How fast can a 256-bit secure MAC be?

Tung Chou

Technische Universiteit Eindhoven, The Netherlands

March 4, 2014

Joint work with Daniel J. Bernstein

How fast can a 256-bit secure MAC be?

Textbook GHASH implementation: $\approx 128 \times 128$ ANDs, $\approx 128 \times 128$ XORs per 128 bits. Total: ≈ 256 ops per bit for $\approx 2^{128}$ (???) security.

How fast can a 256-bit secure MAC be?

Textbook GHASH implementation: $\approx 128 \times 128$ ANDs, $\approx 128 \times 128$ XORs per 128 bits. Total: ≈ 256 ops per bit for $\approx 2^{128}$ (???) security.

Scale up: ≈ 512 ops per bit for $\approx 2^{256}$ security.

How fast can a 256-bit secure MAC be?

Textbook GHASH implementation: $\approx 128 \times 128$ ANDs, $\approx 128 \times 128$ XORs per 128 bits. Total: ≈ 256 ops per bit for $\approx 2^{128}$ (???) security.

Scale up: ≈ 512 ops per bit for $\approx 2^{256}$ security.

New Auth256 MAC: 34 ops per bit for 2^{256} security.

- Software implementation: 1.59 Sandy Bridge cycles/byte.

How fast can a 256-bit secure MAC be?

Textbook GHASH implementation: $\approx 128 \times 128$ ANDs, $\approx 128 \times 128$ XORs per 128 bits. Total: ≈ 256 ops per bit for $\approx 2^{128}$ (???) security.

Scale up: ≈ 512 ops per bit for $\approx 2^{256}$ security.

New Auth256 MAC: 34 ops per bit for 2^{256} security.

- Software implementation: 1.59 Sandy Bridge cycles/byte.

4-round AES MAC: ≈ 76 ops per bit for 2^{114} security.

FFT for polynomial multiplication in binary field

FFT for polynomial multiplication in binary field

What is the smallest n where FFT starts to beat Karatsuba+Toom for n-byte binary-field multiplication?

FFT for polynomial multiplication in binary field

What is the smallest n where FFT starts to beat Karatsuba+Toom for n-byte binary-field multiplication?

Answer: $n = 8$.