PONE
BIOMETRICS

POST-QUANTUM CRYPTOGRAPHY

Be ready for a new era of cryptography

A WHITE PAPER BY PONE BIOMETRICS

Executive Summary

Cryptography is used for all secure digital communications. However, the recent development of quantum computing is an emerging threat against the security landscape of today, possibly breaking all protocols relying on public key cryptography. New standards for post-quantum cryptography will soon be available, and it is important to prepare for the transition already today. PONE Biometrics will offer post-quantum signatures for secure FIDO authentication.

Cryptography Today

Everyone uses cryptography every day; whenever we connect to a website, sign a bank transaction, use our credit card, or send a message to our loved ones. A cryptographic protocol is then running in the background to ensure the authenticity, integrity, and confidentiality of our interactions.

We usually divide cryptography into two categories:

- asymmetric (or public) key cryptography and
- symmetric (or secret) key cryptography.

The former setting assumes that each party has their own public-private key pair, where the public key is made available to everyone else, while the latter assumes that the communicating parties already have a shared secret key in possession.

In the asymmetric key setting, each party creates their own key pair, shares the public key with the world, and keeps the private key protected. It is then crucial that an adversary cannot deduce the private key from the public key. The two most common categories of asymmetric schemes are based on the factoring and the discrete logarithm assumptions. The former says that given a large integer n, which is the product of two distinct prime numbers p and q, it is hard to find these prime factors. This assumption is the basis of the RSA encryption and signature schemes. The latter says that given a base g and some element y, both in a suitable group G, it is hard to find an exponent x such that $g^x = y$, or rather, finding the discrete logarithm $x = \log_g y$. This assumption is the basis of the Diffie-Hellman (DH) key exchange and the Digital Signature Algorithm (DSA), where the operations usually are computed over finite fields (all integers modulo some prime number) or elliptic curves.

In the symmetric setting, we assume that the parties already have a shared key, either obtained by in-person communication, sent using a currier, or, most commonly, agreed upon using the Diffie-Hellman key exchange mentioned above. It is then possible to use this key to encrypt messages using the Advanced Encryption Standard (AES) or ensure the integrity of a message using a message authentication code such as HMAC. Symmetric key cryptography is generally much more efficient than asymmetric key cryptography and is the preferred method when a shared key is already established.

Some of the most used protocols today are the Transport Layer Security (TLS, also called SSL) protocol for secure web communications, the Signal protocol (used in the Signal app in addition to WhatsApp and Messenger), and the FIDO protocol for secure authentication. The two former use the DH key exchange to agree upon a shared key and then continue using AES for all communication, while the latter uses digital signatures (only) to authenticate users in a secure and password-less manner.

The Threats of Quantum Computing

Quantum computing was introduced as a theoretical idea in the 1980s and has gained enormous attention since, with governments and private companies spending billions of dollars every year to build larger and more powerful quantum computers. The current state of the art is roughly 50 logical qubits.

Two quantum algorithms impact the security of the mentioned cryptographic schemes. The first is Grover's algorithm, which in theory allows a quantum computer to find the unknown input to a function given the output much faster than trying all possible inputs. The algorithm gives a square root speed up, meaning it can find a 128-bit AES key using 264 attempts instead of 2128. This can be solved by using 256-bit AES keys instead, which are already standardized and commonly used today. This upgrade has a low cost. However, researchers have analyzed Grover's algorithm and found that the practical cost of running the algorithm is much higher than the theoretical estimates, indicating that 128-bit AES keys are secure as used today.

The more severe threat is Shor's algorithm, a much more efficient algorithm than Grover's, which can be used for period finding – a problem related to both integer factoring and discrete logarithm computations. This algorithm can potentially break all public key cryptography schemes used today. While there is no quantum computer large enough to run Shor's algorithm on the parameters we use for secure communication today, we still need to replace our cryptographic algorithms and update our systems shortly.

The reasons are:

1) it will likely not be public information when the first large-scale quantum computer is available to a nation-state adversary,
2) it takes time to develop, analyze, and implement new cryptographic algorithms, and
3) nation-state adversaries are storing our encrypted information today in the hope that they will be able to break it later.

These are serious concerns.

While the third point describes confidentiality issues, the effect of the first point might be that an adversary can break a digital signature scheme, allowing them to insert backdoors and provide full access to all our software systems.

Post-Quantum Cryptography

Researchers have investigated these problems for a while, and post-quantum (or quantum-safe) cryptography has been an active field for two decades. Post-quantum cryptography is a set of cryptographic algorithms built on hardness problems that we believe no quantum computer can break, replacing the integer factorization and discrete logarithm problems used today.

It is important to note that post-quantum cryptography will be implemented on computers we use today, in contrast to quantum cryptography, consisting of algorithms run by quantum computers. This document covers the former.

The National Institute of Technology and Standards (NIST) in the US invited everyone to an international process in 2016 to standardize new and quantum-secure cryptographic algorithms[1].

The process concluded in 2022 by choosing four algorithms for standardization, and the standards will be ready for use in 2024. NIST has indicated that they will standardize more algorithms in the future, promoting three initial key-encapsulation mechanism (KEM) submissions to an extra round of analysis before more algorithms are standardized, in addition to opening a new call for digital signature schemes.

NIST is standardizing the following schemes:

- CRYSTALS-Kyber (ML-KEM)
- CRYSTALS-Dilithium (ML-DSA)
- Falcon (FN-DSA)
- and SPHINCS+ (SLH-DSA).

The latter is based purely on hash functions, while the security of the three former relies on the following lattice-based problems: Learning with Errors (LWE), Short Integer Solution (SIS), and NTRU.

Kyber and Dilithium are considered main options.

Several other countries are standardizing post-quantum cryptography, and similarly to the NIST competitions for AES and Secure Hash Algorithm 3 (SHA-3), they are standardizing finalists from the NIST process. For example, the German Federal Office for Information Security (BSI) is standardizing the lattice-based FrodoKEM and code-based Classic McEliece KEMs[2], and the French Cybersecurity Agency (ANSSI) is standardizing FrodoKEM, in addition to the NIST standard mentioned above[3].

When these algorithms are standardized, other organizations can upgrade their protocols, building on top of these algorithms, such as TLS, the Signal Protocol, and the FIDO protocol.

Since post-quantum cryptography is still relatively new, and one of the finalists was broken (SIKE, 2022) shortly before the decisions were made, it is important to have a pragmatic view on the security of the new schemes. A standard recommendation is so-called hybrid cryptography, where a classic algorithm is combined with a post-quantum algorithm to achieve the best of both worlds:

1) if a quantum computer breaks the classical algorithm, then the post-quantum algorithm offers protection, and
2) if the post-quantum algorithms had undiscovered vulnerabilities, then the classical algorithm still offer reasonable levels of security for a while into the future.

We will see many organizations combining ECDH and Kyber for key exchange and ECDSA and Dilithium for authentication over the coming year before classical algorithms are abandoned.

The National Security Agency (NSA) in the US has published a timeline for post-quantum mitigation for American organizations, requiring post-quantum software/firmware signing options today and as default and preferred from 2025. Other areas, such as web browsers and servers, traditional network equipment, operating systems, and other niche equipment, also need to offer post-quantum security over the coming few years, with exclusive use from 2030 or 2033, depending on application and use cases.

Recommendations

The timeline for mitigation to post-quantum cryptography depends on the content that needs to be secured; for example, it is more of a rush for governmental organizations than private citizens. However, everyone needs to analyze the cryptographic landscape today to be ready tomorrow.

The first and most crucial step is to get an overview of all cryptographic components: Which cryptographic algorithms are you using today? Which key sizes are used in each algorithm, and how are they stored? Which libraries are imported, and which services and applications rely on these? What is needed to update or replace the algorithms used?

Getting an overview of these factors will ease the transition later. Cryptographic agility is the critical factor in this stage. Hard-coded algorithms might be difficult to replace, while generic encryption or signature functionality in a library might be easy to update. We note that there is a need to buy new cryptographic hardware to accommodate the new algorithms since Hardware Security Modules (HSMs) and Secure Elements (SE) only support specific algorithms.

Furthermore, while the new post-quantum algorithms are reasonably fast, they lead to much larger keys, ciphertexts, and signatures than the algorithms that we use today. This might impact the transition phase, as some protocols have hard-coded packet sizes (such as TLS) or devices have memory constraints (IoT).

We have the following sizes, in Bytes, for classical and post-quantum schemes:

Key Exchange	RSA	DH	ECDH	Kyber
Secret Key [B]	768	32	32	1632
Public Key [B]	384	384	32	800
Ciphertext [B]	384	384	32	768

Signature Scheme	RSA	DSA	ECDSA
Signing Key [B]	768	32	32
Verification Key [B]	384	384	32
Signature [B]	384	416	64

Signature Scheme	Dilithium	Falcon	SPHINCS+
Signing Key [B]	2528	1281	64
Verification Key [B]	1312	897	32
Signature [B]	2420	666	7856

As described earlier, hybrid cryptography is a secure and conservative option to ensure future security without any risk of introducing new vulnerabilities. This depends on if the system can tolerate the performance loss of running two algorithms in parallel and has the flexibility to make this change.

While post-quantum mitigation might be a few years ahead, it is important to get ready today, to get an overview of existing algorithms and how much work it takes to update them, test new algorithms internally to understand what is required for the upgrade and make a detailed timeline for the transition.

OFFPAD Hybrid Signatures for FIDO

PONE Biometrics is already preparing for the quantum apocalypse. Today, the OFFPAD issues FIDO signatures using the ECDSA for secure authentication, where the ECDSA passkeys are stored securely in the secure element of the device. This ensures that no one can impersonate you online, as the passkey is phishing resistant since the key is never in the hands of the user, only publicly verifiable signatures are sent online, and the keys are unavailable even for an adversary that is able to get hold of the OFFPAD.

To protect our users against quantum adversaries, we have started a collaboration with the market-leading UK-based company PQShield, providing secure implementations of post-quantum algorithms. We have implemented their FIPS 140-3 ready PQCryptoLib Embedded library[5] on the MCU of the OFFPAD to provide hybrid ECDSA and Dilithium signatures for post-quantum secure FIDO authentication.

Since no secure element on the market today offers post-quantum signatures, this means that the Dilithium signature algorithm will be executed in untrusted hardware for now. The signing key will be securely stored at the MCU.

This means that we still offer phishing resistance, that the signatures sent online provide post-quantum security, and that an adversary stealing the OFFPAD card still needs to break the hardware security to get both keys, ensuring the best of both.

This ensures long-term secure authentication.

Conclusions

In conclusion, while quantum computers are not a threat today, they might be tomorrow, and it is crucial to be prepared. Post-quantum cryptography is about to get standardized, and it is important to plan the transition today.

PONE BIOMETRICS

References

[1] https://csrc.nist.gov/projects/post-quantum-cryptography
[2] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html?nn=916626
[3] https://cyber.gouv.fr/en/publications/anssi-views-post-quantum-cryptography-transition
[4] https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
[5] Further details and specifications can be found at https://pqshield.com/products/

Photo Credits

https://fr.freepik.com/photos-gratuite/resume-techno-low-poly-background-points-lignes-connexion-sombres_1174285.htm Image de kjpargeter sur Freepik

https://fr.freepik.com/photos-gratuite/vue-laterale-femme-plus-agee-focalisee-lunettes-travaillant-ordinateur-portable_9943241.htm Freepik

https://fr.freepik.com/photos-gratuite/concept-collage-html-css-pirate_36295469.htm Freepik

https://fr.freepik.com/photos-gratuite/gratte-ciel-futuristes-illuminent-horizon-ville-moderne-genere-par-ia_41481646.htm Image de vecstock sur Freepik