

Counter Mode and IPsec ESP

53rd IETF

David A. McGrew
Cisco Systems, Inc.

CM Status

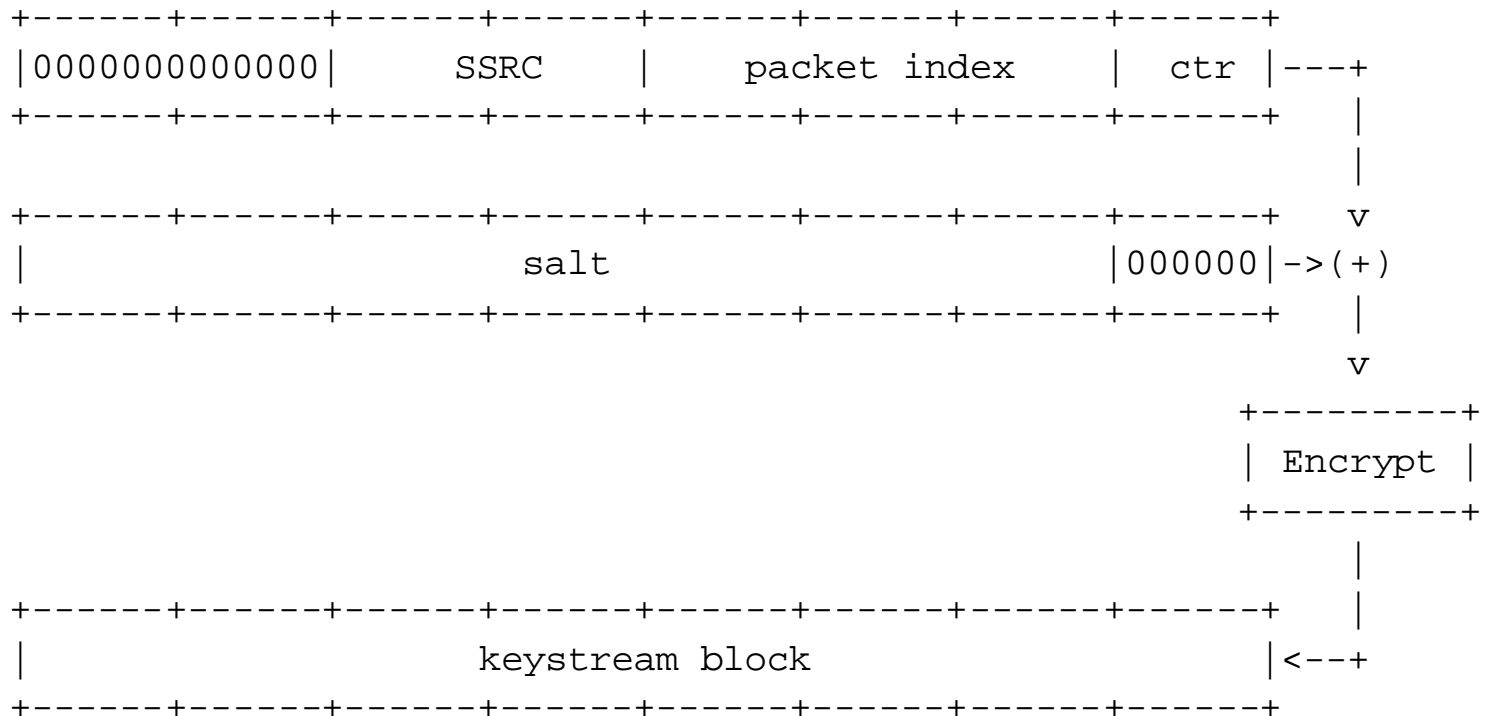
- Included in NIST Modes of Operation spec
SP 800-38A, Recommendation for Block Cipher
Modes of Operation
- NIST CM spec is inclusive
- Three application-specific CM specifications
 - Each segments keystream for packet encryption
- A unified CM is desirable to promote reusability
and extensibility
 - HW can use single core
 - SW can use single API

Application Specific CM Specs

- AES CTR and its use with IPsec
draft-moskowitz-aes128-ctr-00.txt, soon to be
draft-ietf-ipsec-aes128-ctr-00.txt
- Secure RTP (Section 4.1)
draft-ietf-avt-srtp-03.txt
- 802.11 CTR Mode

draft-mcgrew-saag-icm-00.txt NOT compatible

SRTP Counter Mode



IPsec ESP CTR Changes

- Block counter field width change to 16 bits (from 12 bits)
 - Implementor's feedback, spec alignment
- Add XOR with random salt
 - Adds security, spec alignment
- Add explicit counter option
 - Adds utility

Open Issues

- Width of Sequence Number and Block Counter fields
 - Maximum number of blocks (not packets) is 2^{64} (to ensure security)
 - Block limit can be enforced by field widths or by byte-count