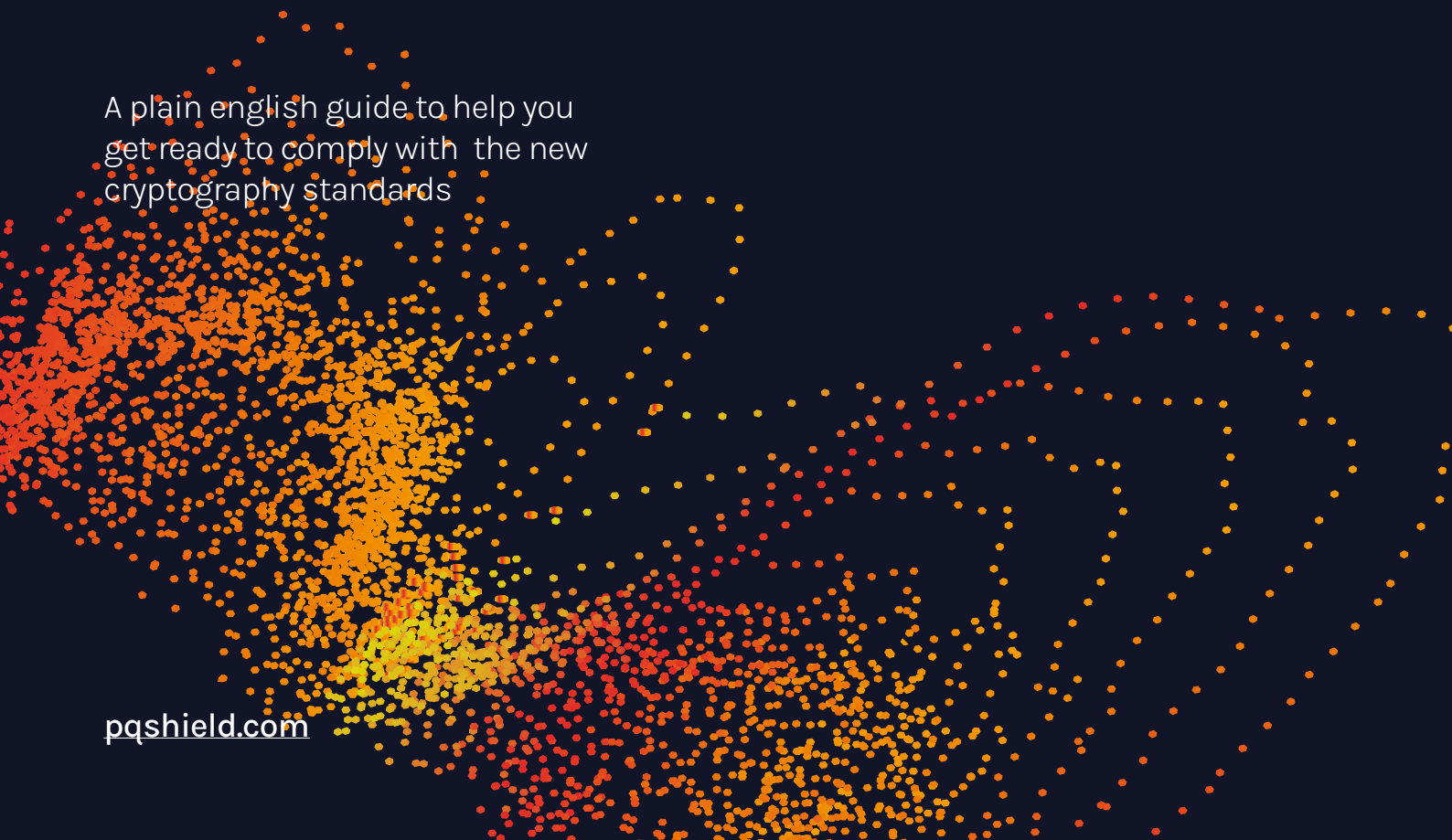
PQ SHIELD

Cryptography Modernization Part 2:

Crypto-agility and hybrid schemes

A plain english guide to help you get ready to comply with the new cryptography standards



pqshield.com

Introduction

As with all technological advances, the development of quantum computing carries with it the potential to change the world for the better, but it also brings the challenge of how to defend against uses of this technology that could disrupt our way of life. It's no secret that within the next few years, quantum computers might easily be able to break the cryptography that currently protects our world, and every industry needs to be aware of the threat.

For example, the World Economic Forum (in collaboration with the Financial Conduct Authority) recently published key guidance on preparing the roadmap for a cross-industry approach[1], NATO have updated their Quantum Technologies Strategy[2], and as the international standards for post-quantum cryptography come ever closer, other industries and global organizations are taking the subject seriously.

In the first part of our series on cryptography modernization[3] we examined how different industries might be affected, which cryptographic techniques might currently be in place, and where to start discovering them in your infrastructure. This first step in cryptography modernization is essential, as a working inventory will help you plan how to start migrating your systems towards quantum-resilience, and potentially beyond.

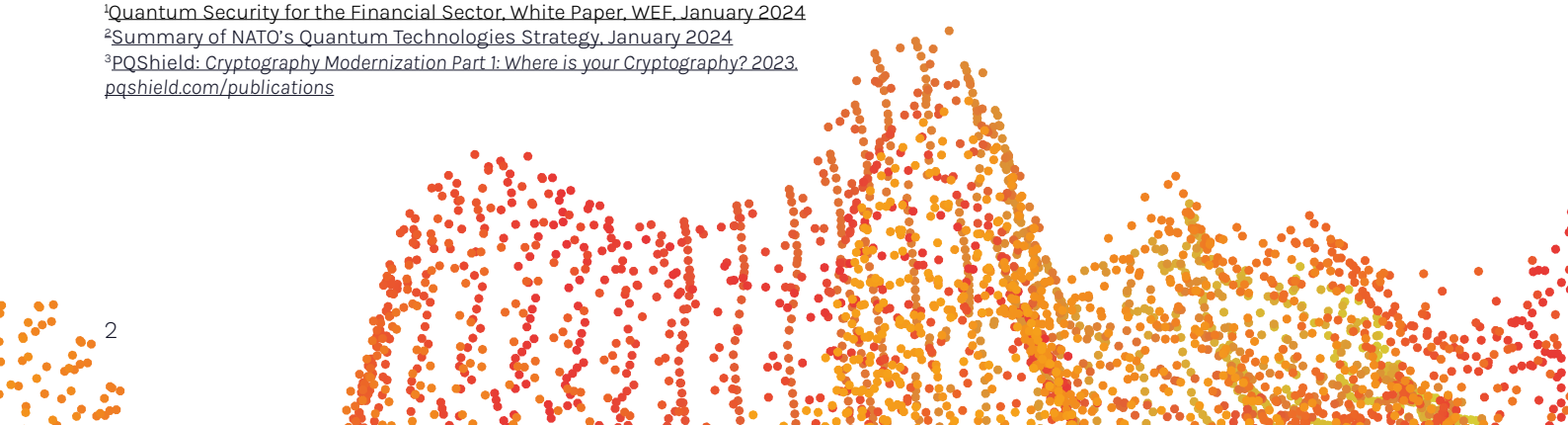
But what strategies should we take to modernize, especially while standardization of PQC algorithms is still underway? And what different approaches are recommended? How do you remain forward-thinking and flexible when it comes to preparing your infrastructure for the future?

In this article, we're going to look at the idea of 'crypto-agility' and investigate some of the differing approaches to hybrid schemes combining classical and post-quantum cryptographic algorithms. Cryptography modernization is effectively about how to keep systems operating securely in the face of a changing world, especially against unforeseen threats.

This concept of crypto-agility is essential to every industry, and to every component in the supply chain that's involved with information security.

Unfortunately, cryptographic techniques don't stay the same forever. Even the advent of quantum computing is not precisely a fixed point, and therefore crypto-agility is all about preparing to be flexible in the face of future threats, both seen and unforeseen. However, even with the uncertainty ahead, there are principles of crypto-agility that can be put into practice now.

[1]Quantum Security for the Financial Sector, White Paper, WEF, January 2024
[2]Summary of NATO's Quantum Technologies Strategy, January 2024
[3]PQShield: *Cryptography Modernization Part 1: Where is your Cryptography? 2023, pqshield.com/publications*



Top Tips on Crypto Agility

1 Make a visible plan

It's important to ensure you know the ownership of each component as part of your inventory (see Part 1 of this series on cryptography modernization). A visible plan of how to track the migration will be essential when it comes to deploying the latest standardized algorithms. In addition, your organization should establish well-documented policies on the use, modification and retiring of cryptographic mechanisms.

2 Update processes and practices

It's important to make sure your development team uses systems and processes that facilitate a culture of crypto-agility. For example, engineers need to be able to update algorithms deployed in a component's lifecycle quickly and easily, and they should be confident that supply chain vendors are able to do the same. This confidence comes from reviewing coding practice and methodology on a regular basis.

3 Identify and monitor vulnerabilities

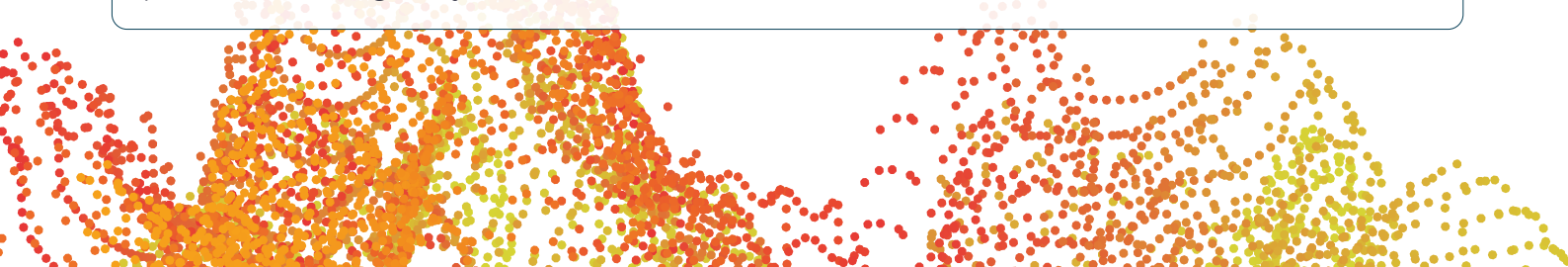
Ensure you know the weak points of your systems. This allows you to refine your plan on a regular basis, and informs the priority of which components should be updated in which order. You could also define role-based access controls to cryptography components to help monitor and manage the continued use of affected systems.

4 Stay up-to-date

In the changing world, you'll need to make sure you're up-to-speed with the latest standards from NIST and other regulatory bodies in your industry. It will become increasingly important to know exactly what you should be deploying and when, and this process will include any hardware vendors used in your infrastructure. Make sure your vendors are quick to release updates, and that those updates are deployed in a strategic plan.

5 Use automation strategically

Remote automation is brilliant at reducing human error, and it is a consideration for managing components through migration phases. However, you should use automation tools in addition to your tracking processes rather than depend on them. It's always best to trust but verify, and be strategic about how you manage the process. Carefully consider how to deploy automation to maintain visibility of your plan, and make sure that any automated processes are regularly reviewed.



Hybrid Cryptography

The key to staying crypto-agile is to be forward-thinking. How should we migrate our systems smoothly from being quantum-vulnerable to our ultimate goal of being fully quantum-safe?

Clearly, the answer is an intermediate step. That's why we need to think about so-called *hybrid cryptographic schemes*. Hybrid schemes are designed to use a combination of traditional public key cryptography and PQC algorithms in combination.

For example, a hybrid key exchange might include the classical Diffie-Hellman key exchange alongside a lattice-based KEM to remain secure against both classical and potential quantum attacks. Equally, lattice-based signature schemes can provide post-quantum protection alongside the traditional method for authenticating digital connections.

There are different approaches to hybrid schemes, as explored in the next section. In effect, crypto-agility will always require some level of hybridization, but there might be considerations to think through as part of your modernization plan. In the following sections, we're going to explore how different national bodies around the world have discussed their approach to hybrid cryptography.

NCSC (UK) Guidelines

Recently, the UK's National Cyber Security Centre (NCSC) published recommendations on Post-Quantum Traditional Hybrid Schemes (PQ/T) as part of their Next Steps in Preparing for Post-Quantum Cryptography series.

In general, the UK's position is a theoretical preference for transitioning to PQC with no long-term hybrid phase, where possible. Their caution is based on the complexity of deploying a hybrid solution, as well as the greater cost of running concurrent algorithms.

"If a PQ/T hybrid scheme is chosen, the NCSC recommends it is used as an interim measure, and it should be used within a flexible framework that enables a straightforward migration to PQC-only in the future."[4]

[4] Next steps in preparing for post-quantum cryptography, National Cyber Security Centre, Nov 23

However, the NCSC also point out that PQ/T schemes could be useful for three important considerations:

Interoperability
In a transition phase, particularly within a large network, there might be multiple systems that require interoperability - in other words, the existing cryptography alongside deployment of PQC algorithms enables these systems to continue to interoperate.

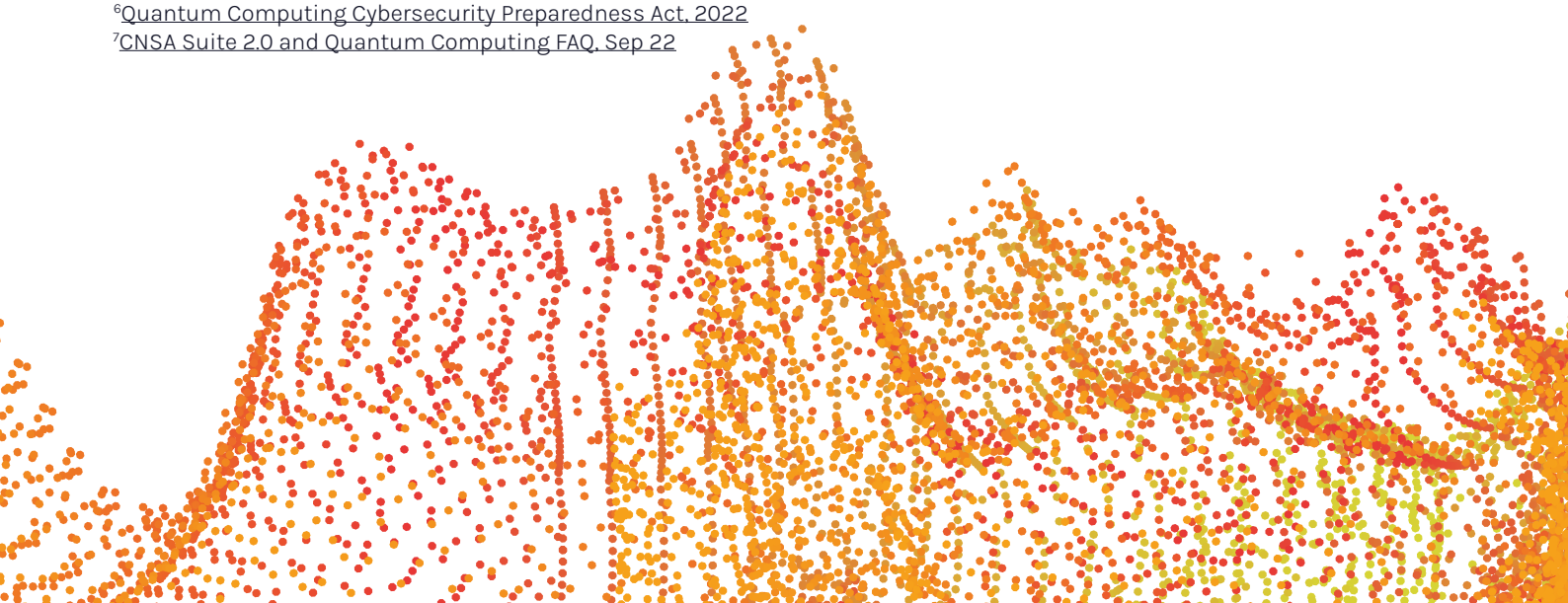
Implementation Security
While the NIST standards are still emerging during the ongoing standardization process, it might be preferable to ensure that a system remains secure by maintaining its existing cryptography alongside PQC.

Protocol Constraints
It is possible that some protocols have technical constraints, making it difficult to remove classical algorithms and replace them with PQC. A hybrid phase would mitigate against this, until the traditional cryptography is removed.

NSA (USA) Guidelines

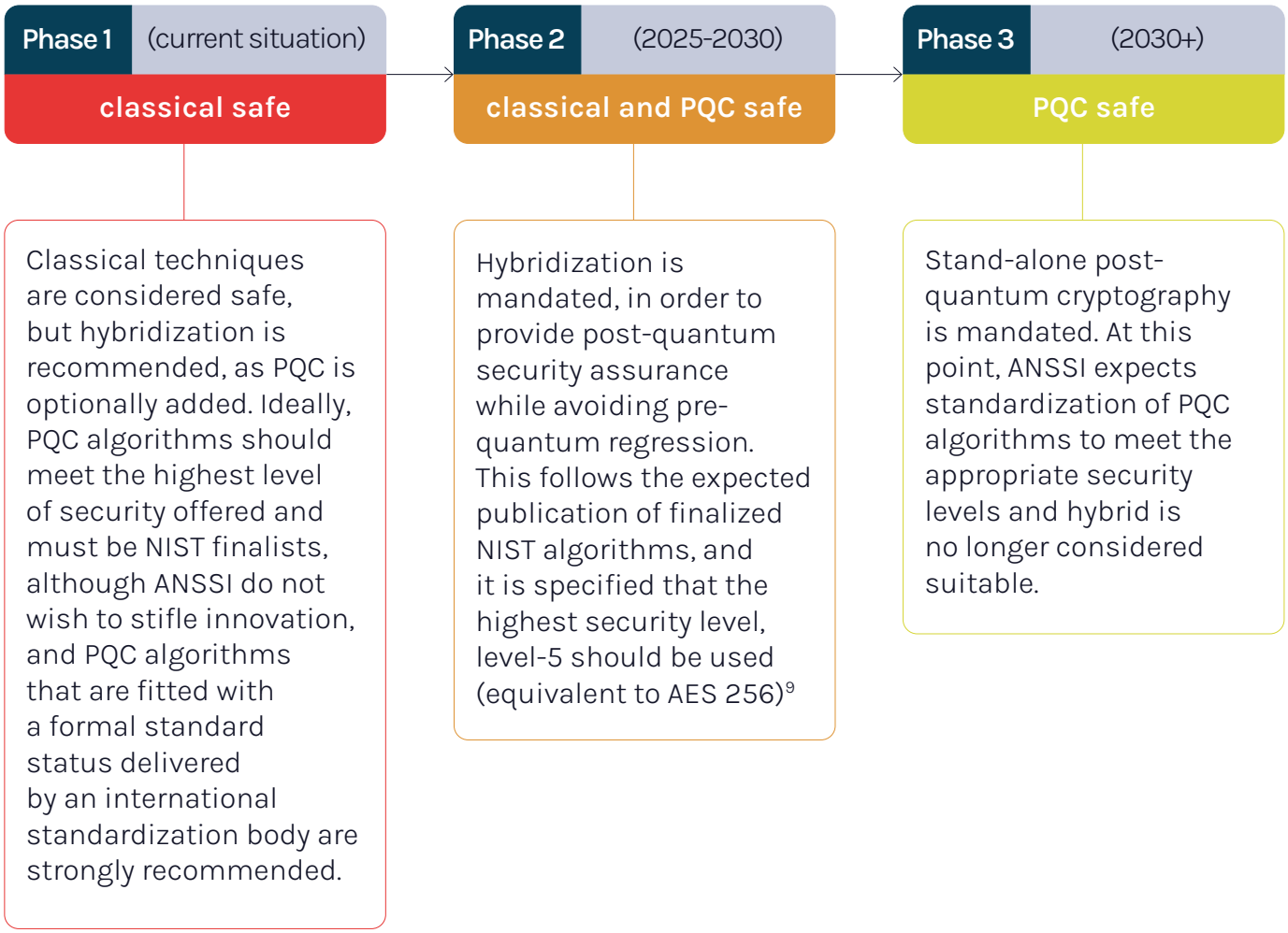
In the US, the focus of crypto-agility is on deploying cryptography that can be easily adapted. The White House has issued a number of guidelines for US agencies and departments, based on a mandated timeline specified in National Security Memorandum 10 (May 2022)[5] and subsequent legislation HR.7535[6]. The NSA's Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) guide[7] points out that the NSA's official position is confidence in the suite of algorithms specifically approved for national security systems. Hybrid solutions are not required, though the guidance also recognizes that 'product availability and interoperability requirements' may lead to their adoption. Further discussion with industry could take place in future, to specify the best implementation options.

[5] National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic System, May 2022
[6] Quantum Computing Cybersecurity Preparedness Act, 2022
[7] CNSA Suite 2.0 and Quantum Computing FAQ, Sep 22



ANSSI (FR) Guidelines

The French Cybersecurity Agency (ANSSI) outlines the introduction of post-quantum defences as part of a three-phase roadmap.[8]



BSI (DE) Guidelines

In Germany, the Federal Bureau of Information Security (BSI) recommends the use of hybrid solutions as an 'important building block' towards crypto-agility. For example, they recommend a hybrid approach to key establishment, where classical techniques and post-quantum algorithms work compositely. They recommend several methods for deriving cryptographic keys from multiple shared secrets, where the shared secrets are established by classical and post-quantum schemes.[10]

[8] ANSSI views on the Post-Quantum Cryptography transition, January 2022
[9] PQC Transition in France - ANSSI Views, March 2023
[10] Use of CatKDF and CasKDF in Quantum-Safe Hybrid Key Echanges, ETSI TS 103 744, NIST Special Publication 800-56C, Recommendation for Key Derivation Methods in Key Establishment Schemes

In general, BSI's view is that hybrid schemes are the way forward, even beyond 2030, as opposed to ANSSI's view that in Phase 3 (beyond the development of cryptographically relevant quantum computing), hybrid schemes will no longer be required. BSI accept security levels 3 and 5.

Both BSI and ANSSI also note that, with certain technical restrictions, stateful hash-based signature methods (XMSS and LMS) are considered sufficiently secure to be used without hybridization. You can find out more about this in the BSI Technical Guideline on *Cryptographic Mechanisms: Recommendations and Key Lengths.*[11]

Hybridization Considerations

The central benefit of hybrid systems is that PQC defends against a quantum adversary, while if an unknown exploit is encountered, the classical component is still in place and best-situated to protect the system. This ensures PQC is not depended upon in isolation.

There are different methods suggested for deploying a hybrid scheme, both for key encapsulation methods, and for handling digital signatures. For example, the classical and post-quantum algorithms could operate together as one entity to generate an encrypted secret, or independently from each other in the event that one technique is broken and the other is not.

You might also want to consider some of the requirements of a hybrid system.

- Can existing hardware cope, in terms of memory and processing power? What would need to be upgraded?
- How long will migration take? It might be that there is a time limit on how long you need public key cryptography to remain unbroken.
- What combinations of algorithms best suit your hybrid model?

Implementation

It's possible to deploy hybrid schemes in a number of ways, depending on requirements and infrastructure. The key to crypto-agility is maintaining a system that's easily able to be updated, not just for operational reasons, but also in a way that makes transition to the next phase equally as straightforward.

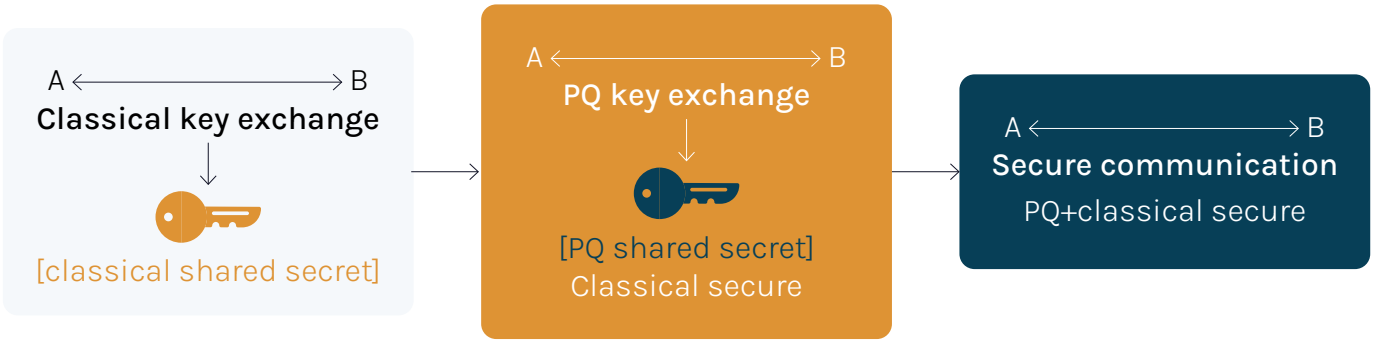
Migrating to a hybrid scheme is important, but implementing with a view to migrating out of it, also needs consideration.

[11] BSI TR-02102-1: "Cryptographic Mechanisms: Recommendations and Key Lengths" Version: 2023-1

Essentially there are a few basic approaches to a hybrid cryptographic scheme using traditional and post-quantum algorithms. For example:

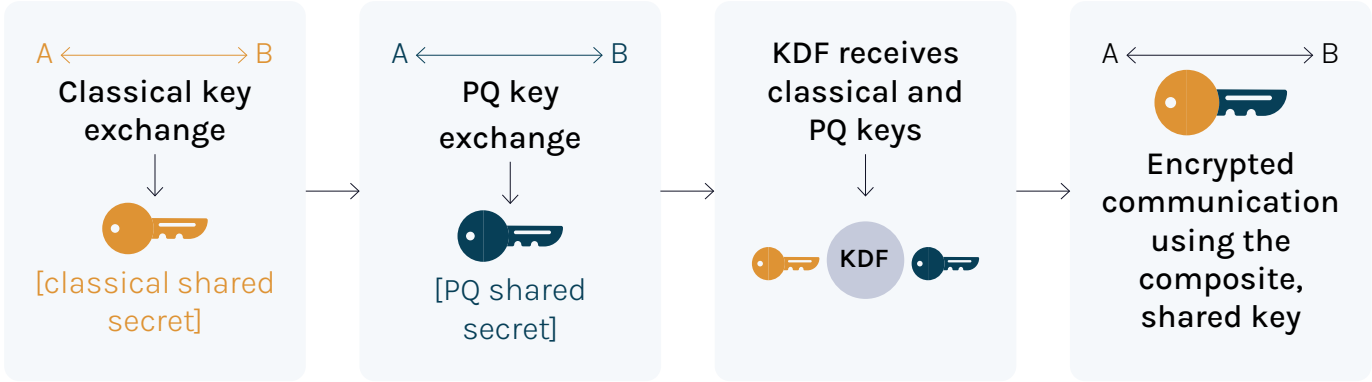
Hybrid Key Exchange - Layered

The layered, or concatenated hybrid approach utilises both the classical and post-quantum techniques in sequence. First, a classical key exchange mechanism (for example, ECDH) is used to establish a secure channel. Then the quantum-safe key mechanism uses this secure channel to establish a shared secret. This reinforces the layer of protection from either a quantum or a classical attack. A potential attacker would in theory, need to break both layers of defence to decrypt the message.



Hybrid Key Exchange - Composite

A composite, or cascade-mode, hybrid system generates two shared secrets independently of each other - one from the post-quantum algorithm and one by the traditional method. These shared secrets can then be combined by a Key Derivation Function (KDF) to generate a key from both outputs. Provided the KDF is configured to process the outputs efficiently, this approach can make it much more difficult for an attacker to succeed.



Hybrid Digital Signature Schemes

The combination of classical and post-quantum schemes for digital signatures follows some similar principles to those of layered key exchange mechanisms. Dilithium, now standardized as FIPS-204 ML-DSA can be combined in a number of ways with a classically secure scheme such as ECDSA. In fact, with digital signatures, you could implement a number of separate signature verifications and then specify that a connection is established only when all the outputs are verified.

Conclusion

In essence, the drive for crypto-agility makes the combination of traditional cryptography and PQC inevitable.

Even if it were possible to switch to post-quantum cryptography overnight, the chances are that legacy applications, devices in the field, connectivity of long-lasting machinery, or connected systems would still need to be supported by classical cryptography.

The advent of quantum computing does not mean the end of traditional public key cryptography by any means, and there will need to be interoperability for many years after the development of the first cryptographically relevant quantum computer. For example, even in the world of classical cryptography today, the symmetric-key block cipher known as Triple-DES was only fully retired at the end of 2023, some 23 years after its replacement was standardized. It's clear that even with the latest advancements, we still need backwards compatibility.

Most preparation for quantum-resilience in this phase will be to deploy the resources you need for the new algorithms, building the infrastructure and platforms required to integrate them. Hybrid combinations are likely to be part of your infrastructure for years to come, and it is worth researching and developing the plan strategically now, in order to protect your organization later.

This preparedness, watchful of the future and mindful of the present, is at the heart of crypto-agility, helping to build the road towards quantum-resilience.

Appendix A: Terminology

It's important to understand some of the details involved in cryptography migration, especially as the world moves towards the use of hybrid schemes. In this section, we'll explore some of the terminology that's commonly used, in order to give more clarity to the topic.

Term	Description
Traditional algorithm/ scheme	An asymmetric algorithm/scheme that's based on mathematical principles not considered quantum-resistant. For example, ECDH or RSA. Sometimes referred to as 'classical'.
Post-quantum algorithms/schemes	Quantum-resistant or quantum-safe algorithms/schemes that are designed to be secure against a quantum attack.
Post-quantum/ Traditional Hybrid scheme (PQ/T)	A scheme that includes two or more components where at least one of those components is a post-quantum algorithm, and at least one is a traditional algorithm.
PKI (Public Key Infrastructure)	Any system of hardware/software that's used to manage digital keys and certificates. PKI is based on the idea of asymmetric encryption where each entity has both a public and private key.
Key Encapsulation Mechanism (KEM)	A cryptography technique used to establish a shared secret key between two parties. It consists of key generation, encapsulation (encryption) and decapsulation (decryption).
Digital Certificate	A cryptographic key pair that helps verify the authenticity of entities involved in a digital communication.
PQ/T Hybrid Protocol	A protocol that uses at least one post-quantum and one traditional component algorithm to produce an output. For example, a protocol could combine the output of a post-quantum KEM and a traditional KEM at the protocol level to generate a single shared secret.
PQ/T Hybrid Certificate	A digital certificate containing public keys for two or more component algorithms where at least one is a post-quantum algorithm and one is a traditional algorithm.

Appendix B: Further Reading

The following resources contain useful guidance on cryptography modernization, including technical developments from organizations referenced here, and some more in-depth papers and articles on different approaches to hybrid schemes.

- BSI Quantum-safe cryptography – fundamentals, current developments and recommendations
- ETSI - Quantum-Safe Hybrid Key Exchanges
- NIST - Recommendation for Key-Derivation Methods in Key-Establishment Schemes
- IETF - Combiner function for hybrid key encapsulation mechanisms (Hybrid KEMs)
- IETF - Hybrid key exchange in TLS 1.3
- Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)

About PQShield

The PQShield team is helping to shape the way our digital world is protected against the threats of tomorrow. At a time when quantum computers will soon be able to break current cryptography methods, we're focused on empowering organizations, industries, and nations, with the ultimate quantum-resistant cryptography solutions.

PQShield began as a spin-out from the University of Oxford, but now with teams in Europe, Japan, the US, and the UK, PQShield has grown into a world-class collaboration of post-quantum cryptographers, engineers, and operators.

We are a source of truth for stakeholders at every level, and we're seen by both customers and competitors as a leading provider of PQC solutions in hardware and software. Our think openly, build securely ethos has helped us to shape all of the first international PQC NIST standards, and to be the first cybersecurity company to develop quantum-safe cryptography on chips, in applications, and in the cloud.

We've also contributed multiple cryptographic extensions to RISC-V, the open standard instruction set architecture (ISA) that is gaining traction from proprietary competitors such as ARM and Intel, alongside working with many other organisations like the World Economic Forum, IETF, ETSI, GSMA, NCCoE, PQCC and GlobalPlatform, to advise and define their own positions. We're also the experts on PQC side-channel attack resistance, having built a dedicated SCA test lab verified by our industry leading partners.

Our mission is to build products and solutions that help modernize the legacy cryptography in the world's technology supply chain, to deliver new global standards alongside real-world hardware and software upgrades, and to keep the world one step ahead of the attackers. Our mature PQC software and hardware solutions are already in the hands of forward- thinking organizations like Microchip, AMD, Collins Aerospace, MBDA Weapons Systems and many more.

PQ SHIELD

think openly, build securely

Ready to learn more? Get in touch: contact@pqshield.com | www.pqshield.com

PQShield Ltd
Oxford
Prama House
267 Banbury Road
Oxford
OX2 7HT

PQShield SAS
Paris
8 Rue des Pirogues de Bercy
Paris
75012

PQShield B.V.
Amsterdam
Keizersgracht 62
1015CS
Amsterdam

PQShield Inc.
New York
228 East 45th Street
Suite 9E
New York
NY 10017

London
City Tower
40 Basinghall Street
London
EC2V 5DE