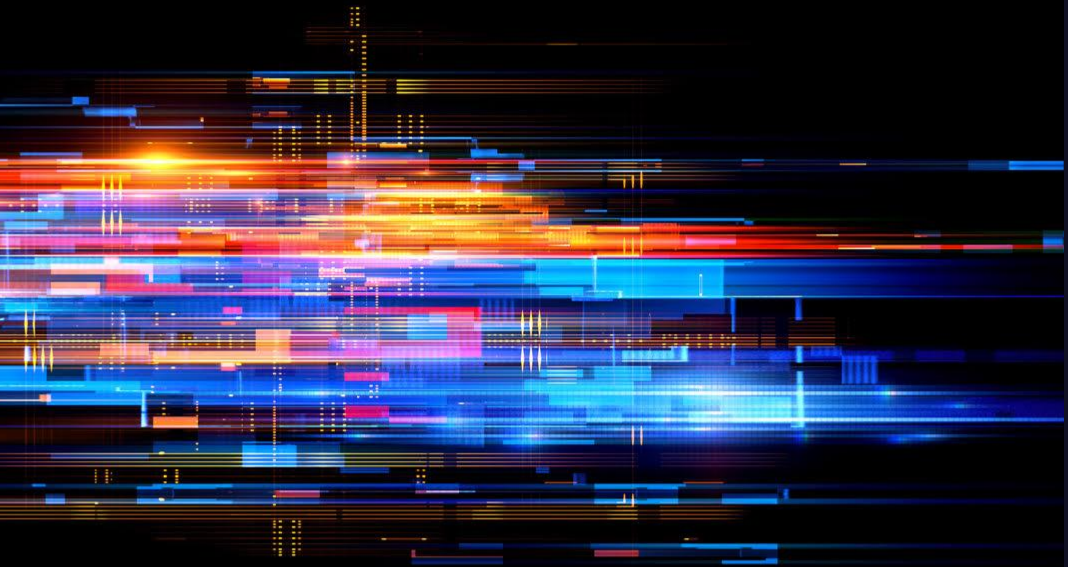


SANDBOXAQ™

Status Report on the NIST PQC Standardisation

Carlos Aguilar Melchor
carlos@sandboxaq.com

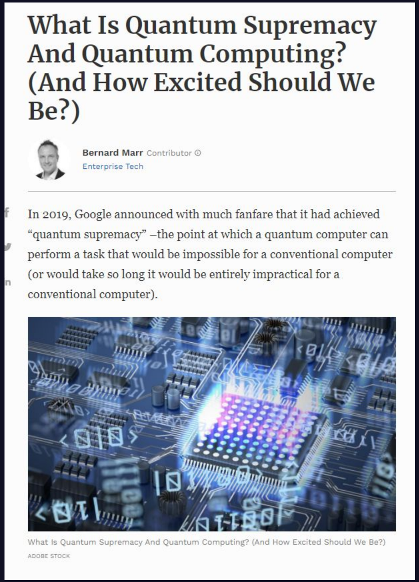
Status report on the NIST Post-Quantum Standardization

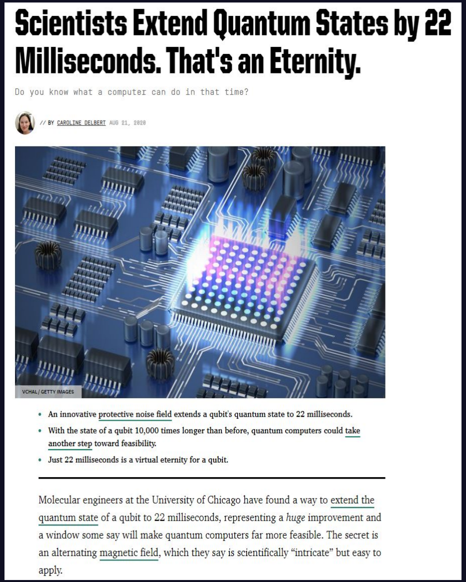
Carlos Aguilar Melchor
carlos@sandboxaq.com

The Quantum Threat
(or why a crypto migration is needed)

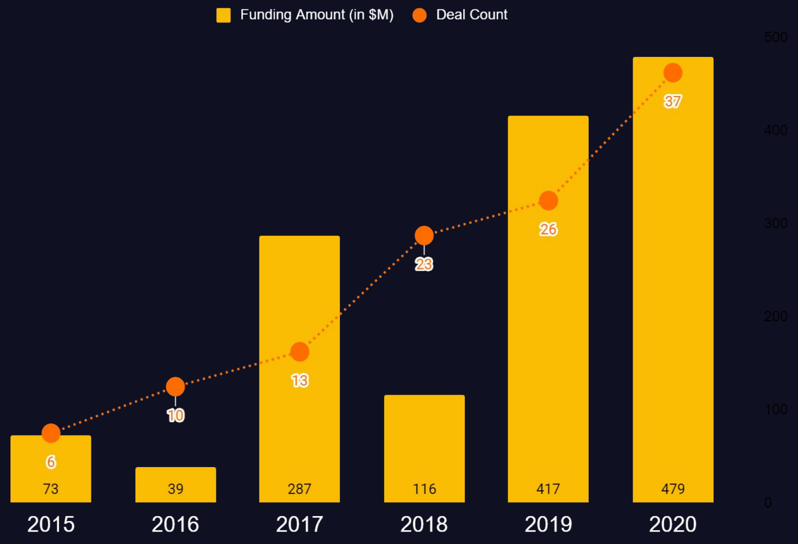
Quantum Computers Are Coming

Quantum computing is becoming a reality...



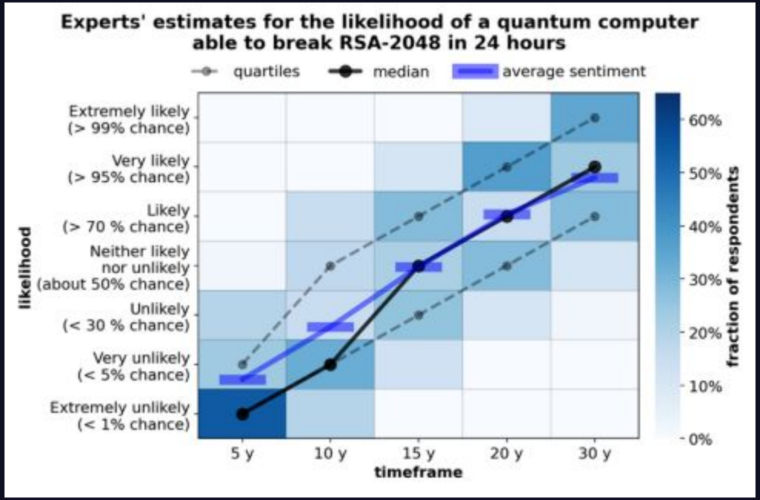


… and growing amount of funding will continue to foster new discoveries



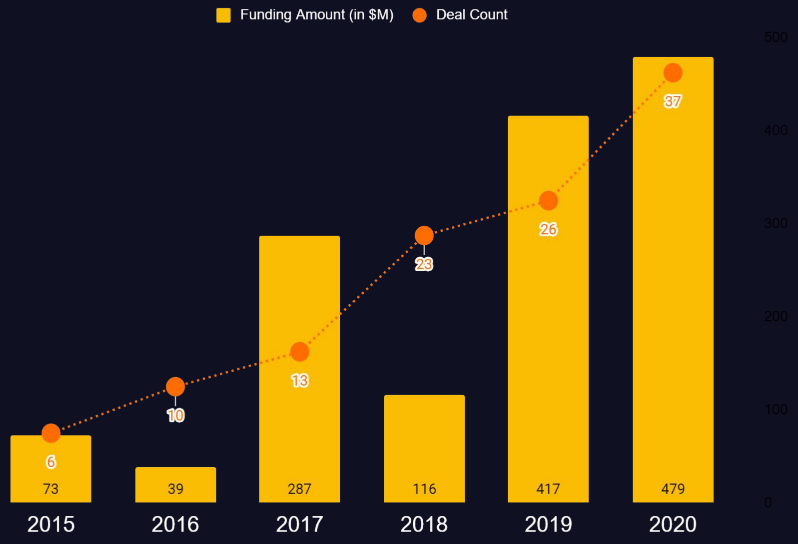
Quantum Computers Are Coming

Quantum computing is becoming a reality...

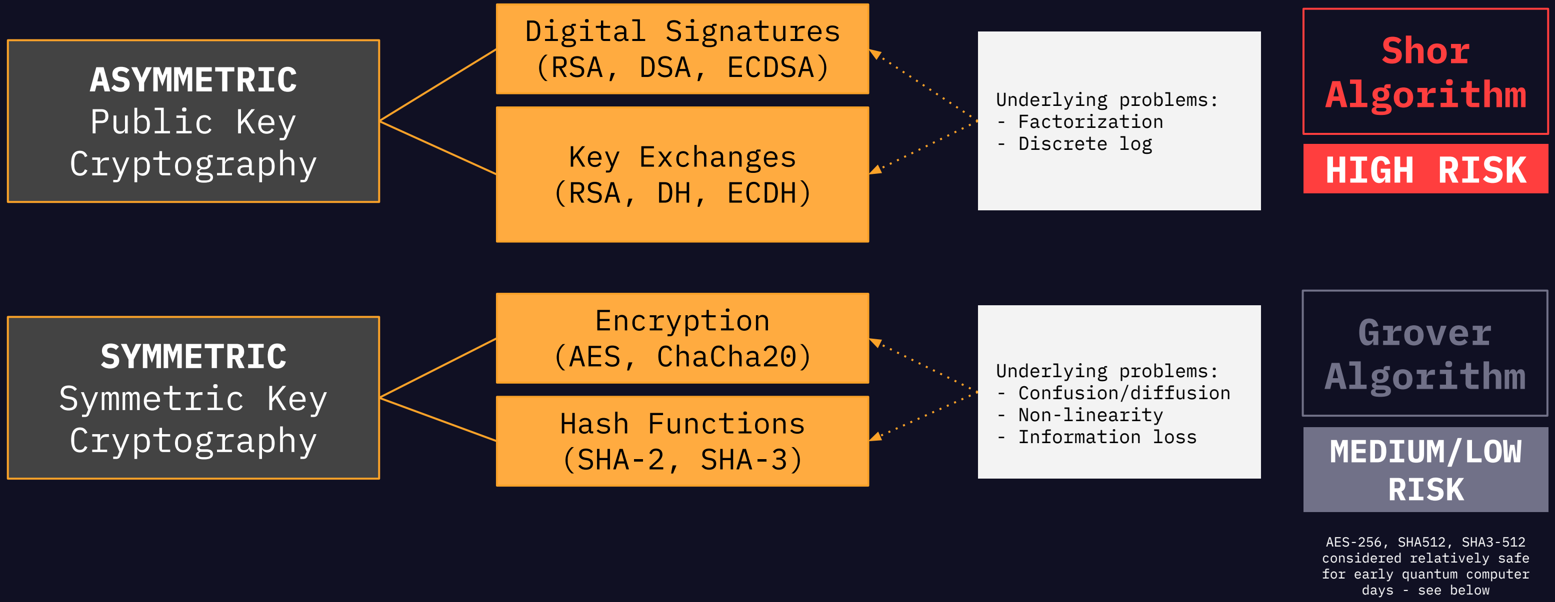


Global Risk Institute 2021 Quantum Threat Timeline Report
https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

... and growing amount of funding will continue to foster new discoveries



Digital Security Is Challenged



Long-Term Attacks
(or why the time to act is now)

Store Now Decrypt Later (SNDL)

Enterprises must migrate <u>now</u> to post-quantum (i.e. quantum-resistant) crypto as their data is being exfiltrated <u>now</u> for decryption later

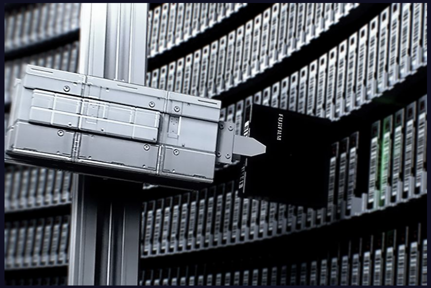
Today

Sensitive data could still be valuable years from now and will be exposed by QC if not secured by PQC

Storage

Tomorrow

Companies and networks need to act today to secure their data and prevent the following actions.



Retrieval

+

Quantum processing

=

Decrypted message

Long-Life Field Devices

Need for a long-term secure alternative

Many vehicles use crypto hardware with multi-decade lifespans

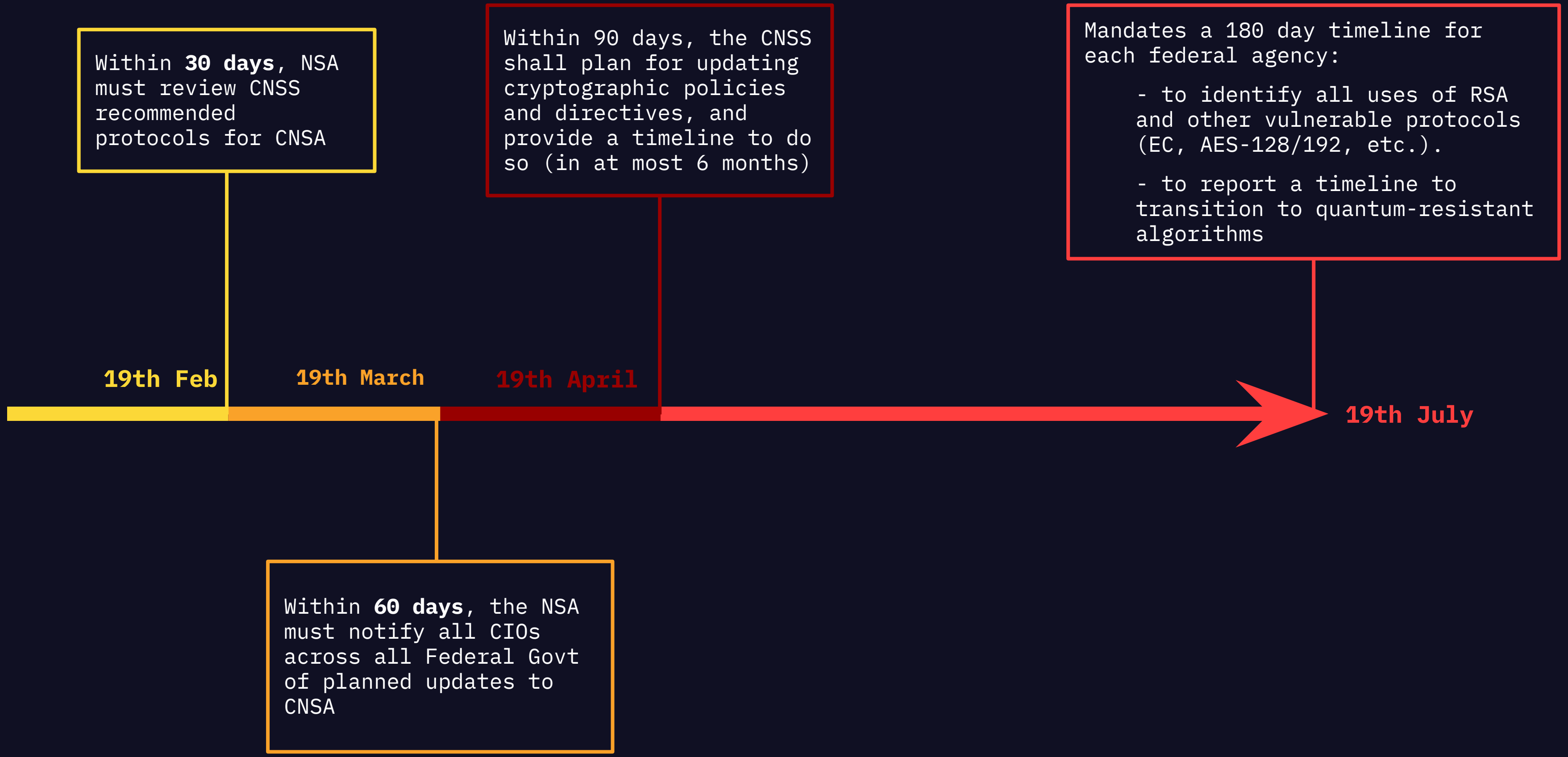
Many industrial control system plants cannot regularly update crypto due to high availability requirements

NSA

> “ For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure to do so at this point but instead to **prepare for the upcoming quantum resistant algorithm transition**.

National Security Memo (NSM) January 2022

The NSM provides a clear set of milestones for migration to post-quantum crypto



Standardisation Landscape

Current Standards

There are different Standardization organizations:

- **NIST – US**
- **ISO – Global**
- **ANSSI – France**
- **BSI – Germany**
- **NCSC – UK**
- ***"IETF"* (through RFCs) – Global**

Digital Signatures (**FIPS-186**):

- DSA
- RSA
- ECDSA

Key Agreement (**SP 800-56A** and **SP 800-56B**):

- ECDH
- RSA

All based on **Factorization** or **Discrete logarithm** problems

NIST PQC Standardization Process

Submissions	Accepted R1	Accepted R2	Accepted R3	Standardized
82	69	26	15	Suite of Algorithms

Apr 2016: NISTIR 8105 Report

Dec 2016: Formal Call for Proposal

Nov 2017: Deadline for Submissions

Dec 2017: 1st Round Candidates Announced

Apr 2018: 1st NIST PQC Standardization Workshop

Jan 2019: 2nd Round Candidates Announced

Aug 2019: 2nd NIST PQC Standardization Workshop

July 2020: 3rd Round Schemes Announced

Q2/Q3 2021: 3rd NIST PQC Standardization Workshop

March 2022: First standards defined and 4th round schemes announced

2022/2023: New Standardization Process for more Digital Signatures

Post-Quantum Cryptography runs on current digital systems

You don’t need a quantum computer.

New standards are to be chosen

	Lattice-based		Hash-based		Code-based		Multivariate Quadratic-based		Isogeny-based	
	PKE	Signature	PKE	Signature	PKE	Signature	PKE	Signature	PKE	Signature
Application	x	x	-	x	x	-	-	x	x	x
Pros	• Fast (thousands ops/s) • Small sizes (KX 1.5KB, Sign 3.5KB)		• Strong underlying problem • Small key size		• Strong underlying problem • OR small sizes (3KB-6KB)		• Tiny signature (66B)		• Tiny sizes (KX, Sign, 600B) • Easy implementation	
Cons	• Somewhat recent underlying problems		• Large signatures (8-18KB) • Slow (hundreds ops/s) • No KX		• Huge key size (260KB) • OR recent underlying problem • (No signatures)		• Huge key size (160KB) • Problem attacked several times • No KX		• Very slow computation (1 op/s) • Very recent underlying problem	

KX cost: All communications (keys + ciphertexts)
Sign cost: Public key + signature

NIST PQC Standardization Process

Round 3

2022 Finalists

Signatures :

- CRYSTALS-DILITHIUM (lattices)
- FALCON (lattices)
- Rainbow (multivariate)

Public Key Encryption / Key Encapsulation Mechanism:

- Classic McEliece (codes)
- CRYSTALS-KYBER (lattices)
- NTRU (lattices)
- SABER (lattices)

2023 Finalists (aka Alternates)

Signatures :

- GeMSS (multivariate)
- Picnic (symmetric)
- SPHINCS+ (symmetric)

Public Key Encryption / Key Encapsulation Mechanism:

- BIKE (codes)
- FrodoKEM (lattices)
- HQC (codes)
- NTRU Prime (lattices)
- SIKE (isogenies)

NIST PQC Standardization Process

Round 3

Rainbow has been recently attacked and most probably will be left out of the process

Breaking Rainbow Takes a Weekend on a Laptop

Ward Beullens

IBM Research, Zurich, Switzerland
wbe@zurich.ibm.com

Abstract. This work introduces new key recovery attacks against the Rainbow signature scheme, which is one of the three finalist signature schemes still in the NIST Post-Quantum Cryptography standardization project. The new attacks outperform previously known attacks for all the parameter sets submitted to NIST and make a key-recovery practical for the SL 1 parameters. Concretely, given a Rainbow public key for the SL 1 parameters of the second-round submission, our attack returns the corresponding secret key after on average 53 hours (one weekend) of computation time on a standard laptop.

2022 Finalists

Signatures :

- CRYSTALS-DILITHIUM (lattices)
- FALCON (lattices)
- ~~Rainbow (multivariate)~~

Public Key Encryption / Key Encapsulation Mechanism:

- Classic McEliece (codes)
- CRYSTALS-KYBER (lattices)
- NTRU (lattices)
- SABER (lattices)

2023 Finalists (aka Alternates)

Signatures :

- GeMSS (multivariate)
- Picnic (symmetric)
- SPHINCS+ (symmetric)

Public Key Encryption / Key Encapsulation Mechanism:

- BIKE (codes)
- FrodoKEM (lattices)
- HQC (codes)
- NTRU Prime (lattices)
- SIKE (isogenies)

NIST – June 2021

- First PQC standards will be announced at the end of 2021 / beginning of 2022
- We expect the final standards to be ready by 2024
- A new Digital Signature standardization process will start at the end of 2021 / beginning of 2022

Existing PQC Standards

Stateful Hash-Based Signatures

- XMSS-MT – RFC 8391 and SP 800-208 and ISO in process
- LMS – RFC 8554 and SP 800-208 and ISO in process

Can start being deployed now →

Software updates

Secure boot

PKI's CAs and RAs

China and Post-Quantum Cryptography

- Ran a PQC Competition in 2019
- Organized by the Chinese Association for Cryptologic Research
- Lasted for 1 year
- Only proposals written fully in Chinese were accepted
- They received 36 submissions
- Selected several PQC winner algorithms →

附件 1

全国密码算法设计竞赛公钥算法评选结果

一等奖：Aigis-sig、LAC.PKE、 Aigis-enc

二等奖：LAC.KEX、SIAKE、SCloud、AKCN(原名 AKCN-MLWE)

三等奖：OKCN(原名 SKCN-MLWE)、Fatseal、木兰、AKCN-E8、TALE、PKP-DSS、Piglet-1

- They *might* organize a second PQC competition in the near future

PQC-Related Standardisations
Hybrid Protocols

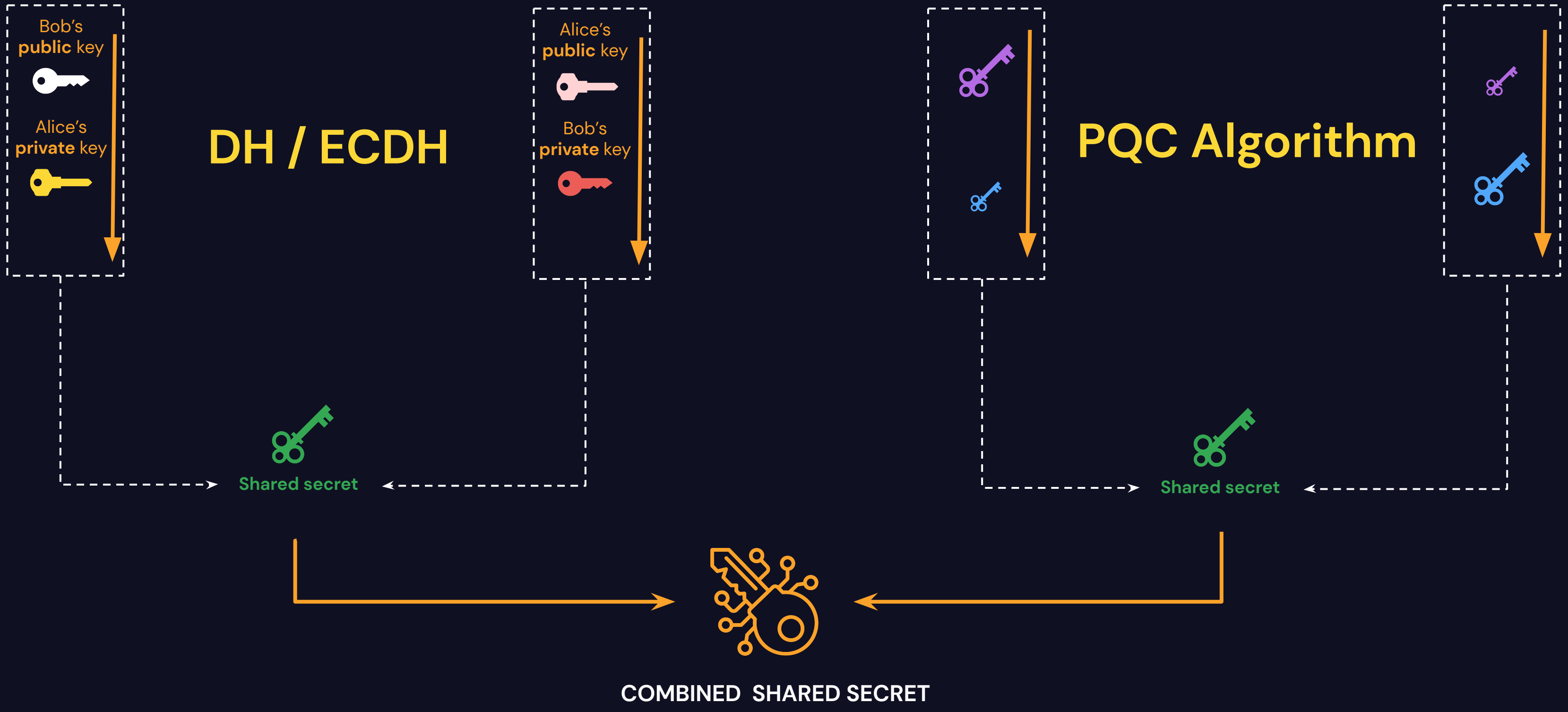
Hybrid protocols

2 Scope and Purpose

This Recommendation specifies two categories of key-derivation methods that can be employed, as required, to derive keying material from a shared secret Z generated during the execution of a key-establishment scheme specified in [SP 800-56A] or [SP 800-56B].

In addition to the currently **approved** techniques for the generation of the shared secret Z as specified in SP 800-56A and SP 800-56B, this Recommendation permits the use of a "hybrid" shared secret of the form $Z' = Z \| T$, a concatenation consisting of a "standard" shared secret Z that was generated during the execution of a key-establishment scheme (as currently specified in [SP 800-56A] or [SP 800-56B]) followed by an auxiliary shared secret T that has been generated using some other method. The content, format, length, and method used to generate T must be known and agreed upon by all parties that will rely upon the derived keying material, as well as by any agents trusted to act on their behalf. The key-derivation methods specified in this Recommendation will process a hybrid Z' in the same way they process a standard Z. Therefore, for simplicity of notation and exposition, any shared secret denoted by the symbol Z in the remainder of this

Complying with SP 800-56C



Toward Hybrid protocols

Network Working Group V. Smyslov
Internet-Draft ELVIS-PLUS
Intended status: Standards Track August 3, 2021
Expires: February 4, 2022

Intermediate Exchange in the IKEv2 Protocol
draft-ietf-ipsecme-ikev2-intermediate-07

Abstract

This documents defines a new exchange, called Intermediate Exchange, for the Internet Key Exchange protocol Version 2 (IKEv2). This exchange can be used for transferring large amount of data in the process of IKEv2 Security Association (SA) establishment. Introducing Intermediate Exchange allows re-using existing IKE fragmentation mechanism, that helps to avoid IP fragmentation of large IKE messages, but cannot be used in the initial IKEv2 exchange.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-

Post-quantum WireGuard

June 16, 2021

Andreas Hülsing, Eindhoven University of Technology, The Netherlands, andreas@huelsing.net
Kai-Chun Ning, KPN B.V., The Netherlands, kaichun.ning@kpn.com
Peter Schwabe, Max Planck Institute for Security and Privacy, Germany & Radboud University, The Netherlands, peter@cryptojedi.org
Florian Weber, Eindhoven University of Technology, The Netherlands, mail@florianjw.de
Philip R. Zimmermann, Delft University of Technology & KPN B.V., The Netherlands, prz@mit.edu

Abstract—In this paper we present PQ-WireGuard, a post-quantum variant of the handshake in the WireGuard VPN protocol (NDSS 2017). Unlike most previous work on post-quantum security for real-world protocols, this variant does not only consider post-quantum confidentiality (or forward secrecy)

not supported by other VPN software, e.g., identity hiding, and DoS-attack mitigation. The security considerations that lead to the design of WireGuard are laid out in [1]. Donenfeld and Milner give a computer-verified proof of the protocol in the

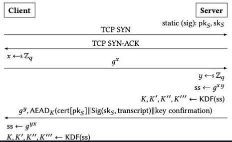
Post-Quantum TLS Without Handshake Signatures

Full version, April 21, 2021

Peter Schwabe, Max Planck Institute for Security and Privacy & Radboud University, peter@cryptojedi.org
Douglas Stebila, University of Waterloo, dstebila@uwaterloo.ca
Thom Wiggers, Radboud University, thom@thomwiggers.nl

ABSTRACT

We present KEMTLS, an alternative to the TLS 1.3 handshake that uses key-encapsulation mechanisms (KEMs) instead of signatures for server authentication. Among existing post-quantum candidates, signature schemes generally have larger public key/signature sizes compared to the public key/ciphertext sizes of KEMs: by using an IND-CCA-secure KEM for server authentication in post-quantum TLS, we obtain multiple benefits. A size-optimized post-quantum instantiation of KEMTLS requires less than half the bandwidth of a size-optimized post-quantum instantiation of TLS 1.3. In a speed-



Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH

Eric Crockett[1], Christian Paquin[2], and Douglas Stebila[3]
[1] *AWS* ericcro@amazon.com
[2] *Microsoft Research* cpaquin@microsoft.com
[3] *University of Waterloo* dstebila@uwaterloo.ca

July 19, 2019

Abstract

Once algorithms for quantum-resistant key exchange and digital signature schemes are selected by standards bodies, adoption of post-quantum cryptography will depend on progress in integrating those algorithms into standards for communication protocols and other parts of the IT infrastructure. In this paper, we explore how two major Internet security protocols,

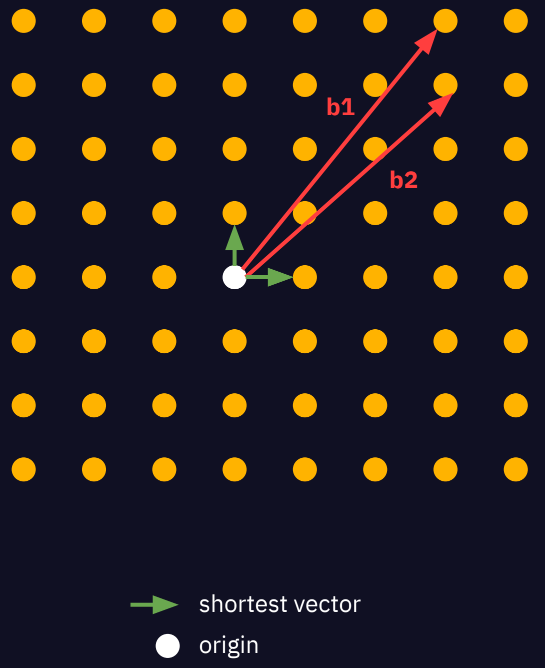
Post-Quantum Cryptography Domains

Quantum-Resistant Approaches

1. Lattice-based
2. Error-correction codes
3. Isogenies
4. Hash functions
5. Multivariate

Lattice-Based Cryptography

- LBC creates a *math workload problem* which is not tractable on either classical or quantum computers
- Setup a lattice geometry problem
  - Original geometry → Private key
  - Modified geometry → Public Key
- Not vulnerable to known quantum attacks
- Robustness to all possible quantum attacks yet to be determined.



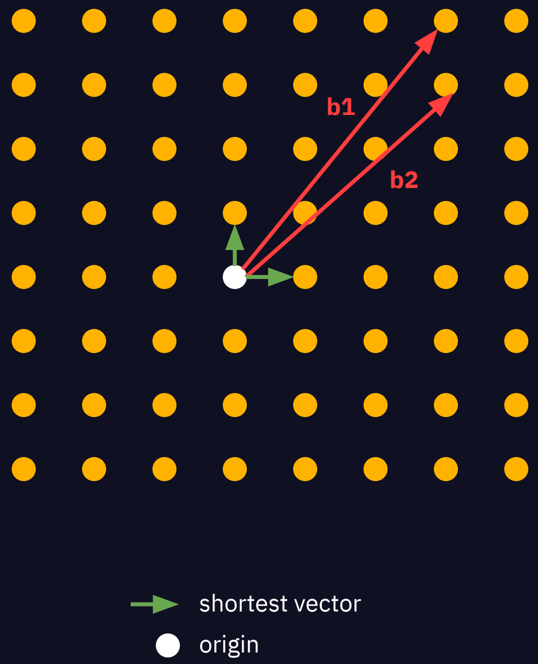
Lattice-Based Cryptography

Based on the hardness of the shortest vector problem (SVP) & analogous problems.

Most promising candidates:

Learning with Errors (LWE), *Module Learning with Errors* (MLWE) and *Ring Learning with Errors* (Ring LWE).

- **Pros:** Fast and relatively small key sizes
- **Con:** Less time out there being studied



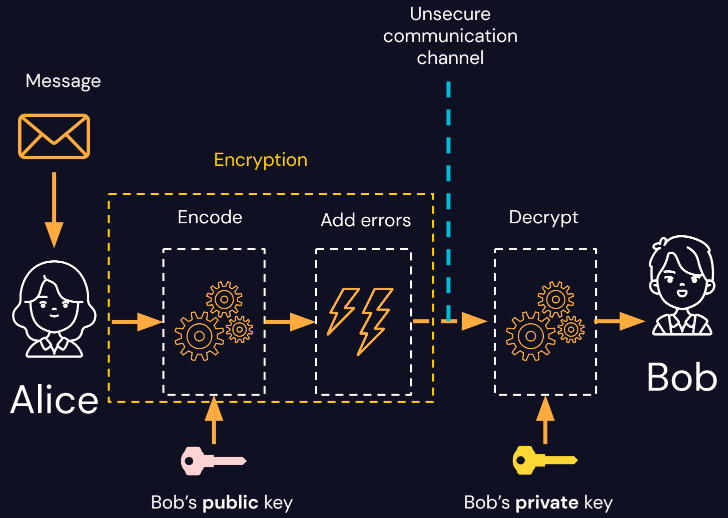
Code–Based Cryptography

Based on the hardness of decoding a linear code which has survived decades of cryptanalysis (*random* linear codes are known to be NP-hard)

Most promising candidate: *McEliece cryptosystem* (using binary Goppa codes)

Intuition: intentionally add errors in encryption so adversary cannot decode

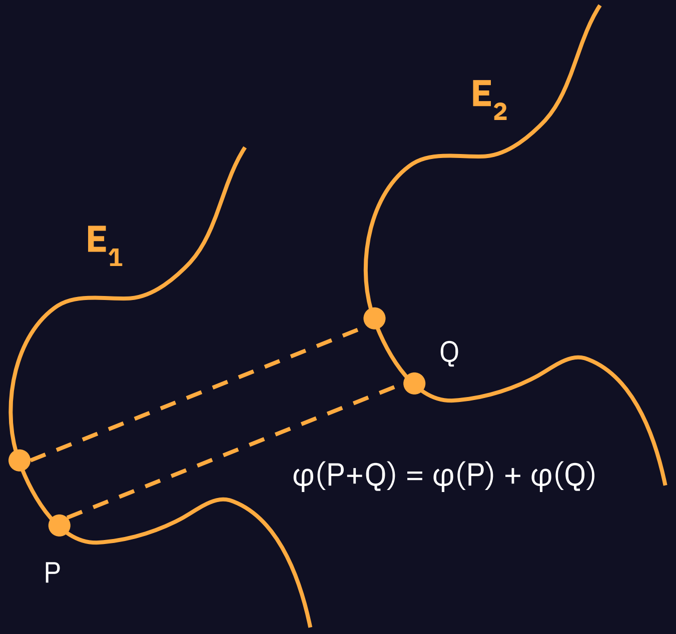
- **Pros:** Fast and small ciphertexts
- **Con:** Large keys



Isogeny-Based Cryptography

Based on the hardness of finding isogeny (mapping) between supersingular elliptic curves.

- **Pros**: Small key size, small ciphertext
- **Con**: Very slow



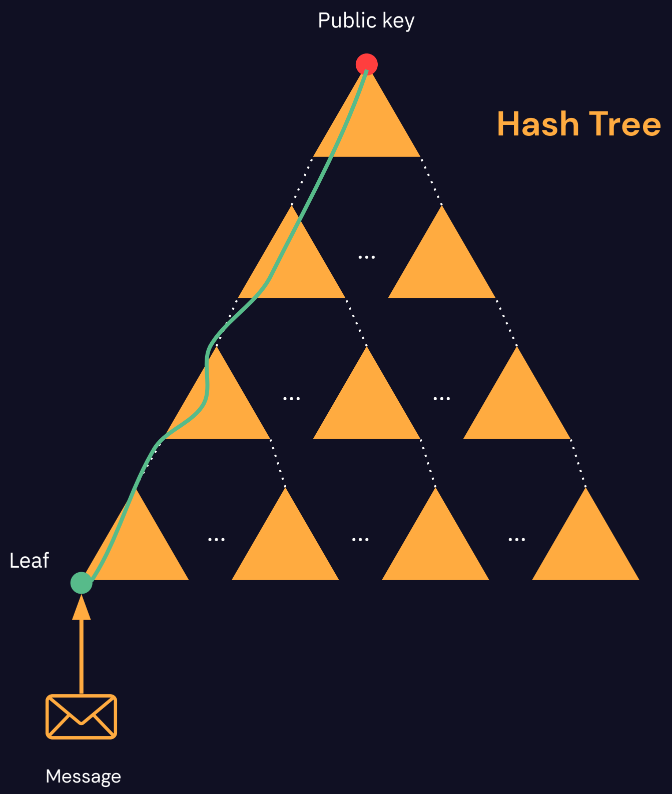
Hash-Based Cryptography

Based on security assumptions of one-way functions.

Popular choices:

- LMS, XMSS (eXtended Merkle Signature Scheme)
- SPHINCS+

- **Pros**: Secure, small keys
- **Con**: Slow and large signatures



Multivariate-Based Cryptography

Based on difficulty of solving systems of multivariate equations.

Promising candidates:

- *GeMSS*
- *Rainbow*

- **Pros:** Fast and short private keys
- **Con:** Long public keys

$$p^{(1)}(x1,\ldots xn) = \sum^{n}_{i=1}\sum^{n}_{j=1} p^{(1)}_{ij} \cdot x_i x_j + \sum^{n}_{i=1} p^{(1)}_{i} \cdot x_i + p^{(1)}_{0}$$

$$p^{(2)}(x1,\ldots xn) = \sum^{n}_{i=1}\sum^{n}_{j=1} p^{(2)}_{ij} \cdot x_i x_j + \sum^{n}_{i=1} p^{(2)}_{i} \cdot x_i + p^{(2)}_{0}$$

$$\ldots$$

$$p^{(m)}(x1,\ldots xn) = \sum^{n}_{i=1}\sum^{n}_{j=1} p^{(m)}_{ij} \cdot x_i x_j + \sum^{n}_{i=1} p^{(m)}_{i} \cdot x_i + p^{(m)}_{0}$$

System of multivariate quadratic (MQ) polynomials

Thank you!