TLS
Internet-Draft
Intended status: Informational
Expires: 14 August 2025

P. Yang
Ant Group
C. Peng
Wuhan University
J. Hu
Infosec
S. Sun
Goodix

10 February 2025

Hybrid Post-quantum Key Exchange SM2-MLKEM for TLSv1.3
draft-yang-tls-hybrid-sm2-mlkem-01

Abstract

This document specifies how to form a hybrid key exchange with CurveSM2 and MLKEM in Transport Layer Security (TLS) protocol version 1.3.

Related IETF drafts include [hybrid] and [ecdhe-mlkem].

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 14 August 2025.

Copyright Notice

Table of Contents

1. Introduction 2
1.1. The SM2 Elliptic Curve 3
1.2. Terminology 3
2. Hybrid Key Exchange Scheme Definitions 3
2.1. TLS Versions 3
2.2. CurveSM2 3
2.3. Hybrid Key Exchange 4
2.3.1. Hello Messages 4
2.3.2. Key Scheduling 5
3. IANA Considerations 5
4. Security Considerations 6
5. References 6
5.1. Normative References 6
5.2. Informative References 7
Appendix A. Contributors 7
Authors' Addresses 8

1. Introduction

This document introduces one new NamedGroup and related key exchange scheme in TLSv1.3 protocol. This NamedGroup is used in the Supported Groups extension during the handshake procedure of TLSv1.3, to achieve a hybrid key exchange in combination with the post-quantum key exchange algorithm ML-KEM768 ([FIPS203]):

```
NamedGroup curveSM2MLKEM768 = { XX };
```

This new NamedGroup uses an elliptic curve called curveSM2 which is defined in SM2 related standards. Those standards are either published by international standard organizations or by Chinese standard organizations. Please read Section 1.1.

Since IANA has not assigned a value for the newly introduced NamedGroup item, a reserved value for private usage is temporarily used in this document at current stage. This value is for testing purpose only.

```
NamedGroup curveSM2MLKEM768 = { 0xFEFE };
```

1.1. The SM2 Elliptic Curve

SM2, ISO/IEC 14888-3:2018 [ISO-SM2] (as well as in [GBT.32918.2-2016]) is a set of elliptic curve based cryptographic algorithms including digital signature, public key encryption and key exchange scheme. In this document, only the SM2 elliptic curve is involved, which has already been added assigned by IANA.

Please read Section 2.2 for more information.

1.2. Terminology

Although this document is not an IETF Standards Track publication it adopts the conventions for normative language to provide clarity of instructions to the implementer, and to indicate requirement levels for compliant TLSv1.3 implementations.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Hybrid Key Exchange Scheme Definitions

2.1. TLS Versions

The new supported group item and related key exchange scheme defined in this document are only applicable to TLSv1.3.

Implementations of this document MUST NOT apply this supported group or key exchange scheme to any older versions of TLS.

2.2. CurveSM2

The hybrid key exchange scheme defined in this document uses a fixed elliptic curve parameter set defined in [GBT.32918.5-2016]. This curve has the name curveSM2.

As per [RFC8998], the SM2 elliptic curve ID used in the Supported Groups extension is defined as:

```
NamedGroup curveSM2 = { 41 };
```

Implementations of the hybrid key exchange mechanism defined in this document MUST conform to what [GBT.32918.5-2016] requires, that is to say, the only valid elliptic curve parameter set for SM2 signature algorithm (a.k.a curveSM2) is defined as follows:

```
curveSM2: a prime field of 256 bits

y^2 = x^3 + ax + b

p  = FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF
     FFFFFFFF 00000000 FFFFFFFF FFFFFFFF
a  = FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF
     FFFFFFFF 00000000 FFFFFFFF FFFFFFFC
b  = 28E9FA9E 9D9F5E34 4D5A9E4B CF6509A7
     F39789F5 15AB8F92 DDBCBD41 4D940E93
n  = FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF
     7203DF6B 21C6052B 53BBF409 39D54123
Gx = 32C4AE2C 1F198119 5F990446 6A39C994
     8FE30BBF F2660BE1 715A4589 334C74C7
Gy = BC3736A2 F4F6779C 59BDCEE3 6B692153
     D0A9877C C62A4740 02DF32E5 2139F0A0
```

The above elliptic curve parameter set is also previously defined in [RFC8998].

2.3. Hybrid Key Exchange

2.3.1. Hello Messages

The use of the hybrid named group defined by this document is negotiated during the TLS handshake with information exchanged in the Hello messages.

The main procedure follows what [hybrid] defines. That is to say, the non-post-quantum part (a.k.a. the ECDHE part) of the hybrid key exchange is based on standard ECDH with curveSM2.

2.3.1.1. ClientHello

To use the hybrid named group curveSM2MLKEM768 defined by this document, a TLSv1.3 client MUST include ’curveSM2MLKEM768’ in the ’supported_groups’ extension of the ClientHello structure defined in Section 4.2.7 of [RFC8446].

Then the TLS client’s ’key_exchange’ value of the ’key_share’ extension is the concatenation of the curveSM2 ephemeral share and ML-KEM768 encapsulation key.

The ECDHE share is the serialized value of the uncompressed ECDH point representation as defined in Section 4.2.8.2 of [RFC8446]. The size of the client share is 1249 bytes (65 bytes for the curveSM2 public key and 1184 bytes for ML-KEM).

2.3.1.2. ServerHello

If a TLSv1.3 server receives a ClientHello message containing the hybrid named group curveSM2MLKEM768 defined in this document, it MAY choose to negotiate on it.

If so, then the server MUST construct its 'key_exchange' value of the 'key_share' extension as the concatenation of the server's ephemeral curveSM2 share encoded in the same way as the client share and an ML-KEM ciphertext encapsulated by the client's encapsulation key. The size of the server share is 1153 bytes (1088 bytes for the ML-KEM part and 65 bytes for curveSM2).

2.3.2. Key Scheduling

According to [hybrid], the shared secret is calculated in a 'concatenation' approach: the two shared secrets are concatenated together and used as the shared secret in the standard TLSv1.3 key schedule.

Thus for curveSM2MLKEM768, the shared secret is the concatenation of the ECDHE and ML-KEM shared secret. The ECDHE shared secret is the x-coordinate of the ECDH shared secret elliptic curve point represented as an octet string as defined in Section 7.4.2 of [RFC8446]. The size of the shared secret is 64 bytes (32 bytes for each part).

Both client and server MUST calculate the ECDH part of the shared secret as described in Section 7.4.2 of [RFC8446].

As already described in [RFC8998], SM2 is actually a set of cryptographic algorithms including one key exchange protocol which defines methods such as key derivation function, etc. This document does not use an SM2 key exchange protocol, and an SM2 key exchange protocol SHALL NOT be used in the hybrid key exchange scheme defined in Section 2.3. Implementations of this document MUST always conform to what TLSv1.3 [RFC8446] and its successors require about the key derivation and related methods.

3. IANA Considerations

IANI has not assigned a value for the name 'curveSM2MLKEM768' yet. One suggestion from IANA expert is to use a temporary value reserved for private usage at current stage. Thus implementations can move forward to test the interoperability. So the value in the following table MUST NOT used in any production environment. The temporary value is as follows:

Value	Description	DTLS-OK	Recommended	Reference
0xFEFE	curveSM2MLKEM768	No	No	this RFC

Table 1

After IANA assigns the real value. The above description should be changed to:

IANA has assigned the value XX with the name ’curveSM2MLKEM768’, to the "TLS Supported Groups" registry:’

Value	Description	DTLS-OK	Recommended	Reference
XX	curveSM2MLKEM768	No	No	this RFC

Table 2

4. Security Considerations

At the time of writing, there are no security issues have been found for relevant algorithms.

5. References

5.1. Normative References

[FIPS203] National Institute of Standards and Technology, "Module-Lattice-Based Key-Encapsulation Mechanism Standard", DOI 10.6028/nist.fips.203, August 2024, <https://doi.org/10.6028/nist.fips.203>.

[ISO-SM2] International Organization for Standardization, "IT Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms", ISO ISO/IEC 14888-3:2018, November 2018, <https://www.iso.org/standard/76382.html>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[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/info/rfc8446>.

[RFC8998] Yang, P., "ShangMi (SM) Cipher Suites for TLS 1.3", RFC 8998, DOI 10.17487/RFC8998, March 2021, <https://www.rfc-editor.org/info/rfc8998>.

5.2. Informative References

[ecdhe-mlkem] Kris Kwiatkowski, Panos Kampanakis, Bas Westerbaan, Douglas Stebila, "Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3", Work in Progress, Internet-Draft , 24 December 2024, <https://datatracker.ietf.org/doc/html/draft-kwiatkowski-tls-ecdhe-mlkem-03>.

[GBT.32918.2-2016] Standardization Administration of China, "Information security technology --- Public key cryptographic algorithm SM2 based on elliptic curves --- Part 2: Digital signature algorithm", GB/T 32918.2-2016, 1 March 2017, <http://www.gmbz.org.cn/upload/2018-07-24/1532401673138056311.pdf>.

[GBT.32918.5-2016] Standardization Administration of China, "Information security technology --- Public key cryptographic algorithm SM2 based on elliptic curves --- Part 5: Parameter definition", GB/T 32918.5-2016, 1 March 2017, <http://www.gmbz.org.cn/upload/2018-07-24/1532401863206085511.pdf>.

[hybrid] Stebila, D., Fluhrer, S., and S. Gueron, "Hybrid key exchange in TLS 1.3", Work in Progress, Internet-Draft , 7 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design-11>.

Appendix A. Contributors

Place Holder
Ant Group
place.holder@antfin.com

Authors' Addresses

Paul Yang
Ant Group
A Space, No. 569 Xixi Road,
Hangzhou
310000
China
Phone: +86-571-2688-8888
Email: kaishen.yy@alipay.com

Cong Peng
Wuhan University
Dongxihu District
Wuhan
430000
China
Phone: +86-186-7403-6424
Email: cpeng@whu.edu.cn

Jin Hu
Infosec
Haidian District
Beijing
100096
China
Phone: +86-158-7172-6539
Email: hujin@infosec.com.cn

Shine Sun
Goodix
No.1 Meikang Road,Futian District
Shenzhen
518000
China
Phone: +86-138-7138-9521
Email: sunjinlong@goodix.com