t_cose 2.0 project
IETF 117 Hackathon

https://github.com/laurencelundblade/t_cose

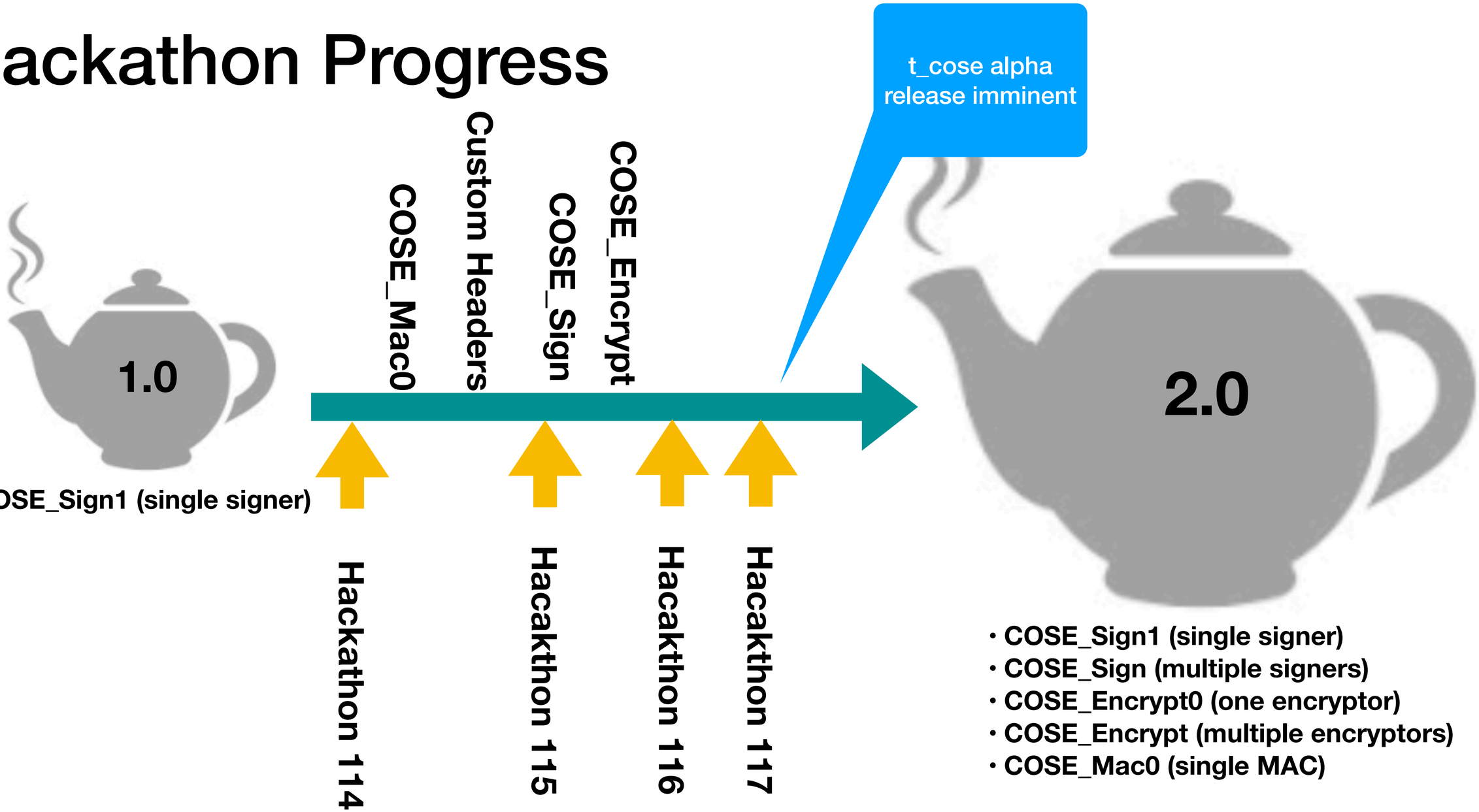
- t_cose == “Trusted-COSE”
- C implementation of COSE, RFC 9052, RFC 9053
- Suited for IoT, embedded — small use of memory
- Commercial quality
- Works with OpenSSL or Mbed TLS crypto libraries

COSE EC Encryption

- Switch to RFC 9053 ECDH encryption rather than HPKE
- Successful interop between t_cose and COSE Examples repository
- Workers: Hannes Tschofenig, Laurence Lundblade
- Hex of the COSE_Encrypt with ECDH—>

```
COSE_Encrypt:     184 bytes
    d8 60 84 43 a1 01 01 a1 05 50 2d be 1e d6 23 c8
    26 b5 c6 14 44 25 15 5a 96 b3 58 23 c8 9a e5 8e
    04 8e d7 73 be 9b 31 fe 23 6c 08 b2 0a 96 dc 61
    44 9e d0 0c 6a fb 7b d0 32 de c0 34 2e 42 4f 81
    83 44 a1 01 38 1c a2 20 a4 01 02 20 01 21 58 20
    ca 89 de 3c 97 7a 90 5e 4b 9e 32 17 98 78 a9 7b
    6f 86 40 d0 4f c9 db c1 eb 2e 18 62 dc a8 06 32
    22 58 20 1d de 39 99 22 47 0f ca 23 0a 55 27 b6
    8e 39 70 1c cb 60 90 12 3a d8 6c 9e 9b 5e ce 6d
    43 e8 ac 04 49 72 65 63 69 70 69 65 6e 74 58 18
    1d 0f 9c 82 81 b7 a0 8f 79 2b 5f 65 0b 5d 9c 1b
    6c c1 05 03 19 36 ee 13
```

Hackathon Progress



- COSE_Sign1 (single signer)

- COSE_Sign1 (single signer)
- COSE_Sign (multiple signers)
- COSE_Encrypt0 (one encryptor)
- COSE_Encrypt (multiple encryptors)
- COSE_Mac0 (single MAC)

Algorithms Progress Since 116