EPHEMERAL DIFFIE-HELLMAN OVER COSE (EDHOC)

IETF99 ACE, JUL 17 2017

SELANDER, MATTSSON, PALOMBINI

DRAFT-SELANDER-ACE-COSE-ECDHE-07

SEVERAL REVIEWS

- Presented for CFRG at Eurocrypt by Jim Schaad

- Security reviews by Dan Harkins and Ilari Liusvaara
  - All comments taken into account in -07

”This is a very well-written draft and I am happy to see SIGMA being applied to every layer of the stack”.

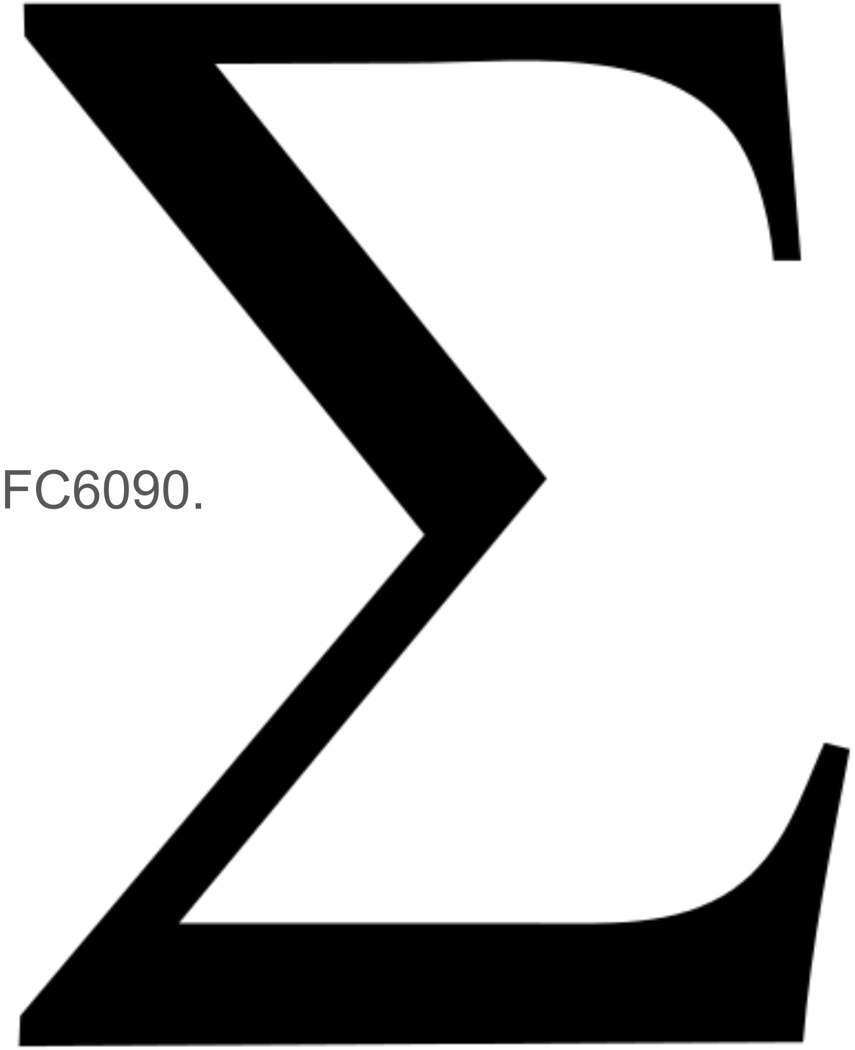
Dan Harkins

NEW IN VERSION -06

- Changes:
  - Error Message (MSG_TYPE = 0)
  - Verification of common preferred ECDH curve
  - Renamed **”extension”** → **“opaque application data”**
  - Removed encryption and integrity protection in message_1
  - Application unique strings now in field AlgorithmID.
  - Default CoAP Uri-Path: "/.well-known/edhoc”
  - PSK Chaining

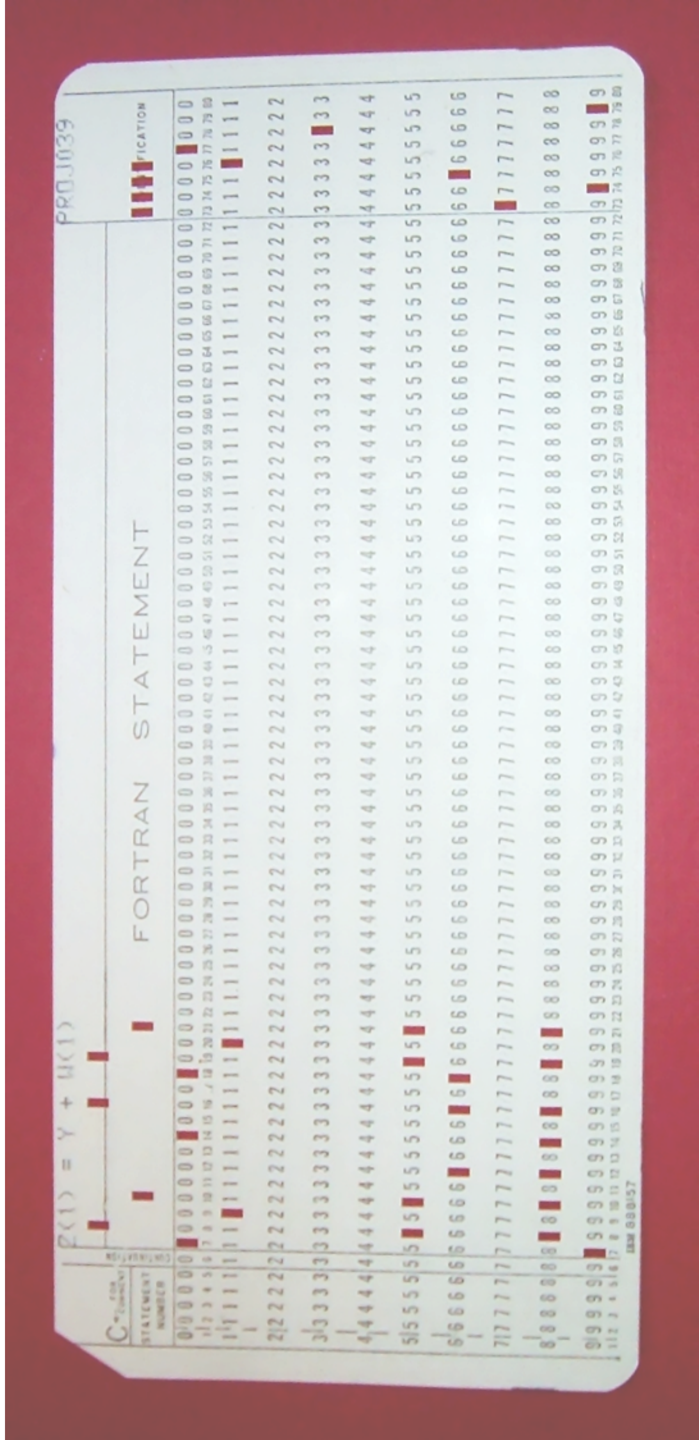
NEW IN VERSION -07

- Changes:
  - AlgorithmID is a tstr
  - Better explanation of session identifiers
  - Compact representation of EC2 points according to RFC6090.
  - ID_V, CERT_V replaced with ID_V, HINT_ID_V sent in the protected field of COSE_SIG_V.
  - Point validation of EC2 points



IMPLEMENTATIONS

- One implementation by Jim Schaad.
- A second implementation by SICS (work-in-progress).
- Test vectors to be added after interop testing.



ERICSSON