HPKE Publication, Kept Efficient
Internet-Draft
Intended status: Standards Track
Expires: 1 January 2026

R. Barnes
Cisco

30 June 2025

Post-Quantum and Post-Quantum/Traditional Hybrid Algorithms for HPKE
draft-ietf-hpke-pq-01

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.

This Internet-Draft will expire on 1 January 2026.

Copyright Notice

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 [I-D.ietf-pquip-pqc-engineers]. 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 [I-D.barnes-hpke-hpke]. It is the foundation of the Messaging Layer Security (MLS) protocol, the Oblivious HTTP protocol, and the TLS Encrypted ClientHello extension [RFC9420] [RFC9458] [I-D.ietf-tls-esni].

This document defines a collection of PQ and 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 [I-D.barnes-hpke-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 operaiton 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 corresponds to the function ML-KEM.KeyGen_internal in [FIPS203]. The input ikm MUST be exactly Nsk = 64 bytes long. The d and z inputs to ML-KEM.KeyGen_internal are the first and last 32-byte segments of ikm, respectively. The output skX is the generated decapsulation key and the output pkX is the generated encapsulation key.

```
def DeriveKeyPair(ikm):
    if len(ikm) != 64:
        raise DeriveKeyPairError

    d = ikm[:32]
    z = ikm[32:]

    dk = ikm
    (ek, _) = ML-KEM.KeyGen_internal(d, z)
    return (dk, ek)
```

The GenerateKeyPair function is simply DeriveKeyPair with a pseudorandom ikm 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():
    dz = random(64)
    return DeriveKeyPair(dz)
```

The SerializePublicKey and DeserializePublicKey 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):
    d = skR[:32]
    z = skR[32:]
    (_, dk) = ML-KEM.KeyGen_internal(d, z)
    return ML-KEM.Decaps(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 a traditional ECDH group with ML-KEM:

QSF-P256-MLKEM768-SHAKE256-SHA3256: P-256 + ML-KEM-768
QSF-X25519-MLKEM768-SHAKE256-SHA3256: X25519 + ML-KEM-768
QSF-P384-MLKEM1024-SHAKE256-SHA3256: P-384 + ML-KEM-1024

These KEMs satisfy the KEM interface defined in [I-D.irtf-cfrg-hybrid-kems]. This interface is mostly the same as the KEM interface in Section 4 of [I-D.ietf-hpke-hpke], with the following mapping:

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

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

* The constants map as follows:

  - Nsecret = Nss

  - Nenc = Nct

- Npk = Nek

- Nsk = Ndk

5. Single-Stage KDFs

This section defines HPKE KDFs for three eXtendable Output Functions (XOF) based on Keccak. SHAKE is defined as part of the SHA-3 specification [FIPS202], and the related TurboSHAKE XOFs is 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 [I-D.ietf-pquip-pqc-engineers], 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 [I-D.irtf-cfrg-hybrid-kems].

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]. QSF-based hybrid KEMs also provide these properties, as discussed in [I-D.irtf-cfrg-hybrid-kems].

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

[I-D.irtf-cfrg-hybrid-kems] for further analysis of hybrid security properties.

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 add the following entries to the HPKE KEM Identifiers registry:

Value	KEM	Nsecret	Nenc	Npk	Nsk	Auth	Reference
0x0050	QSF-P256-MLKEM768-SHAKE256-SHA3256	32	1153	1249	32	no	RFCXXXX
0x0051	QSF-X25519-MLKEM768-SHAKE256-SHA3256	32	1221	1317	32	no	RFCXXXX
0x0052	QSF-P384-MLKEM1024-SHAKE256-SHA3256	32	1120	1600	32	no	RFCXXXX

Table 3: New PQ/T 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] "TODO - CFRG Concrete hybrid KEMs", June 2001.

[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>.

[I-D.barnes-hpke-hpke] Barnes, R., Bhargavan, K., Lipp, B., and C. A. Wood, "Hybrid Public Key Encryption", Work in Progress, Internet-Draft, draft-barnes-hpke-hpke-00, 20 March 2025, <https://datatracker.ietf.org/doc/html/draft-barnes-hpke-hpke-00>.

[I-D.ietf-hpke-hpke]
Barnes, R., Bhargavan, K., Lipp, B., and C. A. Wood, "Hybrid Public Key Encryption", Work in Progress, Internet-Draft, draft-ietf-hpke-hpke-01, 24 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-hpke-hpke-01>.

[I-D.irtf-cfrg-hybrid-kems]
Connolly, D., "Hybrid PQ/T Key Encapsulation Mechanisms", Work in Progress, Internet-Draft, draft-irtf-cfrg-hybrid-kems-03, 25 February 2025, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-hybrid-kems-03>.

[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>.

[I-D.ietf-pquip-pqc-engineers]
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-12, 19 May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-engineers-12>.

[I-D.ietf-tls-esni]
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>.

[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>.

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: 34663634363532303666366653230363132303437373236353633363936313665323035353732366 5
ikmR: 06f7d4f1495a828789f5543cb847369e10751ca5369a473c74e46043080f94f5
      25f2f8cb7d8cfbf3cf8496728611a6567afd446a6ed1d22f6d32f74ef266a97e
pkRm: 33e49cea9c631f102595637291548f7220782f498bca5073b8039759f5582f45
      aa59245f41e5516da2a779b325e039651c348f57502602a3b7b8482b4b1576c9
      3aa8b8c5155e5bc5dbc6a08d57103bc970b016ab7ab22320c430291ba1e80855
      64c4a13686aafefb510ce76e36876f2fdb1b7ba49550c15f5d366abe420e7ff2
      459cd7af36f5c285981adcf84020b04a66a0bc58172f8a34280fc32497a56308
      238a9f27ae95f0a593a70ae7594260e60930695f5f803eb2210fe3ac61c8bc20
      ec2566dafc399cea81a3834619420e5d85476cd573c7a08eaec4c60cf7999acc
      98724b934e259cda793dfda761cfa4289530b1f75b6a592730b8f5607eba701a
      150c38ac0e21038bfef496d2cb808f7342317789d1581b6f8565e3018d796013
      fed26b59fb226b5988633923a72a9acf42960c228f1e25b84f18ba4fd8762067
      9d6c7a9e5f4340dadc3af252afd28231e3d52cb924209e50ba1ca632de811ae1
      097cd89803884a8c750663baec78c90254f038574fdcb74c527610e21469398a
      20abcce9f50e1537867aa036bf1452cbf70850e8a5f5464eccc8a2af260a4550
      7e2da24c4868699065c95e3946ace90a655696f654892d8470a535cda5d58c44
      c8c0cb7bcc7104a847bc4cb1f03b8872143f5491c9e8c8ed46a6a6703c07d42a
      b8fabc4e25477245754d718ad8c88ce753c9756c2403948c06c1345c570fbd9a
      5932982f326a2f2ac69ebf5a58bc788fdb72a4d90865d3169d7752579cc49ad5
      e27479260dbba4800b521d21d22eb633168632b5209c4b81f32026a8111e07b1
      48babf740297af87239bc760b976862c551622416a6fb23825112308867ba70a
      75ba33179c2373b97492235a27c1f266cbc18f71c0596e47a285bc2e09397a63
      2309ff67739cb132d8c4007d2926fafc5eb56a6cf1960e87b4488c4895aacc6f
      cbbc4b6dd2b56cc69616653836550bbb9663b678370c3916fb832e17ba753d04
      787d78b0ddf11f6410bbe847cd6b1abdcee2835d50867a40137723433fdb6e94
      f902fda88b96d95af872000447c3649a93d3e0013dab5350dbb45c6190089c56
      cd4c1fce162daba74abfe8ae673105e0ebb94e52b37967b609741eb4608723e9
      858937b4996269033ca2cb503c4d3ccda0e15137cbc602728cc9bb5cca55b2cb
      c4579d02bdca430a052bbfc68bb5c8eb7c0139272c545d09f345b49a800314ca
      63c5097ef24cd793946410a931d5437becb557197affa37071954eee9c093a34
      86492362595761c83aac2ce46cdaebaa07ab3c3c1363c15bb8c4c869f54c6fdf
```

```
      a78924b954e0b480d3a128a2f64f7527beb2ec92ea6994dddc5eac10bde8a456
      09784e7948b6acc7c5da8526dd970870f46812bb0b53867668e17183fa638926
      1fa5da9a3ad8451094cd8ddb28683c1ce853c0e1cb3a4f79a168502242f66217
      2bc21609492fa57a9f077a1889c42cb2aa3bc2583275ce6b171c3e3aa4279483
      b204cb3a1a98535a2fe7c1b3d322c52dfb9e9ec46f926562ef1c8992a2bc5fc0
      47961898d1eb3d35cb1a018cb440d84de5047e50a4abd891c84f9431e36bb813
      4642e6fa144c15307a5122f07252b1e65b0e9ab3c2a184826c9a9cd938bdd588
      138a731c1b51787f166ca6205dadaaffc05c609f747b99fc3b918359e2ac28c8
skRm: 4e5551f3e501cbc780a5f83ee2b5be7bab15f3d00fa4c191d287a1c7189975d4
      0800d1310641294e830ee75301010756f7452ab50018e4e52a674232fbb489cd
      db7def967bdf0a0b1d7483d914207906b1cad06d3f30597746143a233549e027
      6486b111e3948d886fd51849533323f6346a91b45c867a4709638c1fd930f2b7
      8a9499a185013276033718ea74a02009e0e26fcf792af15cba94ca812ab42890
      3314d0299a102aa6caa49b79fa7bda8c63bceb980207a505c9cd16c0c396d7ab
      a18404fc2acd0b93cf55d9768cc91f970059741a6554674cf3fc2d64b5bac9c5
      9961f64d4ce40fc30b6ce6e431f79b5101c24c7d142afb864c488b87540083cf
      2b0d4ab76048fc37b3739386233d4453cd3a7283e6578e3d51405748109ad231
      c470be3a97a2218b3ca8792f7f314a3322cd263a19e1a6a0f01a3205d5382044
      975dc08c939c16eeb86bb2409c0c85b728d71b281602040c8f477050479a2e36
      9414e68417929190c7f27052376ff8b8cf7f9929e080b497864e28182fd7acb3
      022246b89536fa48256ee71e2eac57e1e65b01411f19a834b196914a6738d974
      3ae2fc7e3f213cdefa336e08ab660081aa7801dc34b64d545cca58284f8cc19f
      216631d0835eacabec2966513b570e2b3a6587be5520498862924e3bb2914620
      509a343105a242e41a85059792333202f38364693527984ad1755ef1b4472578
      c9e7cb3dda98444f5b1c77b0af7097bc2c635af6f261cd0431c402088976c866
      52758574928c19b2c0125f2e37365b2277acc3957ee85b9569a763571345eb4b
      aba8571ef29fa9d4903120ad65b393b5fa678397c9515431cef503c4aa086e8c
      4dd6fb0650107167d795a2d5704b684d08e07da6679386248882182107797 7a1
      569ae0ab9bc5626e1a963c0984341f560944542b1d3a0bb180860a4767a4b942
      f4b828d0b7275d1a44ba2608b62baa62759881cab61b39c869207af755a9dd07
      391ad1cf92b12eb9a370f8fb85d4129024d8976ed78be9ea1dbb6428b5a9aaea
      d8c543316f34988e536216d07c850062521bc2861f15a6e8fa98d2ab02b050c8
      b1269105b5a4f6ca10261ac92060679ce3b8a4802119970b85a0a219bcc723e0
      03f2f29132a12c425ab8eef89564990f8d09b5d3d117eb06a285b123519122a3
      802604514acd75385736730a8ab914f6abe6c8a18e47c5f98b569bc1b6e1fb9c
      757b91556bce7925abf51091cd492628f648fdc56a34917e86e2b405b14c4c22
      14daa82dad539220011e1336807c522233a3c730dbc0c71312f1904f3b2a594c
      9a3eb8ecbeb052b8c1dbbd278c4d37f17f10d8c1be25646dab820a9614ac95b0
      d3d05ee7657ce4871a7f786e15589f169a22212377af8ac036c14e4dc4a32adb
      26ba68421a98596f148b155330a0a2600daca88cab5a7c510c42784eec4c0fd8
      e480da608b82128b0b081be6331713f86c89b400fb5509319998291087b8260e
      a128ce64f116ed224d8fe08329c7bc2680c8d4839c9a555c44aa771d4500e664
      929895bf3edc3c64ea24c356acaec9c7b54a5327093be64c290cd437ae790cb5
      c4abc9d6705508cc93354e68927de2f56b716415fe2a6ba93295c53c3bfa26bd
      33e49cea9c631f102595637291548f7220782f498bca5073b8039759f5582f45
      aa59245f41e5516da2a779b325e039651c348f57502602a3b7b8482b4b1576c9
      3aa8b8c5155e5bc5dbc6a08d57103bc970b016ab7ab22320c430291ba1e80855
      64c4a13686aafefb510ce76e36876f2fdb1b7ba49550c15f5d366abe420e7ff2
```

```
      459cd7af36f5c285981adcf84020b04a66a0bc58172f8a34280fc32497a56308
      238a9f27ae95f0a593a70ae7594260e60930695f5f803eb2210fe3ac61c8bc20
      ec2566dafc399cea81a3834619420e5d85476cd573c7a08eaec4c60cf7999acc
      98724b934e259cda793dfda761cfa4289530b1f75b6a592730b8f5607eba701a
      150c38ac0e21038bfef496d2cb808f7342317789d1581b6f8565e3018d796013
      fed26b59fb226b5988633923a72a9acf42960c228f1e25b84f18ba4fd8762067
      9d6c7a9e5f4340dadc3af252afd28231e3d52cb924209e50ba1ca632de811ae1
      097cd89803884a8c750663baec78c90254f038574fdcb74c527610e21469398a
      20abcce9f50e1537867aa036bf1452cbf70850e8a5f5464eccc8a2af260a4550
      7e2da24c4868699065c95e3946ace90a655696f654892d8470a535cda5d58c44
      c8c0cb7bcc7104a847bc4cb1f03b8872143f5491c9e8c8ed46a6a6703c07d42a
      b8fabc4e25477245754d718ad8c88ce753c9756c2403948c06c1345c570fbd9a
      5932982f326a2f2ac69ebf5a58bc788fdb72a4d90865d3169d7752579cc49ad5
      e27479260dbba4800b521d21d22eb633168632b5209c4b81f32026a8111e07b1
      48babf740297af87239bc760b976862c551622416a6fb23825112308867ba70a
      75ba33179c2373b97492235a27c1f266cbc18f71c0596e47a285bc2e09397a63
      2309ff67739cb132d8c4007d2926fafc5eb56a6cf1960e87b4488c4895aacc6f
      cbbc4b6dd2b56cc69616653836550bbb9663b678370c3916fb832e17ba753d04
      787d78b0ddf11f6410bbe847cd6b1abdcee2835d50867a40137723433fdb6e94
      f902fda88b96d95af872000447c3649a93d3e0013dab5350dbb45c6190089c56
      cd4c1fce162daba74abfe8ae673105e0ebb94e52b37967b609741eb4608723e9
      858937b4996269033ca2cb503c4d3ccda0e15137cbc602728cc9bb5cca55b2cb
      c4579d02bdca430a052bbfc68bb5c8eb7c0139272c545d09f345b49a800314ca
      63c5097ef24cd793946410a931d5437becb557197affa37071954eee9c093a34
      86492362595761c83aac2ce46cdaebaa07ab3c3c1363c15bb8c4c869f54c6fdf
      a78924b954e0b480d3a128a2f64f7527beb2ec92ea6994dddc5eac10bde8a456
      09784e7948b6acc7c5da8526dd970870f46812bb0b53867668e17183fa638926
      1fa5da9a3ad8451094cd8ddb28683c1ce853c0e1cb3a4f79a168502242f66217
      2bc21609492fa57a9f077a1889c42cb2aa3bc2583275ce6b171c3e3aa4279483
      b204cb3a1a98535a2fe7c1b3d322c52dfb9e9ec46f926562ef1c8992a2bc5fc0
      47961898d1eb3d35cb1a018cb440d84de5047e50a4abd891c84f9431e36bb813
      4642e6fa144c15307a5122f07252b1e65b0e9ab3c2a184826c9a9cd938bdd588
      138a731c1b51787f166ca6205dadaaffc05c609f747b99fc3b918359e2ac28c8
      a5c56444bdc60568802791c688afac3c2c14c583277ca2550b7845a996208245
      25f2f8cb7d8cfbf3cf8496728611a6567afd446a6ed1d22f6d32f74ef266a97e
enc:  3d857eb5cb43c7ff163af7fb9ec804af496e4983f139bcf54a5b91a32399f63e
      57d79e8a80489c5355f4d2ce61613cc152da4a30ceef8ba9e36846f54a6dc3cd
      45f0191ba914e7da0e2b82aef47328972509157706f71a101685522602b9e19c
      b0574d2ba630a4b1d6cd140c8906d27c8d9573a59cab066acf2aad92a44d2a03
      1b74d64dd1f1dead0612238a470aa089979a7b0e881cb7655b2182a760e4b4a5
      95f82de5dfc4913bf0326bf66791ed7193e2c3b214d679ab1065823be1c90fce
      2539359338b253d3dd00585c9e4febf87afc2d0cba105e37771cc4b0f5606c09
      c03e10f3c41f5f06273e2e4d7e85a7a7c0fa7aab5b785af951034f0e4cd06da1
      b7b64becb1b2e670a6cea15d5e8cdfe97d401ad9c8411805eb4943cba446c88f
      243650ce185a77e16bf9c8c76b7ab77584462dd68d86cc752f8ca4b4314b6b8c
      ee563b65d47409abfa3c9f71533cd4799d4a0b437525ea0d9f34a76b1aee5903
      f81079486d2cd759326dc3e385903f64c237847449638dc42b4b3af9d2c9c4d3
      8624a7f766de56f82167caf480dfaadc8565b501711f2500d3cd3ced261f1c97
```

```
     a3268c2d501f76c4b84d5c81fca4158d439e0357e2aed6c706955e57aaeb633c
     1490225dcf7160b5d8acc4982a9c5a93fe856dddb86da2d4d68fea777b07f4a0
     50a248876c8750f72c4b0e09a53f98c0b6ea0f62d455c25d200eff9d6c41e95a
     b4d5b402f63bf40720af8d8f5204c2b53c6916e345e38072c7716e6e54261894
     f55a6c0ded181e9edfdaac22282266e6fbbc476654e3502a1056949c28a1e0f0
     6b5372f9826a5723e86bbfe2e74e72028ca2ab0172f5c77c403ac8a5afb650e1
     9eb8580922eba51f8ec89272b15f207cbe443a25d9a3c3b2c3a547caebd0cb1d
     262dd5635ba96e0e83ffead58fed63cd3a44d993138367049b706168c649f5d6
     55edfffacee55ec2ff190baaa437bfd373c2cadcb330ebd6e7ebc416d249a76d4
     bfd871a63d238b64aaf1b7cb8e9007075a9f48fde7338418d3231c3954ec3cb1
     922ebd531d54927630b1166c5a5d33886242016adc74730e7a95c315964eb9d1
     0a7d5c3a2dc3dad3bef04f26cc2ce98decf709cfe2343dcfbb27ff588e0abb57
     25d0c749888aa3369331f389a4b82b427ca8245f4d5555d63067178841c8304c
     f57ed595acc2e0aaefc82bb9234da182498cf33a5936fd075e02f2df1f31d8bd
     4292e7fbb32bce4d1e7839958213c7bef1e2032a4ed049defca29166aff2efc9
     0ce527f24352c3c87de024a561cc97000679fc9b86a5bde16c5b1613e4cf1984
     5e71aa4a7ea9fa41137b075573fc22549b51ddf15eeb5f3fbd5365975e4342d3
     5c976f0bc4c13d8208760b8bccffc5fbe3a979a05c5be681e31821180fe564f2
     0aaa064dec3b9ba3ee158b62a42da3905338714778030d09ff5f3862da161b18
     ce32243e0bee3e56014883d3391a3f2b37fd382f5bda0efa28ebfd64c12b12c3
     a0341fd4c615e18f1d35c1c18f09835cfeb61e2d0ac29901cb2999507dcd55e5
shared_secret: 8219cf90147641e74d200112c5b7f6310ac1fb1faeb822a19b8c078644cbae82
key: b4d1bc90fc6455658b2d7d8f1f2b3d14
base_nonce: 0e0a56bbb96f8a4f6783c7dd
exporter_secret: 02ab578b50c7c9948ffcfe891f28da38e50e17db752857220a1fa19ac077aa37
```

A.1.1.1. Encryptions

```
sequence number: 0
pt: 34323635363137353734373932303639373332303734373237353734363832633230373437323735373437343
638323036323635363137353734373
aad: 436f756e742d30
nonce: 0e0a56bbb96f8a4f6783c7dd
ct: 066fbfe3b5a6a046c2a91150ae385a5567b9b71dd9f1b806c0ab581ff2291fe9
    b1ac414293fb2423bc4c0dedb0dcbd43950d1f039e5f4f56e15fba325d76ee47
    b53e4e8ee68e23bb7a0b

sequence number: 1
pt: 34323635363137353734373932303639373332303734373237353734363832633230373437323735373437343
638323036323635363137353734373
aad: 436f756e742d31
nonce: 0e0a56bbb96f8a4f6783c7dc
ct: ba8df93950d9ce2a380b81de420887880a71d46e7c67a111f7e0237142dd634b
    fd22e309bd73f808b8877611285bb80ab69e34522dce4a1943636fb7263cbcd5
    967af8294b2113c81ea2

sequence number: 2
pt: 34323635363137353734373932303639373332303734373237353734363832633230373437323735373437343
638323036323635363137353734373
aad: 436f756e742d32
nonce: 0e0a56bbb96f8a4f6783c7df
```

```
ct: 7e911a4fa44903564bea06c8b6519f2477b9cd2ef0c6ac23a596829e0addb981
    84241d74f0ac6dfcd0ae35c9b9a710a6ee1a9f425ae41c64dfcf0df247401462
    ac0b98f8216567b97b72

sequence number: 3
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6382303632363536313735373437393
aad: 436f756e742d33
nonce: 0e0a56bbb96f8a4f6783c7de
ct: 6d1e5cb9486be24f74d50f682ea8557a00344baa3c5a33a24f47ba6ceb7ea949
    4c3dcdadc6ff0a04db2de2ed75dacccab6e92857a21eb692ff10f56b429f1def
    6ef0e8a944de8b1fb0e8

sequence number: 4
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6382303632363536313735373437393
aad: 436f756e742d34
nonce: 0e0a56bbb96f8a4f6783c7d9
ct: 3de29dc9a53019232c1cb59a1c149ad3fa29c49ce041d60ba8b2b1471357f193
    124d97b187278ef3e17711c265fd77620d1ee298188d5fe5a5e72223737aef1a
    8168510008d8bcde3e2f

sequence number: 5
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6382303632363536313735373437393
aad: 436f756e742d35
nonce: 0e0a56bbb96f8a4f6783c7d8
ct: fa7116499c40c77c9ee646fd15b696038e99c730b11a78b48f4d1483eeb974a3
    66c6f2f5cdb4c57c1177868c74c608e163e4b8bd331ce0714d73dee2afd228a4
    23b52e5abf21a3ce6e82

sequence number: 6
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6382303632363536313735373437393
aad: 436f756e742d36
nonce: 0e0a56bbb96f8a4f6783c7db
ct: 924bb66b04980a64077f4fc2d8049076df4e1fa0a471efb99b9a07d66c0ac0ce
    56ab291bc2d5ccecd72f4a7313ef80a89c33809424e1cc9518f10c6e924cbc8a
    323446b0b16e6f0f46b6

sequence number: 7
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6382303632363536313735373437393
aad: 436f756e742d37
nonce: 0e0a56bbb96f8a4f6783c7da
ct: e9acec247a7d1c7e170373ef91d0ac3ba240ea4245a3a947f45335af678646e0
    b1f98e1d9fada646f4a698d7384b9d8814d2d911810791f9788bd6b0e72dd60e
    7e834fc109bfa76dd868

sequence number: 8
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6382303632363536313735373437393
aad: 436f756e742d38
nonce: 0e0a56bbb96f8a4f6783c7d5
```

```
ct: fa8d179f8bf0361f669062b8c85c5224a834a102632a329a799ff59d18df6cab
    6df3ee7562fc1b1533ab3df1000a3fc0bfee9c5d53c1d25b8b163528e3bd37ac
    5ac3f4f3fe3acc2489c4

sequence number: 9
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6383230363236353631373537343739
aad: 436f756e742d39
nonce: 0e0a56bbb96f8a4f6783c7d4
ct: 5627e638dec5ff2c710a97c93d6af28dd6fef0df73c9568f21bb5663c0a9e760
    65dd2733e524f3e526a2fa3bee15d53c95e1e0ac34bad47eff503617ca21bc0b
    e9254c17e286c247f58a
```

A.1.1.2. Exported Values

```
exporter_context: 70736575646f72616e646f6d30
L: 32
exported_value: 6e94c470456dc829a017fbb0a46c2a0a7a95201bf47c88a5009c22d10f16900f

exporter_context: 70736575646f72616e646f6d31
L: 32
exported_value: 77d8231301d7da124c55368967d7cfa7815e5461a6d50135b04a8533e8000ee1

exporter_context: 70736575646f72616e646f6d32
L: 32
exported_value: eac9805ad130ef4b8df71cdd2bf39154fdf4696d7d20c3289b5dfbe457db3f36

exporter_context: 70736575646f72616e646f6d33
L: 32
exported_value: 3c5facb777a72abd6ac2495ee8698faffce3a4bc4d92fd245b0f11a844e97e9b

exporter_context: 70736575646f72616e646f6d34
L: 32
exported_value: 7e8ace50c6920301a71481fb0ab80aff2257ad8fc8ebdf53acfd15090db8153c
```

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: 346636343635323036663665323036313230343737323635363336393631366532303535373236 65
ikmR: 870150f8c622ea6866db299c3348c737f0e8da17c1e7f721029b5e035db59421
      68522e0bea336dd93031199ab74b3acd684cbd03d6e56f304e5c28e7a9cba3bc
pkRm: daa944e375a5c36c1f3771be499c297aba61d8762694256ef840460d10bed594
      641d58446e3795792c51f272383e78aa517112197230c3604993182d046679a8
      70495f1c44a6e2b30da7c251034f127561e02a234d0bbbb4ccc5a15224d06431
```

```
      08c44ad2973085371c80a064eaf524ebd90d5ad6057d45326a8b4ef532a7dfa9
      3ff83783ece423106c8b1ed2627b59ca34d71a3b4014698c9969db604589270b
      492124a80eba50909c2847a8bc9881b0788de95ad718a9c71a33b7ba98ab8ac3
      1ed744ffca6d6e08a170084c072bafaf7c25d5f56c519a6e3bdb30b0906192e2
      671da765ef53af8ac0197af2c9ac794a4103859976632371834 7f8821f3888ce
      250b84335eb8c43de4d9720f26b92531685af7576f62c6f39249c6645433387a
      8c617fdeb0650f77580de2af30019eb9959fb39ca2ed5364fc0a54e4809ac6a2
      424d284113e25179427b6a22936dc5839f3a9cb8bb49a5239ecd09278e432f65
      59bba0d56f9a9b87af068369c207b040022306a5fcc64d3264338a0789d7a833
      ad280b9ef2619c75769ed124a19c89a9b00a43c934b0042f24e28d2c353f2718
      ae9eb556bcd7c408f01e07bc7ad1d563b411133899312e5c6125f3cf39448ba6
      4c8a904414c32a8fc233649a2a69b98ab658094908f89c7089765e8211e5c75d
      949c6e53c6445d11902b25b452da79db853b78c8a629f1c5ef762f34f2126a20
      92c85b618c1a1bb506cd60e0c8b39b3c9aec088494c966878db1c3772b0992de
      4cb3a4958d2c43878f681a53cc207f446c6f95addb7047116bb4d5124b5fc532
      20401a7b5531fbb49bafa345479c620bfa8529f2a73f830c975b820b465a9745
      3483a746ec573289a8c02b53906c7423dac584495b6c771a60db498ae478a8f9
      a9833c81666a55a47a01adcd189b0e8c90aaa382a1d2301a873d9370c12ecc61
      04516e6b2957e3a7806c551d96aabe3b5cc47f918c467732dbe3a138305490c3
      8b33760d4b164bd509595415a3b560082a9b688b386c20f05c0667631555015e
      ba61e87174600c1fd0971b4e776e8452ad50748fd5a783ade73d80a97c8b07a3
      74ca53ba95c89157b5e2bb333518adce58c5ad90734ee20cc4646382f4bb91d9
      431968895f541a25da9a892c7086cb361e4240ae996afa5445c0cba188d13e4a
      8863c6918a7e247aa893c055a052bbaa3bd1b2731207006e5403e8742c844605
      d4aa64963b0af4978fbb7a1e409ca5470395dc24a700a850b189039f87bd2c78
      58f28a9e2c624ecea50f1f7889f6a99cfcfacb0c5861586c3e97a41d855319d5
      930e0aba9eb1b1bf013b32f6cb0d1570243eda540538a288d13bad128907d079
      25153925e9253c117e82ab0c27c49fc68162e465b0e3fb7c1671c0965c71b583
      6862301a85606122896e8d9a6d848c1818580ddc7955f3446f148338ca14149a
      205a3c6bb43e30abcf20a69f36a7a5e60efdf69b5922cd6a7744e420311f3b9c
      b2148ab6ea7e11b522c81ab0209a43f8da598f580fc8536b2838bb8ca0c26690
      5270609304ab78d6c40fa8a7015862b80ebc34a9ea25959a3c3fc4abd56a7961
      6215f2caaacb51033e02ba4b446c0fd47e515ca9ad44c7e3a2739b9b69242a6c
      c528880491c72c7858ac13804db088a97541ed11208b369bfab3c8e4890ff1c7
      3f2d783004c482458980eeb21f40c73d5d5282a78279d6f71bad650843c83d03
      23a7e90748b555853a50c091c31a9655b2388226e4524cdcbabb61543eb7caa8
      8396933e1a5986986e41da209f131a9bbc9a44d66ba077229c499386a4418b99
      0e20707c323846c861bcf227b2ff6ca3ee6511b37c190618c1e610be4672507f
      f7c7f5486930670d99bb6c2c28afaca54b815144aed10f82c27ad8922d5a9c86
      b15c9da866ad0ff96a2f569b42d52cdec8793d0414cfc35ddcebca8066b25e93
      0b36743db6b05a6ec6641b9403f88a5320842522f388683c72eb60bfe1db314a
      0b78a0a0cc76a692137c9613bb47c3f54911e67c1ba48a46081fcaf0974783ad
      ddc88492943d8b5934a41b46f95120fce5a21e0223dee7b140a924ce711e0e93
      c434616b58b02c2e30352599380ca04127f40a4134c5862c3bab08a3f265a467
      9c989cfc1f24c9c553cabb37ab2767f5ab2d7a20e57b0b65fb6e4a6119ba33a7
      36a9568de2ee95c312aad4c14639282831a3461d6e08800b592c8aa9d7ef6028
skRm: 853bb5356a7c01b988eb86bf51606f1883675aa8c65af838d436c31a0413f826
      bc31b870405cccd2aa04fc7922787459f2e33460a4ba65e89c9b0b8444f1aa14
```

```
c90ce8d594b54c4e442b2529d1540dd88674b2a4a0c527b419281f733c29b62e
dbf99225296a6405ba4f3997dd54688caa22c9045f27426e3d3a73772a7f5c80
0586a51db77130ec16cc9405cac4273e5977c2bb6a4657487f91e823250c843b
6cbbd2a879b4403b000b83a1d30a6d720f6e8032cfcb50997b0fd0a94bff4482
b3a09484d1ca231caea18292fa37728a2b77bcf8bdc697b288b5b2fa70764751
211c23c4b22272eb072130401363a45b319534160cb7fe393633b07c46b572e9
c1057cd8b586cc67bfecccf7a16d01bb7640fac6e50a557b64500c4ba3a6a025
1e44a332a36afb89a4a816429c415868d557f8694da5c513170359d7e7a63182
a5b2c00618e8bc1a02278c5621421a0bcec1b6c21b86e3319c6dd4831a885c15
b595c576105246489337285484786120 3d5927b231e43801748ec6718b709338
dc32757233a8e3280721a7521b8983d01ab0c88615cf17046240484798821599
3f7fc2c53121b2aab4481c28ab2433180a9c3fccc3191a2a5086b305077c1487
a03f0581a236fb75840450cec723b4b43f369b1e9b87a860c65c9634c3615c58
ea330101fa2d95565804562472a72638945e5495ce647bb5bb1627d61a3e146b
7ee4d870e5d9c975888277b8b6fdc02cab4503a1d59a95e31a2a86cd3608930f
4743f4e59d9b8bc55136ae6e14839ce8c17d136c8e1654aafc0360376cdea7b4
f3b702a53cb7fcfac83f8b1b29269c956c021505493e6c4e7ab1b90ea3cd8bc4
b081aa66f7e752bd32cf7bd96b22f71a64c1b4e452525941b36ea03114612926
b603561824a7308b2e735ccaeb52d2e4ca51a39aa493a14ea3714bea165049ae
0c6aab2d472db7b684ce715daf9771f3cac37a7a944ad3623c8051daf8cb64d4
6f7594a757197103777036d1006bb272b33a649ef38c5027597d5a3ef29b160f
0597539718729839da523c71834b4da496edc830d70561667a2f78960d5b654a
8991325f55063dea5dc601cfd4d042aad14127b9b707bb18cf588550177ddfb4
acde55c769d49f7fda4af5ba042b499ff483a06a587ea2089871d659b2aa5f89
8864a6f46b918057d34440f11927816a0491c5c419c0aebd8c6f99812a1515b4
7d9b7868f614f1ac3782462a0c0a948ad1b4a2b31aeb0aaedaabaac5dac348b6
b257d92d10725baed1105dab630bb736f7c408c2c9cbecabc8852094fec27109
c00b29c0b05cd08206e28667a95e5ba17664569c65c954e6e6497e827cfca732
f3c96bd833067aa971f6a794f71aa9dc42a74d014a4ef408d528606fccb3429c
70f69b43e9cb11e356311c650fce9994c9c639cbc68bb04cadda772ffb3cc3f9
a075eadc4b67009ded3a501a15cb3d730253814ca0055462756d624785c950b7
065265e7334900b666f92093d7a5933c102c42b8c1b039915d1a8b99fca35bb2
5f033416200952419a8e38c11334a5bcf4251b52d0cf27d3ac63935be1a94bb6
598a662c06c188afc74870dc1a689c6203ae9cbbe2400be2f8a07889963e3840
41a3a38fb502aaca8bb83b9ce8c17809c37f2930668bf9c60d680efab8862ff2
05870101548042b0eac9e1428022d926530b9cb85ca005839fee2c246ae29220
26c147079bce10858f70b8547669785c286d7b14b84131d15141c3d6ad1ae89b
58b7bc5d29c2a7c90408300233198ea87c2acf22097ac92117ac9a343721b68b
148a1c28d9d6240191755332cc37e5851af485b814c4bac669ad242da27b43e4
620d888645bcb2b90fa31bea0c3047b9b11c519e01c618b4523f602a88ad2161
e88b6e85f88ea592a1b3a12c0ff52a126958be947311a201efa7b11ddca1b682
c756ecc5a149abda7904c8fba56b92bd583ccae4d12e3c073922d69bf52239af
289a87303deae153ec7255d3011a6123a729a60f7b469f80e05a6198937866a7
5c7636a103bf73772296ca056027a7d9e808a46a47bd385f3740721bf1c6fd33
40c66a64d0fbba1b2385e15c1cd45a8d08c7a03f667a3477ac01c264de1095bd
274c3639982386562ba96b2ddca4e96ca6675cadcf747a91158a2a303c841b4c
daa944e375a5c36c1f3771be499c297aba61d8762694256ef840460d10bed594
641d58446e3795792c51f272383e78aa517112197230c3604993182d046679a8
```

```
70495f1c44a6e2b30da7c251034f127561e02a234d0bbbb4ccc5a15224d06431
08c44ad2973085371c80a064eaf524ebd90d5ad6057d45326a8b4ef532a7dfa9
3ff83783ece423106c8b1ed2627b59ca34d71a3b4014698c9969db604589270b
492124a80eba50909c2847a8bc9881b0788de95ad718a9c71a33b7ba98ab8ac3
1ed744ffca6d6e08a170084c072bafaf7c25d5f56c519a6e3bdb30b0906192e2
671da765ef53af8ac0197af2c9ac794a4103859976632371834 7f8821f3888ce
250b84335eb8c43de4d9720f26b92531685af7576f62c6f39249c6645433387a
8c617fdeb0650f77580de2af30019eb9959fb39ca2ed5364fc0a54e4809ac6a2
424d284113e25179427b6a22936dc5839f3a9cb8bb49a5239ecd09278e432f65
59bba0d56f9a9b87af068369c207b040022306a5fcc64d3264338a0789d7a833
ad280b9ef2619c75769ed124a19c89a9b00a43c934b0042f24e28d2c353f2718
ae9eb556bcd7c408f01e07bc7ad1d563b411133899312e5c6125f3cf39448ba6
4c8a904414c32a8fc233649a2a69b98ab658094908f89c7089765e8211e5c75d
949c6e53c6445d11902b25b452da79db853b78c8a629f1c5ef762f34f2126a20
92c85b618c1a1bb506cd60e0c8b39b3c9aec088494c966878db1c3772b0992de
4cb3a4958d2c43878f681a53cc207f446c6f95addb7047116bb4d5124b5fc532
20401a7b5531fbb49bafa345479c620bfa8529f2a73f830c975b820b465a9745
3483a746ec573289a8c02b53906c7423dac584495b6c771a60db498ae478a8f9
a9833c81666a55a47a01adcd189b0e8c90aaa382a1d2301a873d9370c12ecc61
04516e6b2957e3a7806c551d96aabe3b5cc47f918c467732dbe3a138305490c3
8b33760d4b164bd509595415a3b560082a9b688b386c20f05c0667631555015e
ba61e87174600c1fd0971b4e776e8452ad50748fd5a783ade73d80a97c8b07a3
74ca53ba95c89157b5e2bb333518adce58c5ad90734ee20cc4646382f4bb91d9
431968895f541a25da9a892c7086cb361e4240ae996afa5445c0cba188d13e4a
8863c6918a7e247aa893c055a052bbaa3bd1b2731207006e5403e8742c844605
d4aa64963b0af4978fbb7a1e409ca5470395dc24a700a850b189039f87bd2c78
58f28a9e2c624ecea50f1f7889f6a99cfcfacb0c5861586c3e97a41d855319d5
930e0aba9eb1b1bf013b32f6cb0d1570243eda540538a288d13bad128907d079
25153925e9253c117e82ab0c27c49fc68162e465b0e3fb7c1671c0965c71b583
6862301a85606122896e8d9a6d848c1818580ddc7955f3446f148338ca14149a
205a3c6bb43e30abcf20a69f36a7a5e60efdf69b5922cd6a7744e420311f3b9c
b2148ab6ea7e11b522c81ab0209a43f8da598f580fc8536b2838bb8ca0c26690
5270609304ab78d6c40fa8a7015862b80ebc34a9ea25959a3c3fc4abd56a7961
6215f2caaacb51033e02ba4b446c0fd47e515ca9ad44c7e3a2739b9b69242a6c
c528880491c72c7858ac13804db088a97541ed11208b369bfab3c8e4890ff1c7
3f2d783004c482458980eeb21f40c73d5d5282a78279d6f71bad650843c83d03
23a7e90748b555853a50c091c31a9655b2388226e4524cdcbabb61543eb7caa8
8396933e1a5986986e41da209f131a9bbc9a44d66ba077229c499386a4418b99
0e20707c323846c861bcf227b2ff6ca3ee6511b37c190618c1e610be4672507f
f7c7f5486930670d99bb6c2c28afaca54b815144aed10f82c27ad8922d5a9c86
b15c9da866ad0ff96a2f569b42d52cdec8793d0414cfc35ddcebca8066b25e93
0b36743db6b05a6ec6641b9403f88a5320842522f388683c72eb60bfe1db314a
0b78a0a0cc76a692137c9613bb47c3f54911e67c1ba48a46081fcaf0974783ad
ddc88492943d8b5934a41b46f95120fce5a21e0223dee7b140a924ce711e0e93
c434616b58b02c2e30352599380ca04127f40a4134c5862c3bab08a3f265a467
9c989cfc1f24c9c553cabb37ab2767f5ab2d7a20e57b0b65fb6e4a6119ba33a7
36a9568de2ee95c312aad4c14639282831a3461d6e08800b592c8aa9d7ef6028
3949cfabd3826934e3cf45f4b2434b2a87903b3a96c1583e00a483a275b70b37
```

```
      68522e0bea336dd93031199ab74b3acd684cbd03d6e56f304e5c28e7a9cba3bc
enc: 1802b2a838a68a16dda7b325b012e934176754eddab0f1ee602cb3f2270943f5
     fd80ec521c7206721eb450061ed0c10e492f9db923e2c373b7eea36d73893a12
     d9a02a43ab1ad5a752be1c4a8cdfa07d36e495113036642843e268cce92b841f
     a9a8167c65238c127087207ce067cbb0f1b26552183cc70efa45ec85bf31b627
     a0c1607c8000ad781bf68b8367c2a7338e6517280a12f5c9888b70f4d4eab2b0
     46b6b7d55e3fd7f5b984456032cc7705d16e7a15bbaaf0672a34b0a2fa67fb98
     dfa086b00236c18bfc902d9ff405958247359be38a8944ffbfe7eae2869d315d
     5064818865e04fa4f745dcfd4fd990068948fc95b0e9b016f42fd1b85f2a0a3b
     c62648c9847ee6b9883da7fd80095f1cb2b182499c9203e5e940d7bfa39e44a6
     453259a283ee653dbea2e27a935c69bcc0be69e4e9681993027a5559bd1f6c8a
     4297cb3d9442ea4bcee1c996ca11d8afbc07eaab1bd1fe34a23d5f39070580df
     208f13baf369e6a12134a3fd86ecb6980468fcbdf0df8395540d9b87e159158a
     322dd19f2e554a90bb8436a23ae04ee60416f1dd824cfdaec6e8c800f7183933
     c6b5aa909b0c80bfad0350cf21d06bb1bb0f3409d1ee6aa4e2367c7c3b54e062
     b83ae8a667e02ebf211c037e2debc941a903bba1859f115f48020fc50d61fa24
     0b5f801e425ca7f6047d00ea0d357efb35b2061b03a65dfdfb29df09f207bc60
     abcb47004726e7796f4ddd340227cda7d1041574944b1418675b832c7228e6d2
     6c6e14d69e43fd523f032c34bcd250b900de72ab341c0a25026aa466c5b0c767
     337b0f9db817d4e839c1a67878a3c4174ba5ecc2162ae72c34f1d4448d585aae
     ae3e25d1f7b484ec9653e01176b6f762d21e6a84cee1b6adca09a6a907b1a31a
     d3e8bdfe789736a3027ed785536f7218e34dd10a02c1817389cf5cd1f5d1f4d1
     0e60e7702a5b9df3157be5076811c613d04132a91f904d4bdf54a139e17e1bed
     28adc7c1ee9ff8c1e11aa3fd33d5e78f906663c71fcd3ea7f7c3de70a67dced1
     0f461c169e939365c4c2e78a26622f8334031a9311417793c4fc991f1df2e19b
     c505b063ee338ae49f55c33786783cf57aa98c49168b70e3c5bb2968a9fffe7c
     6eb1ec7fe5dca7c2086ad6732009f1e8dd8add7027eae7de645c88efd8eece46
     2a9524c2c6be2b1b32c70addbcac53b7f8131af32eb2e5cd68efee83c46bbbe7
     9e8e455e443c5c1b567116ca7ce938741acc214fff509aa05187a362a377314a
     7df6245ab73e29caa841def7fafbdf5e8bd70c383f5168edc17e7fd2d05b5f8c
     a965adaecd9b14ba1cb02220ddc518d32cad710dbc1282d2f4f0ebb397527424
     5ff6b0c95db7ed1d1a41aec6d8f89a137d5a775e802c2cdd093efa1412058c47
     dcfe3440d22a2ab547231ca3b0c07c98be34c08fcb8ca82b8607e79527f2e7cd
     394c2c37b6f5ee16ee07e9111d4d56f9342320f9ddc059a6d6a0bbd2046e9c4a
     f28cd9e4d03c5cf2b89d3e2313b1e9dc3e1902efa83b68f19e4bfd2b118b626c
     7b24de303b68d56cb1f14258a1beb52486d58444b1081eba1bbc6b11ae815a61
     6f2bd920feec64007128b635dff762bec12f8c95ac6a23d2a31d3630c572d0ef
     57c5ca1248cae5bfb0b1ba3f28c1838353088d8ead2448eae4e1422fe792eaeb
     00601596d156e9a44f63a0e8f2e8eaae21bec1995fa756127b45e7baac8bd3e2
     410851c7f88e8e3a776ea18552b87237122bd1a8dbd934dce910ad3f9090026e
     bf5f1c4350a59bb3dcd96bef076a6a8641fb938a2e51bb5b20954a841a5c0990
     124effd6e08433046fc6204622181c04825a70e4ed85b75530706e50ef7f68eb
     a5b8390dbac31e7a61717d241d13ecddef20d1bd92b11ada157f85bfe2f44c76
     58f06827b27e94fdbad77acbe27463d8e32bef47f25f449433a14b610285e0c3
     7e3192922ea9af4c14599e4d71f670625a9bdbe15ffbd3cf7c62764ec7ad9619
     07a20011d88cd62e6aa943a3786fba28fc2f9738252a20b437ff165d6eece219
     eec42ef2e4cb796bd486197008e35938952a244bc80c4d50d109f15086a36442
     d0307086eee8f97f609db8bbc3d86a808a71961c21b49366afae13df2c0c788b
```

```
     0a02eaf12914de7b1401f656221f01e6f329ebb56298627a802b1813811986bb
     7b589fb982200855dec230145d10e68302f6f3e8109fe05f51db91d0bb89522c
shared_secret: 75397a4c8153a1e8313a1ec8f8f17ae17f686bea800d11e655bedfdf1240a94d
key: d5a2194904c883579f2d4c979a00828d360397b0a7f536e30aa9924260f79546
base_nonce: f60e5f7f7adecdcb235a6ab3
exporter_secret: 3999dbd59aaaf342fd1c46bed321d69ce3bac2924fe8a1f220ab6b6926e6109b
                 f96f7fcff88c394766f15db00a84417a
```

A.2.1.1. Encryptions

```
sequence number: 0
pt: 34323635363137353734373932303639373332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236353631373537343739
aad: 436f756e742d30
nonce: f60e5f7f7adecdcb235a6ab3
ct: d26a4a372a2bc3611d59820420d1f3702fa593ad75f88051a1797a74dab7fdf6
    0740e027b0f484e5dd46c2c764bf49847b19eb3843cd25030cdd72f34bdb5dcc
    3f1e37f952950a5eb1d9

sequence number: 1
pt: 34323635363137353734373932303639373332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236353631373537343739
aad: 436f756e742d31
nonce: f60e5f7f7adecdcb235a6ab2
ct: e3b2463c516962ff32524ee1d4ad75b4d32eb4a4e257b37ce29ec4c0365c399c
    d421555f13b805f8ca61cf403db298c77a1c967c22ce6dfaa0cc37c81cf93cd3
    ba55eb17f81080590c8f

sequence number: 2
pt: 34323635363137353734373932303639373332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236353631373537343739
aad: 436f756e742d32
nonce: f60e5f7f7adecdcb235a6ab1
ct: a795f543ac801d073373f7e3237fd112d5368a8cb9101ae8f2aac9962436bedc
    0c036a6f070f2c836117e87d3b71a9c65f6c3bf2a17044934615903acca1c6d1
    b39e944e5263bbf19d72

sequence number: 3
pt: 34323635363137353734373932303639373332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236353631373537343739
aad: 436f756e742d33
nonce: f60e5f7f7adecdcb235a6ab0
ct: e2a4ac42b4c29f676552d9be07f4a317a2b0485d6832ab99c4c6add4754ab868
    6e8f026f3f668e7ed5aba6f224b5c0a17507e1d06cc41765243725f6681d511e
    45c34ba06f349f2db911

sequence number: 4
pt: 34323635363137353734373932303639373332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236353631373537343739
aad: 436f756e742d34
nonce: f60e5f7f7adecdcb235a6ab7
ct: 58974681af44f0856a7a0ec11546570d99d7b111ba335168ae5fda7535fdfdf1
    c6b9b4e5e53eb40aed0f888c2cd032a549054a6351f3acb74606826dcef843af
```

```
    66637521274372e8f56c

sequence number: 5
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236356363137353734373437323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343739
aad: 436f756e742d35
nonce: f60e5f7f7adecdcb235a6ab6
ct: 5bcb647f3ff5621af4cc378da15f88e6dbcd5387c7a0434025dc6786ba7a4f8b
    3c9ff1a13e1beadc2c329a14bc60b2f2121db69252417202b01de7985d4824a6
    c374498f9d6518d2b832

sequence number: 6
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236356363137353734373437323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343739
aad: 436f756e742d36
nonce: f60e5f7f7adecdcb235a6ab5
ct: d47f7e7045713d6619c7a233a67728e8eb1217da5562fafa6010c7c5df59ea3b
    e12b5bcfe8653b4ec93b9bcd78d1ef8df22576d6efbb8a22b8ab1cb471fe288c
    5534918adbfcc668558e

sequence number: 7
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236356363137353734373437323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343739
aad: 436f756e742d37
nonce: f60e5f7f7adecdcb235a6ab4
ct: a401b4b367a54d225277aaeec493ce468e7e54eed05b5af4aeaa122f84e70a3e
    57479432ab9dbd1f717493d92fb79c56979c56066296db40edf07a4f19420759
    afd2b09d4d4c87b56572

sequence number: 8
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236356363137353734373437323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343739
aad: 436f756e742d38
nonce: f60e5f7f7adecdcb235a6abb
ct: 33732f5a383fdd87ae9195aa5c5d6131aa9e7c1c1746d3a94a8bc60fc5c9e95d
    2095ffeaf127ba2e30ff4da1051bae3d462f922e3e779f835be930ae7e2e39a8
    4bbc9f342d8e58a47648

sequence number: 9
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236356363137353734373437323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343739
aad: 436f756e742d39
nonce: f60e5f7f7adecdcb235a6aba
ct: d0511487d05701cda50f08a9ff8808942727b54a72613a17ac0f0ed9f3246608
    167f8caf6c3a829ab12f4b71ab0f7c133c940269974ee6f5f03ff6ffb54d290b
    00d57a7d41adb64dda03
```

A.2.1.2. Exported Values

```
exporter_context: 70736575646f72616e646f6d30
L: 32
exported_value: 4485ad8f84ff09f15913e170c7bb5a03371972f040b40c5257f65636dba5a3f5

exporter_context: 70736575646f72616e646f6d31
L: 32
exported_value: d957783c13e45f78f41db5afd809f7e8a8aee43ec39f2a239f0543703f233c49

exporter_context: 70736575646f72616e646f6d32
L: 32
exported_value: 11c9d52c9173c6b2279324fd67d8ea64bb4a683ace914360aab14843e7f3ea85

exporter_context: 70736575646f72616e646f6d33
L: 32
exported_value: c80a55731b4eb0ef577d11823264f2d84c5a1feb50fa83e821a8cd611f4fd8e3

exporter_context: 70736575646f72616e646f6d34
L: 32
exported_value: e2d71245ac6844509a5d2fc582a13aa04d14123f269af7b8abe34e20878f57a0
```

A.3. QSF-P256-MLKEM768, SHAKE256, AES-128-GCM

A.3.1. Base Setup Information

```
mode: 0
kem_id: 80
kdf_id: 16
aead_id: 1
info: 3466363436353230366636653230363132303437373236353633363936313665323035353732366 5
ikmR: 55380da5417c79cdf7ab79fee4974c79512cee6b760e847839dbcd52f2f45590
      dc89e7d0eb410647dc6c3a1046bdcdd20e13f21f6ecb2f52ee8de22ae30f2e10
pkRm: 02b2e67f202265a06ae6767f2de4df43766ce2ab7482de8231c834176d33a90f
      5744120dccd89789b559f484808aba17905b4ec2ea0cc4515f5706196f32449d
      c85912605a2541cbbda4b54392aef9961f69d550d4b76f1d20ab4c1b6876108c
      6f0113867180145821e56c1ceddbb40792182b31441ba669832c95c623bf3a7b
      c6ef719f8837aeb87371c4117db21420a2831ab7ec901a453f033b9ab0d0a75c
      366e5ab584298a6cce59b85932340499302f0610edcb536ff82952dc09e5b995
      90955c8a3b0f92ea8a77ca0e4e353687a25b83a083111b181d37375ea5b63873
      7b65a116cedc6347c37e3d9372ed64161e860481d4a853875a91e4ce8b06950b
      c92a1035c09510b926b42266a1572418b05bf4862cf17c6b740b3f2273ecd0cc
      1e21078a3612cfba9c1e983cc5b5608b9a23ccb989fc29b104028348980a8689
      bffbd31e562cb4dc999c8ad114a476b9d8294a7c86b6baa96f273a54a3b1b977
      635e51040de7295d0ec22691111138a02dd44c1e7ef599c249277bf818aba3c0
      13588c369a1dfe41c8a939c64f1699b10200bd6cb9bd27840d9374fdda7348e1
      a690c75c5c4663019b0911948e6212787602308572c2cc306630318eeed634be
      e186f089c1826581da8952f3a37072d02f2bd7789d7ccf671ab785ec4051b613
      2a646c3f534722c296068c7e4e45ca43a8413806a8fe31009cd1585382193199
      b4658486c970615ada52a62cca8089417f04495383c5b5d36287a27098671fc1
```

```
      519210157450e4c58a63b8aa86cd61c0b2dbccc5377a944057a9cf9ccaf56671
      71301c2425784653cc451a1bf5d5a033149e3a85035bf96d0cc853abeb1cb19c
      1bb8033e3d66750137b4da557b462b6e848917d8c61670f67513375648c710a8
      3011a7d9873be47a6d776e317a9d93455c765c8c7cc9b1b60c1f84531b54870f
      abf0248854c49a607afb186c984c0e634cc940f99f267cc402c2388f9441dc35
      2f072545f16805ea7b5d4cc9223d8728b07048d1d46c19ea7f77e09f7468b775
      a952e6667d01261f0a56282390b8ff7b052f13ae72f194481ac496b67c1b4b8b
      a0fc39fc9879cbdc8a590cb3e4d4207ea45f75d0209006cdb3033b26ea2f1209
      164b1cbdb7e36c9b99ae3d3364ab05c84139c6490c18ead061106855ab550d72
      4b8236544362b19d1d6c631708abbbc38fa0d18e03464b5bd34296c38606226f
      f43c81e5921f66fb48cbf4300428ad48b7c2d8bb5653e8bad65873eaa5a3b08a
      1576792dde541fdf3316cbd06d81accecc250beffb60537c92d736b0e3414bc1
      0961e1d08d4bd50dd77c629a392d07303c0177cfb9d2832445a7a4a4aa39d37a
      697b47b5a86a135c7133778cfb17bbcbc7ab4ce72ac5ea0468437cb775485751
      882a167550882018bc70635b595f9abe3f2a08d67cc48cd282c98473b7bc5779
      f45a825526ff6b1f24f22eb948382a60817de46fe7b4775cf06f0d2bc1a4b024
      c926089901680fa6cac17415548066ca0cc2fba8c460bc8021f833eeac2669f5
      135ee25281879efd415e16e1106e0ca763461ec3302825b234af071585237fd6
      b68e95cc8941b714c48c19c1b163303353e3535ac223273832b6785c355c0939
      f3b25dc9ba33bb6762edaab8341bbcd9b62ff7161ad2c73d6c29624336b40510
      c18dff669e2d7cce239f035d48cac6eff02cae14cc33dbba943c31e77d1728bc
      81
skRm: a32e5c3ff9ca98d2a8a7d70070f10e43786338d7c75c0f67dd11151c89ed04eb
      109b88c56818bed36411b65c80c69995903fdca056755c2cdb055c861ca3262c
      4544b47de91344a580580c616019d3aa2eb5a4e0099540469d34246e9a034b01
      cb8d1a7739b4b09329bc7be92c2a519907754a133877c24cf60980353fd18a82
      6cd8768d6351ed42c678e9a3c62733142ca2781b2465e7cf7453c6b53394ff70
      b8f423097df8bde1eb62521a632b03b3f4e04d96b38b7217ceb2b792b25c7a11
      da88bc883fcda660a6ca04fb053cc2e2990c0492b77a672c913569f0bc5e907f
      8947442e82a42bd45290848d82e542345a6988300b9900265d9b0ac9ea959556
      02c725338e6c7af881c58b04b83727bfd0110de0b6921f95c1a189c1ab5c0cad
      da60782c6b46cb5fd7db48886902cc4451610907d4f838beeb33dd33306fdcb7
      e7f8b52b469361a8a64afb20aeeac8c7870b6cc33f708239c5d1c236ca3d15aa
      81ce09bd446bbcd7ec607370872bea0c5228171681945683598 0cc19adf330e7
      4798ede62b9b6800cdd2037cb09174f376b0084bb51162bfa169a9254a78da08
      d6d3965070b48648cf685c717997654c736ced492b0f0759ea253e3eb7b2fe62
      02fc29bb00910d3103c8adbb6410d537a46a5aafe57750d21343451192b32ac5
      84cf5db5c7304b4956a608f54ac6d2a89794b932722c113ec7196517888bf9b2
      e91698ca5aaf8ca37328f4b7f5b519ce75c49dc279d6f6313d8880b2d7988b6c
      ab8cf41861b70f3f758ee1e88dfbf453a369aa591a7004cb6a5cd98947a50efd
      b25934b77bfcdb0cf8f3a0ef57af7ff1bc426a21dcb5b7d3b29239f576822c8a
      8dc35aa50670abe2c57c8003055a6c8c38797866192864c1f6c93a1891920e3c
      b57be9bd4242765002b21447a88172675c4b6308f28b96065ac63a5402275715
      2592e8702749e26b9e29a81f57522380214f0348c402cecdd097e0511c86027f
      ddf5b57bd5a5ff02a1b9024be9c044eaa0bb2d4239796136ba401d8b62bff4c6
      81eb1c0210c8a8fd730f7a8658943071a87651d2839e77678281873d7f66cc0f
      6cbdcf2bb41849cdacd63c3a374ccb0c45115c2406fa97956098a1c58d9a4cc3
      cd35c9203468c04c672504a91d1924bca63727906918c23283f108b013761357
```

```
bfc5813cf1207ca23c7abd429128454d40da28edcc3b310c6a00187ee9d35a07
a47c83525acaa07c8a0890db568f5ad7b8f3dc5f5f5302bc1b406f9851dbd361
08a67fe6bc83fa1187a12c3283977b5f320fff986952b6ae8a767029b94e4637
57b02a5ce05a80d9817bd6f16037b5081ab8cfe04136efd7123c5cb257ca0066
241aa9bb6256875d94f64135c2ac9e88b57efb36b05c74ed90cb6e07182578a1
e62170a302bd6f66adb1f1bac31cb1c98a81070bbff2595a89545dc1bca5f304
b81260b5761c48fd0ba0324181b283aa7e464379402b94a16366dc762cf28650
f262fb3a57b2a683f9faac77602c33613a6b0993925c3c1bf3bc88a880379c2c
3df506e8626f012931ba2442afc85884b3cb5384b5511431f5157b42e6b67522
969cfb4cf37ba37c3cacf8418bb10a88c281c6733b370a0231fe02aaac08369b
6906534ba2a4992714a5004061c24711268fe1523fa0a2c5d2613ca6049cc7bf
44120dccd89789b559f484808aba17905b4ec2ea0cc4515f5706196f32449dc8
5912605a2541cbbda4b54392aef9961f69d550d4b76f1d20ab4c1b6876108c6f
0113867180145821e56c1ceddbb40792182b31441ba669832c95c623bf3a7bc6
ef719f8837aeb87371c4117db21420a2831ab7ec901a453f033b9ab0d0a75c36
6e5ab584298a6cce59b85932340499302f0610edcb536ff82952dc09e5b99590
955c8a3b0f92ea8a77ca0e4e353687a25b83a083111b181d37375ea5b638737b
65a116cedc6347c37e3d9372ed64161e860481d4a853875a91e4ce8b06950bc9
2a1035c09510b926b42266a1572418b05bf4862cf17c6b740b3f2273ecd0cc1e
21078a3612cfba9c1e983cc5b5608b9a23ccb989fc29b104028348980a8689bf
fbd31e562cb4dc999c8ad114a476b9d8294a7c86b6baa96f273a54a3b1b97763
5e51040de7295d0ec22691111138a02dd44c1e7ef599c249277bf818aba3c013
588c369a1dfe41c8a939c64f1699b10200bd6cb9bd27840d9374fdda7348e1a6
90c75c5c4663019b0911948e6212787602308572c2cc306630318eeed634bee1
86f089c1826581da8952f3a37072d02f2bd7789d7ccf671ab785ec4051b6132a
646c3f534722c296068c7e4e45ca43a8413806a8fe31009cd1585382193199b4
658486c970615ada52a62cca8089417f04495383c5b5d36287a27098671fc151
9210157450e4c58a63b8aa86cd61c0b2dbccc5377a944057a9cf9ccaf5667171
301c2425784653cc451a1bf5d5a033149e3a85035bf96d0cc853abeb1cb19c1b
b8033e3d66750137b4da557b462b6e848917d8c61670f67513375648c710a830
11a7d9873be47a6d776e317a9d93455c765c8c7cc9b1b60c1f84531b54870fab
f0248854c49a607afb186c984c0e634cc940f99f267cc402c2388f9441dc352f
072545f16805ea7b5d4cc9223d8728b07048d1d46c19ea7f77e09f7468b775a9
52e6667d01261f0a56282390b8ff7b052f13ae72f194481ac496b67c1b4b8ba0
fc39fc9879cbdc8a590cb3e4d4207ea45f75d0209006cdb3033b26ea2f120916
4b1cbdb7e36c9b99ae3d3364ab05c84139c6490c18ead061106855ab550d724b
8236544362b19d1d6c631708abbbc38fa0d18e03464b5bd34296c38606226ff4
3c81e5921f66fb48cbf4300428ad48b7c2d8bb5653e8bad65873eaa5a3b08a15
76792dde541fdf3316cbd06d81accecc250beffb60537c92d736b0e3414bc109
61e1d08d4bd50dd77c629a392d07303c0177cfb9d2832445a7a4a4aa39d37a69
7b47b5a86a135c7133778cfb17bbcbc7ab4ce72ac5ea0468437cb77548575188
2a167550882018bc70635b595f9abe3f2a08d67cc48cd282c98473b7bc5779f4
5a825526ff6b1f24f22eb948382a60817de46fe7b4775cf06f0d2bc1a4b024c9
26089901680fa6cac17415548066ca0cc2fba8c460bc8021f833eeac2669f513
5ee25281879efd415e16e1106e0ca763461ec3302825b234af071585237fd6b6
8e95cc8941b714c48c19c1b163303353e3535ac223273832b6785c355c0939f3
b25dc9ba33bb6762edaab8341bbcd9b62ff7161ad2c73d6c29624336b40510c1
8dff669e2d7cce239f035d48cac6eff02cae14cc33dbba943c31e77d1728bc81
```

```
      1f7f35beac35f0d9d0891af5993f385acbf9bfbcf78e1a6a22172eb69701b233
      e5711fbcda10025bf909c43c3913fd55a803a7ad4af1b7cc3e1bc66ed5825f15
enc: 03789ff0079cac0a5970a544fc2afd9d5e67b8be679da649056199bbf24d0b47
     2d7936e3047ae98801e6d16ef42710009aa4aed663adb869c8fdb2edd4543ace
     210845b0e3b37d01a8a514f9af09502c654b8b695a948d1d6209be5ae7c3dbc7
     a5780501a1337215be3421ad1f4ad0105938df4918dd6fb149de82e96824d34e
     167ad8ef8ef14a82b69a0f5b53345c5529d456d35cd999e84856e655534c2281
     050c7453230383018914cbff18ec2963adba2fec9a2256ee68212b01c1a6a723
     b743331b9cda7cc5a2b53d9d29026ebdb9cad710da27285394b5103fb72de3a3
     540abffcc45368c0c5b0baa6b447ee23f31e96b227835ab6153d1da7961b1118
     3d7c4a7ae83148ce69b54f4973772bf9b73aea56134f809fe70fa961bb2f940a
     f3576fce36aa7337d9268556373be21c2fac16b6edd71f20abe8abdc34cd7ebf
     cbead2b59412455794863bd2af4cd900b196a43ce865b816f0a7e693f2ee9cf5
     7d18ab9c6e53822cb62a98a3ec36914d8d79d0879c4f7230f68a7e92e795f3df
     4504c713ccabff038d26889eef1a5daa85dfbc55bea514efaea6a5d2dbfbbbaf
     f9b9399a083d0bfa6ab3e0150e228027f2dec7a382f0bee352e4937726322b0f
     547390237e730e9e5ffe93231d1b274b7a469675c97847200db3e483240e1a40
     8c946ceeba8921d3a21335df852825634b5e4ac415cd4bb9dc7a779580c697c8
     a2e8a44e0caa8b1fc24c131593ae8bfa1ceda3c6354bde687a858048a8ba3208
     83a0008f1416ea354200a165d657dc83d0e70be89e930c110571271154421f36
     bb2697bd000f61c7b81404d63859ab564186bcfcae5ecd3fef794422f5564e18
     336b4d45b3320c8bc58615700a2aff7441daf73f7691538e02566dd30de47141
     24be55f461d8a3cc9afe9aaa16ff0bdc2a00a1c166d86f835a6d9b4af7367a64
     1da4f3473284cb1aae89bbeadcff6833245293bf1e355ab46f2c73a02bfe7faf
     7b49da1d39b3211b5b250b2efb99ed653c67d808c9a3eaaac54d9ec3af4653d2
     ec8f247b6bc91992c3235d6105f75fc2d35b9feb686eaf6650d79b95d3d13493
     5fc357c23588a277cc72d2a12c045e52dc2baf0332b00244c32b89f94412f422
     20f2a0ee9f174e5bf6a40775ad342306606c55f89e71148be23853729f884525
     6475653d8eebafced59a60ed40d22e1494c28d6b85d0bf2d398ebdc57d8c8b01
     e4081768852ceb5c9ab72f823bb5f195112b3281e4f9043eeaf3c318b6c05bcd
     603daf5ace18345695d4fb9a8a3092a2136e0ea76b9a7df45b259427215e960d
     6f4a5115d42e12aaadaece7b0ee54cb8df9a50c625a53d74d28582756d09f8be
     6e575d8ee0a98b0047cee0d7b10c7bdbfa14e5abfaa4ea4fb205d3a5e1a026c2
     7d74f2bf20a4b2c964e0d77d78c99dcc3ecc8eeca6f6045aed2a05640ffb90e8
     b3dcd3a250036661fe25241dde2b1dfe524a0654d43185f9680de661d854af15
     c5de6e198a616c6350efa50840778dd290c0eaf8716dded32c73434e00d51c79
     72c995ca10b70d212e958aa96912eee7e795f355c63110dbcc123c5f7007b440
     2c
shared_secret: f486c3c6cbb6b9eec34c92e1a4c6c34d67c2fc5131fd024e99f91548ca55e6c5
key: 32d5734f193d7d5778e1f74b19ec76e2
base_nonce: 49f4e2c4cf39ad5e89432f6c
exporter_secret: aab252b76068d21edf5618c2e6c9df0bafdcdb470a5d9444bf8f15701be6ce9b
```

A.3.1.1. Encryptions

sequence number: 0
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236353631373537343739
aad: 436f756e742d30
nonce: 49f4e2c4cf39ad5e89432f6c
ct: ece905f63a28c505fab9c5fb505fdfa283f00e211c3a2a591ab88c5d69baec80
    0e67d25eca6877c67b0a3d960608715bc77c09e879da96cb511857af6ed2bb77
    9d5d3a5f19696908a4f1

sequence number: 1
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236353631373537343739
aad: 436f756e742d31
nonce: 49f4e2c4cf39ad5e89432f6d
ct: 2dbd0be2b0f6fae70af1bc63ba4a69a2ed136db379bab588e8b0dc6c557ffd65
    5dd8131c48fc2d749d4497b6c681aa3bbbbdd6376275075c26f214d547859085
    90de4e2817d6c8e3099e

sequence number: 2
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236353631373537343739
aad: 436f756e742d32
nonce: 49f4e2c4cf39ad5e89432f6e
ct: 16560c07a109c5622fe7d7f77c924f7568708baf2a9da53986fc367cc318a3ca
    9201caf2f4d9ec509d5ff8b1b50f7c7d7e0aa83cb376b90e8a043e735a835a71
    bd2e3c36d0bb835119c4

sequence number: 3
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236353631373537343739
aad: 436f756e742d33
nonce: 49f4e2c4cf39ad5e89432f6f
ct: 38655f5116ab1c9c05673fb8253a6b60542fdd893c2d845a2fe6b8e9b2b16510
    bde8ba9a57f6e5bffee687990395009711a9eb728bbfd284bbe4e855b41f26d7
    aceee3cbea76480f3b65

sequence number: 4
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236353631373537343739
aad: 436f756e742d34
nonce: 49f4e2c4cf39ad5e89432f68
ct: f0b9111dbd51dadaa9794890a80e2f0537b84aa93634086fc47957033b6fdecb
    8f63ce954efce6cab68106edf8b9c3a8044324e96f3f347aff66a38b73ae7b5f
    ffa182c2fd94c87dd7aa

sequence number: 5
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236353631373537343739
aad: 436f756e742d35
nonce: 49f4e2c4cf39ad5e89432f69
ct: 408e05bac1f376e6fff2580233433c3831c88dc07c40afe70b7e093502a53a1d
    19f119dbac39422003a59ba1fc781a12eaa8a5a9507778f7de0266e47dbe01a5
    7ccd5fd071499ee68406

```
sequence number: 6
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6383230363236353631373537343739
aad: 436f756e742d36
nonce: 49f4e2c4cf39ad5e89432f6a
ct: 6199f9fa123028ddd7b499e9a0a7d794e72724d7ec4d1b9d1b82a5d215683a49
    39ae28d971af8e00cacafa1daeed195732fb5688ed9acbefa6732f33e5e22323
    3a1b37e9cb78a7d30b10

sequence number: 7
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6383230363236353631373537343739
aad: 436f756e742d37
nonce: 49f4e2c4cf39ad5e89432f6b
ct: ef682408c42dc13b2fe972acc43608e4ee81b0228aac5577a2fd146b0c069f4d
    5d4e863b596469dc48edecc41dfc8a80f391bde2ee29704a629e466a3cb1ad5a
    d906e5e3d763db0269fd

sequence number: 8
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6383230363236353631373537343739
aad: 436f756e742d38
nonce: 49f4e2c4cf39ad5e89432f64
ct: 5ae6bf362c525184737b51ea2c465c2005d7726603b7c76b8912eac93cc0e320
    a1403e2bbfc34c747838243b61bd90e52356dba6cc6fd646892e8980f19bf4d9
    b9bb3c56c33aee52ba3c

sequence number: 9
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6383230363236353631373537343739
aad: 436f756e742d39
nonce: 49f4e2c4cf39ad5e89432f65
ct: 6bc4c433c0a1114c282cff2ab7f67c78bbd0f98d2f81ef3b0836b27f02a8a6a4
    1f7de97b26ce4c4b77688a55534e7ee3c2aa8cf226d6beab5574807bea566caa
    46a1477a50eb968ba7bc
```

A.3.1.2. Exported Values

exporter_context: 70736575646f72616e646f6d30
L: 32
exported_value: 13692d4e39966ab8e802797324308b804b41ded773f817d6f6849db66319e638

exporter_context: 70736575646f72616e646f6d31
L: 32
exported_value: 777a5b866dcb6b65e39b33993197b89a278ff48e8a15c5f2a168d46277f2cdd6

exporter_context: 70736575646f72616e646f6d32
L: 32
exported_value: 35dc03962c54c752024cb04f7ac23294061cc10704f294deec5ce1f37ea8a137

exporter_context: 70736575646f72616e646f6d33
L: 32
exported_value: e2f130ada22bf6fa122a6d8a8c06a5696dafd81e721f79cb4b945b69593c2322

exporter_context: 70736575646f72616e646f6d34
L: 32
exported_value: 0b79b7222eed63ab90c3309aca6e2e2efae3c939db18fc91178154a0063f725c

A.4. QSF-X25519-MLKEM768, SHAKE256, AES-128-GCM

A.4.1. Base Setup Information

mode: 0
kem_id: 81
kdf_id: 16
aead_id: 1
info: 3466363436353230366636653230363132303437373236353633363936313665323035353732366 5
ikmR: c578f6ba281976bc8b51fd32443ff54caa774e3eb7e728ef6255a8e5e632128c
53a4254d24f6a6f6bfaacd0205bf53badc8381d42d623d802f60fa73e09743f3
pkRm: a20ebfe2b3116d5048fbd46e088871badb29478dd57204701ced68cb14ae8d6d
a29361a4f647e0a85536718f4757bfb636a37eb9cfd41c246eab6d4c655154d1
c1dba98831a7391163b30cd74a567104e7349d20ba34c0062faf53c3d5e46fd2
6245c3c50ed320027b799728da45ae1495fe164e3945348a33bcbde000d7087f
021c15130a3139245d8fbacb6d276ad3c4cb92d5a6b3590e99088e95721a6c63
5da32761ed7c7dc2f58e5839ce986141fb7183e485cd269c785d093711a287b1
612e588581fc9aca571207766a1bd4815b03587207f86918c29f0597aa2a4acf
21005a174a595b252116a3a10f7ccb197388a344545ef8c040a7c681b38f3f8a
4a245749d83838fc70499135b77ab5c4c6361be1856e5f1858bb2c0855991bb1
d17cb515b68e2226492ba31d9545ccf6258b2478d6c27183128f1b9400e3e53f
b7327ce41c9fb79b6507c10b2141be88e9c01be9021a2281b049a9e47452d143
02e2ac9d715839517849c9192027969acd3c6b528098196acb2d55ab4f394a3b
e274380a3b73a43f09e4a6d9688ba07cbfde68ac8fc26b821a8597cc0d90bc94
96b4bb52469b4be1a9d76c6347f9a8fd05bd62aa0b041a646415a659cba164ea
32bc611ef9f40e8d1749c0fbce1d717f96c3bfe93b5403699877c240787c3c2e
405bdb1318dbf078a741b9d08423e9539f66892f68791bcb112bac1551c7a46a
3ff8735d9417204a9308672e3a5a2ae2696e7052abb8c5b4e80ca69bb247b2c9

```
      83c3e04ee2595e565aa38a5ab7d1497d234593637c6efbb5c9db792691dc97cf
      d17041550f5ed8349d9b466dc4471c61b3d0eb05a8c0945d9865946992df6212
      ad85764a755dd3241a9efa74110360d10102b9050ac0d1063e8552dd042e541a
      8f6816cd67167b131c5756a337dec7628d8470b5d02055475cfc7c9c75d851c7
      f12334e37e1cf087952339a2c0043cdab7d667879da30922f111b8e60fbf5185
      1ba40830ab92777c897f47c6fa1b629a1b49ee7a02af26a52327800226269848
      561d3b396bc7694b35cbac7bc490f15e2456168d9245dcbba2ba0a6189559039
      b889f9722862f65dc41a57b007316b069deb09d0da6b61aee192c3943c3d7816
      e8909731a98adbbc7a0f569479db07850c19bab248be19caee92bca90b156a18
      14ad1143cc56513f6858e3ea52ad852546392c5b5167f9f608fae4b986a6c5a5
      e6b54c06c8c272aa87eb248fc1b198cb71ee721fd3f1bf26e368398c74ee4b81
      571b79e5360ae88c02f1e371f8548661fc45b9d9911cbca88a2cb912656d7005
      2d92227706e968648b032757556359968336bee0dcab61e5c431225ac0659ad9
      5a91f0290091b0615347453ad83212757b56c251cf8331037623b9625a47a6a6
      3859795a2310c3b37920b4713b677764e06e093b2606b22af59a82b95b472914
      af8e0c6617c16f62f1b150430c62da18e6c02486f94819287b01449a69b97590
      e49d40a728b9834bef9337a0c29464232d1e6a3d0c9274321a952a22aaad239e
      598c7de2758950014795fbc93189bb7447cb8d09c9201054eed806c96a3c6ae8
      0710ba222e764c265b868de68767d3a6bac48ae3b636141302b4470a7c0c45ee
      b269918b71f658be7c24cb6a8337e5b6bcb0cb043ab9b5748504d4e0226c9a1c
      6fb0535722f6b2f0ac2d48fce72db20a1f6dc4c56d7e420ee00c0a72f196c558
skRm: e953f3b1205b17889bd75b1607bc832b27aeca56174c552d7b36923d79856dfb
      3048c15eb74877603af4a6ae4aac8f69f46202a0ca6d992f328354ee435424a1
      a3c3a20202ea8a225596046711771b96ad8389c16594dde913aa724147703393
      58c014595dae90a513e20df30548cd59303233a40f4271821602517a9e0b5008
      c7bbbaa6cc92a388a72571039a5141fa84a8ad7428d6b05e64bb37159909bd46
      54fc52b514767f8213915b8609d7375140b29e5ec03e772c1c45762b80d821cb
      f784415b12a7e7bf7a3b28fb554d405a117b0145ff216f9df200b4c834257684
      38c5c88bdb3059844b70b999a95838c7b10c300a8ccb2c48ba6aa998c73a0e04
      0dbee9342afb293c7a5f9fe17c83e18038c3a1c7a59e344645c0b2cc522540bf
      33737754aa12f48facc28034c5645be1390350984f242091a6b68fc689e9eb00
      f59423c8468952b6c0d7505d6c4263cab3a85455b1c5290e0dd446c65a9bbba6
      9e770163ad74c88e9398b9609d694b2b9df819a7054831c9043c303e0851ce58
      964c35ec337bd147f7902ca35b5107397e86372c2cfbbca6f09dbab899b33032
      0405a7ed47140f9ac701e91a19e30e3456bb3df04c4cf0634708482b856c6db1
      661fc3ae98b05634a407be06813c7008a572a558bc7e7af0a4bce885c0fa03c9
      0a5a57259fddd8ad277107b437905c712113db920829b359b871b40c939e293a
      095a9ed127b4045bc31f79cfc8b069b0aa786bb5ba9db22f4ed79135c83eefc0
      cd1cc4382f31bb70e087ab9657c904a340bb5f1e361eea9734cf406fb48a65ec
      1a047a705614a22b0dca3876dac6918924b2956817d462d647a98487bcbc1049
      8e0627a0a4cc53a2828b2794142a7a0826828cc29459fa6675756b10c7583d9c
      9e32bac10c30adb6815d864968c3415e6b017d4c6000f29c9f3ec28decfcb941
      d059200872202724eb2ab09dc844515598c854a8bb4cce04051ce27997b5f9c6
      327c301ee80bfad98a3e23088a6ccda1420443804c5cc763eef60e328ca1b8da
      281cd14f531509867c52f1f253d08b230f9c32d8800545dc8f5db428979aac7f
      286a47da07d8e290ed73adc00b677b950ea9c71ec3621e71eb967125b9771100
      c52965af2cb6541c39fee02cc381491554525806b043b756a918869bd5711b09
      6755a05f76262243fa14633c8aa61bb32788cc9a039f1d73049ce95dfa5a41f3
```

```
23177eaa562082083c03b59f669746bcbb1346053786bb68b0bbd5d7612de9ba
0d1c7d74752398c9a05bd562f6982847d396f96c8c00f34142b45676ec633a42
b57f5959e38b8633c594245359a11a376e395565e884fd8bb40b61bdda6c8d34
15c34e8598b3b8299274226058a3bb10872e9861071b4fbbb54dd5201469c6b8
a88839cce49740370d021c7ed5d597686b630fe30e86e838a27b55b0246a1808
88f7c3c59278802ae22e2c8869ff033c20117608d17079ca880dd338b65836c0
94a3e7069848b4651d845aaaf68e5fec6ce102375e306e62d4ad5dcbc9f8c2ae
72727715ec2d0b25caeb67166af7a21d855b5025a3f8cc76c715320c0c64dca2
493fd6008c661cf3ab5d264711555251bc690fa5c54af2a5c2540c1608d05d75
d329c27c8fa54bba47890ba4702b1eb16020a041f5e5773d2a63aa6ca87c96ca
a29361a4f647e0a85536718f4757bfb636a37eb9cfd41c246eab6d4c655154d1
c1dba98831a7391163b30cd74a567104e7349d20ba34c0062faf53c3d5e46fd2
6245c3c50ed320027b799728da45ae1495fe164e3945348a33bcbde000d7087f
021c15130a3139245d8fbacb6d276ad3c4cb92d5a6b3590e99088e95721a6c63
5da32761ed7c7dc2f58e5839ce986141fb7183e485cd269c785d093711a287b1
612e588581fc9aca571207766a1bd4815b03587207f86918c29f0597aa2a4acf
21005a174a595b252116a3a10f7ccb197388a344545ef8c040a7c681b38f3f8a
4a245749d83838fc70499135b77ab5c4c6361be1856e5f1858bb2c0855991bb1
d17cb515b68e2226492ba31d9545ccf6258b2478d6c27183128f1b9400e3e53f
b7327ce41c9fb79b6507c10b2141be88e9c01be9021a2281b049a9e47452d143
02e2ac9d715839517849c9192027969acd3c6b528098196acb2d55ab4f394a3b
e274380a3b73a43f09e4a6d9688ba07cbfde68ac8fc26b821a8597cc0d90bc94
96b4bb52469b4be1a9d76c6347f9a8fd05bd62aa0b041a646415a659cba164ea
32bc611ef9f40e8d1749c0fbce1d717f96c3bfe93b5403699877c240787c3c2e
405bdb1318dbf078a741b9d08423e9539f66892f68791bcb112bac1551c7a46a
3ff8735d9417204a9308672e3a5a2ae2696e7052abb8c5b4e80ca69bb247b2c9
83c3e04ee2595e565aa38a5ab7d1497d234593637c6efbb5c9db792691dc97cf
d17041550f5ed8349d9b466dc4471c61b3d0eb05a8c0945d9865946992df6212
ad85764a755dd3241a9efa74110360d10102b9050ac0d1063e8552dd042e541a
8f6816cd67167b131c5756a337dec7628d8470b5d02055475cfc7c9c75d851c7
f12334e37e1cf087952339a2c0043cdab7d667879da30922f111b8e60fbf5185
1ba40830ab92777c897f47c6fa1b629a1b49ee7a02af26a52327800226269848
561d3b396bc7694b35cbac7bc490f15e2456168d9245dcbba2ba0a6189559039
b889f9722862f65dc41a57b007316b069deb09d0da6b61aee192c3943c3d7816
e8909731a98adbbc7a0f569479db07850c19bab248be19caee92bca90b156a18
14ad1143cc56513f6858e3ea52ad852546392c5b5167f9f608fae4b986a6c5a5
e6b54c06c8c272aa87eb248fc1b198cb71ee721fd3f1bf26e368398c74ee4b81
571b79e5360ae88c02f1e371f8548661fc45b9d9911cbca88a2cb912656d7005
2d92227706e968648b032757556359968336bee0dcab61e5c431225ac0659ad9
5a91f0290091b0615347453ad83212757b56c251cf8331037623b9625a47a6a6
3859795a2310c3b37920b4713b677764e06e093b2606b22af59a82b95b472914
af8e0c6617c16f62f1b150430c62da18e6c02486f94819287b01449a69b97590
e49d40a728b9834bef9337a0c29464232d1e6a3d0c9274321a952a22aaad239e
598c7de2758950014795fbc93189bb7447cb8d09c9201054eed806c96a3c6ae8
0710ba222e764c265b868de68767d3a6bac48ae3b636141302b4470a7c0c45ee
b269918b71f658be7c24cb6a8337e5b6bcb0cb043ab9b5748504d4e0226c9a1c
6fb0535722f6b2f0ac2d48fce72db20a1f6dc4c56d7e420ee00c0a72f196c558
1722759680f492171d91acce1cab1b56cf03d2eb47986dad1195cdea0f8a64ff
```

```
      a09ed066ae9e0589abfca7bc8ebfaf1de8c014b02630836e40fb65389bebba53
enc: da06a430bdc5526cef78cae5a8e80ec42ad57fdb13bf4b8425f8fa11fb8b3d06
     a590413a5790746792027983e277eda3cfcd1c0b0029efae9898504f86233a6b
     ced4c1620e8ba28856b35f83a5d01d3a83760e40bb83bbd5eef9babc1d8672d3
     d326ec189bf396effe56407e46c2af480713b3b5b783a927accfaeda95d7d02a
     23d1b3c652e33eef6935d9a4aafaa63fcc6629ec09ad44a0d19fef3afda37a32
     5633c1e898d2be59cf950470b4f2a299b3c8cf345a7e3c0d65c948e2e06bd649
     191ac6819e3567a122bffa017762f9db581ffcfda83a1c42dd66f7f2bb6c61bb
     d98f6f656de10ca53a8846b88fc3f144d63f733dc15e8365b748d23a58dbcfc7
     79b84928e0817aa7a542f77505f0387bed6ffb7444bc2ffbf0687d0a161323e4
     88e643e4599e9c12209c41ae80e5f46e829b1a1b91cda58de429fbef3c5800f2
     841bd563792a56f4921936a2568b2a63c54967b3e0e3f2f7077a8e2fb88d3277
     a4dac8f7ddc809e9bd1ae67ac5a04332c82447d6a5a6f197d57ea06fa739fe68
     970c469f373b507511c26c116f08365d16dd1fb5659ee2194127614ff6b3b85a
     1baa45d525049aadb7606fe1af99a684bc4361907a0b947e5bb7028a4f4544f1
     d6030efd07b972f57d23af15953eaa242b1e62812a0aaf7c168f3cbbe4768d72
     05dd2d397eb3b79272abe0b2d55aee408fc161c82229e9a8bf5160c19cbaa999
     0909be38a6cd7d373fa0e1fb4b48a0c2e95470493955977cadcab25a67b96590
     c3cd218c52b6e72b6dc7a541f7c01467c2c8fdddb3bf104829222844825fcd14
     25543deb202d5d1a6783fc38e437fc012c09d0da78e0608dcd2d38702ba070ba
     da1a3028259a7f10ba912d9b0c68b2d3083eaed6d202475d86abbfe416ae7868
     26c12ed454a4e152f9234baeaa1c43245a9584be11a06640797954dfb37d7a3a
     6684efc4ad02f267004f308b3ae0af118fe4a73c460eb0e796515f1492c86afc
     6f3cf760fb7fa00def6e767cc53187b5a23b89fcdb70327c21c7dd36d0202cb6
     9259e89393ee4c3953fd482f9ffbaba0b706bd652f85a564ce387282d500a0d9
     96d5c43c33308f9913be376e0097132cc944e64dc21073bea86af0b17e10891f
     d258b85a91493418c530746b451f1709420580ade8c23cd5882c57f9eea4a83b
     304ef2a7caa15719786ded78a83ea7937a47e46521bc3ed131dde7a5e426f930
     e56a77141d0b234d5d99b136e7473a2d3d23d728c82a26a94fdca7e1dc3d3ddd
     e74a91e8efd1347848f9a8ba5a530d3148d5e4738085e23ac3c88c1e95e8ac51
     797d3071ef3a42e7d834e4c470358f1a312ebcfe0aad44d7ef26ccc0bac1bc35
     addb9a85cb58f04416175fe98f87e4f38cbcd99102bce312dd93114b8285618b
     38439a1c236155e49938a9a9e8cb937f282b99715457ff4c1d73f5502f74b992
     05a7a9bce8deb29eda60fa90e91b1e3f82abb7868802bc9b6c9280f941583962
     0fc5126893894625a2fb3f4782e4ca3985a02a019f86411086afcad0a733731b
     d14a4c058903925e84f53be782c4ff0d4ffd30ee7c6033a8ee888ae84e4cff8c
shared_secret: 4df3cc9cba7bf5d7dafcc223768d14db875e02501aea8b8e6ad3d50aa59ff696
key: e19766ff8ef162c573ca582f33112f81
base_nonce: 7ce026ebc977d1c4650f060f
exporter_secret: 689735dca0af69034517c6c944501c387f4e86ae344b7a6a600c7566e742b53c
```

A.4.1.1. Encryptions

```
sequence number: 0
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236353631373537343739
aad: 436f756e742d30
nonce: 7ce026ebc977d1c4650f060f
ct: 6301266decd458adf8f166cb67d38b82d9b9b7d741fc974e0b2269c0dd2bd406
    beb41c0ddec7e7a08cdc13753e6de943507b31f1bbe1b4722ece5cfe055f3348
    a052b932a959f680035c

sequence number: 1
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236353631373537343739
aad: 436f756e742d31
nonce: 7ce026ebc977d1c4650f060e
ct: 339e6308fca6817a5aa1d1f5705cda2ccfd8b2c898c7109f9f6e34ff74affbde
    ec21839c40643a0d8a7cd51da3fa33cbe0e013dfcee57968e988cecfef4fd258
    e07c1d7a15d885997bf2

sequence number: 2
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236353631373537343739
aad: 436f756e742d32
nonce: 7ce026ebc977d1c4650f060d
ct: 83b1120096787f9b5089c1b96659fd7b7d36bb9bf19ebe7c0bf2539e9531a068
    a5edc90444963f1ed1cf574830b2f4e260ee81c560acf8674fdc785f6186c88f
    e51bc8ba54b5f4756925

sequence number: 3
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236353631373537343739
aad: 436f756e742d33
nonce: 7ce026ebc977d1c4650f060c
ct: 39992fa028d5d1cce420f795b1a5271c04042f1cd619e65fa8e10de36938b1d0
    4b138c18b8317725dd8818a311a6ba7db93a8f10ef0f29a714b69de90ef3812a
    1471f3c4e0b76827a759

sequence number: 4
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236353631373537343739
aad: 436f756e742d34
nonce: 7ce026ebc977d1c4650f060b
ct: 22c192c5efd4a391d1e0386221f098a9b8a4b4edb01de28ff10be4677c1a3845
    85500cc1bfe1e83ab59ddc9ae2b48ab7c8a2ca865cdb70ebf520332bde1ccb5e
    3d9aac0c9569a2ea9863

sequence number: 5
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734363832633230373437323735373436383263323037343732373537343
6383230363236353631373537343739
aad: 436f756e742d35
nonce: 7ce026ebc977d1c4650f060a
ct: 772a31b59bfe072f9b671aeef3cd3a12937171eabf57703b592be5c28adfffb8
    9a11bcef6bf9346b82934130ff157f9a7c1d61f47c569a6d1bba5c3a215d3231
    76e66a0cb59637a71404
```

```
sequence number: 6
pt: 34323635363137353734373932303639373332303734373237353734363832633230373437323735373436383263323037343732373537343
63832303632363536313735373437393
aad: 436f756e742d36
nonce: 7ce026ebc977d1c4650f0609
ct: 7fe1b71b921a4b265b708c1a16066e4243e7db21618903ac85b4adb19881aab0
    54cbe74c723f568a8e485f943c8e23d8a480fd64bf357a7e16c7813b892b6435
    70a156d5afede9841b5b

sequence number: 7
pt: 34323635363137353734373932303639373332303734373237353734363832633230373437323735373436383263323037343732373537343
63832303632363536313735373437393
aad: 436f756e742d37
nonce: 7ce026ebc977d1c4650f0608
ct: 3a3671d3f8852dec4052d7fa26540d57cb0e3d059deb6b3c6788783c7a42c537
    bd766c30dd34e5d34f8315bd5476e44e6d3b7873b073b27cc04695946f3e63ff
    3976b6aa16e969081521

sequence number: 8
pt: 34323635363137353734373932303639373332303734373237353734363832633230373437323735373436383263323037343732373537343
63832303632363536313735373437393
aad: 436f756e742d38
nonce: 7ce026ebc977d1c4650f0607
ct: b9b2836dad8447612a48ffed2adf37582f17925661572c060e22116c680a74d9
    a4bab0b93bf9baa4a4046f3fdddc953c4dd56dc06aae8a5da7882acd920e72c7
    8089744496a10872c9df

sequence number: 9
pt: 34323635363137353734373932303639373332303734373237353734363832633230373437323735373436383263323037343732373537343
63832303632363536313735373437393
aad: 436f756e742d39
nonce: 7ce026ebc977d1c4650f0606
ct: 63064cb8990b0b72338257ac50ce7a869889895e0c640ae2fc3655ead59bd435
    06dc4d5885f95a2573a5dbb21faf5d04921452fa0e5e19d06f8915a2e870700a
    e697dac206409ae150f6
```

A.4.1.2. Exported Values

exporter_context: 70736575646f72616e646f6d30
L: 32
exported_value: 7e7675b50eaed4142b679607ec84142d1facd33d1d4364dbeb5d44411b0be192

exporter_context: 70736575646f72616e646f6d31
L: 32
exported_value: 78bca296eeceee4f1fd600de5d8cabf93972053925d095478684dfa7f2a76fa5

exporter_context: 70736575646f72616e646f6d32
L: 32
exported_value: beebbcebd435cd2837369a31d07be6081b8dd3e019ee8714dd902c689da541d9

exporter_context: 70736575646f72616e646f6d33
L: 32
exported_value: bb49f37624cf32682c121d3a35b0b30c872c067cf96a3fc2aa64203aeb20e76b

exporter_context: 70736575646f72616e646f6d34
L: 32
exported_value: e9d13086fd2be42b180021393ec7e3951b681bd42afe242b526daf48470df804

A.5. QSF-P384-MLKEM1024, SHAKE256, AES-256-GCM

A.5.1. Base Setup Information

mode: 0
kem_id: 82
kdf_id: 16
aead_id: 2
info: 3466363436353230366636653230363132303437373236353633363936313665323035353732366 5
ikmR: ed3e36faec7b773bb52b1b94ad580717f97bdcc8a1e289923785e6f02fa12819
7421bf2bb4d7f1272518adca10e5b604c8f0c912c9165a92c64172dd2d1f270c
d070204baa9a5d00
pkRm: 021f080b77047f72c37496bd101050741d8d2455552a0fef97f722822833c486
2527c15b37f73c972143092c0b49c1be5e9c98b3a03128db261b5c56cdda9bcb
db514203a3b69f2a93c36b6a20fc3ec2b523a9f2c10396036cf1267654c2f8d8
86ce487e9a47b9bbd630bb2590262544ebf49ebfc09555489af8e2a1328b7885
0211dea77f22cacbd6b2384d762c00b426f1097b2d1c98785631f1c0c9fa01c8
acf192d0f59c4ceb140da311771a1031b63069cb40015067e2fb462364c15380
1ce378c207c8c2cb104b99e1c4f1348003372dc1987830cb4be4d303f8204732
b52d1f10c1f3bbb20e15264f857b946ba1b3d1aed9770c40488613a79387d993
400825f33b1b3de9965995ac769bcec434599ff242ad3c313b3b207dd471118c
260dc321c0186ed0a81712a79069826ad66370b2229508384c4b7659afe8895b
ebb4cb754295c634984011def75faac6654f620a641acb53276653bba14a4625
8d227839948cc89463f5315a904365ef84023bb74ca552323c14bf79163309cc
75754c0b6ee3aa754a174b108e49242a8ae89f5f4b744792512b4753ea082403
db1a0331a720ab7d16b7742c209a59701743b4402876268167449837818b401
21d54ba9ba1a4ba24d765391a003c2ab2636e7c9a962105e064a4a5a3b8ef4c3
b136d14a3c3655c2a104efc5931da0bdcf446c3aa5b716a37d5f950c44232bfc

```
      c5b79ec444c6d92ef228aad3a29e4ddb4f55b6c5caf453a9169a351540a39b26
      0038a0c67a76edd37264a5332b8b00a5720441a7bbcd22cc0a1c9b482c495e02
      6479fb1b6a16459c9a70c0e5b2bd43c297c735aa434bca850bfa2a8209cc5657
      86261cdcbb31d1235ab886718c99c84526f10709ab28acaf442a4a264fb96525
      19e75541f130868b875712c191e51aca87401fa056bd3857e532c7bff4349f22
      2b5fa4290320a1640079cbf61e4f90bd9dac205e4ab0ad3cb0ebd3470a551f56
      bb1a74444d10716af14aa0fbd71b91fc085aa0088ada58b036b6a33a90cbb1bc
      8c97cc81852f74baab7cfc1c52787d70bb737a1b1cd845b17d81807b4bc9e44c
      0f69b57aebcc8926f855b94241ad7165443c29e0f07f6fcb0aeebb6d722a8279
      9c1c4c78a547199abbf0b5204018e84183d75c0b2c9aa2b20070aba9321fe268
      3947ae8eb9534a732211a5007a7c24d84b2950bb6a0538cd0b8b000127223702
      958424a79e612e82221311607b48e453d44acdac855dbc833ffe41269d4430ea
      a2cfe8338ca6603a6702812da64abdfb7febfc3a92943c19dbb08ed36fe0ba77
      40c91fba27565d2412d821c069068b9240106b01486e97b702702f6a77c14d49
      cc1b82a78a45ab8d77233d663a555c5ad478c4edfa7159b0c33c6aa85d3abff4
      d37323469c60e3b5c96655e31693a0db3c2a6a966f950eda8299303935125ba2
      e4a8bb020196161aa741f5a84971275b4604cba7c20e756e04b1252d470c0eb6
      9bc6a46e0b1178f13c075a357476b2899b9c15b7178dc8375db3037cf9356aad
      d9cd54055bd53aba01ab6f7154a82e099b908290b0c81f7711b79c361c70f714
      53c8c20b1005ef98aa9118b6fbd7926176036c80023231bf6248c6cb4250c2f8
      3ac58b17443b05f815c86cea8e81aa12d8045c12f48acd31179dd860e1409cf0
      68ac8f039442a7b939ba288fc65138a24f2bc5b186a7555d9b2e82d2b04e290f
      77c462e1708aebcbb9776ab4fc5068491419630aaeeab30392a818f912043012
      a60776c15ea2c5f881319f14ba14d724e8b92a868b055065af3df00804f0cc2a
      c192f412ba5d1620ab198b5cab783e897bbdd27005d9ab95a083d7cba8679935
      3ee8a00aca6fbef51ab41b62fde22ddc6b3436c05fce57cff807368a3a9c3c5b
      21246a3bbc7c0700877e86d0274ed675f25cb35529acffe08a8563b35b81994f
      4ccb1bdc4b1ca5ca66972399b03b99cac54757662155721ef300b9631db8267e
      ab792a8aa35851c0154142b785d1cd0c05093aec1e4565b66a48405a6b334770
      8da9e73f8e835ad7745dc3f504969b3f76d6095bb97c5eac8c42118644fa4d2f
      c2915c5bc2681a944fc58d4c50378d62b495dc59e3b714041bb9e4a44945860c
      a1dbb99f764b3ce6445d6343146754808b4556b907159061fac92e74a36d1e8c
      2706867b7f1c8c7cbc320a58c59a59baa085aeb4d80caff808be782a6fba241b
      e874c36196f1f5ca85984e1e5942d990685e42effdb68d6cd9e100ac296ce322
      f27ea59a57a843aa633638ac5cdc282cef
skRm: a43930303ac1db313103e6cc9de247fb3bf5b1d5a3138bb9ce15fc2123b61255
      cb26fdca12ffaa6fff9626c320dc16b4636117c1d21cacf411103a49ed4a7e62
      6c3bbabc3889a69efad9b406db803c6898076533e7eb883c36aeecc619f81459
      0355737d134df61bccd665b478725fbc7323700ba0a17b8f54e813835c819598
      8f378b2811ec2e125ac8da24cb16515d0c85c6d83ab28f7998427aa53c6c477f
      c4bb01112e782a9c183191042c4995cc8a7cd64ec17c5c1685be06432e3a387a
      7d946983306cb087cba3299014a9409bfbb824a341fc97c1e19aaf9a99248b64
      661d2370482c9aad56728c423f0e1559f78a39ca753c162cac75c4afea117b75
      d00a673385aacb3ef9444ca1a804e1f5ae645b5c93834197259f267628d23384
      70d46f5ed4444ce15d8dc97d1ba29913c0b8bc3353beca4f39d3515593b93986
      1ea8378a3c659889a5919dd2c96830974c73a38461a5cb48badc38a4a062cbe5
      b64990b43502ba2e6e1aa5ecca5a69338055032255f2c0499cafb4b03840f8b7
      09c8778073a20316aab43076e4e5b1594404dbe0bf5ac25f7882b422e48324f8
```

```
096ff228269b94f068bbd5cbb476da72cfe71471073e30356c0cd1ae316c8d17
89ae6b3b04a48bbc8691cd31ca21400cb8c6a420aadb8df15a4810f132fd905e
b798a55bb05e54258483db6eff4b6519fc315e503d6f4a1415713eed311b440c
7012bc4868710a6a897d47e57021d02b8d032f9b0c96c6d2483d850632d56566
8abc6b1890823630c75c35a85446e0979429e8bebf02b1140735024a241db371
294314aa610d853621a8ab6a08252f55d35a2dc996092acc6116a5ec77b2f133
c3e345a6bd912dac9602eba772a733719d1628dff18e02dc29d294cd5158b573
49a594405c2ca213b51ba17ad2bddfb681ba7710389a5b41408932c35e3dbb26
fbb5564200adc2587c2471c5dd6348d1c571f6e13bc129a8b70786c336bbeda8
7e0aa01467d686573c75a2512feb4b433f377a75d1811d637137fb53cea58898
c57e82d752ade16aa2626bd7c7691f740f45745c730056538264376b0dda6017
bed47ec7603697537a2c7ab213672a200a3881d03d4f3c923ed3a235458c17fa
bff6e3893379a74ab27e7c20c87f7a857743c0f12bb16361abc9e18e637092a2
252af312438faba61c60cae479b571156cbd612462f5cf1749b2c21312f34a6b
e30a599c1aa88cf76e9ed6a19bc17aaddb1edf87b15c05c163f591be8182cbc1
73280ccf655c93a6863504ba7d2b2c7378667f37d8a1be9a9a19772a14e88b45
1a65128985993a43bfe7be41516649c28408a6ce3ed23bed8c6747a09d2c3374
901b937e5b7f6476c3045c49af5397de54a4d15083ecc191546b54d9ac80d2d9
c850d93eda4590e7677d837620274378c4c0646402999e568382d632a3e63de6
c601c3c42fde4681f2c1299afa9438f453d25c42dbdca2b6b83be6051065984b
c6726ffb9bb2e966457055721491879b80878de7c866a9afc8032023401029ec
272afa0656039cd229b06b233256d56f11bb0b06d53f533bb0a2323f5c2a6117
57a6fcc38f49e75220a22f0f9375f0da2474416ef3693c45c1b4d07814ecb70c
966b9b71db3b29ac5b8c277923e0c57a4395890475ad43ceae932cfceabfad43
578cd952b34bb8b4250bfe49be7527b02fc0269c578a9039c508a5b7a9dc6db4
6543c8f17eca399cb538b9a424af09a22c7595acbec66803524019d051ae92a3
8ac396b19a703f1822b46c35d945c5a4f36cc9d6b731fa03fe3851134b3be872
77bdb034f867b07f8c60943218a2246c14e667e658a26c34448f9063105323db
b59d0397102872ca957abbe462c4834a596d659863f48ba4373ce0682a7e948f
bc6b2e34935e49f18528932b1d122da5ea863d989cdb1a596f748d67ca7eb529
3f5d0472434c468d5a47639b6459c89e4156bf8358afd3810eb1809dffc1b9b6
d6a4d08744f72bc4ef9538e52b45de0289b970a1c714cfa4b04ea623af183b20
d3624654c25292e600fe990634bb819cb23f95210acbe4b7259179e907d03f33
b9b8e71fe47b0f0ebaa9cb686da40c7cc2a40896c688a4a6c734d212f26697ea
bcb91caab0f6c35664436d45d57ab258186dca6ea4f16161668ed0a3046dc787
8980387a62671ef47de22aa31799b5ca68254fe01b16883ccce6b28fc513ba02
3a8da0476723157f80b8f2a9c6ec2c7f9c98b3a03128db261b5c56cdda9bcbdb
514203a3b69f2a93c36b6a20fc3ec2b523a9f2c10396036cf1267654c2f8d886
ce487e9a47b9bbd630bb2590262544ebf49ebfc09555489af8e2a1328b788502
11dea77f22cacbd6b2384d762c00b426f1097b2d1c98785631f1c0c9fa01c8ac
f192d0f59c4ceb140da311771a1031b63069cb40015067e2fb462364c153801c
e378c207c8c2cb104b99e1c4f1348003372dc1987830cb4be4d303f8204732b5
2d1f10c1f3bbb20e15264f857b946ba1b3d1aed9770c40488613a79387d99340
0825f33b1b3de9965995ac769bcec434599ff242ad3c313b3b207dd471118c26
0dc321c0186ed0a81712a79069826ad66370b2229508384c4b7659afe8895beb
b4cb754295c634984011def75faac6654f620a641acb53276653bba14a46258d
227839948cc89463f5315a904365ef84023bb74ca552323c14bf79163309cc75
754c0b6ee3aa754a174b108e49242a8ae89f5f4b744792512b4753ea082403db
```

```
      1a0331a720ab7d16b7742c209a59701743b4402876268167449837818 1b40121
      d54ba9ba1a4ba24d765391a003c2ab2636e7c9a962105e064a4a5a3b8ef4c3b1
      36d14a3c3655c2a104efc5931da0bdcf446c3aa5b716a37d5f950c44232bfcc5
      b79ec444c6d92ef228aad3a29e4ddb4f55b6c5caf453a9169a351540a39b2600
      38a0c67a76edd37264a5332b8b00a5720441a7bbcd22cc0a1c9b482c495e0264
      79fb1b6a16459c9a70c0e5b2bd43c297c735aa434bca850bfa2a8209cc565786
      261cdcbb31d1235ab886718c99c84526f10709ab28acaf442a4a264fb9652519
      e75541f130868b875712c191e51aca87401fa056bd3857e532c7bff4349f222b
      5fa4290320a1640079cbf61e4f90bd9dac205e4ab0ad3cb0ebd3470a551f56bb
      1a74444d10716af14aa0fbd71b91fc085aa0088ada58b036b6a33a90cbb1bc8c
      97cc81852f74baab7cfc1c52787d70bb737a1b1cd845b17d81807b4bc9e44c0f
      69b57aebcc8926f855b94241ad7165443c29e0f07f6fcb0aeebb6d722a82799c
      1c4c78a547199abbf0b5204018e84183d75c0b2c9aa2b20070aba9321fe26839
      47ae8eb9534a732211a5007a7c24d84b2950bb6a0538cd0b8b00012722370295
      8424a79e612e82221311607b48e453d44acdac855dbc833ffe41269d4430eaa2
      cfe8338ca6603a6702812da64abdfb7febfc3a92943c19dbb08ed36fe0ba7740
      c91fba27565d2412d821c069068b9240106b01486e97b702702f6a77c14d49cc
      1b82a78a45ab8d77233d663a555c5ad478c4edfa7159b0c33c6aa85d3abff4d3
      7323469c60e3b5c96655e31693a0db3c2a6a966f950eda8299303935125ba2e4
      a8bb020196161aa741f5a84971275b4604cba7c20e756e04b1252d470c0eb69b
      c6a46e0b1178f13c075a357476b2899b9c15b7178dc8375db3037cf9356aadd9
      cd54055bd53aba01ab6f7154a82e099b908290b0c81f7711b79c361c70f71453
      c8c20b1005ef98aa9118b6fbd7926176036c80023231bf6248c6cb4250c2f83a
      c58b17443b05f815c86cea8e81aa12d8045c12f48acd31179dd860e1409cf068
      ac8f039442a7b939ba288fc65138a24f2bc5b186a7555d9b2e82d2b04e290f77
      c462e1708aebcbb9776ab4fc5068491419630aaeeab30392a818f912043012a6
      0776c15ea2c5f881319f14ba14d724e8b92a868b055065af3df00804f0cc2ac1
      92f412ba5d1620ab198b5cab783e897bbdd27005d9ab95a083d7cba86799353e
      e8a00aca6fbef51ab41b62fde22ddc6b3436c05fce57cff807368a3a9c3c5b21
      246a3bbc7c0700877e86d0274ed675f25cb35529acffe08a8563b35b81994f4c
      cb1bdc4b1ca5ca66972399b03b99cac54757662155721ef300b9631db8267eab
      792a8aa35851c0154142b785d1cd0c05093aec1e4565b66a48405a6b3347708d
      a9e73f8e835ad7745dc3f504969b3f76d6095bb97c5eac8c42118644fa4d2fc2
      915c5bc2681a944fc58d4c50378d62b495dc59e3b714041bb9e4a44945860ca1
      dbb99f764b3ce6445d6343146754808b4556b907159061fac92e74a36d1e8c27
      06867b7f1c8c7cbc320a58c59a59baa085aeb4d80caff808be782a6fba241be8
      74c36196f1f5ca85984e1e5942d990685e42effdb68d6cd9e100ac296ce322f2
      7ea59a57a843aa633638ac5cdc282cef30a8575a15977e0a807ba6830d6e5967
      e53c02267c778ea540cf2ad13cad608c368f0c57c77eeabd8f979bb8424bec25
      d6268bd222dfa24538bc7313209c15a6
enc: 02f83d55376a5f005d56f1532ec8a1e2942a75a64b258d94ee54ab236a185352
     eecdfb3935667dd48fec4b9e6b7fc9d9324d92f42b83ae191e75f4d243b7caca
     cdde0a84d4b1bb47f6447214e03c907ac4f59f1917fb332aac94ec82f627f280
     982a6d73db299e7215257388779a17100d530c74fc5d4ae291238757c49e4678
     f99d263f713d2537cb43cedb89c573a245e152fed045baa55343a3e1590a2829
     ed5b42c5b238c584ed57af07eb4b513b3205714dd70970abb28f440f562286e9
     23e66c19f096bf968d9beef678168a1cbb2e52b5cbac6b9e8a72b5d109df5a93
     c5fe8ffa741d3f7035c64163528f8455aa977fda78fa3340efce01ea948f7675
```

```
      82153884848c4c5be5cd4664c9ce250c667b49e6bb8336c8aad4edbd21c1577c
      85afd7e5f0582ee883819c07219bfb5d34d8e5643e8b0a505aca6009288ced94
      01f15765ef099e96d66771d002f160f890316131e804be9fb34cf730e28a1a42
      f79a4522114d7bd7a7765e475c03cfdb660860ff23db8f990a203ab4caa58a06
      bf4c18a5a492b140f47b4f33cfdd99e65a497deabe2ad5f4c06f54ec2bb52c9b
      ef6552a37add9d5e1455f7222eff7c2fcb61b5a29a54fe388c1f00b13229a11d
      cb6b2423a9fdff7576a7afdb8ddff35e9c231ba0227c99c81cf599ab23e37d7d
      713b4b74f4ec30e790a23f3ad58123d29ad77484ed0e8da734e51c1d87bda010
      2cb4e6edd416cc66cd0b90699115e31db39b244b9f954b8655de06a9adf0b485
      3773b67a94116a2161880589bc745d0c2b8057936502d4f936aa9819786de214
      e125216e593cf75ca5641c6075848bde1414ebb103d86bbeb76682a07a2958ab
      99ebe6110fe2562c64bf81443b4babc874a54ebcbe83523c03d816f5f0d7e159
      3432179aa3adf4ce056f6c4ca6cdcc99661bcb6459599b59315c479a2474d3bc
      ff17a7904763383f16e8f07236c4c703a878b9184bfeeb37528173be18e28f79
      a7050e4bf7690d5472ac679e44ae34f20d1bcf1d468e9c1187d2e7190a2d6e7e
      4edfdefb14f35992a8c6986debfb9f00d208a5bea6c1b3b2573321d960a41154
      6316fc5df13ffae0cf214abb19e1f774eb3888d13f8be919f96652640812fcfa
      1c9357847ccde925cf583f255eddd3f4030a7fcdcbc9dbc38a52196c32f183ec
      8bec10f6852e1acec443fcb8a6b4606f51bc8d67bea702712e9d79a917b522a6
      923e1b5a0207691482446290b418ffeb39ec811e82144f28188bc95be90cf6ea
      3f475aee6bfe0ac1d8f23595032bea0ad3e854fec5f87515873ff9534d3d63fe
      28884f3e1ec77113315ab832b605e04fbc2c08c67b51dc19c9e470edf995bc13
      2883167d32b1d80646e83a52596aab2867660b24fb676477372fb3be783460ac
      0e9c679cbdc2585e450374a2149e4f6f2a0e16778e248672b12138a5e8bae21f
      751244517f096ed46370f4792bad4729461087726eb66de827f166278ab356e6
      ff88fb3f18001a7b8ae26c8cc1b6c93631853aeee57b595c4e3cae6119b05e53
      453d1e702da3607d495a4f08e08a55e4b2a49e6195723ce7a6b03702ac1406ab
      cf55cd9f24641feea6ff39077afedcf292306e44a78ec0e9d23b41b2a3cbd3a3
      922a58883ed751d3b456ded8c7f3783b5b148c7d19c2b08406b801edd3dac7d2
      a2af089d4e43271d9e5ee4b2508cdb81f79c296a329db6c0f045d1ed696ad48b
      103ebbf785daabe239b1f84ba812ef53bb6cda1125d3c68f41fdba345cb82823
      05ff5ebea3591886d7d9a0ae1af6ac5ed31abea38446f354934a42f69437d5cd
      d3dcdca348369625e923a78161016462dbc242100eac2fdfe0b45ce4c8649930
      6db07b7f13a26359495c2081cad2c9cd7c28a23da1414616a442a657c63d91d4
      0bc5c6eba106788d7f398ab16545f470b5c08200517646183334f9445e212504
      b0a684b19ca5cb1d6172e6b4c10ebc2e220ad820db9a437d56ea16c8773c45cd
      16983924a0b6a335b8cb72094504f424823bc9123bed718b053de67f97451205
      05724ad0ff6929ad7b57fb00c054d631b44e0014b51c7cc8e8f978ec8e10148a
      2d8660d81e3fde150752d38478c18e6f951142b5cff4c8d2df3d21a2d6e01bbe
      c62a54b1807ae7aae2def15c00a2369e8fb94c33c47c687238849cbf991abb94
      61a6536aa0371279b0fb4b62f5153f94d0b92a650867e15ac655d0dc9f10d5d6
      124c78b73c73eac18d138e9d4246b576ab97d6c0165646cd8553f310cdaab2c5
      1282a30f0b2a5f3dd58dc918e40b105d37
shared_secret: 250dbc9910b47b6f51097fd484d3996dc8335706c006a0fce77729a51280e4c2
key: 45d95d7e3239dc99b4d8cf3b5bb1b89ed74327cc531690fb4ab03066d87a66c1
base_nonce: c7e928d294ac6b06f9f1d34a
exporter_secret: aaadc292e6288db742f9f9e2435e1095324ef7d9029d5c77814328ddd813eed2
```

A.5.1.1. Encryptions

```
sequence number: 0
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6383230363236353631373537343739
aad: 436f756e742d30
nonce: c7e928d294ac6b06f9f1d34a
ct: db5a0fa80eb3481c985374e459afba1ebf2b4358964a3d5bee3833c6250c7fd1
    a73fdc53d0faa3847524a780c2a068d3d618860c38c6547a0134972cd8abbf4d
    f3949b0aed6f8d574262

sequence number: 1
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6383230363236353631373537343739
aad: 436f756e742d31
nonce: c7e928d294ac6b06f9f1d34b
ct: 34cca436f7f47a76c1cbf0b3cd03adb8cb887b6bb4c16d29e808d303a34e3d3b
    78d460f5abf08047f30fd35dd80e46629044a6dfbf163bbf7735d8f6452675f4
    9b7bc245dc39c8cba716

sequence number: 2
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6383230363236353631373537343739
aad: 436f756e742d32
nonce: c7e928d294ac6b06f9f1d348
ct: 1dc4fd3afec1f209714efafc03d6a88527175edea67cfe94b1fa2385e682e764
    ad509a4aad20b2e689edfb6cea6730bec696d8e46500c5aa3dc5c828649e9f57
    edad5807d8efa2c94b88

sequence number: 3
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6383230363236353631373537343739
aad: 436f756e742d33
nonce: c7e928d294ac6b06f9f1d349
ct: f982d7ed749ac1ba7537c3f923137c093f6efa555692a7fbdcb16d66b04d7bc9
    2418ab6862ee6bce1241ec6ef9ddcdafeb6371613cb4304677c9ae128c65119b
    d7e9017cb34cd1e9eb9a

sequence number: 4
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6383230363236353631373537343739
aad: 436f756e742d34
nonce: c7e928d294ac6b06f9f1d34e
ct: b04bce274458f3238b1513be482eea759115dba024cdf7f2a861b5acf8359063
    d1e174c4be2d3fbb54847e6707be8be81480bd1cfd12a6d2905d21de69641c19
    47dfdacfadd7c0794a65

sequence number: 5
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6383230363236353631373537343739
aad: 436f756e742d35
nonce: c7e928d294ac6b06f9f1d34f
ct: a7e7b1e5bd78d5502e0c2ca661b5b698dc482868aaefb465243e427eb4fcd34e
    3775b5909b6d7560d2667ba05afaf4b487110c4a2c8f6913e8ced7863198c0da
```

```
    34316486524828d9758e

sequence number: 6
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6383230363236353631373537343739
aad: 436f756e742d36
nonce: c7e928d294ac6b06f9f1d34c
ct: e0b93d92dcec5e8fc56e146d8c5e4ac64c1a500bd82c65a2180134db3eef9370
    fde03978a6b57dafc43df50ea21b20930a05e9a09968303b20566e8f03d1dacd
    bdc29b590ddeabee8dcd

sequence number: 7
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6383230363236353631373537343739
aad: 436f756e742d37
nonce: c7e928d294ac6b06f9f1d34d
ct: 3e248172063b36398a92a21c17d7011e1e93314fe4a0e9c917f5faa007938c64
    1ad8fb10831e457ec51b541e5306a042b416c37720c3fc9325beb1409f5a6915
    d4bdb096d571173ed793

sequence number: 8
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6383230363236353631373537343739
aad: 436f756e742d38
nonce: c7e928d294ac6b06f9f1d342
ct: bb4b9bdc224960bb607da9e2791c553281b65b113136e09173a64f66afc7468c
    84268b40759a2bac7e6e5a00fd0c01ecd0c1fafc68e4e61b22e5499262baa324
    ec9eb4544369a4b4e586

sequence number: 9
pt: 343236353631373537343739323036393733323037343732373537343638326332303734373237353734
6383230363236353631373537343739
aad: 436f756e742d39
nonce: c7e928d294ac6b06f9f1d343
ct: b679662c42dc37742f3dbee87141059a5f28b24e86b41194586fffac2578b871
    c933d7911c570d0a268fc45ddce76f30c447e696b2d4645987d62ba60de8a5d0
    1ee9be155851b712a11c
```

A.5.1.2. Exported Values

```
exporter_context: 70736575646f72616e646f6d30
L: 32
exported_value: 95ccd83cfd9722eb5d9229d3a1e66c0b6910f30adb6bf1a5550692bd5ad480ec

exporter_context: 70736575646f72616e646f6d31
L: 32
exported_value: a64c081fdac68d7d75a705489019e16c819f9129f217207b9ea440651cc66ade

exporter_context: 70736575646f72616e646f6d32
L: 32
exported_value: 08718f5518054efcdba4f5c1009fe37bf541fc9b7fb204d922fc4a4af79c5a4e

exporter_context: 70736575646f72616e646f6d33
L: 32
exported_value: 064e50fcc7bf7b4559577afc0885d832cdc08b70daba1ab189b53b9a92621705

exporter_context: 70736575646f72616e646f6d34
L: 32
exported_value: 6a715f5b91d2c06baf30b6050511de5c22d981dc27f3d3ff8605b9cde70276e4
```

Author’s Address

Richard Barnes
Cisco
Email: rlb@ipv.sx