ChaCha20 and Poly1305 Cipher Suites for TLS

Adam Langley
Wan-Teh Chang

Outline

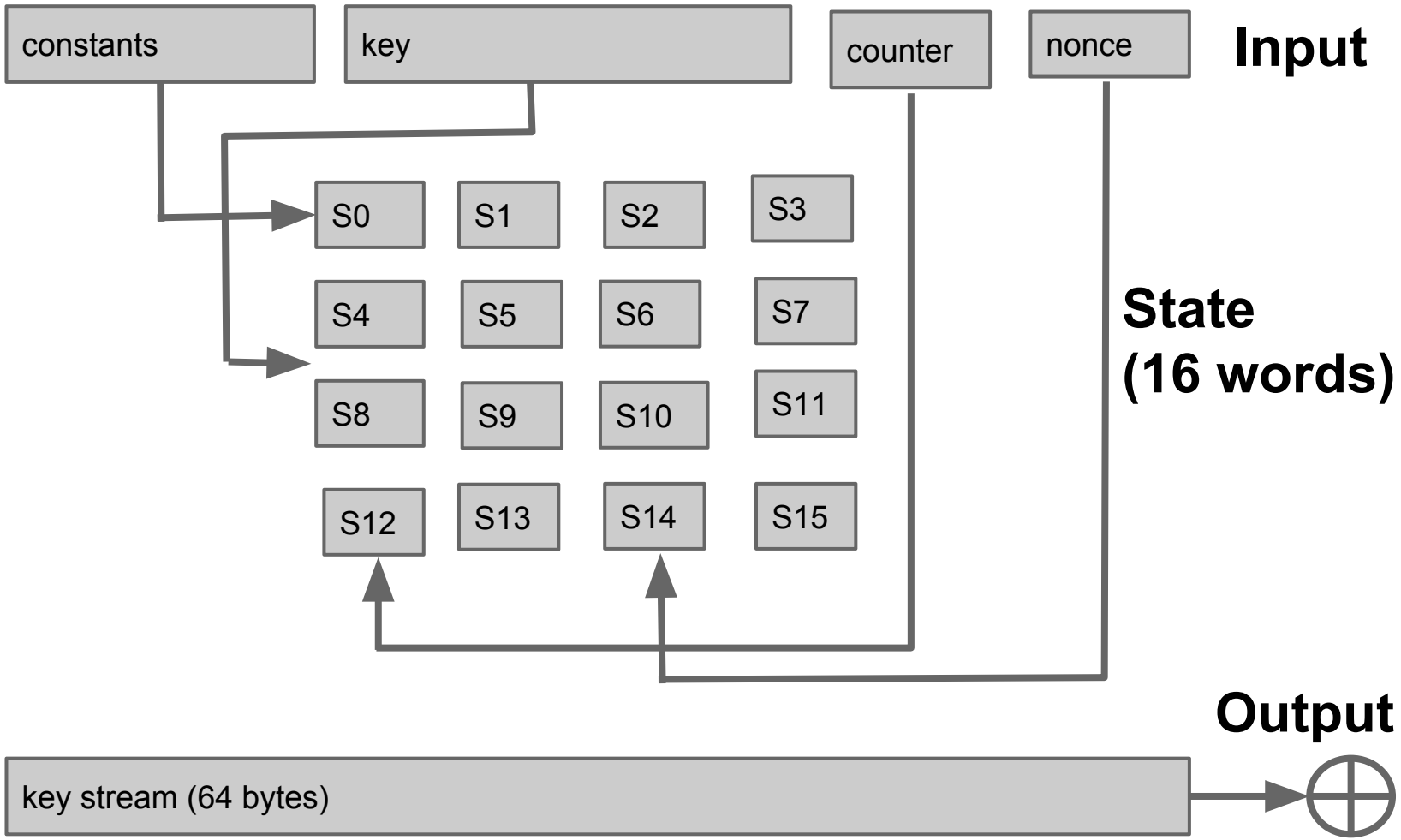
- ChaCha20 stream cipher
- Poly1305 authenticator
- ChaCha20+Poly1305 AEAD construction
- TLS cipher suites
- Performance

ChaCha20 stream cipher

- Designed by Dan J. Bernstein
- A variant of Salsa20 to improve diffusion
- Used in BLAKE, a SHA-3 finalist

- 256-bit key
- 64-bit nonce
- 64-bit block counter
- Outputs a 64-byte block of key stream and increments block counter in each invocation
- Plaintext is XOR'ed with the key stream

ChaCha20 function



Poly1305 authenticator

- A Wegman-Carter, one-time authenticator
- Designed by Dan J. Bernstein
- 256-bit key
- 128-bit output

Poly1305 calculation

Key (r, s): r => integer R, s => integer S

Input is divided into 16-byte chunks

C0 C1 C2 C3 C4 C5 . . . Cn-2 Cn-1

C0*R^n + C1*R^(n-1) + C2*R^(n-2) + … + Cn-2*R^2 + Cn-1*R mod (2^130-5)

Evaluate this polynomial with Horner's Rule

+ S mod 2^128

AEAD construction

- The AEAD key is a ChaCha20 key
- For each nonce, derive:

Poly1305 key = ChaCha20(000...0, counter=0)

Discard the last 32 bytes of output

- A = additional data
- S = ChaCha20(plaintext, counter=1)
- T = Poly1305(A || len(A) || S || len(S))
- Ciphertext = S || T

TLS cipher suites

- Three forward secret, AEAD ciphers:
  - **TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256**
  - **TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256**
  - **TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256**
- No implicit nonce: fixed_iv_length = 0
- No explicit nonce: record_iv_length = 0
  - 8-byte ChaCha20 nonce is the TLS sequence number

Performance

Intel Xeon E5-2690@2.9GHz with Hyper-Threading and Turbo Boost disabled

AES-128-GCM, AES-NI disabled	131 MB/s
AES-128-GCM, AES-NI enabled	892 MB/s
ChaCha20+Poly1305	427 MB/s
ChaCha20+Poly1305, -march=native	560 MB/s

Performance

ARM Cortex-A9@1.2GHz

AES-128-GCM	25 MB/s
ChaCha20+Poly1305	92 MB/s

MAC performance

Intel Xeon E5-2690@2.90GHz with Hyper-Threading and Turbo Boost disabled

- To authenticate 1KB of data

VMAC (128-bit, with AES calls removed)	270 ns with 248 bytes of memory
Poly1305	561 ns

MAC performance

ARM Cortex-A8@1.2GHz, with NEON enabled

- To authenticate 1KB of data

VMAC (128-bit, with AES calls removed)	5015.1 ns with 248 bytes of memory
Poly1305 (code from SUPERCOP)	3567 ns