PQUIP
Internet-Draft
Intended status: Informational
Expires: 8 September 2023

F. Driscoll
UK National Cyber Security Centre

7 March 2023

Terminology for Post-Quantum Traditional Hybrid Schemes
draft-driscoll-pqt-hybrid-terminology-02

Abstract

One aspect of the transition to post-quantum algorithms in cryptographic protocols is the development of hybrid schemes that incorporate both post-quantum and traditional asymmetric algorithms. This document defines terminology for such schemes. It is intended to be used as a reference and, hopefully, to ensure consistency and clarity across different protocols, standards, and organisations.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-driscoll-pqt-hybrid-terminology/.

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-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 8 September 2023.

Table of Contents

1. Introduction

The mathematical problems of integer factorisation and discrete logarithms over finite fields or elliptic curves underpin most of the asymmetric algorithms used for key establishment and digital signatures on the internet. These problems, and hence the algorithms based on them, will be vulnerable to attacks using Shor's Algorithm on a sufficiently large general-purpose quantum computer, known as a Cryptographically Relevant Quantum Computer (CRQC). It is difficult to predict when, or if, such a device will exist. However, it is necessary to anticipate and prepare to defend against such a development. Data encrypted today (2023) with an algorithm vulnerable to a quantum computer could be stored for decryption by a future attacker with a CRQC. Signing algorithms in products that are expected to be in use for many years are also at risk if a CRQC is developed during the operational lifetime of that product.

Preparing for the potential development of a CRQC requires modifying established (standardised) protocols to use asymmetric algorithms that are perceived to be secure against quantum computers as well as today's classical computers. These algorithms are called post-quantum, while algorithms based on integer factorisation, finite-field discrete logarithms or elliptic-curve discrete logarithms are called traditional algorithms.

During the transition from traditional to post-quantum algorithms, there may be a desire or a requirement for protocols that use both algorithm types. A designer may choose to combine a post-quantum algorithm with a traditional algorithm to add protection against an attacker with a CRQC to the security properties provided by the traditional algorithm. They may also choose to implement a post-quantum algorithm alongside a traditional algorithm for ease of migration from an ecosystem where only traditional algorithms are implemented and used, to one that only uses post-quantum algorithms. Examples of solutions that could use both types of algorithm include, but are not limited to, [I-D.ietf-ipsecme-ikev2-multiple-ke], [I-D.ietf-tls-hybrid-design], [I-D.ounsworth-pq-composite-sigs], and [I-D.ietf-lamps-cert-binding-for-multi-auth]. Schemes that combine post-quantum and traditional algorithms for key establishment or digital signatures are often called hybrids. For example:

* NIST defines hybrid key establishment to be a "scheme that is a combination of two or more components that are themselves cryptographic key-establishment schemes" [NIST_PQC_FAQ];

* ETSI defines hybrid key exchanges to be "constructions that combine a traditional key exchange ... with a post-quantum key exchange ... into a single key exchange" [ETSI_TS103774].

The word "hybrid" is also used in cryptography to describe encryption schemes that combine asymmetric and symmetric algorithms [RFC4949], so using it in the post-quantum context overloads it and risks misunderstandings. However, this terminology is well-established amongst the post-quantum cryptography (PQC) community. Therefore, an attempt to move away from its use for PQC could lead to multiple definitions for the same concept, resulting in confusion and lack of clarity.

This document provides language for constructions that combine traditional and post-quantum algorithms. Specific solutions for enabling use of multiple asymmetric algorithms in cryptographic schemes may be more general than this, allowing the use of solely traditional or solely post-quantum algorithms. However, where relevant, we focus on post-quantum traditional combinations as these are the motivation for the wider work in the IETF. This document is intended as a reference terminology guide for other documents to add clarity and consistency across different protocols, standards, and organisations. Additionally, this document aims to reduce misunderstanding about use of the word "hybrid" as well as defining a shared language for different types of post-quantum traditional hybrid constructions.

In this document, a "cryptographic algorithm" is defined, as in [NIST_SP_800-152], to be a "well-defined computational procedure that takes variable inputs, often including a cryptographic key, and produces an output". Examples include RSA, ECDH, CRYSTALS-Kyber and CRYSTALS-Dilithium. The expression "cryptographic scheme" is used to refer to a construction that uses a cryptographic algorithm or a group of cryptographic algorithms to achieve a particular cryptographic outcome, e.g., key agreement. A cryptographic scheme may be made up of a number of functions. For example, a Key Encapsulation Mechanism (KEM) is a cryptographic scheme consisting of three functions: Key Generation, Encapsulation, and Decapsulation. A cryptographic protocol incorporates one or more cryptographic schemes. For example, TLS [RFC8446] is a cryptographic protocol that includes schemes for key agreement, record layer encryption, and server authentication.

2. Primitives

This section introduces terminology related to cryptographic algorithms and to hybrid constructions for cryptographic schemes.

Traditional Algorithm: An asymmetric cryptographic algorithm based on integer factorisation, finite field discrete logarithms or elliptic curve discrete logarithms.

Post-Quantum Algorithm: An asymmetric cryptographic algorithm that is believed to be secure against attacks using quantum computers as well as classical computers.

Component Algorithm: Each cryptographic algorithm that forms part of a cryptographic scheme.

Single-Algorithm Scheme: A cryptographic scheme with one component algorithm.

A single-algorithm scheme could use either a traditional algorithm or a post-quantum algorithm.

Multi-Algorithm Scheme: A cryptographic scheme with more than one component algorithm.

In a multi-algorithm scheme all component algorithms are of the same type; e.g., all are signature algorithms or all are Public Key Encryption (PKE) algorithms. Component algorithms could be all traditional, all post-quantum, or a mixture of the two.

Post-Quantum Traditional (PQ/T) Hybrid Scheme: A multi-algorithm

scheme where at least one component algorithm is a post-quantum algorithm and at least one is a traditional algorithm.

PQ/T Hybrid Key Encapsulation Mechanism (KEM): A multi-algorithm KEM made up of two or more component KEM algorithms where at least one is a post-quantum algorithm and at least one is a traditional algorithm.

PQ/T Hybrid Public Key Encryption (PKE): A multi-algorithm PKE scheme made up of two or more component PKE algorithms where at least one is a post-quantum algorithm and at least one is a traditional algorithm.

PQ/T Hybrid Digital Signature: A multi-algorithm digital signature scheme made up of two or more component digital signature algorithms where at least one is a post-quantum algorithm and at least one is a traditional algorithm.

PQ/T hybrid KEMs, PQ/T hybrid PKE, and PQ/T hybrid digital signatures are all examples of PQ/T hybrid schemes.

PQ/T Hybrid Combiner: A method that takes two or more component algorithms and combines them to form a PQ/T hybrid scheme.

PQ/PQ Hybrid Scheme: A multi-algorithm scheme where all components are post-quantum algorithms.

The definitions for types of PQ/T hybrid schemes can adapted to define types of PQ/PQ hybrid schemes, which are multi-algorithm schemes where all component algorithms are Post-Quantum algorithms.

3. Cryptographic Elements

This section introduces terminology related to cryptographic elements and their inclusion in hybrid schemes.

Cryptographic Element: Any data type (private or public) that contains an input or output value for a cryptographic algorithm or for a function making up a cryptographic algorithm.

Types of cryptographic elements include public keys, private keys, plaintexts, ciphertexts, shared secrets, and signature values.

Component Cryptographic Element: A cryptographic element of a component algorithm in a multi-algorithm scheme.

For example, in [I-D.ietf-tls-hybrid-design], the client's keyshare contains two component public keys, one for a post-quantum algorithm and one for a traditional algorithm.

Composite Cryptographic Element: A cryptographic element that incorporates multiple component cryptographic elements of the same type in a multi-algorithm scheme.

For example, a composite cryptographic public key is made up of two component public keys.

Cryptographic Element Combiner: A method that takes two or more component cryptographic elements of the same type and combines them to form a composite cryptographic element.

A cryptographic element combiner could be concatenation, such as where two component public keys are concatenated to form a composite public key as in [I-D.ietf-tls-hybrid-design], or something more involved such as the dualPRF defined in [BINDEL].

4. Protocols

This section introduces terminology related to the use of post-quantum and traditional algorithms together in protocols.

PQ/T Hybrid Protocol: A protocol that uses two or more component algorithms providing the same cryptographic functionality, where at least one is a post-quantum algorithm and at least one is a traditional algorithm.

For example, a PQ/T hybrid protocol providing confidentiality could use a PQ/T hybrid KEM such as in [I-D.ietf-tls-hybrid-design], or it could combine the output of a post-quantum KEM and a traditional KEM at the protocol level to generate a single shared secret, such as in [I-D.ietf-ipsecme-ikev2-multiple-ke]. Similarly, a PQ/T hybrid protocol providing authentication could use a PQ/T hybrid digital signature scheme, or it could include both post-quantum and traditional single-algorithm digital signature schemes.

Composite PQ/T Hybrid Protocol: A protocol that incorporates one or more PQ/T hybrid schemes in such a way that the protocol fields and message flow are the same as those in a version of the protocol that uses single-algorithm schemes.

In a composite PQ/T hybrid protocol, changes are primarily made to the formats of the cryptographic elements, while the protocol fields and message flow remain largely unchanged. In

implementations, most changes are likely to be made to the cryptographic libraries, with minimal changes to the protocol libraries.

Non-composite PQ/T Hybrid Protocol: A protocol that incorporates multiple single-algorithm schemes of the same type, where at least one uses a post-quantum algorithm and at least one uses a traditional algorithm, in such a way that the formats of the component cryptographic elements are the same as when they are used as part of single-algorithm schemes.

In a non-composite PQ/T hybrid protocol, changes are primarily made to the protocol fields, the message flow, or both, while changes to cryptographic elements are minimised. In implementations, most changes are likely to be made to the protocol libraries, with minimal changes to the cryptographic libraries.

It is possible for a PQ/T hybrid protocol to be designed that is neither entirely composite nor entirely non-composite. For example, in a protocol that offers both confidentiality and authentication, the key establishment could be done in a composite manner while the authentication is done in a non-composite manner.

5. Functionality

This section describes properties that may be desired from or achieved by a PQ/T hybrid scheme or PQ/T hybrid protocol.

PQ/T Hybrid Confidentiality: The property that confidentiality is achieved by a PQ/T hybrid scheme or PQ/T hybrid protocol as long as at least one component algorithm that aims to provide this property remains secure.

PQ/T Hybrid Authentication: The property that authentication is achieved by a PQ/T hybrid scheme or a PQ/T hybrid protocol as long as at least one component algorithm that aims to provide this property remains secure.

EDNOTE 1: It may be useful to distinguish between source authentication (i.e., authentication of the sender of a particular message) and identity authentication (i.e., authentication of the identity of the sender).

The security properties of a PQ/T hybrid scheme or protocol depend on the security of its component algorithms, the choice of PQ/T hybrid combiner, and the capability of an attacker. Changes to the security of a component algorithm can impact the security properties of a PQ/T

hybrid scheme providing hybrid confidentiality or hybrid authentication. For example, if the post-quantum component algorithm of a PQ/T hybrid scheme is broken, the scheme will remain secure against an attacker with a classical computer, but will be vulnerable to an attacker with a CRQC.

PQ/T hybrid protocols that offer both confidentiality and authentication do not necessarily offer both hybrid confidentiality and hybrid authentication. For example, [I-D.ietf-tls-hybrid-design] provides hybrid confidentiality but does not address hybrid authentication. Therefore, if the design in [I-D.ietf-tls-hybrid-design] is used with X.509 certificates as defined in [RFC5280] only authentication with a single algorithm is achieved.

PQ/T Hybrid Interoperability: The property that a PQ/T hybrid scheme or PQ/T hybrid protocol can be completed successfully provided that both parties share support for at least one component algorithm.

  For example, a PQ/T hybrid digital signature might achieve hybrid interoperability if the signature can be verified by either verifying the traditional or the post-quantum component, such as in the OR modes described in [I-D.ounsworth-pq-composite-sigs].

In the case of a protocol that aims to achieve both authentication and confidentiality, PQ/T hybrid interoperability requires that at least one component authentication algorithm and at least one component algorithm for confidentiality is supported by both parties.

It is not possible for a PQ/T hybrid scheme to achieve both PQ/T hybrid interoperability and PQ/T hybrid confidentiality without additional functionality at a protocol level. For PQ/T hybrid interoperability a scheme needs to work whenever one component algorithm is supported by both parties, while to achieve PQ/T hybrid confidentiality all component algorithms need to be used. However, both properties can be achieved in a PQ/T hybrid protocol by building in downgrade protection external to the cryptographic schemes. For example, in [I-D.ietf-tls-hybrid-design], the client uses the TLS supported groups extension to advertise support for a PQ/T hybrid scheme and the server can select this group if it supports the scheme. This is protected using TLS's existing downgrade protection, so achieves PQ/T hybrid confidentiality, but the connection can still be made if either the client or server does not support the PQ/T hybrid scheme, so PQ/T hybrid interoperability is achieved.

The same is true for PQ/T hybrid interoperability and PQ/T hybrid authentication. It is not possible to achieve both with a PQ/T hybrid scheme alone, but it is possible with a PQ/T hybrid protocol that has appropriate downgrade protection.

EDNOTE 2: Other properties may be desired from a PQ/T Hybrid scheme e.g. backwards compatibility, crypt agility. Should these be defined here?

6. Certificates

This section introduces terminology related to the use of certificates in hybrid schemes.

PQ/T Hybrid Certificate: A digital certificate that contains public keys for two or more component algorithms where at least one is a traditional algorithm and at least one is a post-quantum algorithm.

A PQ/T hybrid certificate could be used to facilitate a PQ/T hybrid authentication protocol. However, a PQ/T hybrid authentication protocol does not need to use a PQ/T hybrid certificate; separate certificates could be used for individual component algorithms.

The component public keys in a PQ/T hybrid certificate could be included as a composite public key or as individual component public keys.

The use of a PQ/T hybrid certificate does not necessarily achieve hybrid authentication of the identity of the sender; this is determined by properties of the chain of trust. For example, an end-entity certificate that contains a composite public key as defined in [I-D.ounsworth-pq-composite-keys] but which is signed using a single-algorithm digital signature scheme could be used to provide hybrid authentication of the source of a message, but would not achieve hybrid authentication of the identity of the sender.

Post-Quantum Certificate: A digital certificate that contains a single public key for a post-quantum digital signature algorithm.

Traditional Certificate: A digital certificate that contains a single public key for a traditional digital signature algorithm.

X.509 certificates as defined in [RFC5280] could be either traditional or post-quantum certificates depending on the algorithm in the Subject Public Key Info. For example, a certificate containing a Dilithium public key, as defined in [I-D.ietf-lamps-dilithium-certificates], would be a post-quantum certificate.

Post-Quantum Certificate Chain: A certificate chain where each certificate includes a public key for a post-quantum algorithm and is signed using a post-quantum digital signature scheme.

Traditional Certificate Chain: A certificate chain where all certificates includes a public key for a traditional algorithm and is signed using a traditional digital signature scheme.

PQ/T Hybrid Certificate Chain: A certificate chain where all certificates are PQ/T hybrid certificates and each certificate is signed with two or more component algorithms where at least one is a traditional algorithm and at least one is a post-quantum algorithm.

A PQ/T hybrid certificate chain is one way of achieving hybrid authentication of the identity of a sender in a protocol, but is not the only way. An alternative is to incorporate both a post-quantum certificate chain and a traditional certificate chain in a protocol.

It would be possible to construct a certificate chain containing a mixture of post-quantum certificates, traditional certificates and PQ/T hybrid certificates. For example, a post-quantum end-entity certificate could be signed by a traditional intermediate certificate, which in turn could be signed by a traditional root. The security properties of a certificate chain that mixes post-quantum and traditional algorithms would need to be analysed on a case-by-case basis.

EDNOTE 3: Do we want a definition of multi-cert authentication or something similar?

7. Algorithm Specification

This section introduces terminology for specifying the component algorithms used in PQ/T hybrid schemes or PQ/T hybrid protocols.

PQ/T Hybrid Scheme Identifier: A single code point that specifies all component algorithms used in a PQ/T hybrid scheme.

8. Security Considerations

This document defines security-relevant terminology to be used in documents specifying PQ/T hybrid protocols and schemes. However, the document itself does not have a security impact on Internet protocols. The security considerations for each PQ/T hybrid protocol are specific to that protocol and should be discussed in the relevant specification documents.

9. IANA Considerations

This document has no IANA actions.

10. Informative References

[BINDEL] Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., and D. Stebila, "Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange", Post-Quantum Cryptography pp.206-226, DOI 10.1007/978-3-030-25510-7_12, July 2019, <https://doi.org/10.1007/978-3-030-25510-7_12>.

[ETSI_TS103774] ETSI TS 103 744 V1.1.1, "CYBER; Quantum-safe Hybrid Key Exchanges", December 2020, <https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.01.01_60/ts_103744v010101p.pdf>.

[I-D.ietf-ipsecme-ikev2-multiple-ke] Tjhai, C., Tomlinson, M., Bartlett, G., Fluhrer, S., Van Geest, D., Garcia-Morchon, O., and V. Smyslov, "Multiple Key Exchanges in IKEv2", Work in Progress, Internet-Draft, draft-ietf-ipsecme-ikev2-multiple-ke-12, 1 December 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-ikev2-multiple-ke-12>.

[I-D.ietf-lamps-cert-binding-for-multi-auth] Becker, A., Guthrie, R., and M. J. Jenkins, "Related Certificates for Use in Multiple Authentications within a Protocol", Work in Progress, Internet-Draft, draft-ietf-lamps-cert-binding-for-multi-auth-00, 24 February 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-cert-binding-for-multi-auth-00>.

[I-D.ietf-lamps-dilithium-certificates] Massimo, J., Kampanakis, P., Turner, S., and B. Westerbaan, "Internet X.509 Public Key Infrastructure: Algorithm Identifiers for Dilithium", Work in Progress, Internet-Draft, draft-ietf-lamps-dilithium-certificates-

01, 6 February 2023,
<https://datatracker.ietf.org/doc/html/draft-ietf-lamps-dilithium-certificates-01>.

[I-D.ietf-tls-hybrid-design]
Stebila, D., Fluhrer, S., and S. Gueron, "Hybrid key exchange in TLS 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-hybrid-design-06, 27 February 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design-06>.

[I-D.ounsworth-pq-composite-keys]
Ounsworth, M., Pala, M., and J. Klaußner, "Composite Public and Private Keys For Use In Internet PKI", Work in Progress, Internet-Draft, draft-ounsworth-pq-composite-keys-03, 22 October 2022, <https://datatracker.ietf.org/doc/html/draft-ounsworth-pq-composite-keys-03>.

[I-D.ounsworth-pq-composite-sigs]
Ounsworth, M. and M. Pala, "Composite Signatures For Use In Internet PKI", Work in Progress, Internet-Draft, draft-ounsworth-pq-composite-sigs-07, 8 June 2022, <https://datatracker.ietf.org/doc/html/draft-ounsworth-pq-composite-sigs-07>.

[NIST_PQC_FAQ]
National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography FAQs", 5 July 2022, <https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs>.

[NIST_SP_800-152]
Barker, E. B., Smid, M., Branstad, D., and National Institute of Standards and Technology (NIST), "NIST SP 800-152 A Profile for U. S. Federal Cryptographic Key Management Systems", October 2015, <https://doi.org/10.6028/NIST.SP.800-152>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <https://www.rfc-editor.org/rfc/rfc4949>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/rfc/rfc5280>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

Acknowledgments

TODO

Author's Address

Florence Driscoll
UK National Cyber Security Centre
Email: florence.d@ncsc.gov.uk