CBOR Object Signing and Encryption
Internet-Draft
Intended status: Standards Track
Expires: 14 November 2026

T. Reddy
Nokia
H. Tschofenig
UniBw M.
F. Skokan
Okta

13 May 2026

COSE HPKE PQ & PQ/T Algorithm Registrations
draft-reddy-cose-hpke-pq-pqt-03

Abstract

This document registers Post-Quantum (PQ) and Post-Quantum/Traditional (PQ/T) hybrid algorithm identifiers for use with CBOR Object Signing and Encryption (COSE), building on the Hybrid Public Key Encryption (HPKE) framework.

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://tireddy2.github.io/cose-hpke-pqt-pqc/draft-reddy-cose-hpke-pq-pqt.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-reddy-cose-hpke-pq-pqt/.

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

Source for this draft and an issue tracker can be found at https://github.com/tireddy2/cose-hpke-pqt-pqc.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Copyright Notice

Table of Contents

1. Introduction

[I-D.ietf-cose-hpke] defines how to use Hybrid Public Key Encryption (HPKE) with COSE_Encrypt0 and COSE_Encrypt structures ([RFC9052]) using traditional Key Encapsulation Mechanisms (KEM) based on Elliptic-curve Diffie-Hellman (ECDH).

This document extends the set of registered HPKE algorithms to include Post-Quantum (PQ) and Post-Quantum/Traditional (PQ/T) hybrid KEMs, as defined in [I-D.ietf-hpke-pq]. These algorithms provide protection against attacks by cryptographically relevant quantum computers.

The term "PQ/T hybrid" is used here consistent with [I-D.ietf-hpke-pq] to denote a combination of post-quantum and traditional algorithms, and should not be confused with HPKE's use of "hybrid" to describe the combination of asymmetric and symmetric encryption.

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.

This document uses the terms "Traditional Algorithm", "Post-Quantum Algorithm", "PQ/T Hybrid Scheme", and "PQ/T Hybrid KEM" as defined in [RFC9794]. The term "pure post-quantum" is used in this document to refer to a single-algorithm scheme using only a post-quantum algorithm, with no traditional component.

3. Algorithm Identifiers

This section defines the algorithm identifiers for PQ and PQ/T HPKE-based encryption in COSE. Each algorithm is defined by a combination of an HPKE KEM, a Key Derivation Function (KDF), and an Authenticated Encryption with Associated Data (AEAD) algorithm.

All algorithms defined in this section follow the same operational model as those in [I-D.ietf-cose-hpke], supporting both integrated encryption as defined in Section 3.2 of [I-D.ietf-cose-hpke] and key encryption as defined in Section 3.3 of [I-D.ietf-cose-hpke].

Test vectors for all algorithms defined in this section are provided in Appendix A.

3.1. PQ/T Hybrid Integrated Encryption Algorithms

The following table lists the algorithm identifiers for PQ/T hybrid integrated encryption, where HPKE directly encrypts the plaintext without a separate Content Encryption Key:

Name	Value	HPKE KEM	HPKE KDF	HPKE AEAD
HPKE-8	TBD (Assumed: 54)	MLKEM768-P256 (0x0050)	SHAKE256 (0x0011)	AES-256-GCM (0x0002)
HPKE-9	TBD (Assumed: 56)	MLKEM768-X25519 (0x647a)	SHAKE256 (0x0011)	AES-256-GCM (0x0002)
HPKE-10	TBD (Assumed: 58)	MLKEM1024-P384 (0x0051)	SHAKE256 (0x0011)	AES-256-GCM (0x0002)

Table 1: PQ/T Hybrid Integrated Encryption Algorithms

These algorithms combine ML-KEM with a traditional elliptic curve algorithm in a PQ/T hybrid KEM, with the goal that compromise of either the post-quantum or the traditional component alone does not undermine the security of the resulting encryption.

3.2. Pure PQ Integrated Encryption Algorithms

The following table lists the algorithm identifiers for pure post-quantum integrated encryption:

Name	Value	HPKE KEM	HPKE KDF	HPKE AEAD
HPKE-11	TBD (Assumed: 60)	ML-KEM-512 (0x0040)	SHAKE256 (0x0011)	AES-128-GCM (0x0001)
HPKE-12	TBD (Assumed: 62)	ML-KEM-768 (0x0041)	SHAKE256 (0x0011)	AES-256-GCM (0x0002)
HPKE-13	TBD (Assumed: 64)	ML-KEM-1024 (0x0042)	SHAKE256 (0x0011)	AES-256-GCM (0x0002)

Table 2: Pure PQ Integrated Encryption Algorithms

These algorithms provide pure post-quantum security using ML-KEM without a traditional algorithm component.

3.3. PQ/T Hybrid Key Encryption Algorithms

The following table lists the algorithm identifiers for PQ/T hybrid key encryption, where HPKE encrypts the Content Encryption Key:

Name	Value	HPKE KEM	HPKE KDF	HPKE AEAD
HPKE-8-KE	TBD (Assumed: 55)	MLKEM768-P256 (0x0050)	SHAKE256 (0x0011)	AES-256-GCM (0x0002)
HPKE-9-KE	TBD (Assumed: 57)	MLKEM768-X25519 (0x647a)	SHAKE256 (0x0011)	AES-256-GCM (0x0002)
HPKE-10-KE	TBD (Assumed: 59)	MLKEM1024-P384 (0x0051)	SHAKE256 (0x0011)	AES-256-GCM (0x0002)

Table 3: PQ/T Hybrid Key Encryption Algorithms

These are the key encryption counterparts of the PQ/T hybrid integrated encryption algorithms defined in Table 1.

3.4. Pure PQ Key Encryption Algorithms

The following table lists the algorithm identifiers for pure post-quantum key encryption:

Name	Value	HPKE KEM	HPKE KDF	HPKE AEAD
HPKE-11-KE	TBD (Assumed: 61)	ML-KEM-512 (0x0040)	SHAKE256 (0x0011)	AES-128-GCM (0x0001)
HPKE-12-KE	TBD (Assumed: 63)	ML-KEM-768 (0x0041)	SHAKE256 (0x0011)	AES-256-GCM (0x0002)
HPKE-13-KE	TBD (Assumed: 65)	ML-KEM-1024 (0x0042)	SHAKE256 (0x0011)	AES-256-GCM (0x0002)

Table 4: Pure PQ Key Encryption Algorithms

These are the key encryption counterparts of the pure PQ integrated encryption algorithms defined in Table 2.

4. COSE_Key Representation

Keys for the algorithms defined in this document use the "AKP" (Algorithm Key Pair) COSE key type defined in Section 3 of [I-D.ietf-cose-dilithium]. The required "alg" (label 3) parameter identifies the HPKE ciphersuite as well as whether the key is used for Integrated Encryption or Key Encryption.

The public key parameter (label -1) contains the SerializePublicKey() output for the corresponding KEM, and for private keys the private key parameter (label -2) contains the SerializePrivateKey() output, both as defined in Section 4 of [I-D.ietf-hpke-hpke]. Both values are encoded as CBOR byte strings.

Examples of COSE_Keys for each algorithm are provided in Appendix A.

5. Security Considerations

The security considerations of [I-D.ietf-cose-hpke] and [I-D.ietf-hpke-pq] apply to this document. [I-D.ietf-pquip-pqc-engineers] provides general background on the threat posed by cryptographically relevant quantum computers (CRQCs), the properties of KEMs, and considerations for PQ/T hybrid schemes.

This document registers ciphersuites based on ML-KEM-512. As noted in Section 3 of [I-D.ietf-hpke-pq], given the relative novelty of ML-KEM, there is 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 such cryptanalysis at a modest performance penalty, and is RECOMMENDED where the additional overhead is acceptable.

Unlike the companion JOSE algorithm registration document, this document retains ML-KEM-512-based ciphersuites for COSE. Discussion of this work identified COSE-specific deployment interest in these ciphersuites, including constrained environments and deployments that already support ML-KEM-512 in adjacent protocols and implementations. The ML-KEM-512 ciphersuites are therefore registered here to preserve that deployment option, while the stronger ML-KEM-768- and ML-KEM-1024-based ciphersuites remain the preferred choice when their additional overhead is acceptable.

The PQ/T hybrid ciphersuites registered by this document are motivated by the PQ/T Hybrid Confidentiality property (Section 5 of [RFC9794], Section 13.1 of [I-D.ietf-pquip-pqc-engineers]): confidentiality is preserved as long as at least one of the component algorithms remains secure. The traditional component protects against unforeseen cryptanalysis of ML-KEM, while the post-quantum component protects against Harvest Now, Decrypt Later (HNDL) attacks (Section 7 of [I-D.ietf-pquip-pqc-engineers]) by a future CRQC. PQ/T hybrid ciphersuites are generally preferred for this reason during the transition to post-quantum cryptography.

The pure PQ ciphersuites are registered to accommodate deployments with regulatory or compliance mandates that require the exclusive use of post-quantum algorithms, such as those governed by the Commercial National Security Algorithm Suite 2.0 [CNSA2.0], as well as deployments where the size or performance overhead of a traditional component is undesirable.

When the Key Encryption algorithms defined in Table 3 or Table 4 are used in a COSE_Encrypt structure with multiple COSE_Recipient entries, all recipients MUST use a quantum-resistant Key Management algorithm. Including a recipient that uses an algorithm that is not quantum-resistant would allow an adversary performing an HNDL attack to recover the Content Encryption Key once a CRQC becomes available; see Section 15.4 of [I-D.ietf-pquip-pqc-engineers].

5.1. Security Strength

Ciphersuites based on ML-KEM-512 target NIST post-quantum security level 1; those based on ML-KEM-768 target security level 3; and those based on ML-KEM-1024 target security level 5 (see Section 11 of [I-D.ietf-pquip-pqc-engineers]). In the PQ/T hybrid ciphersuites, the traditional component provides an additional classical security floor: P-256 and X25519 offer approximately 128-bit classical security, while P-384 offers approximately 192-bit classical security. The -KE variants share the same cryptographic properties as their integrated encryption counterparts.

All ciphersuites use SHAKE256 as the KDF, aligning with the hash family used internally by ML-KEM. The AEAD is paired with the KEM security level: ML-KEM-512 ciphersuites use AES-128-GCM, while ML-KEM-768, ML-KEM-1024, and the PQ/T hybrid ciphersuites use AES-256-GCM. As discussed in Section 3.1 of [I-D.ietf-pquip-pqc-engineers], symmetric primitives are only modestly affected by quantum attacks and doubling key sizes is not strictly required; AES-256-GCM is nonetheless selected for the higher-strength ciphersuites to provide a comfortable margin consistent with security level 3 and 5 parameter sets and with contemporary guidance such as [CNSA2.0]. AES-128-GCM is used with ML-KEM-512 since pairing a level-1 KEM with a level-5 AEAD would not improve the overall security level while increasing implementation and bandwidth cost. The widespread hardware acceleration and broad deployment of AES-GCM make it a reasonable choice for all ciphersuites defined in this document.

6. IANA Considerations

6.1. COSE Algorithms Registry

This document requests registration of the following values in the IANA "COSE Algorithms" registry established by [RFC9053]:

Note: The HPKE algorithm numbering is intentionally aligned with the companion JOSE document so that a given HPKE identifier denotes the same HPKE KEM, KDF, and AEAD combination across JOSE and COSE.

6.1.1. HPKE-8

* Name: HPKE-8
* Value: TBD (Assumed: 54)
* Description: Integrated Encryption with HPKE using MLKEM768-P256 KEM, SHAKE256 KDF, and AES-256-GCM AEAD

* Capabilities: [kty]
* Change Controller: IETF
* Reference: Table 1 of this document
* Recommended: Yes

6.1.2. HPKE-8-KE

* Name: HPKE-8-KE
* Value: TBD (Assumed: 55)
* Description: Key Encryption with HPKE using MLKEM768-P256 KEM, SHAKE256 KDF, and AES-256-GCM AEAD
* Capabilities: [kty]
* Change Controller: IETF
* Reference: Table 3 of this document
* Recommended: Yes

6.1.3. HPKE-9

* Name: HPKE-9
* Value: TBD (Assumed: 56)
* Description: Integrated Encryption with HPKE using MLKEM768-X25519 KEM, SHAKE256 KDF, and AES-256-GCM AEAD
* Capabilities: [kty]
* Change Controller: IETF
* Reference: Table 1 of this document
* Recommended: Yes

6.1.4. HPKE-9-KE

* Name: HPKE-9-KE
* Value: TBD (Assumed: 57)

* Description: Key Encryption with HPKE using MLKEM768-X25519 KEM, SHAKE256 KDF, and AES-256-GCM AEAD

* Capabilities: [kty]

* Change Controller: IETF

* Reference: Table 3 of this document

* Recommended: Yes

6.1.5. HPKE-10

* Name: HPKE-10

* Value: TBD (Assumed: 58)

* Description: Integrated Encryption with HPKE using MLKEM1024-P384 KEM, SHAKE256 KDF, and AES-256-GCM AEAD

* Capabilities: [kty]

* Change Controller: IETF

* Reference: Table 1 of this document

* Recommended: Yes

6.1.6. HPKE-10-KE

* Name: HPKE-10-KE

* Value: TBD (Assumed: 59)

* Description: Key Encryption with HPKE using MLKEM1024-P384 KEM, SHAKE256 KDF, and AES-256-GCM AEAD

* Capabilities: [kty]

* Change Controller: IETF

* Reference: Table 3 of this document

* Recommended: Yes

6.1.7. HPKE-11

* Name: HPKE-11
* Value: TBD (Assumed: 60)
* Description: Integrated Encryption with HPKE using ML-KEM-512 KEM, SHAKE256 KDF, and AES-128-GCM AEAD
* Capabilities: [kty]
* Change Controller: IETF
* Reference: Table 2 of this document
* Recommended: Yes

6.1.8. HPKE-11-KE

* Name: HPKE-11-KE
* Value: TBD (Assumed: 61)
* Description: Key Encryption with HPKE using ML-KEM-512 KEM, SHAKE256 KDF, and AES-128-GCM AEAD
* Capabilities: [kty]
* Change Controller: IETF
* Reference: Table 4 of this document
* Recommended: Yes

6.1.9. HPKE-12

* Name: HPKE-12
* Value: TBD (Assumed: 62)
* Description: Integrated Encryption with HPKE using ML-KEM-768 KEM, SHAKE256 KDF, and AES-256-GCM AEAD
* Capabilities: [kty]
* Change Controller: IETF
* Reference: Table 2 of this document

* Recommended: Yes

6.1.10. HPKE-12-KE

* Name: HPKE-12-KE
* Value: TBD (Assumed: 63)
* Description: Key Encryption with HPKE using ML-KEM-768 KEM, SHAKE256 KDF, and AES-256-GCM AEAD
* Capabilities: [kty]
* Change Controller: IETF
* Reference: Table 4 of this document
* Recommended: Yes

6.1.11. HPKE-13

* Name: HPKE-13
* Value: TBD (Assumed: 64)
* Description: Integrated Encryption with HPKE using ML-KEM-1024 KEM, SHAKE256 KDF, and AES-256-GCM AEAD
* Capabilities: [kty]
* Change Controller: IETF
* Reference: Table 2 of this document
* Recommended: Yes

6.1.12. HPKE-13-KE

* Name: HPKE-13-KE
* Value: TBD (Assumed: 65)
* Description: Key Encryption with HPKE using ML-KEM-1024 KEM, SHAKE256 KDF, and AES-256-GCM AEAD
* Capabilities: [kty]
* Change Controller: IETF

* Reference: Table 4 of this document

* Recommended: Yes

7. References

7.1. Normative References

[I-D.ietf-cose-dilithium]
Prorock, M. and O. Steele, "ML-DSA for JOSE and COSE", Work in Progress, Internet-Draft, draft-ietf-cose-dilithium-11, 15 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-cose-dilithium-11>.

[I-D.ietf-cose-hpke]
Tschofenig, H., Jones, M. B., Steele, O., Daisuke, A., and L. Lundblade, "Use of Hybrid Public-Key Encryption (HPKE) with CBOR Object Signing and Encryption (COSE)", Work in Progress, Internet-Draft, draft-ietf-cose-hpke-25, 7 April 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-cose-hpke-25>.

[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-03, 2 March 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-hpke-hpke-03>.

[I-D.ietf-hpke-pq]
Barnes, R. and D. Connolly, "Post-Quantum and Post-Quantum/Traditional Hybrid Algorithms for HPKE", Work in Progress, Internet-Draft, draft-ietf-hpke-pq-04, 2 March 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-hpke-pq-04>.

[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>.

[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>.

7.2. Informative References

[CNSA2.0] National Security Agency, "Announcing the Commercial National Security Algorithm Suite 2.0", May 2025, <https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.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-14, 25 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-engineers-14>.

[RFC8792] Watsen, K., Auerswald, E., Farrel, A., and Q. Wu, "Handling Long Lines in Content of Internet-Drafts and RFCs", RFC 8792, DOI 10.17487/RFC8792, June 2020, <https://www.rfc-editor.org/rfc/rfc8792>.

[RFC9052] Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, DOI 10.17487/RFC9052, August 2022, <https://www.rfc-editor.org/rfc/rfc9052>.

[RFC9053] Schaad, J., "CBOR Object Signing and Encryption (COSE): Initial Algorithms", RFC 9053, DOI 10.17487/RFC9053, August 2022, <https://www.rfc-editor.org/rfc/rfc9053>.

[RFC9794] Driscoll, F., Parsons, M., and B. Hale, "Terminology for Post-Quantum Traditional Hybrid Schemes", RFC 9794, DOI 10.17487/RFC9794, June 2025, <https://www.rfc-editor.org/rfc/rfc9794>.

Appendix A. Test Vectors

This appendix provides test vectors for each algorithm defined in this document. For each algorithm, a private COSE_Key and an example encrypted COSE message (COSE_Encrypt0 for integrated encryption suites, or COSE_Encrypt with a single COSE_Recipient for key encryption suites) are provided, each shown in CBOR diagnostic notation and as hex-encoded CBOR. Long lines in the examples are folded using the single backslash strategy from [RFC8792]. Before using a folded example as a test vector, remove the RFC 8792 header and unfold the lines according to that strategy. The complete unfolded vector set is available as examples/cose-vectors.json in the repository (https://github.com/tireddy2/cose-hpke-pqt-pqc) for this document.

A.1. HPKE-8

NOTE: '\' line wrapping per RFC 8792

```
{
  / kty / 1: 7,
  / kid / 2: h'c3a85366a9abe1a96e7267131e8b8b11c5a4014b21809b28219c3\
    df4818bf5dd',
  / alg / 3: 54 / HPKE-8 /,
  / pub / -1: h'e9746721ab42d4ab48ec36658fc2120f166fb6c15e04e3ca4044\
    cc45161be39751d24c3a4c349bf143171c75a150175b101a1fe60bc825a7191b\
    87b11a4bb826ccac41c73d01547a61d8a1ee468f3508028a22b0f50002342316\
    c76a75ef54550a91921683b069e8cd19978d24a4b88eaba53961501c6b5b5a19\
    7ae0767396464cc61a9d03e11e70438b8730a46c230cb57c5bf9cc545643b142\
    92a43b9a1f98468a1fbb63c8d67256cc6a8146459fa2bc8ceabd83a1823841b8\
    6b0181e80642ef6c8d5cb0c19d50b2ffb38c9f66c07a8b3c02f84791bb0bd21b\
    05163b2759c1bf218bcd3f3500732199969b2a8d7248878014c538ba88578914\
    e134f2734cdca404625c64300ba555ab36138294fd319ea0425e6630394cf595\
    01088f1454389cd461d64a2d7f8387b47415a5a333032a48b485c053c2c8fe09\
    78add14a4df62ed7c30a9f28231273bd67b7b6718c23fe1ab1f8041d03aba540\
    170d4780c54823932e7301db618c5c654e3030a689ac59bdc869f6210a3491b8\
    4e46509a82b047da5b11b6a19ac9b55af51b47a904a8d60e13430cb1158d3374\
    41365b66d08aa8f1128c96946ae5171e59145d8d190a74287286e27679b048d3\
    9891b2e13a0305846c257a750a8d67482a75e5398a61028c558b36a62fb3405a\
    c43826a12760e2b165ab752b67780b0f85134f890cf7b1cee6279dc68a31fffa\
    1cb531042263137fcb892363349ca4c8a5b5811e5a1f4dfba572a5578c5629af\
    d1afb8a33f98495aa09c27dcc418ac534b73063e7f3cbd7eabc616d17eeb67c7\
    72970bed2554bbd296ee282200741fc179829cc433b31c0ba30564f261630d88\
    15da22283487aec1975cf3e23403508b8aa39037008b39b8123157a8f9652fce\
    6a1cb05394b52512d5c84d370a6330218ab87c4e60e72f28bc47ee6bcfa7a733\
    228bcfb2a41465d9680395aab7c535b034597eb8519548b8215a1399ebc1a5a1\
    182bf2737b770830e91129d3b9635b41e1321c00713ca0d51aad4118c7560352\
    29c8a25441043c8102647badb5788867a7187c20793219d1ca69a451036e4017\
    e00686e182867465ab816861883a0f5f699d6bf04b3928a59e5866336061a866\
    4190a2b61350797e0111fbf00c61e565f471282821479ba280a609cb56760c42\
    312fee40bab6cab1b3ea4e7274acd84a4628c324e2074895c14dc6c554eac5c8\
    347003bcd9ad3724208d114a86634fb587215c75b3fed81c7163649b50c3eaa3\
    004cea1972c700bbc041a4a5305089085080b02a96b2e4a52c1632a90bd1cfa9\
    238d54c56eec6632b150bc5034cc7ad5a85e54a20deb688a89701461a922c71f\
    d6273fad485b0f7a72c5523c0ea0ac74583635c4af2094682413b5d8a1ca4486\
    2773c39b802cc90542cd675466739b426e6716fe69a18343a203b1098f08bf7a\
    863cdbf8347a2c80af42b80e6072f32a960d9578e4a7c09d8401419bcaf33963\
    d27a46a955aeb31ccfd66c3f0db867a7e67a4b222b1cd23dba71bb0db78385c9\
    c10f6401a76b7a70d82f52808bccf45e40f632fdbc1513072b3d23b84a3506f2\
    686ec9b894e4d59d808443f79803d40a4d46865e24885f3fbc8cd6fb75642c5f\
    574c44bd449bdb90ce79b8a6ca9944befee7c5a9b685b9e545099ed34079c0fb\
    7da444f13d2404e1951deaeeb453d7ba1770be16a8f07e0ff160c937a0e71943\
    e3f936bb0dc4ade1a3bc66b6948a55a8697ffd8ffe8d95cfc60573bb764bb8c0\
```

```
      c7d6d12d04296c',
    / priv / -2: h'7358a5d4227051d6a37809bc3cc64cab89b0d8f1fd676bd384b\
      907536310d740'
  }
```

Figure 1: HPKE-8 COSE_Key (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
a50107025820c3a85366a9abe1a96e7267131e8b8b11c5a4014b21809b28219c3df4\
818bf5dd031836205904e1e9746721ab42d4ab48ec36658fc2120f166fb6c15e04e3\
ca4044cc45161be39751d24c3a4c349bf143171c75a150175b101a1fe60bc825a719\
1b87b11a4bb826ccac41c73d01547a61d8a1ee468f3508028a22b0f50002342316c7\
6a75ef54550a91921683b069e8cd19978d24a4b88eaba53961501c6b5b5a197ae076\
7396464cc61a9d03e11e70438b8730a46c230cb57c5bf9cc545643b14292a43b9a1f\
98468a1fbb63c8d67256cc6a8146459fa2bc8ceabd83a1823841b86b0181e80642ef\
6c8d5cb0c19d50b2ffb38c9f66c07a8b3c02f84791bb0bd21b05163b2759c1bf218b\
cd3f3500732199969b2a8d7248878014c538ba88578914e134f2734cdca404625c64\
300ba555ab36138294fd319ea0425e6630394cf59501088f1454389cd461d64a2d7f\
8387b47415a5a333032a48b485c053c2c8fe0978add14a4df62ed7c30a9f28231273\
bd67b7b6718c23fe1ab1f8041d03aba540170d4780c54823932e7301db618c5c654e\
3030a689ac59bdc869f6210a3491b84e46509a82b047da5b11b6a19ac9b55af51b47\
a904a8d60e13430cb1158d337441365b66d08aa8f1128c96946ae5171e59145d8d19\
0a74287286e27679b048d39891b2e13a0305846c257a750a8d67482a75e5398a6102\
8c558b36a62fb3405ac43826a12760e2b165ab752b67780b0f85134f890cf7b1cee6\
279dc68a31fffa1cb531042263137fcb892363349ca4c8a5b5811e5a1f4dfba572a5\
578c5629afd1afb8a33f98495aa09c27dcc418ac534b73063e7f3cbd7eabc616d17e\
eb67c772970bed2554bbd296ee282200741fc179829cc433b31c0ba30564f261630d\
8815da22283487aec1975cf3e23403508b8aa39037008b39b8123157a8f9652fce6a\
1cb05394b52512d5c84d370a6330218ab87c4e60e72f28bc47ee6bcfa7a733228bcf\
b2a41465d9680395aab7c535b034597eb8519548b8215a1399ebc1a5a1182bf2737b\
770830e91129d3b9635b41e1321c00713ca0d51aad4118c756035229c8a25441043c\
8102647badb5788867a7187c20793219d1ca69a451036e4017e00686e182867465ab\
816861883a0f5f699d6bf04b3928a59e5866336061a8664190a2b61350797e0111fb\
f00c61e565f471282821479ba280a609cb56760c42312fee40bab6cab1b3ea4e7274\
acd84a4628c324e2074895c14dc6c554eac5c8347003bcd9ad3724208d114a86634f\
b587215c75b3fed81c7163649b50c3eaa3004cea1972c700bbc041a4a53050890850\
80b02a96b2e4a52c1632a90bd1cfa9238d54c56eec6632b150bc5034cc7ad5a85e54\
a20deb688a89701461a922c71fd6273fad485b0f7a72c5523c0ea0ac74583635c4af\
2094682413b5d8a1ca44862773c39b802cc90542cd675466739b426e6716fe69a183\
43a203b1098f08bf7a863cdbf8347a2c80af42b80e6072f32a960d9578e4a7c09d84\
01419bcaf33963d27a46a955aeb31ccfd66c3f0db867a7e67a4b222b1cd23dba71bb\
0db78385c9c10f6401a76b7a70d82f52808bccf45e40f632fdbc1513072b3d23b84a\
3506f2686ec9b894e4d59d808443f79803d40a4d46865e24885f3fbc8cd6fb75642c\
5f574c44bd449bdb90ce79b8a6ca9944befee7c5a9b685b9e545099ed34079c0fb7d\
a444f13d2404e1951deaeeb453d7ba1770be16a8f07e0ff160c937a0e71943e3f936\
bb0dc4ade1a3bc66b6948a55a8697ffd8ffe8d95cfc60573bb764bb8c0c7d6d12d04\
296c2158207358a5d4227051d6a37809bc3cc64cab89b0d8f1fd676bd384b9075363\
10d740
```

Figure 2: HPKE-8 COSE_Key (Hex-Encoded CBOR)

NOTE: '\' line wrapping per RFC 8792

```
/ COSE_Encrypt0 / 16([
  / protected / h'a1011836',
  / unprotected / {
    / kid / 4: h'c3a85366a9abe1a96e7267131e8b8b11c5a4014b21809b28219\
    c3df4818bf5dd',
    / ek / -4: h'ee2bfd015fc29cab76d7024754154e789bb7b17ab53d4c25514\
    b44d5dd2a1215b5e5d5b605cea67cdfa55c038461478cddfa3a7e0b5d3252941\
    5363a37fa81c734da29fe657c8a33b2ced5f7d773a30c9a5d8feec7b9d57f1b0\
    8c541db82014c5f57e917868f7d72817fc9add137a9e06c2570ebc92e3ecb017\
    288e335a5d7445b2e37ba9355c40d355210c25c463873d11f65f0eabc11b8def\
    f6aceb3ccc4b0cd76980cb4903d2783e6728582102e88f2503d2fb94eaab2b9c\
    9577d57c029b623e5605125adf6764254a3fb9d32efd08bf4686f78a68a29f0a\
    c9b5ef55d562b6e9413ba6a8f88265a8f8e70aef5cf55743c226b3d4ca0f00d7\
    0e8bd40d92af6fbb5eed0303f2a7a3d2328e13664929a05cc8e1922950b59fed\
    47273834271b8a9bb40be86f9b8c108d184b06f9d085ecc2201f82c4ee8e6ee1\
    bc7711c53fcda8ea0c722f072ca2755ff981555be2f115d6c3cd5ddd94d2f74f\
    cfe7db1f7818f3abdef0efa8eb2e906258b9e5718be3ea91d27d976c979ae387\
    65bf7957219ed7c70ac7cebda19cd7ca4e6b0cd4dae631fb5a34283463441456\
    695e5bc705fe3cac8ed36b24c4e131b30c06505a941a01788fcd7ee60af2be6f\
    3ca7e497d5bd2fd82e873d3d47fdba7c95b5b2caf23c53ef74a08b096137ebcb\
    a2acb9063be623c5c46c9094eb95144375d34f3ffc514c241e022006f5c089ed\
    e2f5cc94bfe98542b6a3e5e5c2d7e3af973c040b035ea8edd100678f4c509a82\
    3c68501f2e6accfb5d52fbf1962d4b9c83dfbb94562c5effa6e83344d63e28fb\
    9ade840ed2b7c7e3ddaa22199c8bd2bd352c60ea30fe4494d78fb0055e365f1c\
    703f0b8cd77efebf9ebd7c46e4f9456ba5c1745f53d9415f8a17ee4cc991df07\
    a29bf57c1d5aec0991ffede13a866746a071f62279c4ccc1d8385f9b5bb159cf\
    0d435e80752dfce233f3ad5638c54deae75abcab036a5fcecb7406acab1b9e82\
    613cd508c5b21a72c21173c7d97d76c2a3b7126599287965a512772782c75cee\
    09351e6e821e7f115f8c30d5dfb6bd119e9259cd934d7fc01dc6c5249f093bdd\
    b2e2d086d4bde681faa0d262e637025bf4c6152d39587bd4d1e11fae3cfabf47\
    59b30d7ab84b29d58c7b5ff57f7cff98f21e42592f5dc23b484422c25fa26a37\
    816b2f9faad88dedfb7b75167c1990b6db8bff4af3200438f28e4da5196abe95\
    6e4e86d58ffe6f3e350f424cb91f0070c305c862c659d12a083123a6cc01ad8b\
    c1c2decd2aebb1385733e596ae27601cfea9b85c884fadc06bc42c18b0b8d294\
    7330677dbb556ce7f761076af565e07e85b42ef2e248b77efd4cb8ee7c9366a1\
    88885488ee13eb20cad292d000e5a9cc6ab0e471888ae7817c40b17070a2767e\
    24497c2a2f5ccfafa4c1089447968da5a55cb82bc1218efdf110658f9e1900c1\
    3b8ac6cd9cf857c66e69893a750ffb227f461e1ce33f8fbbe18da70eab47be43\
    2f0067033f0c138ec5344a71b2edf52685f83e38650e46aee2533d14bf040f6e\
    b93cee870ddc4044692891949e447dcbd484a73658296de85b8cbc3c3bfd3e2b\
    e23dabf61d9261a7f2af6d0a518d7a8d94c5d8bf1522e35d4ecdcb2828bced22\
    7eef3c62b683dcd'
  },
  / ciphertext / h'3a8c6eca287e2c95d2b50b8a8cb47533d8fd937f714d3750d\
    a6bdcec965e1c5a87c8a5bbc6d5713a75998f63c19756f3b70f1bab9ec905c6c\
    46654725310cffc9361b0a3edb1f792ee5e900b945cbaed4b91911de4809cd2a\
```

```
      5efeb2600e581b3fd53e25af1bd89dab7ff74cdf5fd8ebad8c3154df2067548b\
      edab590abde33880787d17e70553e253f448844257edf5d8a982671ad045ee20\
      e043f8c11ba554b0b743e06a1f1783d1f646f0d620d0d0e1532f728fd033761d\
      37b80229952995054a75aa13b60dc84c91cf30d8905366099629d2c3998b35af\
      cbef29789d1b5d1372f97b1cba338805e1ab7b9d188553890bad36b57370261a\
      7f3ef5d3cc9a6abf272e7ff73e01a4f460535e8f995f282ef8de34a8666645d9\
      307d7c19b28b57df9'
   ])
```

Figure 3: HPKE-8 COSE_Encrypt0 (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
d08344a1011836a2045820c3a85366a9abe1a96e7267131e8b8b11c5a4014b21809b\
28219c3df4818bf5dd23590481ee2bfd015fc29cab76d7024754154e789bb7b17ab5\
3d4c25514b44d5dd2a1215b5e5d5b605cea67cdfa55c038461478cddfa3a7e0b5d32\
529415363a37fa81c734da29fe657c8a33b2ced5f7d773a30c9a5d8feec7b9d57f1b\
08c541db82014c5f57e917868f7d72817fc9add137a9e06c2570ebc92e3ecb017288\
e335a5d7445b2e37ba9355c40d355210c25c463873d11f65f0eabc11b8deff6aceb3\
ccc4b0cd76980cb4903d2783e6728582102e88f2503d2fb94eaab2b9c9577d57c029\
b623e5605125adf6764254a3fb9d32efd08bf4686f78a68a29f0ac9b5ef55d562b6e\
9413ba6a8f88265a8f8e70aef5cf55743c226b3d4ca0f00d70e8bd40d92af6fbb5ee\
d0303f2a7a3d2328e13664929a05cc8e1922950b59fed47273834271b8a9bb40be86\
f9b8c108d184b06f9d085ecc2201f82c4ee8e6ee1bc7711c53fcda8ea0c722f072ca\
2755ff981555be2f115d6c3cd5ddd94d2f74fcfe7db1f7818f3abdef0efa8eb2e906\
258b9e5718be3ea91d27d976c979ae38765bf7957219ed7c70ac7cebda19cd7ca4e6\
b0cd4dae631fb5a34283463441456695e5bc705fe3cac8ed36b24c4e131b30c06505\
a941a01788fcd7ee60af2be6f3ca7e497d5bd2fd82e873d3d47fdba7c95b5b2caf23\
c53ef74a08b096137ebcba2acb9063be623c5c46c9094eb95144375d34f3ffc514c2\
41e022006f5c089ede2f5cc94bfe98542b6a3e5e5c2d7e3af973c040b035ea8edd10\
0678f4c509a823c68501f2e6accfb5d52fbf1962d4b9c83dfbb94562c5effa6e8334\
4d63e28fb9ade840ed2b7c7e3ddaa22199c8bd2bd352c60ea30fe4494d78fb0055e3\
65f1c703f0b8cd77efebf9ebd7c46e4f9456ba5c1745f53d9415f8a17ee4cc991df0\
7a29bf57c1d5aec0991ffede13a866746a071f62279c4ccc1d8385f9b5bb159cf0d4\
35e80752dfce233f3ad5638c54deae75abcab036a5fcecb7406acab1b9e82613cd50\
8c5b21a72c21173c7d97d76c2a3b7126599287965a512772782c75cee09351e6e821\
e7f115f8c30d5dfb6bd119e9259cd934d7fc01dc6c5249f093bddb2e2d086d4bde68\
1faa0d262e637025bf4c6152d39587bd4d1e11fae3cfabf4759b30d7ab84b29d58c7\
b5ff57f7cff98f21e42592f5dc23b484422c25fa26a37816b2f9faad88dedfb7b751\
67c1990b6db8bff4af3200438f28e4da5196abe956e4e86d58ffe6f3e350f424cb91\
f0070c305c862c659d12a083123a6cc01ad8bc1c2decd2aebb1385733e596ae27601\
cfea9b85c884fadc06bc42c18b0b8d2947330677dbb556ce7f761076af565e07e85b\
42ef2e248b77efd4cb8ee7c9366a188885488ee13eb20cad292d000e5a9cc6ab0e47\
1888ae7817c40b17070a2767e24497c2a2f5ccfafa4c1089447968da5a55cb82bc12\
18efdf110658f9e1900c13b8ac6cd9cf857c66e69893a750ffb227f461e1ce33f8fb\
be18da70eab47be432f0067033f0c138ec5344a71b2edf52685f83e38650e46aee25\
33d14bf040f6eb93cee870ddc4044692891949e447dcbd484a73658296de85b8cbc3\
c3bfd3e2be23dabf61d9261a7f2af6d0a518d7a8d94c5d8bf1522e35d4ecdcb2828b\
ced227eef3c62b683dcd5901213a8c6eca287e2c95d2b50b8a8cb47533d8fd937f71\
4d3750da6bdcec965e1c5a87c8a5bbc6d5713a75998f63c19756f3b70f1bab9ec905\
c6c46654725310cffc9361b0a3edb1f792ee5e900b945cbaed4b91911de4809cd2a5\
efeb2600e581b3fd53e25af1bd89dab7ff74cdf5fd8ebad8c3154df2067548bedab5\
90abde33880787d17e70553e253f448844257edf5d8a982671ad045ee20e043f8c11\
ba554b0b743e06a1f1783d1f646f0d620d0d0e1532f728fd033761d37b8022995299\
5054a75aa13b60dc84c91cf30d8905366099629d2c3998b35afcbef29789d1b5d137\
2f97b1cba338805e1ab7b9d188553890bad36b57370261a7f3ef5d3cc9a6abf272e7\
ff73e01a4f460535e8f995f282ef8de34a8666645d9307d7c19b28b57df9
```

Figure 4: HPKE-8 COSE_Encrypt0 (Hex-Encoded CBOR)

A.2. HPKE-8-KE

NOTE: '\' line wrapping per RFC 8792

```
{
  / kty / 1: 7,
  / kid / 2: h'cb289275c0c25add86b439534a99efaade738327a2232af712189\
    01e2ae2892c',
  / alg / 3: 55 / HPKE-8-KE /,
  / pub / -1: h'a714115eb4492e47bc04c0576b5153ef880cf5fabbd5f13044f4\
    67755b26b1800c53a96512725a78a01a823c64e38ca5f4fb27ed8067ded5575c\
    b56ba88c725a11ac3f6a661f86367a880169130605f432f9333f47374513e84a\
    2c7a873e6a8ffcf6444b6b3a3bdb4192f93b0fa7ca64a8810d22abbd682b2822\
    28d4371c81f1c46b2c42b5ec75c35663570788656b5503757f25d8a3ce86c689\
    2534773ab28d504109055c5a24852cbb97eab16d88fa6c6b74a56afa4a1da453\
    219c7fe687023b52c100aab88f07b0e23c67851ba35f855c68e1363104371549\
    93e9480ca5649fca624d04eab0377b94dc43bf92d80c3f075fad1562852822ae\
    4895ec18525bdb8df793938a088922279dc4f57a6ac2b6edc09c3e137494940e\
    ca795a87c063c9260ac1d3111f2c555611839a7277eaf793103a1ba0186ae620\
    2472ac1e77b3be2b00b4f577157227a0abeb5823635630e90175713f5b6aafbc\
    f224269398b4a033b6951cc610413e2b5119071dcfec03e278a4d83164f36b1f\
    0cda42fe557f5d6611dca5708818b1dad081dedc3e8fd96813701ac4679fb329\
    743cf42c146bb68b9aaeb4195472545484c524886732127c794b4c4d633cae33\
    e9406b75a937394473f4a8aa62afa1b669d298be131627a48409ee73c914d5c9\
    f6283792fa4d0b19ca944c2c3f9c3dd526ce70b381439748abe9a887890af590\
    abcbf264026980c61bbd9060ae82169c08f694aa066b8a03bd6d01c7c348225f\
    6101e6103eafa571cccc1825ca31f52c43d2d255b003210941a11ae4b9c2876b\
    3e16b2facb3bf003198979b70f79837beb00d155512da3771e0999c3e92e77cb\
    2eedb2a1f7361e7388876b2810ab6c921a878e2a819eb152bbedf88b9566982c\
    db6a126cb005b95096465b3885267159ac4f0775c991beacf2246bf789f60004\
    e137b85e0131a286892382c075a89fd6cb46fa511917c4663659af9b8c1d00c6\
    5002a3cf2e23b0915021b213147dabcc79588679d824e7bcb724da60a90b97fa\
    c108e4d98d3055b8ef047701eb02a6ebaafd292a8fc11d79659a23087e2fc883\
    60273b37eb4b84dc2024ea67236a47f82a6055286280a8ba6eb22307840457e2\
    6d47328567f645d3033d1984cdb0133b7579713d45158cb0b258559849c45dc0\
    7ca91ff75ecaf6848e7cbed038293ae479a71056b45184b2801024198f645ba6\
    c1807975993205126b40f50434c370d1e67fd72aa5d681487534024201259fd0\
    457c23c1e8c097f246649cfa2f8499aaef80402cf59a20d799867888e3c1467f\
    cb73f15749d7532eeeac6b362507340a5331c91edc0c36a8a97e36d15e47c3ae\
    e9fa901f47764a157e1af09cbb18ca7d474d535cb9cd8865bba659c2f919dfd8\
    ca97eb7b132c3aac012751f580da11175cc683a8155162fab08623349dba0e0e\
    15942545bc384a41a7d788dde7a5eed44556289943b2ac66650157255f18942f\
    87b0cce75540bd45128bfc4f433b33fbec962770c5998585e9e31093b15d517b\
    bb1e617131fb8d3461ccca9c7c4bd46a7c2888f4e7ce7aac1549a6b630077e6f\
    67200c0a3ca9578219c31553d151c2b52c7157a5b5c248e36b1989aa1714f525\
    c802a77326a367a81984535ec480d68920a9e0be789ccf78f0bf8a7281676701\
    ecb9e023889c04f5d732ea452dc90eafd3f3b159bf0eb8cd38bbde86b4e95df3\
    0548701ed01367ddee0f574c2752860a5d98c80d9c62ab24cd00d916ed9a79fe\
```

```
      81dc466f202b24',
    / priv / -2: h'6e250ae4da89cd7cd6100374176cf392b12bf51a7f417e798ac\
      fe3ed562e1c24'
  }
```

Figure 5: HPKE-8-KE COSE_Key (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
a50107025820cb289275c0c25add86b439534a99efaade738327a2232af71218901e\
2ae2892c031837205904e1a714115eb4492e47bc04c0576b5153ef880cf5fabbd5f1\
3044f467755b26b1800c53a96512725a78a01a823c64e38ca5f4fb27ed8067ded557\
5cb56ba88c725a11ac3f6a661f86367a880169130605f432f9333f47374513e84a2c\
7a873e6a8ffcf6444b6b3a3bdb4192f93b0fa7ca64a8810d22abbd682b282228d437\
1c81f1c46b2c42b5ec75c35663570788656b5503757f25d8a3ce86c6892534773ab2\
8d504109055c5a24852cbb97eab16d88fa6c6b74a56afa4a1da453219c7fe687023b\
52c100aab88f07b0e23c67851ba35f855c68e136310437154993e9480ca5649fca62\
4d04eab0377b94dc43bf92d80c3f075fad1562852822ae4895ec18525bdb8df79393\
8a088922279dc4f57a6ac2b6edc09c3e137494940eca795a87c063c9260ac1d3111f\
2c555611839a7277eaf793103a1ba0186ae6202472ac1e77b3be2b00b4f577157227\
a0abeb5823635630e90175713f5b6aafbcf224269398b4a033b6951cc610413e2b51\
19071dcfec03e278a4d83164f36b1f0cda42fe557f5d6611dca5708818b1dad081de\
dc3e8fd96813701ac4679fb329743cf42c146bb68b9aaeb4195472545484c5248867\
32127c794b4c4d633cae33e9406b75a937394473f4a8aa62afa1b669d298be131627\
a48409ee73c914d5c9f6283792fa4d0b19ca944c2c3f9c3dd526ce70b381439748ab\
e9a887890af590abcbf264026980c61bbd9060ae82169c08f694aa066b8a03bd6d01\
c7c348225f6101e6103eafa571cccc1825ca31f52c43d2d255b003210941a11ae4b9\
c2876b3e16b2facb3bf003198979b70f79837beb00d155512da3771e0999c3e92e77\
cb2eedb2a1f7361e7388876b2810ab6c921a878e2a819eb152bbedf88b9566982cdb\
6a126cb005b95096465b3885267159ac4f0775c991beacf2246bf789f60004e137b8\
5e0131a286892382c075a89fd6cb46fa511917c4663659af9b8c1d00c65002a3cf2e\
23b0915021b213147dabcc79588679d824e7bcb724da60a90b97fac108e4d98d3055\
b8ef047701eb02a6ebaafd292a8fc11d79659a23087e2fc88360273b37eb4b84dc20\
24ea67236a47f82a6055286280a8ba6eb22307840457e26d47328567f645d3033d19\
84cdb0133b7579713d45158cb0b258559849c45dc07ca91ff75ecaf6848e7cbed038\
293ae479a71056b45184b2801024198f645ba6c1807975993205126b40f50434c370\
d1e67fd72aa5d681487534024201259fd0457c23c1e8c097f246649cfa2f8499aaef\
80402cf59a20d799867888e3c1467fcb73f15749d7532eeeac6b362507340a5331c9\
1edc0c36a8a97e36d15e47c3aee9fa901f47764a157e1af09cbb18ca7d474d535cb9\
cd8865bba659c2f919dfd8ca97eb7b132c3aac012751f580da11175cc683a8155162\
fab08623349dba0e0e15942545bc384a41a7d788dde7a5eed44556289943b2ac6665\
0157255f18942f87b0cce75540bd45128bfc4f433b33fbec962770c5998585e9e310\
93b15d517bbb1e617131fb8d3461ccca9c7c4bd46a7c2888f4e7ce7aac1549a6b630\
077e6f67200c0a3ca9578219c31553d151c2b52c7157a5b5c248e36b1989aa1714f5\
25c802a77326a367a81984535ec480d68920a9e0be789ccf78f0bf8a7281676701ec\
b9e023889c04f5d732ea452dc90eafd3f3b159bf0eb8cd38bbde86b4e95df3054870\
1ed01367ddee0f574c2752860a5d98c80d9c62ab24cd00d916ed9a79fe81dc466f20\
2b242158206e250ae4da89cd7cd6100374176cf392b12bf51a7f417e798acfe3ed56\
2e1c24
```

Figure 6: HPKE-8-KE COSE_Key (Hex-Encoded CBOR)

```
   NOTE: '\' line wrapping per RFC 8792

   / COSE_Encrypt / 96([
     / protected / h'a10103',
     / unprotected / {
       / iv / 5: h'd3c087cd66a26bc98bdc0348'
     },
     / ciphertext / h'dbf6e759e253d416e9a0cd054dc13184bffefe2a20750c3e4\
       e42a1380a571e4662a8145601c4f4fb97291394f5982394d2cbc3f67d2ea6326\
       4e96c788c4380d02bd7fdd7a5966f7c22ce65cb3ffc632dc0bad0cf300ee2d6f\
       979ec4dca06abd444706e826ac1986abae784e5bb070cb5a22d43660707a2035\
       afbde9a0d6c8759028fb81c569ed84666bf97b07b56356df22fa4098042ec174\
       fc3d2c93801ef0ca3801983f4dd209077ff70406a633c97a7b2a9f8133c906d2\
       239c64ea74a2180b4de0c32c9b2259cc45f144142919e0e6bc8b13953866a189\
       270fb7c9b2963ab72a9a9735747ed904c0ce0117de98edcf74b989c87d6b2f38\
       44be46756bf6b94c0a34a6418c82e2e76d8ca6a97fde52bfbecd37420dcebea2\
       7b81d81779750ce58',
     / recipients / [
       [
         / protected / h'a2011837045820cb289275c0c25add86b439534a99efaa\
       de738327a2232af71218901e2ae2892c',
         / unprotected / {
           / ek / -4: h'c2e3fbb37cc85019bc7369ea564d7b4bd33ae1a4c0323d8\
       b6416951d25b370c49daa5c4075ddfb0decdd1289e6d239106ebb106e6ae9871\
       9e9dd43549cf54233cf901beacb315702d8a4efde1fc5350e19172a103390e9c\
       5b6c131b5402f9b43efcbe2864a98ed40b534df3cc72803c37e89b9dc9f6ac4e\
       3bc219913f6aa49a10fd587ca737284061daed1dc9ded416799f5d0e9483639d\
       8139dfc05813df276a5fbd3b657d37c2d64774d912982e7854eac3983c284822\
       78fa6f819e3f00cd0f113826f1df92eb7164a1bc9961354cb761a491a27499fb\
       b1a9603d1c07b434c772dcccfa2e6a80b9a452eaff50ff23cada98b065003d74\
       f6f5d0bad46893f9d94d5e308f65b848b4fb726a15099123c9e1b918f0a74e77\
       03bd746c2f8e7f5f3d5a4c475469ea2bf37dff5cb3a0b5596b24eb278b5ef849\
       c4143b3429ea6d463eb5a17267e81830e60f11e4803663d07ce029ffe9448980\
       ef0daacc3159194251279591d316c7fc10bb853aafbfe6b6f75d3569855113d5\
       7aa8ecc911e2023fb49e2b8643e00a30bd6c69588eeb19dffacac80d140df33b\
       f09cf16babf76e8d6d82341fecabe76259296b644ee001e10a6f33d4d6cda0bf\
       db742b1c7d33c702563b3d32dec2807610c0b09c07a9fea3002bd4be5c511f18\
       5afbeea7ee11175b70a345ec48658372fb8e79cccc14c47b541dcdbce012ee3e\
       4b3f0f3a01576e34edd5d6e2f4f8b49a7f3f7e831643e6b8b11ce4a4e9b66bdf\
       b9664b5ca5fac6f0089f51cccb4ca076afa0540d089da1486caa3228245e2d0f\
       cb22cd3b4943a0ea4040b283504dd34b2b85453749613e6659f2c91a7652115c\
       4886e7e2030d08edf85db93ae1befe326da6ed92f4c4ac2ea1ce6d5030cfc909\
       a6e821c8d4514d658555e40dd5efa57b6d1c05e85db6284fdbcb778c4d8e09ee\
       a446aa046174e0877998a830974a51b4aee52c896a9f3ee1b5c3bcac9bf4663c\
       a5d100b2bf96daaef9e411297c65a66f4819c95298e05fad7991ceba212d8437\
       9475012e925856ad8d8933f09178428321507e99f00c0fd85ad8a73b27a4b48a\
       0a9c37752fd6ae03d270d173e43720f26a6e5d004108d8ba5652a5ffb0c0af89\
       5af218481f6a3fb0212c7f530dd39950ff945600e29e917314af5378cd175e26\
```

```
      9d9b49c53963fdb31e1553eed7008e842375fed0cb377e2fc1d1de540a6fcbf1\
      d324c9f1f04bd42084b6c9f5ac30bde6f7e3a334999b7003a388ac1604fa651e\
      77daba71457e00d0c528b036d1947ab5bb4c0ce2a29ee37f62690b96c655285a\
      70604881a10ba8bad19ec171fa73be914d0571dbf1e6f01fc8a8b83499a6f507\
      905f6027bdffdbdee06259de85fe11f68a4c414f6c7348f1ec11f1d9777e4c56\
      2b964964359842773f29f0091e953dadbed437c8d35351bf12ec8f91cdde59bf\
      d10f4bb63153039c8baa683102cb90a29029f691a33c274b4391887a036be6a7\
      7e3c9f894f0573ffa5d8c6de1ab01e4af0b428f4bc371d0d5f7af6d40b108fca\
      27431c7bf2a40dae8049a3aceb56d5773f08016039d6d0370b5a081a1a0f2299\
      8330af2fe1643860546847bee9d67c56747da91b42d60c1a4f1686669e34683f\
      24ffceda910176902f7'
        },
        / ciphertext / h'a520aac9e94fe8d7b006488182d6da449ea6d62714155\
      3f613070a6498b2ca27a87f50e20c8f30d621fd20fa83187c28'
      ]
    ]
  ])
```

Figure 7: HPKE-8-KE COSE_Encrypt (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
d8608443a10103a1054cd3c087cd66a26bc98bdc0348590121dbf6e759e253d416e9\
a0cd054dc13184bffefe2a20750c3e4e42a1380a571e4662a8145601c4f4fb972913\
94f5982394d2cbc3f67d2ea63264e96c788c4380d02bd7fdd7a5966f7c22ce65cb3f\
fc632dc0bad0cf300ee2d6f979ec4dca06abd444706e826ac1986abae784e5bb070c\
b5a22d43660707a2035afbde9a0d6c8759028fb81c569ed84666bf97b07b56356df2\
2fa4098042ec174fc3d2c93801ef0ca3801983f4dd209077ff70406a633c97a7b2a9\
f8133c906d2239c64ea74a2180b4de0c32c9b2259cc45f144142919e0e6bc8b13953\
866a189270fb7c9b2963ab72a9a9735747ed904c0ce0117de98edcf74b989c87d6b2\
f3844be46756bf6b94c0a34a6418c82e2e76d8ca6a97fde52bfbecd37420dcebea27\
b81d81779750ce5881835827a2011837045820cb289275c0c25add86b439534a99ef\
aade738327a2232af71218901e2ae2892ca123590481c2e3fbb37cc85019bc7369ea\
564d7b4bd33ae1a4c0323d8b6416951d25b370c49daa5c4075ddfb0decdd1289e6d2\
39106ebb106e6ae98719e9dd43549cf54233cf901beacb315702d8a4efde1fc5350e\
19172a103390e9c5b6c131b5402f9b43efcbe2864a98ed40b534df3cc72803c37e89\
b9dc9f6ac4e3bc219913f6aa49a10fd587ca737284061daed1dc9ded416799f5d0e9\
483639d8139dfc05813df276a5fbd3b657d37c2d64774d912982e7854eac3983c284\
82278fa6f819e3f00cd0f113826f1df92eb7164a1bc9961354cb761a491a27499fbb\
1a9603d1c07b434c772dcccfa2e6a80b9a452eaff50ff23cada98b065003d74f6f5d\
0bad46893f9d94d5e308f65b848b4fb726a15099123c9e1b918f0a74e7703bd746c2\
f8e7f5f3d5a4c475469ea2bf37dff5cb3a0b5596b24eb278b5ef849c4143b3429ea6\
d463eb5a17267e81830e60f11e4803663d07ce029ffe9448980ef0daacc315919425\
1279591d316c7fc10bb853aafbfe6b6f75d3569855113d57aa8ecc911e2023fb49e2\
b8643e00a30bd6c69588eeb19dffacac80d140df33bf09cf16babf76e8d6d82341fe\
cabe76259296b644ee001e10a6f33d4d6cda0bfdb742b1c7d33c702563b3d32dec28\
07610c0b09c07a9fea3002bd4be5c511f185afbeea7ee11175b70a345ec48658372f\
b8e79cccc14c47b541dcdbce012ee3e4b3f0f3a01576e34edd5d6e2f4f8b49a7f3f7\
```

```
e831643e6b8b11ce4a4e9b66bdfb9664b5ca5fac6f0089f51cccb4ca076afa0540d0\
89da1486caa3228245e2d0fcb22cd3b4943a0ea4040b283504dd34b2b85453749613\
e6659f2c91a7652115c4886e7e2030d08edf85db93ae1befe326da6ed92f4c4ac2ea\
1ce6d5030cfc909a6e821c8d4514d658555e40dd5efa57b6d1c05e85db6284fdbcb7\
78c4d8e09eea446aa046174e0877998a830974a51b4aee52c896a9f3ee1b5c3bcac9\
bf4663ca5d100b2bf96daaef9e411297c65a66f4819c95298e05fad7991ceba212d8\
4379475012e925856ad8d8933f09178428321507e99f00c0fd85ad8a73b27a4b48a0\
a9c37752fd6ae03d270d173e43720f26a6e5d004108d8ba5652a5ffb0c0af895af21\
8481f6a3fb0212c7f530dd39950ff945600e29e917314af5378cd175e269d9b49c53\
963fdb31e1553eed7008e842375fed0cb377e2fc1d1de540a6fcbf1d324c9f1f04bd\
42084b6c9f5ac30bde6f7e3a334999b7003a388ac1604fa651e77daba71457e00d0c\
528b036d1947ab5bb4c0ce2a29ee37f62690b96c655285a70604881a10ba8bad19ec\
171fa73be914d0571dbf1e6f01fc8a8b83499a6f507905f6027bdffdbdee06259de8\
5fe11f68a4c414f6c7348f1ec11f1d9777e4c562b964964359842773f29f0091e953\
dadbed437c8d35351bf12ec8f91cdde59bfd10f4bb63153039c8baa683102cb90a29\
029f691a33c274b4391887a036be6a77e3c9f894f0573ffa5d8c6de1ab01e4af0b42\
8f4bc371d0d5f7af6d40b108fca27431c7bf2a40dae8049a3aceb56d5773f0801603\
9d6d0370b5a081a1a0f22998330af2fe1643860546847bee9d67c56747da91b42d60\
c1a4f1686669e34683f24ffceda910176902f75830a520aac9e94fe8d7b006488182\
d6da449ea6d627141553f613070a6498b2ca27a87f50e20c8f30d621fd20fa83187c\
28
```

Figure 8: HPKE-8-KE COSE_Encrypt (Hex-Encoded CBOR)

A.3. HPKE-9

NOTE: '\' line wrapping per RFC 8792

```
{
  / kty / 1: 7,
  / kid / 2: h'f3ea0bc050e5462b22ce7bce2af65e7e265d45cd591840175d2c9\
    ea658069628',
  / alg / 3: 56 / HPKE-9 /,
  / pub / -1: h'6446caaee4cb4d12597fe53280e590c2e04dcc286af32ba11935\
    484cb794ede9860fdb45f68144cb504ff61981456a3ce19ca3afcc65be469d08\
    dcaee6239fba8202ee903924273703b04da7664af139cd3d3b1827d05389c8c2\
    86520c3182954a793d5a30a3dc4a8cf7445a46248763131427455 5f1f63fd3a0\
    6aace0c2c0d3bfe8160669ac47b334805696ab9a4122490399c3207ac6c73476\
    c53630654600d403042bb7352b3681998dd5fb255a9c73ab237862d661c24a33\
    726b06ced39b9e06075c4b60aa9a38e262aa5c77cc048c63becaa067ebcdcc6c\
    a9d38384ae8b46e5039ebb981066ab99e13952ec9ab18e337492d27d5aaa1fbe\
    5ab58b4246f7b54beda2742072699c597cfb871bab0abbf966a7ffd5347c9bb1\
    d7c3c10c1ab78e4422c0b89764e93d2a58229fa046c29c7e24f79d20e3841049\
    ca2e943083794e646b877d71824f906419f938b15551ddd83bb8cbc2e32152e5\
    fb6f8202167cc3c8e0b57edc31021bea437b5bc4a50144e44c12047521a728c0\
    5ae3041dba5329abb9a0699500861744a65f67708815057 7807a0165d650a118\
    445f32a67643c1da3248d7a16714650afc649962c5caebc21493f9449e285369\
    d9c112133bf3ec21f59b405d0b0a810b5475647b9c5b7ac9602449021e826273\
```

```
      ce4130e3f141acd6142170bddf48757588b5b19c39647a37766637562ab8a4b8\
      a28b137d2eb77357a44623047c7e6a6a6ea34073f715b0578f0138879f0050e6\
      47a3d412cc02451f6212695f5955fbdb65a192c0e8976446801e5e712f231c98\
      d53518a6e818b9951e111c255b28159ce89db088bf029a35280526f93a1c47a9\
      b4cc6b46d98434ee651e236caa6dcb5c83a12f6155412c3bbf44978b172030f9\
      777f597816368233a0e3390972ceb4309c2703282c99275b57603717456471b5\
      99083d4f9c0131b101a632bc6bda0e9dfc556e58a4dde5076244bb4d584a4aa0\
      8ebb2381cc342e56d1c0b7d43a382a0e82ea9498978157819277920f4a7a427a\
      776a06310a67625390dc0592eaaa6e68a512760c1c43ad314caf796662ebfaa6\
      da43c6eda55c8c557d538a57644b9120972e82f2541f7ab0f5443bb2682ab1a2\
      4c173ac356c00641622d0c9c5c10e8017414c08a2b7df62818980784c8da0af8\
      6438e8e62c373ab9f82b8288218964a34e6d685d76744e92663a8c51bb2bf93f\
      460bc08ff696d283c81331b3d2306d66a54331314717a778abd7aba4739a3bc8\
      7d7bb9369e7ac6c8782425838f408995acb35cf77384275a8bcd44b025a868f0\
      aab0365387a83b898262a849f121a974117c887af2a36a67a482f49609ffe970\
      a4a93f4d0518c4951d4641c1f5f824070ca81ac8b49cba4e84c8a7b08737d823\
      321ccaaf06c73d0e54a0999381822a2fca712d8ff82a755677658c0301a49a5d\
      31bbc0b33237005f572726e5374c41e66cf1dc2eea989fa3f518cc1863d4463c\
      bb721d4b73956a30ca66a930f7379369c13693056c0a40ce2bfcbec105c4bf21\
      426c0616dc800d6e902e230a62ac625f153587205126d42a8be055cfb7c6bd0e\
      eb061d00aeab76c4902b699d188e4c63aa81549949692ea316c69e5ba286b45c\
      e4d618f3b3c2bcc491571b611cf4baf807f6c8ffc758c91c7eedc3c0dc821710\
      4981fbed5c62c54a6f19aba106e338a974854b78397e320eacffc8c371edbb92\
      2db1a9755058',
    / priv / -2: h'b500d252df8c81dd0b3458942bd54496e267aed834e7ba42abd\
      ec0e7811d6e23'
  }
```

Figure 9: HPKE-9 COSE_Key (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
a50107025820f3ea0bc050e5462b22ce7bce2af65e7e265d45cd591840175d2c9ea6\
5806962803183820590 4c06446caaee4cb4d12597fe53280e590c2e04dcc286af32b\
a11935484cb794ede9860fdb45f68144cb504ff61981456a3ce19ca3afcc65be469d\
08dcaee6239fba8202ee903924273703b04da7664af139cd3d3b1827d05389c8c286\
520c3182954a793d5a30a3dc4a8cf7445a4624876313142745 55f1f63fd3a06aace0\
c2c0d3bfe8160669ac47b334805696ab9a4122490399c3207ac6c73476c536306546\
00d403042bb7352b3681998dd5fb255a9c73ab237862d661c24a33726b06ced39b9e\
06075c4b60aa9a38e262aa5c77cc048c63becaa067ebcdcc6ca9d38384ae8b46e503\
9ebb981066ab99e13952ec9ab18e337492d27d5aaa1fbe5ab58b4246f7b54beda274\
2072699c597cfb871bab0abbf966a7ffd5347c9bb1d7c3c10c1ab78e4422c0b89764\
e93d2a58229fa046c29c7e24f79d20e3841049ca2e943083794e646b877d71824f90\
6419f938b15551ddd83bb8cbc2e32152e5fb6f8202167cc3c8e0b57edc31021bea43\
7b5bc4a50144e44c12047521a728c05ae3041dba5329abb9a0699500861744a65f67\
7088150577807a0165d650a118445f32a67643c1da3248d7a16714650afc649962c5\
caebc21493f9449e285369d9c112133bf3ec21f59b405d0b0a810b5475647b9c5b7a\
c9602449021e826273ce4130e3f141acd6142170bddf48757588b5b19c39647a3776\
6637562ab8a4b8a28b137d2eb77357a44623047c7e6a6a6ea34073f715b0578f0138\
879f0050e647a3d412cc02451f6212695f5955fbdb65a192c0e8976446801e5e712f\
231c98d53518a6e818b9951e111c255b28159ce89db088bf029a35280526f93a1c47\
a9b4cc6b46d98434ee651e236caa6dcb5c83a12f6155412c3bbf44978b172030f977\
7f597816368233a0e3390972ceb4309c2703282c99275b57603717456471b599083d\
4f9c0131b101a632bc6bda0e9dfc556e58a4dde5076244bb4d584a4aa08ebb2381cc\
342e56d1c0b7d43a382a0e82ea9498978157819277920f4a7a427a776a06310a6762\
5390dc0592eaaa6e68a512760c1c43ad314caf796662ebfaa6da43c6eda55c8c557d\
538a57644b9120972e82f2541f7ab0f5443bb2682ab1a24c173ac356c00641622d0c\
9c5c10e8017414c08a2b7df62818980784c8da0af86438e8e62c373ab9f82b828821\
8964a34e6d685d76744e92663a8c51bb2bf93f460bc08ff696d283c81331b3d2306d\
66a54331314717a778abd7aba4739a3bc87d7bb9369e7ac6c8782425838f408995ac\
b35cf77384275a8bcd44b025a868f0aab0365387a83b898262a849f121a974117c88\
7af2a36a67a482f49609ffe970a4a93f4d0518c4951d4641c1f5f824070ca81ac8b4\
9cba4e84c8a7b08737d823321ccaaf06c73d0e54a0999381822a2fca712d8ff82a75\
5677658c0301a49a5d31bbc0b33237005f572726e5374c41e66cf1dc2eea989fa3f5\
18cc1863d4463cbb721d4b73956a30ca66a930f7379369c13693056c0a40ce2bfcbe\
c105c4bf21426c0616dc800d6e902e230a62ac625f153587205126d42a8be055cfb7\
c6bd0eeb061d00aeab76c4902b699d188e4c63aa81549949692ea316c69e5ba286b4\
5ce4d618f3b3c2bcc491571b611cf4baf807f6c8ffc758c91c7eedc3c0dc82171049\
81fbed5c62c54a6f19aba106e338a974854b78397e320eacffc8c371edbb922db1a9\
755058215820b500d252df8c81dd0b3458942bd54496e267aed834e7ba42abdec0e7\
811d6e23
```

Figure 10: HPKE-9 COSE_Key (Hex-Encoded CBOR)

```
   NOTE: '\' line wrapping per RFC 8792

   / COSE_Encrypt0 / 16([
     / protected / h'a1011838',
     / unprotected / {
       / kid / 4: h'f3ea0bc050e5462b22ce7bce2af65e7e265d45cd591840175d2\
       c9ea658069628',
       / ek / -4: h'ff8b5edd7ac5ab9020ddd455aa1738c6140f32481205cd2db43\
       4eb16a52c522a717fa5cb46a3d7dfb918a5901bd8217cf4d5ea2f0004cf90351\
       6d2a8cfbd8ec7b1422bc50a38efe8ccddb6111263a9050a6b984fd9e1aaf7016\
       cab7a511dcdb24dcc12dc1d3ff4cafa386f3c2d5ba1984220644b42db05545c7\
       c0033f315411b49d2f355d0e8c55aec918cec25336e24a33013bfee1e6bdb7a3\
       4781b82835b51829c4a21d25101dd127552ce1ec504de533d605599a296a8d2e\
       952d347a98ae74bca25184da0ce853e1ebe85495e85999685a465ea666dc4fba\
       055e5c424bb1743798334f1716ee55be47682164a067333d2aca1817785f27e9\
       f3640060dca3b12a8e4cd0c2389a5d369922fd69c8e87a521d90f17b4d31d119\
       4b698a5dd28f88ceeec1443c3d5f87d9fb543b305042b2278be1e787a3a2d6a2\
       989cd9ab12d5b692e4ce3dab0ed0a129a14c104a60f4b209609f1778b7c3bea1\
       b27cb7e8bb45d3aff3a6ff6cea318037d04278b6afe3dade816758bca8cca43c\
       b07cdaff5070fdef0b5004a38926fb96648b83d0db20cedec1d2c7ac7a9aacfb\
       fd1ca6d63bb274e6200c023e4f2ca469579d6df4386a7cb393226100c69204fa\
       d3ac5c9326c253c02fe950da8e5a85c5bd29acb044714d97571c108de1eeccde\
       7b26789070b29a3f26b7bafe786238cbbb623bc5528a1100b37ede676a0cf5e9\
       1848399ff5aa48fe5721f05fd2e0c3a8a06e238754bee990795d565f12bea6b2\
       148d0ba5e08443ec202b57b5a0cdecbdf9f5ce5fc896136047d73baef5a47762\
       73ac6a1a11b56ac19d68719be1a96e12d17130aa712566a940ad1dfa7468a96e\
       b76945ca92ae09878cd82c8a5f07417243a02caab38b512eaf1653f65c1e56a1\
       b31daa703885ccc0f129eff8c13b98be82ce8229554f1f6a2524354cd6ebd7be\
       ec66f71b43542c3270085ea637f2f717380f6c04d9eb4c63f957a46905767bde\
       aa4901adf91ab16e74d54f3cc92b692534ee0a9d53d6fff7d80b9253a8108d3a\
       baa5facf066f4eb95df036b6910eb3a0587a19271e74f25b4e8269396f1daee6\
       2aec20992057232cb4d36bd3cba28e7bc8bef5326d49608bfc4f5839b986f140\
       32928b4b86b99d24bfdb3c7d2bb7bf15926e8bf3a2b2adff73828b595b1535d4\
       610c1f459419d1d6214358b2f922371be87bb7c3b8de65f7327a6735f4fb51a0\
       fbef85f61c1833511f8c9c0bced4ffdafa7d5c926dbafa4d0b39970e7e80266f\
       a288b55dab74200e636f23811cfd0d62504deb2f73fd06c389ca44409c8c700d\
       ecb6ed37735dbf34df79725cc526e12b0f791617c4b8a86f862ea07b30b018e0\
       ce91e11d143983cdf8d348d7b82d5d8f9eb41fc9aa61a39da5be90ec402b4753\
       182218d92583d474bb1b8f5d14e7018c269198b7678afde34645fbcbbc284a07\
       80f15786189d06723ca4cd719bbdf396e68fc0745e00357cf806c1d329dcc629\
       33619a1df84a6eb04ac73e95745484c37bd43ee4c9d4aaaca0f3b305e10b2781\
       f204e2227491206b016cf339f16e5bc596976bbe4654efe2a98bd6d919120600\
       6d71daf91ef67'
     },
     / ciphertext / h'e254aa60ccf2d64fa22a94cd2e03c860bf6d6e5f45f785bf7\
       3e0bfa2a232e6d3184bfa52da8ff15505dc214c61b242021d0a65482a415674d\
       b4f4a16318b7bc3c37e3d04e558d0a57d69280644a30fef16ca29b771d0e76a8\
       036c3bab729645c86ff622fe75f5b7a66f476c945732d694e8ac25bebf500d9c\
```

```
      84d88a6594cb28e2d63aa677cb71cd98f972ee2598363eea15e018e2365a889e\
      323b26385007a0016833c0319db0a3ca6c346fa28b8612d30bd02019f67e1427\
      49fb1c728e01c91f20e065c703c1f3cca002eeac8b09d104d02f797a2b43e1f6\
      125773e3378ef6eb18bea6830a4d3ae2e55488183c2331c8a63bcdda3d98b185\
      bd6ea6ae590bee18f9d44de3350cf6a7f2f3aeb42ed03408527709e1321f1ff8\
      0ae0943fb213fed63'
  ])
```

Figure 11: HPKE-9 COSE_Encrypt0 (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
d08344a1011838a2045820f3ea0bc050e5462b22ce7bce2af65e7e265d45cd591840\
175d2c9ea65806962823590460ff8b5edd7ac5ab9020ddd455aa1738c6140f324812\
05cd2db434eb16a52c522a717fa5cb46a3d7dfb918a5901bd8217cf4d5ea2f0004cf\
903516d2a8cfbd8ec7b1422bc50a38efe8ccddb6111263a9050a6b984fd9e1aaf701\
6cab7a511dcdb24dcc12dc1d3ff4cafa386f3c2d5ba1984220644b42db05545c7c00\
33f315411b49d2f355d0e8c55aec918cec25336e24a33013bfee1e6bdb7a34781b82\
835b51829c4a21d25101dd127552ce1ec504de533d605599a296a8d2e952d347a98a\
e74bca25184da0ce853e1ebe85495e85999685a465ea666dc4fba055e5c424bb1743\
798334f1716ee55be47682164a067333d2aca1817785f27e9f3640060dca3b12a8e4\
cd0c2389a5d369922fd69c8e87a521d90f17b4d31d1194b698a5dd28f88ceeec1443\
c3d5f87d9fb543b305042b2278be1e787a3a2d6a2989cd9ab12d5b692e4ce3dab0ed\
0a129a14c104a60f4b209609f1778b7c3bea1b27cb7e8bb45d3aff3a6ff6cea31803\
7d04278b6afe3dade816758bca8cca43cb07cdaff5070fdef0b5004a38926fb96648\
b83d0db20cedec1d2c7ac7a9aacfbfd1ca6d63bb274e6200c023e4f2ca469579d6df\
4386a7cb393226100c69204fad3ac5c9326c253c02fe950da8e5a85c5bd29acb0447\
14d97571c108de1eeccde7b26789070b29a3f26b7bafe786238cbbb623bc5528a110\
0b37ede676a0cf5e91848399ff5aa48fe5721f05fd2e0c3a8a06e238754bee990795\
d565f12bea6b2148d0ba5e08443ec202b57b5a0cdecbdf9f5ce5fc896136047d73ba\
ef5a4776273ac6a1a11b56ac19d68719be1a96e12d17130aa712566a940ad1dfa746\
8a96eb76945ca92ae09878cd82c8a5f07417243a02caab38b512eaf1653f65c1e56a\
1b31daa703885ccc0f129eff8c13b98be82ce8229554f1f6a2524354cd6ebd7beec6\
6f71b43542c3270085ea637f2f717380f6c04d9eb4c63f957a46905767bdeaa4901a\
df91ab16e74d54f3cc92b692534ee0a9d53d6fff7d80b9253a8108d3abaa5facf066\
f4eb95df036b6910eb3a0587a19271e74f25b4e8269396f1daee62aec20992057232\
cb4d36bd3cba28e7bc8bef5326d49608bfc4f5839b986f14032928b4b86b99d24bfd\
b3c7d2bb7bf15926e8bf3a2b2adff73828b595b1535d4610c1f459419d1d6214358b\
2f922371be87bb7c3b8de65f7327a6735f4fb51a0fbef85f61c1833511f8c9c0bced\
4ffdafa7d5c926dbafa4d0b39970e7e80266fa288b55dab74200e636f23811cfd0d6\
2504deb2f73fd06c389ca44409c8c700decb6ed37735dbf34df79725cc526e12b0f7\
91617c4b8a86f862ea07b30b018e0ce91e11d143983cdf8d348d7b82d5d8f9eb41fc\
9aa61a39da5be90ec402b4753182218d92583d474bb1b8f5d14e7018c269198b7678\
afde34645fbcbbc284a0780f15786189d06723ca4cd719bbdf396e68fc0745e00357\
cf806c1d329dcc62933619a1df84a6eb04ac73e95745484c37bd43ee4c9d4aaaca0f\
3b305e10b2781f204e2227491206b016cf339f16e5bc596976bbe4654efe2a98bd6d\
9191206006d71daf91ef67590121e254aa60ccf2d64fa22a94cd2e03c860bf6d6e5f\
45f785bf73e0bfa2a232e6d3184bfa52da8ff15505dc214c61b242021d0a65482a41\
5674db4f4a16318b7bc3c37e3d04e558d0a57d69280644a30fef16ca29b771d0e76a\
8036c3bab729645c86ff622fe75f5b7a66f476c945732d694e8ac25bebf500d9c84d\
88a6594cb28e2d63aa677cb71cd98f972ee2598363eea15e018e2365a889e323b263\
85007a0016833c0319db0a3ca6c346fa28b8612d30bd02019f67e142749fb1c728e0\
1c91f20e065c703c1f3cca002eeac8b09d104d02f797a2b43e1f6125773e3378ef6e\
b18bea6830a4d3ae2e55488183c2331c8a63bcdda3d98b185bd6ea6ae590bee18f9d\
44de3350cf6a7f2f3aeb42ed03408527709e1321f1ff80ae0943fb213fed63
```

Figure 12: HPKE-9 COSE_Encrypt0 (Hex-Encoded CBOR)

A.4. HPKE-9-KE

NOTE: '\' line wrapping per RFC 8792

```
{
  / kty / 1: 7,
  / kid / 2: h'1bac0382c69ab1d21edc61bd062af6bfbef532d1639afb31443c1\
    b4b377de735',
  / alg / 3: 57 / HPKE-9-KE /,
  / pub / -1: h'f2b1ac0dc6035588075c97681bfcb8b2795fff367627b209fddc\
    8669fa14fbc3c1a9d49be1d28002080bbd42ce8bf930ab109d2d7aa1eec8a73e\
    550f11001779a2139ce91826108937fb6958105b65c942e2c01734722d500578\
    29f026120ca59742a2a8a4688584238704a548042103d37000f26160c8193d69\
    037f5cc525ec53fe9aca7252c647353e024b800ae99c6e812b26a19821175755\
    f37b26a7c85df70d23f4024a9729b8093fc0c396c4e223d96c5d08c31f775401\
    14aa008b570cfbf72e2f5256c0e2b94ac0bb14a83960965d64f279dd190552eb\
    193eb85c5ac64cb0e15726680e8de57d6d4580d67a4a109b7b9c3794f4419b20\
    255e97e44286b8877b5b5cc783858140ab081bc4a4997d7746a6e63ab061007e\
    5a6c1567720554733673934 26ff3078649c9b1a0aaad232611427b5c1a5359b7\
    5494c34c322abd3dc7765b0bccca866635a73fc4a9a4e55c6406aa2b59467789\
    e57070662dedc64eda6bc9c2294271cb33e934c8667bb2989539efe279d7411b\
    55f197481377fc10a97f01c002a57ead969be6858f15e6108a48c01e279b9428\
    0dedb48a97a53e342a6868f03e9f54378cc63ebf3172e2268cf1385fa177735d\
    0a34a0b0afc8e6786aa96fe04a98411161e7544de899329397aa51468799a015\
    ff2ca3ef00449193480d634ecbb640ba7683979b5716951a3e61cb4384505757\
    c203c636ee043fe27398db3747867ab5d963abbcd37e0eb7462344a1a4d5b301\
    132d33aca20d7515db247f6fa2930f2ab46323334021c1421b1cad708dd90c57\
    7788478fe823673a099629ba5f26c696b1ba11a324bc829fc2e859ee8c514ee0\
    b78462414a4329b50360dd387896ea25f8597b59ea4cd2f398395c9875100d7a\
    ccc9e964ca6490adcd484f712073788997683a8d78202df632015e9a095fa9bc\
    45588ce1b5bc620b51eaf2b671e356e7258201f380f4d9a204302115a30d4e7b\
    9e8acb6bd9e109873159db026c4f5306faf1b6108cae50d06ac2536356f478bd\
    f10058e99e06e039bfb072df272c38c16fda1936786b2c233984f3a64e8f93a3\
    d7541614f46b48cc79ccb743bb47a9fe93c260d522712b5c0ed22fcbea5f276b\
    84741a09e61744f5db881993a54dea3321675e11c06bbfeb042662a4ee135e39\
    20695690256034c34d5a6f3a293e989011fe16cd9df098e79b050fb0becf139f\
    ae341d63058b0d2487e665782102b3b1e27cc75c3971b596cdb52a176a4d6410\
    c40234a98aaa95c603808a468ec3331a58011134e797e8d15892681ada744497\
    9b78eb0a13bdba814d2c4130ec5c4b72826f399372aacb55f4bd09c8b90da01d\
    52369df0dccc401a07cb05880054c0f01978a7c71bec6a91f45709615b0ce909\
    5c8dc1826792a16a18183a5047e65c3a6d1322e3c2731eb4566b5a2d5f1997a6\
    b70b17842204a1197caa47ad2b2cce508028e2b2b651bbff1b4d3d167f51e666\
    793462c875950c27104b33365bd53fee17c66be044ae65b6d023418ada966661\
    2498645c8b62b13fb70971eb935e3a5801c5569b5c78655375fc9b428ac094e5\
    e803a17222f2e147c198a02a1701501212f807a9bd228d7420371ea796cf274a\
    691ccce87775884ca239065dcf8a5c183ae472c6ce82252908718cfce3de2003\
    e567c0ea46387a5b16bc3bc630cab7c966ceaf2d47008d6f899f901a36940559\
    4fd575b8530d',
```

```
    / priv / -2: h'abf68310c6694408db8aa1f03b6def29c80899889e4aa52c08a\
      ef059912cabc6'
  }
```

Figure 13: HPKE-9-KE COSE_Key (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
a501070258201bac0382c69ab1d21edc61bd062af6bfbef532d1639afb31443c1b4b\
377de735031839205904c0f2b1ac0dc6035588075c97681bfcb8b2795fff367627b2\
09fddc8669fa14fbc3c1a9d49be1d28002080bbd42ce8bf930ab109d2d7aa1eec8a7\
3e550f11001779a2139ce91826108937fb6958105b65c942e2c01734722d50057829\
f026120ca59742a2a8a4688584238704a548042103d37000f26160c8193d69037f5c\
c525ec53fe9aca7252c647353e024b800ae99c6e812b26a19821175755f37b26a7c8\
5df70d23f4024a9729b8093fc0c396c4e223d96c5d08c31f77540114aa008b570cfb\
f72e2f5256c0e2b94ac0bb14a83960965d64f279dd190552eb193eb85c5ac64cb0e1\
5726680e8de57d6d4580d67a4a109b7b9c3794f4419b20255e97e44286b8877b5b5c\
c783858140ab081bc4a4997d7746a6e63ab061007e5a6c1567720554733673939426f\
f3078649c9b1a0aaad232611427b5c1a5359b75494c34c322abd3dc7765b0bccca86\
6635a73fc4a9a4e55c6406aa2b59467789e57070662dedc64eda6bc9c2294271cb33\
e934c8667bb2989539efe279d7411b55f197481377fc10a97f01c002a57ead969be6\
858f15e6108a48c01e279b94280dedb48a97a53e342a6868f03e9f54378cc63ebf31\
72e2268cf1385fa177735d0a34a0b0afc8e6786aa96fe04a98411161e7544de89932\
9397aa51468799a015ff2ca3ef00449193480d634ecbb640ba7683979b5716951a3e\
61cb4384505757c203c636ee043fe27398db3747867ab5d963abbcd37e0eb7462344\
a1a4d5b301132d33aca20d7515db247f6fa2930f2ab46323334021c1421b1cad708d\
d90c577788478fe823673a099629ba5f26c696b1ba11a324bc829fc2e859ee8c514e\
e0b78462414a4329b50360dd387896ea25f8597b59ea4cd2f398395c9875100d7acc\
c9e964ca6490adcd484f712073788997683a8d78202df632015e9a095fa9bc45588c\
e1b5bc620b51eaf2b671e356e7258201f380f4d9a204302115a30d4e7b9e8acb6bd9\
e109873159db026c4f5306faf1b6108cae50d06ac2536356f478bdf10058e99e06e0\
39bfb072df272c38c16fda1936786b2c233984f3a64e8f93a3d7541614f46b48cc79\
ccb743bb47a9fe93c260d522712b5c0ed22fcbea5f276b84741a09e61744f5db8819\
93a54dea3321675e11c06bbfeb042662a4ee135e3920695690256034c34d5a6f3a29\
3e989011fe16cd9df098e79b050fb0becf139fae341d63058b0d2487e665782102b3\
b1e27cc75c3971b596cdb52a176a4d6410c40234a98aaa95c603808a468ec3331a58\
011134e797e8d15892681ada7444979b78eb0a13bdba814d2c4130ec5c4b72826f39\
9372aacb55f4bd09c8b90da01d52369df0dccc401a07cb05880054c0f01978a7c71b\
ec6a91f45709615b0ce9095c8dc1826792a16a18183a5047e65c3a6d1322e3c2731e\
b4566b5a2d5f1997a6b70b17842204a1197caa47ad2b2cce508028e2b2b651bbff1b\
4d3d167f51e666793462c875950c27104b33365bd53fee17c66be044ae65b6d02341\
8ada9666612498645c8b62b13fb70971eb935e3a5801c5569b5c78655375fc9b428a\
c094e5e803a17222f2e147c198a02a1701501212f807a9bd228d7420371ea796cf27\
4a691ccce87775884ca239065dcf8a5c183ae472c6ce82252908718cfce3de2003e5\
67c0ea46387a5b16bc3bc630cab7c966ceaf2d47008d6f899f901a369405594fd575\
b8530d215820abf68310c6694408db8aa1f03b6def29c80899889e4aa52c08aef059\
912cabc6
```

Figure 14: HPKE-9-KE COSE_Key (Hex-Encoded CBOR)

NOTE: '\' line wrapping per RFC 8792

```
/ COSE_Encrypt / 96([
  / protected / h'a10103',
  / unprotected / {
    / iv / 5: h'fd586d64c8d6f44930c12b0a'
  },
  / ciphertext / h'6e6abc1b00632d6607e8f5e673544e72a18a8b0602fd7497d\
    d58f27d109b4560ba367fa0a8391b974d08eade4c5e0aaa7da1faa7906c82381\
    4e3ef41d03ac857d16077a76f2169e952d8d6ace596005f5b951d74b9f275e33\
    7175186d5069477188bcc6e5405798009fc7f7552026713f927f12a0612def3f\
    c5552cbc87e68bb7dabbc2d44fa4f1a34eecb3b4c0e42894c79e71c16ccca6a2\
    2dfbce49bb682fc207cee21ca765589dceb807d03d497b85a2eb0c411439dae1\
    ea47179dfa4fc7ea7550a6a013c453ba2da105810a9ce0e18555da87a70ece33\
    acef5776d768277b437e88e80d259ceaaae0c7271e51fac2b08f6d91428b5d0b\
    4703473f2a4345fa0d04c79d77fb222068b4233765c8c4d23c0dd5e850da551b\
    84f77099a77eab71a',
  / recipients / [
    [
      / protected / h'a20118390458201bac0382c69ab1d21edc61bd062af6bf\
    bef532d1639afb31443c1b4b377de735',
      / unprotected / {
        / ek / -4: h'37695f02689bbe11fd8d98bb22c4a987e16a3c275f6d2b8\
    64b48228e375d67ff5030a8854b0f605820c5d4656b1344e562f13dcfe407206\
    31d05e0d361369a4bc099d0a914de0c2e73a04242d5546f172e0142b6103f321\
    a8bf62f943c5f4078d3b4ae195145ecb1cf72ef0ad778d6d7dc17661ae7c5f93\
    b926f36cb46182566cbff401ae690ec4d1a6fceb049926b53986ee535a939a1d\
    57dc0bb5fdbb7d1b568bea28fa2c9b19b2378dcc9d3677d9920d636b2e4c7745\
    85b2341dc8382d535787ad21cdd64e30007eb6ec0250f384e5ed4e78de1389ba\
    b2fc4a075e051332dd60008325581d0605373d33b42526dec1827386cb8c0b31\
    7cec6457e46187789ec33ffbc936da78435dd4b6f0c950cf4ad7ed0a28396b21\
    d9fae4a12fc78934820ddd09784b1e2fe0f79f88a762319eb8ccddf1629e4253\
    d6ba850baae98b46e03ebccf0664ea2300d67145ad627d01bcda46d267aaf248\
    47fa489418024dcb051735d7f5c674b894fb9117aa631a01acdf2458b8d088af\
    d7e8c1f8c4e6abf4e31c3587dd33ad8385413508d9bf2b2aaf9fce48a2004007\
    7cc671053e659f5f1313e44d3abe4cae01ce61e98bb8a2caa7ae611507465a1e\
    45c707ab1379189e2452685dbe7af446f35df8a4e0c5a0f1c63f1014ef90f822\
    8259a054aa12347ae5658441c3e9442d51689fa31d2ffa1fb9009e1c095039f5\
    37cb7d34bc48b8a4a4f9483e14a560a8fe62038bf9df51e0c674ea07542d3f25\
    fadb5ebb87b5cc1a2f52ec27312e7cd73df864fe257b46c56398d594fca2bcb2\
    b8330d1cc912cd9a2e0c29d260e0ee8c4e5913c131091bbf50eafd6485caac33\
    009a3974f4b314d4c5cec2f7e0b8f00ae81443fc5bb174eafe3b7cbb6a0db010\
    d109355263b2fb4fb2f0481d13084a11260000462a87e0eb65a91bab7a6e0823\
    1eb28d5739ba20426c032349afb9588635cfeb3e4ae9a93c6a0d6df47c7841b6\
    9f2c0a2c49b32a7dcf56c93c4de3ee273b84f69c4c43fb43556ab3638238bfe6\
    c54d200dedb44175230786aa41922866cbedf49e00f8e6629aabd125bcff64bd\
```

```
      533a7cf2cfdc13c5cce4a15411a31f0855b54cd74864bef084da705b6625fc58\
      931398e757906e973113d6f4229e88dcb9cc8686a900936d53b591b38f967156\
      692539b4d48dbb0ae241c0064a2debb1dc7b90f47c23f2fccff5cab8b5f057e8\
      c518e33c766bc4253a30ae9637ff4d6b1f96d4e673a1a12cc85d129ccb4fd01b\
      475dbdfcc876b65dabdb1fbe5f4079298113314549690b49fb6bcae99c106dfd\
      313ccdf6176635b9041eb082f7b10f903b7d01a9c49a14b2279a518922c48fb3\
      d90d1f4069cd0c753b07895cabc197e8dddb5a371265501cd8b6f8531cd116a3\
      8d28e292371c9c2ba7c579811f3420265131b55bd1595d5c7a6a95ed3c88e42a\
      f43f713704aae8848fbfaf2ade792414f1cf5f0f2181f1bb8a8be8233350f0f8\
      42ea2910b34343c3118d472369d77be9a7399238b31becfcea9a7406bc3703c7\
      a30bddbf128e6e769aca976239c5a84a839cb9e4c05b1f255779d4cb5dce9995\
      3f196e90be4f3d813'
        },
        / ciphertext / h'bd5b7833e43a7ce20b533599665d795fdcc8d3e344270\
      425f88d6c778f75b57c5eeb7cf0adc82fe546939cc4b4507998'
      ]
    ]
  ])
```

Figure 15: HPKE-9-KE COSE_Encrypt (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
d8608443a10103a1054cfd586d64c8d6f44930c12b0a5901216e6abc1b00632d6607\
e8f5e673544e72a18a8b0602fd7497dd58f27d109b4560ba367fa0a8391b974d08ea\
de4c5e0aaa7da1faa7906c823814e3ef41d03ac857d16077a76f2169e952d8d6ace5\
96005f5b951d74b9f275e337175186d5069477188bcc6e5405798009fc7f75520267\
13f927f12a0612def3fc5552cbc87e68bb7dabbc2d44fa4f1a34eecb3b4c0e42894c\
79e71c16ccca6a22dfbce49bb682fc207cee21ca765589dceb807d03d497b85a2eb0\
c411439dae1ea47179dfa4fc7ea7550a6a013c453ba2da105810a9ce0e18555da87a\
70ece33acef5776d768277b437e88e80d259ceaaae0c7271e51fac2b08f6d91428b5\
d0b4703473f2a4345fa0d04c79d77fb222068b4233765c8c4d23c0dd5e850da551b8\
4f77099a77eab71a81835827a20118390458201bac0382c69ab1d21edc61bd062af6\
bfbef532d1639afb31443c1b4b377de735a12359046037695f02689bbe11fd8d98bb\
22c4a987e16a3c275f6d2b864b48228e375d67ff5030a8854b0f605820c5d4656b13\
44e562f13dcfe40720631d05e0d361369a4bc099d0a914de0c2e73a04242d5546f17\
2e0142b6103f321a8bf62f943c5f4078d3b4ae195145ecb1cf72ef0ad778d6d7dc17\
661ae7c5f93b926f36cb46182566cbff401ae690ec4d1a6fceb049926b53986ee535\
a939a1d57dc0bb5fdbb7d1b568bea28fa2c9b19b2378dcc9d3677d9920d636b2e4c7\
74585b2341dc8382d535787ad21cdd64e30007eb6ec0250f384e5ed4e78de1389bab\
2fc4a075e051332dd60008325581d0605373d33b42526dec1827386cb8c0b317cec6\
457e46187789ec33ffbc936da78435dd4b6f0c950cf4ad7ed0a28396b21d9fae4a12\
fc78934820ddd09784b1e2fe0f79f88a762319eb8ccddf1629e4253d6ba850baae98\
b46e03ebccf0664ea2300d67145ad627d01bcda46d267aaf24847fa489418024dcb0\
51735d7f5c674b894fb9117aa631a01acdf2458b8d088afd7e8c1f8c4e6abf4e31c3\
587dd33ad8385413508d9bf2b2aaf9fce48a20040077cc671053e659f5f1313e44d3\
abe4cae01ce61e98bb8a2caa7ae611507465a1e45c707ab1379189e2452685dbe7af\
446f35df8a4e0c5a0f1c63f1014ef90f8228259a054aa12347ae5658441c3e9442d5\
```

```
   1689fa31d2ffa1fb9009e1c095039f537cb7d34bc48b8a4a4f9483e14a560a8fe620\
   38bf9df51e0c674ea07542d3f25fadb5ebb87b5cc1a2f52ec27312e7cd73df864fe2\
   57b46c56398d594fca2bcb2b8330d1cc912cd9a2e0c29d260e0ee8c4e5913c131091\
   bbf50eafd6485caac33009a3974f4b314d4c5cec2f7e0b8f00ae81443fc5bb174eaf\
   e3b7cbb6a0db010d109355263b2fb4fb2f0481d13084a11260000462a87e0eb65a91\
   bab7a6e08231eb28d5739ba20426c032349afb9588635cfeb3e4ae9a93c6a0d6df47\
   c7841b69f2c0a2c49b32a7dcf56c93c4de3ee273b84f69c4c43fb43556ab3638238b\
   fe6c54d200dedb44175230786aa41922866cbedf49e00f8e6629aabd125bcff64bd5\
   33a7cf2cfdc13c5cce4a15411a31f0855b54cd74864bef084da705b6625fc5893139\
   8e757906e973113d6f4229e88dcb9cc8686a900936d53b591b38f967156692539b4d\
   48dbb0ae241c0064a2debb1dc7b90f47c23f2fccff5cab8b5f057e8c518e33c766bc\
   4253a30ae9637ff4d6b1f96d4e673a1a12cc85d129ccb4fd01b475dbdfcc876b65da\
   bdb1fbe5f4079298113314549690b49fb6bcae99c106dfd313ccdf6176635b9041eb\
   082f7b10f903b7d01a9c49a14b2279a518922c48fb3d90d1f4069cd0c753b07895ca\
   bc197e8dddb5a371265501cd8b6f8531cd116a38d28e292371c9c2ba7c579811f342\
   0265131b55bd1595d5c7a6a95ed3c88e42af43f713704aae8848fbfaf2ade792414f\
   1cf5f0f2181f1bb8a8be8233350f0f842ea2910b34343c3118d472369d77be9a7399\
   238b31becfcea9a7406bc3703c7a30bddbf128e6e769aca976239c5a84a839cb9e4c\
   05b1f255779d4cb5dce99953f196e90be4f3d8135830bd5b7833e43a7ce20b533599\
   665d795fdcc8d3e344270425f88d6c778f75b57c5eeb7cf0adc82fe546939cc4b450\
   7998
```

Figure 16: HPKE-9-KE COSE_Encrypt (Hex-Encoded CBOR)

A.5. HPKE-10

NOTE: '\' line wrapping per RFC 8792

```
{
  / kty / 1: 7,
  / kid / 2: h'b453b5dfd9661a61fd09e46152c5d7daa9f5c04e3622e55e1ac60\
    45a66ffc4c1',
  / alg / 3: 58 / HPKE-10 /,
  / pub / -1: h'd4a518aacabdd20862c2816e4898cbd6a2a1661450ba319fe9c5\
    c9b524522684a1a4cc9018c76cbbe79325313a16765e51036d5b235fb11023cd\
    0a98802bca07d31665d770ce46250aa4525e57121e681008b923f7f4c82598a9\
    1c85cbd649b8ff69c638843cd0f09bc6c70b37e8b228ab7d8a426dd4ab3de5a6\
    bf3d2c119ee9b5e0c56e1c8c99bb9c004313cd4e3c3d4b7127234383c8368f69\
    51b9cc7a8807e996f3723a59f254150444adf4478d3c16873b6c60b36495d8c7\
    31960ac408b0a2e7a6cddca6a08a01c5a79b5c8c8b9c7b00c9c28fdcd07259ac\
    4c5eb12974930642f783c1b5b5b1739f7c0ba54f3c3b6e878705d41c18837383\
    bc6221772061eabde4a9aa6cda8a32464d162039c05a4e8e8cb591413db270b0\
    56c57e23f754ad67246ab83224d50e36844c382a31e1cbb3884514dd69012bda\
    4e04a5755a3acbd2406a059532d8386c9892c6e908c92e783833a4b80310260b\
    0a7fdb336314668c6cb642a0aa8fb7e1467bfb97c8056aa18799da301f5a042e\
    6eb4409773557847302742 1e21a7880f53fb7d9b04bbb03d64777fb39b4b028\
    aa45e76f3466a0e7d243140231b946b0f97accc95c7a7591b9c5f3a769413c8a\
    fb99eb888f43d6ac012ba0505549b6e4200fba4e365c3471442adbea9557e413\
```

```
      4b7486fc081d9fe48386a7bc8b156ba902344d8985540aae467883804c7af0d3\
      388e6c8fbf0b8441e375d298808fdc3b8ce745f7c76eb6477a52c406a4f7205d\
      cb02457acdf6e48ba554022545331681b748172e504861ec33abea601c1b465a\
      7b473d1397b6a9367a6d4537136299657b9bfb17198fba064aca7082b1b62137\
      7ec738ba69ec6eee0b9830c68fe1e9373c4863505c15e4782dccd4a0a7d48e40\
      400f95826cf260a9139b4db18aae27443709761aeaea9ee5229863c30ea66929\
      b9a8ce9884046ef5239894318d24313d77033f46b4b9c75b1b493492c86aacf0\
      145af4a82d28c057101d832c5ee6975720292b4a3b342ee1bb7da73481cb65c3\
      d448babab7e84178122b6c3345a101eb9b92611dee084807f14899f40ac7b25a\
      26c731d2d69801e8510f794dddd03c9be34d7762645f60c15e64322aa87526c9\
      5c6821cd61a728e6b951aafa70474b7de3f9cd6e494ee68032db965c27689a02\
      2c0090f496a6d7cc4403353ff4cca13153bfa47ea8a01ec60aad29804ae7f689\
      2a91a30ab8b8192930bf544f7970b79ab38934027ff3f8cd975c958d555587d9\
      434934063abb585a598703d8c601344addeb28fc33b938d591cad698fdac1bc4\
      b27765e4adb4b644977263efd91dd4b8a00171662e24b97cdc62a8495c8ee81b\
      dd6c7674d3c485595cd9d234e8d9b89e77c8114643c3391f0dc535f9d255d0f7\
      1409b01b3f2a2b684a95486270315164b796bd42aa945ca634de126c4daa84ba\
      480cd2b6283e5109fd4baa469b6818564159d49cb76a4423b9ae399034962719\
      a6e62ac788c60809234bfc6e6852a389e131035206c92a045f9113b911194ed3\
      5da7d8432b2250efac1572856a9678841de51349dc604c810633734b69cab11c\
      55409a05117c0a23a36502c78b175dd2b8ed1b41b908817f967ed21c760c3aaf\
      8244ce2b3cb9b6b109f4c86f29cb58b1845642c5b3e65cb459302051e2cf5985\
      a42d7c62e416001762aa176c826adc90fc54193bb9b0099501e59bad29073100\
      e01c9b7246411b032f7706d8c0651f85243a285250db1bb2b277a7d8ba1c415c\
      f085668958ae06d1196dd159e30283d49a9a877821923b476e1c0b74c1386502\
      ace63259be318506c1991b428260629b7fd410f0ea1cf8f363c8eab3a36936cb\
      e113b4c0a8b3a29d72719bcab10154a936aca2c9b9a0c5fc243dab461076c43b\
      d156818de7243462cbdb63af86254dee36cbd6427c6ee6c861eca69b52b22d17\
      13d319a90c3818b6f02cca051d43290a6ed4a63b184766b70815e29acd659eea\
      a71264238c2f486ccf2c35e8c19488bb557c402fa7c833ac659014203a68386b\
      9d2b3c603300cf96287e5a76c1a8bc1fb802dbb96dc9c12956c5b3f6806140f7\
      26abd0ba87f917ed1a9faedbac5cf05a8b5a465c1233fedbbd57a113ce0b3331\
      414e15da0ac6c71ce4970d5a059169ac980c1cb4f157a76d08202ec39dfc1b09\
      f24555d9fc27229e1d1949ad86aaa3564ac6b65d4e282617e7fc1bf03ea6081c\
      8f43f06c5c830426abd0609a7c6d2674069dcd52f63b101c0dbccd607cc88ec3\
      fa70717a2095a64d83358b8bf541cd7218f6570ce2a8e280e963f49c9f6d8446\
      3e44c9e468f84da8f9ece0bec085687a87c1c99e6d2c04d804a14fc2303a4a54\
      6123c8f812228d',
    / priv / -2: h'46ef43c31889ec1756061f3616c5da00f3d1e2ce4c66869d28b\
      f72db01a68a7a'
  }
```

Figure 17: HPKE-10 COSE_Key (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
a50107025820b453b5dfd9661a61fd09e46152c5d7daa9f5c04e3622e55e1ac6045a\
66ffc4c103183a20590681d4a518aacabdd20862c2816e4898cbd6a2a1661450ba31\
9fe9c5c9b524522684a1a4cc9018c76cbbe79325313a16765e51036d5b235fb11023\
cd0a98802bca07d31665d770ce46250aa4525e57121e681008b923f7f4c82598a91c\
85cbd649b8ff69c638843cd0f09bc6c70b37e8b228ab7d8a426dd4ab3de5a6bf3d2c\
119ee9b5e0c56e1c8c99bb9c004313cd4e3c3d4b7127234383c8368f6951b9cc7a88\
07e996f3723a59f254150444adf4478d3c16873b6c60b36495d8c731960ac408b0a2\
e7a6cddca6a08a01c5a79b5c8c8b9c7b00c9c28fdcd07259ac4c5eb12974930642f7\
83c1b5b5b1739f7c0ba54f3c3b6e878705d41c18837383bc6221772061eabde4a9aa\
6cda8a32464d162039c05a4e8e8cb591413db270b056c57e23f754ad67246ab83224\
d50e36844c382a31e1cbb3884514dd69012bda4e04a5755a3acbd2406a059532d838\
6c9892c6e908c92e783833a4b80310260b0a7fdb336314668c6cb642a0aa8fb7e146\
7bfb97c8056aa18799da301f5a042e6eb4409773557784730274 21e21a7880f53fb7\
d9b04bbb03d64777fb39b4b028aa45e76f3466a0e7d243140231b946b0f97accc95c\
7a7591b9c5f3a769413c8afb99eb888f43d6ac012ba0505549b6e4200fba4e365c34\
71442adbea9557e4134b7486fc081d9fe48386a7bc8b156ba902344d8985540aae46\
7883804c7af0d3388e6c8fbf0b8441e375d298808fdc3b8ce745f7c76eb6477a52c4\
06a4f7205dcb02457acdf6e48ba554022545331681b748172e504861ec33abea601c\
1b465a7b473d1397b6a9367a6d4537136299657b9bfb17198fba064aca7082b1b621\
377ec738ba69ec6eee0b9830c68fe1e9373c4863505c15e4782dccd4a0a7d48e4040\
0f95826cf260a9139b4db18aae27443709761aeaea9ee5229863c30ea66929b9a8ce\
9884046ef5239894318d24313d77033f46b4b9c75b1b493492c86aacf0145af4a82d\
28c057101d832c5ee6975720292b4a3b342ee1bb7da73481cb65c3d448babab7e841\
78122b6c3345a101eb9b92611dee084807f14899f40ac7b25a26c731d2d69801e851\
0f794dddd03c9be34d7762645f60c15e64322aa87526c95c6821cd61a728e6b951aa\
fa70474b7de3f9cd6e494ee68032db965c27689a022c0090f496a6d7cc4403353ff4\
cca13153bfa47ea8a01ec60aad29804ae7f6892a91a30ab8b8192930bf544f7970b7\
9ab38934027ff3f8cd975c958d555587d9434934063abb585a598703d8c601344add\
eb28fc33b938d591cad698fdac1bc4b27765e4adb4b644977263efd91dd4b8a00171\
662e24b97cdc62a8495c8ee81bdd6c7674d3c485595cd9d234e8d9b89e77c8114643\
c3391f0dc535f9d255d0f71409b01b3f2a2b684a95486270315164b796bd42aa945c\
a634de126c4daa84ba480cd2b6283e5109fd4baa469b6818564159d49cb76a4423b9\
ae399034962719a6e62ac788c60809234bfc6e6852a389e131035206c92a045f9113\
b911194ed35da7d8432b2250efac1572856a9678841de51349dc604c810633734b69\
cab11c55409a05117c0a23a36502c78b175dd2b8ed1b41b908817f967ed21c760c3a\
af8244ce2b3cb9b6b109f4c86f29cb58b1845642c5b3e65cb459302051e2cf5985a4\
2d7c62e416001762aa176c826adc90fc54193bb9b0099501e59bad29073100e01c9b\
7246411b032f7706d8c0651f85243a285250db1bb2b277a7d8ba1c415cf085668958\
ae06d1196dd159e30283d49a9a877821923b476e1c0b74c1386502ace63259be3185\
06c1991b428260629b7fd410f0ea1cf8f363c8eab3a36936cbe113b4c0a8b3a29d72\
719bcab10154a936aca2c9b9a0c5fc243dab461076c43bd156818de7243462cbdb63\
af86254dee36cbd6427c6ee6c861eca69b52b22d1713d319a90c3818b6f02cca051d\
43290a6ed4a63b184766b70815e29acd659eeaa71264238c2f486ccf2c35e8c19488\
bb557c402fa7c833ac659014203a68386b9d2b3c603300cf96287e5a76c1a8bc1fb8\
02dbb96dc9c12956c5b3f6806140f726abd0ba87f917ed1a9faedbac5cf05a8b5a46\
5c1233fedbbd57a113ce0b3331414e15da0ac6c71ce4970d5a059169ac980c1cb4f1\
```

```
57a76d08202ec39dfc1b09f24555d9fc27229e1d1949ad86aaa3564ac6b65d4e2826\
17e7fc1bf03ea6081c8f43f06c5c830426abd0609a7c6d2674069dcd52f63b101c0d\
bccd607cc88ec3fa70717a2095a64d83358b8bf541cd7218f6570ce2a8e280e963f4\
9c9f6d84463e44c9e468f84da8f9ece0bec085687a87c1c99e6d2c04d804a14fc230\
3a4a546123c8f812228d21582046ef43c31889ec1756061f3616c5da00f3d1e2ce4c\
66869d28bf72db01a68a7a
```

Figure 18: HPKE-10 COSE_Key (Hex-Encoded CBOR)

NOTE: '\' line wrapping per RFC 8792

```
/ COSE_Encrypt0 / 16([
  / protected / h'a101183a',
  / unprotected / {
    / kid / 4: h'b453b5dfd9661a61fd09e46152c5d7daa9f5c04e3622e55e1ac\
    6045a66ffc4c1',
    / ek / -4: h'67b7dda74b774aca23a9a6911c02921c0862f0233a6305a15d0\
    6b7e3c69fc3777df95ca24963cb1ff503cd68901de53c6ca17c09cdcc0d7618d\
    2bc91361330dec4aeef70efc366153363d7809e22721977a81158e46921aa83e\
    89770365974f3bbb5a9bf0190da69aeb745dd8f438c949a39414bd94b9464a35\
    5624d3bfe262ccbf1495b160aad391de27e771f3b1232d68a7e1c7a1f2b2cbda\
    9f99342e838acb9319a71c4f2421fa055653c10cb9ece4cc2a78c366e4400195\
    ffb9a55402e2416debb5ecb7e5f9a61f72162468c1b53506fcd50f71926a88f7\
    ba10b54cc74444501a90b4c0e5242043a1bb18c678752568a052a4387689f1e3\
    95c0b3aff128c5a8278baf8d201ae8b34350805185b48be05671a3c96be44bff\
    a039e78b95166dd3cb9042ea193156f742ad8b703dd34ccc1ff35a73205b3fbb\
    6f1e351b87d2802cd6326ae533038fe195db44e4945988fb7bbd29197b1228b2\
    ea25fdca68732b9d133a42dba50a37551f424241e7f22251cb1ed74428f890bd\
    1fc282485eb9173f6a44d209ee89d93439415dfce7b01702314e823d34fa62ff\
    eaf27d1743fcf3e901223709d7813700c37c3188c3ddc76da385be3d52425062\
    39306f19f52dd54c4f380111abbd34169dc0459381a5343cb7deec916bf3f0b3\
    f7e4c9eaa1a8b3434c84622c8eb5b3b29df4e5874a3cbee6ec581271e70a1150\
    fe61d2b906533d5aaba9a11d7585519e53f5c5bfe43918963b7e7df0b49331c2\
    7c54b44cbf4bfb6281fa6e7fdb5a85b11026ee06f2ba45eafbaf478839f658ce\
    2c9bbd735c04d5f60d1295faa4f24d65d59618fcf5659a4914bbad50ca96c661\
    0eb8b48106a449d9a970710db33bf1f7abd750778afc6da78fa1ed8c0d3470ec\
    25242320b7b8ab0547e06212dc3cfa80d86b0e700a81739a227fb8a93ad30626\
    3d40dcd5cd49aeb026c46c035d83710342b4f0367489d4c232c6b6a84d8e73fb\
    431551b5a5f8e113d81e3af95ea74a8179b893eb5a6a045065c8e9feb1150dda\
    174c0a1686585a11c9ff40260a42a1657ee9ef3139250a423be719e2683a7e10\
    59c7d1eb26afe08cd130f6d624d09a161e4fd109b45e3c043699af69ce65825d\
    442546189e5cccf1ac0ceef6045eb864de66e9316206cd90acc0d41311b78980\
    90969ba93ce43f0a46183f823eb19ba2c7161350fc918a4f55a5d8e4a4d1f04f\
    c21e478916ebdee4f29f681d92ac702542e3b0bae88a898c56a9d5625553081a\
    3dd62689af2e0e2bc7145e15032ff06e98bd23e29f3a438f838032ae317ccb18\
    7bf39afd8d7e40be882be499acf0d44b35baabb6369a2b4f21d6e0a87e572a9a\
    621d869a616d971827f7ef8a258af50e7e48c4d7c70ce16c1e9beb95a049e469\
    1ec2c51f0a5a9182baa299572618910c2079f7d05fa19284afb3a2afb584623d\
```

```
      2e7ebbec9c69777439ad82b41617124ec6d842e8eeaf849e79d976350f449ad4\
      924c7086fece4b9ed4d463e8c435f7b11fb278e1e442127d8721d0bae6959a14\
      81f9f6d6027259458333bd461fc7c32f95fac938e0f413d0a4076a41299d7849\
      04fb8591e8a644f188ebfa57187ddc1786f8eb2946b980a647960a9f9bb9fd97\
      029008c20aac50fa7b7c316d174fa535ddb1438f53ef9f5a57db7b02924b629b\
      2c1da86ac983a49cc45f00fe40c11d853cfdb4d56715e749caabc4dc1f41b5c6\
      03363b0beee804e42e561ac1420031a9a02d6c8e15bffee44ff21c80fcdfc83a\
      baf63d0ae444a2f22138252215a4b3b5dfbf72603c166fc0bf7be5ac66c69e8b\
      6e8b18950851c91dec76ab7def61ef8d0d3a486722cd88ed3a8925a31eeb53d6\
      ba267884bfcf5c034b73816a515c433981ae11a7a047d1912c7d20a727bb2b8b\
      08c6495555571968b830b87805c7a1bc9c387532f0e681b729a14e20488f80ab\
      048f9ef980852b29ffe36dacc3dae73ae21656df79f1a53ee16391bab665f3f3\
      7bacf0f804c8e9a38f5303b8766500341ac02324497ff2b2671b81b3ca5bf8ae\
      af871058903a72f80c2f7138a87dcff64ca5b39b1ed2b6e4b5e135db23505ff6\
      a0dcc0f408b5dd3afe7ca46ecba46686c816602d986b5ed16008063de1ad60a9\
      cfbde7326fa9b7b191115a47b3494410549c39616e0008deb32861f197dd02a0\
      b4108ec98cad2f2244a0a9a367ec75174f48e175469760bb6f23e45b2fa0673b\
      486bc930d2d31047b618b7f66c82f19514dcd07a6d732e14f62570b9384c33bb\
      29a0ee4d6bc3512aa625ecfea33e7d0228cee953d57ad3ecca0d601cdfcf2101\
      345d13a07c084833d042d987185689239d390c3970f535c9a35fac1482ecb344\
      bbf0f484cf4f771'
    },
    / ciphertext / h'e2d88c89966fb4430e7977a3fcdaa50f3ab9bdf429f4247b6\
      d32d176893f18665f8c14fc4ced6c60ced9d6d45144b0dab87e23f0f5d69d99b\
      74f5f1dcb732b0d18f676e436da558df3518828510844e432342ed0a95b2ed5d\
      b4664368f3769ea001191e27bf32b23bdb8fd63c34e7bc41ae41f7324186db80\
      7e6f79103cf28c8ec6120dec5dfc6b721e09589c3aab520932c5f14c789247de\
      e62aa26ab9552b2270730db829314d80ae20235050bb28dd54496bcbf5579a53\
      ff824f33595e92b4676f63da7a5ee6eb5a209b9842450dc7a12310141c9ded08\
      7b29e8b4f05629f931e8eaf8b88b11f0e4cc7579edfb131086b9c289eb087b1e\
      4bf7cf5615ddafd6d5d9829887a08d2b5784d4c0156b3775989fc32ae8e57934\
      8620f7318985f9b2c'
])
```

Figure 19: HPKE-10 COSE_Encrypt0 (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
d08344a101183aa2045820b453b5dfd9661a61fd09e46152c5d7daa9f5c04e3622e5\
5e1ac6045a66ffc4c12359068167b7dda74b774aca23a9a6911c02921c0862f0233a\
6305a15d06b7e3c69fc3777df95ca24963cb1ff503cd68901de53c6ca17c09cdcc0d\
7618d2bc91361330dec4aeef70efc366153363d7809e22721977a81158e46921aa83\
e89770365974f3bbb5a9bf0190da69aeb745dd8f438c949a39414bd94b9464a35562\
4d3bfe262ccbf1495b160aad391de27e771f3b1232d68a7e1c7a1f2b2cbda9f99342\
e838acb9319a71c4f2421fa055653c10cb9ece4cc2a78c366e4400195ffb9a55402e\
2416debb5ecb7e5f9a61f72162468c1b53506fcd50f71926a88f7ba10b54cc744445\
01a90b4c0e5242043a1bb18c678752568a052a4387689f1e395c0b3aff128c5a8278\
baf8d201ae8b34350805185b48be05671a3c96be44bffa039e78b95166dd3cb9042e\
```

```
   a193156f742ad8b703dd34ccc1ff35a73205b3fbb6f1e351b87d2802cd6326ae5330\
   38fe195db44e4945988fb7bbd29197b1228b2ea25fdca68732b9d133a42dba50a375\
   51f424241e7f22251cb1ed74428f890bd1fc282485eb9173f6a44d209ee89d934394\
   15dfce7b01702314e823d34fa62ffeaf27d1743fcf3e901223709d7813700c37c318\
   8c3ddc76da385be3d5242506239306f19f52dd54c4f380111abbd34169dc0459381a\
   5343cb7deec916bf3f0b3f7e4c9eaa1a8b3434c84622c8eb5b3b29df4e5874a3cbee\
   6ec581271e70a1150fe61d2b906533d5aaba9a11d7585519e53f5c5bfe43918963b7\
   e7df0b49331c27c54b44cbf4bfb6281fa6e7fdb5a85b11026ee06f2ba45eafbaf478\
   839f658ce2c9bbd735c04d5f60d1295faa4f24d65d59618fcf5659a4914bbad50ca9\
   6c6610eb8b48106a449d9a970710db33bf1f7abd750778afc6da78fa1ed8c0d3470e\
   c25242320b7b8ab0547e06212dc3cfa80d86b0e700a81739a227fb8a93ad306263d4\
   0dcd5cd49aeb026c46c035d83710342b4f0367489d4c232c6b6a84d8e73fb431551b\
   5a5f8e113d81e3af95ea74a8179b893eb5a6a045065c8e9feb1150dda174c0a16865\
   85a11c9ff40260a42a1657ee9ef3139250a423be719e2683a7e1059c7d1eb26afe08\
   cd130f6d624d09a161e4fd109b45e3c043699af69ce65825d442546189e5cccf1ac0\
   ceef6045eb864de66e9316206cd90acc0d41311b7898090969ba93ce43f0a46183f8\
   23eb19ba2c7161350fc918a4f55a5d8e4a4d1f04fc21e478916ebdee4f29f681d92a\
   c702542e3b0bae88a898c56a9d5625553081a3dd62689af2e0e2bc7145e15032ff06\
   e98bd23e29f3a438f838032ae317ccb187bf39afd8d7e40be882be499acf0d44b35b\
   aabb6369a2b4f21d6e0a87e572a9a621d869a616d971827f7ef8a258af50e7e48c4d\
   7c70ce16c1e9beb95a049e4691ec2c51f0a5a9182baa299572618910c2079f7d05fa\
   19284afb3a2afb584623d2e7ebbec9c69777439ad82b41617124ec6d842e8eeaf849\
   e79d976350f449ad4924c7086fece4b9ed4d463e8c435f7b11fb278e1e442127d872\
   1d0bae6959a1481f9f6d6027259458333bd461fc7c32f95fac938e0f413d0a4076a4\
   1299d784904fb8591e8a644f188ebfa57187ddc1786f8eb2946b980a647960a9f9bb\
   9fd97029008c20aac50fa7b7c316d174fa535ddb1438f53ef9f5a57db7b02924b629\
   b2c1da86ac983a49cc45f00fe40c11d853cfdb4d56715e749caabc4dc1f41b5c6033\
   63b0beee804e42e561ac1420031a9a02d6c8e15bffee44ff21c80fcdfc83abaf63d0\
   ae444a2f22138252215a4b3b5dfbf72603c166fc0bf7be5ac66c69e8b6e8b1895085\
   1c91dec76ab7def61ef8d0d3a486722cd88ed3a8925a31eeb53d6ba267884bfcf5c0\
   34b73816a515c433981ae11a7a047d1912c7d20a727bb2b8b08c6495555571968b83\
   0b87805c7a1bc9c387532f0e681b729a14e20488f80ab048f9ef980852b29ffe36da\
   cc3dae73ae21656df79f1a53ee16391bab665f3f37bacf0f804c8e9a38f5303b8766\
   500341ac02324497ff2b2671b81b3ca5bf8aeaf871058903a72f80c2f7138a87dcff\
   64ca5b39b1ed2b6e4b5e135db23505ff6a0dcc0f408b5dd3afe7ca46ecba46686c81\
   6602d986b5ed16008063de1ad60a9cfbde7326fa9b7b191115a47b3494410549c396\
   16e0008deb32861f197dd02a0b4108ec98cad2f2244a0a9a367ec75174f48e175469\
   760bb6f23e45b2fa0673b486bc930d2d31047b618b7f66c82f19514dcd07a6d732e1\
   4f62570b9384c33bb29a0ee4d6bc3512aa625ecfea33e7d0228cee953d57ad3ecca0\
   d601cdfcf2101345d13a07c084833d042d987185689239d390c3970f535c9a35fac1\
   482ecb344bbf0f484cf4f771590121e2d88c89966fb4430e7977a3fcdaa50f3ab9bd\
   f429f4247b6d32d176893f18665f8c14fc4ced6c60ced9d6d45144b0dab87e23f0f5\
   d69d99b74f5f1dcb732b0d18f676e436da558df3518828510844e432342ed0a95b2e\
   d5db4664368f3769ea001191e27bf32b23bdb8fd63c34e7bc41ae41f7324186db807\
   e6f79103cf28c8ec6120dec5dfc6b721e09589c3aab520932c5f14c789247dee62aa\
   26ab9552b2270730db829314d80ae20235050bb28dd54496bcbf5579a53ff824f335\
   95e92b4676f63da7a5ee6eb5a209b9842450dc7a12310141c9ded087b29e8b4f0562\
   9f931e8eaf8b88b11f0e4cc7579edfb131086b9c289eb087b1e4bf7cf5615ddafd6d\
```

```
5d9829887a08d2b5784d4c0156b3775989fc32ae8e579348620f7318985f9b2c
```

Figure 20: HPKE-10 COSE_Encrypt0 (Hex-Encoded CBOR)

A.6. HPKE-10-KE

NOTE: '\' line wrapping per RFC 8792

```
{
  / kty / 1: 7,
  / kid / 2: h'79051e8fc75f95a1ea2186f37ea0458a0870a0bc0ea8051422d2e\
    b3849505d9a',
  / alg / 3: 59 / HPKE-10-KE /,
  / pub / -1: h'f402ceb7d6c085770bea7caec0fcbe72accc80f6c00e12167be8\
    3720503a7c551e89d67f483ba7e736c84811358b960a4fd49328205856509466\
    5028f259ccb5b73bddb372dc336442f8a2e93a6d60d98f4d79b06ae379aac505\
    339a2eaa316dc018504c59154758b962e3b29ea842e1fa7967795c11eb031514\
    3187018994d83188d19690d2a479605510bc54e3250f1d4b77eba679ffc785c4\
    6c694402cac6b7cd6a6b94e737a8900c662c0b152999307c8212c5057a120434\
    242800a5f457a7581a1d693fe6106b0fa58a9706a00c558ef67a5fae116d1c73\
    429b953f15d4cd85e6a6a6985fd0b26974e2cbd811995ada989fbc43b9e83110\
    9081896a01a04978c2931ccf892a2037215b34c0bda08bb57bc1d0539894aa86\
    63f328b033087d84697e4c654dd283c4cc560bf6197534025bd68666abbe82ac\
    394429b0933514c4aacc5bc95559b4571ec19ad564263132654cb18646704fe7\
    86308acbc9a77b51bf3cb7cbe2570da740c5e2b9bbd50920c64bbe0980b3d702\
    df1b7bf586a165ba3c173211090229509b21eee0bb55a1bb7f82b38036521086\
    88a8c44a63bb9352f6ac9a265bb6804c53f18faf06745e614d8b74796ee6b489\
    e06ed1159db9c41aaab95000f6157d192e14790fb0c99c153a15990b6ae18961\
    13786c4a9755215b3e3c419e29c722043b49108909cf1b76b6c0cf7da81bec39\
    50426a8cb1383977d2bed85605527cba9f7b172f7c1d7dfa0cda41bf5cbc26a4\
    f111cb13a2daeabfad861acce1c158fc4274f83e6c1916cb8b8b3aaa7cd6f487\
    c7447e2696af00c11fb347732c0158a3b6bc044a54726368e1c72256ca0e57b9\
    5492a36c9215c2b527a848ac3ccc3c42a34c9ed5c30636ea2066728d08f84651\
    2a3d8a0780706aa41e87cc4b70784897271d830c0f4409ede0c4fc787470cb13\
    e786ae7aeb89f0f6ae2c7b93e26a241b5b367b164fdee6971b50663ccb69011c\
    8225335ac7641dd4e56aab1ba4ba6995df725af29742db350b53f5c04f366305\
    d89067a7b7477bcb420b47e6fa6f9f3047bdb44701b2897504bfb3356285b794\
    c6011d192c2d7201cd40c31a99e74edea98762c46a73d94fa3e5b7e3f0948720\
    c7aba2bc9f492073114123e46633f884f112327ebba533234f5dd9c9d5d26872\
    29637125328e9648460139042792eec1a9d5927a73cc3b2618920c4593976394\
    6fd1ac6d734ba3a3ccac805692097f039129322a6ac202d03c74c24e6209174b\
    ac1dc62732d1024fb53574f4152a04af36eb1a5e5754e6688046bbce9f4a2c06\
    793fbb33c16b20a2f0353b721457327a0c4909613a678d2304ba77d44ceb81c8\
    d2801cc00005918c95fa932fa91bb3e00c7e116947b9bac60ef6cc593c0c3696\
    4e873361c0322c95a8203a8a87a9931e828ccee2a92372e78b0cf0416536a68d\
    d79285b9107ef712462c7f7dda61bfab1d9d7c8ded49abf64c40ff774b4b89b4\
    005b8f0400a7fd2a2173e80bc114872ee7a8defbadf5551b96d3574f24121c1c\
    c2fd381856d0813cb296952bc684dc3979788045823ae7d97639b783fbc25016\
```

```
      3c0dd5f11c7ac0637d758928e849a186c2d9d50ee9f2caa25c6def6514e5959c\
      770623abd5b55843bccfa0b5b3f42a6833ab282b6e2d108ed3795c5cb2242879\
      3001ab294d5c379e107cffa927d617827e369f03595db36771fb8cc179c86cab\
      613b97a1a7a1b867854a74f87417b867934a23b869a9a6d2da2edfe8a75e9373\
      b97b11e8260f1b6ab5458025816a0b2403228e04cc44dc6dbc648f835779daac\
      435c1408a4939349c41fddf38d9c705be466474e6890f815bdcf284f33929412\
      8674ee7c7f6de121cebb4c5fc5593897b9b3071d6a5302f0c7a3cce62f2e187b\
      8dd15891e21b6e09313013191241c7b5f8a31600b44fba822d391002d5c0eb02\
      992e08c7c31b160e3b130eeb978250c5c7186ffdd24d5172c3e9741ee2f903c6\
      7108df1141cd59a867a56c466c0a759568dd6ca50528583b587c601693f22011\
      8fcc7a35e9083ec68515bb3f28e84b47fb6d03b1138860ab9ff53f1385058c2a\
      b219c64f105bcf73b60d732322eb4ba3c08875a564042031bc239aac67030f45\
      763531763f8a9c8e566136b3151b856183ac783197b466d2cc0606663c25d047\
      fdd67b22a4149a97dc166b33b647c8a15dfafa56bc526aa348de7ac5a72f9562\
      ba5b08fb453704e6392cb5463fac1c17d64054f082139c0f22ad3dafb11d36f3\
      04b696c54521572694696821b094e8e6b3ce6dccba3a81a1b6c730aa979eff4e\
      a78dfba423658a5c8db405d2ffa64470b75421edf04d3c4077989dc1a3e264ac\
      bda372b28e2599',
    / priv / -2: h'b920cf667c309cba49d7c9700061e3ef97be7c6a215bbcce5a1\
      006fbb0c62e2b'
  }
```

Figure 21: HPKE-10-KE COSE_Key (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
a5010702582079051e8fc75f95a1ea2186f37ea0458a0870a0bc0ea8051422d2eb38\
49505d9a03183b20590681f402ceb7d6c085770bea7caec0fcbe72accc80f6c00e12\
167be83720503a7c551e89d67f483ba7e736c84811358b960a4fd493282058565094\
665028f259ccb5b73bddb372dc336442f8a2e93a6d60d98f4d79b06ae379aac50533\
9a2eaa316dc018504c59154758b962e3b29ea842e1fa7967795c11eb031514318701\
8994d83188d19690d2a479605510bc54e3250f1d4b77eba679ffc785c46c694402ca\
c6b7cd6a6b94e737a8900c662c0b152999307c8212c5057a120434242800a5f457a7\
581a1d693fe6106b0fa58a9706a00c558ef67a5fae116d1c73429b953f15d4cd85e6\
a6a6985fd0b26974e2cbd811995ada989fbc43b9e831109081896a01a04978c2931c\
cf892a2037215b34c0bda08bb57bc1d0539894aa8663f328b033087d84697e4c654d\
d283c4cc560bf6197534025bd68666abbe82ac394429b0933514c4aacc5bc95559b4\
571ec19ad564263132654cb18646704fe786308acbc9a77b51bf3cb7cbe2570da740\
c5e2b9bbd50920c64bbe0980b3d702df1b7bf586a165ba3c173211090229509b21ee\
e0bb55a1bb7f82b3803652108688a8c44a63bb9352f6ac9a265bb6804c53f18faf06\
745e614d8b74796ee6b489e06ed1159db9c41aaab95000f6157d192e14790fb0c99c\
153a15990b6ae1896113786c4a9755215b3e3c419e29c722043b49108909cf1b76b6\
c0cf7da81bec3950426a8cb1383977d2bed85605527cba9f7b172f7c1d7dfa0cda41\
bf5cbc26a4f111cb13a2daeabfad861acce1c158fc4274f83e6c1916cb8b8b3aaa7c\
d6f487c7447e2696af00c11fb347732c0158a3b6bc044a54726368e1c72256ca0e57\
b95492a36c9215c2b527a848ac3ccc3c42a34c9ed5c30636ea2066728d08f846512a\
3d8a0780706aa41e87cc4b7078497271d830c0f4409ede0c4fc787470cb13e786ae\
7aeb89f0f6ae2c7b93e26a241b5b367b164fdee6971b50663ccb69011c8225335ac7\
```

```
641dd4e56aab1ba4ba6995df725af29742db350b53f5c04f366305d89067a7b7477b\
cb420b47e6fa6f9f3047bdb44701b2897504bfb3356285b794c6011d192c2d7201cd\
40c31a99e74edea98762c46a73d94fa3e5b7e3f0948720c7aba2bc9f492073114123\
e46633f884f112327ebba533234f5dd9c9d5d2687229637125328e96484601390427\
92eec1a9d5927a73cc3b2618920c45939763946fd1ac6d734ba3a3ccac805692097f\
039129322a6ac202d03c74c24e6209174bac1dc62732d1024fb53574f4152a04af36\
eb1a5e5754e6688046bbce9f4a2c06793fbb33c16b20a2f0353b721457327a0c4909\
613a678d2304ba77d44ceb81c8d2801cc00005918c95fa932fa91bb3e00c7e116947\
b9bac60ef6cc593c0c36964e873361c0322c95a8203a8a87a9931e828ccee2a92372\
e78b0cf0416536a68dd79285b9107ef712462c7f7dda61bfab1d9d7c8ded49abf64c\
40ff774b4b89b4005b8f0400a7fd2a2173e80bc114872ee7a8defbadf5551b96d357\
4f24121c1cc2fd381856d0813cb296952bc684dc3979788045823ae7d97639b783fb\
c250163c0dd5f11c7ac0637d758928e849a186c2d9d50ee9f2caa25c6def6514e595\
9c770623abd5b55843bccfa0b5b3f42a6833ab282b6e2d108ed3795c5cb224287930\
01ab294d5c379e107cffa927d617827e369f03595db36771fb8cc179c86cab613b97\
a1a7a1b867854a74f87417b867934a23b869a9a6d2da2edfe8a75e9373b97b11e826\
0f1b6ab5458025816a0b2403228e04cc44dc6dbc648f835779daac435c1408a49393\
49c41fddf38d9c705be466474e6890f815bdcf284f339294128674ee7c7f6de121ce\
bb4c5fc5593897b9b3071d6a5302f0c7a3cce62f2e187b8dd15891e21b6e09313013\
191241c7b5f8a31600b44fba822d391002d5c0eb02992e08c7c31b160e3b130eeb97\
8250c5c7186ffdd24d5172c3e9741ee2f903c67108df1141cd59a867a56c466c0a75\
9568dd6ca50528583b587c601693f220118fcc7a35e9083ec68515bb3f28e84b47fb\
6d03b1138860ab9ff53f1385058c2ab219c64f105bcf73b60d732322eb4ba3c08875\
a564042031bc239aac67030f45763531763f8a9c8e566136b3151b856183ac783197\
b466d2cc0606663c25d047fdd67b22a4149a97dc166b33b647c8a15dfafa56bc526a\
a348de7ac5a72f9562ba5b08fb453704e6392cb5463fac1c17d64054f082139c0f22\
ad3dafb11d36f304b696c54521572694696821b094e8e6b3ce6dccba3a81a1b6c730\
aa979eff4ea78dfba423658a5c8db405d2ffa64470b75421edf04d3c4077989dc1a3\
e264acbda372b28e2599215820b920cf667c309cba49d7c9700061e3ef97be7c6a21\
5bbcce5a1006fbb0c62e2b
```

Figure 22: HPKE-10-KE COSE_Key (Hex-Encoded CBOR)

NOTE: '\' line wrapping per RFC 8792

```
/ COSE_Encrypt / 96([
  / protected / h'a10103',
  / unprotected / {
    / iv / 5: h'0c747a20a846a6813de21f17'
  },
  / ciphertext / h'cf17007911e2b25fb5cc1fcfb62fb8424a6d4ea8a3cff3474\
    dc84a43f847527cf659eb9ac9c563aa98d4447e26d303940e76cf900f19857ee\
    c2da96c64a2fd0edd38036f51d076b09aff810c9abfbb4a2e818a064da3154da\
    aa6bdb2240bd9dc1ab1faee542ea875f9e5c58f04f9b7132c70b20b9b9b5c582\
    78ca59620ed693de6b2dc675766216b317e5ac82b192350ef1426cd0e8bb18b2\
    9fc3b4314e49ad3ad0e9ee9775937128232840 68d82af2b4347fa5eb87d3cadd\
    92f40f9ef03d1c59678487b2716a756aecb45f1b39ebf8ae4204a1f784a3a351\
    87c334db817752083706d1c44c6a01f46ed74a34c8523d0c75287c91b57df3cd\
```

```
      76b26c98145feccd6ccaf640857cc8fee4726d834ccac3ecd45b3c154e537571\
      3e327aaf675e5d579',
    / recipients / [
      [
        / protected / h'a201183b04582079051e8fc75f95a1ea2186f37ea0458a\
      0870a0bc0ea8051422d2eb3849505d9a',
        / unprotected / {
          / ek / -4: h'f2a9112fc88e0ca3a5ae9575603332317b01fb2509b0544\
      0b1cbdd6fed8c246a8d27f979954acdf0f3ecf6e499cef02e535e0a628f0d169\
      b3d5f14ac52ae309f00f89294096d2602bfe42a4741be240906ce525057c45d4\
      e8b2d6069b0c37920ae1785b93526226e43bb7390d3860a5c1d08b25567054e1\
      d53d8568117cddcd12e13bd923dd7976f619d17d6c6a1e29fce3143b83bb2a03\
      2e9242b3d6ec270fd1131cd3ace3741a0d4ae62f43823b02faf8af2ca59426a4\
      88084d5d741aa219ddf16d6430888e438759580127b6cef085cdf7598ed0243e\
      84de61457903ed8d75f9a74f9a425bcbc2d147650631b3930b1a63c0c43c75c2\
      a8f95977d8620c30e01ae3c28b79ad691425cad1716c3e17300d79e9e5d4a7c6\
      c5f3243233edc9cb1ea43a53a18c29dc5176f7856e45d7cb2c1ca2cab4b94b0f\
      ce81bfbbbd45177bbfdc028d39a684388291bf23e4acfdc6d61fa1f4a6ece1ad\
      5afc23675e4bdd8ad1f164b58f84cec337bfeafb1228c3dbbb82fdc54e38a4a4\
      027ea036f4a58eda43388678c19b64bfb7c46f4e6224000a8f695122dd120a5a\
      cd8773c2516bf996f6947992513c022e0329ff2973af756422c25846ebb3adda\
      90a7bbbff8267dc91d9d378af8c9aeb07571c4b465c6eafdf830d3aa7f26e593\
      ca2423f373b1daf9e11352ba8b7f895630c07a378b5a646a5922f5f5ebb096a8\
      27ca9714200bc5a2a2101526985fa920d4e6be44a3a6126d328d00220a529363\
      e62541a3195dfc9ee2607978e99c61dd5d10ab44da385063998d75199c989ebf\
      b986c83249ce086119fceb14b85c79ba937b0f6ac234b7789c63a6509527b680\
      dde6d785f019aad4f7618b0e7d6ac3202358aa386e1d1c7a669089ea47e82b9a\
      99463202a9d2ddbe60d81d90256a0429cf06a1b79d56a2f8c4acd298ed8d897c\
      07838b66a95ccb06384d587cc79b7404052cb0690a0258ec6889694e383794fe\
      869aa937ebe2b1a998f224c08be34300a563195d072be8f9d9015e3908debc9f\
      5dec0fd4fa5d9d1e365601940ac55973e2ad106ab23064d0c0a24f8976c302cf\
      55dd6a7444dc9eee744c36833e6b9adbff1f2d97b69970e4ce3f234dbbad8679\
      50c17a70ef054c47ae3e75d1690a3b5b39ef7cc6420f4f2c86c78c05e1627088\
      3a0d82411b5b6c385a05a757848e351b4b9f0cf58a014f6ec567d7c97bdbda49\
      609ffbbf9e61ea65e2d3c1f82c584153c43c8c9c7f6ae3850ebf6044a521ee1e\
      93c634cefa0f426158ddb6a5117cb9a2b1f2d6dd5bd6790d3a0e36b8bde827f5\
      723664b51fe0b75c3c0019066b1e32c86472fdad663ad7359548ab58e99650f1\
      37b32770892245f216809a7b7882c7c370f7bd56542bd43b30d920989cea5b6d\
      ce62bb44d18b2913267bf1cab194de802e76466bc241fa685db01330d2911bce\
      1218a3e5da7fc7df392a22c579c0d59c1e12cbf4f9da7c5a25b595b17c9f89a3\
      9563b710de8710888ecad66f694766e21ae7b99353c3976fa69cb579e8845b88\
      92a8971f1d87887820beebcc07555643fec0405ab8e5e9c6bebf78b3a00fad9b\
      97c43cfca49103d5d9b2695405a5a239198a78669fc26ef5123c64015c7e73f2\
      3eae5ed252ff6ad4f477f6f61f2e8316ca9282f08a02135ca7ea3f1fc0f45a90\
      d804c42ecfd54b69b5b298db29d6a73113fb1eec918b27869dba90524029a0aa\
      d1cccb670c975217b3d201e68a958b2797fc0994460ba139b7fe3bedd64bd480\
      163d09e6bc4cdba189fce14965697807f376e12d292c4d6bdc68ad79ad20f887\
      d852879dc2fd3c04e076c6507bb2979ef241ac59466a0f95ade0d7196968b911\
```

```
      b4eb4af35c5385a962469c584f149664fbd3024be5a372c5caa0b797806d9ea0\
      a2d0cc7fe7cef02c28eb3496f4fda62797424412bfa618b9ae0381548676c46a\
      46a396d30271f16d6ff1363f3ef6c65d8382cd165473b290da2b07c4b9161069\
      38bcf7868b67795adba13739e1638cf9bb6bc70fdc85998c96ac8bd641744593\
      a224ebf4a810d28875e57fce6e78830f6e382b00cf214993b18359e4538c5290\
      dbeac69e696e280412372c2f5a4c42f5b0ca2b717edcab6b8308b92b07bf81a1\
      52035dbead0b6a1918106a2136284acad6ef314ce861fbc779928a6bf563bd50\
      5962738924778b9b07722e7bef8be2c4562348fabee0b44a2e5c292faf1d125e\
      42942f155d0e2ccb604304c74c681234a55ad8f30ea281012b5912054007f492\
      253384fe74892d5ff2d6f9f417d950ea9c738c1ef3ed322b7cb8cf89710e53fb\
      e5a7a3fe13cbb5b61735da4132ee3d411b9cc55bdae719a7df5face00f85ffe0\
      3ca1b2f4bcee85e9baa'
        },
        / ciphertext / h'22d73ba82dc4d024fe6b933349ac0538531495e3cbf9b\
      45e1712d3c170a97f9d33fb2e5eb3a4ee625e8caf2be9a64ca2'
      ]
    ]
  ])
```

Figure 23: HPKE-10-KE COSE_Encrypt (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
d8608443a10103a1054c0c747a20a846a6813de21f17590121cf17007911e2b25fb5\
cc1fcfb62fb8424a6d4ea8a3cff3474dc84a43f847527cf659eb9ac9c563aa98d444\
7e26d303940e76cf900f19857eec2da96c64a2fd0edd38036f51d076b09aff810c9a\
bfbb4a2e818a064da3154daaa6bdb2240bd9dc1ab1faee542ea875f9e5c58f04f9b7\
132c70b20b9b9b5c58278ca59620ed693de6b2dc675766216b317e5ac82b192350ef\
1426cd0e8bb18b29fc3b4314e49ad3ad0e9ee977593712823284068d82af2b4347fa\
5eb87d3cadd92f40f9ef03d1c59678487b2716a756aecb45f1b39ebf8ae4204a1f78\
4a3a35187c334db817752083706d1c44c6a01f46ed74a34c8523d0c75287c91b57df\
3cd76b26c98145feccd6ccaf640857cc8fee4726d834ccac3ecd45b3c154e5375713\
e327aaf675e5d57981835827a201183b04582079051e8fc75f95a1ea2186f37ea045\
8a0870a0bc0ea8051422d2eb3849505d9aa123590681f2a9112fc88e0ca3a5ae9575\
603332317b01fb2509b05440b1cbdd6fed8c246a8d27f979954acdf0f3ecf6e499ce\
f02e535e0a628f0d169b3d5f14ac52ae309f00f89294096d2602bfe42a4741be2409\
06ce525057c45d4e8b2d6069b0c37920ae1785b93526226e43bb7390d3860a5c1d08\
b25567054e1d53d8568117cddcd12e13bd923dd7976f619d17d6c6a1e29fce3143b8\
3bb2a032e9242b3d6ec270fd1131cd3ace3741a0d4ae62f43823b02faf8af2ca5942\
6a488084d5d741aa219ddf16d6430888e43875958012 7b6cef085cdf7598ed0243e8\
4de61457903ed8d75f9a74f9a425bcbc2d147650631b3930b1a63c0c43c75c2a8f95\
977d8620c30e01ae3c28b79ad691425cad1716c3e17300d79e9e5d4a7c6c5f324323\
3edc9cb1ea43a53a18c29dc5176f7856e45d7cb2c1ca2cab4b94b0fce81bfbbbd451\
77bbfdc028d39a684388291bf23e4acfdc6d61fa1f4a6ece1ad5afc23675e4bdd8ad\
1f164b58f84cec337bfeafb1228c3dbbb82fdc54e38a4a4027ea036f4a58eda43388\
678c19b64bfb7c46f4e6224000a8f695122dd120a5acd8773c2516bf996f69479925\
13c022e0329ff2973af756422c25846ebb3adda90a7bbbff8267dc91d9d378af8c9a\
eb07571c4b465c6eafdf830d3aa7f26e593ca2423f373b1daf9e11352ba8b7f89563\
```

```
   0c07a378b5a646a5922f5f5ebb096a827ca9714200bc5a2a2101526985fa920d4e6b\
   e44a3a6126d328d00220a529363e62541a3195dfc9ee2607978e99c61dd5d10ab44d\
   a385063998d75199c989ebfb986c83249ce086119fceb14b85c79ba937b0f6ac234b\
   7789c63a6509527b680dde6d785f019aad4f7618b0e7d6ac3202358aa386e1d1c7a6\
   69089ea47e82b9a99463202a9d2ddbe60d81d90256a0429cf06a1b79d56a2f8c4acd\
   298ed8d897c07838b66a95ccb06384d587cc79b7404052cb0690a0258ec6889694e3\
   83794fe869aa937ebe2b1a998f224c08be34300a563195d072be8f9d9015e3908deb\
   c9f5dec0fd4fa5d9d1e365601940ac55973e2ad106ab23064d0c0a24f8976c302cf5\
   5dd6a7444dc9eee744c36833e6b9adbff1f2d97b69970e4ce3f234dbbad867950c17\
   a70ef054c47ae3e75d1690a3b5b39ef7cc6420f4f2c86c78c05e16270883a0d82411\
   b5b6c385a05a757848e351b4b9f0cf58a014f6ec567d7c97bdbda49609ffbbf9e61e\
   a65e2d3c1f82c584153c43c8c9c7f6ae3850ebf6044a521ee1e93c634cefa0f42615\
   8ddb6a5117cb9a2b1f2d6dd5bd6790d3a0e36b8bde827f5723664b51fe0b75c3c001\
   9066b1e32c86472fdad663ad7359548ab58e99650f137b32770892245f216809a7b7\
   882c7c370f7bd56542bd43b30d920989cea5b6dce62bb44d18b2913267bf1cab194d\
   e802e76466bc241fa685db01330d2911bce1218a3e5da7fc7df392a22c579c0d59c1\
   e12cbf4f9da7c5a25b595b17c9f89a39563b710de8710888ecad66f694766e21ae7b\
   99353c3976fa69cb579e8845b8892a8971f1d87887820beebcc07555643fec0405ab\
   8e5e9c6bebf78b3a00fad9b97c43cfca49103d5d9b2695405a5a239198a78669fc26\
   ef5123c64015c7e73f23eae5ed252ff6ad4f477f6f61f2e8316ca9282f08a02135ca\
   7ea3f1fc0f45a90d804c42ecfd54b69b5b298db29d6a73113fb1eec918b27869dba9\
   0524029a0aad1cccb670c975217b3d201e68a958b2797fc0994460ba139b7fe3bedd\
   64bd480163d09e6bc4cdba189fce14965697807f376e12d292c4d6bdc68ad79ad20f\
   887d852879dc2fd3c04e076c6507bb2979ef241ac59466a0f95ade0d7196968b911b\
   4eb4af35c5385a962469c584f149664fbd3024be5a372c5caa0b797806d9ea0a2d0c\
   c7fe7cef02c28eb3496f4fda62797424412bfa618b9ae0381548676c46a46a396d30\
   271f16d6ff1363f3ef6c65d8382cd165473b290da2b07c4b916106938bcf7868b677\
   95adba13739e1638cf9bb6bc70fdc85998c96ac8bd641744593a224ebf4a810d2887\
   5e57fce6e78830f6e382b00cf214993b18359e4538c5290dbeac69e696e280412372\
   c2f5a4c42f5b0ca2b717edcab6b8308b92b07bf81a152035dbead0b6a1918106a213\
   6284acad6ef314ce861fbc779928a6bf563bd505962738924778b9b07722e7bef8be\
   2c4562348fabee0b44a2e5c292faf1d125e42942f155d0e2ccb604304c74c681234a\
   55ad8f30ea281012b5912054007f492253384fe74892d5ff2d6f9f417d950ea9c738\
   c1ef3ed322b7cb8cf89710e53fbe5a7a3fe13cbb5b61735da4132ee3d411b9cc55bd\
   ae719a7df5face00f85ffe03ca1b2f4bcee85e9baa583022d73ba82dc4d024fe6b93\
   3349ac0538531495e3cbf9b45e1712d3c170a97f9d33fb2e5eb3a4ee625e8caf2be9\
   a64ca2
```

Figure 24: HPKE-10-KE COSE_Encrypt (Hex-Encoded CBOR)

A.7. HPKE-11

```
NOTE: '\' line wrapping per RFC 8792

{
  / kty / 1: 7,
  / kid / 2: h'400faa06149080d620fa067cabef42e03b05a7705da72188cd273\
    2e034e493dc',
  / alg / 3: 60 / HPKE-11 /,
  / pub / -1: h'fc609d52449d94b11ce376a4c3a961938c271278b3b455cfc150\
    25fce33af0c51db9b7cb9cba8a87dc141609bf7e9861dad8c7c01827378b39d2\
    69a22b6616bce298309a13a357a7cff45ab281437c8bbcc8848ab1441c17171f\
    883146a3956ee5d48309e752b186094a42b7989b86fbfcb04ea733c63325b299\
    290b379c9ec3780106510d8aa638102a705348509249b1babdc867a221c168d1\
    d9ae132b1cc4c796df11ab689ac996c5830feb1c2d43c296018711601a92715a\
    13f998e5e78e75e55b68f71f07406b1b0c0c8607a4f5ea4bd3d58d156c783b74\
    ac9201760ce589bee23d08e7c067403d7ac55d5c360227106af4b49739cb4080\
    f31ffd695015f5c59b70bc297c80ac080953e3aa57f13353486d34580bcebc56\
    b3582664b21efd2375dd69aaade42948577ae780c393b4c07ae84872ec0d3e9b\
    6b59507ec6f558a4e9108e4c1206873c255b234ae2460dc79103b7a27de46807\
    b517d05762f7e7bad01bc07554cfa9b0cd42904c1ebba8b0930e8147c470b598\
    55eb0d27e48e6939a165b3bc84c9adbddb9d1c846e2e5469ebd85dfc70adc829\
    8e931a132dd532ce237cedba33d8a86f6da769103c9199f8c968a60004c1732a\
    d953aff9120105636a18bac04cbb4346617d7b77f87592818a7db0aa980fc07f\
    34a9951c8c500ed88b503954f8fc1b049900c3173db00b5f10e05e28b3258fb8\
    95fa98ba47157a14ab40074545f4a10c7742c3ee5a4fed53945c24cc6c84b3ae\
    172a23839d3975a4dcc8cd9d1a2f7dd54235e779e3bc093a33073947bc680a0e\
    96cc326c21aae8973b26fb25a2d8bd6bba7df014c44f5cad01782617b1aedb43\
    354ba99a433c9b106a0ff5d99d650b4ec21c84d1e0a32e39b67ae4a52269936e\
    129f416962442447bfd77264c20a7f891f0773a4609c0662d37fdcd22d899b5c\
    aa9b962141c7299813cae683a983a11522b37a39a35f05c6cd3b9b40f420c6d6\
    015792c9fdd1c0e107479e94bdf98c61346291e7d93abf9a033f20c7246377fd\
    3235d863c791dc76cf3276197a949432a3ee02130bca8b3a4c58ec2146b756b4\
    b903037ae8b0031fde14458c8de3cba81a178f4589e0d5dd2f74834b85ff01bc\
    e4a78e90a712',
  / priv / -2: h'ca322edfb263988f8c6e07c81206da527199e2e15701563fb65\
    40e4bade3867b7ee9716b72649d2029df4c750bcf64a91bbf3cfc79892b2ba99\
    cffa2acddda5b'
}
```

Figure 25: HPKE-11 COSE_Key (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
a50107025820400faa06149080d620fa067cabef42e03b05a7705da72188cd2732e0\
34e493dc03183c20590320fc609d52449d94b11ce376a4c3a961938c271278b3b455\
cfc15025fce33af0c51db9b7cb9cba8a87dc141609bf7e9861dad8c7c01827378b39\
d269a22b6616bce298309a13a357a7cff45ab281437c8bbcc8848ab1441c17171f88\
3146a3956ee5d48309e752b186094a42b7989b86fbfcb04ea733c63325b299290b37\
9c9ec3780106510d8aa638102a705348509249b1babdc867a221c168d1d9ae132b1c\
c4c796df11ab689ac996c5830feb1c2d43c296018711601a92715a13f998e5e78e75\
e55b68f71f07406b1b0c0c8607a4f5ea4bd3d58d156c783b74ac9201760ce589bee2\
3d08e7c067403d7ac55d5c360227106af4b49739cb4080f31ffd695015f5c59b70bc\
297c80ac080953e3aa57f13353486d34580bcebc56b3582664b21efd2375dd69aaad\
e42948577ae780c393b4c07ae84872ec0d3e9b6b59507ec6f558a4e9108e4c120687\
3c255b234ae2460dc79103b7a27de46807b517d05762f7e7bad01bc07554cfa9b0cd\
42904c1ebba8b0930e8147c470b59855eb0d27e48e6939a165b3bc84c9adbddb9d1c\
846e2e5469ebd85dfc70adc8298e931a132dd532ce237cedba33d8a86f6da769103c\
9199f8c968a60004c1732ad953aff9120105636a18bac04cbb4346617d7b77f87592\
818a7db0aa980fc07f34a9951c8c500ed88b503954f8fc1b049900c3173db00b5f10\
e05e28b3258fb895fa98ba47157a14ab40074545f4a10c7742c3ee5a4fed53945c24\
cc6c84b3ae172a23839d3975a4dcc8cd9d1a2f7dd54235e779e3bc093a33073947bc\
680a0e96cc326c21aae8973b26fb25a2d8bd6bba7df014c44f5cad01782617b1aedb\
43354ba99a433c9b106a0ff5d99d650b4ec21c84d1e0a32e39b67ae4a52269936e12\
9f416962442447bfd77264c20a7f891f0773a4609c0662d37fdcd22d899b5caa9b96\
2141c7299813cae683a983a11522b37a39a35f05c6cd3b9b40f420c6d6015792c9fd\
d1c0e107479e94bdf98c61346291e7d93abf9a033f20c7246377fd3235d863c791dc\
76cf3276197a949432a3ee02130bca8b3a4c58ec2146b756b4b903037ae8b0031fde\
14458c8de3cba81a178f4589e0d5dd2f74834b85ff01bce4a78e90a712215840ca32\
2edfb263988f8c6e07c81206da527199e2e15701563fb6540e4bade3867b7ee9716b\
72649d2029df4c750bcf64a91bbf3cfc79892b2ba99cffa2acddda5b
```

Figure 26: HPKE-11 COSE_Key (Hex-Encoded CBOR)

```
NOTE: '\' line wrapping per RFC 8792

/ COSE_Encrypt0 / 16([
  / protected / h'a101183c',
  / unprotected / {
    / kid / 4: h'400faa06149080d620fa067cabef42e03b05a7705da72188cd2\
    732e034e493dc',
    / ek / -4: h'8e6c3c2040aadc5e88394e9f8e64459062d0ae76c941e7e4a20\
    158310056e59cacd8a62ba1569fe2e9b4495c61201afac15702398412e4e92c9\
    dfb098ef00ea417a67235b9b4582c83efb1fe47a8d77143d322618aab4960ca6\
    ff3bc6e0b0a3a891620f21eb9f877253ae8768d5beb72683ee9d54c375e06a6e\
    460fe963f47aa7950fb246b3432cc75e2b86421363a324fd2baddbbdefa71de7\
    f304a6c1aad4e4e0bac4e62daffa1fa05605065d4bdcfab842b2777a35f69eac\
    c452037b0efb4c6d7f1522b31e19a5f8d06c10ba42803ab58b4c6106d5c98f88\
    872256fce8d1e7858b9020ffa8243a617077fc51f90dc939ff42ce3cccd62a64\
    ad3e45e4d2cadf1353922c73fa503369ea34b9cbbb5b20b2c69b88a5f7fa07c4\
    1c820a1fc0cfc8b702f67407bb1e5c8beecce96b5c925c564cbaebbf874cc60b\
    65ae469e9a28c859220ed3732933891963566a4d4ff744f0716be4fb7b40015d\
    00e138b552500f804a68393086d259318e9dbc2cc17ec3d4d32b3890e31cca17\
    eb6cca9f36d6cfb7274fc8cd4d8dcdd0b20fa4e609a5e17a7c60293c308bb00c\
    5abc63fee3f811bac44a39b6175854bf7b923120edd2ab52d3052a373f1762e7\
    cc0fee18f550a30667a2054fddb4d498a96407b282671d4e650189fe7544a232\
    eb9bcab0d28dda0e523fad70d5bbad428de286e1c7e4f774a125ba577daa0ae1\
    29cd17a40746e484f88c1debdd2101d4cd6becf08cd0a2574aec253045dd4e0e\
    2e21b7c3da70b07712725299a48db218189f7daae5250c22cde5237e64efe366\
    ddedd519098de1ccad4a55a1d0a5fd6760b16839d3bb887b3eedd3459c162779\
    129cf62941dc04fae9ae494ded2cad4f082be84bbd362e66896bb5d970c8f4cf\
    0875a160cc5b612189d8ffa64b0ffd93efdf4d21ef996908a764a4ec8c00a3ce\
    90adb38e9c2c4aacbfb2957f7a8207db1b2a586ea2c8938982549e744e56086e\
    f2053233c540f559f0bce03be1c5f1c18d791c3681a26391796017114b2b35f9\
    199e8fff11a25f5d3f06d1aec79d08131f022d1c2fa541e6476e59cf6c514333\
    1cb807016cb07'
  },
  / ciphertext / h'934bb9f49942192bea7a56a9f52f2070a2ded7eaebaddb44b\
    cd5335c743a7b5fc84fa37b3643bc66e8863b0fc560a1615ada8570b64497f8a\
    afb73bd44f280d92ce6f55c9afa535337c43fc422927cbc0e46683b946701c11\
    e889d4bee35fd7c9ef335def2edd594c5a5fdeda6ea9478d0fb93abe2ed4c8cb\
    9c8af87dfbb9c2a095cf9a4fdfecd4e0ea307205b1a8408e9676fb91a1ee3db6\
    fce27b73366f590ad47546aefef17dd144a2cde568a08b5072fa2a144fe8d784\
    07a70ceb6704a01d76fa4d8dc45ef3adbb1cfa1ee59791b81f88e4c81b15b39b\
    b892c53cb339d3205a45c96da5a1e0c2511b7436a38c9c12565fa057c962395c\
    c15ceadc8b6c4720a445ddefbcb18d9c36fd6c0d5ce584cacd80c1f6b40cd2e5\
    e6082e5db579140b3'
])
```

Figure 27: HPKE-11 COSE_Encrypt0 (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
d08344a101183ca2045820400faa06149080d620fa067cabef42e03b05a7705da721\
88cd2732e034e493dc235903008e6c3c2040aadc5e88394e9f8e64459062d0ae76c9\
41e7e4a20158310056e59cacd8a62ba1569fe2e9b4495c61201afac15702398412e4\
e92c9dfb098ef00ea417a67235b9b4582c83efb1fe47a8d77143d322618aab4960ca\
6ff3bc6e0b0a3a891620f21eb9f877253ae8768d5beb72683ee9d54c375e06a6e460\
fe963f47aa7950fb246b3432cc75e2b86421363a324fd2baddbbdefa71de7f304a6c\
1aad4e4e0bac4e62daffa1fa05605065d4bdcfab842b2777a35f69eacc452037b0ef\
b4c6d7f1522b31e19a5f8d06c10ba42803ab58b4c6106d5c98f88872256fce8d1e78\
58b9020ffa8243a617077fc51f90dc939ff42ce3cccd62a64ad3e45e4d2cadf13539\
22c73fa503369ea34b9cbbb5b20b2c69b88a5f7fa07c41c820a1fc0cfc8b702f6740\
7bb1e5c8beecce96b5c925c564cbaebbf874cc60b65ae469e9a28c859220ed373293\
3891963566a4d4ff744f0716be4fb7b40015d00e138b552500f804a68393086d2593\
18e9dbc2cc17ec3d4d32b3890e31cca17eb6cca9f36d6cfb7274fc8cd4d8dcdd0b20\
fa4e609a5e17a7c60293c308bb00c5abc63fee3f811bac44a39b6175854bf7b92312\
0edd2ab52d3052a373f1762e7cc0fee18f550a30667a2054fddb4d498a96407b2826\
71d4e650189fe7544a232eb9bcab0d28dda0e523fad70d5bbad428de286e1c7e4f77\
4a125ba577daa0ae129cd17a40746e484f88c1debdd2101d4cd6becf08cd0a2574ae\
c253045dd4e0e2e21b7c3da70b07712725299a48db218189f7daae5250c22cde5237\
e64efe366ddedd519098de1ccad4a55a1d0a5fd6760b16839d3bb887b3eedd3459c1\
62779129cf62941dc04fae9ae494ded2cad4f082be84bbd362e66896bb5d970c8f4c\
f0875a160cc5b612189d8ffa64b0ffd93efdf4d21ef996908a764a4ec8c00a3ce90a\
db38e9c2c4aacbfb2957f7a8207db1b2a586ea2c8938982549e744e56086ef205323\
3c540f559f0bce03be1c5f1c18d791c3681a26391796017114b2b35f9199e8fff11a\
25f5d3f06d1aec79d08131f022d1c2fa541e6476e59cf6c5143331cb807016cb0759\
0121934bb9f49942192bea7a56a9f52f2070a2ded7eaebaddb44bcd5335c743a7b5f\
c84fa37b3643bc66e8863b0fc560a1615ada8570b64497f8aafb73bd44f280d92ce6\
f55c9afa535337c43fc422927cbc0e46683b946701c11e889d4bee35fd7c9ef335de\
f2edd594c5a5fdeda6ea9478d0fb93abe2ed4c8cb9c8af87dfbb9c2a095cf9a4fdfe\
cd4e0ea307205b1a8408e9676fb91a1ee3db6fce27b73366f590ad47546aefef17dd\
144a2cde568a08b5072fa2a144fe8d78407a70ceb6704a01d76fa4d8dc45ef3adbb1\
cfa1ee59791b81f88e4c81b15b39bb892c53cb339d3205a45c96da5a1e0c2511b743\
6a38c9c12565fa057c962395cc15ceadc8b6c4720a445ddefbcb18d9c36fd6c0d5ce\
584cacd80c1f6b40cd2e5e6082e5db579140b3
```

Figure 28: HPKE-11 COSE_Encrypt0 (Hex-Encoded CBOR)

A.8. HPKE-11-KE

```
NOTE: '\' line wrapping per RFC 8792

{
  / kty / 1: 7,
  / kid / 2: h'66b4942df6e05b245389a93dcc1303ac63a692f4ea92b2cb62c1c\
    d191a7751f0',
  / alg / 3: 61 / HPKE-11-KE /,
  / pub / -1: h'bdda40b91285e7e4c2106c1e8ad834817816ac961ed7fc13ca6a\
    ad917b3d3f01345cba4a01a8acabc39e5fb18d13c9bf91a071ec78b2564831e6\
    1613c58931f0a079790a0bd097099f8ca00627c5abaac4cb03460c9991baea35\
    7f007fa0bb937fe47f8ac42e165452093c61bcc3616b39c105d4a0229c099d1b\
    4104b61d99856bcba90bae76c418fa8c7d35c0fe604404122af3c6556116b394\
    eb2c6f2076d3098017a24fed82433b9181d09c76dd319aa95a3ba0a02a509679\
    89f0090088acb4ac6f44ebae51bba5cddb2da3a013dd28caa2304a630ba32854\
    437fea97fe712921cc524636b6b5955129ab8e813b50f420741ed30a0df47970\
    842d0b5222f2450ab862213567a0cc2b83507c71cec909d4e1559873c4ac6c1d\
    68a7971ca7a032421279d061ef4356da81983a9a0f3e7b9639214d3467b8d7f8\
    3f729843311038213ac61b80a5726106491c779a83c5ca0447b7fa95c3cab3f3\
    961e66845efa6993db976eb69149bfc5b6970510e6aba20759396610c8bd5705\
    cb75ae53c735f9873834399511471b0ca11626682ddac33515009ed8311d97bb\
    2a35a6c4ce34717cfc68d4a427f758c6a7276fa60987b0615e343a6b7d3b91ef\
    e728886694243ca52c989fdb45328da161ebc9cc2a1bcf019b741695544cb637\
    48c03a5e23bc7101678ad49b3bb440a1675b14db8c4bd532068733703c7b3753\
    6a033b484fe28a4590b630a7cb9128248a65052631c827a4c621c446d336bb99\
    e7b96d4b879c291a3c123b5fd66664726e479c99161a756a269eb7fb3827527f\
    8a539e5e556e78588037823aa1d61939b6230691ce6cf16215b6a85da8ae45e0\
    8362209413c927b6e914af7645bd0c503f90c137f5626bf1ce5ca55a951b0eb2\
    837bd46817854a198145a96b9172983783276c11aa703b1b7030bb0576997b8b\
    8d357708a9b5f8b311ea2aa3909696dec9a8b7a49bcdb553dec8952d724f20d8\
    9790d101014c3c08e35decf201dcf9b23ed43b8cb4c10b455c27a54b47661a64\
    8304a9d83572386b2d135456ca33bda631de586ae9008fd7c465d2bc79de8a1a\
    8ab55c5318818fad5f369b21b1ece6c7d52af1c6a1f08cc5df299abcd2c996dd\
    ba296065465b',
  / priv / -2: h'6206c57ba5f678eb6d06ac44d428ed461701f48d7b2ed06c8f6\
    4f25cb72cf9a59afeea9c511fcf152c7760e1fea926431880974236eaa9f36dd\
    83a4cd871888b'
}
```

Figure 29: HPKE-11-KE COSE_Key (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
a5010702582066b4942df6e05b245389a93dcc1303ac63a692f4ea92b2cb62c1cd19\
1a7751f003183d20590320bdda40b91285e7e4c2106c1e8ad834817816ac961ed7fc\
13ca6aad917b3d3f01345cba4a01a8acabc39e5fb18d13c9bf91a071ec78b2564831\
e61613c58931f0a079790a0bd097099f8ca00627c5abaac4cb03460c9991baea357f\
007fa0bb937fe47f8ac42e165452093c61bcc3616b39c105d4a0229c099d1b4104b6\
1d99856bcba90bae76c418fa8c7d35c0fe604404122af3c6556116b394eb2c6f2076\
d3098017a24fed82433b9181d09c76dd319aa95a3ba0a02a50967989f0090088acb4\
ac6f44ebae51bba5cddb2da3a013dd28caa2304a630ba32854437fea97fe712921cc\
524636b6b5955129ab8e813b50f420741ed30a0df47970842d0b5222f2450ab86221\
3567a0cc2b83507c71cec909d4e1559873c4ac6c1d68a7971ca7a032421279d061ef\
4356da81983a9a0f3e7b9639214d3467b8d7f83f729843311038213ac61b80a57261\
06491c779a83c5ca0447b7fa95c3cab3f3961e66845efa6993db976eb69149bfc5b6\
970510e6aba20759396610c8bd5705cb75ae53c735f9873834399511471b0ca11626\
682ddac33515009ed8311d97bb2a35a6c4ce34717cfc68d4a427f758c6a7276fa609\
87b0615e343a6b7d3b91efe728886694243ca52c989fdb45328da161ebc9cc2a1bcf\
019b741695544cb63748c03a5e23bc7101678ad49b3bb440a1675b14db8c4bd53206\
8733703c7b37536a033b484fe28a4590b630a7cb9128248a65052631c827a4c621c4\
46d336bb99e7b96d4b879c291a3c123b5fd66664726e479c99161a756a269eb7fb38\
27527f8a539e5e556e78588037823aa1d61939b6230691ce6cf16215b6a85da8ae45\
e08362209413c927b6e914af7645bd0c503f90c137f5626bf1ce5ca55a951b0eb283\
7bd46817854a198145a96b9172983783276c11aa703b1b7030bb0576997b8b8d3577\
08a9b5f8b311ea2aa3909696dec9a8b7a49bcdb553dec8952d724f20d89790d10101\
4c3c08e35decf201dcf9b23ed43b8cb4c10b455c27a54b47661a648304a9d8357238\
6b2d135456ca33bda631de586ae9008fd7c465d2bc79de8a1a8ab55c5318818fad5f\
369b21b1ece6c7d52af1c6a1f08cc5df299abcd2c996ddba296065465b2158406206\
c57ba5f678eb6d06ac44d428ed461701f48d7b2ed06c8f64f25cb72cf9a59afeea9c\
511fcf152c7760e1fea926431880974236eaa9f36dd83a4cd871888b
```

Figure 30: HPKE-11-KE COSE_Key (Hex-Encoded CBOR)

NOTE: '\' line wrapping per RFC 8792

```
/ COSE_Encrypt / 96([
  / protected / h'a10101',
  / unprotected / {
    / iv / 5: h'0aab0d623e3ade196aaf572b'
  },
  / ciphertext / h'cade8e5050387bff05b73e1d021e368978103becabbe5f52a\
    cb2a2618e1f1e75fa422e018846784975323e6df2f410fbd512a1ae4814ce83d\
    ca6f3646ccee64d6e415a0978bcd42e307d7ee711cb2cb38591c9ca62b61f211\
    f7da7c8d4e5a59ed978815aedf10dfb05abb7afaf283d11ca81ee6f9fd52b0e2\
    4dc7fadc0313c2a66e31d766002680c940f90d4d3c365a4f89f6d4c0bde503de\
    012c1ab22cac3a690f4cf9682430a6b386cadf93e71e908ad369cdcfb1d1e9ec\
    06e5208a7bb423534ae95ec6e28c204228ee8ada8c3cd28957c7cfb99d51aa2a\
    10125c047f5a094faeeb0f60c19aab9ab23cbb71d9d8c146b04bc88ce1a74366\
    8509d839df106f21e2f958c8f2a69c0d8f8122d9bdbc44b3bf370b44f3859cde\
```

```
      4db01bf5a20813eb4',
    / recipients / [
      [
        / protected / h'a201183d04582066b4942df6e05b245389a93dcc1303ac\
      63a692f4ea92b2cb62c1cd191a7751f0',
        / unprotected / {
          / ek / -4: h'089da49105ce8802dcdb0629fb6f759a18528ec91ea1f41\
      afdaa4e56a15d3c01cf5105e5f16255aea6daa7b9ba145edaae3a7f868b53ce2\
      38a2f071495b7c7b82c503fbc2d1b1ffaaca3dd76e81f2030da5c5a3b6417a36\
      3e4ae2985302565825becd6b4b9a0e821bbcad2f9e872e9c09981c6af8238ce0\
      f32a3d7eca23127eba7086f72b008498237527a3089d033b10528d8b74a88050\
      7fddfd63bc43db80365c9dd5c5dd4063e186ea01c8344697b093856708ad3b06\
      db0cfd310051c8eb97bd83fdb81fba3e49ca74532697cf9a5cdf858d6c5d2000\
      5ab61ed2fc10ed8af811bc19ade46f00586c09108dbf8c0a3caaa155614be58d\
      4b3289cebba34f120c934d339cccc7a9fe45e1b20cd13511508569775a0a53dd\
      12ee7570ce49213ff4f10685da97a2544ca8203082a8cf31a85a036739ed613d\
      c82c4ce0aef9fc3f1d6610ef8c77121efafc1c7bced3a4830a68da73b48c7e86\
      3353250645ae550b810b3b60dced2677f4b1385213cfd842362abfc19ebd097d\
      dd9adbd08bcc754bad9f264f266fc2a6400cbbcb499589a40e8c9cb2b64a47ac\
      61480c75096cfdea8bb62479f6451c956ab5f27d97aa2efd94139444f59d9426\
      ebfd3bec8e48f42b8f206810453570b5de626bd7c100494329e24c7e65d52eae\
      ff933a88a742400a2d5e58d36cb87a1c87e6a8a753665491dcfb94d8e25b14dd\
      aacef28d79a194d336ee9abc15cd50ba90905ecacb37e52a5401799980f94069\
      c4f4c622fb7d3ad6611b764703c08382cf512ce4ec3187e11789f3cccd452497\
      4a12ef73b231aa34d920394bf34be6c8f71dbb250039da1d5f8853f9c51562b7\
      1b164f8885b9b85c6adf427fbed5d2921a93d87e155c95412549d98673182946\
      077485300089b3b09b0501d7207b4810d11ac835cc90c6ce6560fb53131b2708\
      af3f7cd500bad364c3917660b0072debfebfe69a2b1c4a05921bb6d8defad807\
      87875fd42765e66ea7a9374f01024f4b110686809805e3dd341795a0e322eda4\
      39c728d47c17029f1af393a08f22fdb423346ae9cdf67779df91676e6b5a3a2d\
      0b39f451dccad9f82'
        },
        / ciphertext / h'011bea833595a8ce3a0c1b2434dc841c245451bed09f3\
      26299b0f8012c234124'
      ]
    ]
  ])
```

Figure 31: HPKE-11-KE COSE_Encrypt (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
d8608443a10101a1054c0aab0d623e3ade196aaf572b590121cade8e5050387bff05\
b73e1d021e368978103becabbe5f52acb2a2618e1f1e75fa422e018846784975323e\
6df2f410fbd512a1ae4814ce83dca6f3646ccee64d6e415a0978bcd42e307d7ee711\
cb2cb38591c9ca62b61f211f7da7c8d4e5a59ed978815aedf10dfb05abb7afaf283d\
11ca81ee6f9fd52b0e24dc7fadc0313c2a66e31d766002680c940f90d4d3c365a4f8\
9f6d4c0bde503de012c1ab22cac3a690f4cf9682430a6b386cadf93e71e908ad369c\
dcfb1d1e9ec06e5208a7bb423534ae95ec6e28c204228ee8ada8c3cd28957c7cfb99\
d51aa2a10125c047f5a094faeeb0f60c19aab9ab23cbb71d9d8c146b04bc88ce1a74\
3668509d839df106f21e2f958c8f2a69c0d8f8122d9bdbc44b3bf370b44f3859cde4\
db01bf5a20813eb481835827a201183d04582066b4942df6e05b245389a93dcc1303\
ac63a692f4ea92b2cb62c1cd191a7751f0a123590300089da49105ce8802dcdb0629\
fb6f759a18528ec91ea1f41afdaa4e56a15d3c01cf5105e5f16255aea6daa7b9ba14\
5edaae3a7f868b53ce238a2f071495b7c7b82c503fbc2d1b1ffaaca3dd76e81f2030\
da5c5a3b6417a363e4ae2985302565825becd6b4b9a0e821bbcad2f9e872e9c09981\
c6af8238ce0f32a3d7eca23127eba7086f72b008498237527a3089d033b10528d8b7\
4a880507fddfd63bc43db80365c9dd5c5dd4063e186ea01c8344697b093856708ad3\
b06db0cfd310051c8eb97bd83fdb81fba3e49ca74532697cf9a5cdf858d6c5d20005\
ab61ed2fc10ed8af811bc19ade46f00586c09108dbf8c0a3caaa155614be58d4b328\
9cebba34f120c934d339cccc7a9fe45e1b20cd13511508569775a0a53dd12ee7570c\
e49213ff4f10685da97a2544ca8203082a8cf31a85a036739ed613dc82c4ce0aef9f\
c3f1d6610ef8c77121efafc1c7bced3a4830a68da73b48c7e863353250645ae550b8\
10b3b60dced2677f4b1385213cfd842362abfc19ebd097ddd9adbd08bcc754bad9f2\
64f266fc2a6400cbbcb499589a40e8c9cb2b64a47ac61480c75096cfdea8bb62479f\
6451c956ab5f27d97aa2efd94139444f59d9426ebfd3bec8e48f42b8f20681045357\
0b5de626bd7c100494329e24c7e65d52eaeff933a88a742400a2d5e58d36cb87a1c8\
7e6a8a753665491dcfb94d8e25b14ddaacef28d79a194d336ee9abc15cd50ba90905\
ecacb37e52a5401799980f94069c4f4c622fb7d3ad6611b764703c08382cf512ce4e\
c3187e11789f3cccd4524974a12ef73b231aa34d920394bf34be6c8f71dbb250039d\
a1d5f8853f9c51562b71b164f8885b9b85c6adf427fbed5d2921a93d87e155c95412\
549d986731829460774853000 89b3b09b0501d7207b4810d11ac835cc90c6ce6560f\
b53131b2708af3f7cd500bad364c3917660b0072debfebfe69a2b1c4a05921bb6d8d\
efad80787875fd42765e66ea7a9374f01024f4b110686809805e3dd341795a0e322e\
da439c728d47c17029f1af393a08f22fdb423346ae9cdf67779df91676e6b5a3a2d0\
b39f451dccad9f825820011bea833595a8ce3a0c1b2434dc841c245451bed09f3262\
99b0f8012c234124
```

Figure 32: HPKE-11-KE COSE_Encrypt (Hex-Encoded CBOR)

A.9. HPKE-12

NOTE: '\' line wrapping per RFC 8792

```
{
  / kty / 1: 7,
  / kid / 2: h'6af47f413f10204703b2f48ba4c8d69b5a41148d36a47c7f49726\
    1757a8a0dcc',
```

```
    / alg / 3: 62 / HPKE-12 /,
    / pub / -1: h'd9d98bc2e3bff7e7a9b6277829385e3c184a1c505d3b054f73c9\
      4d8db79218b3a615d9b3477c83ffe66e71982b487a9a70d543fe8112d99092f4\
      211e150c8d818431ac145bd6043c2580bd3e688d15675b37e7a2c52696b1868b\
      4f07a40a2b9cc0e86c4b04aeb1180cb74222d83c8a97a9b62757c38030827af5\
      617bc208d00c66d8968965a3607ed53da4b13c43000a63db5fa2dc77c334115d\
      d13ad6b99c11039f210889afa4c6f984a5fdc111c5bb0916bc87d609ae816923\
      7053a37bd3528997cb6b69a2ff4b3a307a640108719b61156827c733c7ccb02a\
      6406a28e80f4ca9021931b403a4672a003b49c9578bc3fc909ba9c78e8a9b7b9\
      e47a284185d91b41b7a4a616471eba3677a16b7b4e8aad7354818c538d934191\
      b99001662b22521a9733d23f4fbc9a80b85d42a3afb2b21596509f14e1478898\
      4f1443cb380332414ac28fb77557c87e72b021ca9890610145a92ab7d3da1e46\
      a606547c8f2c47b99bf96f7f17c53128ad45c16b99c84ed8e4426d94139beb62\
      a32b25bba50d0f06166ab47452680920f95f34b27df1734ee4b3b77e38b3f388\
      470b49cb9ceaa60ff3b89161035e40423d6b3f9b3a269592a7719762403197b2\
      e70c51486cfb24a8fdaaac96cc2e99f938e46b0ffe9523e7544e715aa08f3092\
      c9db6468a3769e4a25b9b1afe26bcd01a733f7da0b28bcc36ea008aa845301b1\
      80255cb036906ecc5c3fda01a2a9289db6b52608972e6a2867a0007e765a422e\
      070d51301327546d0a549b5e9196f57250f5c434d375307d5229f28c3112c16a\
      8241c48d1b038c927db2292af40692ce827aabe99049173270068cf8e7706a88\
      45b2b104b55459d3b0bc51a85e944326676aad10c107a6410188d010f7997a98\
      18cb15d5c62a83af048bbda2c8586b71bfada04ee2b83a17890a9213b4874bbb\
      bac282f2659079d7c9dd6b409a988dc0d27109d4518ed762823a156d13242265\
      6f26169a2362914370189de59c01b46b6b7698dd290a8e43213d9a76355ab277\
      75c350d0221601c339fbc93053a4cfe56059395f3337b6cfcc37c0f52d6698c7\
      e1b414b57b25995c541b08b5fc3bbaa87ca29fdc4f3bc4afe9e34aaad856f58c\
      188818c4efd007349631ee743adc833d1bd46d17719b590b4ff64c9ed7a5a1a3\
      9b198bd93ef4184ec70c172de8aa1cec0f445306c90139c9277d84e51268d19a\
      8d5599cad58e9a9b7c452acb9d76389a8c402991067e12056083954489a3b4b1\
      9e10165f4725526307cf2c99c7e520c10629a896dc35521c771d004e77a166b8\
      6b1156262efd47ca0f12ac7008090741584ba172a0ac487a49cf1e9a30949749\
      75ba4c17d40817698dca775d1447c624762575f071c87402209696c47c054df6\
      317a22abb6e727ac29a6db0056237c27b5452b0b9775bc698b23faba55c779b1\
      78959b966f10d75dacf7889c668b614823e8d9791e23215e3a7bb7694b31134d\
      b64a28991c74520c2c810271e8b102ebfb341ba1389d77b9d9455d91fb10ccaa\
      41edd99ac52916586ba99a0741717a725fdcaa603a99885caede96c7a3b54400\
      2d0ba753b26b5a423fa90e34966e0c646c710ace6c8b81999c338f807f0b049e\
      bba667278418091dfbe0b946e151cc5fd848c3b4beb69d63d1065bde88e69dae\
      bb43274eb7e3',
    / priv / -2: h'a0dad96b56dd010b716e9dbac3999c660cf0edf291d16c446e9\
      461547e6d70f450c73224dc88aab7aa7d167f3ca636286949a695a3729ae4e4f\
      f0b355a059dda'
  }
```

Figure 33: HPKE-12 COSE_Key (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
a501070258206af47f413f10204703b2f48ba4c8d69b5a41148d36a47c7f49726175\
7a8a0dcc03183e205904a0d9d98bc2e3bff7e7a9b6277829385e3c184a1c505d3b05\
4f73c94d8db79218b3a615d9b3477c83ffe66e71982b487a9a70d543fe8112d99092\
f4211e150c8d818431ac145bd6043c2580bd3e688d15675b37e7a2c52696b1868b4f\
07a40a2b9cc0e86c4b04aeb1180cb74222d83c8a97a9b62757c38030827af5617bc2\
08d00c66d8968965a3607ed53da4b13c43000a63db5fa2dc77c334115dd13ad6b99c\
11039f210889afa4c6f984a5fdc111c5bb0916bc87d609ae8169237053a37bd35289\
97cb6b69a2ff4b3a307a640108719b61156827c733c7ccb02a6406a28e80f4ca9021\
931b403a4672a003b49c9578bc3fc909ba9c78e8a9b7b9e47a284185d91b41b7a4a6\
16471eba3677a16b7b4e8aad7354818c538d934191b99001662b22521a9733d23f4f\
bc9a80b85d42a3afb2b21596509f14e14788984f1443cb380332414ac28fb77557c8\
7e72b021ca9890610145a92ab7d3da1e46a606547c8f2c47b99bf96f7f17c53128ad\
45c16b99c84ed8e4426d94139beb62a32b25bba50d0f06166ab47452680920f95f34\
b27df1734ee4b3b77e38b3f388470b49cb9ceaa60ff3b89161035e40423d6b3f9b3a\
269592a7719762403197b2e70c51486cfb24a8fdaaac96cc2e99f938e46b0ffe9523\
e7544e715aa08f3092c9db6468a3769e4a25b9b1afe26bcd01a733f7da0b28bcc36e\
a008aa845301b180255cb036906ecc5c3fda01a2a9289db6b52608972e6a2867a000\
7e765a422e070d51301327546d0a549b5e9196f57250f5c434d375307d5229f28c31\
12c16a8241c48d1b038c927db2292af40692ce827aabe99049173270068cf8e7706a\
8845b2b104b55459d3b0bc51a85e944326676aad10c107a6410188d010f7997a9818\
cb15d5c62a83af048bbda2c8586b71bfada04ee2b83a17890a9213b4874bbbbac282\
f2659079d7c9dd6b409a988dc0d27109d4518ed762823a156d132422656f26169a23\
62914370189de59c01b46b6b7698dd290a8e43213d9a76355ab27775c350d0221601\
c339fbc93053a4cfe56059395f3337b6cfcc37c0f52d6698c7e1b414b57b25995c54\
1b08b5fc3bbaa87ca29fdc4f3bc4afe9e34aaad856f58c188818c4efd007349631ee\
743adc833d1bd46d17719b590b4ff64c9ed7a5a1a39b198bd93ef4184ec70c172de8\
aa1cec0f445306c90139c9277d84e51268d19a8d5599cad58e9a9b7c452acb9d7638\
9a8c402991067e12056083954489a3b4b19e10165f4725526307cf2c99c7e520c106\
29a896dc35521c771d004e77a166b86b1156262efd47ca0f12ac7008090741584ba1\
72a0ac487a49cf1e9a3094974975ba4c17d40817698dca775d1447c624762575f071\
c87402209696c47c054df6317a22abb6e727ac29a6db0056237c27b5452b0b9775bc\
698b23faba55c779b178959b966f10d75dacf7889c668b614823e8d9791e23215e3a\
7bb7694b31134db64a28991c74520c2c810271e8b102ebfb341ba1389d77b9d9455d\
91fb10ccaa41edd99ac52916586ba99a0741717a725fdcaa603a99885caede96c7a3\
b544002d0ba753b26b5a423fa90e34966e0c646c710ace6c8b81999c338f807f0b04\
9ebba667278418091dfbe0b946e151cc5fd848c3b4beb69d63d1065bde88e69daebb\
43274eb7e3215840a0dad96b56dd010b716e9dbac3999c660cf0edf291d16c446e94\
61547e6d70f450c73224dc88aab7aa7d167f3ca636286949a695a3729ae4e4ff0b35\
5a059dda
```

Figure 34: HPKE-12 COSE_Key (Hex-Encoded CBOR)

```
   NOTE: '\' line wrapping per RFC 8792

   / COSE_Encrypt0 / 16([
     / protected / h'a101183e',
     / unprotected / {
       / kid / 4: h'6af47f413f10204703b2f48ba4c8d69b5a41148d36a47c7f497\
       261757a8a0dcc',
       / ek / -4: h'2ce85d7e6308f65d42e8464f86a5ece10df9f3bb2d523531f64\
       8b5849783d109175d632a7b8e20fc5d22929c9df78ab2c9d94ee56efe6dc2056\
       36684ef6cadc4cb66edbb56abe7775842c5f4e90d525f709e82270af4981ebce\
       6dc2f7faae61f7ff1f4908b7b19006c6e1480ad38226276efd60d81e3a3fc4f1\
       7f52102af8d9fecc008199291f74a58902d94124cd8cc3dd1f9e31658297991\
       97d2ef503213a7fc54e6831c481686802b23ac30a1191dc7a3ff70490dad8164\
       8ceba9787e874f57b2bc63b005bb5aedd72b52390867e3a8ba61a0e9bdd33c6a\
       f95b8f4ab01e32d87fd53a5e5cac1703797bc12ed82fe9109293cb4030357109\
       a57eeb27c8633802449c6f8fba98fb492fde0ca81e3fe06d6cd67f3eb845bbde\
       34c837e9e499e864bf9f3459ea776a85e0621a8aceb0b9f2dafec5e28199f981\
       217ccb1ab3eb2cb5146232395c99e8ddb5842c8a83e9192365cbbcda226886fe\
       f36a11c8eaf2a3fa92ff872984febad97bf8e2f356d7bb494cefa2f904010818\
       559414ad992c17e801a93f7b36125ea73cd17ff1019dcd0b1367f1332a178ca7\
       bbc06fed0ac7f133ce3b63126e829f4b18db709e8373099b0cd3edbebef1df48\
       955bcfa7c142b46d951cdf02689ada8ad4bc64481f2f27b19e5e5b01c89854ce\
       9bb0f84e095235b2983d46e758464f0e7b91c819d7fe8c75c595eb8ffb8e90bc\
       982f0420a395c0399f7fbd6530c194072068014dea9a41df748f2d871e55eb47\
       2b7c81500164302a716148f667a132d69ed90f6f4a40a32ce674890761a35701\
       39c69406b6b5b382e1284d4b1f92eda241547793d6fc7bc680b700fbd65b7c7f\
       4be8d0a53dc7b68987ffb47d6dff01e663034cb47e8a1c320148ae7a2451d556\
       020a010bb34991942766b4b5ce44395bde79a6b82a57de39a20ee076aaf4f642\
       90d734f04620b5f8acc5bcf2b3e01262315722bc32eb07b93afbd1e26d2a62ec\
       6c34249e822ba344dd2898378d205e5f240df0ea45513811f3b22cc17e8f6c88\
       0157cfd7fe141f0701fbefa2e5a7d7f07854ef6a8707072a43f85e605dbe4f41\
       450c147a78d40814defb5fd0766353b21ddecf032c0d7a644067d11979d9ed98\
       93b7ec989d4f4e3a518b3042ba0bb14e9764da68f6981b2c63e56a23a8ea6174\
       f6b059d0fe74e2625c4dd932d2dbb12fdb4fb7834e3b6a6b8f152c14ad488a71\
       dc6225eb5aac9bb7e67bae2c09de0428a41655f095b15fd1872dd51e5be306f5\
       15737e8e431c22d7e8c0ce4598fda7f050cad02999f0dbe47af810b29240d0b1\
       17dd412900d372a5b82d0f42f5e998dfb861b254798cbb007b68230c685316dc\
       5a141fb2c2c82a362c5ca1429c05a25f5a22954228376af6e9e6f198c24e8597\
       98ccec85cd295f196bf493cc8a1927964baf379ea8eb3597ed048eb91715efa1\
       be0a93be4ff56ed4bfe4017099c1ce1bcd15461fa62a3eff4d402c7ebf624acd\
       7fe4d74a74e32c9627f99424fd903002788319d9677ce52a3c9c0d7988c0b6d4\
       388bd7a67712e'
     },
     / ciphertext / h'80480620adaaf2d3ee5fbda6219e8e7f1a9d086d0a1b11335\
       995b11d68518bfaa15765eaed343d2ec7dfecef907e19851e27d25d21ee4bc23\
       542a17afa09734305abfec9a872bfbf3fff1608577cf84d78d49ef339644d4ac\
       dd09167e5ff71171d0b08f974567ffd03d3f3bcfd38f1610eeddd91401684f8f\
       71d529d7525e53f2f31cd70aa6e287e2ac3bd5bf76af19236e78760912348985\
```

```
      d191e839e3518daf8ac7c12d1fb0276dd7244aa83bff12147c403873f15213fb\
      0d3fb2001b3e6b83226298f663f262f7521e516ae3d02a029c0dae7df73e5837\
      1504d48edddfbf68d74fec4f1b65a9ab319b60c90e62aa7f316533555774514e\
      5302651177ae0b6c794707aaa3ba13f5c0e21d595251c8d84973f762ce3f5d56\
      e2162e2b5094052e1'
  ])
```

Figure 35: HPKE-12 COSE_Encrypt0 (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
d08344a101183ea20458206af47f413f10204703b2f48ba4c8d69b5a41148d36a47c\
7f497261757a8a0dcc235904402ce85d7e6308f65d42e8464f86a5ece10df9f3bb2d\
523531f648b5849783d109175d632a7b8e20fc5d22929c9df78ab2c9d94ee56efe6d\
c205636684ef6cadc4cb66edbb56abe7775842c5f4e90d525f709e82270af4981ebc\
e6dc2f7faae61f7ff1f4908b7b19006c6e1480ad38226276efd60d81e3a3fc4f17f5\
2102af8d9feccc008199291f74a58902d94124cd8cc3dd1f9e3165829799197d2ef5\
03213a7fc54e6831c481686802b23ac30a1191dc7a3ff70490dad81648ceba9787e8\
74f57b2bc63b005bb5aedd72b52390867e3a8ba61a0e9bdd33c6af95b8f4ab01e32d\
87fd53a5e5cac1703797bc12ed82fe9109293cb4030357109a57eeb27c8633802449\
c6f8fba98fb492fde0ca81e3fe06d6cd67f3eb845bbde34c837e9e499e864bf9f345\
9ea776a85e0621a8aceb0b9f2dafec5e28199f981217ccb1ab3eb2cb5146232395c9\
9e8ddb5842c8a83e9192365cbbcda226886fef36a11c8eaf2a3fa92ff872984febad\
97bf8e2f356d7bb494cefa2f904010818559414ad992c17e801a93f7b36125ea73cd\
17ff1019dcd0b1367f1332a178ca7bbc06fed0ac7f133ce3b63126e829f4b18db709\
e8373099b0cd3edbebef1df48955bcfa7c142b46d951cdf02689ada8ad4bc64481f2\
f27b19e5e5b01c89854ce9bb0f84e095235b2983d46e758464f0e7b91c819d7fe8c7\
5c595eb8ffb8e90bc982f0420a395c0399f7fbd6530c194072068014dea9a41df748\
f2d871e55eb472b7c81500164302a716148f667a132d69ed90f6f4a40a32ce674890\
761a3570139c69406b6b5b382e1284d4b1f92eda241547793d6fc7bc680b700fbd65\
b7c7f4be8d0a53dc7b68987ffb47d6dff01e663034cb47e8a1c320148ae7a2451d55\
6020a010bb34991942766b4b5ce44395bde79a6b82a57de39a20ee076aaf4f64290d\
734f04620b5f8acc5bcf2b3e01262315722bc32eb07b93afbd1e26d2a62ec6c34249\
e822ba344dd2898378d205e5f240df0ea45513811f3b22cc17e8f6c880157cfd7fe1\
41f0701fbefa2e5a7d7f07854ef6a8707072a43f85e605dbe4f41450c147a78d4081\
4defb5fd0766353b21ddecf032c0d7a644067d11979d9ed9893b7ec989d4f4e3a518\
b3042ba0bb14e9764da68f6981b2c63e56a23a8ea6174f6b059d0fe74e2625c4dd93\
2d2dbb12fdb4fb7834e3b6a6b8f152c14ad488a71dc6225eb5aac9bb7e67bae2c09d\
e0428a41655f095b15fd1872dd51e5be306f515737e8e431c22d7e8c0ce4598fda7f\
050cad02999f0dbe47af810b29240d0b117dd412900d372a5b82d0f42f5e998dfb86\
1b254798cbb007b68230c685316dc5a141fb2c2c82a362c5ca1429c05a25f5a22954\
228376af6e9e6f198c24e859798ccec85cd295f196bf493cc8a1927964baf379ea8e\
b3597ed048eb91715efa1be0a93be4ff56ed4bfe4017099c1ce1bcd15461fa62a3ef\
f4d402c7ebf624acd7fe4d74a74e32c9627f99424fd903002788319d9677ce52a3c9\
c0d7988c0b6d4388bd7a67712e59012180480620adaaf2d3ee5fbda6219e8e7f1a9d\
086d0a1b11335995b11d68518bfaa15765eaed343d2ec7dfecef907e19851e27d25d\
21ee4bc23542a17afa09734305abfec9a872bfbf3fff1608577cf84d78d49ef33964\
4d4acdd09167e5ff71171d0b08f974567ffd03d3f3bcfd38f1610eeddd91401684f8\
f71d529d7525e53f2f31cd70aa6e287e2ac3bd5bf76af19236e78760912348985d19\
1e839e3518daf8ac7c12d1fb0276dd7244aa83bff12147c403873f15213fb0d3fb20\
01b3e6b83226298f663f262f7521e516ae3d02a029c0dae7df73e58371504d48eddd\
fbf68d74fec4f1b65a9ab319b60c90e62aa7f316533555774514e5302651177ae0b6\
c794707aaa3ba13f5c0e21d595251c8d84973f762ce3f5d56e2162e2b5094052e1
```

Figure 36: HPKE-12 COSE_Encrypt0 (Hex-Encoded CBOR)

A.10. HPKE-12-KE

NOTE: '\' line wrapping per RFC 8792

```
{
  / kty / 1: 7,
  / kid / 2: h'da3c1ad21455112a22a022e2a9f3738002fc448ca06f10222076f\
    8e24cb37c88',
  / alg / 3: 63 / HPKE-12-KE /,
  / pub / -1: h'1f3a20ac944450f00eb8456a6be0cffed5733a322f4373c10f0a\
    333192be2e7421b7f9a3604a61ba09958c5ab622c19f17d7cad937af40342f9d\
    0287a04467485ccfe3b681c5706309902891d57fc3a948fe396b64b366127716\
    ecac90a59564aeb75002b60b891431964a330fb15a5e5504ebfc940981703858\
    a70b455b7fbb43a99c06a2b759a02c215f0746cd4a94e473c794477355397e36\
    d19076863437b136ce260aabd0b413d412b2dc980812aa77fa96483c264c1889\
    46a8cd857793b787ba0c42363b12b6e4a2b1adf61dea4a47605a59602c2d7c66\
    05ea3596363a52595717b83c74c4b728f0c81593970def696fbd5960d9f0c138\
    b7b1180c0796a7a70795a203cab11d8709afdc498bc7058c2769568aa655b1b1\
    39447f940335b3f7a847a304f3e200199465b93c509386c73884a3882659bbb4\
    9efdd34537884d08ec5c52705dbf745be4483b08d81814164087f41754c18b88\
    c1a069057a21f938c02a3197872198b567a90b048e5b326d3c33ab388e2cd902\
    81a268a2b46f6e9c3e8c06945db0adab070153cb21a4d850ee5892cd714e7704\
    1a055b0a6307d0093a6c91b54b2ea3992928c5bb43cdbf74cf6160cfe8952015\
    d8794f848a60620b0a555ad03a4045eb0aa263c6fd7c72296145a943a182fc43\
    6719917acb2c50e440b7f843b263741a646971fac1f1242f5e399b98474e571b\
    039763cdc39cc8a2f39940956dbec0b81ff3c8fe4276850c9dc58076f0f918ba\
    232289ba4b7eec7ab5994f07e356bfb724f86a599d9c6b11961b31e11b48b066\
    bc054b615555bd8c7a45c61106749147401f8091bc2093ca5c499c33ccbbd93b\
    0517acc38901ac99fab5684c1451127b3e797f92005c6585a0c3a327d55b02ee\
    c02396f4a749fa305b5c994ab0a4c24705cdf92ad8b1ade4f639c4f3ca05dc15\
    6860bd1e93a56f37a03dd9c1e057106913c41e57af4ac2c4f2d8631e6891749b\
    1517362ca094823320429e431a2e527bbfc63262c92027b97aa16a82c327058d\
    43774561b46edbb09f221b6872504dc6a4d0804d0012992842534975114de19a\
    61593c1ea7715d6232d2e1389e4a15674b3580177db061ca3ce8443ad76c111c\
    4964fb0c8436a22e31aeb853141213c4d0341e2ab128993712c1b5b13d7c1424\
    0a542acbc428136815c44657e63438613324f48ce09b6543b14154f8b9e6265d\
    f5b777e2aac26e4a450feca2c730a79eb05177782c2b4b725e276f8d3b523646\
    b8f1a06723c94529cbc9cce58bc56365ba044df9eacffb2393c06a0be6e281c8\
    7876477cca3476cfbd1caf4d590302933198f3ab6b279232984be7e1b73f6152\
    b38a8b097cb9accb0df0a280f7502a31d630017aac73701b1a5284e889373373\
    582b9048fc2b054a4660524c3b5caba00a846d06d37d75596ed1768b9ae207ea\
    821cfffc17c8114c5fa13d6cd744493c0dea31811a9c85547b74dd04310b1996\
    4f503b6f105e780775a0747a831a2a0f581e082021fd1a8b049cae93562822cc\
    b9e4489f2f0c8f2c2430930491877b7ca9358c2006172fd37700bb8208a8717d\
    926c9b35b992679971326b4c436278fb3764129a948343aca8ad3817c6a25cce\
    c1f96e00d42eac7a6047b39825f3553712ab2aab647a26349090691e732cb137\
    a45f64d0b8a4',
  / priv / -2: h'af95ba4ef8653e7bb31fe8363a081d6000e54565bb71c1a151d\
```

```
    d8c00309d005c59d68097d5800d4dc8d7bc45528d843a70b6211e09183e60aa2\
    c992ff49b8695'
}
```

Figure 37: HPKE-12-KE COSE_Key (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
a50107025820da3c1ad21455112a22a022e2a9f3738002fc448ca06f10222076f8e2\
4cb37c8803183f205904a01f3a20ac944450f00eb8456a6be0cffed5733a322f4373\
c10f0a333192be2e7421b7f9a3604a61ba09958c5ab622c19f17d7cad937af40342f\
9d0287a04467485ccfe3b681c5706309902891d57fc3a948fe396b64b366127716ec\
ac90a59564aeb75002b60b891431964a330fb15a5e5504ebfc940981703858a70b45\
5b7fbb43a99c06a2b759a02c215f0746cd4a94e473c794477355397e36d190768634\
37b136ce260aabd0b413d412b2dc980812aa77fa96483c264c188946a8cd857793b7\
87ba0c42363b12b6e4a2b1adf61dea4a47605a59602c2d7c6605ea3596363a525957\
17b83c74c4b728f0c81593970def696fbd5960d9f0c138b7b1180c0796a7a70795a2\
03cab11d8709afdc498bc7058c2769568aa655b1b139447f940335b3f7a847a304f3\
e200199465b93c509386c73884a3882659bbb49efdd34537884d08ec5c52705dbf74\
5be4483b08d81814164087f41754c18b88c1a069057a21f938c02a3197872198b567\
a90b048e5b326d3c33ab388e2cd90281a268a2b46f6e9c3e8c06945db0adab070153\
cb21a4d850ee5892cd714e77041a055b0a6307d0093a6c91b54b2ea3992928c5bb43\
cdbf74cf6160cfe8952015d8794f848a60620b0a555ad03a4045eb0aa263c6fd7c72\
296145a943a182fc436719917acb2c50e440b7f843b263741a646971fac1f1242f5e\
399b98474e571b039763cdc39cc8a2f39940956dbec0b81ff3c8fe4276850c9dc580\
76f0f918ba232289ba4b7eec7ab5994f07e356bfb724f86a599d9c6b11961b31e11b\
48b066bc054b615555bd8c7a45c61106749147401f8091bc2093ca5c499c33ccbbd9\
3b0517acc38901ac99fab5684c1451127b3e797f92005c6585a0c3a327d55b02eec0\
2396f4a749fa305b5c994ab0a4c24705cdf92ad8b1ade4f639c4f3ca05dc156860bd\
1e93a56f37a03dd9c1e057106913c41e57af4ac2c4f2d8631e6891749b1517362ca0\
94823320429e431a2e527bbfc63262c92027b97aa16a82c327058d43774561b46edb\
b09f221b6872504dc6a4d0804d001299284253497511 4de19a61593c1ea7715d6232\
d2e1389e4a15674b3580177db061ca3ce8443ad76c111c4964fb0c8436a22e31aeb8\
53141213c4d0341e2ab128993712c1b5b13d7c14240a542acbc428136815c44657e6\
3438613324f48ce09b6543b14154f8b9e6265df5b777e2aac26e4a450feca2c730a7\
9eb05177782c2b4b725e276f8d3b523646b8f1a06723c94529cbc9cce58bc56365ba\
044df9eacffb2393c06a0be6e281c87876477cca3476cfbd1caf4d590302933198f3\
ab6b279232984be7e1b73f6152b38a8b097cb9accb0df0a280f7502a31d630017aac\
73701b1a5284e889373373582b9048fc2b054a4660524c3b5caba00a846d06d37d75\
596ed1768b9ae207ea821cfffc17c8114c5fa13d6cd744493c0dea31811a9c85547b\
74dd04310b19964f503b6f105e780775a0747a831a2a0f581e082021fd1a8b049cae\
93562822ccb9e4489f2f0c8f2c2430930491877b7ca9358c2006172fd37700bb8208\
a8717d926c9b35b992679971326b4c436278fb3764129a948343aca8ad3817c6a25c\
cec1f96e00d42eac7a6047b39825f3553712ab2aab647a26349090691e732cb137a4\
5f64d0b8a4215840af95ba4ef8653e7bb31fe8363a081d6000e54565bb71c1a151dd\
8c00309d005c59d68097d5800d4dc8d7bc45528d843a70b6211e09183e60aa2c992f\
f49b8695
```

Figure 38: HPKE-12-KE COSE_Key (Hex-Encoded CBOR)

```
NOTE: '\' line wrapping per RFC 8792

/ COSE_Encrypt / 96([
  / protected / h'a10103',
  / unprotected / {
    / iv / 5: h'a121e56c3d426e69ce917fe3'
  },
  / ciphertext / h'3a36b87e2d53080f2e52a2994b6c04babccbf27cfcaabed6e\
    10eff448ff2cb3b805efcb59e7101877f30d55760684e0ce472c9979170ad401\
    ddb6fdd70fb879b2192e8720eea24de9d3d29f80e01a6438c0f4198c3409eccb\
    195816dc509c85dba59574e9d6286219af5bd78dfd13c25dd6de22b8a1a824dd\
    464edd4a51fd714ada330f404bef0debfa9e51ab6aba8cef919fd669102ea59c\
    907b5cecc962ca95f9b8a74b3ac2de437d1746f5478813d2f92e9f83be48ffd6\
    cda04c63285cb3f422895bd41b1acee46a4b6640073af51ad3248b9c7e9304d9\
    332a68d819873d0f424185f3562a8d736054b361ae4c8c4e26f9f7242ff429fe\
    45921215e9e7b7387451c77790f8dd6677dce5f94c72ce86106403624af5bbf6\
    6dcd3d017ae838d02',
  / recipients / [
    [
      / protected / h'a201183f045820da3c1ad21455112a22a022e2a9f37380\
    02fc448ca06f10222076f8e24cb37c88',
      / unprotected / {
        / ek / -4: h'2c5249f8084eac277dd297f8a7c6cfb2ff13f86c680c1fa\
    5de6ee1e78cdf917bff9cabefa8445a3309d512c1f5046416b940c8aaecff1d1\
    29204900a0d100a28ef64b0983b421081e038e721c9b7dd52348b5be6ab678ca\
    e398cd55fad307e4e7f4fb97728cdddb05e22a95db7f99ee17350141f659090c\
    2894499455df9f1d88a25cee3197f499683582994a09d026d271dc97e4b48d3b\
    78d3e8fcef38b9651d2e4ba038c0b8523dfa42dfeac1a5b8e4f4434b6a06a0e2\
    ab10ded0e6940de3dbffb2a1633f2aed4440366640acfdaaab5cc149631b0139\
    ab079a773b3d8e6cab0764426f06f77ca64c7dce75c58f4f8cde8d7cd72aae77\
    d18f993ef865152d24d04d9352d482ad65f427d462e0ae9f4ea50e031a06875a\
    afb5850ff7eca81c311e50858a2fde35ac327e765f7e0f1208b354762948a0fb\
    f4c8f0ff0d97d3bd93a6b6c8c300e4696228fe2af60a9adafd00b1c7ec530cdb\
    c56f0853a0400c7125b7d0bcb7db5083cf4531125880094e1ccb493ff2914b24\
    eb29b396fcabb0c7a9f2156ea5a28fc8b9ee94c21a588dace4aa0bd7d2001f6a\
    05df667e7470c4b62882b3233f759d07a3194e4779778fa7117a347eb128bf7b\
    9df3c3def710a6f556b895f77939ff1e18c4b112262cbcf175c2a207cd5eb9d6\
    eb38ed70746973f4d67e7477fa82969c3b5594dc43e0a8f29b2f8f2eda23827e\
    b6283a2340f59022abc2f27d106497c4501859af3e7c50ca3fd8e136350547bd\
    29b5501004654e8d8438cc51ed32281cc2c4b9a9c8d8a2c81552926b1c3ef624\
    8c32eefead5c8303c6a38d5dece07855e1e2b3cea600e4edf9ce1db1e854eb39\
    cf1067d004683189e55a964d0834129bfbd2b3bec2f1f58fc6e3d742bc09c26d\
    bb59cb6ae746e0df59fd9e714c6ecdce7feb32cb199252dabdb34e60185e75d1\
    48b143d1a91f939af1c9339dd2c20b0bc0af87e694dc587233084968e77e90cb\
    869ba8578aeedd3d7420bd2ccd253f3ab48dd6009819e94ace223558cec54a16\
    35199a3a5b3fdc4aa3aa3ed965a06558a9224c3d1d410cbf689352c300ec60f8\
```

```
      47761248d1ca1009cbcac4a0d67e40c32ad7c8bc28a72ef2c53f9646d790ea72\
      2118404a033b8a5030804f633102be56506920143c65f2125c981bfbc939c14a\
      6338b8ce257d68368847472f9daa2a68db5e71d125780416796c406f6f07699f\
      ca2a322631ef3646bd55097c6e7ba856ddbd2b60f7568c90d88ce0c2ff62f82a\
      17b4bfd2415559732e2d1df4e2b9b1de855ffcba9b29f9ff63d90fef6db94188\
      8b6988f22a9ebfa6180fc7f3e2666ae2edf7d345acb48339dc6491821e47e306\
      db53f3785f87ae2dce1567a0b33e9e5ce5aa82854166d7670b396d6bd1e1e546\
      5032186d247a5c7a0e05f098951382fa3f821995943db26c1b4c56e503da58e9\
      3e94b7a60ca6ce2e35d61c80bf826aefff14e4ffe6e3f0f0bb5ce3effb72354d\
      088ca882d775d3ce4e8435210dd6859118b76932e63c14de0e5ed149c626afa4\
      5f58cbffe01a3b1f3'
        },
        / ciphertext / h'588672ac7f578fbee9a786df21a1afa2f8d45647485c6\
      ad74b04887016a74fee077784d67433fae3642f285348f5bb11'
      ]
    ]
  ])
```

Figure 39: HPKE-12-KE COSE_Encrypt (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
d8608443a10103a1054ca121e56c3d426e69ce917fe35901213a36b87e2d53080f2e\
52a2994b6c04babccbf27cfcaabed6e10eff448ff2cb3b805efcb59e7101877f30d5\
5760684e0ce472c9979170ad401ddb6fdd70fb879b2192e8720eea24de9d3d29f80e\
01a6438c0f4198c3409eccb195816dc509c85dba59574e9d6286219af5bd78dfd13c\
25dd6de22b8a1a824dd464edd4a51fd714ada330f404bef0debfa9e51ab6aba8cef9\
19fd669102ea59c907b5cecc962ca95f9b8a74b3ac2de437d1746f5478813d2f92e9\
f83be48ffd6cda04c63285cb3f422895bd41b1acee46a4b6640073af51ad3248b9c7\
e9304d9332a68d819873d0f424185f3562a8d736054b361ae4c8c4e26f9f7242ff42\
9fe45921215e9e7b7387451c77790f8dd6677dce5f94c72ce86106403624af5bbf66\
dcd3d017ae838d0281835827a201183f045820da3c1ad21455112a22a022e2a9f373\
8002fc448ca06f10222076f8e24cb37c88a1235904402c5249f8084eac277dd297f8\
a7c6cfb2ff13f86c680c1fa5de6ee1e78cdf917bff9cabefa8445a3309d512c1f504\
6416b940c8aaecff1d129204900a0d100a28ef64b0983b421081e038e721c9b7dd52\
348b5be6ab678cae398cd55fad307e4e7f4fb97728cdddb05e22a95db7f99ee17350\
141f659090c2894499455df9f1d88a25cee3197f499683582994a09d026d271dc97e\
4b48d3b78d3e8fcef38b9651d2e4ba038c0b8523dfa42dfeac1a5b8e4f4434b6a06a\
0e2ab10ded0e6940de3dbffb2a1633f2aed4440366640acfdaaab5cc149631b0139a\
b079a773b3d8e6cab0764426f06f77ca64c7dce75c58f4f8cde8d7cd72aae77d18f9\
93ef865152d24d04d9352d482ad65f427d462e0ae9f4ea50e031a06875aafb5850ff\
7eca81c311e50858a2fde35ac327e765f7e0f1208b354762948a0fbf4c8f0ff0d97d\
3bd93a6b6c8c300e4696228fe2af60a9adafd00b1c7ec530cdbc56f0853a0400c712\
5b7d0bcb7db5083cf4531125880094e1ccb493ff2914b24eb29b396fcabb0c7a9f21\
56ea5a28fc8b9ee94c21a588dace4aa0bd7d2001f6a05df667e7470c4b62882b3233\
f759d07a3194e4779778fa7117a347eb128bf7b9df3c3def710a6f556b895f77939f\
f1e18c4b112262cbcf175c2a207cd5eb9d6eb38ed70746973f4d67e7477fa82969c3\
b5594dc43e0a8f29b2f8f2eda23827eb6283a2340f59022abc2f27d106497c450185\
9af3e7c50ca3fd8e136350547bd29b5501004654e8d8438cc51ed32281cc2c4b9a9c\
8d8a2c81552926b1c3ef6248c32eefead5c8303c6a38d5dece07855e1e2b3cea600e\
4edf9ce1db1e854eb39cf1067d004683189e55a964d0834129bfbd2b3bec2f1f58fc\
6e3d742bc09c26dbb59cb6ae746e0df59fd9e714c6ecdce7feb32cb199252dabdb34\
e60185e75d148b143d1a91f939af1c9339dd2c20b0bc0af87e694dc587233084968e\
77e90cb869ba8578aeedd3d7420bd2ccd253f3ab48dd6009819e94ace223558cec54\
a1635199a3a5b3fdc4aa3aa3ed965a06558a9224c3d1d410cbf689352c300ec60f84\
7761248d1ca1009cbcac4a0d67e40c32ad7c8bc28a72ef2c53f9646d790ea7221184\
04a033b8a5030804f633102be56506920143c65f2125c981bfbc939c14a6338b8ce2\
57d68368847472f9daa2a68db5e71d125780416796c406f6f07699fca2a322631ef3\
646bd55097c6e7ba856ddbd2b60f7568c90d88ce0c2ff62f82a17b4bfd2415559732\
e2d1df4e2b9b1de855ffcba9b29f9ff63d90fef6db941888b6988f22a9ebfa6180fc\
7f3e2666ae2edf7d345acb48339dc6491821e47e306db53f3785f87ae2dce1567a0b\
33e9e5ce5aa82854166d7670b396d6bd1e1e5465032186d247a5c7a0e05f09895138\
2fa3f821995943db26c1b4c56e503da58e93e94b7a60ca6ce2e35d61c80bf826aeff\
f14e4ffe6e3f0f0bb5ce3effb72354d088ca882d775d3ce4e8435210dd6859118b76\
932e63c14de0e5ed149c626afa45f58cbffe01a3b1f35830588672ac7f578fbee9a7\
86df21a1afa2f8d45647485c6ad74b04887016a74fee077784d67433fae3642f2853\
48f5bb11
```

Figure 40: HPKE-12-KE COSE_Encrypt (Hex-Encoded CBOR)

A.11. HPKE-13

NOTE: '\' line wrapping per RFC 8792

```
{
  / kty / 1: 7,
  / kid / 2: h'423cd82d6d196a643d0f928c0f026e178391d6602b0b4aa0458de\
    094758b4562',
  / alg / 3: 64 / HPKE-13 /,
  / pub / -1: h'e7da03e1e9a9593b4c84e47ba465720442846f996db605212130\
    aaf397b2246a726576b9eb077e1dfa078fd331338a60e127bf8b09a3044659bf\
    95076d8a68506296f90161e421a3082bafb63200a1f01284d11a0694367411a7\
    917781199871fc43c0dc5c6fdf7b58f5602850d5611046b5b11b80c0b2397457\
    bc6512c30c2528cfd875031a5ada9c4fd4f9668fa811b436b27c053d9af59986\
    1a70677c9d6e72048cf14b830c0f60650262d363f3b8b82b86876b641c5a5c89\
    95238ed2e9821c525bb04b0d2f454d690b2279258fff6141f7499806e42c6395\
    0237583ca7e0c589c580004b54134bae9187bd5f9bb7cfacbb03a05bf47c8016\
    1287e137a56ab4bbc527c12bac712ba3296c6ccfe58481a1917c30105e30d6cb\
    c0d489f5d94c2986663c83bb67f6386e39675330ac2be682fec1116c495a4b31\
    622c8988c10a7520cc6e0be8a0cea963b717a96170a29d18bcca1ca21cd32e02\
    50c901c2cbd75b96edf6976f627739dac52eb74a8f0358ace74cc3cb9969ec57\
    916742525295f02749ac128ac776baa09029521337940a25caab93797786c750\
    2bcb2846b9a94110fac523744e72044758815a098145ed866391507b09828e54\
    ea5758e7671c248d38f3165ad1af54445745b7b42ba79e5f489707f63175d072\
    ab72300887335f0600d65b998ca8cc5ce463bffa954f323b1cf04579519d5c87\
    394f14c0449475e65104a0b44838fbb371e936abe2a5cb22334aa66aac779ead\
    e46124704f96232c25818e02c47f3522cbc700c75a080ee66ab19f1a0dc95317\
    60f8317ab07beb779966dc2306ea1bbc6a70b4dc208e5aa664b7cb3f5c2a75ca\
    4836585e419710b2320edd8756210bb4d55b2f9a03c0964480627aa486625b9c\
    393745ca8674767315e92471ab36fec4ab06c11daa1b105c15a86243aaadb2cf\
    e4ca9a21a2a342e3b0bad0a0b143a82c8986c1cc293585be809ca3e1d7240df8\
    6ba9c376ceb7905be82a98c8275d465ae62131f3ec5ae6c45099598a13096cdf\
    f1a932bb54576c86d9e94f16d4c0947c59b205239be131c60c669b26a0b2dcc9\
    1450ab98902a3422a753d11eda968acd0070eea8a132f341342439bed990abe0\
    56c0340378cc116a2258255a869cd3ce50aa13db7853537acfa2c00672da4e0d\
    53b214f2c763b668425a8a93067b17f75b4962c944ec8556b6a170f32db7801f\
    ca2a334aa949020a5f4be981c627a8e161c3ffb1b11de4b35bd5a4fa99a69438\
    b2b6a6b0f65c820c36672f1513daa179e5242ebcf62bf89160c9599ae0bb01da\
    4011212750d36790c19bc19584c72b810df5f84532f4b631961f6ce289a1c68a\
    39aa7e763702316a7cca8c943fd38ab9a69bb3da39d5ba8a0a072846a163a964\
    190965c181b0cec81021030949472722a23787e8db54043c52334b7f235abc95\
    0962f6734628792518477ceaca66d6744c4c0473cbeaa61939546fc83d1d4bc5\
    de5cb9d7a62829e54172e529a54a74bf8bb64e67bf96584d6b9105fba207c9b8\
    cffd550183834e1a6184e7d90a5d4471880533f2f89d4962cef51906d4842836\
    d27daf7532c7ec28153529dc80bf78709f03819be45948a8351c09164890780e\
    a1d0287dbb56c9045990016cffc8904b55064fe3b6e5a8c00f68cc9c08176d63\
```

```
      aa76b22f45a3243a797440e399c0a90c7e8939def3aa449ba63bc74622e08ae4\
      8500451749b2917c76432cae4cb6339040fd0a9f18867bbd87c6fcb7227cda50\
      0310a3ef7aab359642120587dca56ad1069a477408317192f8083b2cc602de53\
      4f07c54e52f802eb011921d99cb78351e3c20f3438ce122846f2acc582d919f2\
      b749e75500de5145319851b2e723f861a484284646489be2bc4bf919288b955b\
      770c5990e6083038535d8377a54386fb6a74678cb8fd37b34f706f6ed9b31033\
      a24948923af3154a986c11e024bf8c28cbc85ef390cfc71330b000a0a5e94a5f\
      e863a9831aa2db7ef160a1b6bac43733c797177a1fb8a9a32a3d9c00a4f0c91e\
      e7540207133563674bf9f2c42a33036e54b9f70b24d721c8fc117abba91d0c08\
      6f7f2350ff883eb85c6a4a481b0b5158b3b8cd82e72224450549f36d6b864351\
      cc96aeb9879b29a6eddc06cc7056a1a05cfdc23b821346336c86856bb75d274b\
      a7568b9da0a24577986f950d8915d42fa08d02aa742ba1951e4c68c14b040485\
      7da80f8188b8',
    / priv / -2: h'24a7ee9c4a51fcef865fc3de9c07231e5dfb141de448fdd7eaf\
      f0183c1c8708475b27ca68d08e25a899c02ad7b1db63279e3a6db22048338ee9\
      dc5c31257d76c'
  }
```

Figure 41: HPKE-13 COSE_Key (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
a50107025820423cd82d6d196a643d0f928c0f026e178391d6602b0b4aa0458de094\
758b4562031840205906 20e7da03e1e9a9593b4c84e47ba465720442846f996db605\
212130aaf397b2246a726576b9eb077e1dfa078fd331338a60e127bf8b09a3044659\
bf95076d8a68506296f90161e421a3082bafb63200a1f01284d11a0694367411a791\
7781199871fc43c0dc5c6fdf7b58f5602850d5611046b5b11b80c0b2397457bc6512\
c30c2528cfd875031a5ada9c4fd4f9668fa811b436b27c053d9af599861a70677c9d\
6e72048cf14b830c0f60650262d363f3b8b82b86876b641c5a5c8995238ed2e9821c\
525bb04b0d2f454d690b2279258fff6141f7499806e42c63950237583ca7e0c589c5\
80004b54134bae9187bd5f9bb7cfacbb03a05bf47c80161287e137a56ab4bbc527c1\
2bac712ba3296c6ccfe58481a1917c30105e30d6cbc0d489f5d94c2986663c83bb67\
f6386e39675330ac2be682fec1116c495a4b31622c8988c10a7520cc6e0be8a0cea9\
63b717a96170a29d18bcca1ca21cd32e0250c901c2cbd75b96edf6976f627739dac5\
2eb74a8f0358ace74cc3cb9969ec57916742525295f02749ac128ac776baa0902952\
1337940a25caab93797786c7502bcb2846b9a94110fac523744e72044758815a0981\
45ed866391507b09828e54ea5758e7671c248d38f3165ad1af54445745b7b42ba79e\
5f489707f63175d072ab72300887335f0600d65b998ca8cc5ce463bffa954f323b1c\
f04579519d5c87394f14c0449475e65104a0b44838fbb371e936abe2a5cb22334aa6\
6aac779eade46124704f96232c25818e02c47f3522cbc700c75a080ee66ab19f1a0d\
c9531760f8317ab07beb779966dc2306ea1bbc6a70b4dc208e5aa664b7cb3f5c2a75\
ca4836585e419710b2320edd8756210bb4d55b2f9a03c0964480627aa486625b9c39\
3745ca8674767315e92471ab36fec4ab06c11daa1b105c15a86243aaadb2cfe4ca9a\
21a2a342e3b0bad0a0b143a82c8986c1cc293585be809ca3e1d7240df86ba9c376ce\
b7905be82a98c8275d465ae62131f3ec5ae6c45099598a13096cdff1a932bb54576c\
86d9e94f16d4c0947c59b205239be131c60c669b26a0b2dcc91450ab98902a3422a7\
53d11eda968acd0070eea8a132f341342439bed990abe056c0340378cc116a225825\
5a869cd3ce50aa13db7853537acfa2c00672da4e0d53b214f2c763b668425a8a9306\
```

```
   7b17f75b4962c944ec8556b6a170f32db7801fca2a334aa949020a5f4be981c627a8\
   e161c3ffb1b11de4b35bd5a4fa99a69438b2b6a6b0f65c820c36672f1513daa179e5\
   242ebcf62bf89160c9599ae0bb01da4011212750d36790c19bc19584c72b810df5f8\
   4532f4b631961f6ce289a1c68a39aa7e763702316a7cca8c943fd38ab9a69bb3da39\
   d5ba8a0a072846a163a964190965c181b0cec81021030949472722a23787e8db5404\
   3c52334b7f235abc950962f6734628792518477ceaca66d6744c4c0473cbeaa61939\
   546fc83d1d4bc5de5cb9d7a62829e54172e529a54a74bf8bb64e67bf96584d6b9105\
   fba207c9b8cffd550183834e1a6184e7d90a5d4471880533f2f89d4962cef51906d4\
   842836d27daf7532c7ec28153529dc80bf78709f03819be45948a8351c0916489078\
   0ea1d0287dbb56c9045990016cffc8904b55064fe3b6e5a8c00f68cc9c08176d63aa\
   76b22f45a3243a797440e399c0a90c7e8939def3aa449ba63bc74622e08ae4850045\
   1749b2917c76432cae4cb6339040fd0a9f18867bbd87c6fcb7227cda500310a3ef7a\
   ab359642120587dca56ad1069a477408317192f8083b2cc602de534f07c54e52f802\
   eb011921d99cb78351e3c20f3438ce122846f2acc582d919f2b749e75500de514531\
   9851b2e723f861a484284646489be2bc4bf919288b955b770c5990e6083038535d83\
   77a54386fb6a74678cb8fd37b34f706f6ed9b31033a24948923af3154a986c11e024\
   bf8c28cbc85ef390cfc71330b000a0a5e94a5fe863a9831aa2db7ef160a1b6bac437\
   33c797177a1fb8a9a32a3d9c00a4f0c91ee7540207133563674bf9f2c42a33036e54\
   b9f70b24d721c8fc117abba91d0c086f7f2350ff883eb85c6a4a481b0b5158b3b8cd\
   82e72224450549f36d6b864351cc96aeb9879b29a6eddc06cc7056a1a05cfdc23b82\
   1346336c86856bb75d274ba7568b9da0a24577986f950d8915d42fa08d02aa742ba1\
   951e4c68c14b0404857da80f8188b821584024a7ee9c4a51fcef865fc3de9c07231e\
   5dfb141de448fdd7eaff0183c1c8708475b27ca68d08e25a899c02ad7b1db63279e3\
   a6db22048338ee9dc5c31257d76c
```

Figure 42: HPKE-13 COSE_Key (Hex-Encoded CBOR)

NOTE: '\' line wrapping per RFC 8792

```
   / COSE_Encrypt0 / 16([
     / protected / h'a1011840',
     / unprotected / {
       / kid / 4: h'423cd82d6d196a643d0f928c0f026e178391d6602b0b4aa0458\
       de094758b4562',
       / ek / -4: h'199f52b68d2a9093bf80f906e6bbaa63af8a7a1a9dab6d5a288\
       018dbeb45c7bf8e1d51a74e9a0549dfd5f2b1b325004a50c7584c1e88af9bbae\
       4559b833ae1711912798ea6093542c2afbdddb9feb1deda0931e29529466fc36\
       6772574867b512a175d4181ae2ffd66c8d57f6d61f253fd451a5ea04971f64ae\
       6519965a9c43d2627e7eb4926ebdcaf9fcc36a9cc184d80668aa417a20c44981\
       aa1b6aeb106114c4f8a842a5c67ceb404c27d4316b0a561955ddf7856334ab34\
       c5fff65366f914c22f9b375fef57b1627b29e0d84e097f4de5175eecd5a369fb\
       a10a974960ab99242041a566b310553eb71aa5a3963d9d5060c09c01d26cca65\
       4b91bc36ad9460672ff173da460f5947982993bc88b1d825ab16e262c8344e2f\
       84de94b94644b80d1c2ee64565887181d036ec6fa6f20543e250e1b4648f375b\
       f39bda55a2799993703106558f1d811bb9b6d699116e858107d2076bef5e16d4\
       7dfb430d9b12a1adfa3e57a1091bf79103f0d61fab364195902f759d1819c695\
       f42c95d4405cc1f11813c051c825e9865a5a8f679e5a291079b55c51b3917be8\
       0522c987cf40dca483378587bf07a7575c1e6f7cc5edae846cd08d5f87df7630\
```

```
      52002175b391b06a13c23a6a18626f91696ad35be92a4cd7c55c40b369c38b3c\
      0225d15cf4e12a08ecc6dc5e9871d715b181e6b2bcbf94b6c207ae99b9b59be5\
      e7bd2a16a1460cd3d1aeb90f54511337283acaa30b9751d840e2db5436717df6\
      fdcb4d02432f3a6179d66def397266c5f5202e8e4e6b8a99c6201a2ba052ba1d\
      5c0b80732f9e664fe9a081e9318d86b67c205bfd712c230f25e6c169f0848f84\
      d8157f674c2dc695d9d8360f7630fbf279d3b91d973ac991dd7308abfe13c6ef\
      19e813db506483c4bb8dd9801f451986d8ba4982e366730bfef6d6c3b375fb85\
      a9fdda55955379158654ac7a495a47f81ab481960cbeb4886b7515381204f5c3\
      04816800ff9d9dc54c2aba95c6a9311dfa6e1e4d335bc90fc5ec233c677ef6b7\
      d3c9b17fa236b7de673216866f8ceaa2d4692d62798826ab8bae7996cc23bccb\
      e0eedbbda41a67ba63665c13e210f2a2516e5f2b904f35f6a3a49fb895b22cbe\
      48618a03f7d608d8c3afd824d08d037dc1ecc7d4c6b266d69aae37c73ea83e99\
      7a6caecc5f03d1d0217df4defd65d90f8e7669e993547954b57cb58203c8b048\
      30257b5622b7fa619aaec33a0efed5dae20439a782c097f530a55c690bb5c156\
      5b6df88ba667d74e31dc43e7648dc555d2f66c03d8ad1e20c202686308593cfb\
      b8d067f5c94f57b7871f0e5822a6c3e8ff7e0011baf8e6c80a534e81a2b4681e\
      7fb7ca7370bf0458d40f6520b03aea435e478078c18a067040fddd14771a9ccd\
      ac526a14fe8f947c734441eede0d045607e812f9fd4990d89a01ada99f07b6d4\
      b05ab1e9fabd3b13d25e7fe01f96579895f296367120c7d812a56afdaeb176d4\
      52079f31bc1561193448e07aec4647fa1230708e7fb216547582af0c890aaffa\
      087e507ccb4ceac15aef09bf82cd448aa62d48e337339cabac9e0c535f03fd93\
      416a22cb33054ba3a1cb1636dd0965c9a2ff56667f8b0d51e965d5b2bb04f0aa\
      15f194db99dcacf5c26a2ba92267fa145fc2e24625072e3346dbe989d21acf3b\
      7b113f36f987dd81ca01637cd540a817129560331cd383eb9ad3761f34a5468a\
      b8d13ba6abeb0d19b25c3d0a2a7e583170f9a559b7952cc7f4379dcdd6e0f383\
      3106c81ad2d8f2a024054033b267e8d6a4c89d552ac7af35f62ec47f6550d796\
      7faad29d7ab089bf29ac01e13a7ceecf61f68998c1608e8c74eadcd4063cbf30\
      d3d580062b86242af27fc087152bd329c0d3918690b993e0e9bb78a2fbed4984\
      430abb25fae063646ee3da9ecd936fca7984c0a690d0477cbe393f170ecb3159\
      50d98dee64b66a83634472c757ae37dd51ad7eea26937d4d18a20d5c2f10e3ff\
      ece64fe26b6c2d0ae71780c7b8ec4d4d3fe0045d5c8b26035faa039210694f88\
      cb8f2792c54ac1a91bf0ed7cfd04c3ed4df849a37120e3752f62cf18dd5b3965\
      aa215e561ae8b24e3480b1ee52a7960d302cab769123db55dc4dc2e03c10ac0c\
      f41fec8104cc1104907f93cc9c35ee571390e1132f7978e2b1f6f76fcaee62e2\
      627d6ddd79e29fd21577fd281c64318aedea8a2eb7bfecd23b0e2507c31ad1de\
      c30bc16b2312b'
    },
    / ciphertext / h'e29b847767387a40e1e4c6f1d87a4c15d3946751f85e71643\
      3078c6456d5c98c54b494a5b7b9e6fb072be4a99af3e01c8a306583e274fd1d5\
      5f2ffe0d36529c7e016950450dc2002f08106f1d33debc1068b816e58b158c8a\
      fdee84a0d4c0a9d4fdad7e0ed655a2b7c8adbe9308eed4bf36409c86555c716c\
      c36d3e4a167f1691d21357d80de14fcbd095be2c425d84c81adacbab738daa67\
      7f87e670881f82f85a3dd7588ca34fa932c5d5f30f6cb1e532e25b3b13ed09ab\
      01810c8b5050a7362de24a5345b9f348e767884ead86428f65e23a0c59b2cc9d\
      64ec21541e0a5f429fb96731b7f308daf53aef5ba37e19a232a7abf25f008f0c\
      ea0bf2525f1cb7c91a8ca4d19be3c2e3851d8b75397ff9cae9af640af920e657\
      7172cbfa6cff90843'
  ])
```

Figure 43: HPKE-13 COSE_Encrypt0 (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
d08344a1011840a2045820423cd82d6d196a643d0f928c0f026e178391d6602b0b4a\
a0458de094758b456223590620199f52b68d2a9093bf80f906e6bbaa63af8a7a1a9d\
ab6d5a288018dbeb45c7bf8e1d51a74e9a0549dfd5f2b1b325004a50c7584c1e88af\
9bbae4559b833ae1711912798ea6093542c2afbdddb9feb1deda0931e29529466fc3\
66772574867b512a175d4181ae2ffd66c8d57f6d61f253fd451a5ea04971f64ae651\
9965a9c43d2627e7eb4926ebdcaf9fcc36a9cc184d80668aa417a20c44981aa1b6ae\
b106114c4f8a842a5c67ceb404c27d4316b0a561955ddf7856334ab34c5fff65366f\
914c22f9b375fef57b1627b29e0d84e097f4de5175eecd5a369fba10a974960ab992\
42041a566b310553eb71aa5a3963d9d5060c09c01d26cca654b91bc36ad9460672ff\
173da460f5947982993bc88b1d825ab16e262c8344e2f84de94b94644b80d1c2ee64\
565887181d036ec6fa6f20543e250e1b4648f375bf39bda55a2799993703106558f1\
d811bb9b6d699116e858107d2076bef5e16d47dfb430d9b12a1adfa3e57a1091bf79\
103f0d61fab364195902f759d1819c695f42c95d4405cc1f11813c051c825e9865a5\
a8f679e5a291079b55c51b3917be80522c987cf40dca483378587bf07a7575c1e6f7\
cc5edae846cd08d5f87df763052002175b391b06a13c23a6a18626f91696ad35be92\
a4cd7c55c40b369c38b3c0225d15cf4e12a08ecc6dc5e9871d715b181e6b2bcbf94b\
6c207ae99b9b59be5e7bd2a16a1460cd3d1aeb90f54511337283acaa30b9751d840e\
2db5436717df6fdcb4d02432f3a6179d66def397266c5f5202e8e4e6b8a99c6201a2\
ba052ba1d5c0b80732f9e664fe9a081e9318d86b67c205bfd712c230f25e6c169f08\
48f84d8157f674c2dc695d9d8360f7630fbf279d3b91d973ac991dd7308abfe13c6e\
f19e813db506483c4bb8dd9801f451986d8ba4982e366730bfef6d6c3b375fb85a9f\
dda55955379158654ac7a495a47f81ab481960cbeb4886b7515381204f5c30481680\
0ff9d9dc54c2aba95c6a9311dfa6e1e4d335bc90fc5ec233c677ef6b7d3c9b17fa23\
6b7de673216866f8ceaa2d4692d62798826ab8bae7996cc23bccbe0eedbbda41a67b\
a63665c13e210f2a2516e5f2b904f35f6a3a49fb895b22cbe48618a03f7d608d8c3a\
fd824d08d037dc1ecc7d4c6b266d69aae37c73ea83e997a6caecc5f03d1d0217df4d\
efd65d90f8e7669e993547954b57cb58203c8b04830257b5622b7fa619aaec33a0ef\
ed5dae20439a782c097f530a55c690bb5c1565b6df88ba667d74e31dc43e7648dc55\
5d2f66c03d8ad1e20c202686308593cfbb8d067f5c94f57b7871f0e5822a6c3e8ff7\
e0011baf8e6c80a534e81a2b4681e7fb7ca7370bf0458d40f6520b03aea435e47807\
8c18a067040fddd14771a9ccdac526a14fe8f947c734441eede0d045607e812f9fd4\
990d89a01ada99f07b6d4b05ab1e9fabd3b13d25e7fe01f96579895f296367120c7d\
812a56afdaeb176d452079f31bc1561193448e07aec4647fa1230708e7fb21654758\
2af0c890aaffa087e507ccb4ceac15aef09bf82cd448aa62d48e337339cabac9e0c5\
35f03fd93416a22cb33054ba3a1cb1636dd0965c9a2ff56667f8b0d51e965d5b2bb0\
4f0aa15f194db99dcacf5c26a2ba92267fa145fc2e24625072e3346dbe989d21acf3\
b7b113f36f987dd81ca01637cd540a817129560331cd383eb9ad3761f34a5468ab8d\
13ba6abeb0d19b25c3d0a2a7e583170f9a559b7952cc7f4379dcdd6e0f3833106c81\
ad2d8f2a024054033b267e8d6a4c89d552ac7af35f62ec47f6550d7967faad29d7ab\
089bf29ac01e13a7ceecf61f68998c1608e8c74eadcd4063cbf30d3d580062b86242\
af27fc087152bd329c0d3918690b993e0e9bb78a2fbed4984430abb25fae063646ee\
3da9ecd936fca7984c0a690d0477cbe393f170ecb315950d98dee64b66a83634472c\
757ae37dd51ad7eea26937d4d18a20d5c2f10e3ffece64fe26b6c2d0ae71780c7b8e\
c4d4d3fe0045d5c8b26035faa039210694f88cb8f2792c54ac1a91bf0ed7cfd04c3e\
```

```
   d4df849a37120e3752f62cf18dd5b3965aa215e561ae8b24e3480b1ee52a7960d302\
   cab769123db55dc4dc2e03c10ac0cf41fec8104cc1104907f93cc9c35ee571390e11\
   32f7978e2b1f6f76fcaee62e2627d6ddd79e29fd21577fd281c64318aedea8a2eb7b\
   fecd23b0e2507c31ad1dec30bc16b2312b590121e29b847767387a40e1e4c6f1d87a\
   4c15d3946751f85e716433078c6456d5c98c54b494a5b7b9e6fb072be4a99af3e01c\
   8a306583e274fd1d55f2ffe0d36529c7e016950450dc2002f08106f1d33debc1068b\
   816e58b158c8afdee84a0d4c0a9d4fdad7e0ed655a2b7c8adbe9308eed4bf36409c8\
   6555c716cc36d3e4a167f1691d21357d80de14fcbd095be2c425d84c81adacbab738\
   daa677f87e670881f82f85a3dd7588ca34fa932c5d5f30f6cb1e532e25b3b13ed09a\
   b01810c8b5050a7362de24a5345b9f348e767884ead86428f65e23a0c59b2cc9d64e\
   c21541e0a5f429fb96731b7f308daf53aef5ba37e19a232a7abf25f008f0cea0bf25\
   25f1cb7c91a8ca4d19be3c2e3851d8b75397ff9cae9af640af920e6577172cbfa6cf\
   f90843
```

Figure 44: HPKE-13 COSE_Encrypt0 (Hex-Encoded CBOR)

A.12. HPKE-13-KE

NOTE: '\' line wrapping per RFC 8792

```
{
  / kty / 1: 7,
  / kid / 2: h'1b28d7cad6a4ba7cdfceac81643186b3b4853d872f0d35e427b8f\
    e98260ef2a6',
  / alg / 3: 65 / HPKE-13-KE /,
  / pub / -1: h'877b92a75b89cff82420abca15213ebfa20ced24378516690e9c\
    6bfb75b29bc943bf344ceb252b38eccf40a16d51c53c170c6152656532778d8b\
    b31e9f2016fc0c99b646820216998564541a75167023599053bc2bbc8d539a97\
    d0acc3139225c9b8941f91a95d6acbc797cda8553b069cc27b72ba5f924774b1\
    be49c7ce55f82ce046a86b29b85bca062f1a52ac1a99ff0621b1288609d82e4c\
    859fbb8a2d98533268a218e3abb345347676fac41f57990e151cfe5b142d4486\
    4be22ec04c8123954d1e0263d1846ec44814f765ad14b95a46281c92cccd47aa\
    ab9f7420419742fcf93be2a58f265a5b30886cfb2b474ea6618bb465b8851e0c\
    c96339234c34cc3b9e17ba95ca3ad6c4838ab2b87de605a82723322a0bdf28a9\
    3c99165a5577d4c33d8b3697192521ae835d024c0c08369480f58dffc75eed9a\
    4d4c872773793921c520d6a7b43f69986f0c0990f0cae62295b1ca9d261300e7\
    050ae9b3ba55bb250c92217c8a776b8b5eb3514588342dad306dcfbbc900c33c\
    24a044cbc9c848c7ca33d651bb717ffd4bc3166b24bdd97e60c759e52c42b780\
    781e765b77ab7f3335865d9a05a8eb9a3c420bce171e9cd1a453195d2307c833\
    d50a55e1ae60136b38dc9e7ff06e0a98c62c253447056b0091312e3a203bfba4\
    2b68a91ccb80fde001fd834469081aaca41bf99a688eb519b7c5cc4853367404\
    c84c61ce22b9240501662301d07c247dd9fc26cf56334465211d745f8d0185db\
    7839bbf20423fc0f0a898f01013787e85a8c003d6d5c62918726810c946ff117\
    5f345d25e5580b58c559a32247a4705fa4ac3fe7c188823193b7548406345d79\
    49819a24d8f5312ee22aae85745f8036559319426a1a140bb7e428a049ea3791\
    7296d54914e8a18a610380d390a7b1527b2662768622615df14fe198bbef1490\
    17b4a8c50b22e4fab3ba0940da483631192ad1f0b61f1196a1539eef25814c40\
    2f96f107bdb828de5ba9f0c502b29a448da42025b2453a295ba6257b6ca247fd\
```

```
      20a40df13d2ea5142de3b291757cb69691b5e7b04dd650cc98952d590ba6f425\
      54942a1a829b0bc7170fd5243c02410fb01212fbc1612aa548c232707ba72597\
      64cddb86bc93be3bd895966b608ac4b9c29c7cdab7ba233813d5bb2788110263\
      897e005b37eedb83849650a7c90eba547889c09c7a6c84ccc72220b234322101\
      ff8b2469798563f9ba89fcb53cbb3f1024595db5a661164ee93a6206550380b4\
      a2c2055255421bc80c4becb3a255943cff9abfc48788b3252a62471e70649d52\
      c79cecc2489d84253c9293ed6b25300017df397da38b9bb776815d37bca52579\
      bb374d54548bf2b29e775956c390644f9aa2252632d04bc37a663b314791829c\
      27b720c51d1483f7e12cd4e7c1f38b6ad98a5e1c14768351a76da1267e529bfb\
      7bb6d1e07d49086b1e893b93097f3920849ba10b8dfb08d6b9b15dbc65fda93e\
      004319fe1bbbe4ccab73e00335f6167b1991259156b426355491c11a32956fc7\
      98f6ea73c363c8d5b371d4200891342d60e09b8b79cadc415281d56e75930045\
      b2203d1717d420ae9c58047d38119bf97111caba42471ae7d25c7d64c017848e\
      741a22f23427fb2a135fcb99acbaaa1f68021d4b9367c0389c150b81207c67bb\
      1b74d07f94e7729ffcab169002004025eda27a31685bfad3c227c05287b430d7\
      2a425b355785549c45e83db6d90bd2c306632c912390767607a960985530bc2c\
      4002207697c21921224d64acd93a4ba558b4ce7c30f503c849021ada958df07b\
      793d25be8b279f55d3180e8b03cdb3a842b60dc1576107f93a32189f2a928eaf\
      302841960a77083492b295edfb64abba50fbd31ce47a308cc9837cb865b44009\
      1ed56d6f3cb79e7608d3e2788006b9887b36e940bd2101002c59361b1c7cf243\
      b708fbb74afc462bccc3fa396b82f31f7d5344c60a629aa821373c9084f312c3\
      601e03c539fdfa45f5c6cdd14409c7bb7a82613573b9247a93404d179c11e7ac\
      76bbca925cb1b916b323818beea94a1d4ca492d4c1c1041f84da3f54c540ac64\
      94fe08ccf9569620427179f3099d016c82a43400bbc102cc741c22b539c52422\
      e59a69f71c2b6c8abfa56f7fdc32b6e9718979270e484c57b81359829cb87583\
      60026a7b3a8195657acaf1865a41aa5aabaaec7c323d8fae01355bbbc99d2b3f\
      c7dac82661d4',
    / priv / -2: h'4cae5ae552c32ce31cc6c60d4b8f6f1a36b034c325d016e6f38\
      e8f3d5c0f00a32f6b0990170c15043f8eb6137e2eb1965ba7fe7768f3fd19487\
      2748f85c920e4'
}
```

Figure 45: HPKE-13-KE COSE_Key (Diagnostic Notation)

```
NOTE: '\' line wrapping per RFC 8792

a501070258201b28d7cad6a4ba7cdfceac81643186b3b4853d872f0d35e427b8fe98\
260ef2a603184120590620877b92a75b89cff82420abca15213ebfa20ced24378516\
690e9c6bfb75b29bc943bf344ceb252b38eccf40a16d51c53c170c6152656532778d\
8bb31e9f2016fc0c99b646820216998564541a75167023599053bc2bbc8d539a97d0\
acc3139225c9b8941f91a95d6acbc797cda8553b069cc27b72ba5f924774b1be49c7\
ce55f82ce046a86b29b85bca062f1a52ac1a99ff0621b1288609d82e4c859fbb8a2d\
98533268a218e3abb345347676fac41f57990e151cfe5b142d44864be22ec04c8123\
954d1e0263d1846ec44814f765ad14b95a46281c92cccd47aaab9f7420419742fcf9\
3be2a58f265a5b30886cfb2b474ea6618bb465b8851e0cc96339234c34cc3b9e17ba\
95ca3ad6c4838ab2b87de605a82723322a0bdf28a93c99165a5577d4c33d8b369719\
2521ae835d024c0c08369480f58dffc75eed9a4d4c872773793921c520d6a7b43f69\
986f0c0990f0cae62295b1ca9d261300e7050ae9b3ba55bb250c92217c8a776b8b5e\
```

```
   b3514588342dad306dcfbbc900c33c24a044cbc9c848c7ca33d651bb717ffd4bc316\
   6b24bdd97e60c759e52c42b780781e765b77ab7f3335865d9a05a8eb9a3c420bce17\
   1e9cd1a453195d2307c833d50a55e1ae60136b38dc9e7ff06e0a98c62c253447056b\
   0091312e3a203bfba42b68a91ccb80fde001fd834469081aaca41bf99a688eb519b7\
   c5cc4853367404c84c61ce22b9240501662301d07c247dd9fc26cf56334465211d74\
   5f8d0185db7839bbf20423fc0f0a898f01013787e85a8c003d6d5c62918726810c94\
   6ff1175f345d25e5580b58c559a32247a4705fa4ac3fe7c188823193b7548406345d\
   7949819a24d8f5312ee22aae85745f8036559319426a1a140bb7e428a049ea379172\
   96d54914e8a18a610380d390a7b1527b2662768622615df14fe198bbef149017b4a8\
   c50b22e4fab3ba0940da483631192ad1f0b61f1196a1539eef25814c402f96f107bd\
   b828de5ba9f0c502b29a448da42025b2453a295ba6257b6ca247fd20a40df13d2ea5\
   142de3b291757cb69691b5e7b04dd650cc98952d590ba6f42554942a1a829b0bc717\
   0fd5243c02410fb01212fbc1612aa548c232707ba7259764cddb86bc93be3bd89596\
   6b608ac4b9c29c7cdab7ba233813d5bb2788110263897e005b37eedb83849650a7c9\
   0eba547889c09c7a6c84ccc72220b234322101ff8b2469798563f9ba89fcb53cbb3f\
   1024595db5a661164ee93a6206550380b4a2c2055255421bc80c4becb3a255943cff\
   9abfc48788b3252a62471e70649d52c79cecc2489d84253c9293ed6b25300017df39\
   7da38b9bb776815d37bca52579bb374d54548bf2b29e775956c390644f9aa2252632\
   d04bc37a663b314791829c27b720c51d1483f7e12cd4e7c1f38b6ad98a5e1c147683\
   51a76da1267e529bfb7bb6d1e07d49086b1e893b93097f3920849ba10b8dfb08d6b9\
   b15dbc65fda93e004319fe1bbbe4ccab73e00335f6167b1991259156b426355491c1\
   1a32956fc798f6ea73c363c8d5b371d4200891342d60e09b8b79cadc415281d56e75\
   930045b2203d1717d420ae9c58047d38119bf97111caba42471ae7d25c7d64c01784\
   8e741a22f23427fb2a135fcb99acbaaa1f68021d4b9367c0389c150b81207c67bb1b\
   74d07f94e7729ffcab169002004025eda27a31685bfad3c227c05287b430d72a425b\
   355785549c45e83db6d90bd2c306632c912390767607a960985530bc2c4002207697\
   c21921224d64acd93a4ba558b4ce7c30f503c849021ada958df07b793d25be8b279f\
   55d3180e8b03cdb3a842b60dc1576107f93a32189f2a928eaf302841960a77083492\
   b295edfb64abba50fbd31ce47a308cc9837cb865b440091ed56d6f3cb79e7608d3e2\
   788006b9887b36e940bd2101002c59361b1c7cf243b708fbb74afc462bccc3fa396b\
   82f31f7d5344c60a629aa821373c9084f312c3601e03c539fdfa45f5c6cdd14409c7\
   bb7a82613573b9247a93404d179c11e7ac76bbca925cb1b916b323818beea94a1d4c\
   a492d4c1c1041f84da3f54c540ac6494fe08ccf9569620427179f3099d016c82a434\
   00bbc102cc741c22b539c52422e59a69f71c2b6c8abfa56f7fdc32b6e9718979270e\
   484c57b81359829cb8758360026a7b3a8195657acaf1865a41aa5aabaaec7c323d8f\
   ae01355bbbc99d2b3fc7dac82661d42158404cae5ae552c32ce31cc6c60d4b8f6f1a\
   36b034c325d016e6f38e8f3d5c0f00a32f6b0990170c15043f8eb6137e2eb1965ba7\
   fe7768f3fd194872748f85c920e4
```

Figure 46: HPKE-13-KE COSE_Key (Hex-Encoded CBOR)

NOTE: '\' line wrapping per RFC 8792

```
/ COSE_Encrypt / 96([
  / protected / h'a10103',
  / unprotected / {
    / iv / 5: h'5edd2f32c88a7ed5084ba5e9'
  },
```

```
    / ciphertext / h'a89e91fbc720130044ea756b46c459be83a87b4ddf5d71e82\
      e60131ecd374d81ede7a955b473e45874af6f8624813cc37d33d6dee98cde887\
      a898f12263444f2eb0d01295a46e406b5e7474879163fa93f6ff3d053ab2c87f\
      84bbd8712aa6b31ee6d3207c792ef8c25990e64d2606712523e5c4bd5a0e8573\
      bf244255b2fa82cde8662a2dc93a334c1eba037e8ef86647632aab02bd883c4f\
      f8cdbc94086e12d28584508132b6f84423b4a3fd46149ac44fbf6eb9ef7d057d\
      9d3f9c170767d66afc7d1215b7d1f24acfc99f2f42e7db065672200235149808\
      fecb682f101b8526de33bc89099cfff488fae35a7eba7f254814293937318466\
      afac175a37be0cf2d08d9a113bcbaf7ac034a44bf2b3e7b2e9983ea682128910\
      a30c60010e0c84331',
    / recipients / [
      [
        / protected / h'a20118410458201b28d7cad6a4ba7cdfceac81643186b3\
      b4853d872f0d35e427b8fe98260ef2a6',
        / unprotected / {
          / ek / -4: h'7649b0acc2ecaa9725a3afddb317645725a4628cac13380\
      e56983ed07f545ef9c54d551e7bf990fe66ae902498e38ee50ca825eacfd0f84\
      3a2f1c1ff6585d46d14e019361e757ab65f031b00d3cd1b20a7c929579d37ed6\
      af700fb3718b129376fa00ab6a91f6d4dc08218fcc5c061329d3d18737132cba\
      a3157edd2afabc8a169c7649c19da9f751fff11298bab658584e8166dd4b0e07\
      0f23807e74604e002dcf57b26c61503188bdeed680f937e9bdd24121c5126fa9\
      63cad99dde48a04dee29494860d6fa3b1709a00c13ee127f51e2ad73c2ad840f\
      f33f93eee3b5ed2176c87c6314f7e98ee5b0e265576e967875f20c120fbb59a8\
      0ffa3df20e364b1ab5f68b76c2baa95e336a45e977413d97d7227e3777587797\
      cf5552749e1e5943dbadd71f3dd9d959b3530e67611cf0c3f4f17759302cc796\
      e0a7620cb759210b8d97b07dbb4d56cbb35dbd14c57d3936dbae0ae4ab624b15\
      0903f29250991da9f8c10dc3da1bc584a61c7c455c9164cd3ab5d0453eed9a8b\
      e4bb1f8cc5dc5fb9243b218b685a93d4466af77c4925a6803edae64f9b584d93\
      2e07771511458913cc6c35e54468242a89a53d1f1bdeb0f3107cc99959d5668d\
      3c4b13c537a0897baa295506ec786fc0ce0a1f669b39f6d79cba0901ea79e0c4\
      b005491be47a52f0147bb406b289d656e379c6eb69b20cdcb426eb8af207ba58\
      64d304e90336e034e87415224a34d95d9cf1206cb0c0d063362b36981c820b0c\
      ff56f81e46b0b2823a108ca1b413e063eb7af17e86ec42a481d07817325a7c91\
      7fbc12790a8dc0fdfa7f5fba208bf308e0cf31a96b3d5406e65db00b58cd4b65\
      9cc46ae8ca15542534e3a3f30ef69b4c8c435ec0c7b56cc0ee6130d0e5beeeb3\
      3c3683befd7c6bf882d72fb02b2f82e7d68da3f36404ddd3e6e1b3270fe4ec7a\
      c72bfb661a672c13f2b253acab4fbc9cead329f32edbd540f45b5dec3d76411a\
      6cdbcc3ceea277e32f51b540ef7fd188db51ace93461e7c1e68ef17defdc6301\
      52f7464f6a801ee4faa5a61fd88334d08013e2ef01743eaf88ad89f557d12821\
      4a22e44333643539b21a7477bc2f91b5441087247070b9fa96ce70f6508256d5\
      868fd5a8d5082aee432a9882afc4d63389b05470ea02099ceaebe86b5b15f019\
      9106aa085ff9608a1bf1ad19e6f4f7677c1bbad03fd17b9c3696f8e6b233faa4\
      3b73e6e501d7b48e7f02a4d235352d2c1da56082778638971e128e34eff4a4ae\
      40e745fa232990440d3c3eaac4679730e6eb15d06d3078807c82f20c79af301f\
      f251420f75f44193e2b41a267de3fde14d95b6940950b548f2be7167be1b1f21\
      3fbd3d03a04bc238889c683788c79442a4288ee2ed9c386b034d2337d1daa06c\
      c287835c8901f75977cdbbe196ff6f8fafed48c332ce6d0a6c80bf4a61aa37b6\
      56902893af189757f8701945cf72fd53f5b13a760af59395186f243e8e300227\
```

```
      d96b50ff6afed9dfe3cbb94119a403bf48680eac959c7aab8054b71f3796b977\
      a48198cc765ffb0f619e5f2eaad20c0a35ded23fcc3069adb090ee72c719b9cc\
      69059a88573f241f5b10ed0c3a81905a8de8e69f1fb4bfca3c7eaf31df7269c4\
      a9c865a293c98e8533859390caab3b73f0a1bcacf6aea39402b64d88c9feeb93\
      1e7e5fa6bbfb852139ebfec068734e8fab63c2c766f591a95c3ca6301a11bfc2\
      f9b8c8b06dc1390635c4f327672e967145370126748e831d12812480430b9635\
      4059cb879e8112d2e52262cde0bf7546e02e557f9c95b0572e8b9d250c82901d\
      b2ca02b107304be196184e2901603f302bb2270e32da6beccfb6a15ede48b6af\
      5c336d60750fe26ff9f6d5f91aebe3ba8e88a811bf496325f13ef2630cb467c6\
      019cb7a03cd5df5a3b08b2272914a06b7958919a7f86d0c3082536843202998e\
      63bb8e66b74802b08fb0c54ad8e117a4c65f8de46ee159d73ccec523a4a4a695\
      03a684c29bd47dede6b73ebbbaa57baa844a90a7786496bcb4cdd111f2efaed9\
      c580409a6c4e521b00caedb45f0e5efb45ce71a0f046af6d4917aa098554f369\
      a138a1e381d52b18081acce71292a79c23fa350b8117edc2a0cc45729d0fc0b2\
      bd718e5997c9e9020a8d8b555d8bbaed335af7bc8978547c6dda823004e5efa2\
      da88439fc1c44c3ebc9709c8d9c45de41b6562fac35b14b568610a10c17253b6\
      f72417424d601c1eb'
        },
        / ciphertext / h'3189523afc770f72fd8c287e0e58d1a17f4f43a3c035d\
      16474e06b1ac66e9c645adff5b2103e086fa767544acbc85adb'
      ]
    ]
  ])
```

Figure 47: HPKE-13-KE COSE_Encrypt (Diagnostic Notation)

NOTE: '\' line wrapping per RFC 8792

```
d8608443a10103a1054c5edd2f32c88a7ed5084ba5e9590121a89e91fbc720130044\
ea756b46c459be83a87b4ddf5d71e82e60131ecd374d81ede7a955b473e45874af6f\
8624813cc37d33d6dee98cde887a898f12263444f2eb0d01295a46e406b5e7474879\
163fa93f6ff3d053ab2c87f84bbd8712aa6b31ee6d3207c792ef8c25990e64d26067\
12523e5c4bd5a0e8573bf244255b2fa82cde8662a2dc93a334c1eba037e8ef866476\
32aab02bd883c4ff8cdbc94086e12d28584508132b6f84423b4a3fd46149ac44fbf6\
eb9ef7d057d9d3f9c170767d66afc7d1215b7d1f24acfc99f2f42e7db06567220023\
5149808fecb682f101b8526de33bc89099cfff488fae35a7eba7f254814293937318\
466afac175a37be0cf2d08d9a113bcbaf7ac034a44bf2b3e7b2e9983ea682128910a\
30c60010e0c8433181835827a20118410458201b28d7cad6a4ba7cdfceac81643186\
b3b4853d872f0d35e427b8fe98260ef2a6a1235906207649b0acc2ecaa9725a3afdd\
b317645725a4628cac13380e56983ed07f545ef9c54d551e7bf990fe66ae902498e3\
8ee50ca825eacfd0f843a2f1c1ff6585d46d14e019361e757ab65f031b00d3cd1b20\
a7c929579d37ed6af700fb3718b129376fa00ab6a91f6d4dc08218fcc5c061329d3d\
18737132cbaa3157edd2afabc8a169c7649c19da9f751fff11298bab658584e8166d\
d4b0e070f23807e74604e002dcf57b26c61503188bdeed680f937e9bdd24121c5126\
fa963cad99dde48a04dee29494860d6fa3b1709a00c13ee127f51e2ad73c2ad840ff\
33f93eee3b5ed2176c87c6314f7e98ee5b0e265576e967875f20c120fbb59a80ffa3\
df20e364b1ab5f68b76c2baa95e336a45e977413d97d7227e3777587797cf5552749\
e1e5943dbadd71f3dd9d959b3530e67611cf0c3f4f17759302cc796e0a7620cb7592\
```

```
   10b8d97b07dbb4d56cbb35dbd14c57d3936dbae0ae4ab624b150903f29250991da9f\
   8c10dc3da1bc584a61c7c455c9164cd3ab5d0453eed9a8be4bb1f8cc5dc5fb9243b2\
   18b685a93d4466af77c4925a6803edae64f9b584d932e07771511458913cc6c35e54\
   468242a89a53d1f1bdeb0f3107cc99959d5668d3c4b13c537a0897baa295506ec786\
   fc0ce0a1f669b39f6d79cba0901ea79e0c4b005491be47a52f0147bb406b289d656e\
   379c6eb69b20cdcb426eb8af207ba5864d304e90336e034e87415224a34d95d9cf12\
   06cb0c0d063362b36981c820b0cff56f81e46b0b2823a108ca1b413e063eb7af17e8\
   6ec42a481d07817325a7c917fbc12790a8dc0fdfa7f5fba208bf308e0cf31a96b3d5\
   406e65db00b58cd4b659cc46ae8ca15542534e3a3f30ef69b4c8c435ec0c7b56cc0e\
   e6130d0e5beeeb33c3683befd7c6bf882d72fb02b2f82e7d68da3f36404ddd3e6e1b\
   3270fe4ec7ac72bfb661a672c13f2b253acab4fbc9cead329f32edbd540f45b5dec3\
   d76411a6cdbcc3ceea277e32f51b540ef7fd188db51ace93461e7c1e68ef17defdc6\
   30152f7464f6a801ee4faa5a61fd88334d08013e2ef01743eaf88ad89f557d128214\
   a22e44333643539b21a7477bc2f91b5441087247070b9fa96ce70f6508256d5868fd\
   5a8d5082aee432a9882afc4d63389b05470ea02099ceaebe86b5b15f0199106aa085\
   ff9608a1bf1ad19e6f4f7677c1bbad03fd17b9c3696f8e6b233faa43b73e6e501d7b\
   48e7f02a4d235352d2c1da56082778638971e128e34eff4a4ae40e745fa232990440\
   d3c3eaac4679730e6eb15d06d3078807c82f20c79af301ff251420f75f44193e2b41\
   a267de3fde14d95b6940950b548f2be7167be1b1f213fbd3d03a04bc238889c68378\
   8c79442a4288ee2ed9c386b034d2337d1daa06cc287835c8901f75977cdbbe196ff6\
   f8fafed48c332ce6d0a6c80bf4a61aa37b656902893af189757f8701945cf72fd53f\
   5b13a760af59395186f243e8e300227d96b50ff6afed9dfe3cbb94119a403bf48680\
   eac959c7aab8054b71f3796b977a48198cc765ffb0f619e5f2eaad20c0a35ded23fc\
   c3069adb090ee72c719b9cc69059a88573f241f5b10ed0c3a81905a8de8e69f1fb4b\
   fca3c7eaf31df7269c4a9c865a293c98e8533859390caab3b73f0a1bcacf6aea3940\
   2b64d88c9feeb931e7e5fa6bbfb852139ebfec068734e8fab63c2c766f591a95c3ca\
   6301a11bfc2f9b8c8b06dc1390635c4f327672e967145370126748e831d128124804\
   30b96354059cb879e8112d2e52262cde0bf7546e02e557f9c95b0572e8b9d250c829\
   01db2ca02b107304be196184e2901603f302bb2270e32da6beccfb6a15ede48b6af5\
   c336d60750fe26ff9f6d5f91aebe3ba8e88a811bf496325f13ef2630cb467c6019cb\
   7a03cd5df5a3b08b2272914a06b7958919a7f86d0c3082536843202998e63bb8e66b\
   74802b08fb0c54ad8e117a4c65f8de46ee159d73ccec523a4a4a69503a684c29bd47\
   dede6b73ebbbaa57baa844a90a7786496bcb4cdd111f2efaed9c580409a6c4e521b0\
   0caedb45f0e5efb45ce71a0f046af6d4917aa098554f369a138a1e381d52b18081ac\
   ce71292a79c23fa350b8117edc2a0cc45729d0fc0b2bd718e5997c9e9020a8d8b555\
   d8bbaed335af7bc8978547c6dda823004e5efa2da88439fc1c44c3ebc9709c8d9c45\
   de41b6562fac35b14b568610a10c17253b6f72417424d601c1eb58303189523afc77\
   0f72fd8c287e0e58d1a17f4f43a3c035d16474e06b1ac66e9c645adff5b2103e086f\
   a767544acbc85adb
```

Figure 48: HPKE-13-KE COSE_Encrypt (Hex-Encoded CBOR)

Acknowledgments

Thanks to Ilari Liusvaara and Orie Steele for the discussion and comments.

Document History

draft-reddy-cose-hpke-pq-pqt-03

* Folded long test-vector lines using the RFC 8792 single backslash strategy

draft-reddy-cose-hpke-pq-pqt-02

* Added rationale for retaining ML-KEM-512-based ciphersuites for COSE

* Added a note that HPKE algorithm numbering is intentionally aligned with the companion JOSE registrations

draft-reddy-cose-hpke-pq-pqt-00

* Replaces draft-reddy-cose-jose-pqc-hybrid-hpke

* Removed ChaCha20Poly1305 AEAD ciphersuites

* Adapted source from draft-skokan-jose-hpke-pq-pqt-04 for COSE

* Added Filip Skokan as author

Authors' Addresses

Tirumaleswar Reddy
Nokia
Email: k.tirumaleswar_reddy@nokia.com

Hannes Tschofenig
University of the Bundeswehr Munich
Email: hannes.tschofenig@gmx.net

Filip Skokan
Okta
Email: panva.ip@gmail.com