The Use of TESLA in SRTP

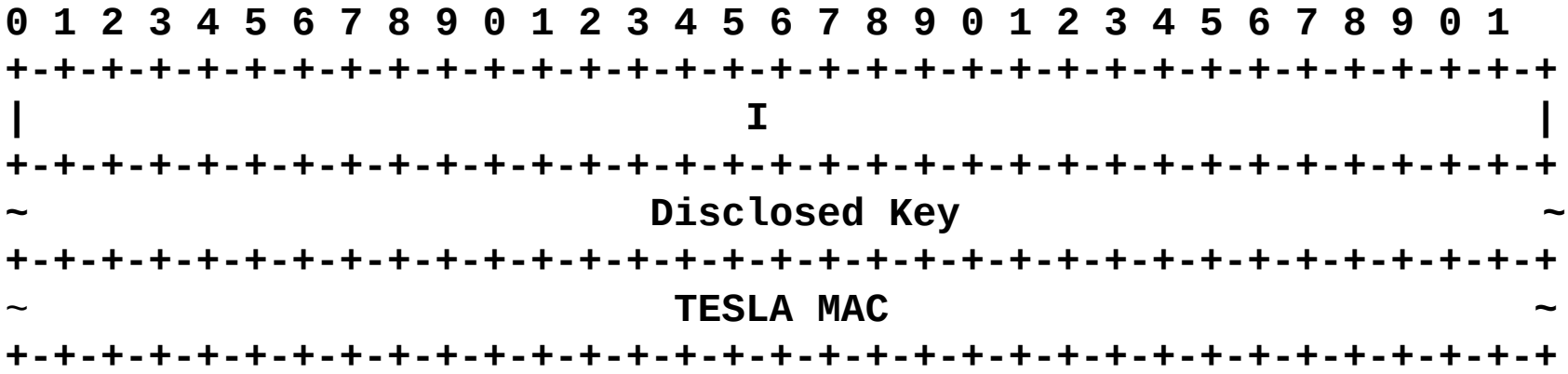
<draft-ietf-msec-srtp-tesla-01.txt>

Baugher, Carrara

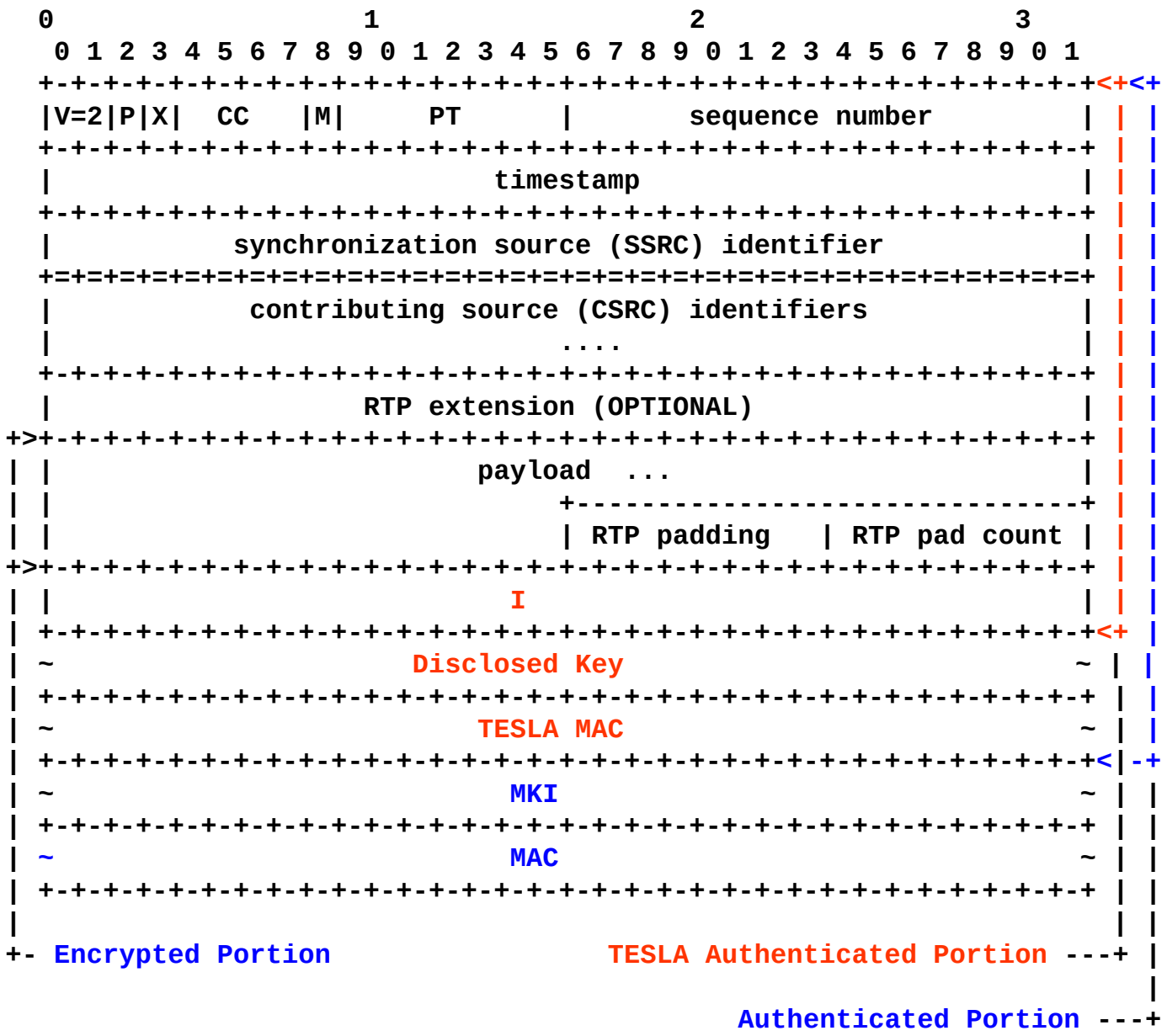
Components

- SRTP (RFC3711) for protection of RTP/RTCP traffic
  - Message integrity, anti-replay, confidentiality
  - Framework
  - Lack of Data Origin Authentication (DOA) for multicast and broadcast
- Timed Efficient Stream loss-tolerant Authentication (TESLA)
  - draft-ietf-msec-tesla-intro-02.txt
  - New option in SRTP

The TESLA extension

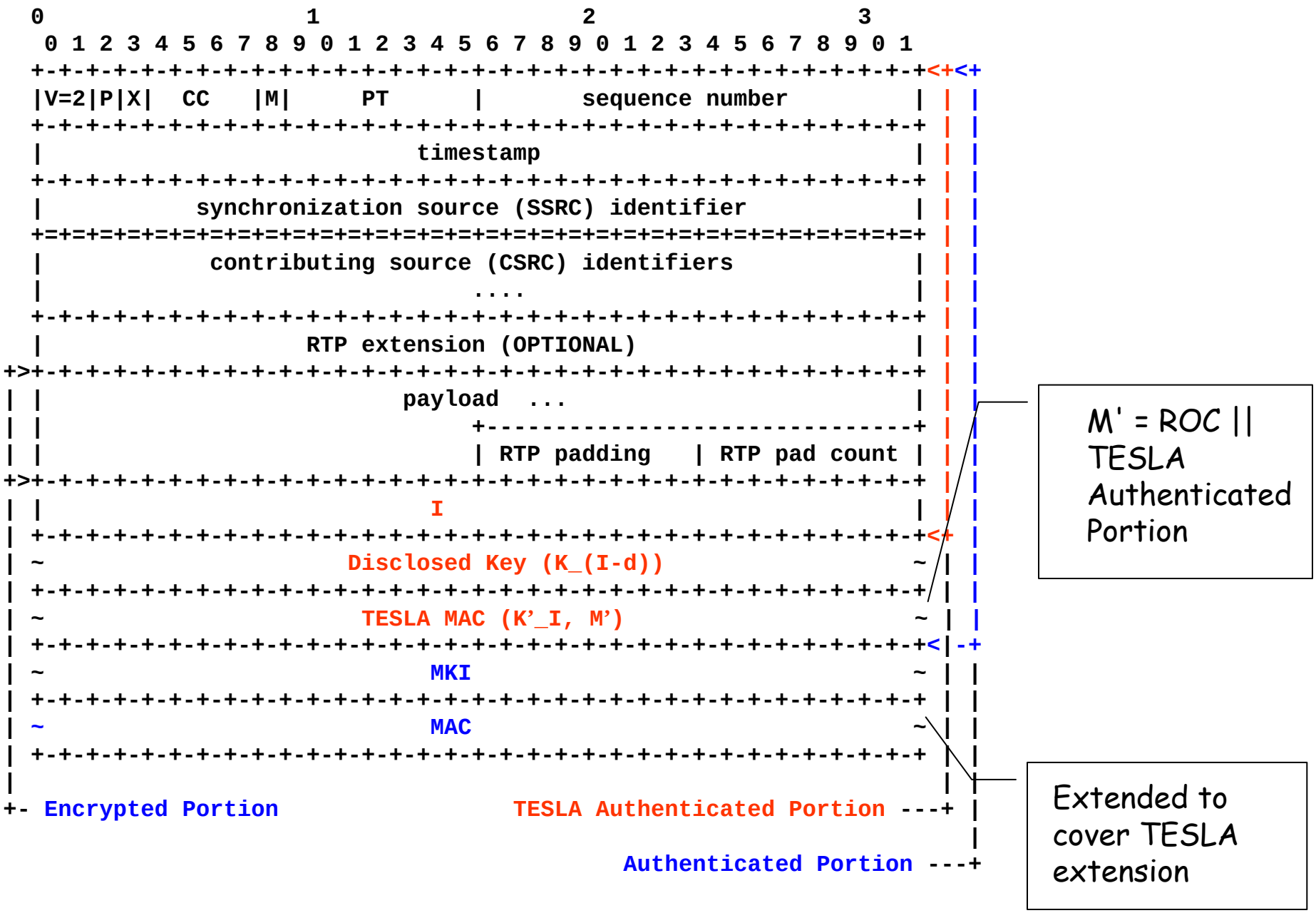


- *I*: id of the time interval i (corresponding to key K_i for the TESLA MAC in current packet) [32 bits].
- *Disclosed Key*: K_(i-d), to authenticate packets from earlier time intervals.
- *TESLA MAC*: using key K'_i (derived from K_i), then disclosed in a subsequent packet


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|V=2|P|X| CC |M| PT | sequence number
timestamp
synchronization source (SSRC) identifier
contributing source (CSRC) identifiers
....
RTP extension (OPTIONAL)
payload ...
RTP padding
RTP pad count
I
Disclosed Key
TESLA MAC
MKI
MAC
Encrypted Portion
TESLA Authenticated Portion
Authenticated Portion

Changes/additions to SRTP

- Some new parameters in the SRTP crypto context
- SRTP MAC is used against DoS from outsiders
- Sender and receiver processing includes TESLA verification
  1. Verify normal SRTP MAC (against external DoS)
  2. Buffer the packet
  3. TESLA-verify packet once the key is disclosed in later packet
  4. (Decrypt)
  5. Update Replay List
- SRTP MAC's coverage extended


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|V=2|P|X| CC |M| PT | sequence number |
timestamp
synchronization source (SSRC) identifier
contributing source (CSRC) identifiers
....
RTP extension (OPTIONAL)
payload ...
RTP padding | RTP pad count
I
Disclosed Key (K_(I-d))
TESLA MAC (K'_I, M')
MKI
MAC
Encrypted Portion
TESLA Authenticated Portion
Authenticated Portion
M' = ROC || TESLA Authenticated Portion
Extended to cover TESLA extension

Misc

- TESLA Bootstrapping
  - Out of scope
  - Key management
- PRFs for key derivation (keychain and MAC key)
  - HMAC/SHA1, 160-bit default
- SRTP MAC: 32 bits default
- TESLA MAC: 80 bits default
- Some overhead
  - 38 bytes added in default setting
  - Might be expensive for certain applications (e.g. 3GPP MBMS)