QUBIP

Quantum-oriented Update to Browsers and Infrastructure for the PQ Transition

POST QUANTUM NEWS

Updates

MOLTENI MARIA CHIARA | SECURITY PATTERN

The QUBIP project is funded by the European Union under the Horizon Europe framework programme [Grant Agreement No. 101119746]

QUBIP Horizon Europe

GA 101119746

- Started September 2023
- 3 years project

We are a multi-disciplinary team of experts united by a single goal, to design a reference and replicable transition process to Post-Quantum Cryptography of protocols, networks and systems

Key length and security levels

Conventional VS Quantum computing

Key length and security levels

- **Key length** is a parameter of security
- **Security level**: idea of bits of security
  - For a cryptosystem with *n* bits of security, an attacker would need to perform *2^n* operations to break the encryption

- https://www.redcom.com/wp-content/uploads/2019/08/08-2019-Equivalencies-in-Security.pdf
- https://www.keylength.com/

Key length and security levels (conventional computing)

- AES: an attacker must do a guess in the set of the keys
- RSA: what an attacker guesses is the prime numbers between 0 and the modulus
  - The modulus size needs to be greater than the size of the AES key
- ECC: the security level is computed taking into account some algorithms used to solve the math problem on which are based

Bits of Security	*AES Key Size Needed (bits)*	*RSA Modulud Size Needed (bits)*	*ECC Public Key Sieze Needed (bits)*
128	128	3072	256
192	192	7680	384
256	256	15360	512

Security levels: Conventional VS Quantum computing

Algorithm	Key Length (in bits)	Security Level (in bits)	
		Conventional Computing	Quantum Computing
RSA-1024	1024	80	-
RSA-2048	2048	112	-
ECC-256	256	128	-
ECDH curve25519	32	< 128	-
AES-128	128	128	64
AES-192	192	192	96
AES-256	256	256	128
SHA-256	256	128	$85\frac{1}{3}$

Duits, I. J. te. “The Post-Quantum Signal Protocol : Secure Chat in a Quantum World.” (2019).

Post Quantum security levels

Level	Security Description
I	At least as hard to break as AES128 (exhaustive key search)
II	At least as hard to break as SHA256 (collision search)
III	At least as hard to break as AES192 (exhaustive key search)
IV	At least as hard to break as SHA384 (collision search)
V	At least as hard to break as AES256 (exhaustive key search)

https://openquantumsafe.org/liboqs/algorithms/kem/ml-kem.html

Algorithm	Security level	Sizes
ML-KEM-512	1	encapsulation (public) key: 800 decapsulation (private) key: 1632 ciphertext: 768 shared secret key: 32
ML-KEM-768	3	encapsulation (public) key: 1184 decapsulation (private) key: 2400 ciphertext: 1088 shared secret key: 32
ML-KEM-1024	5	encapsulation (public) key: 1568 decapsulation (private) key: 3168 ciphertext: 1568 shared secret key: 32
ML-DSA-44	1	Private Key: 2560 Public Key: 1312 Signature Size: 2420
ML-DSA-65	3	Private Key: 4032 Public Key: 1952 Signature Size: 3309
ML-DSA-87	5	Private Key: 4896 Public Key: 2592 Signature Size: 4627

Blog posts

Standards with Open Questions regarding PQC Adoption

- Here are analysed the standards that **would require** the integration of post-quantum (PQ) algorithms or **mitigate** the quantum computing risk to cryptography
  - SSH
  - MACsec
  - UEFI
  - TCP and QUIC
  - FIDO2
  - DNSsec

https://pqcc.org/standards-with-open-questions-regarding-pqc-adoption/

A look at the latest post-quantum signature standardization candidates

- Blogpost from Claudflare, which focus on the **digital signatures algorithms**
- **Feasibility of digital signatures algos** for use in TLS — handshake
  - For signature that are not create online
    - fast verification is much more important than fast signing
  - Public keys of the leaf and intermediate certificates are transmitted during the handshake
    - Minimize the combined size of the signature and the public key
  - For the other signatures, the public key is not transmitted during the handshake
    - better if it trades larger public keys for smaller signatures

https://blog.cloudflare.com/another-look-at-pq-signatures/

A look at the latest post-quantum signature standardization candidates

Fourteen schemes advanced to the **second round of the on ramp**

			Sizes (bytes)		CPU time (lower is better)	
Family	Name variant		Public key	Signature	Signing	Verification
Elliptic curves	Ed25519	❌	32	64	0.15	1.3
Factoring	RSA 2048	❌	272	256	80	0.4
Lattices	ML-DSA 44	✅	1,312	2,420	1 (baseline)	1 (baseline)
Symmetric	SLH-DSA 128s	✅	32	7,856	14,000	40
	SLH-DSA 128f	✅	32	17,088	720	110
	LMS M4_H20_W8	✅	48	1,112	2.9 !	8.4
Lattices	Falcon 512	📝	897	666	3 !	0.7
Codebased	CROSS R-SDP(G)1 small	🤔	38	7,956	20	35
	LESS 1s	🤔	97,484	5,120	620	1800
MPC in the head	Mirath Mirith Ia fast	🤔	129	7,877	25	60
	MQOM L1-gf251-fast	🤔	59	7,850	35	85
	PERK I-fast5	🤔	240	8,030	20	40
	RYDE 128F	🤔	86	7,446	15	40
	SDitH gf251-L1-hyp	🤔	132	8,496	30	80
VOLE in the head	FAEST EM-128f	🤔	32	5,696	6	18
Lattices	HAWK 512	🤔	1,024	555	0.25	1.2
Isogeny	SQISign I	🤔	64	177	17,000	900
Multivariate	MAYO one	🤔	1,168	321	1.4	1.4
	MAYO two	🤔	5,488	180	1.7	0.8
	QR-UOV I-(31,165,60,3)	🤔	23,657	157	75	125
	SNOVA (24,5,4)	🤔	1,016	248	0.9	1.4
	SNOVA (25,8,3)	🤔	2,320	165	0.9	1.8
	SNOVA (37,17,2)	🤔	9,842	106	1	1.2
	UOV Is-pkc	🤔	66,576	96	0.3	2.3
	UOV Ip-pkc	🤔	43,576	128	0.3	0.8

Legend

- 🤔 candidates that progressed
- ❌ classical algorithms vulnerable to quantum attack
- ✅ post-quantum algorithms that are already standardized
- 📝 post-quantum algorithms that are soon to be standardized

Discussion on algorithms deprecation

- Future of RSA-2048:
  - In the current standard (NIST SP800-57)
    - It is disallowed from 2031
  - In the new (draft) standard:
    - It is deprecated from 2030
    - It is disallowed from 2035
- **NIST may be not the only applicable standard in some countries!**
  - In Europe, SOG-IS and ETSI TS 119: RSA with keys smaller than 3000 bits are going to be disallowed in 2026

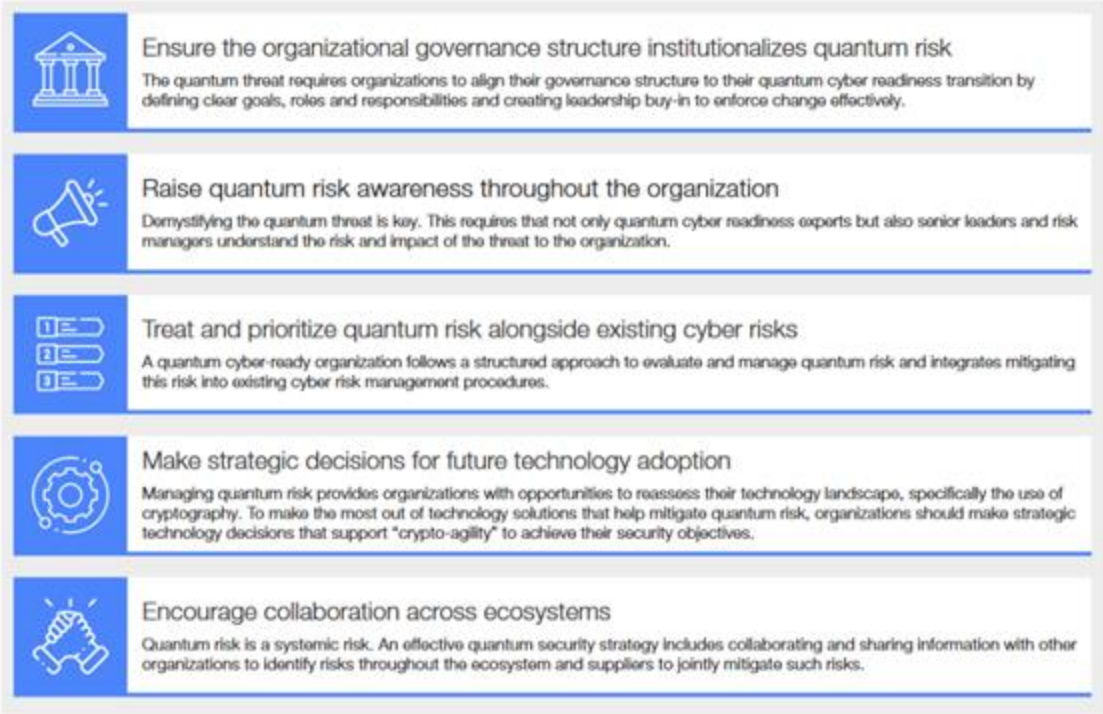
https://www.linkedin.com/posts/itanbarmes_cryptography-pqc-activity-7264393667069591553-oUlQ/?utm_source=share&utm_medium=member_android

NIST SP800-57: https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final

SOG-IS: https://www.sogis.eu/uk/supporting_doc_en.html

ETSI TS 119: https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.04.03_60/ts_119312v010403p.pdf

Why the new NIST standards mean quantum cryptography may just have come of age



https://www.weforum.org/stories/2024/10/quantum-cryptography-nist-standards/

QUBIP

Quantum-oriented Update to Browsers and Infrastructure for the PQ Transition

CONTACTS

Molteni Maria Chiara

Security Pattern

m.molteni@securitypattern.com

https://qubip.eu

The QUBIP project is funded by the European Union under the Horizon Europe framework programme [Grant Agreement No. 101119746]