@DEFCON 30

PQC in the Real World

James Howe
Senior Research Scientist

SANDBOXAQ™

CONTENTS

SANDBOXAQ™

01

A POST-QUANTUM CRYPTOGRAPHY PRIMER

QUANTUM ALGORITHMS: The good, the bad, and the ugly

	The good	The bad	The ugly
SHOR'S ALGORITHM	gives exponential speed-up for factoring integers.	requires quantum hardware, i.e. a LFT quantum computer.	combining these breaks current public-key standards.
GROVER'S ALGORITHM	gives quadratic speed-up for unstructured searching.	requires quantum hardware, i.e. a LFT quantum computer.	combining these means symmetric-key security is halved.

SANDBOXAQ™

New Public-Key Cryptography Standards

A method for establishing a shared key.

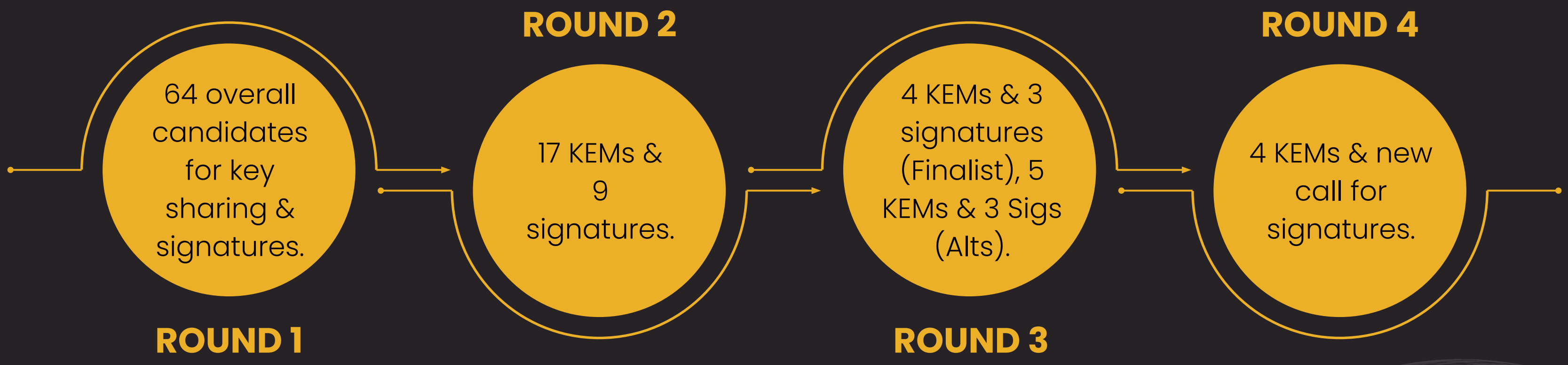
Basically, what we want is:

A method for authentication.

How is this being addressed?

Acted early due to "Store Now, Decrypt Later" and for Future-Proofing.

In 2016, NIST began its PQC standardization effort.



1st Standards: 1 KEM and 3 signatures.

Kyber (KEM) and Dilithium, Falcon, and SPHINCS+ (sigs).

NIST PQC Standardization Process

Submissions	Accepted R1	Accepted R2	Accepted R3	Accepted R4	Standardized
82	69	26	15	4	4

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

July 2022
Algorithms to standardize and 4th round schemes announced

Jan 2023
New Standard-ization Process for more Signatures.

SANDBOXAQ™

Other entities preparing for Quantum threat

Acted early due to “Store Now, Decrypt Later” and for Future-Proofing.

Other government standards bodies will or are likely to directly follow NIST.

Including BSI 🇩🇪, CCCS 🇨🇦, NCSC 🇬🇧, IETF 🗺️, ISO 🗺️, ITU 🗺️, etc.

ANSSI 🇫🇷 *“l’ANSSI est satisfaite du choix effectué par le NIST”.*

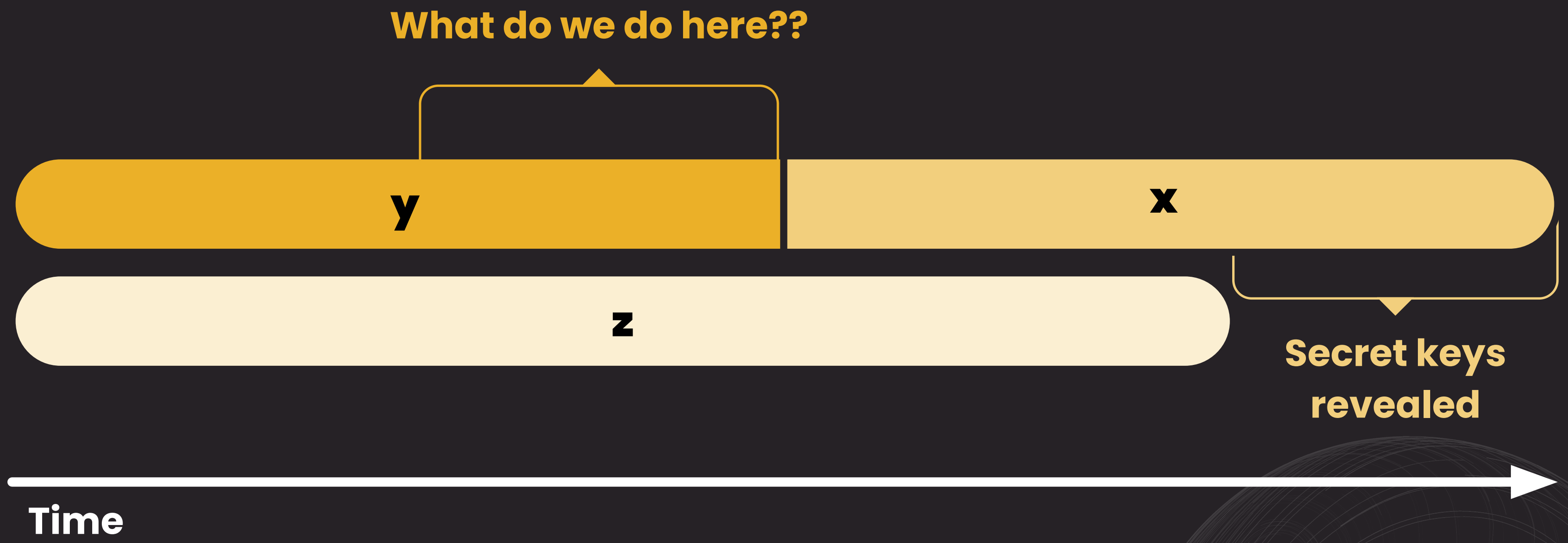
Some (BSI and ANSSI) even supporting ‘rejected’ candidates.

It’s worth noting that the CACR 🇨🇳 have their own PQC standards.

References:
https://www.ssi.gouv.fr/actualite/selection-par-le-nist-de-futurs-standards-en-cryptographie-post-quantique/
https://eprint.iacr.org/2021/462

Other entities preparing for Quantum threat

Theorem 1: If $x + y > z$, then worry.



References:
https://www.ssi.gouv.fr/actualite/selection-par-le-nist-de-futurs-standards-en-cryptographie-post-quantique/
https://eprint.iacr.org/2021/462

What are the PQC standards we have?

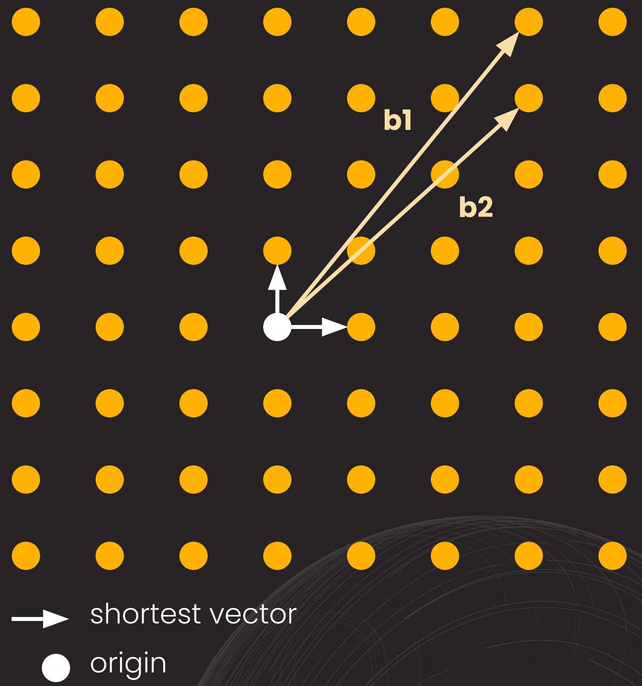
CRYSTALS-Kyber is the only KEM and CRYSTALS-Dilithium is the primary signature.

Both Kyber and Dilithium are ‘lattice-based’, a problem akin to:

Given **A** and **b**, where **b = A*s + e** mod q, find s.

Equivalent to finding short vector in a lattice.

They also significantly overlap codebases.

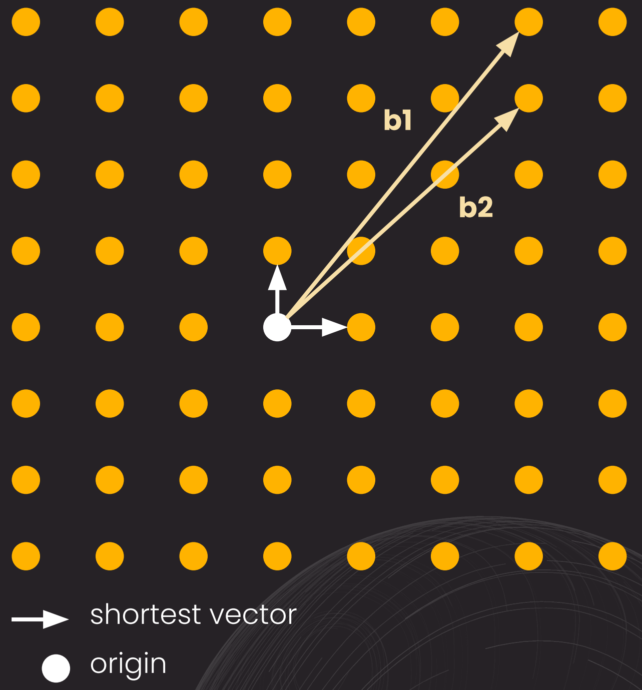


What are the PQC standards we have?

CRYSTALS-Kyber is the only KEM and CRYSTALS-Dilithium is the primary signature.

*"The security of **Kyber** has been thoroughly analyzed […] based on a strong framework of results in lattice-based cryptography. Kyber has excellent performance overall in software, hardware and many hybrid settings."*

"Dilithium is a signature scheme with high efficiency, relatively simple implementation, a strong theoretical security basis, and an encouraging cryptanalytic history."



SANDBOXAQ

What are the PQC standards we have?

We also have two other PQ signatures:

Falcon, lattice-based, different performance profile.

More complex design and implementati on.

Offers significantly smaller signature sizes and fast verificationn.

Falcon was chosen for standardization because NIST has confidence in its security (under the assumption that it is correctly implemented) and because its small bandwidth may be necessary in certain applications.

SANDBOXAQ

What are the PQC standards we have?

We also have two other PQ signatures:

SPHINCS+, a (stateless) hash-based scheme, provides diversity.

Signature scheme based on hardness of cryptographic hash functions.

"SPHINCS+ was selected for standardization because it provides a workable (albeit rather large and slow) signature scheme whose security seems quite solid and is based on an entirely different set of assumptions than those of our other signature schemes to be standardized.

Public Key, Signature, and Cipher Text Sizes

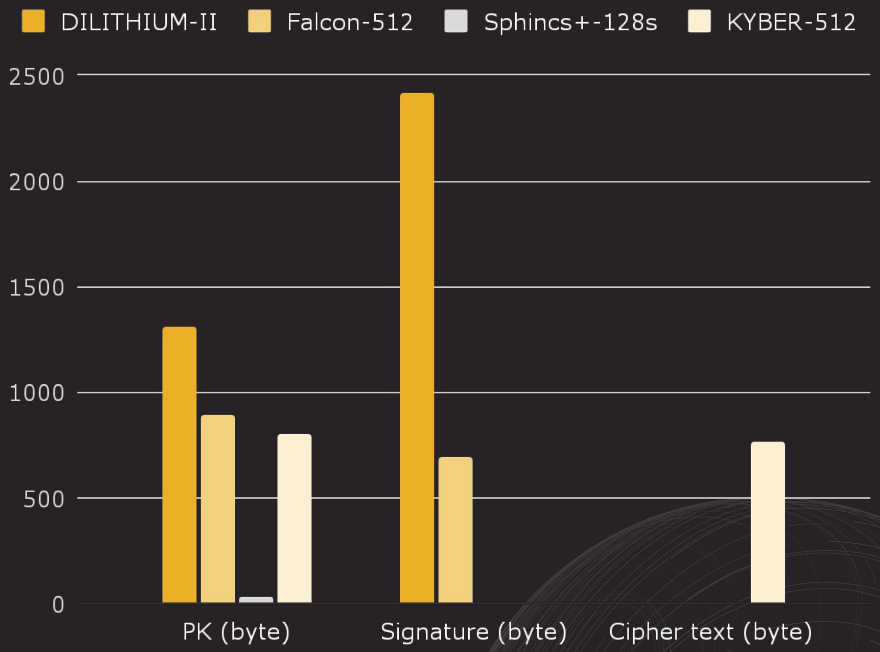
Kyber KEM is fast and reasonably small

On the signature side things aren't as nice

Sphincs+ is considered very secure but it is somewhat slow and signature size very large

Dilithium is very fast but still considered too large for some applications

Falcon is small but extremely complex and quite slower than Dilithium

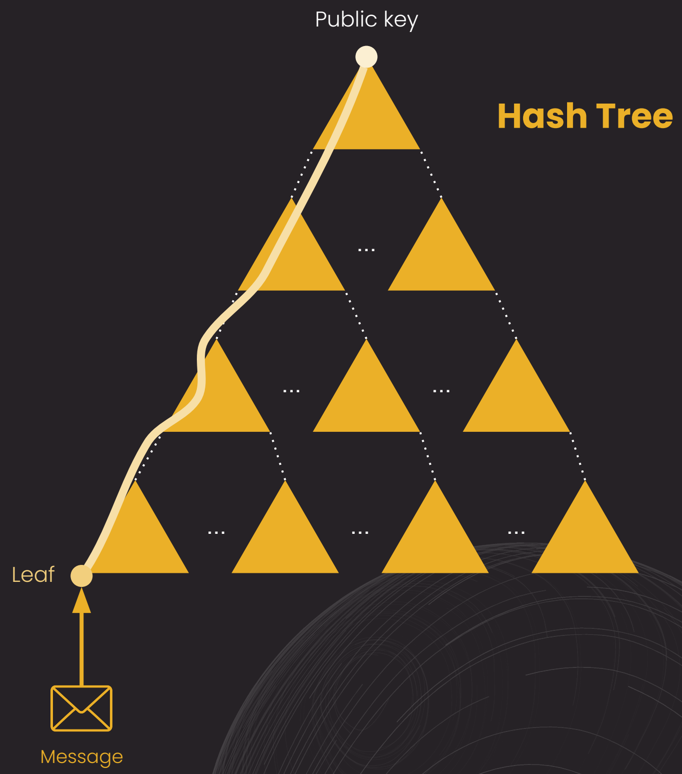


SANDBOXAQ

What are the PQC standards we have?

Stateful hash-based signatures also exist:

- Separate from the NIST PQC project.
- XMSS (IETF RFC 8391)
- LMS (IETF RFC 8554)
- Both adopted into NIST SP 80-208.
- Requires careful state management.
- Can sign limited number of messages.
- Is relatively slow compared to NIST PQC.



What are potential future PQC standards?

We have 4 KEMs remaining in Round 4:

- SIKE, isogeny-based, but was recently attacked.
- BIKE, HQC, & Classic McEliece, all code-based.
- NIST requested more scrutiny, may standardize later.

We also hope to see more signatures in the future:

- Lots of recent research on signatures using MPC-in-the-Head
- MPCitH paradigm is used in Picnic (a Round 3 candidate).
- Isogeny-based signatures also developing.

Recent attacks on NIST PQC candidates

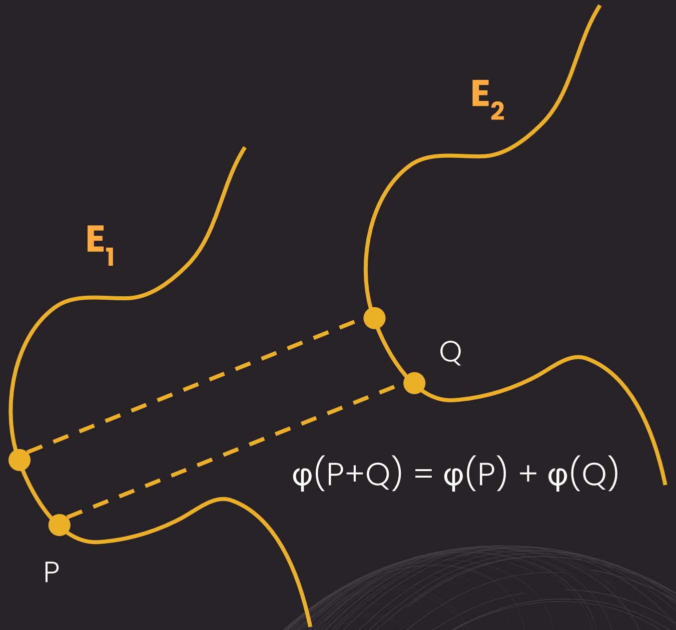
Supersingular isogeny-based KEM, SIKE.

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

The attack exploits the fact that SIDH has auxiliary points and that the degree of the secret isogeny is known.

Breaks NIST Level 1 security in 1 hour on 1 core.

Running Time	SIKEp64	SIKEp217	SKEp434	SIKEp503	SIKEp610	SIKEp751
Paper Implementation (Magma)	-	6 mininutes	62 mininutes	2h19m	8h15m	20h37m
Our implementation (SageMath)	5 seconds	2 mininutes	10 mininutes	15 mininutes	25 mininutes	1 – 2 hours



References:
https://ellipticnews.wordpress.com/2022/07/31/breaking-supersingular-isogeny-diffie-hellman-sidh/
https://eprint.iacr.org/2022/975
code available for the attack: https://homes.esat.kuleuven.be/~wcastryc/

Recent attacks on NIST PQC candidates

Rainbow 🌈, a multivariate signature scheme.

- Based on solving a set of random multivariate quadratic system is NP-hard.
- But a recent attack breaks/weakens it.
- Requires guessing a solution to a problem taking ~3.5 hours with probability ~1/15.
- Breaks NIST Level 1 parameters in "a weekend on a laptop".

$$p^{(1)}(x1,\dots xn) = \Sigma^n_{i=1}\Sigma^n_{j=1} p^{(1)}_{ij} \cdot x_i x_j + \Sigma^n_{i=1} p^{(1)}_i \cdot x_i + p^{(1)}_0$$

$$p^{(2)}(x1,\dots xn) = \Sigma^n_{i=1}\Sigma^n_{j=1} p^{(2)}_{ij} \cdot x_i x_j + \Sigma^n_{i=1} p^{(2)}_i \cdot x_i + p^{(2)}_0$$

...

$$p^{(m)}(x1,\dots xn) = \Sigma^n_{i=1}\Sigma^n_{j=1} p^{(m)}_{ij} \cdot x_i x_j + \Sigma^n_{i=1} p^{(m)}_i \cdot x_i + p^{(m)}_0$$

System of multivariate quadratic (MQ) polynomials

References:
https://eprint.iacr.org/2022/214
https://github.com/WardBeullens/BreakingRainbow

Recent attacks on NIST PQC candidates

What do these attacks mean?

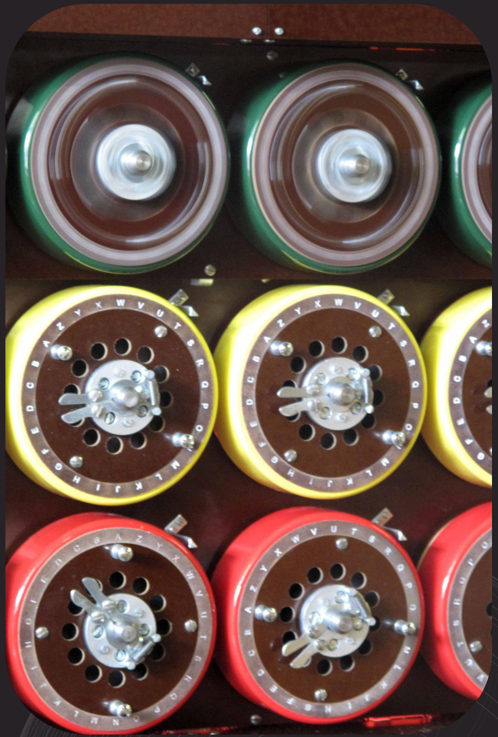
Both attacks were devastating for the candidates.

- Rainbow removed from NIST PQC process.
- SIKE unknown if a fix is possible.

Rainbow potentially made a finalist to attract more attention from the community for cryptanalysis.

These results show our checks are working.

Both problems were understudied before this.



PQC: A Plug-and-play solution?

Quantum threat against classical schemes

Uncertainty about PQC schemes

Classic schemes are unable to give more than a few years of confidentiality

PQC algorithms are new, and therefore some implementation or theoretical vulnerabilities may exist

How to choose between two dangerous alternatives?

Hybrid Algorithms

U.S Standard

e.g. RSA 2048

Additional KEM

e.g. PQC KEM

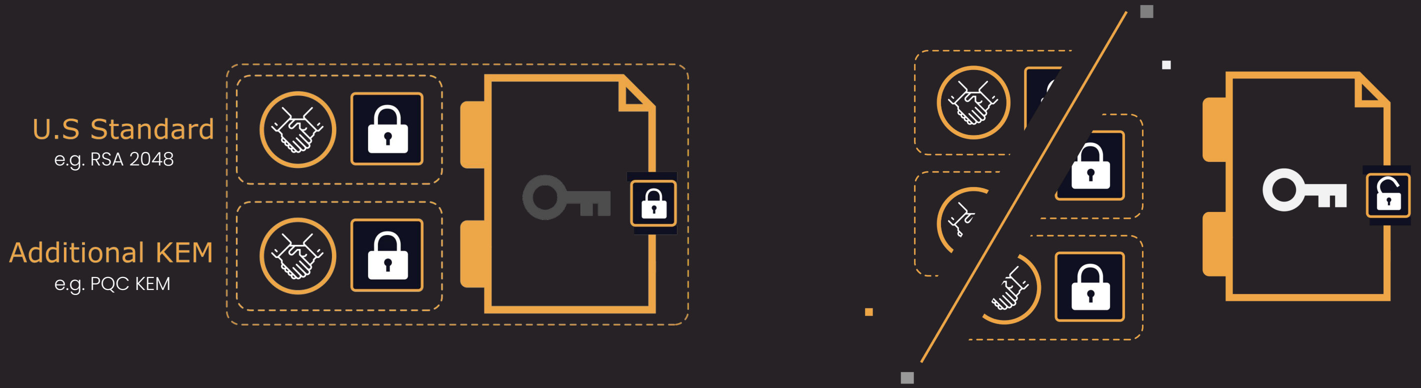
IDEA:

- Do two key exchanges to obtain two secrets.
- Combine both secrets to protect a common final secret (greyed key).

If one of the key exchanges is a US standard, the result is also compliant with US standards now
(no need to wait thanks to NIST SP 800-56C Rev2).

Hybrid Algorithms

Breaking one of the Key Exchanges is not enough to obtain the final (greyed) key.



To obtain the key the attacker needs to:

break the US Standard

this is **at least as secure** as the US Standard.

break the Additional KEM

it is a PQC KEM, this **resists to SNDL.**

SANDBOXAQ™

Using PQC with Current Standards

What is the hybrid mode approach?

NIST SP 800-56C permits a shared secret, Z, between two parties can be of the form Z′ = Z ǁ T.

We can use one (or more) PQC KEMs for T.

Need to break both KEMs to find the shared secret.

Standards: NIST SP 800-56C, IETF TLS 1.3 Hybrid

Most will use hybrid for the next few years.

Experiments: Google/Cloudflare CECPQ1 and CECPQ2,

Currently advocating hybrid: AWS KMS, Cloudflare, ETSI, ANSSI, etc.

Integrating PQC in the Real World

Will everyone use the hybrid mode approach?

NSA decided the national security strategy is "towards strictly-PQ solutions".

A Jan 2022 White House National Security Memo instructs agencies to prepare for a PQC transition:

> *"Within 180 days of the date of this memorandum, agencies shall implement multifactor authentication and encryption for NSS data-at-rest and data-in-transit.*

02

POST-QUANTUM CRYPTOGRAPHY IN THE REAL WORLD

Public Key Cryptography Algorithms Are Everywhere

Protect the Certificates (X.509)

X.509 certificates play a central role in the Information Security ecosystem of the Internet, as servers are authenticated to clients using X.509v3 certificates.

Protect VPN Tunnels

Internet Key Exchange (IKEv2) is a protocol used to establish keys and security associations for the purpose of setting up a secure VPN connection. Other well-known VPN protocols are WireGuard or OpenVPN.

Protect the web (TLS 1.3)

TLS is used to secure a variety of applications, including web traffic (the HTTP protocol), file transfer (FTP), and mail transport (SMTP).

Protect secure emails (S/MIME)

Secure/Multipurpose Internet Mail Extension is a standard for digital signatures and public-key encryption used to securely send email messages. It offers origin authentication non-repudiation, data integrity, and confidentiality through use of digital signatures and message encryption.

Protect remote login (SSH)

Secure Shell (SSH) is a secure remote-login protocol. It can be used for a variety of purposes, including the construction of cost-effective secure Wide Local Area Networks (WLAN), secure connectivity for cloud-based services, and essentially any other enterprise process that requires secure access to a server from a remote client.

...and they enable a wide variety of use cases

Encryption and authentication of endpoints devices

Any embedded technology connected to a broader network (computers, mobile phone, terminal, stores, etc.).

One can use an endpoint devices to penetrate a much larger network and cause irreversible damages.

Network Infrastructure Encryption

Network infrastructure encryption refers to the idea that as data moves throughout a network, the reliant network infrastructure must use cryptography.

Impact the Internet backbone over which much of the principal internet traffic travels between the Internet's many networks (HTTP/TLS), the encryption between linked enterprise data centers, and the encryption used to secure wide-area networks.

Big data & ML DB/SQL security

The rise of big data has fostered the gathering of information on user, sometimes very sensitive ones. As a result, the need for encrypting DB and data pull protocols (SQL, etc.) is stronger than ever.

Cloud storage and computing

Cloud works on remote access and is becoming prevalent in every companies in the world. Moving to PQ encryption is essential in particular because cloud storage is remotely accessed, requiring data to traverse a public network between the user and the cloud. The need for strong encryption is further amplified by the multitude of distinct and untrusted users sharing the infrastructure.

Supervisory Control & Data Acquisition systems

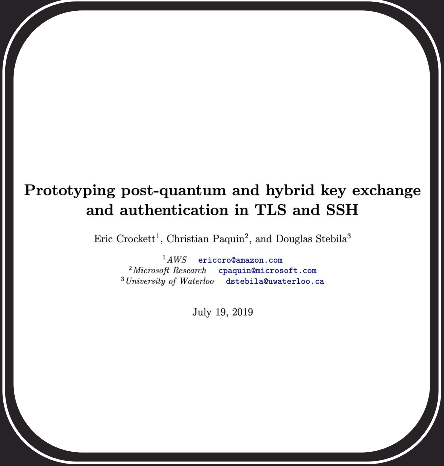
SCADA is a system of software and hardware elements that allows industrial organizations to:

- Control industrial processes locally or at remote locations.
- Monitor, gather, and process real-time data.
- Directly interact with devices such as sensors, valves, pumps, motors, and more through human-machine interface (HMI) software.
- Record events into a log file.

Attacks on SCADA systems can lead to the remote take-over of factories, oil pipes, electrical grids, airports, miningoperations, power supply, etc. (Stuxnet example).

SANDBOXAQ™

Towards a PQ-Secure Internet



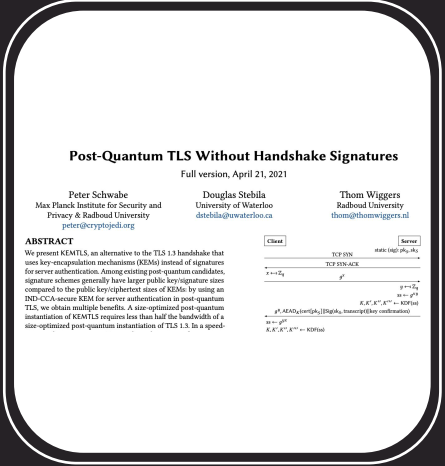
Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH

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

PQC have performance drawbacks.



Post-Quantum TLS Without Handshake Signatures

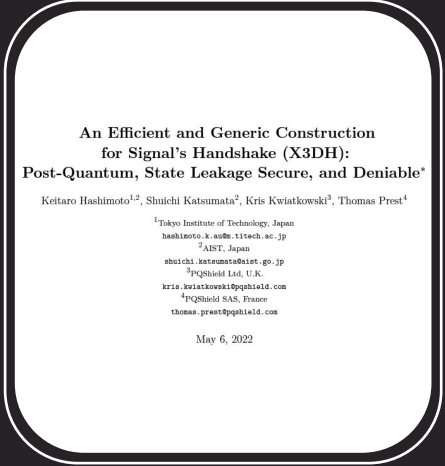
Full version, April 21, 2021

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-

Client
Server
static (sig): pk_S, sk_S
TCP SYN
TCP SYN-ACK
$x \leftarrow_s \mathbb{Z}_q$
g^x
$y \leftarrow_s \mathbb{Z}_q$
$ss \leftarrow g^{xy}$
$K, K', K'', K''' \leftarrow KDF(ss)$
g^y, $AEAD_K(cert[pk_S] \| Sig(sk_S, transcript) \| key\ confirmation)$
$ss \leftarrow g^{yx}$
$K, K', K'', K''' \leftarrow KDF(ss)$

Compared to elliptic-curve cryptography PQC is generally slower and larger.



An Efficient and Generic Construction for Signal's Handshake (X3DH): Post-Quantum, State Leakage Secure, and Deniable*

Keitaro Hashimoto[1,2], Shuichi Katsumata[2], Kris Kwiatkowski[3], Thomas Prest[4]

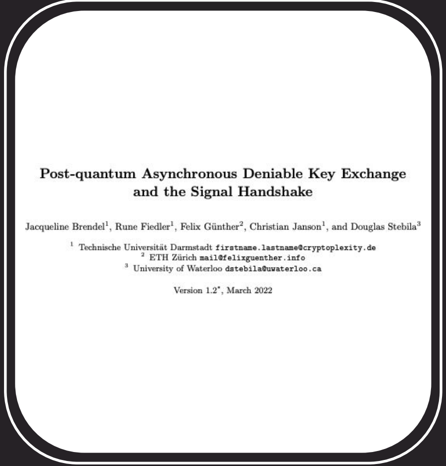
[1] Tokyo Institute of Technology, Japan
hashimoto.k.au@m.titech.ac.jp
[2] AIST, Japan
shuichi.katsumata@aist.go.jp
[3] PQShield Ltd, U.K.
kris.kwiatkowski@pqshield.com
[4] PQShield SAS, France
thomas.prest@pqshield.com

May 6, 2022

KEMs are not drop-ins for Diffie-Hellman.

KEMs inherently interactive.

Non-interactivity (NIKE) still unsolved.



Post-quantum Asynchronous Deniable Key Exchange and the Signal Handshake

Jacqueline Brendel[1], Rune Fiedler[1], Felix Günther[2], Christian Janson[1], and Douglas Stebila[3]

[1] Technische Universität Darmstadt firstname.lastname@cryptoplexity.de
[2] ETH Zürich mail@felixguenther.info
[3] University of Waterloo dstebila@uwaterloo.ca

Version 1.2*, March 2022

Non-interactive also critical in Signal's "double ratchet", PQCising this in progress.

SANDBOXAQ

Towards a PQ-Secure Internet

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.

IETF have RFC 9242 for "Intermediate Exchange" for IKEv2 to deal with the much larger keys in PQC KEMs.

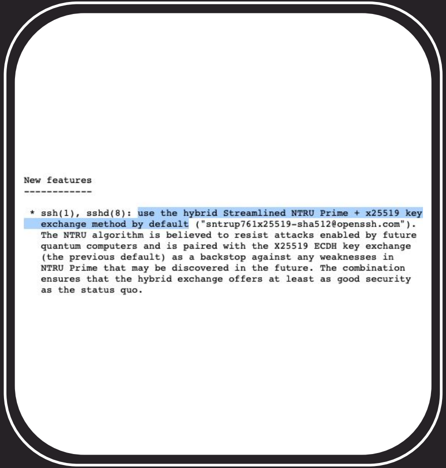
CURDLE P. Kampanakis
Internet-Draft Cisco Systems
Intended status: Experimental D. Stebila
Expires: 24 April 2021 University of Waterloo
M. Friedl
OpenSSH
T. Hansen
AWS
D. Sikeridis
University of New Mexico
21 October 2020

Post-quantum public key algorithms for the Secure Shell (SSH) protocol
draft-kampanakis-curdle-pq-ssh-00

Abstract

This document defines hybrid key exchange methods based on classical ECDH key exchange and post-quantum key encapsulation schemes. These methods are defined for use in the SSH Transport Layer Protocol. It also defines post-quantum public key authentication methods based on post-quantum signature schemes. These methods are defined for use in the SSH Authentication Protocol.

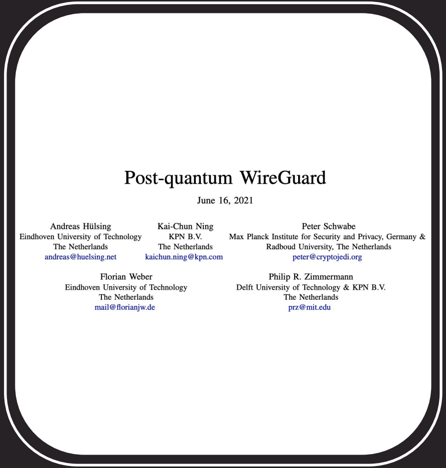
IETF have a working group on integrating PQC into the SSH Transport Layer Protocol.



New features
----

* ssh(1), sshd(8): use the hybrid Streamlined NTRU Prime + x25519 key exchange method by default ("sntrup761x25519-sha512@openssh.com"). The NTRU algorithm is believed to resist attacks enabled by future quantum computers and is paired with the X25519 ECDH key exchange (the previous default) as a backstop against any weaknesses in NTRU Prime that may be discovered in the future. The combination ensures that the hybrid exchange offers at least as good security as the status quo.

OpenSSH using NTRU Prime, a scheme not selected by NIST, with ECC as standard.



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

PQ-Wireguard / PQ-OpenVPN solutions.

Towards PQ-Secure Email

IETF working group on PQC in OpenPGP using hybrid.

- multi-algorithm KEM and signature (lattice-based)
- in Thunderbird (via RNP and Botan)
- in GnuPG / Libgcrypt.

PUBLIC KEY

IETF working group on S/MIME and PKIX;

- S/MIME: which is used in modern email software.
- PKIS: Internet standards to support X.509-based Public Key Infrastructures.
- X.509 being an ITU standard format for public-key certificates.

Current PQC Standards and Uses

We do have NIST approved signature schemes.

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**

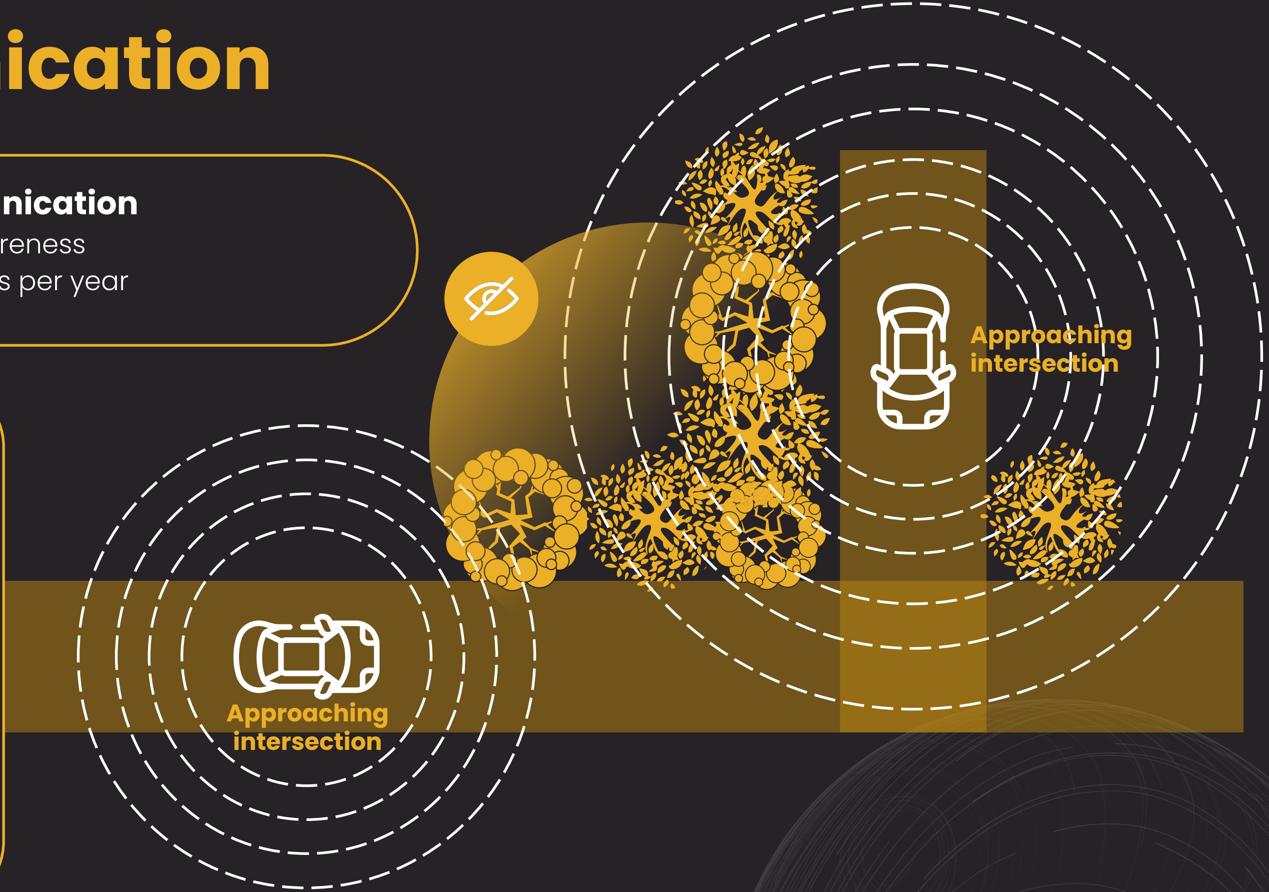
V2V Communication

Direct wireless communication

- Increases situational awareness
- Prevents 600,000 collisions per year

Described in

- Dedicated Short Range Communication/Wireless Access in Vehicular Environments
  IEEE 802.11p
- Cellular Vehicle-to-Everything
  3GPP Release 14/15



Future Wishlist of PQC Protocols

Non-Interactive Key Exchange (NIKE).

- ECDH gave us a lot of simplicity, we'd love that back.

DNSSEC: requires small signatures or small computations for verification.

The Noise protocol also uses Diffie-Hellman, PQNoise uses KEMs.

Post-quantum version of the QUIC network protocol?

Password Authenticated Key Exchange (PAKE).

- Most PAKE designs use Diffie-Hellman assumptions.
- Work replaces DH with KEMs, but can we get better performance.

Post-quantum also required for blockchains.

- 25% of all Bitcoin are potentially vulnerable to a quantum attack.
- How can we migrate an inherently distributed system?

Takeaways from this Talk

A few other things to consider emphasizing:

01 Design with cryptographic agility in mind.

02 Beware "snake oil cryptography": follow what NIST and other reputable standards bodies are doing

03 All the other things that make cryptography complicated are still there: key management, secure implementations (Hertzbleed), side-channels.

04 Cryptanalysis and attacks are expected and positive.

05 It will take time for the community to rebuild all of these with PQ algorithms.

06 There's the long path from research to standardization to deployment.

SANDBOXAQ™

THANK YOU