HPKE Publication, Kept Efficient
Internet-Draft
Intended status: Standards Track
Expires: 10 May 2026

R. Barnes
Cisco
D. Connolly
Selkie Cryptography

6 November 2025

Post-Quantum and Post-Quantum/Traditional Hybrid Algorithms for HPKE
draft-ietf-hpke-pq-03

Abstract

Updating key exchange and public-key encryption protocols to resist attack by quantum computers is a high priority given the possibility of "harvest now, decrypt later" attacks. Hybrid Public Key Encryption (HPKE) is a widely-used public key encryption scheme based on combining a Key Encapsulation Mechanism (KEM), a Key Derivation Function (KDF), and an Authenticated Encryption with Associated Data (AEAD) scheme. In this document, we define KEM algorithms for HPKE based on both post-quantum KEMs and hybrid constructions of post-quantum KEMs with traditional KEMs, as well as a KDF based on SHA-3 that is suitable for use with these KEMs. When used with these algorithms, HPKE is resilient with respect to attacks by a quantum computer.

About This Document

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

The latest revision of this draft can be found at https://hpkewg.github.io/hpke-pq/draft-barnes-hpke-pq.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-hpke-pq/.

Discussion of this document takes place on the HPKE Publication, Kept Efficient mailing list (mailto:hpke@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/hpke. Subscribe at https://www.ietf.org/mailman/listinfo/hpke/.

Source for this draft and an issue tracker can be found at https://github.com/hpkewg/hpke-pq.

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 10 May 2026.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

A cryptographically relevant quantum computer may or may not exist as of this writing. The conventional wisdom, however, is that if one does not already, then it likely will within the lifetime of information that is cryptographically protected today. Such a computer would have the ability to infer decapsulation keys from encapsulation keys used for traditional KEMs, e.g., KEMs based on Diffie-Hellman over finite fields or elliptic curves. And it would be able to do this not just for data encrypted after the creation of the computer, but also for any information observed by the attacker previously, and stored for later decryption. This is the so-called "harvest now, decrypt later" attack.

It is thus a high priority for many organizations right now to migrate key exchange technologies to use "post-quantum" (PQ) algorithms, which are resistant to attack by a quantum computer [PQCE]. Since these PQ algorithms are relatively new, there is also interest in hybrid constructions combining PQ algorithms with traditional KEMs, so that if the PQ algorithm fails, then the traditional algorithm will still provide security, at least against classical attacks.

Hybrid Public Key Encryption (HPKE) is a widely-used public key encryption scheme based on combining a Key Encapsulation Mechanism (KEM), a Key Derivation Function (KDF), and an Authenticated Encryption with Associated Data (AEAD) scheme [HPKE]. It is the foundation of the Messaging Layer Security (MLS) protocol, the Oblivious HTTP protocol, and the TLS Encrypted ClientHello extension [RFC9420] [RFC9458] [TLS-ECH].

This document defines a collection of PQ and post-quantum/traditional (PQ/T) KEM algorithms for HPKE, which allows HPKE to provide post-quantum security, as discussed in Section 7:

* ML-KEM-512

* ML-KEM-768

* ML-KEM-1024

* X25519 + ML-KEM-768

* P-256 + ML-KEM-768

* P-384 + ML-KEM-1024

ML-KEM, X25519, and P-256/P-384 are defined in [FIPS203], [RFC7748], and [FIPS186], respectively.

This selection of KEM algorithms was chosen to provide a reasonably consolidated set of algorithms (in the interest of broad interoperability), while still allowing HPKE users flexibility along a few axes:

* Pure PQ vs. PQ/T hybrid

* CFRG-defined vs. NIST-defined elliptic curves

* Different security levels (NIST category 3 vs. category 5)

We also define HPKE KDF algorithms based on the SHA-3 family of hash functions. SHA-3 is used internally to ML-KEM, and so it could be convenient for HPKE users using the KEM algorithms in this document to rely solely on SHA-3.

2. Conventions and Definitions

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.

We generally use the terminology defined in the HPKE specification [HPKE].

There are two meanings of "hybrid" in this document. In the context of "hybrid public key encryption", it refers to the combination of an asymmetric KEM operation and a symmetric AEAD operation. In the context of "PQ/T hybrid", refers to the combination of PQ and traditional KEMs. For clarity, we always use "HPKE" for the former, and "PQ/T hybrid" for the latter.

3. ML-KEM

The NIST Module-Lattice-Based Key-Encapsulation Mechanism is defined in [FIPS203]. In this section, we define how to implement the HPKE KEM interface using ML-KEM.

The HPKE DeriveKeyPair function uses the SHAKE256 KDF (see Section 5) to derive an ML-KEM decapsulation key in the 64-byte seed format, then uses the function ML-KEM.KeyGen_internal from [FIPS203] to compute the corresponding encapsulation key.

```
def expandDecapsKey(dk):
    d = dk[:32]
    z = dk[32:]
    (ek, expanded_dk) = ML-KEM.KeyGen_internal(d, z)
    return (expanded_dk, ek)

def DeriveKeyPair(ikm):
    dk = SHAKE256.LabeledDerive(ikm, "DeriveKeyPair", "", 64)
    (_expanded_dk, ek) = expandDecapsKey(dk)
    return (dk, ek)
```

As discussed in [HPKE], the value of suite_id used within LabeledDerive identifies the KEM in use:

* ML-KEM-512: KEM\x00\x40 (hex: 4b454d0040)

* ML-KEM-768: KEM\x00\x41 (hex: 4b454d0041)

* ML-KEM-1024: KEM\x00\x42 (hex: 4b454d0042)

The GenerateKeyPair function simply calls ML-KEM.KeyGen_internal with a pseudorandom dk value. As long as the bytes supplied by random meet the randomness requirements of [FIPS203], this corresponds to the ML-KEM.KeyGen function, with the distinction that the decapsulation key is returned in seed format rather than the expanded form returned by ML-KEM.KeyGen.

```
def GenerateKeyPair():
    dk = random(64)
    (_expanded_dk, ek) = expandDecapsKey(dk)
    return (dk, ek)
```

The SerializePublicKey, DeserializePublicKey, SerializePrivateKey, and DeserializePrivateKey functions are both the identity function, since the ML-KEM already uses fixed-length byte strings for public encapsulation keys. The length of the byte string is determined by the ML-KEM parameter set in use.

The Encap function corresponds to the function ML-KEM.Encaps in [FIPS203], where an ML-KEM encapsulation key check failure causes an HPKE EncapError.

The Decap function corresponds to the function ML-KEM.Decaps in [FIPS203], where any of an ML-KEM ciphertext check failure, decapsulation key check failure, or hash check failure causes an HPKE DecapError. To be explicit, we derive the expanded decapsulation key from the 64-byte seed format and invoke ML-KEM.Decaps with it:

```
def Decap(enc, skR):
    (expanded_dk, _ek) = expandDecapsKey(skR)
    return ML-KEM.Decaps(expanded_dk, enc)
```

The constants Nsecret and Nsk are always 32 and 64, respectively. The constants Nenc and Npk depend on the ML-KEM parameter set in use; they are specified in Table 2.

> Note: While this document defines an HPKE KEM for ML-KEM-512 in the interest of completeness, implementors should generally prefer ML-KEM-768 or ML-KEM-1024, or the PQ/T hybrids described in Section 4. According to current cryptanalysis, ML-KEM-512 provides security compatible with a 128-bit security level (or NIST security category 1). Given the relative novelty of ML-KEM, however, there is some concern that new cryptanalysis might reduce the security level of ML-KEM-512. Use of ML-KEM-768 or ML-KEM-1024 acts as a hedge against cryptanalysis of ML-KEM that removes some bits of security but is not catastrophic, at a modest performance penalty.

4. Hybrid KEMs with ECDH and ML-KEM

[CONCRETE] defines a collection of concrete PQ/T hybrid KEMs. These KEMs combine ML-KEM with a traditional ECDH group:

MLKEM768-P256: ML-KEM-768 and P-256
MLKEM768-X25519: ML-KEM-768 and X25519
MLKEM1024-P384: ML-KEM-1024 and P-384

These KEMs satisfy the KEM interface defined in [GENERIC]. This interface maps to the KEM interface in [HPKE] in the following way:

* The HPKE DeriveKeyPair function uses the SHAKE256 KDF (see Section 5) to derive a 32-byte seed for the hybrid KEM, then uses the function DeriveKeyPair from [GENERIC] to compute the key pair for the hybrid KEM. The input to this function SHOULD be at least 32 bytes long.

```
def DeriveKeyPair(ikm):
    seed = SHAKE256.LabeledDerive(ikm, "DeriveKeyPair", "", 32)
    return KEM.DeriveKeyPair(seed)
```

* The GenerateKeyPair, Encap, and Decap algorithms are identical.

* The SerializePublicKey, DeserializePublicKey, SerializePrivateKey, and DeserializePrivateKey algorithms are the identity, since encapsulation and decapsulation keys are already fixed-length byte strings.

* The constants map as follows:

  - Nsecret = Nss

  - Nenc = Nct

  - Npk = Nek

  - Nsk = Ndk

As discussed in [HPKE], the value of suite_id used within LabeledDerive identifies the KEM in use:

* MLKEM768-P256: KEM\x00\x50 (hex: 4b454d0050)

* MLKEM768-X25519: KEM\x64\x7a (hex: 4b454d647a)

* MLKEM1024-P384: KEM\x00\x51 (hex: 4b454d0051)

5. Single-Stage KDFs

This section defines HPKE KDFs for eXtendable Output Functions (XOF) based on Keccak. SHAKE is defined as part of the SHA-3 specification [FIPS202]. The related TurboSHAKE XOFs are defined in [I-D.irtf-cfrg-kangarootwelve].

The Derive() function for SHAKE is as follows, where <SIZE> is either 128 or 256:

```
def SHAKE<SIZE>.Derive(ikm, L):
    return SHAKE<SIZE>(M = ikm, d = 8*L)
```

The Derive() function for TurboSHAKE is as follows, where <SIZE> is either 128 or 256:

```
def TurboSHAKE<SIZE>.Derive(ikm, L):
    return TurboSHAKE<SIZE>(M = ikm, D = 0x1f, L)
```

The Nh values for the KDFs defined in this section are listed in Table 1.

Value	KDF	Nh	Two-Stage	Reference
0x0010	SHAKE128	32	N	RFC XXXX
0x0011	SHAKE256	64	N	RFC XXXX
0x0012	TurboSHAKE128	32	N	RFC XXXX
0x0013	TurboSHAKE256	64	N	RFC XXXX

Table 1: Single-Stage KDF IDs

[[RFC EDITOR: Please change "XXXX" above to the RFC number assigned to this document.]]

6. Selection of AEAD Algorithms

As discussed in Section 2.1 of [PQCE], the advent of quantum computers does not necessarily require changes in the AEAD algorithms used in HPKE. However, some compliance regimes call for the use of AEAD algorithms with longer key lengths, for example, the AES-256-GCM or ChaCha20Poly1305 algorithms registered for HPKE instead of AES-128-GCM.

7. Security Considerations

As discussed in the HPKE Security Considerations, HPKE is an IND-CCA2 secure public-key encryption scheme if the KEM it uses is IND-CCA secure. It follows that HPKE is IND-CCA2 secure against a quantum attacker if it uses a KEM that provides IND-CCA security against a quantum attacker, i.e., a PQ KEM. The KEM algorithms defined in this document provide this level of security. ML-KEM itself is IND-CCA secure, and the IND-CCA security of the hybrid constructions used in this document is established in [CONCRETE].

Another security property that is salient in some use cases is "key binding". In [CDM23], these notions are referred to with the shorthand X-BIND-P-Q. The most salient for protocol design provide assurances similar to those provided by transcript hashing in protocols like TLS:

LEAK-BIND-K-PK: If the sender and receiver have the same key (K,

shared_secret above), then there is only one encapsulation key (PK, pk) that could have produced it, even if the decapsulation key is leaked to an attacker after the encryption has been done.

LEAK-BIND-K-CT: If the sender and receiver have the same key (K, shared_secret above), then there is only one KEM ciphertext (CT, enc) that could have produced it, even if the decapsulation key is leaked to an attacker after the encryption has been done.

DHKEM and ML-KEM meet these properties, as shown in [CDM23]. The hybrid KEMs used in this document also provide these properties, as discussed in [GENERIC].

7.1. PQ Hybrid vs. Pure PQ

Assuming that ML-KEM is secure, either the PQ/T hybrid KEMs defined in Section 4 or the pure PQ KEMs defined in Section 3 provide security against a quantum attacker. Hybrid KEMs can be used to provide security against a non-quantum attacker in the event of failures with regard to the PQ algorithm, including both implementation flaws as well as new cryptanalysis. See [GENERIC] for further analysis of hybrid security properties.

7.2. Asymmetric-Key-Authenticated Modes of RFC9180

In the [RFC9180] version of HPKE, KEMs could optionally define the additional functions AuthEncap and AuthDecap. These functions allowed a sender to authenticate the message to the recipient without interaction.

The KEMs defined in this document do not support AuthEncap/AuthDecap and cannot be used to migrate uses of HPKE that rely on this mode. PSK-authenticated HPKE (Section 5.1.2 of [HPKE]) or digital signatures may be suitable alternatives.

8. IANA Considerations

This section requests that IANA perform three actions:

1. Update the entries in HPKE KEM Identifiers registry corresponding to ML-KEM algorithms.

2. Add entries to the HPKE KEM Identifiers registry for the PQ/T hybrid KEMs defined in this document.

3. Add entries to the HPKE KDF Identifiers registry for the SHA-3 KDFs defined in this document.

8.1. Updated ML-KEM KEM Entries

IANA is requested to replace the entries in the HPKE KEM Identifiers registry for values 0x0040, 0x0041, and 0x0042 with the following values:

Value	KEM	Nsecret	Nenc	Npk	Nsk	Auth	Reference
0x0040	ML-KEM-512	32	768	800	64	no	RFCXXXX
0x0041	ML-KEM-768	32	1088	1184	64	no	RFCXXXX
0x0042	ML-KEM-1024	32	1568	1568	64	no	RFCXXXX

Table 2: Updated ML-KEM entries for the HPKE KEM Identifiers table

The only change being made is to update the "Reference" column to refer to this document.

8.2. PQ/T Hybrid KEM Entries

IANA is requested to replace the entry for the value 0x647a and add two entries for values 0x0050 and 0x0051 with the following values:

Value	KEM	Nsecret	Nenc	Npk	Nsk	Auth	Reference
0x0050	MLKEM768-P256	32	1153	1249	32	no	RFCXXXX
0x0051	MLKEM1024-P384	32	1665	1665	32	no	RFCXXXX
0x647a	MLKEM768-X25519	32	1120	1216	32	no	RFCXXXX

Table 3: PQ/T hybrid entries for the HPKE KEM Identifiers table

8.3. SHA-3 KDF Entries

IANA is requested to add the values listed in Table 1 to the HPKE KDF Identifiers registry.

9. References

9.1. Normative References

[CONCRETE] Connolly, D. and R. Barnes, "Concrete Hybrid PQ/T Key Encapsulation Mechanisms", Work in Progress, Internet-Draft, draft-irtf-cfrg-concrete-hybrid-kems-02, 6 November 2025, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-concrete-hybrid-kems-02>.

[FIPS186] "Digital Signature Standard (DSS)", National Institute of Standards and Technology (U.S.), DOI 10.6028/nist.fips.186-5, February 2023, <https://doi.org/10.6028/nist.fips.186-5>.

[FIPS202] "SHA-3 standard :: permutation-based hash and extendable-output functions", National Institute of Standards and Technology (U.S.), DOI 10.6028/nist.fips.202, 2015, <https://doi.org/10.6028/nist.fips.202>.

[FIPS203] "Module-lattice-based key-encapsulation mechanism standard", National Institute of Standards and Technology (U.S.), DOI 10.6028/nist.fips.203, August 2024, <https://doi.org/10.6028/nist.fips.203>.

[GENERIC] Connolly, D., Barnes, R., and P. Grubbs, "Hybrid PQ/T Key Encapsulation Mechanisms", Work in Progress, Internet-Draft, draft-irtf-cfrg-hybrid-kems-07, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-hybrid-kems-07>.

[HPKE] Barnes, R., Bhargavan, K., Lipp, B., and C. A. Wood, "Hybrid Public Key Encryption", Work in Progress, Internet-Draft, draft-ietf-hpke-hpke-02, 4 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-hpke-hpke-02>.

[I-D.irtf-cfrg-kangarootwelve] Viguier, B., Wong, D., Van Assche, G., Dang, Q., and J. Daemen, "KangarooTwelve and TurboSHAKE", Work in Progress, Internet-Draft, draft-irtf-cfrg-kangarootwelve-17, 21 February 2025, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-kangarootwelve-17>.

[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/rfc/rfc2119>.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <https://www.rfc-editor.org/rfc/rfc7748>.

[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/rfc/rfc8174>.

9.2. Informative References

[CDM23] Cremers, C., Dax, A., and N. Medinger, "Keeping Up with the KEMs: Stronger Security Notions for KEMs and automated analysis of KEM-based protocols", 2023, <https://eprint.iacr.org/2023/1933.pdf>.

[PQCE] Banerjee, A., Reddy.K, T., Schoinianakis, D., Hollebeek, T., and M. Ounsworth, "Post-Quantum Cryptography for Engineers", Work in Progress, Internet-Draft, draft-ietf-pquip-pqc-engineers-14, 25 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-engineers-14>.

[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/rfc/rfc9180>.

[RFC9420] Barnes, R., Beurdouche, B., Robert, R., Millican, J., Omara, E., and K. Cohn-Gordon, "The Messaging Layer Security (MLS) Protocol", RFC 9420, DOI 10.17487/RFC9420, July 2023, <https://www.rfc-editor.org/rfc/rfc9420>.

[RFC9458] Thomson, M. and C. A. Wood, "Oblivious HTTP", RFC 9458, DOI 10.17487/RFC9458, January 2024, <https://www.rfc-editor.org/rfc/rfc9458>.

[TestVectors] "HPKE Test Vectors for Post-Quantum Algorithms", 2025, <https://github.com/hpkewg/hpke-pq/blob/main/test-vectors.json>.

[TLS-ECH] Rescorla, E., Oku, K., Sullivan, N., and C. A. Wood, "TLS Encrypted Client Hello", Work in Progress, Internet-Draft, draft-ietf-tls-esni-25, 14 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-esni-25>.

Appendix A. Test Vectors

Each section below contains test vectors for a single selection of HPKE algorithms and contains the following values:

1. Configuration information and private key material: This includes the mode, info string, HPKE ciphersuite identifiers (kem_id, kdf_id, aead_id), and all sender and recipient key material. For each role S or R, (sender and recipient, respectively) key pairs are generated as (skX, pkX) = DeriveKeyPair(ikmX). Each key pair (skX, pkX) is written in its serialized form, where skXm = SerializePrivateKey(skX) and pkXm = SerializePublicKey(pkX). For the PSK mode, the shared PSK and PSK identifier are also included.

2. Context creation intermediate values: This includes the KEM outputs enc and shared_secret used to create the context, as well as the context values key, base_nonce, and exporter_secret.

3. Encryption test vectors: A fixed plaintext message is encrypted using different sequence numbers and AAD values using the context computed in (2). Each test vector lists the sequence number and corresponding nonce computed with base_nonce, the plaintext message pt, AAD aad, and output ciphertext ct.

4. Export test vectors: Several exported values of the same length with differing context parameters are computed using the context computed in (2). Each test vector lists the exporter_context, output length L, and resulting export value.

These test vectors are also available in JSON format at [TestVectors].

A.1. ML-KEM-768, HKDF-SHA256, AES-128-GCM

A.1.1. Base Setup Information

```
mode: 0
kem_id: 65
kdf_id: 1
aead_id: 1
info: 3466363436353230366636653230363132303437373236353633363936313665
      3230353537323665
ikmR: 19aaaad124d9e3a3645aa45cb7f5b6db21f54832f659e0b01d54b630eb8fbb5d
      9738866d84c4e597178ae106038a6a6b475ed76cad81a5daa312c3f838a2edaf
pkRm: fba8082d27891eb10fc349579dca26ba414831527d41e0841bb0154cc85436f0
      7ed2c3afed532dda70420c0c9c45a879f2774be124824c762140f11191503a24
      03a5fb353a4220b7ff9b854be523ad76031b46736f3a5021f3bd61eb9ce1931e
      5d8938a60357fcac41fc900d2d5566a9233f56c663c068b3e8e759df5b461d14
      2ec5e55b4e568894ac0a8647ccfba4b91ba9887cc1bf4bac5b31bac6586a2fa4
      7046f95bb71a0b231c7bbca1694e895711b612ae004b0c4bd3a3ada3198c2882
      0dc38c47438f5c1a338be3945a8a8b0a986dd7f6682f58c3b3d870bcdcbf6d35
      024e453d0af106c0fc1ea8549083e59d43bb867e04837cf635ae935f4dd5a30b
```

```
        7c87fa6b8167b2113c9c5fade1c59d685432b96a1772b1c98c39fcf44b13837c
        f1a982721454c8d64b9ed72e137834773b18d64bc57786941087109e8c3f5f74
        4afa3426aee52f19dc53656274d706a3f6b149bbe05a465b69cf484d8c76b67f
        38c8a1b2744fac8136e7991fabc9d296b591778f48a703a705223e1a794158b9
        1ccc78a90a3e1823059539519bf96803e7b20d99ac7206a6c93b8b859734c140
        c334261948e45e275517880b6f7b82bae01c256c633f1bf0758d2a958747695c
        d155922b29ea6b444e0c8dab9b3937f57d2c421d539a1356546221b77dc288ce
        d2f32c25744a8673c268e34e75e0cc3dc39807622754c1a3000b55446056f035
        4c119a487a67139c087768cb889729a0cf30937c89b42b65b0859337b2e17d39
        dcc65a2cad8f08c6f0192472665346d32e48f492b9931e33aa458b385c96b04d
        0614946451b7c8ebae65884d430a63199316ca997caa689911a999f41451dd62
        59e205a533d52912d0c8a8b30fcc277c0e411afa21ae98a25c2ff51d56494215
        83baedb2902db177e7bb267bdc56a4db1a82a097e0d440f3b938759ca4636990
        09cab3a5069b51a1037c81654eda9371e028ff00bc09a444dcc38f1bcb25974c
        413903252ce93999ab70b889b5c39a34d0e40f07f5485759b8cd36bca2d9c27b
        a5633ea44d8a66178ccb917b6c099fa2944d6a2354c08faf5316bda183d95045
        cb641d79bc98d7b89cbc93765f72b5e4cc1195872a35251edf229aecf92305e9
        317f3b5dcdb54ad377ccc6e5798bd18c1f587f67e932bf812ae4606bfc711831
        524d86db28956509cfdc503a9564d0561c994cca3b15b4fab316d1c48388f364
        0163a693519040c3ccdd69219b17b8ae73518ee92d99812a1c4b3af1b70736bc
        1e0269b9a8e361ec8547800a144abb2b4e269167f41dee76afd459451ae06069
        88a574f6afde2335c14216b628aad1d76d9020a49f366e8e14bc97785f40f438
        717a6f5fb29a2fec936af13cc7eaba4b52c89edbaf54d340d05a8f2ecbafd750
        08096506fa6b91f6815a3805bcc0d064dca0101bf17c8ce9ba8a951f9e259128
        6432f5591e949289eac495d68780f1d1b5855827a6316c2071af4d0510faea93
        81c580131ba6d45c51b568633255009a366e33a40a1935894e76c6a81c16054a
        26e8760fcb9c6d63e33b891c400c69aaf61c125288b73f5053e74c2a00a27636
        61141c097ebc7ac5bec419dac87133f40499557c2262aacb366a111875f4f11d
        300e82e74147801e16b36b517e05e5de2dd13ca38ef99495fc4658be484f8d7e
  skRm: 934ba54b52a6f432074ea5f067f330d82a4da438b3aad1c93effa038b9454fd7
        72311b43acd502f94bbbad2cd16cb1d07418f7e48e74c816ca83b4d5d4be5752
  enc: 7319e22bc7ef6d39ed28c489b24534c6df8190cb62308380ebe500897ad62d00c
       89bc1af4b4a5a1ab1c444b3728ff512cca5656cd81f6569599ce47477986dc79c
       8855fb2475e48e29f16a34b10b76f13fca41c2f8ef37d1e8ef5762efce11f3b55
       2aa94f4c68714c813a370b1d4bde0e8fc1fbc61e63a4e3a4b971e4b9928610bfa
       bfbb8f248fba8c481ab175a9b64eb8ca8743be7bf7ff754a5059444465468c1c5
       3abdfe8cdce9256d89ccbf3dc3e763118a528a673257f8da74b61281467a3293d
       c61bb3a98bb123494e6abdb82334ecccc079a85ef6f31c59b55e6955b3100488d
       13558db7e936b4d58262af3173720076028cb4ef51d63dd59d6cc8eb64fed4027
       8ff81b6336f6953ae587c8907f9486be2e074e88de72ffc81ccb9d5f3007cf4b5
       1246c5eb2479600debb3c9c3c7ca035102ef25bc7c9049b7b4a1d4443338516db
       08729123ff522ab7b9651a9e18a64dc552ed822fa2d38afa1293184e4fd0f5f57
       881018757610260ffc29abe5e9125a3b79e91b81bb9d6c8afd089116c27713738
       cc98547d3e84fa81db8bbcc3a90736781b38b011f9c640c4e40e94da11bef7e10
       04a9f021d2ad8701adcdf207c76e0540af82fa74573ab6d2c46eeea060729b85e
       8b44a1a41d33f50ca79e6d5a40ef3474ac8c40ee4e4d607f4ab0d222b3b710f05
       c42b74514375dc564385703b2c4abc857e7842f6964666997e088af9a178e65af
       da20a70fd88ac0bd2efeeeb4d8ad1355c19212832fa943ecef03bd1a9cf03a7f5
```

```
      f1b0e8455cbe16488cecb0a90fac3a88b58441a51892de677b22c121942bbd6af
      63073691315110f3d028718891237566badd09ea6dcaf905f02c5a483346a2ef0
      ec3ea6571d2a0cf57f26680c398a82f7c59c14237f79d628d7cf89fbe1b5ef6c0
      b1ae455f535937eadcc8742940c695336306a955627019d9201ee7f68c62c7f34
      f4e0901150d27025a50c69a08664cfe74b9c8d9f8c67ead1c606c10c613a1ee50
      86a8f8802dfa05fc31d684b9a4b64b665ccd3ad75e7cc384c15064d5114a38dfe
      f5070b7cbbe306a45d480fad64f2cf44641d7b61ee24ac59994ac87aa95c2b07a
      d8aceb7ca0f7dffc54e4611159c14888216abce6e9c57c3b670cfea091962c4ee
      d37b2c5aaf48ae7e09315950349bd0baacd377442d3bc6fbeb5afaa19bd1a6e26
      6a5aa7ae2737d0eec4d2e1a17793dc3364c5d79e8cb048c0cc638bd9a019833bf
      780803da5eabea8a05cca08defad47310d898c901a13f1ae61e9bf917e9033851
      85dc53cf085e8e80e4b7fb91d600f928478d01f552105d0f08e7cc56276930cf0
      819b643acd0080de144647e9d19a137385fd17c74c8e406129a178fb2db567c44
      1ea3fc00f3ed666fbc99301e8c7c21163a466075eed818fa19f3c5b9a3b89c346
      af5ce2b8dc65bbbf19a47d676ceb0a4422ccb395ab959a247da8cd679555c7d4a
      7d1b57cadf8184a5ad3f0e961dcf7b6bd83f420b3e8ef03195703f3549b7e891f
      9db6fe51e8d03e42ec73e4b222ca983
  shared_secret: ab72523ee276c1b5653bf19ef201178a312297b47b813b271c68b89
                 aabcf52a1
  key: 40d9ae28dd3a899e48a737dea17f4071
  base_nonce: e263b670fc7cc4ec31f0c733
  exporter_secret: ee31d2118ae0c4d92d5011a6954ae932bb013925ed485c9d2d22b
                   70428f1c9ed
```

A.1.1.1. Encryptions

```
  sequence number: 0
  pt: 34323635363137353734373932303639373332303734373237353734363832633
      230373437323735373436383230363236353631373537343739
  aad: 436f756e742d30
  nonce: e263b670fc7cc4ec31f0c733
  ct: c7cc1822fee767a90cde7b17f66f98acc96742159ceac9f9403c6a8f378411f4a1
      26124d3c267ed86389a670c69db9cf49b351ca29c4a5e2688ac6818a7761d9656d
      4bd0ae2634c7306b

  sequence number: 1
  pt: 34323635363137353734373932303639373332303734373237353734363832633
      230373437323735373436383230363236353631373537343739
  aad: 436f756e742d31
  nonce: e263b670fc7cc4ec31f0c732
  ct: 1fb9a4f62097c68343babbc54ce313909a181d22eeafe58ea2505087096e6ae3ed
      06144b7d68a0e37a1f6b6108b1553651cd7ac323ecce898f73df0b88c3787126d0
      9a459380d0ba6eb4

  sequence number: 2
  pt: 34323635363137353734373932303639373332303734373237353734363832633
      230373437323735373436383230363236353631373537343739
  aad: 436f756e742d32
```

```
  nonce: e263b670fc7cc4ec31f0c731
  ct: e49e7b7acae26ec13df7b5da4f7ee024002067eba64580ed61268167c8555de214
      f52ac3bdc07c234583e751533f5096506a23dddf132fc4bae4324e1e426da0b932
      f5cf999fd233ea59

  sequence number: 3
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d33
  nonce: e263b670fc7cc4ec31f0c730
  ct: 9c0de11cfa514489738dc7513fe547b622b7387f2e27e3b60c6b1ba2bfa6971b2f
      3a0718c9b5f50535a25113f9d561243d66b2ccfae742b9c46f9901506977dade26
      8ebf12711e7bff5a

  sequence number: 4
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d34
  nonce: e263b670fc7cc4ec31f0c737
  ct: 7c475fd52cb8b85ca923019509286eb7c21e8d388e1dba1d0e00b2d5eeb66468d2
      583e889aaebe3032cad13b2dc5afb0054140cb46248ae1a8a1f9bc3687926fb05f
      aa6223207e950c51

  sequence number: 5
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d35
  nonce: e263b670fc7cc4ec31f0c736
  ct: 49d42de2efd980171db50b9350cc2d6aa2aa2e6d7a0b6a822b9a78757482abff39
      76a2b59d0c0a0ab1d325758ee0957e299d1d415382dbd133344cefa5227c10a0df
      d51e6be4674671cd

  sequence number: 6
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d36
  nonce: e263b670fc7cc4ec31f0c735
  ct: cc53b4fbfbc53ddf35981ea026e0b706c571e5cc6d07398bef38fb40dcf129a4dd
      1c21ac432a1504f224f28b02fec5d63a64eb4985f4ec29bfe87aa786fefcb2668d
      aad455f5179c3af5

  sequence number: 7
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d37
  nonce: e263b670fc7cc4ec31f0c734
  ct: fc6e39b69727dee5792da4c71cdb1df372a1386e0ae3f113b895dbae8ce5a4b1ca
      ac9681017dbe25e3838b7e03311f2b2da40d41cfb1af0619c2ed2680d0d5d32e11
```

```
      1c9cbaebd1de8c25

  sequence number: 8
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d38
  nonce: e263b670fc7cc4ec31f0c73b
  ct: f868871ca3b3a38272b5843760420d6f43cad1e0c0dd6edf9b0b0cb08c6837745e
      b0ca2245982ab50685c23993af2411a82ec5d2b2de7e4c36c3867793bc53d5d3ff
      8510ed55aa76c941

  sequence number: 9
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d39
  nonce: e263b670fc7cc4ec31f0c73a
  ct: 49b9ddec6d460af9b6def49cdeada13f399a6f3a09ce211a431f0fc68d3cc817bc
      33f885475e57ddc75e85a2744d5c09197e204185c6854a9d444d90359a80337150
      57b9350036324a8d
```

A.1.1.2. Exported Values

```
  exporter_context: 70736575646f72616e646f6d30
  L: 32
  exported_value: 64f2184266a8c370cef38ec4f387dba0ae9fbe05d237ec515ce217
                  4bc85b2369

  exporter_context: 70736575646f72616e646f6d31
  L: 32
  exported_value: 1852e4a7396747d3e302cb1eeaed2b3b8307b477711cc9c8a82df3
                  6d5f0013bc

  exporter_context: 70736575646f72616e646f6d32
  L: 32
  exported_value: 8e35644489b6666c0aacf0c8ef1e106c2451dcd441887e35ff0d56
                  444f742e10

  exporter_context: 70736575646f72616e646f6d33
  L: 32
  exported_value: 30996075815e5a8c4074e16f33b621c6fc1e8cf7c4868ecf523d21
                  73b7b50abf

  exporter_context: 70736575646f72616e646f6d34
  L: 32
  exported_value: 2ee2d209f29f1ce4c2b3c5ea529ba5d92cd852efccdaa753a1e727
                  54974148a3
```

A.2. ML-KEM-1024, HKDF-SHA384, AES-256-GCM

A.2.1. Base Setup Information

```
  mode: 0
  kem_id: 66
  kdf_id: 2
  aead_id: 2
  info: 3466363436353230366636653230363132303437373236353633363936313665
        3230353537323665
  ikmR: 30f75d13c02f5eed4fe46696b45424e5dd3ef6109797d2f0ac661affabf16595
        853e623063b54d4569d99e9c8b8a64d34822faca8947fc5c00c3943a49b88c5d
  pkRm: d7673326e702e98a9db79aa259b3a384978015743ebfebaf181a6f8fc5778266
        78aea1a846cb1b87395be441146f501ba908cbd38904551abc56169b24ba6555
        57935e34b83ab869e2cc9bb00549fe3ca7cf8c59898212d3f2aa292a91c2497d
        22abaeedd330b42074af4baf321031bc05435a6353f281104415c494355983f9
        1f0f657182909512ab260e19018d7300aba33e09934851bba4c3d326a5c80a4c
        f96a11f4b191f226d80b62b1e093f6034b20710eb4728a377765ca157748b5b3
        2e315f3abc7582e69af1d1c78a44cc97a8ab8f2c103c66ab8aea2b25a861e8cb
        6ea07907e8734bd74420596081dfd14a7e57b5e650bdf0bccf22dc9636ec3743
        3a474eb6124e2c144bfcbf4e3a5a453125ecd208f9ec228fd96d929c958f67be
        29a98d0450a29cb468fbb58b6c273964abbc7bec9a2cf7a8be424a57379fa861
        a58e7baadeda270c723b42209fcd593462a75272850ba50129f63bb15270cd39
        623d69f7306c75a9297b6219ccaca21bca63e8a8c7709648db85827814f137ca
        032724c7ab659c8988dc9952fcc8ac6041bcea29ae51744c87799d0ab3358e63
        4890944595b3c5267ac1ccd473a85cbd0e1839218368457378a6e401eb257781
        d1370d1860657679de292c45884f8a995960e3af398c54539628ac785cafa1b4
        78e992976452e6a15c44827367dc14e6944422b5188c7a438a998b3f51944350
        237cac37d46bac8ad51be7fb4f9d60b27910920d2174fa27b5ff0cbdf1035300
        d6840cc71028ab4d46885acf21300da2867b8220e27b463e18bde80b8ba75754
        f9988c08181f154b402f3414832cba4a78a41a263949d46b44389ae9f4550718
        98a3637642b3511af302b4b522d801246494961f1c8369d62aa8106b254344a4
        902d0542cb71e1bdd974a1328315de962feb775b5478572bb12737901ff8f257
        b8752f05c3465b7400b60534866154d6e640ba5038ae5779c510adfd751dbb45
        28a89c8456d51196766ad69147ac73a65311a4c6442058e969e85c10985551da
        63017df11551d12bc0768c336a19ceba7790641092ab90b28a3c55b56d765966
        f5292a350010f3c6b206d0be3e2a21e57675fbcb758a44c44fd88c815535049b
        7abf7a6db8c8bae5f0b0e6c19e6b264e71678878bc024803c5d7e98f148039b2
        2c97963019622812e3086995982709d170a686cbfc5b099e0c07c11118c6a215
        49105a088abdb5a3a9e7d96f2ab02f55b66ba26aaa08921896c9b191cb4c8375
        17d8a73901d014cf543845d95d77c26ed49c78315911c05cbffdd046616a6bf1
        71347dfbbc45b6059253aaa93623f2157690a9073c4a9d05b76aa9d62dd53a78
        58e26970d97121ac824158a70df837b0560b691a0f0201316ecc50e6f7040e27
        8ba46050f8bcbe61eaccc58530b24567943384c15a550ea8853298ca69f01d19
        16976be74368833aff3680bf13b2a308ac426935a93b70cf0b31e8c87dff3a20
        29d947e861a27a829995a83948c00121f5ad6c48841594l801fbcbe4c461a176
        c35aa2922aa782b7b40042a560ebc39fa2f26813a47cc2b77e34265a56351552
        c0be52278e098aa38ea53eac2450b165762a53ac3ff39069d456507681eadc9f
```

```
        30cc3fba635e7c4426c5b85b6ed9139f12397d91a91e023de1c8aaf348a47803
        2eaf48650f68336b2687d564adbc5611ad1416f4401836a539389a68354a996f
        c2b850e718d9d4c57bf38dd9892b3110224d1c6f2c2b20da8a060dfc343ff153
        b2d3bd5e52ae106357dc7b490be82079800773502ef4024384a743c2ac9742b4
        2b9f5533eef9bb74f60f832470e029506d91b7dbdc44b5a05ff19c09bd903fa2
        8270a168a95ce6231f35bf79726050a697b146622c1c4fdcd2aede0570766c68
        998c5ed19b7832e108ae18a9f7088226923b59917cd9f62365768f629a13daea
        4cbde23531202433061414c846c0239d70d7ba26f83ce2dcc2e0db22b1f75120
        b104f776cb97f45655928ec3a32c260893c03c36e4d0ad6134cc47920f902731
        17931ef6b6268c803712d78fc9b3bd62148e5ec49546e5b624568c19638d2539
        38db039b31795a64818e0f915aec0a3ae8c752396346a2f9213aa80ce30364f7
        e810b508949d71bca5a3a806c9c5e57bb03d540b7df42fbfb210a31b36c0cb82
        0011fa80540512f7e37c3b0ca5f342f46065d64f132fe8dd137f27856a982419
  skRm: 1ac1cf1fdbb5a854937963f1d18537a461815522da648b94a607f8b5831962a1
        07a34caa9203ea0178cea9a2e89e9e52c2143423d22af331a72c9ce10a133fc2
  enc: 90d3bc233d3daad86ba35343ef9db886deb170dabc3c7751ed46fa11cec64b9ac
       f593beb26434d8a7d85c9113e2c09f4eeaf76c40d91c8dc54b1d21cdf4c5eea89
       d218919baf2e3dee51d6ef2f5a7841afebb408a9f4525b42d0d8b27de847d1501
       6e9d60c6b4e9c627aa6b8f4cc22eb38b2d801f02ad143eebcc65e31414f1d7c0b
       a5873aa48453f7565b539bd7c73911829550c58ac5c422146e64f3257f4edf6d3
       ccb7086ab2f06e2da9ba9d935ccd2b86de9b7bc74a0c6187fc589f8eb45f44b48
       0989f0965a15a9ca715fcb0f4bdc15933daa90d91cfdff61e5b9ffda7322a17cd
       5f70a99e05dd619e04b08ad61e762e858b4ad90062a85840106b7e632e5294b71
       0225d6050e74a11dc13454535047e4a19615b9bdb5d172bdc0e300aec455d24d9
       d900ea78b81e80fe497ec53dba2dbea149aebe0d0f9238c5bdce9ae6fa5c89a42
       e633a2a9d831e20db53de08de0dd2919ed8122b058bfd177ee8b0b4469466dc1c
       4aae00a62f1f968fcb06ca9023a59b43dc68bf4c359a31f6b31b9b5022b9cf21a
       79612de558ba9e94987e9693c55992d4deaf8f77910894d9bbf59503c1e6aa1ce
       f4ac4064d36c23c10f36ebecf6142ec14c03815c0a14c9e54eb39a625484ca328
       e025875b875c3b6f5df221246fad83a9f0f740ed66fc2d166d51acab9eb8d133c
       e30f9399f9e62915bb5ffd566343cb339d9dce31a68fec86bf03c4ca68bd20085
       d690afabfad1891b722bd6d0c8a71aa5f226c219704d139de0deaa624661133bb
       d3dfcd40f58fa9d69ec256b89e2c060760f1d37f44e64f5e57615d20599cc6ae2
       127509e4ccb0b002549fba8ff367cb75a86aac8c42cb93eee32a97c42243a4078
       7f11ee990ffd03934f59a8341d8ff72f0fa87e0358691836f91e2274eda9c1b77
       c33367e6b87968a75751550fe05b08e97aebdd5930386568a1543f83bba96fd46
       9da7f1ade90bc95cfce3c15516f8dee3c644c5a130120ce1b9fc518ec974fb64f
       f7416a21eee6140ca35c44ac2ddda01ba52659e720a130ef5af60300523e38490
       d71667d9664339277b3a9f382a61848969686326fadb69c9597778f7a04c114da
       c32fb8418c90ab81cc02f8d3f5c10448f247701a3b0c65dac417d867a5ea0cf82
       ef81f006c36dbd91862e69bdb44116b9ae583afdc42ace6e6ab655771e92f95f1
       be64a841e6028145f7ce998cc400c5ddc261b182095e451003859bac43bbf15fa
       ba56a7ff00328e81ce1b17536871d34fbc89a9aea3dfca0c8d44517de921d0996
       a0f316665f9706127b83d2d9326dbbb11e66250d9853a1f3edcc6f75dab803bf6
       c904af59b0cce6f51b636912f9cccbe4c8b1665751b449e495f10b567b682aeb5
       ecbf04d18d321f98d8f3e068ac84bd7918595df9a819b60e77841f407e60697b0
       715b9c8b426b0995d7fb372b261911f1947a4fc4c4bc259091f963393f384a590
       12b60bac7f68cbc0c4e4dbd8a28a0f7cba688dc9155b9b994db01b2c897a2e12f
```

```
      502379a344052f03f619861c426e70c3147a07737ae434130c76fafdb630a8387
      6e38120186442a535613cba2bc1e995bdf514b4544db16212f44f58f4cca2d4dc
      6fab1950d1489789ae32e13d0880725ba5ff09f841b2b105cc3ed8d653d8d92e4
      cfe7cb8b35f3394829cf1ed2a1c4f60cb259e93e6c7fd6a734c4e997d85b93b27
      dcf72f95660ad2dde3829ac0fc255756b4070a1e0c8e8f5c2e72e251710d0c7c5
      f0ad9f5f83ce74c4625235c9f12c04082eac22faeffd4c1900c0898b3dfa4db1f
      6e7ab039c33f33741baf10ba0f6adb8a02634deab73b88f8aaa8a735714478d5b
      9f951ec4dfd491310d7769d8d1384d879afdc296562ba96ebb2311513161dbfe1
      b5400b1591e8827e2526a7bc837ca5e3546a300afefc26229dab431b797ea6cc0
      c5ebcc68258315e9883a2fc027fcf4bdd257cccad2f577316a6c8be53602b4bb0
      4b793e984e2a3dee7f0eb10087e61785e6c6a126717c20a799865d8f71c7f5b0a
      673473557f9842e7e8565c629e1f180ce757884fd4bda718aedb09ac500b07745
      39d67633d8bfa00c6c7e53451f7e9d19cd71c974d55f4ed42c4bb8d20b93ed1c6
      5ba2babaf9a0adf6b225b5f2a72c51f7a04d0e3a8a7915465dc0694b45280cd1e
      6405728509536b98f07954ddf98df2a0cb07980317352239aed0108199080bade
      97b5078a4a2fbf26
  shared_secret: 3a8c0fe7356b0208769fbc76237adc9650ff17ff7c6ee1e23801e84
                 6e2b95742
  key: fce1270fe05d40a6aeb0592ac71ddfd55101b4d318863839511d908f3983f485
  base_nonce: f09225e3efc44884518d6fb4
  exporter_secret: ed85347a28a6c60123cd0cd5cd03f7919e9af237ab0a0a0855cad
                   93decc04ef8a03ecdf7beeff4a3d21d30c44f61b71a
```

A.2.1.1. Encryptions

```
  sequence number: 0
  pt: 34323635363137353734373932303639373332303734373237353734363832633
      230373437323735373436383230363236353631373537343739
  aad: 436f756e742d30
  nonce: f09225e3efc44884518d6fb4
  ct: 005ed7cf363d8ddc0ae98272ca1a7a52a41881084299d9c8e4cfc12b00f52fd8f1
      791107b25ed7481532981fe7afa8bb9e4586199a285dbd38883832b88a24a2db8b
      cf44775cf755d1ec

  sequence number: 1
  pt: 34323635363137353734373932303639373332303734373237353734363832633
      230373437323735373436383230363236353631373537343739
  aad: 436f756e742d31
  nonce: f09225e3efc44884518d6fb5
  ct: c0f89431f47e694b63be6c1d303a980d48a1464592b91ab27ba200fd416559dbd6
      f2344318e841c7c2257384a47f55853f174f31f2efff37429c73120c4dd72e24d4
      319d382609253f40

  sequence number: 2
  pt: 34323635363137353734373932303639373332303734373237353734363832633
      230373437323735373436383230363236353631373537343739
  aad: 436f756e742d32
  nonce: f09225e3efc44884518d6fb6
```

```
  ct: c3ba83ed646ba64dc7aa06eb22bc5579b58d84d4d03c9f9de193b34b00573d0df1
      d956b676efff34c3f360dfeb383daf78cfa196cb67faea134d495e5f590ff3d9ad
      a88d5dc9f55b5170

  sequence number: 3
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d33
  nonce: f09225e3efc44884518d6fb7
  ct: 1a767b62404633ae888b79c33ae9709e56a82cfd3fbf36de2bf05f179ed9b945df
      5193449352775cab553acf1a8457938037abdf73440919fae0136913f04dd3d8e9
      e6676d9ac3a349a3

  sequence number: 4
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d34
  nonce: f09225e3efc44884518d6fb0
  ct: 00efe15bf41f2dff2914a74df744e9de3c6b0df647238e500d73440b786d174d9f
      d73232f923673456b28d20385d0f18dd153e48ab9c4f7aea11a626c546f0f4f43c
      c6231ce4a0f4e5b5

  sequence number: 5
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d35
  nonce: f09225e3efc44884518d6fb1
  ct: 8518ae4e17bba1f8462c789ecb21c17690f67268b1e5bd8f03c2ee1789886517b8
      3a921de7e06e15d2ee33e6c7e258467ed973d64c3329f9a8e86c55e937dc7a4228
      b1764b2804496dc8

  sequence number: 6
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d36
  nonce: f09225e3efc44884518d6fb2
  ct: 04f1b184ef65633ae9840cb2998d1901d53d4369fce2c588514f166a431169acba
      f751594d9e1e23abe5af2362ca8f09b1177274b1cb773999fdea344284e191d35b
      7f745ddf5a0f3b86

  sequence number: 7
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d37
  nonce: f09225e3efc44884518d6fb3
  ct: edbf292e1f01118553f1496e17c74994641f33e62366aec941c7491303d6665d84
      be45b11aa8abcbf25cebd675bb8c5da6bb48732da29f2055428748baef035a12ff
      30b000f744bfcf74
```

```
  sequence number: 8
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d38
  nonce: f09225e3efc44884518d6fbc
  ct: d0b1d68af5c205bc4307b2be1b0364d61d60b9c6950e713e09054c3d3dc353899e
      30cace87174aacb6a5c8f2adc3e148356d82a31f1481b0ec969fc0630de4e6cb36
      ff618fd50f240c00

  sequence number: 9
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d39
  nonce: f09225e3efc44884518d6fbd
  ct: aa4d9877be290f799011cb5e39786a67f420b0a3755bf844d775e25465e506c7e3
      5bd4437665d4bc6cbe70967a4eba6ea63efe3d99c58398dcbe05bcf42d712abb80
      6fca9f1859d041eb
```

A.2.1.2. Exported Values

```
  exporter_context: 70736575646f72616e646f6d30
  L: 32
  exported_value: 03cc889db1e10b62bb1d4aba594f9480911fb3ea785c94735944d3
                  b37592afef

  exporter_context: 70736575646f72616e646f6d31
  L: 32
  exported_value: 22f64bead57f2fced75f040fe88e42ce086f0c8266a0bfca2577ca
                  0f928a86b6

  exporter_context: 70736575646f72616e646f6d32
  L: 32
  exported_value: a8fcc0f119a648e277a7817955dfe2260e6b62d1bd77e88195e62b
                  00d469f52f

  exporter_context: 70736575646f72616e646f6d33
  L: 32
  exported_value: f3552b35ce7dd69b574bbc6a0463500b8b8043f1cdd82fb6468c05
                  b49cc781f9

  exporter_context: 70736575646f72616e646f6d34
  L: 32
  exported_value: 7bb29784b7a100a424f682d129e1301baaaf60433de0022e72f2a8
                  fb717de6b4
```

A.3. QSF-P256-MLKEM768, Unknown KDF, AES-128-GCM

A.3.1. Base Setup Information

```
  mode: 0
  kem_id: 80
  kdf_id: 17
  aead_id: 1
  info: 3466363436353230366636653230363132303437373236353633363936313665
        3230353537323665
  ikmR: 53030f657b3571b44f1b2b85ad6c72e6607d2538c7118b254c76e15277ffc0a2
  pkRm: 4466431596c2bda2b49ce5aa83ac520e72bf763a5295009ee6fc7c7cf3a5cd5b
        7e373ac6e2b03685846d36bb691fda571fd149f08aa94d748c67b095b002b4bc
        315df4526469640908580cb2e88afbb692a13a8a372cb17b768925d4367b2a64
        e75b81941651ca0aa24d65bec90c9443c0897207362a8727100356f4006f6e33
        64edb7c310f390c0dc0971b870bcacbc7d5a4770e22dc5e95353181581927555
        f87fd15c48db0455bac9a53639b26e18c854f5bdd7c821d04b2c25aa972ef619
        c54671fa14679fd652ff980bf0906a7d2b396c9bbd2045a916952f7cb920f4bb
        199010a8129b08ffac3305b6388bc59f435b5e1c483c0cc248ed1c15b63a9717
        555476e7a2a5b9b732447340651510079886c66db8a777b704068ac748161a91
        86d201a50675398003d773c4bfb895e1267b6c952fc542b485518affa69de663
        a7af22367910624779460496921 6a5b2b2e98d6cbb4aa5993682d0aafb713f56
        568d2537a32f3a5b8443c3455364b3982a73fb5bac928b12f817a39811f8d6aa
        2ae0c5a73145d7e03b785278fc360ae93472c7e0c0f24b75fb57cb348c2a9fa4
        280975c7fbc8a11dbb56d0c4ad74225b7186cbbf5a82b377592c0ab5bbd69851
        b664130ab47438cab5db0891d28e2b556754a094e16729cd566c87f2c57dd17b
        35430b48309153f9295d671d3da8797e0a91ad7087597c819557368bc83a24b7
        a980713f0a937c3925aa02a7c98d499c61632052219ff350c4118126c78346ee
        f9167cd39c37ea67eb67c2d6f3310c521d7bd17ef3fa2d58e7827064255419ad
        d24147a99a2ecf128542947367f74ed31085a2874f7e300b71286327e712a4e3
        3c4d856535038088898a23f42c3541ce3afc5e57e259225c1d86499b09943479
        352c85113e86238158a440cf24af9cd74b60b4135990586 4801f349556ca712d
        a0013adf566aa1f82e20949f076a2e5d9064c8895500a825a49ca8e9326b3dc5
        85fef48da3340a6005538236a61e898cd9f7116e381a86d992a740670fc733a2
        b8bf2729a4c571aaf2733c01690fd563cce52854d3c39fa903afc522cf957b27
        98f165cc41203096a7a2e517a92c891fd30d553308524a22e48802a374a5abb3
        7e7b894697057dd0babdc2cac5157744bc465bafc51809f66ca3893be26064b2
        0b8bcc4bce02b808dd1645cda41754871dd3929232618a649b0c26dc9705d4a1
        70e67fd1982785f595874a604b946babe85b4486354e904eaf9629c1a0bfe438
        800915bcff568273a991313357f8acc8df276a9441a167e78e32dc9c93c5c8da
        e009a687cb255953d6d0905246a2bcb091b3036ea77011fe0a012b528b705b62
        489a8babd78c369a9d0779b80974804c0baf12b42627632b8050a1bc28889e47
        12b4113276735d9cc4b2d9e0b80b95853ef36cfd0168644b95e9e423da6ba92e
        9c79b67b9c35239ea5ec251004bda34818bba919e6958790c52da42328c9321b
        502997458bad9967c0f23a9df73bbef7b2268f363d9fea33ef474a5b67a37499
        18f0c9b87f6aaf54611e5a32b2db13b140c5a03d3ac3ee0b7d91ea47bf1513fb
        66bbf772a9a7904ca1613e921111fbb6cd77f6a73713cd5861c5d208706b6acd
        93a97f2ba2f2e51fc8ca3311df611f41e151ac3c147247d36e7eed9e17727f67
```

```
        045657593e448dd0a5bdb8d6666517d7c7b977f2b5ce7dad79aff17f74077d58
        ecdce06e3ff69d53437b89cfac002386023159fbc66dd533807ad7515b05034c
        85
  skRm: b7e8e6ce3110eedd569219287bf268cc99730e051cee6b3ce66206bc2b426329
  enc: e9743db2238854898474eae10e2bc6178ac503dc6284cd2e4531c969b1987e610
       45b2680c61206dfd50d073628fd3f0261b397febcb9e9952a5bc2d56a3eff03a8
       0abe8a206d1cb076dc65f68bcd3006cf219c09f62589ba9fa70a68368b1d2d44
  shared_secret: 8df7a90edb611789d1f050a9d83977c7e9d92fcc1a70bd4267e11f9
                 559bf527a
  key: cabfa97a26e47c523be48c109889218f
  base_nonce: d487025c75fb2a8a793e477c
  exporter_secret: fc8f3659b9f1b1b30abac50bde4a98f1b7bd0d81d44bbdef0fd83
                   fb10d5d14247b76f5750852c3e2919856623325aa4ea18c01c0af
                   bb379269ca826a0fda7bda
```

A.3.1.1. Encryptions

```
  sequence number: 0
  pt: 34323635363137353734373932303639373332303734373237353734363832633
      2303734373237353734363832303632363536313735373437393
  aad: 436f756e742d30
  nonce: d487025c75fb2a8a793e477c
  ct: f7e73ca84e172f332d695a87157949be5dbdd7040f247426de0d20688dafbe838d
      13c9f196d22db2be915a6f327580b698551c6d466684ad4d76ad30d36d9f8f751d
      40a55d2998464e1d

  sequence number: 1
  pt: 34323635363137353734373932303639373332303734373237353734363832633
      2303734373237353734363832303632363536313735373437393
  aad: 436f756e742d31
  nonce: d487025c75fb2a8a793e477d
  ct: 0d2e8f2a74b74ff848f14c76976b8f6b70466a50e21925f3a2fcd2d6d65cbcb046
      9c6ec6e5f276e121072cf6ebde57c5fa0dd0f7ac95b3fdac93adcabae009096c62
      5b6fb62b47024d1f

  sequence number: 2
  pt: 34323635363137353734373932303639373332303734373237353734363832633
      2303734373237353734363832303632363536313735373437393
  aad: 436f756e742d32
  nonce: d487025c75fb2a8a793e477e
  ct: aa3542c825da42e2655f0aa9c1b0ea07d3745824464cb14e03057fb0ef4328824b
      f86d419996f7ab9a5f3c598b8ab40e08b44e622ff96444c1e65fd0096ba3650423
      dda6cf16d6adc098

  sequence number: 3
  pt: 34323635363137353734373932303639373332303734373237353734363832633
      2303734373237353734363832303632363536313735373437393
  aad: 436f756e742d33
```

```
  nonce: d487025c75fb2a8a793e477f
  ct: fea1ea4811fc70ab5ebc90ae8ac71dc4076f9642d7ad55108322316298b91066be
      4619c16967d9f58c598079dc2827d6811c52a0bfa4a948b346261bfce69d7ab59a
      bf9c45483f47b168

  sequence number: 4
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d34
  nonce: d487025c75fb2a8a793e4778
  ct: 655f90aab3a4be5b405333751046be18f90eef3487fc584eeaed610236f70bebef
      7d41c86d9856b3705de786b3d6477ddaee74782d7c470daa41cfef2d402bd147c4
      f915d12a9e4f9e9b

  sequence number: 5
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d35
  nonce: d487025c75fb2a8a793e4779
  ct: 52905cacd608e573a287994fa962c56ac41562de26deb068ae89cf8bbce9f2ab4f
      25d76ac59e44eb341b674aeb23fee8f9397579f32cd6ac57d5ec731218cda2fb54
      7471f6127285c9b0

  sequence number: 6
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d36
  nonce: d487025c75fb2a8a793e477a
  ct: 250431ca60dff5dccdf2412f7f07e2a9c161e7f8e9827168647c62cd4a8350a13b
      63faddaf4552c90f72f19be562b82d32fb7e483184a1b9df74038983d59f314ada
      a376a8bed9b674a2

  sequence number: 7
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d37
  nonce: d487025c75fb2a8a793e477b
  ct: 296ed3c241c323cc8b8d0c273f34135545d1cb7ce0cf4555e500f023cb14c47340
      35a52a29881221c4e3a93c2b9b3a10f71efa361c211e9d3c4a015f5af23f51995c
      b75ad42d47f89d3b

  sequence number: 8
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d38
  nonce: d487025c75fb2a8a793e4774
  ct: 0f97e25178bec86e756f16e8c5f0778248a77e41e1b5a2225965692c50b167e41c
      cb4b4c87bc314501e7c0610459ac1c78d67df685a21ebda3d9d380312c379a9eb4
```

```
      4ab920ae9f5e551d

  sequence number: 9
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d39
  nonce: d487025c75fb2a8a793e4775
  ct: cb4aee72bd33525353f2f5d10667e1785b73657713c5790fd83a055ec8d2e1e0ee
      3b7427c411187e587e616588cdabce70bed9414ac9a7e6724e891a0a6b8d4a3b6d
      49b82645c55e4d30
```

A.3.1.2. Exported Values

```
  exporter_context: 70736575646f72616e646f6d30
  L: 32
  exported_value: 8ddcdc93b2a031952576836c11f24f0bf8ef9fb76907588544cf50
                  af3745b277

  exporter_context: 70736575646f72616e646f6d31
  L: 32
  exported_value: 46349e0b2fb97b59f41a1013cd1719cfdcd1a1b379fad2fbb67c3a
                  8a1f3eb1d6

  exporter_context: 70736575646f72616e646f6d32
  L: 32
  exported_value: 34dd1d1d1e6b1689e3382e153f295ba6c4c2cea94da8975e2dc65a
                  f81bc721b6

  exporter_context: 70736575646f72616e646f6d33
  L: 32
  exported_value: 5e8f5b50fb7104ee2ad0be44a63c20fa279df05398133984458ffd
                  21533f42f7

  exporter_context: 70736575646f72616e646f6d34
  L: 32
  exported_value: 2b49c8189cdae9aa43ca0d056846c7a49e264879c1e7c93d99d34b
                  6ba463c83a
```

A.4. QSF-X25519-MLKEM768, HKDF-SHA256, AES-128-GCM

A.4.1. Base Setup Information

```
  mode: 0
  kem_id: 25722
  kdf_id: 1
  aead_id: 1
  info: 3466363436353230366636653230363132303437373236353633363936313665
        3230353537323665
```

```
  ikmR: 40b788ef18afdd04b04c3c0097298981d17000fbde80f26410af13972c2392a6
  pkRm: dbca2aaf9b531844221bf5b4c3a2a50c557a5ea82686544e8ab211bf12ae3e91
        cae13192e66baefa713732c580d5a17d493741593c395f3acdc9c6349e4abd3f
        0a46f0f2a7a28c883a783a6111973a272117956e0219858514862b41774590bf
        43c173139cb7e1401069428365e77c6fc67dd60a4b412a17a3d1a86f87065598
        6c883082ea3bbf2b1386a9800a59335b7c72831b72c28fb966454827d28aa38f
        51a67138310607b58c00752bd012e44103c0fc2d3de1284f6c9d1ea659d6579f
        c50442f3654b162473cad076cb11c16c159fbee9931fab5014d55550d58d2460
        7383e0c8d1f4bf9c44836fccc39c8584f9a15f2a3885353b39e6080f2b1482f2
        76beb6726dcfd197ba63bbaab9226f0ba58de627eae2ac60275067fab60520a5
        2ea215c8f96293b85256017c3107091fd7cbf53c6379296c175338a1302467aa
        8f49a76189e311305256da625fbf0070abc52f2f3b72293298857231e015b720
        0b3b18521f4cbc843a82290925a907fb22a0592704d22c21d3520303264cd548
        39683fde63872ebb06dbbaad2294bcf525529cdb3937a49bd652261aeb0552ac
        39a2d373a5770184ca2abfcaae8321167839c21f75b4f02836727a19ceeac87c
        91ce34589badf8728a06c3dfd1643e73087d27b6bd153ba7c09712caa87d4679
        82290f76e6227ca095e78ba18e9b8615c184f43180eaa57ef81899f13a5fa700
        93ac46210c890f93974f268124bd39b7d2962ed1ea6928fb96cf832df95a9142
        b97f3a7703ee899961c352d3d4a103818f1c486642330bb4d8a4f6c7638ac36c
        ab66b1b47530a35925dd8a2c2824a407fbcf062b46e03235c333b64cca84cf53
        1ea92614b9487ae9dbc6d723120f66ca42b676d75c3cad68a14f351849daa032
        e0190b9016b7cb6837065149c5c98b36705112424a07af3b008ea8e33c5d08b3
        09d95e1953237db87aad9b7219529481ba97dd67b732d020bdd22b8f6a0b930a
        48f9c60c521c7a3b78baa7d9882c2ac8e5e3b12c3a2d11d41c0110b0becb1404
        ec99d6754d03aa77e6a785bddb491a0a701b9c7400f3ca864275f74bb350e314
        85a03649ca5c2eac3d65e2a562e98a3aeb727e0792157450a163beea8362845a
        600ee81888f47e5b6c5c35db7f1355b69a084cc7ba6f4d56b09ab8416b73c5fc
        808db150224d7c406e04389ab43a02bcc3a2a3049921b1f9470c74b1a2027942
        6d948fe3544069cc1b37e3189a67586ebc9f11c75a5f1a67a3c097d9e6a8abc9
        244cf10f314c92b6b1939957b23290ad6043911cbc55a4887f484600fbd11874
        8a3f3ad34da5474ae8b5c7d86b0e7468364c408ccab4c057264aa3d1a0c4acb0
        f4da6eeb576062b73328b15b0416cd7cda84a969764f54c063c17e6d4b88acd4
        0c25d2627908a750a1353169983a0363ab58c3370389e066a9a5da7580239d8a
        e77f6d985d9a97498a3a708958868dc53dc581573723c00921c915a50cba27ba
        0b653e2d6152312284a6584fc2261f932243f694922f240d2f18c314cb51fb62
        0318867eb3bc4b85e47f1d92798ff77bfc495472d9cae08946829a2dd8ab4a37
        725524fa24e773915c9b15c3971706ebb6c020b500c3063775790ddac2dd0296
        0d3926191a5ad266012dc66d577a2e7b215f58ba789a2636ab34aaf103df986b
        fdd5a19f5970fceefe08bc7f6dff9feb9fecf8d580afc5a7881b653c9823ac1f
  skRm: d61fe5a7623cb620e8abfba744d8397c16ba339b6e6d536750f986eb7da0af0a
  enc: 069565d41df602f1a83bc1ec4c9cf063a1e9516e831b56c6afa5d5a8aef881e3e
       6d21a6c10fd13c159ceb5ed0660d485df4e3cc4c7832fff505f1391e1da084b
  shared_secret: 9b746d4dc64172d615b7f74d084ec77b4b58dc081a7f87e9737be34
                 953116b51
  key: e71a6311821a4df86d57f80aecda6d94
  base_nonce: 14e49e81eb673f90f3d18e99
  exporter_secret: ffcb6f7e5ccf6997d735623393ccd23ca4c2406e94c005b07297e
                   03449a2c2e4
```

A.4.1.1. Encryptions

```
  sequence number: 0
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393739
  aad: 436f756e742d30
  nonce: 14e49e81eb673f90f3d18e99
  ct: 5f2436c0804f2e0da5a883dc2270c2cb90f1ccce206bf3a871ff022c110e69620c
      3c1a2a23206576d46b74e362a4c377fbe46af1d2167b711b8edcd2f4ef3688617c
      4b6197edef6d539c

  sequence number: 1
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393739
  aad: 436f756e742d31
  nonce: 14e49e81eb673f90f3d18e98
  ct: b4ac95303ea779d868538504b1e16762b1955e7cc84b443f1f5c187fff4fb057aa
      a12d515e7c0db7712d984065a911591d2efe06edad28f8fc3d0f1aae15044d4934
      91c406b4bc3f3e3f

  sequence number: 2
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393739
  aad: 436f756e742d32
  nonce: 14e49e81eb673f90f3d18e9b
  ct: fde3f15e3788e3db72ea37f0c0066c90ee85f93a15e1fcca36d82a5a2a10f87b06
      a932c85b2e2e6af3044f9f2de2b8a0ee74d21f1c259e7433f28d2cf87156242f71
      4eef67d963615ef0

  sequence number: 3
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393739
  aad: 436f756e742d33
  nonce: 14e49e81eb673f90f3d18e9a
  ct: 3741ed2fea281e84163397229cc1177294b91fcbaf3146cebf7672c8cd86f17831
      209930728f3ad064ad2b02809e9b08a7c25526257ec754f65474d6fdf897090492
      441bc8f7b4f403ca

  sequence number: 4
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393739
  aad: 436f756e742d34
  nonce: 14e49e81eb673f90f3d18e9d
  ct: f1b382f02ad2de9f55b9d7d4db61ac3573fa00aa9ffeae2a660add2042f938e126
      128d2f98bdfe78999e88b298c68163e9927e7b85bf11b88b670b717256c461d255
      b22b0bd36399f186

  sequence number: 5
```

```
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d35
  nonce: 14e49e81eb673f90f3d18e9c
  ct: 2e941578779da8b407c5dc7dd87f06e11ac311cd9240845a3f34c3279529097d9e
      9ef84df001af0440c49a2717e77417fe784266d39295df2f25d404c904c14bb776
      74b181cdea631863

  sequence number: 6
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d36
  nonce: 14e49e81eb673f90f3d18e9f
  ct: e7dcaa54d1939b48278a2d5cee0726be1d1f6e60cf2a0e6523c4c2aa95aa05a9f5
      14c1363c7e4f8ef5b8fec3f7d83cad870f723aff40870b3bfb1579551181480983
      a9817527da5817ee

  sequence number: 7
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d37
  nonce: 14e49e81eb673f90f3d18e9e
  ct: f378aae6edaa00efdb6ccc30e126ff5f68510cc9dfc55f83d4c17eae6f80730804
      563f011d35c0f9cc6293e18081b4b7dc8983822626ce362952135b7c6596699e3e
      ecbf76e07847d20a

  sequence number: 8
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d38
  nonce: 14e49e81eb673f90f3d18e91
  ct: 74e06e15e9ceea06d3f1e970beba9281f199961f475ee45d541660e87329e342eb
      f3b20d2ecc4fff073dd15a3dc6d474373bc3a381c53cbe786da4aa3647dd829bf0
      5d9157ea6c1b7bd8

  sequence number: 9
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d39
  nonce: 14e49e81eb673f90f3d18e90
  ct: f426f8017dc8e43786163cb3dfb59c14cfc2fffa9242246f4a3d4b93d9f612f4bc
      47b49325528e307b13707ab793cc3bc2d31f48b37a88619ef10f46a4d88aac96cd
      43359c4b4e68e425
```

A.4.1.2. Exported Values

```
  exporter_context: 70736575646f72616e646f6d30
  L: 32
  exported_value: 6411e8f2c3a297f09b2cb99b333ea82b8a7cf43390754cf7b145a3
                  07f81fb061

  exporter_context: 70736575646f72616e646f6d31
  L: 32
  exported_value: 5127eb7fe8c51f2ce10f2e7645759e6d6bf8c90e656f5811775493
                  0de41e53aa

  exporter_context: 70736575646f72616e646f6d32
  L: 32
  exported_value: 8cf3662a91df890a85c7888665810b719c2ef2b9a787f19f8441bd
                  1aa8734cf0

  exporter_context: 70736575646f72616e646f6d33
  L: 32
  exported_value: 593d89effbe51361193a86867f645df2a1cdb48e5ebcf0533d3442
                  37bf60842a

  exporter_context: 70736575646f72616e646f6d34
  L: 32
  exported_value: 787b7f9a412146bf812d9640cf6892497afea1cb1af68a679ad148
                  c0f2aa81ad
```

A.5. QSF-X25519-MLKEM768, Unknown KDF, AES-128-GCM

A.5.1. Base Setup Information

```
  mode: 0
  kem_id: 25722
  kdf_id: 17
  aead_id: 1
  info: 3466363436353230366636653230363132303437373236353633363936313665
        3230353537323665
  ikmR: 300495cc3d5349e45e700a4b3b57aed43f5c930092ef27c77dc8eea28f9d659c
  pkRm: 25165a85c6450338519454bb15404c835307cc3bb261a39df9958c7e5cadcbf9
        36f638846b979326ea9f029a5620371375e9c8e878a73cd98afad8b8afbc609b
        b3ad1db41708f09faa693fdaf1063cb80d3602b3fe0188b89887c2bb9dcd1734
        b61000ac7c3604c776f8f177f2615e8d7800fff3380229c2478a04535039df73
        711b18358a99ac8e222f2e5a652bd040e103581f48362cf1a5fca7c00fe287d8
        dbac5d202d89660307261f8af568c96c5ee4188a1dc2b1098b6588cac56ae5c8
        90dc8fea3b0e1a3b8927132cd689651a54240239b7c79a2882e04ef5fcc3b39b
        b9737acfe015c7afe7cbf1cb0dfdfa09d1b0171914b3a3199c2638b1c6293b9f
        43114d06030036559709 48d1383f16ea80dfb39907c08f79c08c092267b57303
        96628dbd458eaf1719bd493074ea13af5b3ecac60b05215c250831d043c3653c
        0e0c91aaee69c8b5a3189e8c5c88c587fdb332e64abae74585f0a29900e67dde
        b47048a4849360b3b6d508bb447b846b0729b3aadedb05c63ab88a50988595a8
```

```
        20040f13a5a61f7ccb65b1a8b30998ef4c56d0a3b0a41241d6f85aa3c6b37259
        b7a034a022a9a21bd7accf252dbd2b9868909b2f10cc727b652f4217f65ab3e8
        3b038f056a5dcc26f56052b4836a08d21b988b48f7b86d94057437686330199a
        52530855961e41a422e92685737a5c080a2723240a65258d12020f322528514c
        00ad628f10a533afd2a818eb6b207a93ee42cdb13b5dbb6700ea58ce3cca1923
        e2b295990aca10a115d5b7bf903b2ca5097ca2353cc1a81d9407c6c24e1640c9
        3ad7c1c493b369db5756c1a94050187a5472688580b7348b1fd58ff0c8763299
        73f1e27a4db7617473696ca779ec77814592982e82231d11b4f706581615a381
        236fa1d90ae424a18e5b7d96495b81700bf082b5a7fbaaa9725892e1796b7c2a
        5c1923b1907aa3c75d6aa75ca6081bccc25c9d0c6316a759a6a532139c884c48
        3f24989f4cdab312f0268df2167e4370bbf20832220d6db47c254b8d664c7db8
        a0aee12608feaa57f783c2995497533385d979c98275c611d18d2754aee4e588
        999548c05779a60bbbede8cf48ac34ea6665f1028ad6767c9923618a6a46b7e6
        922532522b15b0631918937270b184793337187704a929cbc13c3c4be5e2b00d
        d9249d0a61344b742d3a4c21154a8cb3bc27b1ac3c1818f233c8419c1f44c727
        2930be46db6a1a4ba6339a8e2e795820e06e9d812d15d46d48e7bcf9b7b2e0b4
        cdfddcb2d9c6c85d650b3eb52ab4d992f1441a5db389b71b5d9f33cca70370a2
        2512eae42da47367a10b2ff321b28c44c4b5a85b46010dc7ebb220218f76138e
        f5da4cfdd9429c2a14af883533a39eececbef0931336ec82aaf30c19646760e0
        c3d3f50cc291414512a273b522005d51e7521209e37fb74bae743a1b00036498
        543044a11bc380971a6ccc9e05861c54bf52f53deb8a5fab9c87d12181e165a9
        fae2632783a12ae515c1c7433003049eb070a5a97c805631db6597c19a22dd5b
        692b3a5a2d20cda0b9548d75600c8824e5f81b51138f7af6c59341b5a200869d
        9b7f033c02738a970753c35835564d02c68d748cf7bba0137a8f041234001d41
        3c99ef9eff24bf6311eb7d76bb793e5b76a589590e4e1b05997fbc526d804664
        ed341de14f5e4e780f21450f814a2f9a15cd912305f5f02c7ff919d7aa6bdc2b
  skRm: 56caee1294459fc2f369b0262b0a35f9783c547aedfcca0ad4f0d30e9e907663
  enc: 4ad3f1b8953b7a17754e3b218ac95dac187bd00656e183443afea90b37166f04d
       ceb74d52ba53e4a9950262b1889220955c794b061bbcc076292486b8cfa045c
  shared_secret: 47953ab0754bb180269445f55a488ca272b41ffe24507a6264f1d8d
                 1e2826098
  key: 44168255b16df6a4dd369364bad0215e
  base_nonce: 275ece3cb4f1208402598fa9
  exporter_secret: d3f07b6b8ce4d770ec483ec697ec0533510112c02b76f51d93fcd
                   4a4296ae52d0b28baf2ec03882395dea009aa03d303c71201f931
                   c03af325faa049e7de30cd
```

A.5.1.1. Encryptions

```
  sequence number: 0
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d30
  nonce: 275ece3cb4f1208402598fa9
  ct: 8da5574267755033cf034fabcaf9bea059c16181359044a16c387252ec4bde8353
      036e953631eca1b1cbe44a049f100bb8a4d552b543c3dcc6839675a543d9b69371
      093c3d42c9183bbc
```

```
  sequence number: 1
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536311373537343739
  aad: 436f756e742d31
  nonce: 275ece3cb4f1208402598fa8
  ct: 359933374b4291aa75c1bed03f1d93221c7eb23a451366e30d179c632188760121
      fd5c1e8cbdf135d145a97c036af56972ef381db008c3d42ec3631cf238de852e0b
      a16371e63c2f30a4

  sequence number: 2
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536311373537343739
  aad: 436f756e742d32
  nonce: 275ece3cb4f1208402598fab
  ct: 1e9d57384560f06b47d90e703f55a1bca69efb6241d62aa171e99b000a582eecb5
      53ef9a9abdea833e92250ad3828558778b09033baed8ee0b66d0d30c4eeb3b209f
      39596c2d79dfbc3b

  sequence number: 3
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536311373537343739
  aad: 436f756e742d33
  nonce: 275ece3cb4f1208402598faa
  ct: 3e519e8a7205fa57de4b881cb6cbf8eaa9ed35877b784311cb5a2eb4b2f0da877e
      2bdb434731de191944689d05bff3ccacdf879ef3c51b06888a5caf29a1f8dbf530
      52a7a6a2e06dd7b8

  sequence number: 4
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536311373537343739
  aad: 436f756e742d34
  nonce: 275ece3cb4f1208402598fad
  ct: 1cdc78bc5e30788b81ffd322551911111d802180f2f100599b2b07e9ce738e9e13
      d00cf1af6af849d66cc76c9ab19a87ddc256c880647465ac1a108ec9faccacd9e8
      66607e7391a4a945

  sequence number: 5
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536311373537343739
  aad: 436f756e742d35
  nonce: 275ece3cb4f1208402598fac
  ct: 5ee03703e1d7b25222daa9bba5c8bcca934b97b275a72e5bfcb58ab8178acbdd5b
      9cfc703d2b981ceb331cbd69c166fee11825fe5e55eaad6b21343a21c915e04be2
      9cd8d4af699de972

  sequence number: 6
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536311373537343739
```

```
  aad: 436f756e742d36
  nonce: 275ece3cb4f1208402598faf
  ct: 9b64451bd28d604341cd96b5e5a47e6c08d08e8cea9e681c63728410f2d7363b51
      92b71943a5b1fe8b9c87a9c3d27c03c3cb914659d671a694d919c4943486b0ca73
      5b72bc994c9802a5

  sequence number: 7
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d37
  nonce: 275ece3cb4f1208402598fae
  ct: c8de844f848eae007947cfc775a9a6fbc37f31f4bb093d77f6e0199c5f93945b6e
      cd2e3080ef3647f60729a5fb1ccccd5be4d8d3ea93c460469e96d4eee7180aabe5
      80ae008b9f1ecfa0

  sequence number: 8
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d38
  nonce: 275ece3cb4f1208402598fa1
  ct: 8d2c7f276db9c8789986d4c98153909b491fb2443a55bd65b1b1e068fa74ffe7d1
      f790f6b20df5413352aba206610fede4d08b26126f4a9e763d69a6b71a26965a0c
      fa5aa6947e7e60b0

  sequence number: 9
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d39
  nonce: 275ece3cb4f1208402598fa0
  ct: 2aa9aa15937cae9772553a5faa564551e1e2bbb2ca8a772cf2c26cc832e0df4dd8
      e657f36cd9dcc4e0d7f10dee471c96ac4b97bfa6a3366dd9964b684057cbbb23f0
      bedb83d772651ed2
```

A.5.1.2. Exported Values

```
  exporter_context: 70736575646f72616e646f6d30
  L: 32
  exported_value: ced05e418c1df4b8a6a21a589f0cfd33b0e7edb444f9ff6c23bbd0
                  e4ed380636

  exporter_context: 70736575646f72616e646f6d31
  L: 32
  exported_value: e59059003114582360b2c1176c5e8cf70e0b242d3cb8e9aee808a1
                  b30924f0db

  exporter_context: 70736575646f72616e646f6d32
  L: 32
  exported_value: 344badf31ccbbf98abfcf5559ba1e52fe16620e1ebf3d1d7931fb9
                  2b8e0b4f46

  exporter_context: 70736575646f72616e646f6d33
  L: 32
  exported_value: ef0b3544284c0276470d6c88cfdfbb4408ab592a17ad530e2df175
                  08abfc217c

  exporter_context: 70736575646f72616e646f6d34
  L: 32
  exported_value: a8249daf6e1ff595cd035021d6db5c6b17d27cc31dcc616f5a04c1
                  df0f2c0438
```

A.6. QSF-P384-MLKEM1024, Unknown KDF, AES-256-GCM

A.6.1. Base Setup Information

```
  mode: 0
  kem_id: 81
  kdf_id: 17
  aead_id: 2
  info: 3466363436353230366636653230363132303437373236353633363936313665
        3230353537323665
  ikmR: 6a206c70294ca1d907679a1739327522c5c3b04aaf3950bcf5b1ba7463954021
  pkRm: 58ba2106c3c59680a0e7272a30c038fde90e6b11bf4cf54bbfc3171e39415698
        b168fc1a792acc7a7037de424fb805509d085b50b07aea08814bc38989da188e
        e7841762c4e4b5cb682b6febfaab69c00e0f1451c385386c4a77b4a83c83015e
        b6575fe9c7cc4a91c1bd33a8e71a36980a809c174b86e43e41c741ec27651d61
        ccdd723bc9e14193f801f21656392c521c9a712b6b919afb7fb53bc4db9c062b
        d62a680c8aacd0ac0963556429a604731e4406af0c0572d017adea480d989460
        6ec625367a14dfd727f4256d0c24af2bb92eedc9be4b896a4ec7ad26b0822dcb
        14f8e834030356df118ade762350ebbf822521bbc692c04382048ca8ec8c0f46
        f47941fa095600215740674f6a7acfc86f98896b938002ca4c72fa74861b476f
        b7f4b353e3444006633d69a3d60c278b2c04fa70371d5387af12197c579208b6
        c63d2aaadee6656ddc1109284631624fb57656c51c406dc1779b410bfe270c8a
        ab666b8501deb03c7dac31b4216c933164ff1cbf1fe45ac38409ff4cc9443b31
```

```
        4f932e7e2b97abb91d76da6b8748028cc292683736fbe9b166aaa7fc108744a7
        189fe2261222821e78955e613b57567433e84638c93032947555113fb6aa299f
        526e1d015a012a1095bc08167731dad92e99342f3894b3e50712e89268ca1823
        edb68b2d763de3510d7a56bf0cc9c3335cbf21765e58dc60c8ebb40cf817925b
        ca7b08642415509968b7dfa80328b29e6e9aa1f8054e7b08a555c4602f51879e
        f10e70b735f8e35a17326558d443a76b44b769489d2076128bb2e3814fc37c7a
        dc4b10c2d16f22c579597907bd59a0621757a18848e4e813e5920670d783f9d2
        bf3becac75b16932367a61846d043b7070453bde730996b099e6b6700e0411c0
        4abc591682c6a25a0a1c11817375bde7a5a3f3523d08464bb091976b02a0277d
        f0da8212b27edea6042829654654115853c05bd7b18ec47638275560c1569e71
        373a443262ca5b68dac2eb7279eca47748d624ebb35442f50aef8a474fb22b44
        945f30e58e85a79ab8997b853b09c74a3536f863f1f81ca3307a1ffc8259b87e
        86c975a9db5f4a471b31137d04462fbc6415dd2a435fb097df3499ba9b1bd22a
        9670f939a0bbb9ca597b5e1caebd14b4d07ace7f9694bc13350c20801682cb68
        1bcdc8469ba19a814028845095540f9ac51f4b3a2176abd8230b8ee9061dca7b
        9268817e649f87267c40d5095063a7b8f5003708aa1f04988b83c6ddfb1bb424
        a2343c8389e4cba0f72510719df443520f205696b657e0173a70b81dad274084
        fb3189c2abf0b4c760f8cdb6ea18f54c97c1c9b95c987ca544637c743723897c
        797c7294cbca996c9ef0d849c2542f93e23a632a2fc9a2aa3aeac7bba3c1f945
        c82fc1be6f46aca0796a08780ed2527e60e1c131b9049956969e6370c8424845
        d34a6b4b45a01b2254701c9155533d4062214a61b196734551bd74c412278b45
        740c5905dcc39545ac13c727833b5cdea8a0eeb5a9fd15c6a27c922c8b0b67b7
        3fb0160f5641583ff70dcf96a62f540f08b3b51c9cc1df5a19886a2b24f67ed0
        a38fa821610d547b5016cae503ba7cb37fe3da2d71caba4d4b79141ba797b24e
        92c2bc77eb7559933b50e76d7707ab72bb7ffdc8a7ac95431c7649ded8b143d4
        247178ccff9c3b2ab098d8aa1c2465c5814ac493a27005033a8725317b284c4a
        abb90063cca18b0ea15251a1108e9231bce7926516901f2cc524e65798535880
        98c33572e48a1bf7789f3357611c37874898d8689dbc03a5aec003b7b97c19d4
        c266ea6a8289859734985ccb0241cb1ed4755e4c5b5fe9b48ae8307b5b0629d3
        ab10159201497066616107439 44f572781b8f04d368825b8d7a4906b42f78117
        6fe90637f2698a0860f5616415f447798278ec415fa3623d926286e4e0409ad7
        ba403a1178ec21297c176aba4e2b91604e7a22afb53ad477b1e203707e9c4d3f
        bc79baacb15832ada4f9c4af91669022c5a008949bbba38f53ae92a041146917
        ae9c49dd4a2bd5a263da2c9e4f4184958c3fcc1c722ae071882baf1cecb251f8
        8a9ffbc32dc9b48b9b42b4a59a6a21978ec59e93a825ca642433809b0b098fda
        1b9e1a0a05c41ba0a2a91d66e56755588202fab248b8afa59976a472176e9573
        0a678297a305a9c288116ed96e44a825a9e10e5cf6d08de4c5cc9456bee0e22d
        044ae9db3d1d9e509523d7b0fe9eb8aae8c435c6860add6a537fc5b319011985
        b5d1e306d6cf495e3c0cbb939f618b1aeaaf0a2961b974ff20cda4c94c915aa4
        6c0f06b9f88a964beef0ce9f2bb578cfe39408c340ab68f3658ce90d4fc84491
        c9
  skRm: 23456b644f15c3f35650958af845450ca744f66246d21150e2b49278b02650fe
  enc: d85713a50e982ba6a4ca74452118a34be465f2bd6cf2acf588c9d5773b4faf880
       43ae2cc3efd62c5034f19628e5563ec7e8c2698d5a16dc5e838eca6c8c8d0fa92
       97bfc63d305fe5d1c8efc0c92661914a8cf8186a0e3d7eec52a6872b01a6aeb20
       caec6437c33de0a22e743d2e6936ac1baf96f286c2e4de1b81d6446517aa07a
  shared_secret: 4bcadf4606299ecfbe8a5193800b63cd53984d0ea241ae6b66ae0c4
                 43fd820ea
```

```
  key: 538a0a1d73b7be0e8f9e5023864ea48e08dd2af83249e95d310af9e8421be977
  base_nonce: 0388f071808bc02561c04e66
  exporter_secret: f5fa529c1fcd60940e203532137da133038b69b729c84c581bd23
                   6b7e4205b4e5ca2227e8369e570550dfcc153e32609fbcb78e92b
                   8ef63ca5765e8240dcae17
```

A.6.1.1. Encryptions

```
  sequence number: 0
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d30
  nonce: 0388f071808bc02561c04e66
  ct: 0da5904c1b45fea510d0c8a9a78717c2cda95a940f2dde4b8163f30bd7eda66ef9
      ee2981c1529f9cbd9a33b0ed677840063ea8d54a43ca55db95df5bf7a4b8b68180
      36afe30ca034e498

  sequence number: 1
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d31
  nonce: 0388f071808bc02561c04e67
  ct: 0e7f44421927c8dca2170ba0481d19d405d87ae696e65a3cf84a6274bb2c330a2f
      621bb2ee7168cc1c240f805bdf58951b20adc9850a19a30b67d766de81bc124d13
      645254bd397886f7

  sequence number: 2
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d32
  nonce: 0388f071808bc02561c04e64
  ct: fb2322a567ba2e62edeb84aacb644039f9f7661b9490e63d2c0b61674b748e030c
      d6082a294418f83f65a540636db3b45522b287a7f06bce35f3b6a2d8d82aa0e0a4
      d7a087fa0338d4fe

  sequence number: 3
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d33
  nonce: 0388f071808bc02561c04e65
  ct: 06c79d3e229c4a2d4d59629b1c815063655c60c14ad067c23a37703d8558b2808a
      9f8f0b6e30692617fa4bb5daae722ae6279e012e3b89b49eab089b02428fd6aba8
      c795c20647bdf839

  sequence number: 4
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d34
```

```
  nonce: 0388f071808bc02561c04e62
  ct: 2d9eef1a5d380b936d1d08b252c7a146f0e3fdc32596acbf6f4126b563e8a420d8
      8553504d710554f3cd1150025f12fdced5a1bef0f163ca16e06edefb5ac57fb511
      11949a0a74eb80d3

  sequence number: 5
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d35
  nonce: 0388f071808bc02561c04e63
  ct: bd16d58b56befea667415fe4af95ea45328d99933c6c6c93ee0aab5f4cf5d7f80f
      83d06cf63f12ffa03dd1022761d7b37536cde0be424051d8f174c1e948ea216ccf
      5489bb2288fc2049

  sequence number: 6
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d36
  nonce: 0388f071808bc02561c04e60
  ct: ed9199186ae68367537030d7d147be83c5e1598347226bf88d33cbaa3a34f9091c
      c4d9a9ff050e033e0803dfd3f104d89d04df51254c00928cfae5f9366a6ae0c109
      6a04be70828e3ea1

  sequence number: 7
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d37
  nonce: 0388f071808bc02561c04e61
  ct: feec22e8ea27d10cec705121aa9346d7682e4ae416bf9992be9820a48da6a00076
      d48e8fb0acc20ebdde04ab5495e55644fc595609150ce82b547b83bbbb092e5b70
      f5ff7627468149a3

  sequence number: 8
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d38
  nonce: 0388f071808bc02561c04e6e
  ct: bbe4f188d8e4911cad6ba433fb4d251cfd8a66ba131952c5516020c305d038775e
      bf98c0b530edc506815ef2254e3b589c82ab88740d3d24f80cb7e4fe3c1eee37ae
      0f628e4d7c350df5

  sequence number: 9
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d39
  nonce: 0388f071808bc02561c04e6f
  ct: 943e1fe8c7e32b4315f1a840c055b22566fca4e8a44e0f90dbb10a4c73c8630aa4
      f78a7b986c42cd9b779a226f264f1ed4c0b238af6197cee3b1c9f84181c0e29993
```

```
      159f4b34fc0ce18a
```

A.6.1.2. Exported Values

```
  exporter_context: 70736575646f72616e646f6d30
  L: 32
  exported_value: 6614c70cafc82afb78baaee187268ca467f1d7816922a47863f41f
                  d25a6defb6

  exporter_context: 70736575646f72616e646f6d31
  L: 32
  exported_value: 573336571c21ad4085c82d6903653330caf9025d189154e8fb0ca8
                  d926df399b

  exporter_context: 70736575646f72616e646f6d32
  L: 32
  exported_value: 423fe21843425bbf3ee41dd2bf7dd9c99a6c9676f7666a2a2c08c7
                  0ce2c97653

  exporter_context: 70736575646f72616e646f6d33
  L: 32
  exported_value: 64d4945422e190e877f84ce997e289bc0bbca9defc5b59dc631a08
                  9e5dac05be

  exporter_context: 70736575646f72616e646f6d34
  L: 32
  exported_value: 796b22d8ceaceccc4a700c7e943f0cc10de5da4174d20399ff6edf
                  9bcd162422
```

Authors' Addresses

Richard Barnes
Cisco
Email: rlb@ipv.sx

Deirdre Connolly
Selkie Cryptography
Email: durumcrustulum@gmail.com