COSE

t_cose 2.0 project

IETF 116 Hackathon

https://github.com/laurencelundblade/t_cose

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

HPKE COSE draft-4

- Prototype implementation of draft-ietf-cose-hpke-04

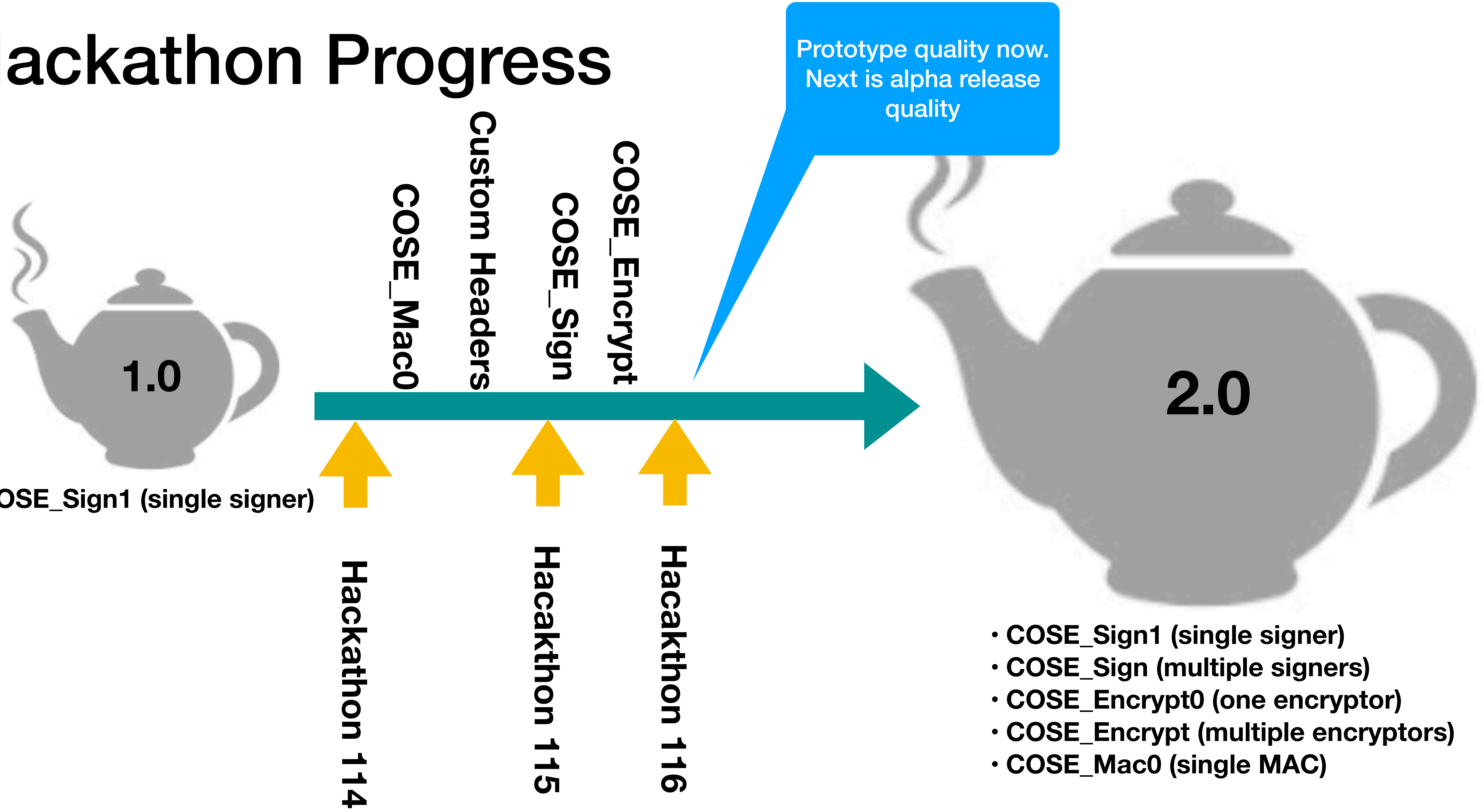
- Successful interop between t_cose in C and python implemenation by AJITOMI Daisuke

- Workers: Hannes Tschofenig (remote), AJITOMI Daisuke, Laurence Lundblade

- Hex dump of the COSE_Encrypt with HPKE—>

```
d8 60 84 43 a1 01 01 a1 05 50 68 45 27 37 f4 84
a1 ae d7 d4 c3 de cc 63 b1 74 58 23 88 56 81 c0
30 28 fc c8 e3 73 a0 1c 90 a1 b8 af 88 2a 51 11
43 0a 72 b7 d5 7c f0 c7 13 58 a4 1c 2a a0 70 81
83 43 a1 01 20 a2 23 84 10 01 01 58 41 04 d3 34
5a 18 7a 33 d4 b5 70 62 7c e3 97 cc 3e 8a 0d d4
26 f6 bb cb ba 41 99 01 61 4f 9c 0a d6 48 aa 18
1e 6f 33 76 ad 56 38 ee b2 aa 7c 83 34 6f b7 ca
25 38 b2 f8 7b 25 2b cd ea 26 71 88 d2 5c 04 55
66 69 78 65 64 5f 74 65 73 74 5f 6b 65 79 5f 70
32 35 36 72 31 58 20 a6 95 fc b3 79 26 4e 64 3c
fe 50 f6 7d 34 7c 5e 36 f7 c2 13 f1 6a 7c 76 f7
1d 01 bf a1 66 d1 c3
```

Hackathon Progress

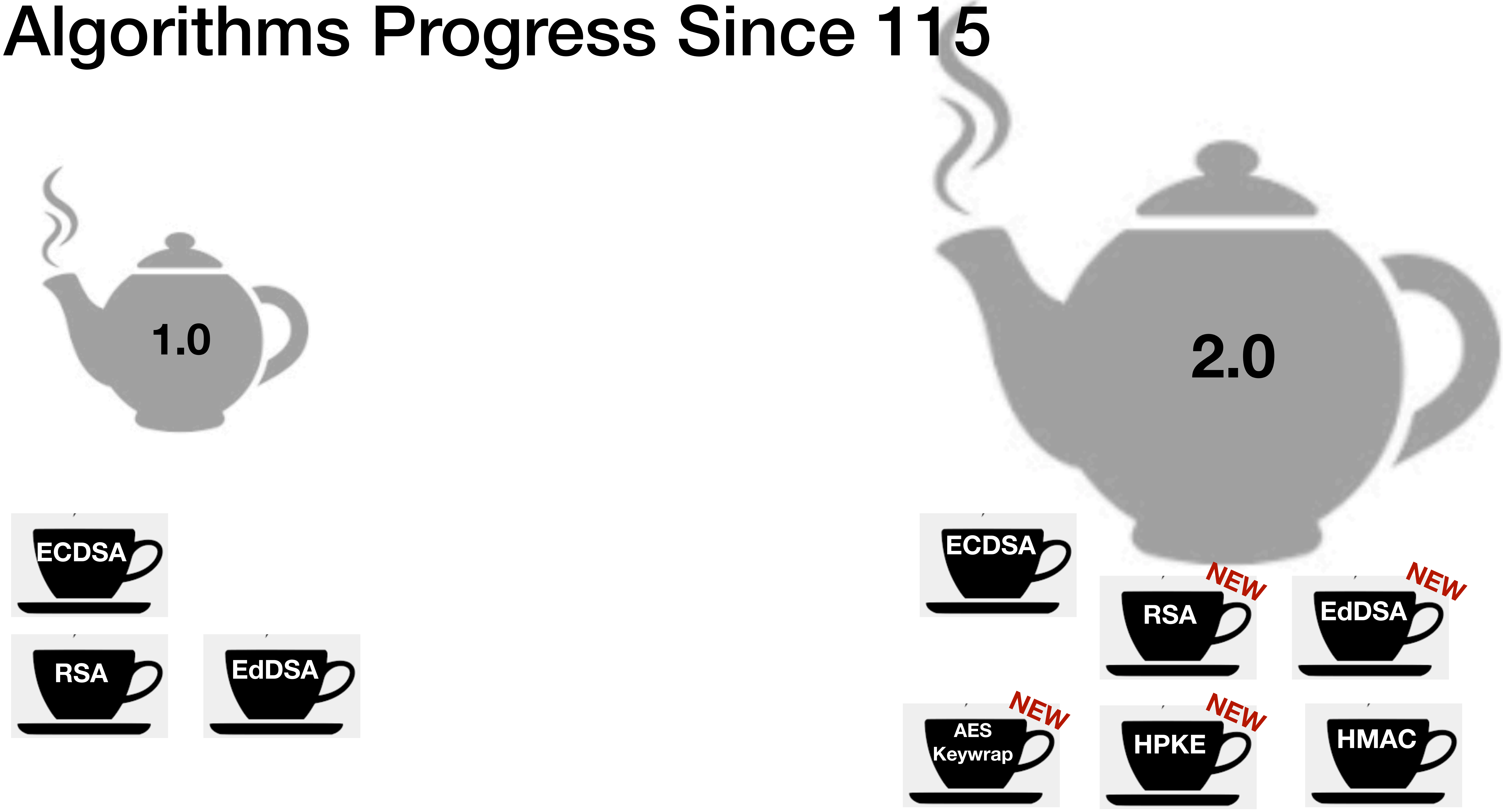


Prototype quality now. Next is alpha release quality

- 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 115



1.0

- ECDSA
- RSA
- EdDSA

2.0

- ECDSA
- RSA NEW
- EdDSA NEW
- AES Keywrap NEW
- HPKE NEW
- HMAC