SPAE & CSPAE algorithms

v1.00, April 10th 2019, Sebastien Riou

Introduction

As of 2019, it seems that none of the published AEAD schemes using AES are entirely satisfactory. We reviewed the schemes listed in table Comparison of selected AEAD schemes.

Table 1. Comparison of selected AEAD schemes

Name	Non trivial operations count	Consequence of Nonce reuse
OCB	(2+m+a)Ek + (1+m+a)Inc	• Forgeability • Equality of blocks revealed
GCM	(1+m)Ek + (1+m+a)MultH	• Forgeability • Xor of plaintexts revealed
CCM	(2m+a+2)Ek	Xor of plaintexts revealed
EAX	(2m+a+1)Ek	Xor of plaintexts revealed
SIV	(2m+a)Ek	Equality of message revealed

Notation

- m: length of message, in blocks.
- a: length of associated data, in blocks.
- Ek: the encryption with the key k. The slowest of all operations.
- MultH: GF128 multiplication. It is typically faster than Ek.
- Inc: The "inc" operation defined in OCB. It is typically faster than MultH.

The risks of nonce reuse in GCM and OCB are just too high for applications where the nonce is generated in the field (IoT, smart cards...). SIV has good robustness against nonce reuse however it is expensive as it is a "two pass" scheme. CCM and EAX robustness against nonce reuse is in between but still leak quite a lot of information. They are not faster than SIV anyway, so no incentive to use them at all.

NOTE	XCBC and XECB have been excluded from the review as they are patented and not well documented. OCB is also patented but the author license it for free to open source projects and the author gives clear diagrams.

We propose a new alternative which leaks slightly more than SIV but has much better performances, we call it SPAE for "Single Pass Authenticated Encryption". A conservative variant dubbed CSPAE is also described in this document.

Table 2. SPAE & CSPAE properties

Name	Non trivial operations count	Consequence of Nonce reuse
SPAE	(1+m+a)Ek	Equality of first blocks revealed
CSPAE	(2+m+a)Ek	Equality of first blocks revealed

NOTE	In SPAE there is a Ek operation which can be precomputed. If this operation is counted like the others then the operation count is (2+m+a)Ek.

The abstract box model

Typically AEAD algorithms are evaluated in a security model where the attacker can submit any combination of nonce, message and associated data as long as the nonce is not reuse for two encryptions. We feel that the general security model for the study of AEAD is putting a lot of constraints on the algorithm which in practice can be avoided. The abstract box model intent to define a security model which takes into account practical aspects to relax the constraints on the algorithm. The abstract box is an object which contains a secret key, an implementation of the AEAD algorithm, and a mechanism to generate nonce internally. Its purpose is to encrypt or decrypt data submitted by the user without revealing the key. As it is abstract, the user cannot attempt any physical measurement or modification on it. The only thing possible is to invoke either the encryption or the decryption processes described below.

AEAD encryption

In encryption, the abstract box takes as input the message and the associated data. It outputs the cipher text, the authentication tag and the nonce. As a result, the attacker cannot choose the nonce. At best it may be able to predict it if, for example, the abstract box use a counter to generate the nonce. If the predictability of the nonce is a problem, an AEAD algorithm may simply state that the nonce has to be unpredictable. If the abstract box is unable to generate a fresh nonce, it outputs nothing (this may happen if, for example, the abstract box use a counter and it has reach its maximum value). The nonce may be output before any input has been fed in, so the attacker can adapt the message and the associated data after observing the nonce chosen by the abstract box.

NOTE	In practice a secure system can easily enforce that it output the nonce only after receiving all inputs. The downside is that the nonce would be considered secret during the whole computation. As a result the nonce would be an additional target for side channel attacks, so it is best to not rely on this approach in the security model.

AEAD decryption

In decryption, the secure box takes as input the nonce, the cipher text, the associated data and the expected tag. If the computed tag match the expected tag, it outputs the message otherwise it outputs nothing.

NOTE	When the mode support padding, the bit length of the plain-text and the associated data are also inputs to the decryption algorithm. Those inputs are in full control of the attacker unless the length are somehow encoded in the cipher-text or the expected tag.

Advantages

This security model allow to create optimized AEAD algorithms because it avoids the attack scenarios on the encryption which involve a chosen nonce. The nonce remains under the attacker's control for decryption but this is less critical as the decryption gives its output only if the expected tag matches the computed tag.

This security model also allows an algorithmic protection against DFA attacks: the encryption can be efficiently protected at algorithmic level by ensuring that each output cannot be repeated. If a given output can be seen only once, the attacker can get a correct output or a faulty output but not a matching pair of correct and faulty output. Similarly the AEAD decryption can be efficiently protected at algorithmic level by ensuring that the tag is correct only if all the outputs subject to DFA are correct.

NOTE	The potential protection of decryption against DFA is not specific to the abstract box model, this is a simple consequence of the definition of AEAD decryption operation. We nevertheless discuss it here as few AEAD algorithm leverage this. For example in GCM, most of Ek steps remains exposed to DFA.

SPAE mode specification

Notation

Table 3. Operators on integers

a << b	right bit shift
a ^ b	bitwise xor
a + b	addition
a - b	subtraction
a * b	multiplication
a / b	integer division, return only the integer part of the result without any rounding

Table 4. Operators used on data blocks

Ex	block encryption with key x
Dx	block decryption with key x
a ^ b	bitwise xor
xor	bitwise xor
HSWAP	swap of the left half with the right half within a block

Instantiation parameters

SPAE rely on a block cipher to underpin its security. The block cipher choice determine the following parameter values:

- BLOCKSIZE: the size in bits of a block processed in one call to the block cipher. It is assumed to be a power of two.
- KEYSIZE: the size in bits of the secret key required by the block cipher.

In addition, SPAE has the following parameters:

- TAGSIZE: the size in bits of the tag. It is freely selectable up to BLOCKSIZE.

Requirements on the block cipher

The block cipher shall not have weak keys and shall resist related key attacks in which the related keys are derived solely by exclusive-or on the original key. As of 2019 AES-128 and AES-256 fulfills those requirements. Related keys attacks have been published on AES-256 however they involve the the round keys rather than the original key, so the SPAE requirement is met.

SPAE encryption

Inputs

- k: the secret key.
- mlen: the message length in bits.
- alen: the associated data length in bits.
- Message: the data to encrypt and authenticate, also called plain-text. It is composed of an integer number **m** of blocks noted P_i with 0<=i<m. m = (mlen + BLOCKSIZE - 1) / BLOCKSIZE .
- Associated data: the data to authenticate without encryption. It is composed of an integer number **a** of blocks noted A_j with 0<=j<a. a = (alen + BLOCKSIZE - 1) / BLOCKSIZE.
- Nonce: a value that is used only once for invoking SPAE encryption.

NOTE	Message and associated data are padded with zeros from **mlen**, **alen**, to the next full block boundary. This shall be enforced by the implementation.

Outputs

- Cipher-text: the encrypted data. It is composed of an integer number m of blocks noted C_i with 0<=i<m.
- Tag: the authentication tag, it is a single block.

Internal variables

- kn = k ^ nonce
- mpadinfo = mlen & ((1<<64)-1)
- apadinfo = mlen & ((1<<64)-1)
- mpadinfo32 = mlen & ((1<<32)-1)
- apadinfo32 = mlen & ((1<<32)-1)
- apadinfo_swap = (apadinfo>>32)^((apadinfo & 0xFFFFFFFF)<<32)
- PADINFO = ((apadinfo_swap ^ mpadinfo)<<64) ^ (apadinfo32<<32) ^ mpadinfo32 (bytes in little endian order)

Cipher-text and PT_i and CT_i equations:

- PT_0 = k^Ek(k)
- CT_0 = Ek(k)
- For i=0 to m-1
  - $C_i = CT_i \wedge Ekn(PT_i \wedge P_i)$
  - $PT_{i+1} = P_i \wedge Ekn(PT_i \wedge P_i)$
  - $CT_{i+1} = CT_i \wedge PT_i$

Tag equations:

- $AT_0 = 0$
- For j=0 to a-1:
  - $AT_{j+1} = Ek(AT_j \wedge A_j)$
- if m == 0
  - $MT = k \wedge ((1 << BLOCKSIZE)-1)$
  - $IT = MT \wedge AT_a$
  - $TAG = PT_m \wedge Ekn(IT \wedge PADINFO)$
- else
  - $MT = HSWAP(CT_m) \wedge PT_m$
  - $IT = MT \wedge AT_a$
  - $TAG = CT_m \wedge Ekn(IT \wedge PADINFO)$

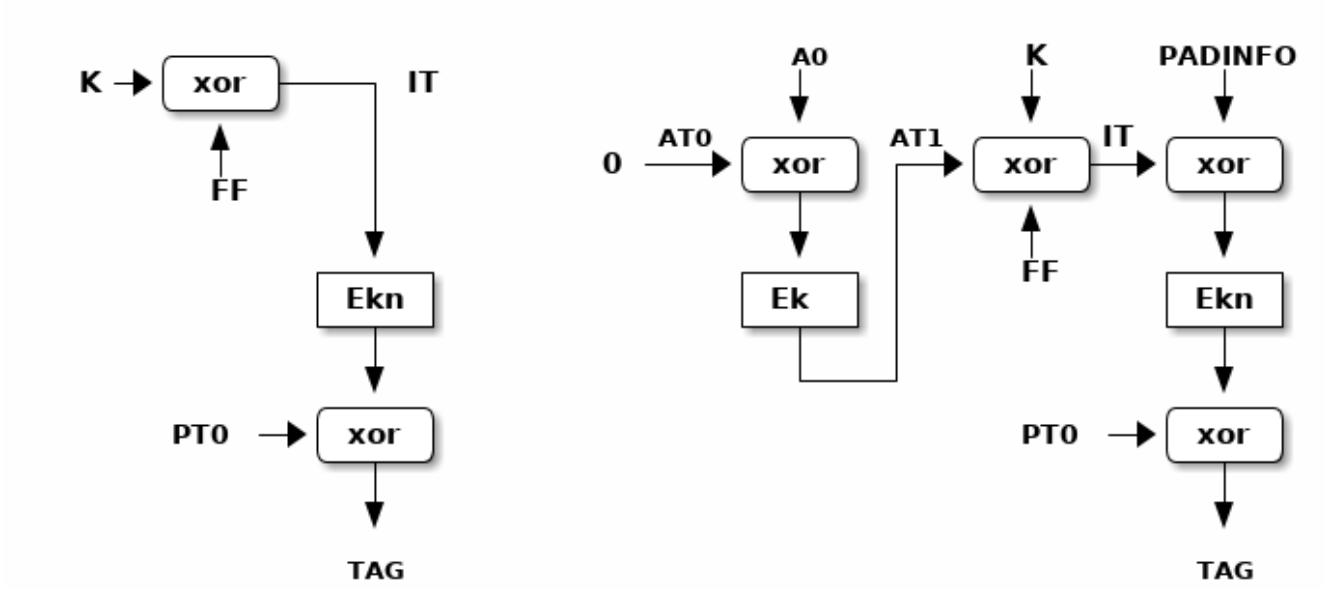

Figure 1. SPAE encryption description, m=0 a=[0,1]

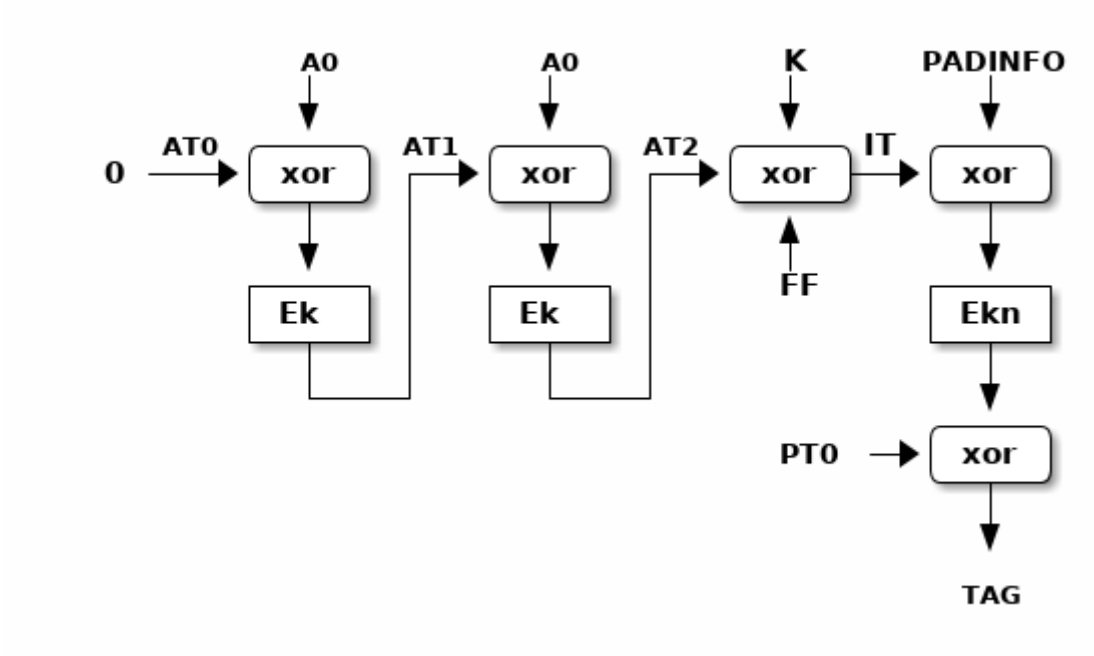

Figure 2. SPAE encryption description, m=0 a=2

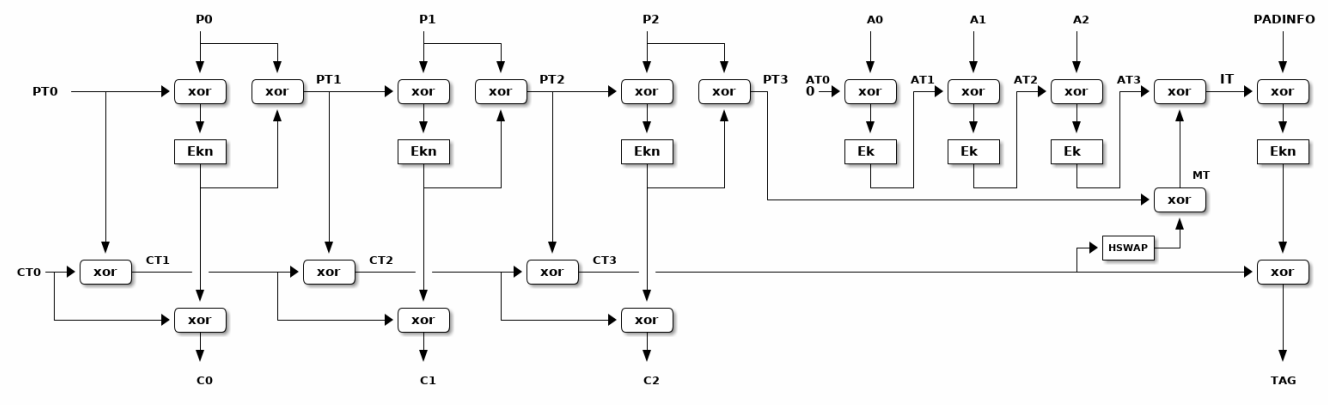

Figure 3. SPAE encryption description, m=3,a=3

SPAE reference test vector AES-128, m=3,a=3 encryption

TODO

SPAE decryption

Inputs

- k: the secret key
- mlen: the output plain text length in bits.
- alen: the associated data length in bits.
- Cipher-text: the encrypted data. It is composed of an integer number **m** of blocks noted C_i with 0<=i<m.
- ProvidedTag: the authentication tag generated for Message.
- Associated data: the data integrity protected but not encrypted. It is composed of an integer number **a** of blocks noted A_i with 0<=i<a.
- Nonce: the value which was used to generate Message.

NOTE	Associated data is padded with zeros from **alen** to the next full block boundary. This shall be enforced by the implementation.

NOTE	The implementation shall verify that mlen < m * BLOCKSIZE. If it is not the case, the decryption shall be aborted.

Outputs

- Plain-text: the decrypted data. It is NOT returned if the integrity check fails, that is if the provided tag is different than the computed tag.

Plain-text and PT_i and CT_i equations:

- PT_0 = k^Ek(k)
- CT_0 = Ek(k)
- For i=0 to m-1
  - $P_i = PT_i \wedge Dkn(CT_i \wedge C_i)$
  - $PT_{i+1} = P_i \wedge CT_i \wedge C_i$
  - $CT_{i+1} = CT_i \wedge PT_i$

NOTE	Tag equations are exactly the same as in the encryption

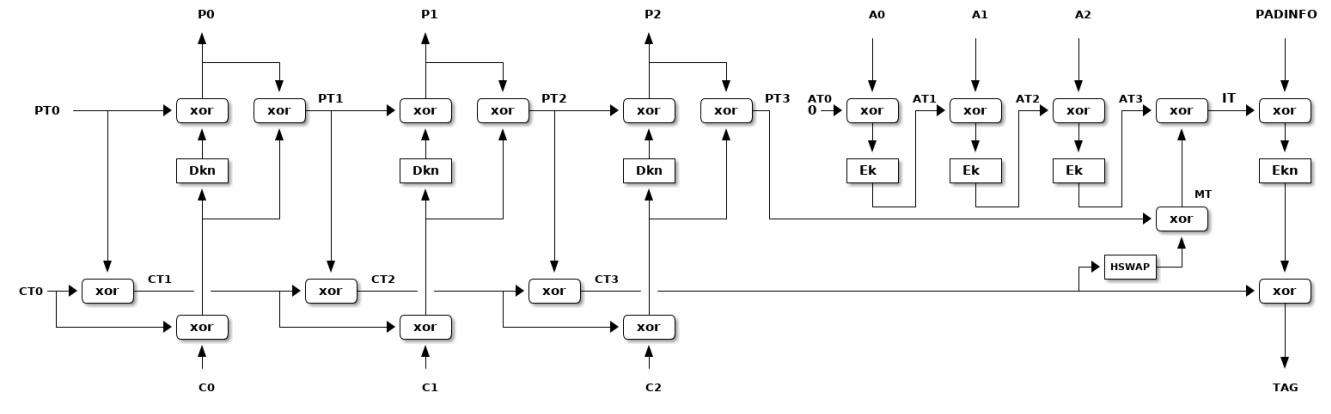

Figure 4. SPAE decryption description

SPAE reference test vector AES-128, m=3,a=3 decryption

TODO

Design Rational

HSWAP and PADINFO encoding

Both the HSWAP operation and the redundant encoding of PADINFO are not really useful from a pure cryptographic point of view. Their purpose is to prevent some DFA on the Dkn operations during decryption. The section on DFA protection gives detailed explanations.

Built in DFA protection

This section discuss the feasibility of a DFA attack on Ek, Ekn and Dkn steps within SPAE. A successful DFA involve getting a pair of Ex or Dx outputs, one without fault and one with a faulty result. Crucially the outputs must be obtained from the same input and the same key. In this section we call such outputs "exploitable pair". DFA attacks are relevant to smart card and other highly secure chips. In this context it is assumed that the implementation has the means to enforce nonce uniqueness for encryption.

Encryption

Assuming the nonce is not in the control of the attacker, each AEAD encryption use a different kn so DFA is possible using outputs belonging to the same AEAD encryption. Within an AEAD encryption, the attacker is not able to get two C_i with the same value or to get the tag equal to a C_i. The attacker is not able to achieve this because that would contradict the security proofs.

The final Ekn used to compute TAG is a special case: a kind of advanced DFA is possible on it. Assuming an injected fault result in a low hamming weight error pattern, an attacker can inject a fault on the final E KN and then try to guess the error pattern by submitting variations of the faulty TAG to the decryption. A successful guess will result in a successful decryption while all other guesses will result in Failure.

To conclude, in SPAE encryption, all Ekn computations can be done without DFA countermeasures except the last one.

Decryption

In decryption the nonce is in the control of the attacker, as a result the reasoning used for the encryption does not hold. The SPAE decryption protects Ek, Ekn and Dkn computation nevertheless by leveraging the tag verification.

The tag is computed from all the outputs of Ek, Ekn and Dkn computation, as a result if there is a faulty result the tag will be incorrect and the output will not be provided to the attacker.

This approach has some limitations. The main reason is that unlike cipher text corruptions, fault injected in E can result in an error pattern with a low hamming weight. For example a fault injected on the last round of AES will typically impact only a single byte.

An attacker can leverage this by targeting the final Ekn operation which produce the TAG. If the faulty TAG can be guessed or brute forced, an attacker may simply inject always the same fault and

submit each time a new guess for the TAG. A DFA in which the attacker guess the fault pattern is certainly an "advanced DFA" we nevertheless consider it a likely attack scenario. To avoid such attack, an implementation need to protect the final Ekn step used to compute the tag.

A fault on the first Dkn propagates to the tag via the PT_i and P_i, and, depending on the number of blocks, via the CT_i. Propagation via the CT_i depends on the number of blocks because the error cancels out every two blocks: The error would be in CT_2 but would disappear in CT_3 since it is also present in PT_2. At this point it will still propagate further via PT_2 to P_2 and then PT_3.

This error cancellation phenomenon is the reason for the introduction of the HSWAP operation. Thanks to the HSWAP operation, any error present in both PT_m and CT_m does not cancels out and propagates to IT. The propagation of DFA errors to IT is crucial: it ensure that the resulting faulty TAG cannot be easily guessed. Since IT goes through a call to Ekn, even if a single bit is corrupted the resulting TAG will be impractical to guess.

Faults injected on the penultimate Dkn operation propagates only via PT_m. On its way to the final TAG, the error pattern is xored with PADINFO. An attacker could attempt to manipulate PADINFO in such a way that it would cancel out the error pattern. We mitigate this by formatting PADINFO in such a way that it is unable to cancel typical fault patterns on the late AES rounds. The bytes 0,5,8 and 13 have been chosen because this pattern is easily generated in software: the shift between 0 and 5 is the same as the shift between 8 and 13. A fault in the sbox 0 in the 8th round of AES-128 could disturb byte 0 and 5, but it would also disturb byte 10 and 15.

To conclude, in SPAE decryption, at most one Ekn computation need DFA countermeasures, all other computations of Ek, Ekn and Dkn do not.

Summary of properties

This is a summary of properties as suggested by NIST.

Security Function

Authenticated Encryption with Associated Data (AEAD).

Error Propagation

As in any valid AEAD scheme, the error propagation is infinite.

Synchronization

Synchronization is optional: If the nonce is transmitted along with each cipher-text, there are no synchronization requirements. If it is not sent the receiver must maintain the corresponding value.

Parallelization

Message processing is sequential, associated data processing is sequential. Both can be performed in parallel.

Keying Material Requirements

A single block-cipher key is required.

Counter/IV/Nonce Requirements

A nonce of at most the block size is required.

Memory Requirements

7 blocks are necessary to maintain the state of a running operation:

1. kn
2. PT_i
3. CT_i
4. P_i
5. C_i
6. AT_j
7. provided tag (decryption only)

NOTE	Implementation can reduce this by enforcing a strict order of processing. For example, always process associated data first

Pre-processing Capability

- Block cipher key scheduling
- Associated data can be pre-processed even before choosing the nonce. The resulting AT_j value can be reused unlimited times.
- PT0 and CT0 can be cached rather than computed every time as they depend only on the secret key.

Message Length Requirements

The plain-text can be of arbitrary length however it must be padded to a multiple of the block size. Associated data must be padded to a multiple of the block size. The padding bits must be 0.

Ciphertext Expansion

The cipher-text expansion consist of:

- Tag (at most 1 block)
- Nonce (at most 1 block)
- Padding bits if message length is not multiple of block size
- Padding bits if associated data is not multiple of block size

Other Characteristics

- SPAE is an "on-line" algorithm: it is possible to process data blocks as they come with constant memory, without knowing how many blocks will be added. (Note that for decryption, like for any AE scheme, this is not entirely true since the output cannot be sent out as long as the tag verification has not been done).
- It uses only a block cipher and xor, so no dedicated hardware accelerator is required other than the one for underlying block cipher.
- DFA attacks targeting the Ex and Dx computations are mostly prevented at algorithmic level. Only the last Ekn computation need implementation level countermeasures.
- SPAE is not patented.

SPAE Test Vectors

```
m=0,a=0
SPAE - encryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
associated data    =
               PT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6e'
               CT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6f'
                MT =  b'fffffffffffffffffffffffffffffffe'
                IT =  b'fffffffffffffffffffffffffffffffe'
           PADINFO =  b'00000000000000000000000000000000'
authentication tag =  b'6b52a86d2741165af5ad9b4694d978e7'
out                =  b'6b52a86d2741165af5ad9b4694d978e7'
```

```
m=0,a=1
SPAE - encryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
associated data    =  b'00000000000000000000000000000006'
               PT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6e'
               CT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6f'
               AT1 =  b'131527259dc7975992e4bbfd0510e9fa'
                MT =  b'fffffffffffffffffffffffffffffffe'
                IT =  b'ecead8da623868a66d1b4402faef1604'
           PADINFO =  b'00000000800000000000000080000000'
authentication tag =  b'840fa2e1542e22a1146b8ccb4f98410f'
out                =  b'840fa2e1542e22a1146b8ccb4f98410f'
```

```
m=1,a=0
SPAE - encryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =  b'00000000000000000000000000000003'
associated data    =
               PT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6e'
               CT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6f'
               P0  =  b'00000000000000000000000000000003'
               C0  =  b'731bdd384f415c11081d08ecdc3efe5d'
               PT1 =  b'd2654251abb3069a8e3dbc43a4d00331'
               CT1 =  b'00000000000000000000000000000001'
                MT =  b'd2654251abb3069b8e3dbc43a4d00331'
                IT =  b'd2654251abb3069b8e3dbc43a4d00331'
           PADINFO =  b'80000000000000008000000000000000'
authentication tag =  b'8f11c2f7f934270ebbd7c3033fbbabef'
out                =
b'731bdd384f415c11081d08ecdc3efe5d8f11c2f7f934270ebbd7c3033fbbabef'
```

```
m=2,a=0
SPAE - encryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
b'000000000000000000000000000000030000000000000000000000000000000004'
associated data    =
               PT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6e'
               CT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6f'
               P0  =  b'00000000000000000000000000000003'
               C0  =  b'731bdd384f415c11081d08ecdc3efe5d'
               PT1 =  b'd2654251abb3069a8e3dbc43a4d00331'
               CT1 =  b'00000000000000000000000000000001'
               P1  =  b'00000000000000000000000000000004'
               C1  =  b'd454792a75871ce616511d13983f9681'
               PT2 =  b'd454792a75871ce616511d13983f9684'
               CT2 =  b'd2654251abb3069a8e3dbc43a4d00330'
                MT =  b'5a69c569d1571fd6c4345f42338c901e'
                IT =  b'5a69c569d1571fd6c4345f42338c901e'
           PADINFO =  b'00010000000000000001000000000000'
authentication tag =  b'773ff95c3282ff9ea8794295685191ea'
out                =
b'731bdd384f415c11081d08ecdc3efe5dd454792a75871ce616511d13983f9681773ff95c3282ff9ea879
4295685191ea'
```

```
m=3,a=0
SPAE - encryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
b'00000000000000000000000000000003000000000000000000000000000000040000000000000000000
000000000005'
associated data    =
               PT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6e'
               CT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6f'
               P0  =  b'00000000000000000000000000000003'
               C0  =  b'731bdd384f415c11081d08ecdc3efe5d'
               PT1 =  b'd2654251abb3069a8e3dbc43a4d00331'
               CT1 =  b'00000000000000000000000000000001'
               P1  =  b'00000000000000000000000000000004'
               C1  =  b'd454792a75871ce616511d13983f9681'
               PT2 =  b'd454792a75871ce616511d13983f9684'
               CT2 =  b'd2654251abb3069a8e3dbc43a4d00330'
               P2  =  b'00000000000000000000000000000005'
               C2  =  b'406d307c0f1f9a95878e7bb968108aaa'
               PT3 =  b'9208722da4ac9c0f09b3c7faccc0899f'
               CT3 =  b'06313b7bde341a7c986ca1503cef95b4'
                MT =  b'0a64d37d984309bb0f82fc8112f493e3'
                IT =  b'0a64d37d984309bb0f82fc8112f493e3'
           PADINFO =  b'80010000000000008001000000000000'
authentication tag =  b'a4d864382672b6abbfeb80563bbfefa1'
out                =
b'731bdd384f415c11081d08ecdc3efe5dd454792a75871ce616511d13983f9681406d307c0f1f9a95878e
7bb968108aaaa4d864382672b6abbfeb80563bbfefa1'
```

```
m=3,a=1
SPAE - encryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
b'000000000000000000000000000000300000000000000000000000000000004000000000000000000000
000000000005'
associated data    =  b'00000000000000000000000000000006'
               PT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6e'
               CT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6f'
               P0  =  b'00000000000000000000000000000003'
               C0  =  b'731bdd384f415c11081d08ecdc3efe5d'
               PT1 =  b'd2654251abb3069a8e3dbc43a4d00331'
               CT1 =  b'00000000000000000000000000000001'
               P1  =  b'00000000000000000000000000000004'
               C1  =  b'd454792a75871ce616511d13983f9681'
               PT2 =  b'd454792a75871ce616511d13983f9684'
               CT2 =  b'd2654251abb3069a8e3dbc43a4d00330'
               P2  =  b'00000000000000000000000000000005'
               C2  =  b'406d307c0f1f9a95878e7bb968108aaa'
               PT3 =  b'9208722da4ac9c0f09b3c7faccc0899f'
               CT3 =  b'06313b7bde341a7c986ca1503cef95b4'
               AT1 =  b'131527259dc7975992e4bbfd0510e9fa'
                MT =  b'0a64d37d984309bb0f82fc8112f493e3'
                IT =  b'1971f45805849ee29d66477c17e47a19'
           PADINFO =  b'80010000800000008001000080000000'
authentication tag =  b'b2d2286e176bbe8120af02dd378a22f0'
out                =
b'731bdd384f415c11081d08ecdc3efe5dd454792a75871ce616511d13983f9681406d307c0f1f9a95878e
7bb968108aaab2d2286e176bbe8120af02dd378a22f0'
```

```
m=3,a=2
SPAE - encryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
b'000000000000000000000000000000300000000000000000000000000000004000000000000000000000
000000000005'
associated data    =
b'000000000000000000000000000000600000000000000000000000000000007'
               PT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6e'
               CT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6f'
               P0  =  b'00000000000000000000000000000003'
               C0  =  b'731bdd384f415c11081d08ecdc3efe5d'
               PT1 =  b'd2654251abb3069a8e3dbc43a4d00331'
               CT1 =  b'00000000000000000000000000000001'
               P1  =  b'00000000000000000000000000000004'
               C1  =  b'd454792a75871ce616511d13983f9681'
               PT2 =  b'd454792a75871ce616511d13983f9684'
               CT2 =  b'd2654251abb3069a8e3dbc43a4d00330'
               P2  =  b'00000000000000000000000000000005'
               C2  =  b'406d307c0f1f9a95878e7bb968108aaa'
               PT3 =  b'9208722da4ac9c0f09b3c7faccc0899f'
               CT3 =  b'06313b7bde341a7c986ca1503cef95b4'
               AT1 =  b'131527259dc7975992e4bbfd0510e9fa'
               AT2 =  b'dba2c410fd3d0a66d02984fc6e85d61a'
                MT =  b'0a64d37d984309bb0f82fc8112f493e3'
                IT =  b'd1c6176d657e03dddfab787d7c7145f9'
           PADINFO =  b'800100000001000080010000000010000'
authentication tag =  b'baf2944c6cf3b3a0883a024b23f34fec'
out                =
b'731bdd384f415c11081d08ecdc3efe5dd454792a75871ce616511d13983f9681406d307c0f1f9a95878e
7bb968108aaabaf2944c6cf3b3a0883a024b23f34fec'
```

```
m=3,a=3
SPAE - encryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
b'000000000000000000000000000000300000000000000000000000000000004000000000000000000000
000000000005'
associated data    =
b'000000000000000000000000000000600000000000000000000000000000007000000000000000000000
000000000008'
               PT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6e'
               CT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6f'
               P0  =  b'00000000000000000000000000000003'
               C0  =  b'731bdd384f415c11081d08ecdc3efe5d'
               PT1 =  b'd2654251abb3069a8e3dbc43a4d00331'
               CT1 =  b'00000000000000000000000000000001'
```

```
               P1  =  b'00000000000000000000000000000004'
               C1  =  b'd454792a75871ce616511d13983f9681'
               PT2 =  b'd454792a75871ce616511d13983f9684'
               CT2 =  b'd2654251abb3069a8e3dbc43a4d00330'
               P2  =  b'00000000000000000000000000000005'
               C2  =  b'406d307c0f1f9a95878e7bb968108aaa'
               PT3 =  b'9208722da4ac9c0f09b3c7faccc0899f'
               CT3 =  b'06313b7bde341a7c986ca1503cef95b4'
               AT1 =  b'131527259dc7975992e4bbfd0510e9fa'
               AT2 =  b'dba2c410fd3d0a66d02984fc6e85d61a'
               AT3 =  b'7152d55728d8c03e547ab64cd21531fa'
                MT =  b'0a64d37d984309bb0f82fc8112f493e3'
                IT =  b'7b36062ab09bc9855bf84acdc0e1a219'
           PADINFO =  b'80010000800100008001000080010000'
authentication tag =  b'6606f31a266516b3f3c57529ef402421'
out                =
b'731bdd384f415c11081d08ecdc3efe5dd454792a75871ce616511d13983f9681406d307c0f1f9a95878e
7bb968108aaa6606f31a266516b3f3c57529ef402421'
SPAE - decryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
b'731bdd384f415c11081d08ecdc3efe5dd454792a75871ce616511d13983f9681406d307c0f1f9a95878e
7bb968108aaa'
associated data    =
b'00000000000000000000000000000006000000000000000000000000000000070000000000000000000
000000000008'
               PT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6e'
               CT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6f'
               P0  =  b'00000000000000000000000000000003'
               C0  =  b'731bdd384f415c11081d08ecdc3efe5d'
               PT1 =  b'd2654251abb3069a8e3dbc43a4d00331'
               CT1 =  b'00000000000000000000000000000001'
               P1  =  b'00000000000000000000000000000004'
               C1  =  b'd454792a75871ce616511d13983f9681'
               PT2 =  b'd454792a75871ce616511d13983f9684'
               CT2 =  b'd2654251abb3069a8e3dbc43a4d00330'
               P2  =  b'00000000000000000000000000000005'
               C2  =  b'406d307c0f1f9a95878e7bb968108aaa'
               PT3 =  b'9208722da4ac9c0f09b3c7faccc0899f'
               CT3 =  b'06313b7bde341a7c986ca1503cef95b4'
               AT1 =  b'131527259dc7975992e4bbfd0510e9fa'
               AT2 =  b'dba2c410fd3d0a66d02984fc6e85d61a'
               AT3 =  b'7152d55728d8c03e547ab64cd21531fa'
                MT =  b'0a64d37d984309bb0f82fc8112f493e3'
                IT =  b'7b36062ab09bc9855bf84acdc0e1a219'
           PADINFO =  b'80010000800100008001000080010000'
authentication tag =  b'6606f31a266516b3f3c57529ef402421'
provided tag       =  b'6606f31a266516b3f3c57529ef402421'
out                =
b'00000000000000000000000000000003000000000000000000000000000000040000000000000000000
```

```
000000000005'
```

```
m=3,a=3 padded
SPAE - encryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
b'000000000000000000000000000000030000000000000000000000000000000409'
associated data    =
b'00000000000000000000000000000006000000000000000000000000000000070a0b'
               PT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6e'
               CT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6f'
               P0  =  b'00000000000000000000000000000003'
               C0  =  b'731bdd384f415c11081d08ecdc3efe5d'
               PT1 =  b'd2654251abb3069a8e3dbc43a4d00331'
               CT1 =  b'00000000000000000000000000000001'
               P1  =  b'00000000000000000000000000000004'
               C1  =  b'd454792a75871ce616511d13983f9681'
               PT2 =  b'd454792a75871ce616511d13983f9684'
               CT2 =  b'd2654251abb3069a8e3dbc43a4d00330'
               P2  =  b'09000000000000000000000000000000'
               C2  =  b'804fcc83143603242c36fe10cab4de85'
               PT3 =  b'5b2a8ed2bf8505bea20b42536e64ddb5'
               CT3 =  b'06313b7bde341a7c986ca1503cef95b4'
               AT1 =  b'131527259dc7975992e4bbfd0510e9fa'
               AT2 =  b'dba2c410fd3d0a66d02984fc6e85d61a'
               AT3 =  b'd23963e8cabeaa4a76899b5f5e3ee58d'
                MT =  b'c3462f82836a900aa43a7928b050c7c9'
                IT =  b'117f4c6a49d43a40d2b3e277ee6e2244'
           PADINFO =  b'08010000100100000801000010010000'
authentication tag =  b'5c2209f570ef626cb211725de2a9af06'
out                =
b'731bdd384f415c11081d08ecdc3efe5dd454792a75871ce616511d13983f9681804fcc83143603242c36
fe10cab4de855c2209f570ef626cb211725de2a9af06'
SPAE - decryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
b'731bdd384f415c11081d08ecdc3efe5dd454792a75871ce616511d13983f9681804fcc83143603242c36
fe10cab4de85'
associated data    =
b'00000000000000000000000000000006000000000000000000000000000000070a0b'
               PT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6e'
               CT0 =  b'a17e9f69e4f25a8b8620b4af78eefd6f'
               P0  =  b'00000000000000000000000000000003'
               C0  =  b'731bdd384f415c11081d08ecdc3efe5d'
               PT1 =  b'd2654251abb3069a8e3dbc43a4d00331'
               CT1 =  b'00000000000000000000000000000001'
               P1  =  b'00000000000000000000000000000004'
               C1  =  b'd454792a75871ce616511d13983f9681'
```

```
               PT2 =  b'd454792a75871ce616511d13983f9684'
               CT2 =  b'd2654251abb3069a8e3dbc43a4d00330'
               P2  =  b'09000000000000000000000000000000'
               C2  =  b'804fcc83143603242c36fe10cab4de85'
               PT3 =  b'5b2a8ed2bf8505bea20b42536e64ddb5'
               CT3 =  b'06313b7bde341a7c986ca1503cef95b4'
               AT1 =  b'131527259dc7975992e4bbfd0510e9fa'
               AT2 =  b'dba2c410fd3d0a66d02984fc6e85d61a'
               AT3 =  b'd23963e8cabeaa4a76899b5f5e3ee58d'
                MT =  b'c3462f82836a900aa43a7928b050c7c9'
                IT =  b'117f4c6a49d43a40d2b3e277ee6e2244'
           PADINFO =  b'08010000100100000801000010010000'
authentication tag =  b'5c2209f570ef626cb211725de2a9af06'
provided tag       =  b'5c2209f570ef626cb211725de2a9af06'
out                =
b'00000000000000000000000000000003000000000000000000000000000000000409'
```

```
SPAE - encryption
key                =  b'000102030405060708090a0b0c0d0e0f'
nonce              =  b'000102030405060708090a0b0c0d0e0f'
message            =
associated data    =
               PT0 =  b'0a9509b6456bf642f9ca9e53ca5ee455'
               CT0 =  b'0a940bb5416ef045f1c39458c653ea5a'
                MT =  b'fffefdfcfbfaf9f8f7f6f5f4f3f2f1f0'
                IT =  b'fffefdfcfbfaf9f8f7f6f5f4f3f2f1f0'
           PADINFO =  b'00000000000000000000000000000000'
authentication tag =  b'0a52cf639cf84370fe50b76d60eff179'
out                =  b'0a52cf639cf84370fe50b76d60eff179'
b'0a52cf639cf84370fe50b76d60eff179'
```

```
SPAE - encryption
key                =  b'000102030405060708090a0b0c0d0e0f'
nonce              =  b'000102030405060708090a0b0c0d0e0f'
message            =  b'000102030405060708090a0b0c0d0e0f'
associated data    =  b'000102030405060708090a0b0c0d0e0f'
               PT0 =  b'0a9509b6456bf642f9ca9e53ca5ee455'
               CT0 =  b'0a940bb5416ef045f1c39458c653ea5a'
               P0  =  b'000102030405060708090a0b0c0d0e0f'
               C0  =  b'9f7562a92c45ee0719ef6b6586554360'
               PT1 =  b'95e06b1f692e1845e025f5364c0ba735'
               CT1 =  b'000102030405060708090a0b0c0d0e0f'
               AT1 =  b'0a940bb5416ef045f1c39458c653ea5a'
                MT =  b'9de961146523164ae024f735480ea132'
                IT =  b'977d6aa1244de60f11e7636d8e5d4b68'
           PADINFO =  b'80000000800000008000000080000000'
authentication tag =  b'b524324d75cef37f1f2bc1ad2b242db8'
out                =
b'9f7562a92c45ee0719ef6b6586554360b524324d75cef37f1f2bc1ad2b242db8'
b'9f7562a92c45ee0719ef6b6586554360b524324d75cef37f1f2bc1ad2b242db8'
```

```
SPAE - encryption
key                =  b'000102030405060708090a0b0c0d0e0f'
nonce              =  b'000102030405060708090a0b0c0d0e0f'
message            =
b'000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f'
associated data    =
b'000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e'
               PT0 =  b'0a9509b6456bf642f9ca9e53ca5ee455'
               CT0 =  b'0a940bb5416ef045f1c39458c653ea5a'
               P0  =  b'000102030405060708090a0b0c0d0e0f'
               C0  =  b'9f7562a92c45ee0719ef6b6586554360'
               PT1 =  b'95e06b1f692e1845e025f5364c0ba735'
               CT1 =  b'000102030405060708090a0b0c0d0e0f'
               P1  =  b'101112131415161718191a1b1c1d1e1f'
               C1  =  b'80df406383afdf4ef689443e2c82916b'
               PT2 =  b'90cf507393bfcf5ee699542e3c92817b'
               CT2 =  b'95e1691c6d2b1e42e82cff3d4006a93a'
               AT1 =  b'0a940bb5416ef045f1c39458c653ea5a'
               AT2 =  b'68e2c19fa9096698ae35d29b54b0c601'
                MT =  b'78e3af4ed3b9666473783d3251b99f39'
                IT =  b'10016ed17ab000fcdd4defa905095938'
           PADINFO =  b'00010000f800000000010000f8000000'
authentication tag =  b'60dc7498e5e41a0ad07bd975ed5e97a3'
out                =
b'9f7562a92c45ee0719ef6b658655436080df406383afdf4ef689443e2c82916b60dc7498e5e41a0ad07b
d975ed5e97a3'
b'9f7562a92c45ee0719ef6b658655436080df406383afdf4ef689443e2c82916b60dc7498e5e41a0ad07b
d975ed5e97a3'
```

```
SPAE - encryption
key                =  b'000102030405060708090a0b0c0d0e0f'
nonce              =  b'000102030405060708090a0b0c0d0e0f'
message            =
b'000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f'
associated data    =
b'000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f'
               PT0 =  b'0a9509b6456bf642f9ca9e53ca5ee455'
               CT0 =  b'0a940bb5416ef045f1c39458c653ea5a'
               P0  =  b'000102030405060708090a0b0c0d0e0f'
               C0  =  b'9f7562a92c45ee0719ef6b6586554360'
               PT1 =  b'95e06b1f692e1845e025f5364c0ba735'
               CT1 =  b'000102030405060708090a0b0c0d0e0f'
               P1  =  b'101112131415161718191a1b1c1d1e1f'
               C1  =  b'80df406383afdf4ef689443e2c82916b'
               PT2 =  b'90cf507393bfcf5ee699542e3c92817b'
               CT2 =  b'95e1691c6d2b1e42e82cff3d4006a93a'
               AT1 =  b'0a940bb5416ef045f1c39458c653ea5a'
               AT2 =  b'3cf456b4ca488aa383c79c98b34797cb'
                MT =  b'78e3af4ed3b9666473783d3251b99f39'
                IT =  b'4417f9fa19f1ecc7f0bfa1aae2fe08f2'
           PADINFO =  b'000100000001000000001000000010000'
authentication tag =  b'697844f03d7e73f226d888d556f53058'
out                =
b'9f7562a92c45ee0719ef6b658655436080df406383afdf4ef689443e2c82916b697844f03d7e73f226d8
88d556f53058'
b'9f7562a92c45ee0719ef6b658655436080df406383afdf4ef689443e2c82916b697844f03d7e73f226d8
88d556f53058'
```

Conservative variant: CSPAE

In SPAE the key used for the block cipher calls is the result of the xor between the secret key and the nonce. This allows to mix the nonce with every block at minimal cost however this is unusual, all major mode of operations use the secret key directly. Due to this novel aspect, SPAE may be considered an experimental proposition rather than a drop in replacement in real world applications. This section describes a more conservative variant dubbed CSPAE. The differences are minimal so implementers may support both without significant overhead.

NOTE	When the nonce are null, CSPAE is equivalent to SPAE.

Differences with SPAE

kn equation

In CSPAE, the block cipher is always using the secret key directly. The nonce is injected in PT0 instead.

kn = k

CT0 and PT0

In CSPAE, CT0 and PT0 are values which depends on the nonce, as a result they cannot be precomputed anymore.

CT0 = Ek(nonce ^ k)

PT0 = nonce ^ k ^ Ek(nonce ^ k)

Built in DFA protection

CSPAE has the same level of DFA protection as SPAE. This section discuss the feasibility of a DFA attack on Ek, Ekn and Dkn steps within CSPAE.

Encryption

Assuming the nonce is not in the control of the attacker, C_i are unique to each computation. It follows that the C_i can't be used for a DFA since the attacker cannot get any exploitable pair.

The final Ekn must be protected for the same reason as in SPAE.

To conclude, in CSPAE encryption, all Ek and Ekn computations can be done without DFA countermeasures except the last one.

Decryption

When m > 0, the argumentation is exactly the same as SPAE. When m = 0, DFA is not possible for the simple reason that there is no output.

To conclude, in CSPAE decryption, all Ek and Ekn computations can be done without DFA countermeasures except the last one.

CSPAE Test Vectors

```
m=0,a=0
CSPAE - encryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
associated data    =
               PT0 =  b'd0017f493d6d576c9ea7d5683209ff1b'
               CT0 =  b'd0017f493d6d576c9ea7d5683209ff18'
                MT =  b'fffffffffffffffffffffffffffffffe'
                IT =  b'fffffffffffffffffffffffffffffffe'
           PADINFO =  b'00000000000000000000000000000000'
authentication tag =  b'0bec7271c5d3f69c28d934da38f0ac8c'
out                =  b'0bec7271c5d3f69c28d934da38f0ac8c'
```

```
m=0,a=1
CSPAE - encryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
associated data    =  b'00000000000000000000000000000006'
               PT0 =  b'd0017f493d6d576c9ea7d5683209ff1b'
               CT0 =  b'd0017f493d6d576c9ea7d5683209ff18'
               AT1 =  b'131527259dc7975992e4bbfd0510e9fa'
                MT =  b'fffffffffffffffffffffffffffffffe'
                IT =  b'ecead8da623868a66d1b4402faef1604'
           PADINFO =  b'00000000800000000000000080000000'
authentication tag =  b'74600b9d86873ce2999a6928ed9ac152'
out                =  b'74600b9d86873ce2999a6928ed9ac152'
```

```
m=1,a=0
CSPAE - encryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =  b'00000000000000000000000000000003'
associated data    =
               PT0 =  b'd0017f493d6d576c9ea7d5683209ff1b'
               CT0 =  b'd0017f493d6d576c9ea7d5683209ff18'
               P0  =  b'00000000000000000000000000000003'
               C0  =  b'af06863bfe5ab6f4d07ef32afba1baea'
               PT1 =  b'7f07f972c337e1984ed92642c9a845f1'
               CT1 =  b'00000000000000000000000000000003'
                MT =  b'7f07f972c337e19b4ed92642c9a845f1'
                IT =  b'7f07f972c337e19b4ed92642c9a845f1'
           PADINFO =  b'80000000000000008000000000000000'
authentication tag =  b'69d6f0bbc6c56a135b4cb34b6752c7bd'
out                =
b'af06863bfe5ab6f4d07ef32afba1baea69d6f0bbc6c56a135b4cb34b6752c7bd'
```

```
m=2,a=0
CSPAE - encryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
b'000000000000000000000000000000030000000000000000000000000000000004'
associated data    =
               PT0 =  b'd0017f493d6d576c9ea7d5683209ff1b'
               CT0 =  b'd0017f493d6d576c9ea7d5683209ff18'
               P0  =  b'00000000000000000000000000000003'
               C0  =  b'af06863bfe5ab6f4d07ef32afba1baea'
               PT1 =  b'7f07f972c337e1984ed92642c9a845f1'
               CT1 =  b'00000000000000000000000000000003'
               P1  =  b'00000000000000000000000000000004'
               C1  =  b'ecd2adc6b87c84f9a9f079b100f5bc96'
               PT2 =  b'ecd2adc6b87c84f9a9f079b100f5bc91'
               CT2 =  b'7f07f972c337e1984ed92642c9a845f2'
                MT =  b'a20b8b8471d4c10bd6f780c3c3c25d09'
                IT =  b'a20b8b8471d4c10bd6f780c3c3c25d09'
           PADINFO =  b'00010000000000000001000000000000'
authentication tag =  b'de39ac5f602ef05afc8729933de7b8be'
out                =
b'af06863bfe5ab6f4d07ef32afba1baeaecd2adc6b87c84f9a9f079b100f5bc96de39ac5f602ef05afc87
29933de7b8be'
```

```
m=3,a=0
CSPAE - encryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
b'000000000000000000000000000000300000000000000000000000000000004000000000000000000000
000000000005'
associated data    =
               PT0 =  b'd0017f493d6d576c9ea7d5683209ff1b'
               CT0 =  b'd0017f493d6d576c9ea7d5683209ff18'
               P0  =  b'00000000000000000000000000000003'
               C0  =  b'af06863bfe5ab6f4d07ef32afba1baea'
               PT1 =  b'7f07f972c337e1984ed92642c9a845f1'
               CT1 =  b'00000000000000000000000000000003'
               P1  =  b'00000000000000000000000000000004'
               C1  =  b'ecd2adc6b87c84f9a9f079b100f5bc96'
               PT2 =  b'ecd2adc6b87c84f9a9f079b100f5bc91'
               CT2 =  b'7f07f972c337e1984ed92642c9a845f2'
               P2  =  b'00000000000000000000000000000005'
               C2  =  b'38d4e578462b696ca7aed596e3fd14e3'
               PT3 =  b'47d31c0a851c88f4e977f3d42a555114'
               CT3 =  b'93d554b47b4b6561e7295ff3c95df963'
                MT =  b'a0fa43f94c4171977aa2a760511e3475'
                IT =  b'a0fa43f94c4171977aa2a760511e3475'
           PADINFO =  b'80010000000000008001000000000000'
authentication tag =  b'ddbd5c3f4573463da81445b8cc221bea'
out                =
b'af06863bfe5ab6f4d07ef32afba1baeaecd2adc6b87c84f9a9f079b100f5bc9638d4e578462b696ca7ae
d596e3fd14e3ddbd5c3f4573463da81445b8cc221bea'
```

```
m=3,a=1
CSPAE - encryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
b'00000000000000000000000000000003000000000000000000000000000000040000000000000000000
000000000005'
associated data    =  b'00000000000000000000000000000006'
               PT0 =  b'd0017f493d6d576c9ea7d5683209ff1b'
               CT0 =  b'd0017f493d6d576c9ea7d5683209ff18'
               P0  =  b'00000000000000000000000000000003'
               C0  =  b'af06863bfe5ab6f4d07ef32afba1baea'
               PT1 =  b'7f07f972c337e1984ed92642c9a845f1'
               CT1 =  b'00000000000000000000000000000003'
               P1  =  b'00000000000000000000000000000004'
               C1  =  b'ecd2adc6b87c84f9a9f079b100f5bc96'
               PT2 =  b'ecd2adc6b87c84f9a9f079b100f5bc91'
               CT2 =  b'7f07f972c337e1984ed92642c9a845f2'
               P2  =  b'00000000000000000000000000000005'
               C2  =  b'38d4e578462b696ca7aed596e3fd14e3'
               PT3 =  b'47d31c0a851c88f4e977f3d42a555114'
               CT3 =  b'93d554b47b4b6561e7295ff3c95df963'
               AT1 =  b'131527259dc7975992e4bbfd0510e9fa'
                MT =  b'a0fa43f94c4171977aa2a760511e3475'
                IT =  b'b3ef64dcd186e6cee8461c9d540edd8f'
           PADINFO =  b'80010000800000008001000080000000'
authentication tag =  b'bf5292625deaa4a645b78d47902ef71f'
out                =
b'af06863bfe5ab6f4d07ef32afba1baeaecd2adc6b87c84f9a9f079b100f5bc9638d4e578462b696ca7ae
d596e3fd14e3bf5292625deaa4a645b78d47902ef71f'
```

```
m=3,a=2
CSPAE - encryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
b'000000000000000000000000000000300000000000000000000000000000004000000000000000000000
000000000005'
associated data    =
b'000000000000000000000000000000600000000000000000000000000000007'
               PT0 =  b'd0017f493d6d576c9ea7d5683209ff1b'
               CT0 =  b'd0017f493d6d576c9ea7d5683209ff18'
               P0  =  b'00000000000000000000000000000003'
               C0  =  b'af06863bfe5ab6f4d07ef32afba1baea'
               PT1 =  b'7f07f972c337e1984ed92642c9a845f1'
               CT1 =  b'00000000000000000000000000000003'
               P1  =  b'00000000000000000000000000000004'
               C1  =  b'ecd2adc6b87c84f9a9f079b100f5bc96'
               PT2 =  b'ecd2adc6b87c84f9a9f079b100f5bc91'
               CT2 =  b'7f07f972c337e1984ed92642c9a845f2'
               P2  =  b'00000000000000000000000000000005'
               C2  =  b'38d4e578462b696ca7aed596e3fd14e3'
               PT3 =  b'47d31c0a851c88f4e977f3d42a555114'
               CT3 =  b'93d554b47b4b6561e7295ff3c95df963'
               AT1 =  b'131527259dc7975992e4bbfd0510e9fa'
               AT2 =  b'dba2c410fd3d0a66d02984fc6e85d61a'
                MT =  b'a0fa43f94c4171977aa2a760511e3475'
                IT =  b'7b5887e9b17c7bf1aa8b239c3f9be26f'
           PADINFO =  b'800100000010000800100000010000'
authentication tag =  b'8896a7c8d4d6e585753fbecf68d12e69'
out                =
b'af06863bfe5ab6f4d07ef32afba1baeaecd2adc6b87c84f9a9f079b100f5bc9638d4e578462b696ca7ae
d596e3fd14e38896a7c8d4d6e585753fbecf68d12e69'
```

```
m=3,a=3
CSPAE - encryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
b'000000000000000000000000000000300000000000000000000000000000004000000000000000000000
000000000005'
associated data    =
b'000000000000000000000000000000600000000000000000000000000000007000000000000000000000
000000000008'
               PT0 =  b'd0017f493d6d576c9ea7d5683209ff1b'
               CT0 =  b'd0017f493d6d576c9ea7d5683209ff18'
               P0  =  b'00000000000000000000000000000003'
               C0  =  b'af06863bfe5ab6f4d07ef32afba1baea'
               PT1 =  b'7f07f972c337e1984ed92642c9a845f1'
               CT1 =  b'00000000000000000000000000000003'
```

```
               P1  =  b'00000000000000000000000000000004'
               C1  =  b'ecd2adc6b87c84f9a9f079b100f5bc96'
               PT2 =  b'ecd2adc6b87c84f9a9f079b100f5bc91'
               CT2 =  b'7f07f972c337e1984ed92642c9a845f2'
               P2  =  b'00000000000000000000000000000005'
               C2  =  b'38d4e578462b696ca7aed596e3fd14e3'
               PT3 =  b'47d31c0a851c88f4e977f3d42a555114'
               CT3 =  b'93d554b47b4b6561e7295ff3c95df963'
               AT1 =  b'131527259dc7975992e4bbfd0510e9fa'
               AT2 =  b'dba2c410fd3d0a66d02984fc6e85d61a'
               AT3 =  b'7152d55728d8c03e547ab64cd21531fa'
                MT =  b'a0fa43f94c4171977aa2a760511e3475'
                IT =  b'd1a896ae6499b1a92ed8112c830b058f'
           PADINFO =  b'80010000800100008001000080010000'
authentication tag =  b'1b2c40d4b921b5fea3a2c773367276b3'
out                =
b'af06863bfe5ab6f4d07ef32afba1baeaecd2adc6b87c84f9a9f079b100f5bc9638d4e578462b696ca7ae
d596e3fd14e31b2c40d4b921b5fea3a2c773367276b3'
CSPAE - decryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
b'af06863bfe5ab6f4d07ef32afba1baeaecd2adc6b87c84f9a9f079b100f5bc9638d4e578462b696ca7ae
d596e3fd14e3'
associated data    =
b'000000000000000000000000000000060000000000000000000000000000000700000000000000000000
000000000008'
               PT0 =  b'd0017f493d6d576c9ea7d5683209ff1b'
               CT0 =  b'd0017f493d6d576c9ea7d5683209ff18'
               P0  =  b'00000000000000000000000000000003'
               C0  =  b'af06863bfe5ab6f4d07ef32afba1baea'
               PT1 =  b'7f07f972c337e1984ed92642c9a845f1'
               CT1 =  b'00000000000000000000000000000003'
               P1  =  b'00000000000000000000000000000004'
               C1  =  b'ecd2adc6b87c84f9a9f079b100f5bc96'
               PT2 =  b'ecd2adc6b87c84f9a9f079b100f5bc91'
               CT2 =  b'7f07f972c337e1984ed92642c9a845f2'
               P2  =  b'00000000000000000000000000000005'
               C2  =  b'38d4e578462b696ca7aed596e3fd14e3'
               PT3 =  b'47d31c0a851c88f4e977f3d42a555114'
               CT3 =  b'93d554b47b4b6561e7295ff3c95df963'
               AT1 =  b'131527259dc7975992e4bbfd0510e9fa'
               AT2 =  b'dba2c410fd3d0a66d02984fc6e85d61a'
               AT3 =  b'7152d55728d8c03e547ab64cd21531fa'
                MT =  b'a0fa43f94c4171977aa2a760511e3475'
                IT =  b'd1a896ae6499b1a92ed8112c830b058f'
           PADINFO =  b'80010000800100008001000080010000'
authentication tag =  b'1b2c40d4b921b5fea3a2c773367276b3'
provided tag       =  b'1b2c40d4b921b5fea3a2c773367276b3'
out                =
b'000000000000000000000000000000030000000000000000000000000000000400000000000000000000
```

```
000000000005'
```

```
m=3,a=3 padded
CSPAE - encryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
b'000000000000000000000000000000030000000000000000000000000000000409'
associated data    =
b'000000000000000000000000000000060000000000000000000000000000070a0b'
               PT0 =  b'd0017f493d6d576c9ea7d5683209ff1b'
               CT0 =  b'd0017f493d6d576c9ea7d5683209ff18'
               P0  =  b'00000000000000000000000000000003'
               C0  =  b'af06863bfe5ab6f4d07ef32afba1baea'
               PT1 =  b'7f07f972c337e1984ed92642c9a845f1'
               CT1 =  b'00000000000000000000000000000003'
               P1  =  b'00000000000000000000000000000004'
               C1  =  b'ecd2adc6b87c84f9a9f079b100f5bc96'
               PT2 =  b'ecd2adc6b87c84f9a9f079b100f5bc91'
               CT2 =  b'7f07f972c337e1984ed92642c9a845f2'
               P2  =  b'09000000000000000000000000000000'
               C2  =  b'a5405b16f5db2622e1c90deba9f25963'
               PT3 =  b'd347a26436ecc7baaf102ba9605a1c91'
               CT3 =  b'93d554b47b4b6561e7295ff3c95df963'
               AT1 =  b'131527259dc7975992e4bbfd0510e9fa'
               AT2 =  b'dba2c410fd3d0a66d02984fc6e85d61a'
               AT3 =  b'd23963e8cabeaa4a76899b5f5e3ee58d'
                MT =  b'346efd97ffb13ed93cc57f1d1b1179f0'
                IT =  b'e6579e7f350f94934a4ce442452f9c7d'
           PADINFO =  b'08010000100100000801000010010000'
authentication tag =  b'e6b45ced002704ca27ac396b78007bd9'
out                =
b'af06863bfe5ab6f4d07ef32afba1baeaecd2adc6b87c84f9a9f079b100f5bc96a5405b16f5db2622e1c9
0deba9f25963e6b45ced002704ca27ac396b78007bd9'
CSPAE - decryption
key                =  b'00000000000000000000000000000001'
nonce              =  b'00000000000000000000000000000002'
message            =
b'af06863bfe5ab6f4d07ef32afba1baeaecd2adc6b87c84f9a9f079b100f5bc96a5405b16f5db2622e1c9
0deba9f25963'
associated data    =
b'000000000000000000000000000000060000000000000000000000000000070a0b'
               PT0 =  b'd0017f493d6d576c9ea7d5683209ff1b'
               CT0 =  b'd0017f493d6d576c9ea7d5683209ff18'
               P0  =  b'00000000000000000000000000000003'
               C0  =  b'af06863bfe5ab6f4d07ef32afba1baea'
               PT1 =  b'7f07f972c337e1984ed92642c9a845f1'
               CT1 =  b'00000000000000000000000000000003'
               P1  =  b'00000000000000000000000000000004'
               C1  =  b'ecd2adc6b87c84f9a9f079b100f5bc96'
```

```
               PT2 =  b'ecd2adc6b87c84f9a9f079b100f5bc91'
               CT2 =  b'7f07f972c337e1984ed92642c9a845f2'
               P2  =  b'09000000000000000000000000000000'
               C2  =  b'a5405b16f5db2622e1c90deba9f25963'
               PT3 =  b'd347a26436ecc7baaf102ba9605a1c91'
               CT3 =  b'93d554b47b4b6561e7295ff3c95df963'
               AT1 =  b'131527259dc7975992e4bbfd0510e9fa'
               AT2 =  b'dba2c410fd3d0a66d02984fc6e85d61a'
               AT3 =  b'd23963e8cabeaa4a76899b5f5e3ee58d'
                MT =  b'346efd97ffb13ed93cc57f1d1b1179f0'
                IT =  b'e6579e7f350f94934a4ce442452f9c7d'
           PADINFO =  b'08010000100100000801000010010000'
authentication tag =  b'e6b45ced002704ca27ac396b78007bd9'
provided tag       =  b'e6b45ced002704ca27ac396b78007bd9'
out                =
b'00000000000000000000000000000000300000000000000000000000000000000409'
```

```
CSPAE - encryption
key                =  b'000102030405060708090a0b0c0d0e0f'
nonce              =  b'000102030405060708090a0b0c0d0e0f'
message            =
associated data    =
               PT0 =  b'c6a13b37878f5b826f4f8162a1c8d879'
               CT0 =  b'c6a13b37878f5b826f4f8162a1c8d879'
                MT =  b'fffefdfcfbfaf9f8f7f6f5f4f3f2f1f0'
                IT =  b'fffefdfcfbfaf9f8f7f6f5f4f3f2f1f0'
           PADINFO =  b'00000000000000000000000000000000'
authentication tag =  b'7525d79334164e254cba038b814d9c20'
out                =  b'7525d79334164e254cba038b814d9c20'
b'7525d79334164e254cba038b814d9c20'
```

```
CSPAE - encryption
key                =  b'000102030405060708090a0b0c0d0e0f'
nonce              =  b'000102030405060708090a0b0c0d0e0f'
message            =  b'000102030405060708090a0b0c0d0e0f'
associated data    =  b'000102030405060708090a0b0c0d0e0f'
               PT0 =  b'c6a13b37878f5b826f4f8162a1c8d879'
               CT0 =  b'c6a13b37878f5b826f4f8162a1c8d879'
               P0  =  b'000102030405060708090a0b0c0d0e0f'
               C0  =  b'732b2b535f23f219b6ffc139248d2dc2'
               PT1 =  b'b58b1267dca9af9cd1b94a508948fbb4'
               CT1 =  b'00000000000000000000000000000000'
               AT1 =  b'0a940bb5416ef045f1c39458c653ea5a'
                MT =  b'b58b1267dca9af9cd1b94a508948fbb4'
                IT =  b'bf1f19d29dc75fd9207ade084f1b11ee'
           PADINFO =  b'80000000800000008000000080000000'
authentication tag =  b'0a1315ef625aedc8e354116928defef3'
out                =
b'732b2b535f23f219b6ffc139248d2dc20a1315ef625aedc8e354116928defef3'
b'732b2b535f23f219b6ffc139248d2dc20a1315ef625aedc8e354116928defef3'
```

```
CSPAE - encryption
key                =  b'000102030405060708090a0b0c0d0e0f'
nonce              =  b'000102030405060708090a0b0c0d0e0f'
message            =
b'000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f'
associated data    =
b'000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e'
               PT0 =  b'c6a13b37878f5b826f4f8162a1c8d879'
               CT0 =  b'c6a13b37878f5b826f4f8162a1c8d879'
               P0  =  b'000102030405060708090a0b0c0d0e0f'
               C0  =  b'732b2b535f23f219b6ffc139248d2dc2'
               PT1 =  b'b58b1267dca9af9cd1b94a508948fbb4'
               CT1 =  b'00000000000000000000000000000000'
               P1  =  b'101112131415161718191a1b1c1d1e1f'
               C1  =  b'b85c0d5fa953bf572a125c9479b2e862'
               PT2 =  b'a84d1f4cbd46a940320b468f65aff67d'
               CT2 =  b'b58b1267dca9af9cd1b94a508948fbb4'
               AT1 =  b'0a940bb5416ef045f1c39458c653ea5a'
               AT2 =  b'68e2c19fa9096698ae35d29b54b0c601'
                MT =  b'79f4551c340e52f4878054e8b90659e1'
                IT =  b'111694839d07346c29b58673edb69fe0'
           PADINFO =  b'00010000f800000000010000f8000000'
authentication tag =  b'6918ce72c046c8e5159254cfe2065600'
out                =
b'732b2b535f23f219b6ffc139248d2dc2b85c0d5fa953bf572a125c9479b2e8626918ce72c046c8e51592
54cfe2065600'
b'732b2b535f23f219b6ffc139248d2dc2b85c0d5fa953bf572a125c9479b2e8626918ce72c046c8e51592
54cfe2065600'
```

```
CSPAE - encryption
key                =  b'000102030405060708090a0b0c0d0e0f'
nonce              =  b'000102030405060708090a0b0c0d0e0f'
message            =
b'000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f'
associated data    =
b'000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f'
               PT0 =  b'c6a13b37878f5b826f4f8162a1c8d879'
               CT0 =  b'c6a13b37878f5b826f4f8162a1c8d879'
               P0  =  b'000102030405060708090a0b0c0d0e0f'
               C0  =  b'732b2b535f23f219b6ffc139248d2dc2'
               PT1 =  b'b58b1267dca9af9cd1b94a508948fbb4'
               CT1 =  b'00000000000000000000000000000000'
               P1  =  b'101112131415161718191a1b1c1d1e1f'
               C1  =  b'b85c0d5fa953bf572a125c9479b2e862'
               PT2 =  b'a84d1f4cbd46a940320b468f65aff67d'
               CT2 =  b'b58b1267dca9af9cd1b94a508948fbb4'
               AT1 =  b'0a940bb5416ef045f1c39458c653ea5a'
               AT2 =  b'3cf456b4ca488aa383c79c98b34797cb'
                MT =  b'79f4551c340e52f4878054e8b90659e1'
                IT =  b'450003a8fe46d8570447c8700a41ce2a'
           PADINFO =  b'00010000000100000001000000010000'
authentication tag =  b'5135faad34fa275762e1dc2399a40705'
out                =
b'732b2b535f23f219b6ffc139248d2dc2b85c0d5fa953bf572a125c9479b2e8625135faad34fa275762e1
dc2399a40705'
b'732b2b535f23f219b6ffc139248d2dc2b85c0d5fa953bf572a125c9479b2e8625135faad34fa275762e1
dc2399a40705'
```