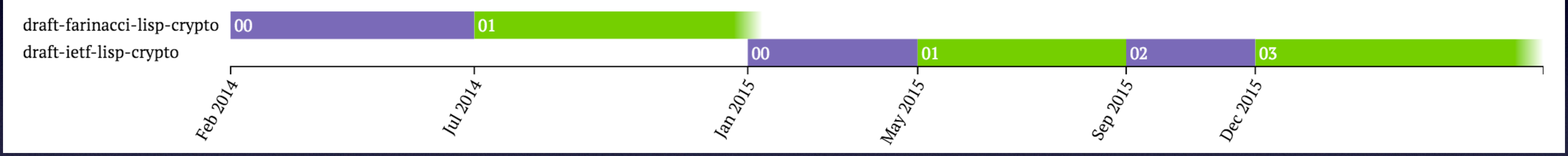
# LISP Data-Plane Cryptography

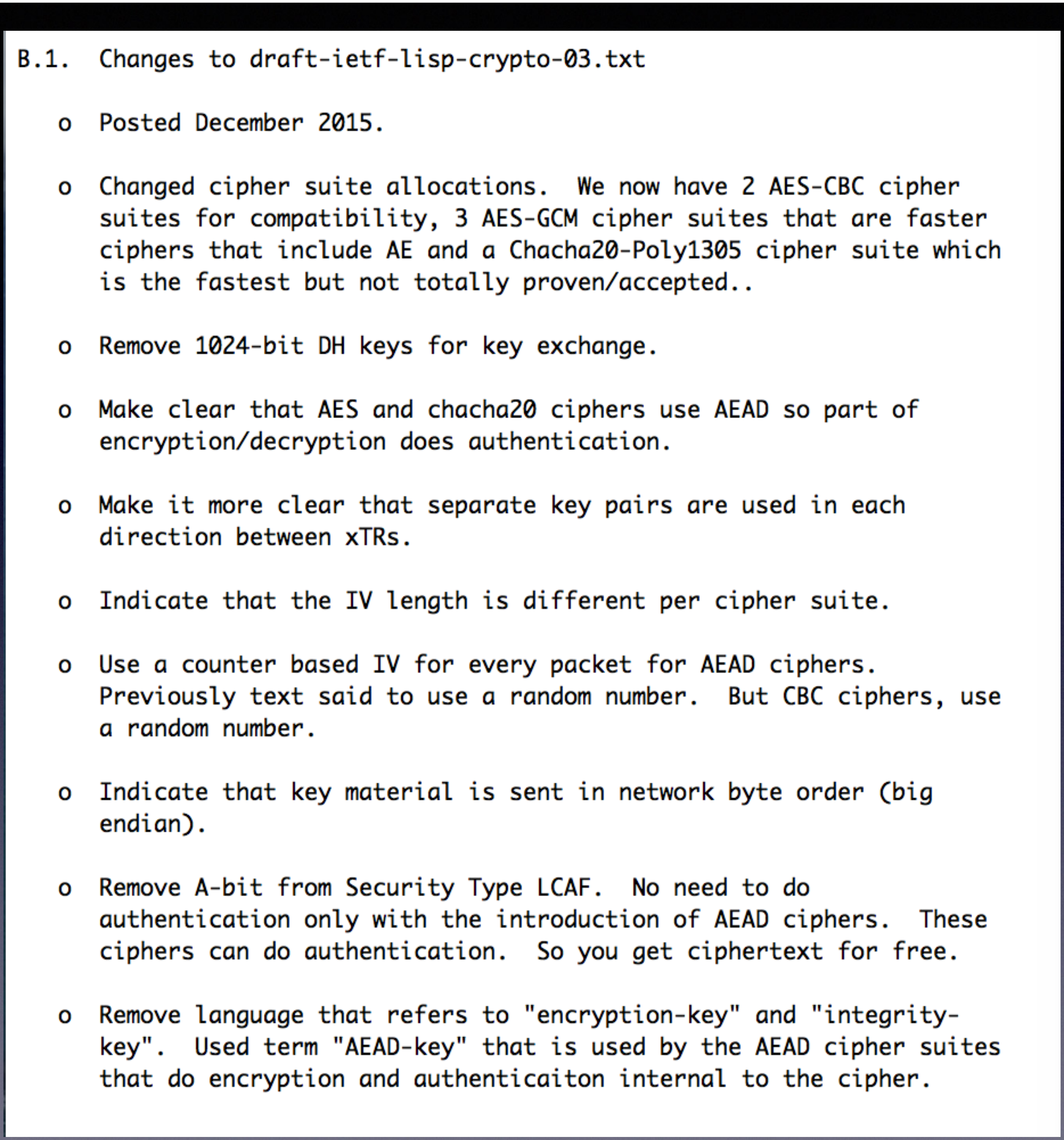
`draft-ietf-lisp-crypto-03`

*LISP Working Group - Buenos Aires IETF*
April 2016

*Dino Farinacci & Brian Weis*

# Draft History

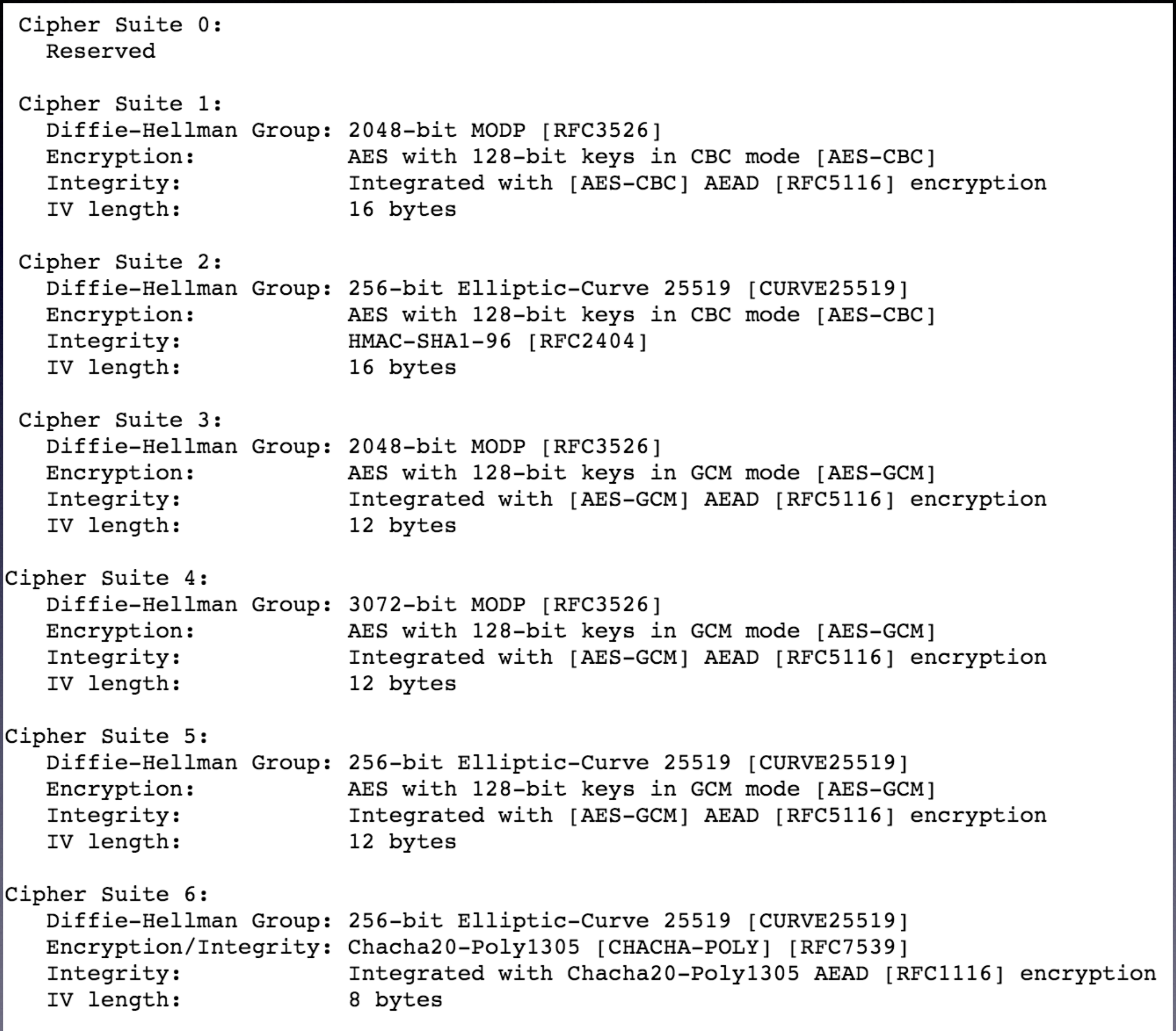




## B.1. Changes to draft-ietf-lisp-crypto-03.txt

- Posted December 2015.
- Changed cipher suite allocations. We now have 2 AES-CBC cipher suites for compatibility, 3 AES-GCM cipher suites that are faster ciphers that include AE and a Chacha20-Poly1305 cipher suite which is the fastest but not totally proven/accepted..
- Remove 1024-bit DH keys for key exchange.
- Make clear that AES and chacha20 ciphers use AEAD so part of encryption/decryption does authentication.
- Make it more clear that separate key pairs are used in each direction between xTRs.
- Indicate that the IV length is different per cipher suite.
- Use a counter based IV for every packet for AEAD ciphers. Previously text said to use a random number. But CBC ciphers, use a random number.
- Indicate that key material is sent in network byte order (big endian).
- Remove A-bit from Security Type LCAF. No need to do authentication only with the introduction of AEAD ciphers. These ciphers can do authentication. So you get ciphertext for free.
- Remove language that refers to "encryption-key" and "integrity-key". Used term "AEAD-key" that is used by the AEAD cipher suites that do encryption and authenticaiton internal to the cipher.

# Current Cipher Suites



```
 Cipher Suite 0:
   Reserved
```

DH with CBC traditional

```
 Cipher Suite 1:
   Diffie-Hellman Group: 2048-bit MODP [RFC3526]
   Encryption:           AES with 128-bit keys in CBC mode [AES-CBC]
   Integrity:            Integrated with [AES-CBC] AEAD [RFC5116] encryption
   IV length:            16 bytes
```

ECDH with CBC

```
 Cipher Suite 2:
   Diffie-Hellman Group: 256-bit Elliptic-Curve 25519 [CURVE25519]
   Encryption:           AES with 128-bit keys in CBC mode [AES-CBC]
   Integrity:            HMAC-SHA1-96 [RFC2404]
   IV length:            16 bytes
```

DH with GCM big keys

```
 Cipher Suite 3:
   Diffie-Hellman Group: 2048-bit MODP [RFC3526]
   Encryption:           AES with 128-bit keys in GCM mode [AES-GCM]
   Integrity:            Integrated with [AES-GCM] AEAD [RFC5116] encryption
   IV length:            12 bytes
```

DH with GCM bigger keys

```
Cipher Suite 4:
   Diffie-Hellman Group: 3072-bit MODP [RFC3526]
   Encryption:           AES with 128-bit keys in GCM mode [AES-GCM]
   Integrity:            Integrated with [AES-GCM] AEAD [RFC5116] encryption
   IV length:            12 bytes
```

ECDH with GCM

```
Cipher Suite 5:
   Diffie-Hellman Group: 256-bit Elliptic-Curve 25519 [CURVE25519]
   Encryption:           AES with 128-bit keys in GCM mode [AES-GCM]
   Integrity:            Integrated with [AES-GCM] AEAD [RFC5116] encryption
   IV length:            12 bytes
```

ECDH/chacha/poly

```
Cipher Suite 6:
   Diffie-Hellman Group: 256-bit Elliptic-Curve 25519 [CURVE25519]
   Encryption/Integrity: Chacha20-Poly1305 [CHACHA-POLY] [RFC7539]
   Integrity:            Integrated with Chacha20-Poly1305 AEAD [RFC1116] encryption
   IV length:            8 bytes
```

# Implementation Status

- *lispers.net* has a -02 implementation (not -03 yet)
- Supports ECDH with Curve25519
- Supports rekeying via RLOC-probing
- Added Poly1305 authentication
    - So cipher-suite 6 is an AEAD implementation

# Should we advance document?