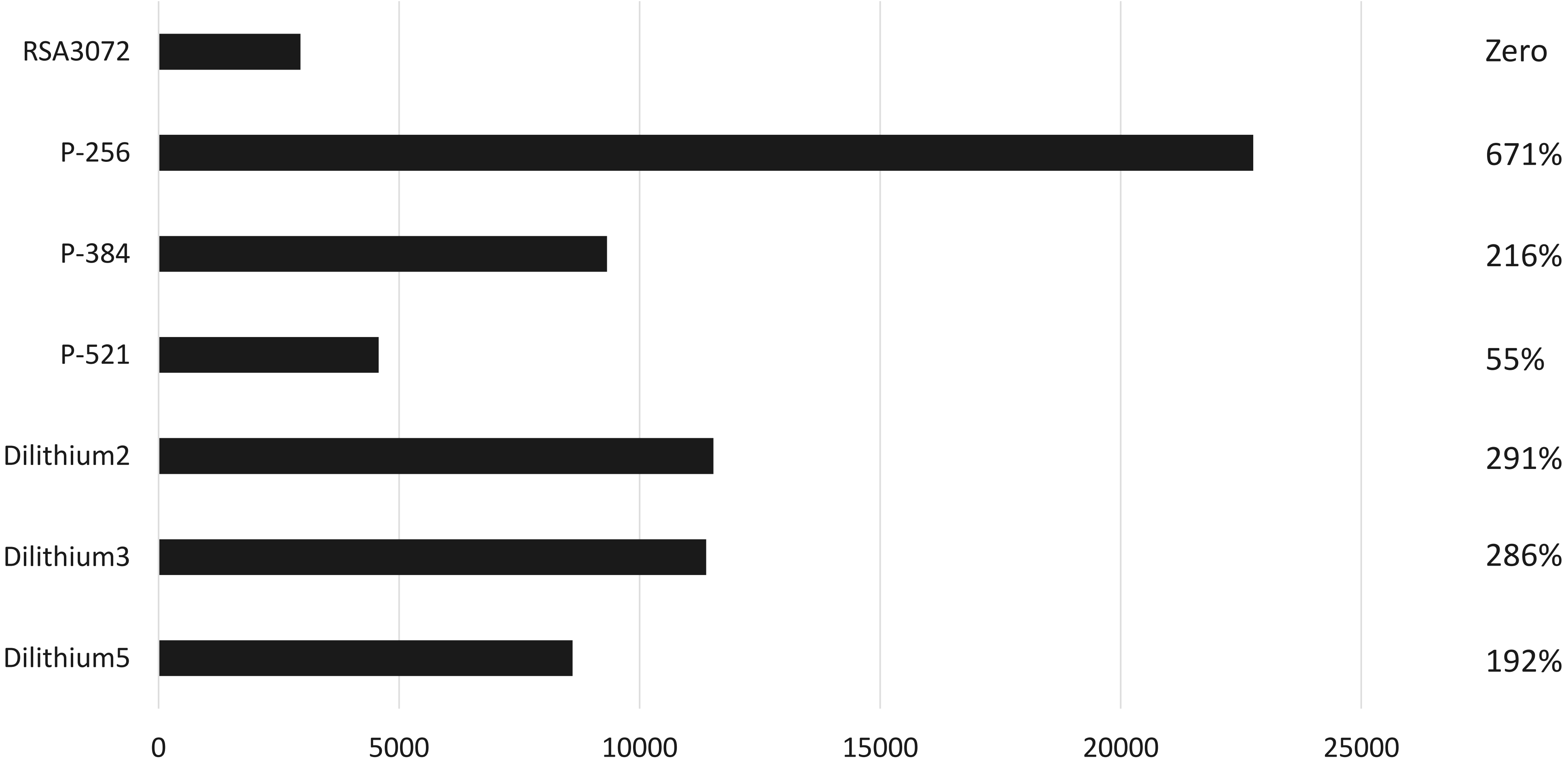
Signing Speed – HSM 2



KEYFACTOR

Local installed – low (no) latency

Signing Speed – HSM 3



KEYFACTOR

Key Generation

LMS

The other are “normal”

BC 1.76

KEYFACTOR

Stateful Hash Based Signature Algorithms (SHBS)

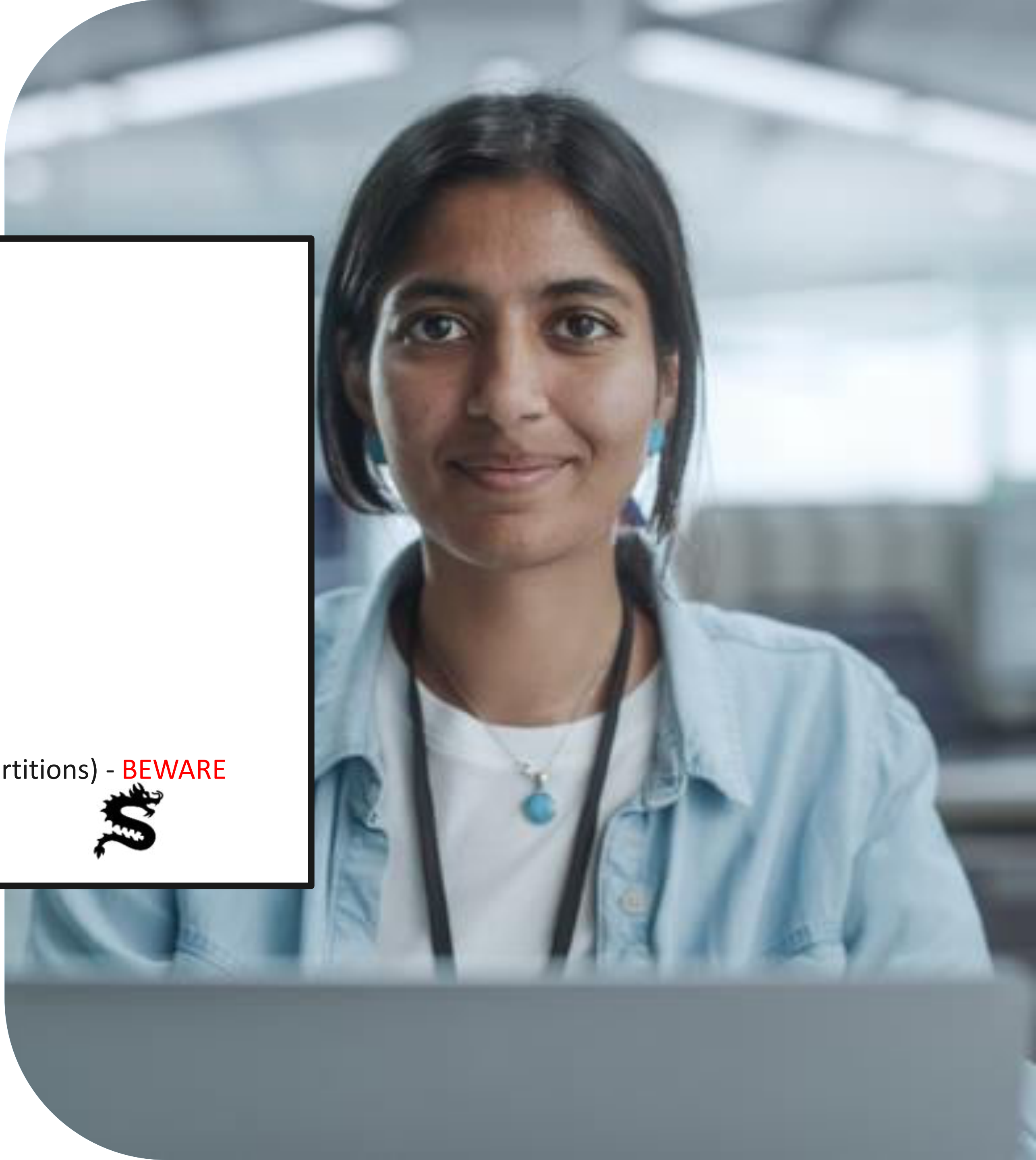
LMS TREE TYPE	HEIGHT	SIGNATURES	KEY GEN
LMS_SHA256_M32_H5	5	32	Fast (ms)
LMS_SHA256_M32_H10	10	1024	Fast (ms)
LMS_SHA256_M32_H15	15	32,768	Fast (s)
LMS_SHA256_M32_H20	20	1,048,576	Slow (m)
LMS_SHA256_M32_H25	25	33,554,432	Unbearable (h)

KEYFACTOR

Ok, so what does this mean to me?

- Signing and verification will not be horribly slow
- Database size
  - 1M certificates – 1GB -> 4GB
  - 1B certificates – 1TB -> 4TB
  - Signed Transactions and Logs?
- Optimizations will come

LMS for firmware signing - no H25 expected (but maybe partitions) - BEWARE



Open Questions?

- Constrained Devices
- Hardware and Software Optimizations
- CloudHSM efficiency
- ~~Which algorithms will be widely used?~~
- IT Eco Systems
  - How hard will the migration be? MD5 still seen...

Thanks!

KEYFACTOR

Post-Quantum

Cryptography Conference

PKI Consortium