McMambo V1: A new kind of Latin Dance

Watson Ladd

University of California, Berkeley

August 12, 2013

Outline

1 Motivation

2 Mambo

From Tweakable Cipher to Authenticated Encryption

- OCB3 can be seen as taking a tweakable cipher to an AEAD scheme
- McOE: avoids problems of counter reuse
- We have tweakable ciphers: Threefish, standard constructions
- So done?

Size Matters

- McOE requires a tweak the size of a block
- Can use AES-128 plus standard construction
- Inherits problems of AES plus key agility issues
- Threefish doesn't have a big enough tweak

Mambo

- Tweakable Block cipher: 512 bit block and tweak, 256 bit key
- State organized as 4x4 array of 32-bit words
- Key is 8 32-bit words
- Tweak is 16 32-bit words

Mambo Structure

- Similar to Salsa
- Reversable transformation of four words
- Repeated on rows and columns
- Alternates with xoring in key and round counter
- Key in checkerboard, round counter down diagonal
- Tweak is xored into entire state midway through encryption

The Quarterround Transformation

- $y_1 = x_1 \oplus R(x_0 \wedge x_2, 7)$
- $y_2 = x_2 \oplus R(x_0 \vee x_3, 9)$
- $y_3 = x_3 \oplus R(y_1 \uparrow x_0, 13)$
- $y_0 = x_0 \oplus R(y_1 \downarrow y_2, 18)$

From Transformation to Mode

- $C_i = E(P_i, N_i)$
- $N_{i+1} = C_i \oplus P_i$
- Initialize with message number
- Add in tag as encryption of message number
- 512 bit nonce and tag

Cryptographic properties

- Given ideal tweakable cipher McOE has nice properties
- Leaks only common prefixes if message number fixed
- Online computation
- State size one block
- Tag ridiculously big: truncation possible but uninvestigated

Performance

- 12 cycles per byte on modern Intel hardware
- 25 for AES (From recent OpenSSL)
- Complete implementation 20 kilobytes executable
- Note: aggressively optimizing compiler only trick used

Where to focus

- McOE paper: If tweaked cipher is secure, so is the mode
- Impact of truncation of tag
- Security means commonality of prefix revealed: implications
- Attacks on Mambo
- Faster, smaller, better software
- Hardware size and implementations: what choices exist