Workgroup: TBD
Internet-Draft:
draft-driscoll-pqt-hybrid-terminology-00
Published: 8 July 2022
Intended Status: Informational
Expires: 9 January 2023
Authors: F. Driscoll
UK National Cyber Security Centre

Terminology for Post-Quantum Traditional Hybrid Schemes

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 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 9 January 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 defend against this possibility. Data encrypted today with an algorithm vulnerable to a quantum computer could be stored for decryption by a future attacker with a CRQC. Signing algorithms that are expected to be in use for many years are also at risk if a CRQC is developed during the operational lifetime of the algorithm.

Preparing for the potential development of a CRQC requires modifying standardised protocols to use asymmetric algorithms that are believed 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 types of algorithm. Most post-quantum algorithms are less well studied than traditional asymmetric algorithms, so 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. A designer 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 which uses post-quantum algorithms. Work on solutions that could use both types of algorithm includes [I-D.ietf-ipsecme-ikev2-multiple-ke], [I-D.ietf-tls-hybrid-design], [I-D.ounsworth-pq-composite-sigs], [I-D.becker-guthrie-noncomposite-hybrid-auth]. Schemes that combine post-quantum and traditional algorithms for key establishment or digital signatures are often called hybrids. For example, NIST define 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] and ETSI define 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 [RFC9180], so using it in the post-quantum context overloads it and risks misunderstandings. However, this terminology is well-established amongst the post-quantum cryptography community so an attempt to move away from its use 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 in fact 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. It is intended as a terminology guide for other documents to add clarity and consistency across different protocols, standards, and organisations. Additionally, it 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, ECH, CRYSTALS-Kyber and CRYSTALS-Dilithium. The expression "cryptographic scheme" is used to

mean a construction that uses an algorithm or a group of 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 is a cryptographic protocol which includes schemes for key agreement, record layer encryption, and server authentication.

2. Primitives

This section introduces terminology related to cryptographic algorithms, as well as 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 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.

Post-Quantum Traditional (PQT) Hybrid Scheme: A cryptographic scheme that uses two or more component algorithms where at least one is a post-quantum algorithm and at least one is a traditional algorithm.

PQT Hybrid Key Encapsulation Mechanism: A Key Encapsulation Mechanism (KEM) that uses two or more component algorithms where at least one is a post-quantum algorithm and at least one is a traditional algorithm.

PQT Hybrid Public Key Encryption: A Public Key Encryption (PKE) scheme that uses two or more component algorithms where at least one is a post-quantum algorithm and at least one is a traditional algorithm.

PQT Hybrid Digital Signature: A digital signature scheme that uses two or more component algorithms where at least one is a post-quantum algorithm and at least one is a traditional algorithm.

PQT Hybrid KEMs, PQT Hybrid PKE, and PQT Hybrid Digital Signatures are all examples of PQT Hybrid schemes.

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

3. Functionality

This section describes properties that may be desired from or achieved by a PQT Hybrid scheme.

Hybrid Confidentiality: The property that confidentiality is achieved provided that at least one component algorithm remains secure.

EDNOTE 1: In the PQT Hybrid case what does this property mean if the attacker has a quantum computer?

Hybrid Authentication: The property that authentication is achieved provided that at least one component algorithm remains secure.

EDNOTE 2: This may benefit from expanding. Whether this is achieved or not depends on whether the verifier verifies all signatures, which they may not do in all cases, or may not be defined in the protocol. Either the definition of hybrid authentication could be expanded or more definitions could be added to this section.

EDNOTE 3: 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).

EDNOTE 4: Other properties may be desired from a PQT Hybrid scheme e.g. backwards compatibility, crypt agility. Should these be defined here?

4. Cryptographic Elements

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

Cryptographic Element: Any data (private or public) that is an input or output value for a cryptographic algorithm or 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.

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].

5. Protocols

This section introduces terminology related to the use of PQT Hybrid schemes in protocols.

PQT Hybrid Protocol: A protocol that incorporates one or more PQT Hybrid schemes.

A PQT Hybrid protocol that provides hybrid confidentiality may use a PQT Hybrid KEM, PQT Hybrid PKE, or a different combination of primitives. A PQT Hybrid protocol that provides hybrid authentication may use a PQT Hybrid Digital Signature or could alternatively use a PQT Hybrid KEM or PQT Hybrid PKE to prove possession of long-term component private keys.

PQT 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.

Composite PQT Hybrid Protocol: A protocol that incorporates one or more PQT 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 PQT 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 PQT Hybrid Protocol: A protocol that incorporates one or more PQT Hybrid schemes 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 PQT 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.

NOTE: It is possible for a PQT 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.

6. Certificates

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

PQT 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 PQT Hybrid certificate could be used to facilitate a PQT Hybrid authentication protocol. However, a PQT Hybrid authentication protocol does not need to use a PQT Hybrid certificate; separate certificates could be used for individual component algorithms.

The component public keys in a PQT Hybrid certificate could be included as a composite public key or as individual component public keys.

The use of a PQT 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.

EDNOTE 5: Is it helpful to define composite and non-composite certificates?

TODO 1: Terminology for certificate chains and PKI.

TODO 2: Terminology for algorithm specification.

7. Security Considerations

This document defines security-relevant terminology to be used in documents specifying PQT Hybrids. However, the document itself does not have a security impact on internet protocols. The security considerations for each PQT Hybrid protocol are specific to that protocol and should be discussed in the relevant documents.

8. IANA Considerations

This document has no IANA actions.

9. 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.becker-guthrie-noncomposite-hybrid-auth] Becker, A., Guthrie, R., and M. Jenkins, "Non-Composite Hybrid Authentication in PKIX and Applications to Internet Protocols", Work in Progress, Internet-Draft, draft-becker-guthrie-noncomposite-hybrid-auth-00, 22 March 2022, <https://www.ietf.org/archive/id/draft-becker-guthrie-noncomposite-hybrid-auth-00.txt>.

[I-D.ietf-ipsecme-ikev2-multiple-ke] Tjhai, C., Tomlinson, M., Bartlett, G., Fluhrer, S., Geest, D. V., Garcia-Morchon, O., and V. Smyslov,

"Multiple Key Exchanges in IKEv2", Work in Progress, Internet-Draft, draft-ietf-ipsecme-ikev2-multiple-ke-06, 13 June 2022, <https://www.ietf.org/archive/id/draft-ietf-ipsecme-ikev2-multiple-ke-06.txt>.

[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-04, 11 January 2022, <https://www.ietf.org/archive/id/draft-ietf-tls-hybrid-design-04.txt>.

[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-02, 8 June 2022, <https://www.ietf.org/archive/id/draft-ounsworth-pq-composite-keys-02.txt>.

[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://www.ietf.org/archive/id/draft-ounsworth-pq-composite-sigs-07.txt>.

[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>.

[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/info/rfc5280>.

[RFC9180] Barnes, R., Bhargavan, K., Lipp, B., and C. Wood, "Hybrid Public Key Encryption", RFC 9180, DOI 10.17487/RFC9180, February 2022, <https://www.rfc-editor.org/info/rfc9180>.

Acknowledgments

TODO acknowledge.

Author's Address

Florence Driscoll
UK National Cyber Security Centre

Email: florence.d@ncsc.gov.uk