LEVERAGING TECHNOLOGY - THE JOINT IMPERATIVE

MILCOM 2015

Customizable Sponge-Based Authenticated Encryption Using 16-bit S-boxes

Matthew Kelly[1], Alan Kaminsky[1], Michael Kurdziel[2], Marcin Łukowiak[1], Stanisław Radziszowski[1]

[1]Rochester Institute of Technology, [2]Harris Corporation

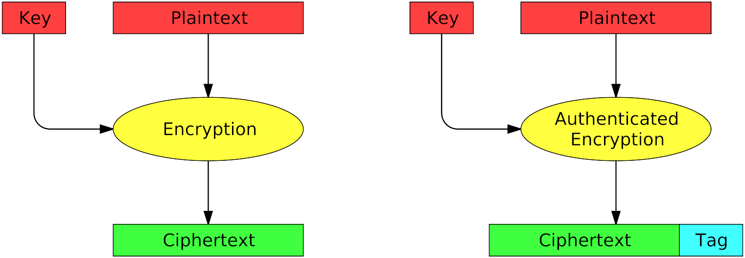
October 26, 2015

Agenda

1. Motivation
   - Shortcomings of Block Ciphers
   - Shortcomings of AES
2. Prior Work
   - Duplex Sponge Construction
3. The MK3 Cipher
   - Design
   - Security Analysis
4. Conclusion

Motivation—Shortcomings of Block Ciphers

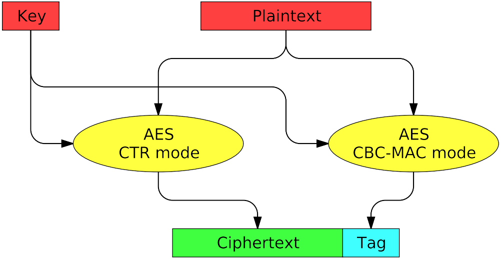
Secure communication requires *both* encryption *and* authentication
But a block cipher only does encryption



Motivation—Shortcomings of Block Ciphers

Block cipher authenticated encryption modes do exist
But they typically require two passes over the plaintext
A faster, single-pass algorithm would be preferable

CCM mode

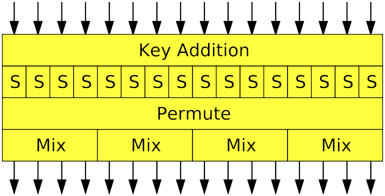


Motivation—Shortcomings of AES

AES is not customizable

- Fixed S-box, permutation, and mixing operations
- Fixed key sizes (128, 192, 256 bits)
- Fixed number of rounds (10, 12, 14 rounds)

One AES round



Motivation—Shortcomings of AES

AES is not customizable, therefore . . .

AES cannot adapt to new attacks

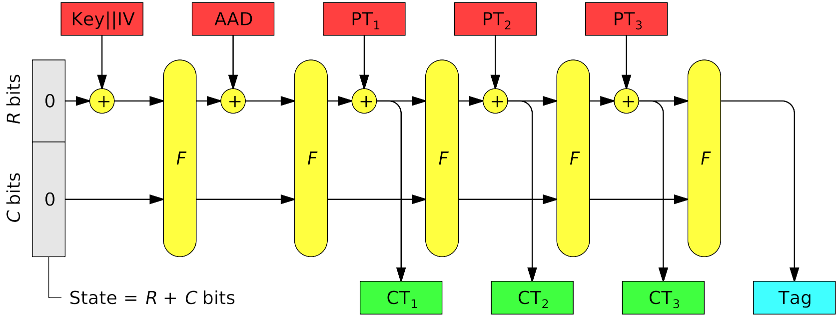
- AES was theoretically broken in 2011 [1]
- The attack breaks AES-128 with $2^{126.1}$ work
- The attack breaks AES-192 with $2^{189.7}$ work
- The attack breaks AES-256 with $2^{254.4}$ work
- If we could do more rounds, we could nullify the attack

AES is less attractive to non-U.S.-government customers

- Each prefers its own customized, yet secure, algorithm

Prior Work—Duplex Sponge Construction

Invented by Bertoni *et al.* in 2011 [2]
Based on the earlier sponge construction [3]
Supports authenticated encryption and other operations



Prior Work—Duplex Sponge Construction

Sponge construction generic security

- If the bijective function F is indistinguishable from a random bijection, then the whole sponge construction is indistinguishable from a random bijection [3]
- We only need to analyze the security of F

Duplex sponge construction generic security

- Security level $=$ min $(2^{(R+C)/2}, 2^C, 2^K)$, where $K =$ key size [4]
- We need to have $(R+C)/2 \geq K$ and $C \geq K$ to get a security level of 2^K

The MK3 Cipher—Design

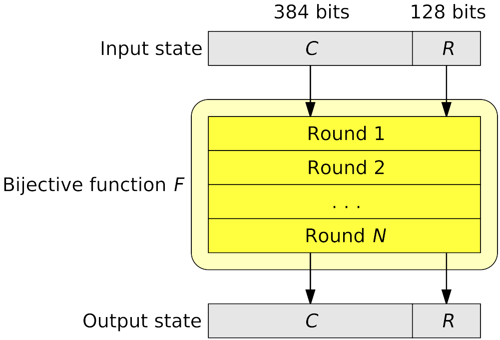
Goals

- Support authenticated encryption as well as encryption-only
- Support 128-bit and 256-bit key sizes
- Utilize state-of-the-art cryptographic design
- One pass over the plaintext
- Customizable
- Security analysis applicable to all customized versions
- FPGA implementation

The MK3 Cipher—Design

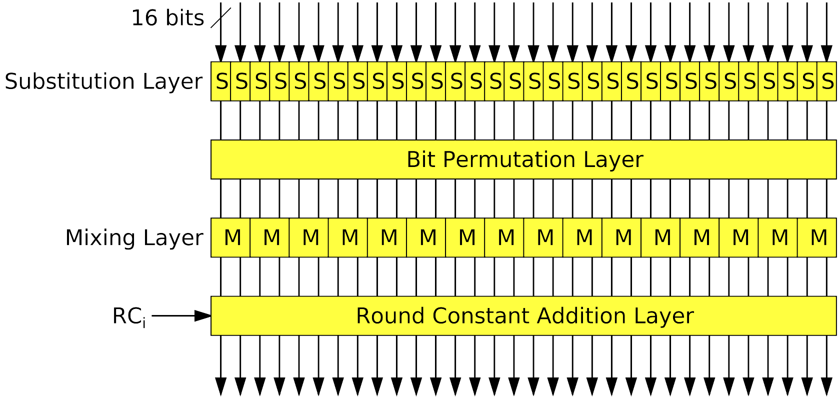
Overall design

- Uses the duplex sponge construction
- State = 512 bits; $R = 128$, $C = 384$
- Bijective function F consists of N iterated rounds



The MK3 Cipher—Design

Bijective function round design



The MK3 Cipher—Design

Substitution Layer design

- Purpose: Nonlinear confusion
- Thirty-two 16×16-bit S-boxes, developed by Wood [5]
- Uses GF(2^{16}) inversion plus an affine transformation
- $S(x) = A\,x^{-1} + b$
- Efficient in hardware; 1,238 XOR gates, 144 AND gates per S-box

Substitution Layer customization requirements

- S-box maximum differential probability $\leq 2^{-14}$
- S-box maximum linear bias $\leq 2^{-8}$

The MK3 Cipher—Design

Bit Permutation Layer design

- Purpose: Linear diffusion
- Permutes the order of the 512 bits in the state
- Input bit position x moves to output bit position $31x + 15 \pmod{512}$
- Efficient in hardware; just wires

Bit Permutation Layer customization requirements

- For each S-box, each output bit goes to a different mixer
- No fixed points in the permutation
- No short cycles in the permutation

The MK3 Cipher—Design

Mixing Layer design

- Purpose: Increase branch number, leading to fewer rounds
- Each of sixteen mixers combines two 16-bit inputs A and B, yielding two 16-bit outputs C and D
- Uses matrix multiplication in GF(2^{16}); $\begin{bmatrix} C \\ D \end{bmatrix} = \begin{bmatrix} 1 & x \\ x & x+1 \end{bmatrix} \times \begin{bmatrix} A \\ B \end{bmatrix}$
- Efficient in hardware; 54 XOR gates per mixer

Mixing Layer customization requirements

- Matrix must be maximum distance separable and invertible
- Consequently, at least three S-boxes will be active in any two consecutive rounds (branch number = 3)

The MK3 Cipher—Design

Round Constant Addition Layer design

- Purpose: Inject asymmetry; prevent slide attacks
- Add a 512-bit round constant to the state
- Different round constant in each round
- Efficient in hardware; 512 XOR gates

Round Constant Addition Layer customization requirements

- Each round constant should be a different randomly-chosen number

The MK3 Cipher—Security Analysis

Number of rounds N needed in the bijective function F [6]

Key size	Minimum rounds	Recommended rounds
128	6	10
256	12	16

Minimum rounds = Needed for differential and linear cryptanalysis to require more work than exhaustive key search

Recommended rounds = Minimum + 4 rounds security margin

Conclusion

MK3: Best-practices cryptographic design

- Duplex sponge construction for authenticated encryption
- AES-like bijective function

MK3: Novel contributions

- 16×16-bit S-boxes
- Customizable round function
- Security analysis applicable to all customized versions

Ongoing work

- Further cryptanalysis
- Statistical analysis
- FPGA hardware implementation

References

1. A. Bogdanov, D. Khovratovich, and C. Rechberger. Biclique cryptanalysis of the full AES. Cryptology ePrint Archive, Report 2011/449, 2011.
2. G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. Duplexing the sponge: single-pass authenticated encryption and other applications. *18th International Workshop on Selected Areas in Cryptography*, 2011.
3. G. Bertoni, J. Daemen, M. Peeters and G. Van Assche. On the indifferentiability of the sponge construction. *EUROCRYPT*, 2008.
4. P. Jovanovic, A. Luykx, and B. Mennink. Beyond $2^{c/2}$ security in sponge-based authenticated encryption modes. Cryptology ePrint Archive, Report 2014/373, 2014.
5. C. Wood. Large substitution boxes with efficient combinational implementations. Rochester Institute of Technology Computer Science M.S. thesis, 2013.
6. M. Kelly. Design and cryptanalysis of a customizable authenticated encryption algorithm. Rochester Institute of Technology Computer Engineering M.S. thesis, 2014.