Workgroup: Crypto Forum
Internet-Draft:
draft-connolly-cfrg-xwing-kem-01
Published: 22 January 2024
Intended Status: Informational
Expires: 25 July 2024
Authors: D. Connolly P. Schwabe
SandboxAQ MPI-SP & Radboud University
B. E. Westerbaan
Cloudflare

X-Wing: general-purpose hybrid post-quantum KEM

Abstract

This memo defines X-Wing, a general-purpose post-quantum/traditional hybrid key encapsulation mechanism (PQ/T KEM) built on X25519 and ML-KEM-768.

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://dconnolly.github.io/draft-connolly-cfrg-xwing-kem/draft-connolly-cfrg-xwing-kem.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-connolly-cfrg-xwing-kem/.

Discussion of this document takes place on the Crypto Forum Research Group mailing list (mailto:cfrg@ietf.org), which is archived at https://mailarchive.ietf.org/arch/search/?email_list=cfrg. Subscribe at https://www.ietf.org/mailman/listinfo/cfrg/.

Source for this draft and an issue tracker can be found at https://github.com/dconnolly/draft-connolly-cfrg-xwing-kem.

Status of This Memo

at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 25 July 2024.

Copyright Notice

Table of Contents

1. Introduction
  1.1. Warning: ML-KEM-768 has not been standardised
  1.2. Motivation
  1.3. Design goals
  1.4. Not an interactive key-agreement
  1.5. Not an authenticated KEM
  1.6. Comparisons
    1.6.1. With HPKE X25519Kyber768Draft00
    1.6.2. With generic combiner
2. Requirements Notation
3. Conventions and Definitions
4. Cryptographic Dependencies
5. X-Wing Construction
  5.1. Encoding and sizes
  5.2. Key generation
    5.2.1. Key derivation
  5.3. Combiner
  5.4. Encapsulation
    5.4.1. Derandomized
  5.5. Decapsulation
  5.6. Use in HPKE
  5.7. Use in TLS 1.3
6. Security Considerations
7. IANA Considerations
8. TODO
9. References
  9.1. Normative References
  9.2. Informative References
Appendix A. Test vectors # TODO: replace with test vectors that re-use ML-KEM, X25519 values

Appendix B. Acknowledgments
Appendix C. Change log
C.1. Since draft-connolly-cfrg-xwing-kem-00
Authors' Addresses

1. Introduction

1.1. Warning: ML-KEM-768 has not been standardised

X-Wing uses ML-KEM-768, which has not been standardised yet. Thus X-Wing is not finished, yet, and should not be used, yet.

1.2. Motivation

There are many choices that can be made when specifying a hybrid KEM: the constituent KEMs; their security levels; the combiner; and the hash within, to name but a few. Having too many similar options are a burden to the ecosystem.

The aim of X-Wing is to provide a concrete, simple choice for post-quantum hybrid KEM, that should be suitable for the vast majority of use cases.

1.3. Design goals

By making concrete choices, we can simplify and improve many aspects of X-Wing.

* Simplicity of definition. Because all shared secrets and cipher texts are fixed length, we do not need to encode the length. Using SHA3-256, we do not need HMAC-based construction. For the concrete choice of ML-KEM-768, we do not need to mix in its ciphertext, see Section 6.

* Security analysis. Because ML-KEM-768 already assumes QROM, we do not need to complicate the analysis of X-Wing by considering stronger models.

* Performance. Not having to mix in the ML-KEM-768 ciphertext is a nice performance benefit. Furthermore, by using SHA3-256 in the combiner, which matches the hashing in ML-KEM-768, this hash can be computed in one go on platforms where two-way Keccak is available.

We aim for "128 bits" security (NIST PQC level 1). Although at the moment there is no peer-reviewed evidence that ML-KEM-512 does not reach this level, we would like to hedge against future cryptanalytic improvements, and feel ML-KEM-768 provides a comfortable margin.

We aim for X-Wing to be usable for most applications, including specifically HPKE [RFC9180].

1.4. Not an interactive key-agreement

Traditionally most protocols use a Diffie-Hellman (DH) style non-interactive key-agreement. In many cases, a DH key agreement can be replaced by the interactive key-agreement afforded by a KEM without change in the protocol flow. One notable example is TLS [HYBRID] [XYBERTLS]. However, not all uses of DH can be replaced in a straight-forward manner by a plain KEM.

1.5. Not an authenticated KEM

In particular, X-Wing is not, borrowing the language of [RFC9180], an *authenticated* KEM.

1.6. Comparisons

1.6.1. With HPKE X25519Kyber768Draft00

X-Wing is most similar to HPKE's X25519Kyber768Draft00 [XYBERHPKE]. The key differences are:

- X-Wing uses the final version of ML-KEM-768.
- X-Wing hashes the shared secrets, to be usable outside of HPKE.
- X-Wing has a simpler combiner by flattening DHKEM(X25519) into the final hash.
- X-Wing does not hash in the ML-KEM-768 ciphertext.

There is also a different KEM called X25519Kyber768Draft00 [XYBERTLS] which is used in TLS. This one should not be used outside of TLS, as it assumes the presence of the TLS transcript to ensure non malleability.

1.6.2. With generic combiner

The generic combiner of [I-D.ounsworth-cfrg-kem-combiners] can be instantiated with ML-KEM-768 and DHKEM(X25519). That achieves similar security, but:

- X-Wing is more performant, not hashing in the ML-KEM-768 ciphertext, and flattening the DHKEM construction, with the same level of security.
- X-Wing has a fixed 32 byte shared secret, instead of a variable shared secret.

*X-Wing does not accept the optional counter and fixedInfo arguments.

2. Requirements Notation

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.

3. Conventions and Definitions

This document is consistent with all terminology defined in [I-D.driscoll-pqt-hybrid-terminology].

The following terms are used throughout this document to describe the operations, roles, and behaviors of HPKE:

*concat(x0, ..., xN): returns the concatenation of byte strings. concat(0x01, 0x0203, 0x040506) = 0x010203040506.

*random(n): return a pseudorandom byte string of length n bytes produced by a cryptographically-secure random number generator.

4. Cryptographic Dependencies

X-Wing relies on the following primitives:

*ML-KEM-768 post-quantum key-encapsulation mechanism (KEM) [MLKEM]:

-ML-KEM-768.KeyGen(): Randomized algorithm to generate an ML-KEM-768 key pair (pk_M, sk_M) of an encapsulation key pk_M and decapsulation key sk_M. Note that ML-KEM-768.KeyGen() returns the keys in reverse order of GenerateKeyPair() defined below.

-ML-KEM-768.Encaps(pk_M): Randomized algorithm to generate (ss_M, ct_M), an ephemeral 32 byte shared key ss_M, and a fixed-length encapsulation (ciphertext) of that key ct_M for encapsulation key pk_M.

-ML-KEM-768.Decap(ct_M, sk_M): Deterministic algorithm using the decapsulation key sk_M to recover the shared key from ct_M.

To generate deterministic test vectors, we also use

-ML-KEM-768.KeyGenDerand(seed): Same as ML-KEM-768.KeyGen(), but derandomized as follows. seed is 64 bytes. seed[0:32] is

used for z (line 1 algorithm 15), and seed[32:64] is used for d (line 1 algorithm 12).

- ML-KEM-768.EncapsDerand(pk_M, seed): Same as ML-KEM-768.Encaps() but derandomized as follows. seed is 32 bytes and used for m (line 1 algorithm 16).

* X25519 elliptic curve Diffie-Hellman key-exchange defined in Section 5 of [RFC7748]:

  - X25519(k,u): takes 32 byte strings k and u representing a Curve25519 scalar and curvepoint respectively, and returns the 32 byte string representing their scalar multiplication.

  - X25519_BASE: the 32 byte string representing the standard base point of Curve25519. In hex it is given by 0900000000000000000000000000000000000000000000000000000000000000.

Note that 9 is the standard basepoint for X25519, cf Section 6.1 of [RFC7748].

* Symmetric cryptography.

  - SHAKE128(message, outlen): The extendable-output function (XOF) defined in Section 6.2 of [FIPS202].

  - SHA3-256(message): The hash defined in defined in Section 6.1 of [FIPS202].

5. X-Wing Construction

5.1. Encoding and sizes

X-Wing encapsulation key, decapsulation key, ciphertexts and shared secrets are all fixed length byte strings.

Decapsulation key (private): 2464 bytes

Encapsulation key (public): 1216 bytes

Ciphertext: 1120 bytes

Shared secret: 32 bytes

5.2. Key generation

An X-Wing keypair (decapsulation key, encapsulation key) is generated as follows.

```
def GenerateKeyPair():
  (pk_M, sk_M) = ML-KEM-768.KeyGen()
  sk_X = random(32)
  pk_X = X25519(sk_X, X25519_BASE)
  return concat(sk_M, sk_X, pk_X), concat(pk_M, pk_X)
```

GenerateKeyPair() returns the 2464 byte secret encapsulation key sk and the 1216 byte decapsulation key pk.

5.2.1. Key derivation

For testing, it is convenient to have a deterministic version of key generation. An X-Wing implementation **MAY** provide the following derandomized variant of key generation.

```
def GenerateKeyPairDerand(seed):
  (pk_M, sk_M) = ML-KEM-768.KeyGenDerand(seed[0:64])
  sk_X = seed[64:96]
  pk_X = X25519(sk_X, X25519_BASE)
  return concat(sk_M, sk_X, pk_X), concat(pk_M, pk_X)
```

seed must be 96 bytes.

GenerateKeyPairDerand() returns the 2464 byte secret encapsulation key sk and the 1216 byte decapsulation key pk.

5.3. Combiner

Given 32 byte strings ss_M, ss_X, ct_X, pk_X, representing the ML-KEM-768 shared secret, X25519 shared secret, X25519 ciphertext (ephemeral public key) and X25519 public key respectively, the 32 byte combined shared secret is given by:

```
def Combiner(ss_M, ss_X, ct_X, pk_X):
  return SHA3-256(concat(
    XWingLabel,
    ss_M,
    ss_X,
    ct_X,
    pk_X
  ))
```

where XWingLabel is the following 6 byte ASCII string

```
XWingLabel = concat(
    "\./",
    "/^\",
)
```

5.4. Encapsulation

Given an X-Wing encapsulation key pk, encapsulation proceeds as follows.

```
def Encapsulate(pk):
  pk_M = pk[0:1184]
  pk_X = pk[1184:1216]
  ek_X = random(32)
  ct_X = X25519(ek_X, X25519_BASE)
  ss_X = X25519(ek_X, pk_X)
  (ss_M, ct_M) = ML-KEM-768.Encaps(pk_M)
  ss = Combiner(ss_M, ss_X, ct_X, pk_X)
  ct = concat(ct_M, ct_X)
  return (ss, ct)
```

pk is a 1216 byte X-Wing encapsulation key resulting from GeneratePublicKey()

Encapsulate() returns the 32 byte shared secret ss and the 1120 byte ciphertext ct.

5.4.1. Derandomized

For testing, it is convenient to have a deterministic version of encapsulation. An X-Wing implementation **MAY** provide the following derandomized function.

```
def EncapsulateDerand(pk, seed):
  pk_M = pk[0:1184]
  pk_X = pk[1184:1216]
  ek_X = seed[32:64]
  ct_X = X25519(ek_X, X25519_BASE)
  ss_X = X25519(ek_X, pk_X)
  (ss_M, ct_M) = ML-KEM-768.EncapsDerand(pk_M, seed[0:32])
  ss = Combiner(ss_M, ss_X, ct_X, pk_X)
  ct = concat(ct_M, ct_X)
  return (ss, ct)
```

pk is a 1216 byte X-Wing encapsulation key resulting from GeneratePublicKey() seed **MUST** be 64 bytes.

EncapsulateDerand() returns the 32 byte shared secret ss and the 1120 byte ciphertext ct.

5.5. Decapsulation

```
def Decapsulate(ct, sk):
  ct_M = ct[0:1088]
  ct_X = ct[1088:1120]
  sk_M = sk[0:2400]
  sk_X = sk[2400:2432]
  pk_X = sk[2432:2464]
  ss_M = ML-KEM-768.Decapsulate(ct_M, sk_M)
  ss_X = X25519(sk_X, ct_X)
  return Combiner(ss_M, ss_X, ct_X, pk_X)
```

ct is the 1120 byte ciphertext resulting from Encapsulate() sk is a 2464 byte X-Wing decapsulation key resulting from GenerateKeyPair()

Decapsulate() returns the 32 byte shared secret.

5.6. Use in HPKE

X-Wing satisfies the HPKE KEM interface as follows.

The SerializePublicKey, DeserializePublicKey, SerializePrivateKey and DeserializePrivateKey are the identity functions, as X-Wing keys are fixed-length byte strings, see Section 5.1.

DeriveKeyPair() is given by

```
def DeriveKeyPair(ikm):
  return GenerateKeyPairDerand(SHAKE128(ikm, 96))
```

where the HPKE private key and public key are the X-Wing decapsulation key and encapsulation key respectively.

The argument ikm to DeriveKeyPair() **SHOULD** be at least 32 octets in length. (This is contrary to [RFC9180] which stipulates it should be at least Nsk=2432 octets in length.)

Encap() is Encapsulate() from Section 5.4.

Decap() is Decapsulate() from Section 5.5.

X-Wing is not an authenticated KEM: it does not support AuthEncap() and AuthDecap(), see Section 1.5.

Nsecret, Nenc, Npk, and Nsk are defined in Section 7.

5.7. Use in TLS 1.3

For the client's share, the key_exchange value contains the X-Wing encapsulation key.

For the server's share, the key_exchange value contains the X-Wing ciphertext.

6. Security Considerations

Informally, X-Wing is secure if SHA3 is secure, and either X25519 is secure, or ML-KEM-768 is secure.

More precisely, if SHA3-256, SHA3-512, SHAKE-128, and SHAKE-256 may be modelled as a random oracle, then the IND-CCA security of X-Wing is bounded by the IND-CCA security of ML-KEM-768, and the gap-CDH security of Curve25519, see [PROOF].

The security of X-Wing relies crucially on the specifics of the Fujisaki-Okamoto transformation used in ML-KEM-768. In particular, the X-Wing combiner cannot be assumed to be secure, when used with different KEMs.

7. IANA Considerations

This document requests/registers a new entry to the "HPKE KEM Identifiers" registry.

Value: TBD (please)

KEM: X-Wing

Nsecret: 32

Nenc: 1120

Npk: 1216

Nsk: 2464

Auth: no

Reference: This document

Furthermore, this document requests/registers a new entry to the TLS Named Group (or Supported Group) registry, according to the procedures in Section 6 of [TLSIANA].

Value: TBD (please)

Description: X-Wing

DTLS-OK: Y

Recommended: Y

Reference:
This document

Comment: PQ/T hybrid of X25519 and ML-KEM-768

8. TODO

*Which validation do we want to require?

9. References

9.1. Normative References

[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>.

9.2. Informative References

[FIPS202] National Institute of Standards and Technology, "FIPS 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions", n.d., <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf>.

[HYBRID] Stebila, D., Fluhrer, S., and S. Gueron, "Hybrid key exchange in TLS 1.3", Work in Progress, Internet-Draft, draft-stebila-tls-hybrid-design-03, 12 February 2020, <https://datatracker.ietf.org/doc/html/draft-stebila-tls-hybrid-design-03>.

[I-D.driscoll-pqt-hybrid-terminology]
D, F., "Terminology for Post-Quantum Traditional Hybrid Schemes", Work in Progress, Internet-Draft, draft-driscoll-pqt-hybrid-terminology-02, 7 March 2023, <https://datatracker.ietf.org/doc/html/draft-driscoll-pqt-hybrid-terminology-02>.

[I-D.ounsworth-cfrg-kem-combiners] Ounsworth, M., Wussler, A., and S. Kousidis, "Combiner function for hybrid key encapsulation mechanisms (Hybrid KEMs)", Work in Progress, Internet-Draft, draft-ounsworth-cfrg-kem-

combiners-04, 8 July 2023, <https://datatracker.ietf.org/doc/html/draft-ounsworth-cfrg-kem-combiners-04>.

[MLKEM] National Institute of Standards and Technology, "FIPS 203 (Initial Draft): Module-Lattice-Based Key-Encapsulation Mechanism Standard", n.d., <https://csrc.nist.gov/pubs/fips/203/ipd>.

[PROOF] Barbosa, M., Connolly, D., Duarte, J., Kaiser, A., Schwabe, P., Varner, K., and B. E. Westerbraan, "X-Wing: The Hybrid KEM You've Been Looking For", n.d., <https://eprint.iacr.org/2024/039>.

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

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

[TLSIANA] Salowey, J. A. and S. Turner, "IANA Registry Updates for TLS and DTLS", Work in Progress, Internet-Draft, draft-ietf-tls-rfc8447bis-08, 23 January 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-rfc8447bis-08>.

[XYBERHPKE] Westerbaan, B. and C. A. Wood, "X25519Kyber768Draft00 hybrid post-quantum KEM for HPKE", Work in Progress, Internet-Draft, draft-westerbaan-cfrg-hpke-xyber768d00-02, 4 May 2023, <https://datatracker.ietf.org/doc/html/draft-westerbaan-cfrg-hpke-xyber768d00-02>.

[XYBERTLS] Westerbaan, B. and D. Stebila, "X25519Kyber768Draft00 hybrid post-quantum key agreement", Work in Progress, Internet-Draft, draft-tls-westerbaan-xyber768d00-03, 24 September 2023, <https://datatracker.ietf.org/doc/html/draft-tls-westerbaan-xyber768d00-03>.

Appendix A. Test vectors # TODO: replace with test vectors that re-use ML-KEM, X25519 values

seed

7f9c2ba4e88f827d616045507605853ed73b8093f6efbc88eb1a6eacfa66ef263cb1ee
88004b93103cfb0aeefd2a686e01fa4a58e8a3639ca8a1e3f9ae57e235b8cc873c23dc
b8d260169afa2f75ab916a58d974918835d25e6a435085b2

sk

24c59d1c7603e7b74bc7aa1bc2cb3a214b3cfaebb63bd85b65408427c498ba394371bb
1f92a3b506b81d54a95a7c0ddfbaa1519553d6f3cd5a601b7db6b0e91a5149468f1f68
26478bf3c6670e093ac4c49e7a90ba46595de94c50e04129a811a841b39534a87f0ae7
116553e20c9a566b9b8ff7c7e728b8b201893403a4f252a55230874c256b897834cda3
807b25cbd75a30867bfb80328200017f1cb70b56cc546b65d3dc9cdb45107cf10dba34
19043ac35c0b9546309a239039813ed5c40f353a5e8e42193564496112bda56cb38c08
f252ae9c2c7e441a062e92a7c8da7a240c9952d86b5f1bb6a53b38a5ac0a54a84b43f1
a1d0525655684a12090b60b28b0c628db092015547d1070af5d6192e639636615d03c6
bb90008ca15b784119f6178a00d7bef4a54a274ac922e55c61a3a8840aa258639484a3
e2e43b6c969b11275631daa129a61ea0e2939f0877e1a110c8a44b24c54fbb07a958db
eeca1eb52b086c87bf43a9b02a5b2c4762117c3a99ae4c4e2eaa7a33b9a714737215c1
17514f6c4299ef92acd64c4858e85ce737a801890022d7381f3540230c0c8ef50a848a
b09ba0bf8b50619c905751601d7629767449c9c0b2bae321f438a77f412a55e45ecab4
9053c6561801c639be6495be8fa144ef6029af663407ca9181946de5f3aec7236343ab
c5a38a09c01b412baf0afb23f9e9b8f2b40810f2ce4ffbcdbfd87972323e98065160bc
34b3afd6c25b664745fca99a9ea75cef019d768485ec23336d9b39e4d05d8d587b3063
4f69ade5753a39680235e44f27995da96798f3a85e184a9fad19320829629f4140417b
dbf5851ab79258134146d088452774991a087a1c2beaea89f218087ba774ae253b494c
750b1de04b44d953c5e47ab10f65205ee212f9c30391e5299553954916873a0b411645
e801c0b099cb44f48995675823c10b40f4bbac9177a558ca0c30765c2aabfd6a4da54c
13e33902d63f064330f0464982429de2604cd03b4de84a9f821a5470423a40a964dcc4
63363d77b02c3127304f942ee71c98c643a427533ef300104948b825277953aaabfd85
88f75a77d199a213ad348116e9e539f6d37068a551c710548b7a2c7ee95f9cd9b34833
673cc44bcb18a778a49455c768e0b340f81102ac6b76b064057151ef101ae143787f54
53558df8035a3ce00c9c43cda43142cca39034b09a7e6089867b4c64980a69ecab2e68
724c35cb909d5d45bc6a349c71b306567664adc0cc8ef698049b4b4b432dd0f69fac07
0f77c4f79b22bb90cb97b341880716853431694c9120f6724ad58d57127fced999ff62
a5d4c3c240129cc812acc73698f949d8e73661f2528262bfccfa5cdf5a2104649806e2
ea161217083365aa26cee6ae2f1356e8e1c5cefcc85703447ef1160a1b4a0e8c017b17
02c66c88ab70d39a6c96c1569d5a86245a7eeb087d682219080768745b44bf244f65b5
b2658dbae6962ba52b322118e214cfadd7cf3502582dc9cafba952a9637ad360071025
78d99d23f8235da90791604b4f0a4f7640680f59b633d93dfb84282ba54c674b115684
1bc331b659a61a04883d0c5ebbc0772754a4c33b6a90e52e0678ce06a0453ba8a188b1
496bae6a24177b636d12fbb088f2cd9504ac200231473031a31a5c62e46288fb3edb85
21bc0ea59a212fd1c6dba09e920712d068a2be7abcf4f2a3533443ee1780dd419681a9
cd90af5fcaab8c1552ef25572f157a2bbb934a18a5c57a761b54a45d774ac6bc593583
bcfc4dcd0cca87ab9cff463dc5e80ebbb501d18c8b39e324dbd07ca06cbf75ba33297a
c7aabdd5b308401ba387f533f3927b51e91380f5a59b119e354835ab182db62c76d6d8
a63241743a52012aac281222bc0037e2c493b4777a99cb5929aba155a006bc9b461c36
a3583fac5414b403af9135079b33a10df8819cb462f067253f92b3c45a7fb1c1478d40
e39010ba44071019010daa15c0f43d14641a8fa3a94cfaa2a877ae8113bbf8221ee132
376494fb128b825952d5105ae4157dd6d70f71d5bd48f34d469976629bce6c12931c88
0882965e27538f272b19796b251226075b131b38564f90159583cd9c4c3c098c8f06a2
b262b8731b9e962976c41152a76c30b502d0425635357b43cd3a3ecef5bc9910bb89ca

91ba75e8121d53c2329b5222df12560d242724523ff60b6ead310d99954d483b91383a
6a937f1b60b474b22ea5b81954580339d81c9f47bab44a3fe0c833a7dba1f5b33a5a2a
9812645c6537c2317163d71b7bd7a4a5459a28a1c28659aad9a1ca9a99a363062d4533
108445a673438e77624e73757c1a84d031cf0fb24b1187aafbe6738e9abaf5b42b004b
a0d96426d3c5324235dd871e7a89364d335ebb6718ad098154208b143b2b43eb9e5fd8
6c5225d494b40809b2459903c6486a1db9ac3414945e1867b5869c2f88cf9edc0a2166
804578d34923e5a353babba923db907725b384e74e66987292e007e05c6766f267f839
617c55e28b0fa2121da2d037d6830af9d869e1fb52b0cb645fe221a79b2a46e41980d3
71ccc58d8756054b2cca7b13715a05f3925355cca838ab8d2425255f61135727167ad6
b0632ebf86384b950ad21088c292b4a4fcc0e59c42d3f77fac85cd9f5cb049b3a29505
84c4c6ac98ca3d0a8f30d2b1bd9815b94b27051b40ffc3455a668b9e141428611b280c
8f2b55f6eb04e10c68f1340ef1582115f10ee2b785b7ebb0ec3a0c61670cf48107b594
6e238e0d68961b47983b87879771519d2b7c21681cd494b420f03d004bb06eeb54f9c0
c2f2aff6759074d5b3a3b11c73f1af6dc874eeec254d5409fceaa90ff66d90b6930a54
d1d9be1844af1d861ff96a611a414a6c61a78fb2a78e74383ab05ebc73855a818a6272
d523a3e2a35ab4285b4a2564f76772aaf8cdc9f87c65f1b4b5819905fb4f9ea59166fb
b201c5eefc0df7418ca211b5b079a511b8b94429847b537fbed82d57632d63e815d821
8a280d43328604a6c4d2c1887e7ab061f120a0168db2f4735369b193780f0aeb381ff2
3f3b46e206afe77a7e814c7716a1b166727dd2a0b9a7d8aeace425da63977f8103457c
438a2676c10e3a9c630b855873288ee560ca05c37cc7329e9e502cfac918b942054444
4cfa93f56ee922c7d660937b5937c3074d62968f006d1211c60296685953e5def3804c
ad5c36180137c1df12f31385b670fde5cfe76447f6c4b5b50083553c3cb1eea988004b
103cfb0aeefd2a686e01fa4a58e8a3639ca8a1e3f9ae57e235b8cc873c23dc62b8d260
9afa2f75ab916a58d974918835d25e6a435085b2e56f17576740ce2a32fc5145030145
b97e63e0e41d354274a079d3e6fb2e15

pk

1bc331b659a61a04883d0c5ebbc0772754a4c33b6a90e52e0678ce06a0453ba8a188b1
496bae6a24177b636d12fbb088f2cd9504ac200231473031a31a5c62e46288fb3edb85
21bc0ea59a212fd1c6dba09e920712d068a2be7abcf4f2a3533443ee1780dd419681a9
cd90af5fcaab8c1552ef25572f157a2bbb934a18a5c57a761b54a45d774ac6bc593583
bcfc4dcd0cca87ab9cff463dc5e80ebbb501d18c8b39e324dbd07ca06cbf75ba33297a
c7aabdd5b308401ba387f533f3927b51e91380f5a59b119e354835ab182db62c76d6d8
a63241743a52012aac281222bc0037e2c493b4777a99cb5929aba155a006bc9b461c36
a3583fac5414b403af9135079b33a10df8819cb462f067253f92b3c45a7fb1c1478d40
e39010ba44071019010daa15c0f43d14641a8fa3a94cfaa2a877ae8113bbf8221ee132
376494fb128b825952d5105ae4157dd6d70f71d5bd48f34d469976629bce6c12931c88
0882965e27538f272b19796b251226075b131b38564f90159583cd9c4c3c098c8f06a2
b262b8731b9e962976c41152a76c30b502d0425635357b43cd3a3ecef5bc9910bb89ca
91ba75e8121d53c2329b5222df12560d242724523ff60b6ead310d99954d483b91383a
6a937f1b60b474b22ea5b81954580339d81c9f47bab44a3fe0c833a7dba1f5b33a5a2a
9812645c6537c2317163d71b7bd7a4a5459a28a1c28659aad9a1ca9a99a363062d4533
108445a673438e77624e73757c1a84d031cf0fb24b1187aafbe6738e9abaf5b42b004b
a0d96426d3c5324235dd871e7a89364d335ebb6718ad098154208b143b2b43eb9e5fd8
6c5225d494b40809b2459903c6486a1db9ac3414945e1867b5869c2f88cf9edc0a2166
804578d34923e5a353babba923db907725b384e74e66987292e007e05c6766f267f839
617c55e28b0fa2121da2d037d6830af9d869e1fb52b0cb645fe221a79b2a46e41980d3
71ccc58d8756054b2cca7b13715a05f3925355cca838ab8d2425255f61135727167ad6
b0632ebf86384b950ad21088c292b4a4fcc0e59c42d3f77fac85cd9f5cb049b3a29505
84c4c6ac98ca3d0a8f30d2b1bd9815b94b27051b40ffc3455a668b9e141428611b280c

```
  8f2b55f6eb04e10c68f1340ef1582115f10ee2b785b7ebb0ec3a0c61670cf48107b594
  6e238e0d68961b47983b87879771519d2b7c21681cd494b420f03d004bb06eeb54f9c0
  c2f2aff6759074d5b3a3b11c73f1af6dc874eeec254d5409fceaa90ff66d90b6930a54
  d1d9be1844af1d861ff96a611a414a6c61a78fb2a78e74383ab05ebc73855a818a6272
  d523a3e2a35ab4285b4a2564f76772aaf8cdc9f87c65f1b4b5819905fb4f9ea59166fb
  b201c5eefc0df7418ca211b5b079a511b8b94429847b537fbed82d57632d63e815d821
  8a280d43328604a6c4d2c1887e7ab061f120a0168db2f4735369b193780f0aeb381ff2
  3f3b46e206afe77a7e814c7716a1b166727dd2a0b9a7d8aeace425da63977f8103457c
  438a2676c10e3a9c630b855873288ee560ca05c37cc7329e9e502cfac918b942054444
  4cfa93f56ee922c7d660937b5937c3074d62968f006d1211c60296685953e5dee56f17
  6740ce2a32fc5145030145cfb97e63e0e41d354274a079d3e6fb2e15
eseed
  badfd6dfaac359a5efbb7bcc4b59d538df9a04302e10c8bc1cbf1a0b3a5120ea17cda7
  ad765f5623474d368ccca8af0007cd9f5e4c849f167a580b14aabdef
ct
  718ad10318b367fc4390f63147fa5250ef61b65384a563f2c7951b2d45881fcf9f446d
  4443417eed0c001e635a994cda366f118bdd1cf0be0417abd1b615cc669e1b949280e2
  52d3d5035c6420ff6c943421ee7589e681828c95942d4f9968f32b9ad30cccff0d98fa
  b187164530dc83f9cde75ab1958c22dbff8af921c9ebc678a658b69663f72e7c1632b6
  8ddcbc6c8a06c3316b1aefdd07989ef944fc51406e12db6865344e03f447520d50c93f
  1513d80cbc836950e2b52f424bb46155ba4c2e21ec5dff762bf7e92e54e0fb7618e730
  607ba03b1de16f109e22dd5832a7eadfeb2ef00244bbaf930106cbcd2ab008f468de6d
  632e9e225091a010e361ce751d633e6c37ba2530bca6fbe9d2e5348e4e168e15492299
  ef45a265ec649ce21480504b609ad5f1b0b094b74d55aaea60b8f71398cd9340802e91
  5937ffaa482c6678f8421c63583e8acd8d00bf285b52a26fa577aed109acd94ef75595
  aa378f87283a7ee94af98e21a6fbac8802336ff980e15e498042a8148b69e1d8aab0b7
  6d0b885f9a57c1ea83efcce8dccfee076dbc2f9c074525ed4e7472c3e09a9f1c50ff51
  50159c1be7730686c04e46368e37f2e8c82b8436463445b0edaefab876731497abcc56
  1978eac34cf73b5b213549d1f74271d48f6a085155acd8d7db739ce6e70ad25ee63623
  4151725d55ea781d483e54850e1ebda401276616e7a62b22efa2e3098a006dfacaa1fc
  4ade6a119f3a215b523210164a7f299d2c7b8ad8a637bc1fba56de28ffa800b522246d
  c7148ced56ed292c7d92004065598bc573dd30259d84b6d923d2769ce260cdab0ad176
  ef7388c020b8e8bcd055232a7240fe2fa4fcbeadbc46366aa47729f5502dbfee8a623a
  ec6f6020013aeff975f255b597a11eed1335457b9903da42a27a39fdb0edbb11742e4e
  1c833b7952d3fd28f428eecb6f78b99ff0a5eb097793f78f1a70612811766fcbe0f9aa
  a4afd8a364f5584333d8a4cdc096a3762ea6cce70dfa42967f5a7c2dbef688b37885fa
  220dc800bcb1ae83d35ffca54a6dabba730764d60b1a4a506206efa380d7d1d8906977
  082bb92396af4547024797797e01c927c78c9f70750ef2002dfe1516baa4f165a31769
  d35d9527f4b33505484130cd573f9d4a1f1e6656aff881aab482fb3d6151ab02f76267
  3f3feb9718fbfed05a9b69a8d817a7e4a41efbe3ffeb355d1013778f14d4c30c92a386
  0fa23b388feddc635b22d8fa4998b65d483cd3b595553092123e144c49d91ddc2f7a88
  ef1ad2b0b19636bc3f50f61ea5157c73a1a5b956349b6cdf3ff50ec9ef7cbc1137b27d
  39276a3ed4e778c505206669686ef038b5808117fedf60ef3598e8ed1db1e5ad64f04a
  8e60e82fe04bc75594fd9fcd8bb79237adb9c9ffd3dc2c907345f874aec7055576a322
  486120ff62ad690a988919e941d33ed93706f6984032e205084cc46585b5aef035c22d
  b3b0ba04e83f80c1b06b4975f00207b357550d24405189412ea6a83ad56c4873f499fd
  c761aa72
ss     2fae7214767890c4703fad953f5e3f91303111498caa135d77cde634151e71b5
```

seed

aee7eef47cb0fca9767be1fda69419dfb927e9df07348b196691abaeb580b32def5853
8d23f87732ea63b02b4fa0f4873360e2841928cd60dd4cee8cc0d4c922a96188d03267
8ac850933c7aff1533b94c834adbb69c6115bad4692d8619

sk

89722dd1c8829af93f6e5405ecd93a5aaabcb9264aafc363d731bb4f276021b0c06826
3022ae1e85acc6679ccb583a37ba4d30e0564ae6421ab1b5c2374a058cb6bca4050ce1
d5c51bcc90be82454b332aa21069623d8a8b393a2c2b6cb5bffc55ae369614a77d9bc9
d47496ab21239bb7691ac65494225889b7b45ba10b0aac10c3c41fa7a4a51fa14d3e92
d364be59ba7d9d4592944968e97a2d947868a0624a97a9c8ad226d81a12a17777eafaa
e30436a5c743003078d830734ec97e6a625f6d9c10f9da3f956b5583578478e6311f27
9d6188ede84510442c9f556696378faa622b1e935be62c733da96b023c31b2ba6abfbc
748088251042d46559bf132d2a43b7690cb4666722ebc53849843125f9a900aa476af4
b7b410f18300f048ce26dc7f35b50f7eb5bccf23c95b7c0064e92662eb22927359df1b
ce43ce014384ae68822f4c3f64583643355c6746290d224a70c818158884e2aa8f15e1
09100848255c277144f051ab8b40775c297cafb238cdb70e8ce687c9e195d0823b3903
e245852ca99c079211161a79409247ae721a59b358ef097ed8dc386f982d36a9220c35
eacb3674f671f171afb0d14f0890c0c7f77d06f7c61ca83a15974083e72678f180f35c
aa633166d429432599f9d9432fe791318ab14a3988496a14c2417e03990136e91aa3a8
085abbc4aa0c38a45e7e009f3577739172396f7b7e61734eaacc5b484971e9a9384b58
dff9307a98222a3813f9269fe793b7ef582ab8c36feaf447d3136285f76d5f46314135
73650441e092dc73bcf483cb1f2944016936db2a34b743830cb890e85660acd077ea51
7e664df7ab803c9b0c96e143b4f5788311a841b76be728aea60270104564575bb723f5
acaab5e379c3cdd97bdac84ad6738587bcbbdf1c66a0da65f87a673f840e1d7c5a722a
5568429ae36cdde9cd54ac3d4a94c4c6508361984e1c211771998641816fa392a4ffb9
64381a84900eb52502f04816a3d70090b55ee2d3b7f3d459af4008ec8c1b19c08d1284
fdc81508647ecb9b45e65c084d456f9fa87a68f26bc05b4e8415887b602ff28b28e412
7ff9019a90ac21c7c4ae9670a538a2bd2604616689b034c33cb1cc9d634eb37c8d4d46
40e335582b539d3215bf70960cc1c0b11011449c2a09265101f55366dc0213a6411288
76c3a223b19cf6951b5968452aa7b839370646db5eee1893346a58c116133dbc8fc1c5
34e04cda171b041c0133563a682855a9cb18896c6179ac2eac83c70547942e54b2e133
f68450f4f4b14bda3af5f129b3e292c6a676aa0b7a045c7251e315ca3707ff23bec349
50d49718560b2ff66cbd49c848b4036c2186a0315c4e6a32f3035207a48651891f50ec
0eb19d13e90457611e0c7ccdf012a3e19412d8c1563f1ab22b39859b27a7bcac72cbf2
3c666deb401e4239603645872b997673b6205d97cdd68b0a782742e62c24ad74626108
e3c95f49dbb8172c05f3f2414e63652c3b358d603e867173e03203af06a26bb0bfc0b5
118b6fd99613a160829b04475374b8214859bcc316f4e06a84f264ec3cb513f66b71ac
3d135aa589198cb02113cc17e13a0f15fc1d3d734966c3751a74ac27c781323043e363
dca9a2af6508bdba0260662691426d1d8899cd77736c21b17eb3a31fc118154264e2b1
22c506b7803b1f4b25d178b688b641d0943185107eed18b228e8b68753a8d75a77f29b
5e97abd028354ce4cd6961797a757c4ff44aeea2c0a16cbfdcb07314fb3e64d7c26a4c
5782a2ee198d73e7bf05eb85bd420cee20ac24c36613d6bd0c53133443527c32bd0f8b
3be9918c7caea71748de6bacfa27710845ad0b528c087349e9faa3c83869e1d0ac9267
4dba1dc3434976f60b59d443bad51e87d974c9f747b76017bd17021c24246a9987db1b
8562bf665b41fb153c0ba675cac593b990ce595a7851fa18ea345bf20c352486253254
05e5c69daa0dc4f2b24704338e29144d653657d47a20f39ed2b1174cb3120ed1590e4a
32579dc2da9f12f6c07ec7a31963208faa5c758615713965b9d5661860cfe5652d7423
2ce9b696ea9e45305a28d84c082709d2238bbc849b6b3cac64b78b532995af6b4ce988
9149a5ae083320624e3b54851d48a6f24266258a0a14d342e4ca3133c33c5e16ad91b2

521100076527cefc5f0417b332463c5c5c52dc4b00a2d29959109244d2810839a310cb
f282503d5cbf3f0cbe3e68873407b7e5e960ca214709919b65301da2b3a7e488205a3a
5f24cd61d18c757040b14a4e80e8c09e74a9a71265ed213a91da6d7a8655de3b4a8312
e2e66cb673733e3717d99023a6683712767ab2da9b54a26dd3b695a80b54226a1a967b
c3f76e679914470803bc6805a6b4b1b78261259acd8f703dd10ba6e8e1a00dd94e7741
d13103253cb70edab948c38072629b949261b7c439445bc498444e86b6a9a7da8b1530
0bf2939532a8e7ea84ea0b5c6db5335e826aa0325b536ccc21d943890b2c2a5c44f337
2355867be87965175f2dbbb0aba89f9311b0873a15db6a4128682a8bca019a04a351a0
646868f9bbb6f8d0bea3db0865f1239b16c93ca09d19857d747abfc846b27dd77ee5d4
fab5ce949635e7d34ec1b9546aea75df571cfed74b7112218e4153e7f6a7a3a910ec4c
1576b3bb27c29852746e645fa501b0642678aefa2209c745939a2ab000033862b88e70
e7e25ec1e3cd379b54bc457a85d9af0680160c57b3a4e90308bc28b8da13ac0c563c55
9a88bd90b51f691525e50a260a0507a2174447ea93f5d5acec6c16a5d7909e275f612c
283310e8124d28f18000f811fb929e03f30d1472644851bcb73c4af6b095acd7328a07
e9187a836a15307c6076210c9b410493505bc4814e3c327386796c5932c8cab7a695b9
ac24561b2a9657c3157531ba3cba699b6424fda24cc6c72edac1a6bf091b87c3c594c9
d24a1126f998aee120ae372a27a268a0c76ab8f84957f461e7c04dd2d59f0f217d9e07
8990533b16bbc125b2737a1a7e1cc1ed7c47e8f8464ba78c5d3298f2dc7d0be944ad29
7ec774ad1b1f1485b114a9a9b93c488c89c0c7609f2bf9533c2929f667bca8b68999e3
54597cf83ba7450b237188c3364172c1351bd349a699672d31b9598bab79a18b3d8cb2
5f53c0b22bfa065690a16184db4f9731cea1a08f5876ec187e7b1ae79c593415d06883
5ce0bf2c28b1e389ae4a768f871b2761a29178a51845eb0b939f0ee9ef58538b8d23f8
32ea63b02b4fa0f4873360e2841928cd60dd4cee8cc0d4c922a96188d032675c8ac850
3c7aff1533b94c834adbb69c6115bad4692d8619c7dd2bf4e3b5b93f77f4576d55d300
9e75e14084b0bc85620499bf468ae161

pk

3d135aa589198cb02113cc17e13a0f15fc1d3d734966c3751a74ac27c781323043e363
dca9a2af6508bdba0260662691426d1d8899cd77736c21b17eb3a31fc118154264e2b1
22c506b7803b1f4b25d178b688b641d0943185107eed18b228e8b68753a8d75a77f29b
5e97abd028354ce4cd6961797a757c4ff44aeea2c0a16cbfdcb07314fb3e64d7c26a4c
5782a2ee198d73e7bf05eb85bd420cee20ac24c36613d6bd0c53133443527c32bd0f8b
3be9918c7caea71748de6bacfa27710845ad0b528c087349e9faa3c83869e1d0ac9267
4dba1dc3434976f60b59d443bad51e87d974c9f747b76017bd17021c24246a9987db1b
8562bf665b41fb153c0ba675cac593b990ce595a7851fa18ea345bf20c352486253254
05e5c69daa0dc4f2b24704338e29144d653657d47a20f39ed2b1174cb3120ed1590e4a
32579dc2da9f12f6c07ec7a31963208faa5c758615713965b9d5661860cfe5652d7423
2ce9b696ea9e45305a28d84c082709d2238bbc849b6b3cac64b78b532995af6b4ce988
9149a5ae083320624e3b54851d48a6f24266258a0a14d342e4ca3133c33c5e16ad91b2
521100076527cefc5f0417b332463c5c5c52dc4b00a2d29959109244d2810839a310cb
f282503d5cbf3f0cbe3e68873407b7e5e960ca214709919b65301da2b3a7e488205a3a
5f24cd61d18c757040b14a4e80e8c09e74a9a71265ed213a91da6d7a8655de3b4a8312
e2e66cb673733e3717d99023a6683712767ab2da9b54a26dd3b695a80b54226a1a967b
c3f76e679914470803bc6805a6b4b1b78261259acd8f703dd10ba6e8e1a00dd94e7741
d13103253cb70edab948c38072629b949261b7c439445bc498444e86b6a9a7da8b1530
0bf2939532a8e7ea84ea0b5c6db5335e826aa0325b536ccc21d943890b2c2a5c44f337
2355867be87965175f2dbbb0aba89f9311b0873a15db6a4128682a8bca019a04a351a0
646868f9bbb6f8d0bea3db0865f1239b16c93ca09d19857d747abfc846b27dd77ee5d4
fab5ce949635e7d34ec1b9546aea75df571cfed74b7112218e4153e7f6a7a3a910ec4c
1576b3bb27c29852746e645fa501b0642678aefa2209c745939a2ab000033862b88e70

```
  e7e25ec1e3cd379b54bc457a85d9af0680160c57b3a4e90308bc28b8da13ac0c563c55
  9a88bd90b51f691525e50a260a0507a2174447ea93f5d5acec6c16a5d7909e275f612c
  283310e8124d28f18000f811fb929e03f30d1472644851bcb73c4af6b095acd7328a07
  e9187a836a15307c6076210c9b410493505bc4814e3c327386796c5932c8cab7a695b9
  ac24561b2a9657c3157531ba3cba699b6424fda24cc6c72edac1a6bf091b87c3c594c9
  d24a1126f998aee120ae372a27a268a0c76ab8f84957f461e7c04dd2d59f0f217d9e07
  8990533b16bbc125b2737a1a7e1cc1ed7c47e8f8464ba78c5d3298f2dc7d0be944ad29
  7ec774ad1b1f1485b114a9a9b93c488c89c0c7609f2bf9533c2929f667bca8b68999e3
  54597cf83ba7450b237188c3364172c1351bd349a699672d31b9598bab79a18b3d8cb2
  5f53c0b22bfa065690a16184db4f9731cea1a08f5876ec187e7b1ae79c593415c7dd2b
  e3b5b93f77f4576d55d300739e75e14084b0bc85620499bf468ae161
eseed
  f90b0cdf8a7b9c264029ac185b70b83f2801f2f4b3f70c593ea3aeeb613a7f1b1de33f
  5081f592305f2e4526edc09631b10958f464d889f31ba010250fda7f
ct
  f98f274dc74db1798915be81f089fbf792116ec03539b6c02cfbe649267f100df0ef51
  6e51fd4a9b75cc2f1806d470b56984df3d368e4d09be4b4ffd59907e11b2d4497b7dd2
  1afb3cc52a6ea661f2c6495a7f5fbef3dfac143f65bc9f6eb48d548df01d6a0bb52dab
  fda5e92f7a223289ec4e45cf76d47ab3a79086481f4bb4e95cd69bfdf388762e775bf6
  9694f72ca5a90883be5b8ac08c1737d5eced830466e9426fe5bec61bc63f1962358b66
  3d8fdd5dfa887b0da5f15c8868bafce3d998b85ab34ced43ac9b9869c84c59fb2f094d
  a1dee97db9a941c3cc319401d9db08569d8eb248ec2ff51e7e18c22d810bf512c28d5d
  9c4bf5237bac6d14ec33b673453cb0129f31a0b532240ac257d7813370c7addd3ec957
  034b8e4c539506c7827a82e37f5b2405236c914783c35a8aaeaacdea194d699dcfd6d0
  27cbfcac58e3157a16c20b11dfaf6256ae3037252baac3a25f3d1f7e3f14dd231fc50d
  f8788575799e6be241717e9634456be9eb04989cdf312dddd8a24939ebb90de0f5b006
  9b2b19350dce76a415230f49374fa45ced3eed165cc92ed1d6e17c233f36030a61cb61
  93a55d939c9c7e964f9086ccdb41b8638f14f9202cdb9f1e3ffac235ccda32a92a71e8
  88297cdba4a309e085c56826bb6121462ac6ee36beb9ee72c824294b6026c60d478f17
  082cca6d6d7a3e86dbe5f7fc9bbc2a07873c686e53f9040aa60dce89b179643741457f
  e371c8aaf41eceee8e1a1b3246665723224997312 42ee48134eb6dfb8961b06b5a04c5
  c6a9113a9c161f36806a284e03b01940286b2de59689607b2b64b46d6fc2ba044c9a42
  cb600cfd6ca0bdf4915a47fe02d71b8fcc27f0f17c78a300c6345ccc2f77a438772f42
  f7b2160aec93e4c8c72c0dbe67868753c18491861a1c1b96eaae07023436602fbb6f2b
  161a5f778bb3086c2255423a8c51052833f6b63ed2cc732a7e2c4d36123471b451b640
  0421fd4edc83a9527d91203aa7e41867e3a7dfd5610aa20646738754883935af2b09cb
  d93a332c9671e6a00cc29a6346de406f5fb28fe84f0b0d3a43c98213bfc2eb2802f1ca
  1c560a705edceb262c44c2fd2e9e5caf0bf9eafc6be84c8a00d4bfd57e2468254e4560
  6e8d62ff72c55c403ce5a8e8c87cb4d7f693344918138a8f1621107492d8c0a8c74ae7
  23f7e1fa84220da14a9ae978b207aa692e2ba13ee5ed924c75e472e1b77cc496519704
  87bde2ac15fdde0184d799288b60873b7f85a113b5b8d76a5237f26586ef2cb5cb940c
  5a4789267575ed223fdb9d7ed57a390076857d3c0207360a3d039e4f7961dfe25d8e7c
  4df6ec0503b5589a89911e54d4831b5cc9ed0abc66143b5482d35dec97ed94e65ba7d0
  126348960804ec2f19463b8daaa9927c05eecae3bb58b2575fcec762c14cd7d27f51e0
  ec3ddf00e90dafcf91d31ac09eaad73d675504798170b703667d2175a37b40e4b78090
  b1c1ca3062cdb98b0ba79b61c1c3f692b6e75940077ab7aea8649f38e34406282704f1
  0208a15c
ss     d482dd1a592f072109a0d8a86991ca6bd5bab25f13e788377fc34506f508ffdd
```

seed

1368ec2967fc84ef2ae9aff268e0b1700affc6820b523a3d917135f2dff2ee06bfe72b
24721d4a26c04e53a75e30e73a7a9c4a95d91c55d495e9f51dd0b5e9d83c6d5e8ce803
62b8d654db53d09b8dcff273cdfeb573fad8bcd45578bec2

sk

f58497af7a5854c214be50bd9694011740619f4042d1a9b5e3d813bf419c9e70b6b6e3
17644378d7a097047c1be007b9973f3ec7c2c1c7af23726160db834503bc5381625ab0
c831b60a04c54a360d2222ab0918358e84a038c41775456f7c6c1de0f27d5b538a9e80
1484cb96d17b52825410661cc43a576669a92cb7b97b97aa0e7b55a0589bc1295000a0
dfa5236a737a95a7029d2a5f4429494ee4b1299613fb76a573092915f6c37d472beea0
3b082eb546b4ad268fc0fa9eedc8a19faab8a857ad09e24b042374ce9566e3b3ba33bc
441781f74421d00bcf0598103d9620fe0b35ab904c3676c3e970525c7507917850ff99
4eb57eeaf4b0615097a1e970de6aa9ba609fe8ac11fdfa4e7c4cb90a30c03cb8baeb50
cb6ba6c755bdaca4c9448bcc24188991a659adfbc219b3ca16258f3c0b8791846cd9e8
7ed33f97b1bfebeaa93628421a348596a72ed8a248219779cedb38f9fb0f064a4bf89a
5dd485564c30ab16bc83d19fc9257467598ef713cff3a0470f4983db6540e52a7667fc
85c031e989601972b2ca61c97218c6470498679523c5957ccd0b4f30836429287d4720
8a32ad0c3c01c38611537a417e28284d58b1dc415f8cc6025ba1603073206e9372bcd1
d94311eb2966fa9ac48ea68fb889c2925859017961l8949545a77ad8129d3c989f0f04
77d35ce9b715695b61e46aaf74fb9b753a489842592514c2c41b1e3a22621a5369ff4a
6702b2805cba6f945209a22613ec254937bc65fb40371b26f808cac5fa66437603fe17
4f039ebef88e2e3757692718229a7167780f032666e9f35a1f316c278270891057390a
552b9b53e92ce6325b12a8475768a5eaba388b5b4740a4b4867705c74caa54eb139d47
6b845fd6c97a01138509aa3cb34232504a4609850f464b27d3a6c792a2a326f78ea750
7ffb36349405442bcb7914be2bd482f4686cebf96c38fa67db608953039eb5446a2696
a0f023499261bc29356547612a472d9dd135e8744649656995178ad2b38d80850b180b
6c255a0aba7e8c656fe782a63f48bde8cc5899351e308a3d48e5322a7b8b48ec1c9939
9cc39d381146846567ed0143c6c1682cd06faa64467a00919c53a374281b86e6744569
eb1b099bea5b5c8a9e8024498ad70fc2cab20bd67a72073901a3bae643619342aa0107
3992428dea1755d870cbb86315b2bea4a6753359216e939f7d1aaaf0903b82fba7228a
15f0779de2a19056c4e0b066e98b2a99865df3825caca00a1313c2e8a66cb8165fbebb
fefb9e2e0916f4d753bb354b1cdb0ec61840ae14a0b0a6b89419cbcd4c2cc9fa8df8da
ef4a829e17b996461b499ca051b5989b17738b158057342454745051e7b01aa5a89711
c4d44e20f3950873aa1a436cf7255328dc73f312119395213ec852dcbc9d0634c722b2
3e154746402a3d289b3abb14a8d70494b761c3f66242f06cc534a761c19cee82a41ea7
08fb580a19762ea34f2f931cc3fca3a7484b0c0023ea2285dc1b04a46489ea5a673a5a
5db5745b72704670487c1c1c61f06184d1be1fb8c770857cfb03c5c3575181cb7f54eb
8c8b6a200a0ef6b66eec364c0015ceb802081800ab5bd1150ba20e5d2c6012d70fe700
6c101752242397627c89156f667a28ffc32c56d20abe3834d2a05a0390c7f2a893d641
fb772ae12468a1f6260af39066ab7ecf694db179436c54a707092a87aa22a274691ee0
3e7a98a6d2c633d6c0f13a1542b094e7505d8dd92063b3972dd036a2e68ca9d2af000d
28b27fb55178b3794d41755a4dd32abde2cf2d93a5c59605e372114bfbbbc443045365
d1aaad9d385f82278576840cb1f340c0d53db7b0c8cf3794d2f0ba99267ef5d01064c9
3aca71aaa2cbb85011c6687472e20419680441cb0c7bc70aaf1361797b1c2f5a5c60c1
86d981299bbfc2c15d77f4077c40500938bbb2e52aef37c3d516148d5ac84e216e0568
6ea476fde89685578f8df91281b648d1359bbd53768f27596f3b3845293d698b3a1ae2
5e0190be513cf950234399a51487073671736a0c4479672595b2b07a7c3b1143a2fa46
383a183e0880e580793e5892349600cd6c3adb903e078c31d7d50a90c5734537784267
8d35a6982b61098190befc3185020d2c175df7b1acec91c3d5fc6f7cd298f878bd2ab8

e7ca340ae21377f79a2f73cf219c7f9e85649d089356cc082f655d72e8035128b910b4
e7833abc11348305943b049a9d6b7df1f98af6c5bf9a6214f073ab28f1492748574881
f160139e60307d32086515bb93c502e6c20106801c095380d82467b9d56b72f566830a
72aaaba8dbbd755c262704af12475febf3cb6268289bdaab09997b8c309dfb436927e7
7dcbba3f772b85e753493417cb134c3604410399238da584d1c495c0793fc5e9583f87
e97c9d45e63c1fd42ee7c5aaf9cc901748c87438c91d6964fcab436c6c0b74b34c6a35
f688ace32a869411ca57cc3bb0455d981a16b655984ad90bf7c3add506b6821248cc52
5da27310fb57738254c8730241e2281c3b18728a12c458b8af8c2c3b500bed5c749e99
b4c44f116aa971b043a8b77b62f7a2fc9621ae71763fb0a43758b40e09aae6f574f932
1372a7bc120331c34800ed2113203eeb180905d89a88a4cc48d8c3acf19f44ba00b846
1ddc0fe1e3554ac059a9fa2b11807173f1190dea271119c087c605dc8b945fb069bfb1
c464a28758c1822b2c1e5a8ba0779833c6937c9c02ca61285c67557dd958e00840fd1c
9095409dc6caf13360a8d5a1d864a903c429b3054ee83448a1f71beb70a93dccae8e69
485b47df44202d931e2c99316a23a4e396b7c704b832a0b855106f29c20c3c447ad391
b77186cfb94b3e973d415636a0950284f50efa9248bb1643e793cc7a6c343395a8a245
69b32821f2b80214481ca4416d9009dd3174c4cbb29da7386a7404b21a72ce5a295deb
712a3fb01c927b9b2e73d95aa65c3e92169c72662d7ccab10c8a369d50b90a74c41d59
bc4ac104a147855131b1da730116bc17e430599a8d64999d9450b237002fa1021237db
a096a95ea0542ca7937b7c1971b53ce82087d7e114e446b81265cfd540176cd069deb9
6fa45bd2f3464e7cc908cac220e642fd3610f18aac2b594192bb7a72a64ffe156e77ac
576a0511b9768798c79590d8d37f58628ef69837335bfa984cde027d87d45cf83e597b
5d3130d6210e9d974bab5643cdf4d1cc7c8282ffe68f827e0cac9926bfe72b3124721d
26c04e53a75e30e73a7a9c4a95d91c55d495e9f51dd0b5e9d83c6d5e8ce803aa62b8d6
db53d09b8dcff273cdfeb573fad8bcd45578bec241c2f9459a0447d7f7ae5f1e8dc1cf
76cdd9add2eba7768b4ac7abb269b07e

pk

8c8b6a200a0ef6b66eec364c0015ceb802081800ab5bd1150ba20e5d2c6012d70fe700
6c101752242397627c89156f667a28ffc32c56d20abe3834d2a05a0390c7f2a893d641
fb772ae12468a1f6260af39066ab7ecf694db179436c54a707092a87aa22a274691ee0
3e7a98a6d2c633d6c0f13a1542b094e7505d8dd92063b3972dd036a2e68ca9d2af000d
28b27fb55178b3794d41755a4dd32abde2cf2d93a5c59605e372114bfbbbc443045365
d1aaad9d385f82278576840cb1f340c0d53db7b0c8cf3794d2f0ba99267ef5d01064c9
3aca71aaa2cbb85011c6687472e20419680441cb0c7bc70aaf1361797b1c2f5a5c60c1
86d981299bbfc2c15d77f4077c40500938bbb2e52aef37c3d516148d5ac84e216e0568
6ea476fde89685578f8df91281b648d1359bbd53768f27596f3b3845293d698b3a1ae2
5e0190be513cf950234399a51487073671736a0c4479672595b2b07a7c3b1143a2fa46
383a183e0880e580793e5892349600cd6c3adb903e078c31d7d50a90c5734537784267
8d35a6982b61098190befc3185020d2c175df7b1acec91c3d5fc6f7cd298f878bd2ab8
e7ca340ae21377f79a2f73cf219c7f9e85649d089356cc082f655d72e8035128b910b4
e7833abc11348305943b049a9d6b7df1f98af6c5bf9a6214f073ab28f1492748574881
f160139e60307d32086515bb93c502e6c20106801c095380d82467b9d56b72f566830a
72aaaba8dbbd755c262704af12475febf3cb6268289bdaab09997b8c309dfb436927e7
7dcbba3f772b85e753493417cb134c3604410399238da584d1c495c0793fc5e9583f87
e97c9d45e63c1fd42ee7c5aaf9cc901748c87438c91d6964fcab436c6c0b74b34c6a35
f688ace32a869411ca57cc3bb0455d981a16b655984ad90bf7c3add506b6821248cc52
5da27310fb57738254c8730241e2281c3b18728a12c458b8af8c2c3b500bed5c749e99
b4c44f116aa971b043a8b77b62f7a2fc9621ae71763fb0a43758b40e09aae6f574f932
1372a7bc120331c34800ed2113203eeb180905d89a88a4cc48d8c3acf19f44ba00b846
1ddc0fe1e3554ac059a9fa2b11807173f1190dea271119c087c605dc8b945fb069bfb1

c464a28758c1822b2c1e5a8ba0779833c6937c9c02ca61285c67557dd958e00840fd1c
9095409dc6caf13360a8d5a1d864a903c429b3054ee83448a1f71beb70a93dccae8e69
485b47df44202d931e2c99316a23a4e396b7c704b832a0b855106f29c20c3c447ad391
b77186cfb94b3e973d415636a0950284f50efa9248bb1643e793cc7a6c343395a8a245
69b32821f2b80214481ca4416d9009dd3174c4cbb29da7386a7404b21a72ce5a295deb
712a3fb01c927b9b2e73d95aa65c3e92169c72662d7ccab10c8a369d50b90a74c41d59
bc4ac104a147855131b1da730116bc17e430599a8d64999d9450b237002fa1021237db
a096a95ea0542ca7937b7c1971b53ce82087d7e114e446b81265cfd540176cd069deb9
6fa45bd2f3464e7cc908cac220e642fd3610f18aac2b594192bb7a72a64ffe156e77ac
576a0511b9768798c79590d8d37f58628ef69837335bfa984cde027d87d45cf841c2f9
9a0447d7f7ae5f1e8dc1cf4e76cdd9add2eba7768b4ac7abb269b07e
eseed
e770d01efde86e721a3f7c6cce275dabe6e2143f1af18da7efddc4c7b70b5e345db93c
36bea323491ccb38a388f546a9ff00dd4e1300b9b2153d2041d205b4
ct
137d93a41362f50229305c688633ded3c474cf399858d60e668ca77d04fd869168a235
e177eed970cd8c4b8a8bcad3ba1bdf3cef0d697b2c1a1e9a4259cce54248d5f47b59e9
ca20799888ec7ee44efd7414bfc71a543648bea1edd9da0234a3af27dcfe4854792caa
6a3dcce1eb31cf4d5d8b85855fe1ba7dd94b188ffec719354d43c445960766e26f1756
5ec3872bfa9cfa370a00ac6bb9e196bb57a9f1fd0577d664077b81558565e50b0f2964
e0093353618de2f2f6d5999c1d27279032f788cb3cf59c127e7c7e0297871112264543
d06c81b2affbd099493c34704bb8f0759c4ce568cf721239014b1f00e808b5dc76ea4f
20408c7e510e27832921b022000f9dabdac2e5bcb47060efd1a169e4eefa80ed6fbd1f
473c2038d742df4e286bbcb854281aa28c283f81d8d8c0324b5d354e8b6e2c5e28d5b3
88a790f926c7b5270630c5087990f7ce5afe2fc9e327ed33f760c8d3ea520d9c01960d
60566647820c98c859052ea770c5efbed12b0e7536a409562e2fbb0cd6ce67011f6233
23239f1ed44035963ca9470c439a7e588226307be4cf7a6e27766a28730843a6865c9a
53f66e8ab121ff234fa3dd0cfc9736b40fb8bb3e64919ec4a5de20282928f60260c63a
439e0658339437b3f1735f38c9481d7edc344ef6dd34d93e0ee013a93cdc8a7207b9d7
65bee8a768934c2b386f47d85891fd316aaa378af13c8892099075b75cc8d9ce0419ce
f0f55ea0aeea03fcce14e3a4c766ed09fe4577c6cb9372d00e95c86b41989d6e6ff235
579b66f76a5a1bf41b2c1f53db1e8b49d822455ea4afe8198b5e7f039263e10885d38d
fa0ee727cc4ff2769f9ed0abc08a3e77f8bc65a7a75b7b0fc74c2a9027e94f1757acaf
ee5e6e28c0b0238a5435712ea1c055d79e0558a2d149ecfb8d129e19c2d9aef804b3e4
6f60ab43c5254f81a9cccbb3bed13a67f436159b0cf5c7134d6d5a577bcea4f8648eb0
728b0864ec8751576c6fc302a76831d1672daaa2e17c5991efca743cf55d64ca59e8fe
a59ec52099d7bfb00a3ccde4084825145f022d89a126519f7904eb7ec4db0b08e70d7d
bf18e537476b4ce97b2ad1c84c0630ba053a13affff42ecea695c080942df74369a23f
a1f397f14dce28acbedb6a90e7a0a6423c277254b71be2d887386915e5924e85f1c652
2f8c0db076364a97d7acaf0f238c912fd56403593a8b2526884737790a887d9a8382fa
d2967803d0a1e62b610289af4ea26c66ef29c4832a4b48ffa225d5be2401656753a9ed
c45a057efc666abaecfaeef972643de281f5d6a6ef43ed2fbba963a95c8d36461323d5
18f92e58e4de1b4edd1d93ba14ea6adc3b8b63e71d0edc92555f3f962e68fbf42a0fc0
b7da107203468589655f1b3b979ccc2efee6f10f0ec631c040e4436b8acaa4716708bf
d2db8108a36117d10664cb2a3e3af672a10b0de5c2a284e6b9de37533bd181bc14fa04
35d5050b5526ba59f893a1778103b6e2d946090c0eba049e5c1ad843a3121d53956486
f5647437
ss 1e037823ddbf1875756d86a3374b2d2347d5b7f3c84d229ecc5960523cdaa8b4

Appendix B. Acknowledgments

TODO acknowledge.

Appendix C. Change log

RFC Editor's Note: Please remove this section prior to publication of a final version of this document.

C.1. Since draft-connolly-cfrg-xwing-kem-00

*A copy of the X25519 public key is now included in the X-Wing decapsulation (private) key, so that decapsulation does not require separate access to the X-Wing public key. See #2.

Authors' Addresses

Deirdre Connolly
SandboxAQ

Email: durumcrustulum@gmail.com

Peter Schwabe
MPI-SP & Radboud University

Email: peter@cryptojedi.org

Bas Westerbaan
Cloudflare

Email: bas@cloudflare.com