

# LISP Data-Plane Cryptography

draft-ietf-lisp-crypto-02

LISP Working Group - Yokohama IETF  
October 2015

*Dino Farinacci & Brian Weis*

# Document Status

- WG draft -00 created **Jan 2015**, presented in Dallas **spring 2015**
- WG draft -01 created **May 2015**, presented in Prague **summer 2015**
- WG draft -02 created **Sep 2015**, presented here in Yokohama **fall 2015**

# Design Summary

- Diffie-Hellman exchange via Map-Request/Map-Reply
- Keys not stored by third-party
- Keys are ephemeral
- *ITR encrypt-n-encap -> ETR decap-n-decrypt*
- Rekeying part of RLOC-probing
- Cipher suite negotiation for AEAD
  - AES and Chacha20 ciphers
  - SHA1/Poly1305 HMACs

# Changes to -02

## Cipher Suite 4:

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](#)]

## Cipher Suite 5:

Diffie-Hellman Group: 256-bit Elliptic-Curve 25519 [[CURVE25519](#)]  
Encryption: Chacha20 [[CHACHA-POLY](#)]  
Integrity: Poly1305 [[CHACHA-POLY](#)] (i.e. AEAD\_CHACHA20\_POLY1305)

# Implementation Status

- *lispers.net* has a -02 implementation

```
Cipher Suite 1:  
  Diffie-Hellman Group: 1024-bit Modular Exponential (MODP) [RFC2409]  
  Encryption:          AES with 128-bit keys in CBC mode [AES-CBC]  
  Integrity:           HMAC-SHA1-96 [RFC2404]  
  
Cipher Suite 4:  
  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]
```

- Uses ECDH instead of regular DH:
  - RFC5114 *gx* value from the “192-bit Random ECP Group”
  - Added Curve25519
- Supports rekeying via RLOC-probing
- Support for unidirectional encryption across NATs
  - RTR to xTR-behind NAT as well as xTR-behind-NAT to RTR

# Chacha20 vs AES

Look at “crypto-time” below in microseconds.

With AES for 1000-byte packets:

```
09/17/15 17:20:05.151: itr: Receive en0, MACs: b8f6-b11b-ac49 -> b475-0e4d-2f4a, [255]5.5.5.5 -> [255]2.2.2.2, tos/ttl: 0/64, length: 1028, packet: 45000404 6b120000 4001fdd9 05050505 02020202 08003f85 ba480011 55fb58b5 0001c9fb 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f ...
09/17/15 17:20:05.151: itr: Lookup for EID [255]2.2.2.2 found map-cache entry [255]2.2.2.2/32
09/17/15 17:20:05.151: itr: Packet hash is 0, best-rloc-list: [['1.0.0.2', 'up-state']]
09/17/15 17:20:05.152: itr: Encrypt (aes) for key-id: 1, RLOC: 1.0.0.2, ICV: 0x7c36fb8a...b548d41f, crypto-time: 790855 usec
09/17/15 17:20:05.152: itr: Send LISP packet, outer RLOCs: [255]1.0.0.1 -> [0]1.0.0.2, outer tos/ttl: 0/63, outer ttl: 0x1f0 -> 4341, inner EIDs: [255]5.5.5.5 -> [255]2.2.2.2, inner tos/ttl: 0/63, length: 1112, encrypt/encap LISP-header -> flags: NlevIpK1, nonce: 0x8f4dff, iid/lbsb: 0xff00, packet: 45000458 ddfd4000 3f1155b3 01000001 01000002 f00010f5 04440000 858f4dff 0000ff00 37a57b5e c4b7d831 a15fed84 4d870b77 e560001c ...
09/17/15 17:20:06.161: itr: Receive en0, MACs: b8f6-b11b-ac49 -> b475-0e4d-2f4a, [255]5.5.5.5 -> [255]2.2.2.2, tos/ttl: 0/64, length: 1028, packet: 45000404 c9570000 40019f94 05050505 02020202 08003086 ba480012 55fb58b6 0001d8f8 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f ...
09/17/15 17:20:06.161: itr: Lookup for EID [255]2.2.2.2 found map-cache entry [255]2.2.2.2/32
09/17/15 17:20:06.161: itr: Packet hash is 0, best-rloc-list: [['1.0.0.2', 'up-state']]
09/17/15 17:20:06.161: itr: Encrypt (aes) for key-id: 1, RLOC: 1.0.0.2, ICV: 0x1770b5e0...641d9f5b, crypto-time: 694129 usec
09/17/15 17:20:06.161: itr: Send LISP packet, outer RLOCs: [255]1.0.0.1 -> [0]1.0.0.2, outer tos/ttl: 0/63, outer ttl: 0x1f0 -> 4341, inner EIDs: [255]5.5.5.5 -> [255]2.2.2.2, inner tos/ttl: 0/63, length: 1112, encrypt/encap LISP-header -> flags: NlevIpK1, nonce: 0xdf0e47, iid/lbsb: 0xff00, packet: 45000458 ddfd4000 3f1155b3 01000001 01000002 f00010f5 04440000 85df0e47 0000ff00 37a57b5e c4b7d831 a25fed84 4d870b77 fb9fd50d ...
```

With CHACHA for 1000-byte packets:

```
09/17/15 17:20:19.193: itr: Receive en0, MACs: b8f6-b11b-ac49 -> b475-0e4d-2f4a, [255]5.5.5.5 -> [255]2.2.2.2, tos/ttl: 0/64, length: 1028, packet: 45000404 2af50000 40013df7 05050505 02020202 0800ad0d ba48001f 55fb58c3 00025c56 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f ...
09/17/15 17:20:19.193: itr: Lookup for EID [255]2.2.2.2 found map-cache entry [255]2.2.2.2/32
09/17/15 17:20:19.193: itr: Packet hash is 0, best-rloc-list: [['1.0.0.2', 'up-state']]
09/17/15 17:20:19.195: itr: Encrypt (chacha) for key-id: 1, RLOC: 1.0.0.2, ICV: 0xdb08af47...e480685c, crypto-time: 1658 usec
09/17/15 17:20:19.195: itr: Send LISP packet, outer RLOCs: [255]1.0.0.1 -> [0]1.0.0.2, outer tos/ttl: 0/63, outer ttl: 0x1f0 -> 4341, inner EIDs: [255]5.5.5.5 -> [255]2.2.2.2, inner tos/ttl: 0/63, length: 1104, encrypt/encap LISP-header -> flags: NlevIpK1, nonce: 0x2d8be, iid/lbsb: 0xff00, packet: 45000450 ddfd4000 3f1155bb 01000001 01000002 f00010f5 043c0000 8502d8be 0000ff00 f8059f7e ef90083f e3fad633 35cb3768 2c876185 ...
09/17/15 17:20:20.200: itr: Receive en0, MACs: b8f6-b11b-ac49 -> b475-0e4d-2f4a, [255]5.5.5.5 -> [255]2.2.2.2, tos/ttl: 0/64, length: 1028, packet: 45000404 f7bc0000 4001712f 05050505 02020202 08009f1e ba480020 55fb58c4 00026a43 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f ...
09/17/15 17:20:20.200: itr: Lookup for EID [255]2.2.2.2 found map-cache entry [255]2.2.2.2/32
09/17/15 17:20:20.200: itr: Packet hash is 0, best-rloc-list: [['1.0.0.2', 'up-state']]
09/17/15 17:20:20.202: itr: Encrypt (chacha) for key-id: 1, RLOC: 1.0.0.2, ICV: 0xb0c71472...c9bf718a, crypto-time: 1800 usec
09/17/15 17:20:20.202: itr: Send LISP packet, outer RLOCs: [255]1.0.0.1 -> [0]1.0.0.2, outer tos/ttl: 0/63, outer ttl: 0x1f0 -> 4341, inner EIDs: [255]5.5.5.5 -> [255]2.2.2.2, inner tos/ttl: 0/63, length: 1104, encrypt/encap LISP-header -> flags: NlevIpK1, nonce: 0x7eaa61, iid/lbsb: 0xff00, packet: 45000450 ddfd4000 3f1155bb 01000001 01000002 f00010f5 043c0000 857eaa61 0000ff00 f9059f7e ef90083f 20b9a473 8b3d2139 cc6b216a ...
09/17/15 17:20:21.210: itr: Receive en0, MACs: b8f6-b11b-ac49 -> b475-0e4d-2f4a, [255]5.5.5.5 -> [255]2.2.2.2, tos/ttl: 0/64, length: 1028, packet: 45000404 ebbf0000 40017d2c 05050505 02020202 08009dbd ba480021 55fb58c5 00026ba2 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f ...
09/17/15 17:20:21.210: itr: Lookup for EID [255]2.2.2.2 found map-cache entry [255]2.2.2.2/32
09/17/15 17:20:21.210: itr: Packet hash is 0, best-rloc-list: [['1.0.0.2', 'up-state']]
09/17/15 17:20:21.212: itr: Encrypt (chacha) for key-id: 1, RLOC: 1.0.0.2, ICV: 0xf8e8415c...5c739a0f, crypto-time: 1690 usec
09/17/15 17:20:21.212: itr: Send LISP packet, outer RLOCs: [255]1.0.0.1 -> [0]1.0.0.2, outer tos/ttl: 0/63, outer ttl: 0x1f0 -> 4341, inner EIDs: [255]5.5.5.5 -> [255]2.2.2.2, inner tos/ttl: 0/63, length: 1104, encrypt/encap LISP-header -> flags: NlevIpK1, nonce: 0x4d244b, iid/lbsb: 0xff00, packet: 45000450 ddfd4000 3f1155bb 01000001 01000002 f00010f5 043c0000 854d244b 0000ff00 fa059f7e ef90083f 09df2147 f2ddf068 11e3cfd4 ...
```

# Chacha20 for 100-byte pings

```
dino-macbook-> egrep chacha-time logs/lisp-etr.log
09/23/15 11:09:15.695: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0xa62dcb19...b82810a7 (good),
chacha-time 581 usec
09/23/15 11:09:16.697: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x128b04a3...e715570e (good),
chacha-time 454 usec
09/23/15 11:09:17.703: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0xbd6d943f...70cf2012 (good),
chacha-time 266 usec
09/23/15 11:09:18.709: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0xabfd1027...724a05e2 (good),
chacha-time 513 usec
09/23/15 11:09:19.712: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0xdc2e7319...e600549c (good),
chacha-time 498 usec
09/23/15 11:09:20.720: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x261b62f2...f237501d (good),
chacha-time 725 usec
09/23/15 11:09:21.723: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x40298619...24bb57c5 (good),
chacha-time 527 usec
09/23/15 11:09:22.728: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x3b3c2335...fc678639 (good),
chacha-time 370 usec
09/23/15 11:09:23.740: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x98f2f50d...848992f9 (good),
chacha-time 383 usec
09/23/15 11:09:24.744: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0xddb3454c...0564cca6 (good),
chacha-time 380 usec
09/23/15 11:09:25.661: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0xcc64e190...de1feb61 (good),
chacha-time 380 usec
09/23/15 11:09:26.660: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0xa51d9200...dff2f901 (good),
chacha-time 368 usec
09/23/15 11:09:27.671: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x32465ffe...0450f060 (good),
chacha-time 485 usec
09/23/15 11:09:28.680: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x35576703...70eb07df (good),
chacha-time 380 usec
09/23/15 11:09:29.688: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x01c6ab42...e1253fdc (good),
chacha-time 372 usec
09/23/15 11:09:30.697: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x48926ccd...1e2d15c9 (good),
chacha-time 401 usec
09/23/15 11:09:31.705: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x9cae2e34...9fbd11c8 (good),
chacha-time 380 usec
09/23/15 11:09:32.711: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x7db401c8...66c03003 (good),
chacha-time 250 usec
09/23/15 11:09:33.719: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x86f531d4...d665ddd5 (good),
chacha-time 370 usec
09/23/15 11:09:34.729: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x3d92efe7...2fec1789 (good),
chacha-time 313 usec
09/23/15 11:09:35.736: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0xd3b45543...b86b0c74 (good),
chacha-time 377 usec
09/23/15 11:09:36.748: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x6fd5154f...aad0ab5f (good),
chacha-time 380 usec
```

# Implementation Todo List

- Key Related Testing
  - Larger keys, other ECDH groups, and other ciphers ✓
  - Multi-key rekeying logic
- Multi-Feature Testing
  - Test multicast in unicast encapsulation ✓
  - Test with LISP-SEC
- Interoperability Testing
  - Making a call for more implementations ✓
  - How about *lispmob* and open source the code?



Questions?