Symmetric Key Cryptography

PQCRYPTO Summer School on Post-Quantum Cryptography 2017

Stefan Kölbl

June 20th, 2017

DTU Compute, Technical University of Denmark

Introduction to Symmetric Key Cryptography

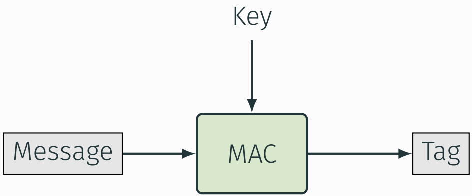
What can we do?

- Encryption
- Authentication (MAC)
- Hashing
- Random Number Generation
- Digital Signature Schemes
- Key Exchange

Authentication

Authentication

Message Authentication Code (MAC)



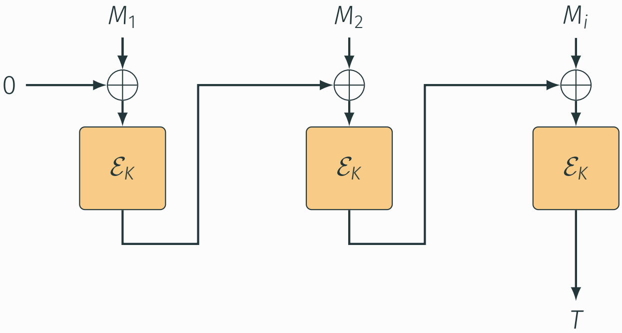
- Produces a tag
- Provide both *authenticity* and *integrity*
- It should be *hard* to forge a valid tag.
- Similar to hash but has a key
- Similar to digital signature but same key

Authentication

MAC Algorithm

- Block Cipher Based (CBC-MAC)
- Hash-based (HMAC, Sponge)
- Universal Hashing (UMAC, Poly1305)

CBC-MAC



Authentication

Hash-based:

- $H(k \mid\mid m)$
  - Okay with Sponge, fails with MD construction.
- $H(m \mid\mid k)$
  - Collision on H allows to construct Tag collision.
- HMAC: $H(k \oplus c_1 \mid\mid H(k \oplus c_2 \mid\mid m))$

Authentication

Universal Hashing (UMAC, Poly1305, ...)

- We need a universal hash function family $\mathcal{H}$.
- Parties share a secret member of $\mathcal{H}$ and key k.
- Attacker does not know which one was chosen.

Definition

A set $\mathcal{H}$ of hash functions $h : U \to N$ is universal iff $\forall x, y \in U$:

$$\Pr_{h \in H}(h(x) = h(y)) \leq \frac{1}{|N|}$$

when h is chosen uniformly at random.

Authenticated Encryption

In practice we **always** want Authenticated Encryption

- Encryption **does not** protect against malicious alterations.
- WEP [TWP07]
- Plaintext recovery OpenSSH [APW09]
- Recover TLS cookies [DR11]

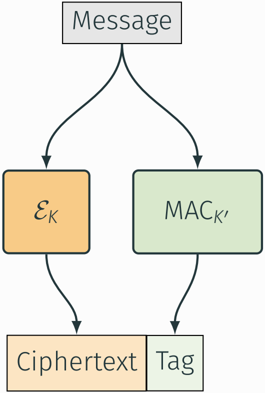
Problem

Lot of things can go wrong when combining encryption and authentication.

Note: This can allow to recover plaintext, forge messages…

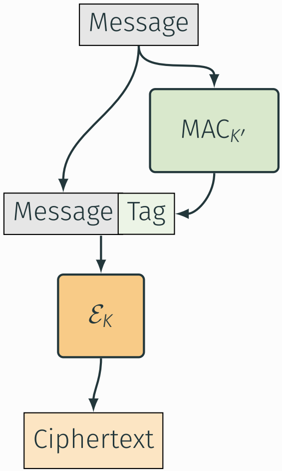
Authenticated Encryption [BN00]

Encrypt-and-MAC



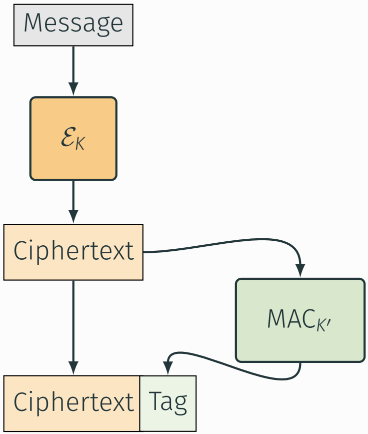
Authenticated Encryption [BN00]

MAC-then-Encrypt



Authenticated Encryption [BN00]

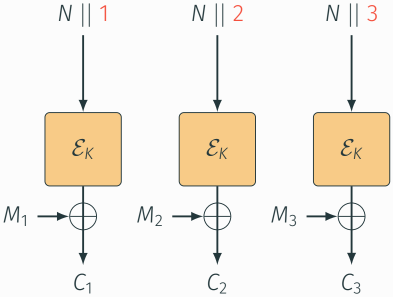
Encrypt-then-MAC



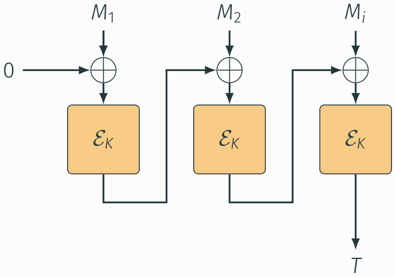
Authenticated Encryption

You have to be careful!

CTR-Mode



CBC-MAC

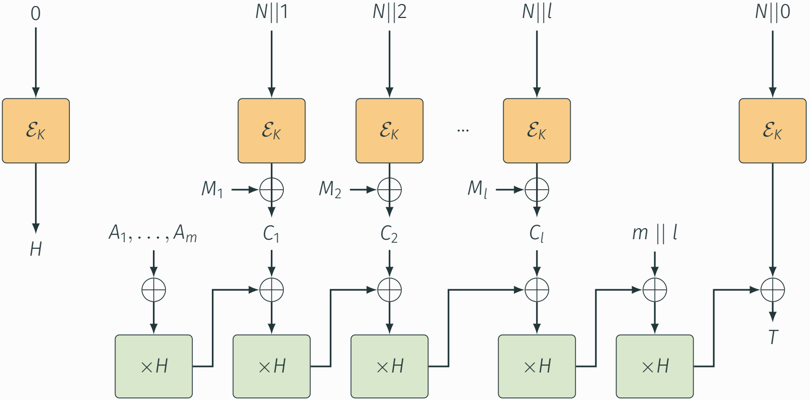


Authenticated Encryption

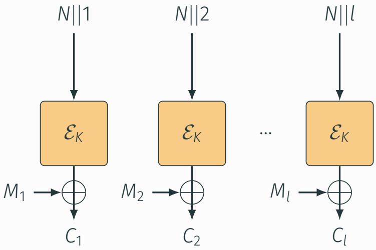
Authenticated Encryption with Associated Data (AEAD)

- Associcated Data A (e.g. packet header)
- Nonce N (unique number)

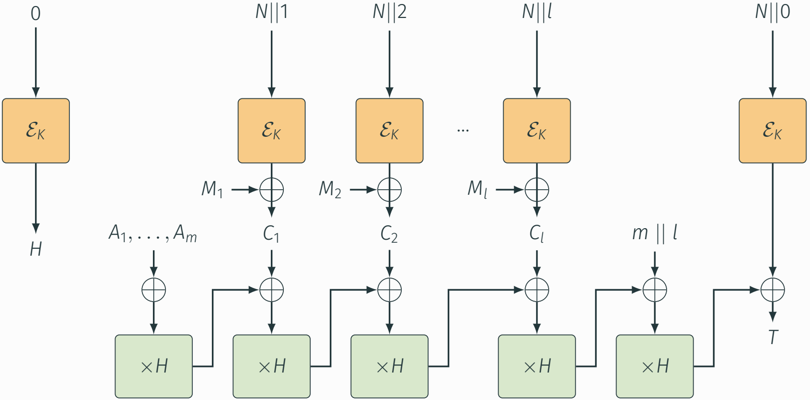
Galois/Counter Mode (GCM)



Galois/Counter Mode (GCM)



Galois/Counter Mode (GCM)



Authenticated Encryption

AES-GCM

- Widely used (TLS)
- Reusing nonce compromises security
- Weak keys for $\times H$
- Hardware support for AES + `PCLMULQDQ`
- AES-GCM-SIV?

Authenticated Encryption

CAESAR[1]: Competition for Authenticated Encryption: Security, Applicability, and Robustness

- Initially 57 submissions.
- Third round: 15 Submissions left
- Goal is to have a portfolio of AE schemes

Summary

Most applications need Authenticated Encryption!

[1] https://competitions.cr.yp.to/caesar.html

Quantum Attacks

Quantum Attacks

Attack Model

- Attacker listens to communication over classical channel.
- Can query a classic blackbox with the secret key.
- Attacker has large quantum computer.
- Only limited set of quantum algorithms available.

Quantum Attacks

Encryption / MACs

- Recover Key in $O(2^{k/2})$ with Grover's.

Hash Function

- Find Preimage in $O(2^{n/2})$ with Grover's.
- Find Collisions in $O(2^{n/3})$ [BHT97] ... but needs $O(2^{n/3})$ hardware.

Quantum Attacks

The costs are not so simple

- Costs of quantum operation vs. classic operations
- Collision finding not really faster [Ber09].

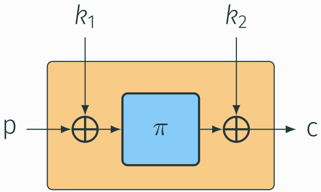
There is some work on better understanding this:

- Preimage SHA-256: 2^{166} *logical-qubit-cycles* [Amy+16].
- Preimage SHA3-256: 2^{166} *logical-qubit-cycles* [Amy+16].

Quantum Attacks

Even-Mansour

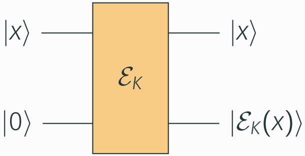
- Two keys k_1, k_2.
- Uses public permutation π.



Classic Security

- D queries to $\mathcal{E}$
- T queries to π
- *Proof* for upper bound on attack success $O(DT/2^n)$

Quantum Oracle Access to encryption algorithm



- Very strong model for adversary.

Simon's Algorithm

Given

$$f : \{0,1\}^n \to \{0,1\}^n$$

with promise that there exists

$$s \in \{0,1\}^n$$

such that

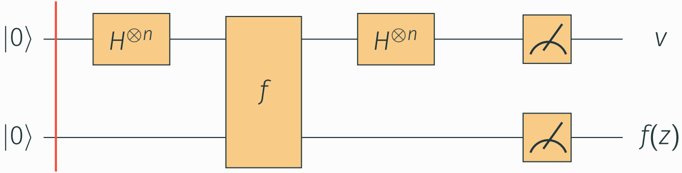
$$\forall (x,y) \in \{0,1\}^n : f(x) = f(y) \iff x \oplus y \in \{0^n, s\}$$

Output: s

Only needs $O(n)$ quantum queries.

Simon's Algorithm

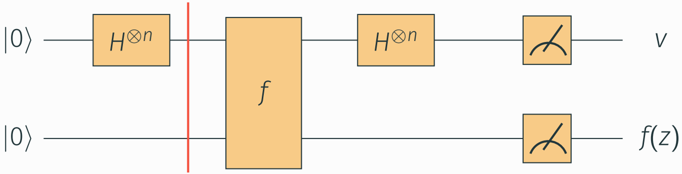
Circuit



$$|0^n\rangle|0^n\rangle$$

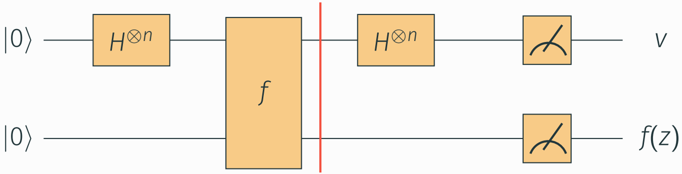
Simon's Algorithm

Circuit



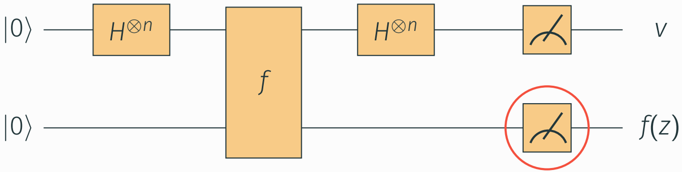
$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle|0^n\rangle$$

Circuit



$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$$

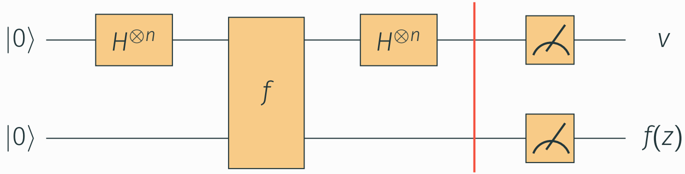
Circuit



$$\frac{1}{\sqrt{2}}|z\rangle + \frac{1}{\sqrt{2}}|z \oplus s\rangle$$

Simon's Algorithm

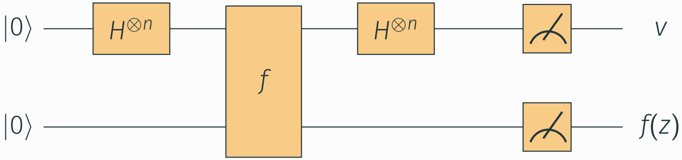
Circuit



$$\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\sum_y(-1)^{y\cdot z}(1+(-1)^{y\cdot s})|y\rangle$$

Simon's Algorithm

Circuit



$$\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\sum_y (-1)^{y\cdot z}(1+(-1)^{y\cdot s})|y\rangle$$

Result

One steps finds a vector such that $y \cdot s = 0$.

Breaking Even-Mansour [KM12]

$$\mathcal{E}_{k_1,k_2}(x) = \pi(x \oplus k_1) \oplus k_2$$

Construct:

$$\begin{aligned} f : \{0,1\}^n &\to \{0,1\}^n \\ x &\to \mathcal{E}_{k_1,k_2}(x) \oplus \pi(x) = \pi(x \oplus k_1) \oplus k_2 \oplus \pi(x) \end{aligned}$$

This function fulfills Simon's promise:

$$\begin{aligned} f(x) &= \pi(x \oplus k_1) \oplus k_2 \oplus \pi(x) \\ f(x \oplus k_1) &= \pi(x \oplus k_1 \oplus k_1) \oplus k_2 \oplus \pi(x \oplus k_1) \end{aligned}$$

Quantum

Breaking Even-Mansour [KM12]

$$\mathcal{E}_{k_1,k_2}(x) = \pi(x \oplus k_1) \oplus k_2$$

Construct:

$$\begin{aligned} f : \{0,1\}^n &\to \{0,1\}^n \\ x &\to \mathcal{E}_{k_1,k_2}(x) \oplus \pi(x) = \pi(x \oplus k_1) \oplus k_2 \oplus \pi(x) \end{aligned}$$

This function fulfills Simon's promise:

$$\begin{aligned} f(x) &= \pi(x \oplus k_1) \oplus k_2 \oplus \pi(x) \\ f(x \oplus k_1) &= \pi(x) \oplus k_2 \oplus \pi(x \oplus k_1) \end{aligned}$$

Quantum

Breaking Even-Mansour [KM12]

$$\mathcal{E}_{k_1,k_2}(x) = \pi(x \oplus k_1) \oplus k_2$$

Construct:

$$\begin{aligned} f : \{0,1\}^n &\to \{0,1\}^n \\ x &\to \mathcal{E}_{k_1,k_2}(x) \oplus \pi(x) = \pi(x \oplus k_1) \oplus k_2 \oplus \pi(x) \end{aligned}$$

This function fulfills Simon's promise:

$$\begin{aligned} f(x) &= \pi(x \oplus k_1) \oplus k_2 \oplus \pi(x) \\ f(x \oplus k_1) &= \pi(x \oplus k_1) \oplus k_2 \oplus \pi(x) \end{aligned}$$

Recover k_1 with $O(n)$ quantum queries.

Quantum Attacks

Similar attacks [Kap+16] apply to

- Block Cipher Modes
- MACs
- Authenticated Encryption
- Improving Slide Attacks

Quantum Attacks

Similar attacks [Kap+16] apply to

- Block Cipher Modes
- MACs
- Authenticated Encryption
- Improving Slide Attacks

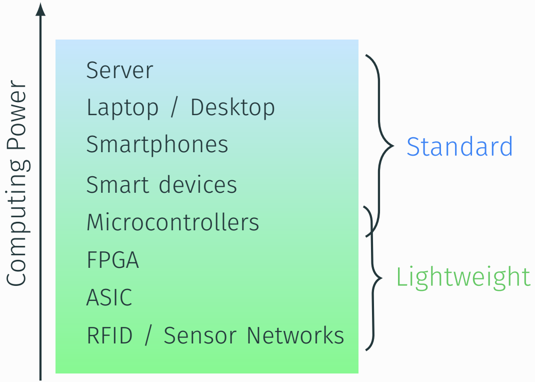
Goal

Construct f such that $f(x) = f(x \oplus s)$ for some secret s.

Current Directions in Symmetric Key Cryptography

Lightweight Cryptography

- Resource constraint
  - Chip area
  - Memory
  - Computing Power
  - Power/Energy
- NIST Project[5]
- Many designs exists



[1] https://beta.csrc.nist.gov/projects/lightweight-cryptography

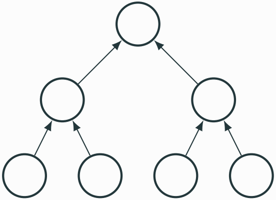
Symmetric Key Cryptography

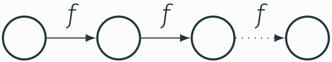
Hash-based Signatures:

- Many calls to a hash function...
- ...but only very short inputs.
- No collision resistance required

Current Designs:

- Often slow on short inputs.
- Too conservative for this restricted setting?
- Designs: ChaCha in SPHINCS, Haraka [Köl+]





Symmetric Key Cryptography

Multiparty Computation, Zero Knowledge, Fully Homomorphic Encryption

- Multiplications in primitives very costly for these applications.
- Signature size directly relates to number of ANDs (for ZK).

Symmetric Key Primitives which:

- Minimize number of ANDs
- Minimize circuit depth
- Examples: LowMC [Alb+15], MiMC [Alb+16], Kreyvium [Can+16], Flip [Méa+16]

Conclusion

Symmetric Key Cryptography

- Encryption: AES-CTR
- Hash: SHA-2, SHA-3
- Authenticated Encryption: AES-GCM, ChaCha20-Poly1305, CAESAR

Quantum Attacks

- Mostly fine with double the parameter sizes.
- Improve cryptanalytic attacks with quantum algorithms.

[1] Thanks to `https://www.iacr.org/authors/tikz/` for some of the figures.

Questions?

References i

Martin R. Albrecht, Kenneth G. Paterson, and Gaven J. Watson. “Plaintext Recovery Attacks against SSH”. In: *30th IEEE Symposium on Security and Privacy (S&P 2009)*. 2009, pp. 16–26.

Martin R. Albrecht et al. “Ciphers for MPC and FHE”. In: *Advances in Cryptology - EUROCRYPT 2015*. 2015, pp. 430–454.

Martin R. Albrecht et al. “MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity”. In: *Advances in Cryptology - ASIACRYPT 2016*. 2016, pp. 191–219.

Matthew Amy et al. *Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3*. Cryptology ePrint Archive, Report 2016/992. `http://eprint.iacr.org/2016/992`. 2016.

Gilles Brassard, Peter Høyer, and Alain Tapp. “Quantum cryptanalysis of hash and claw-free functions”. In: *SIGACT News* 28.2 (1997), pp. 14–19.

References ii

Mihir Bellare and Chanathip Namprempre. “Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm”. In: *Advances in Cryptology - ASIACRYPT 2000*. 2000, pp. 531–545.

Daniel J Bernstein. “Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?”. In: *SHARCS’09 Special-purpose Hardware for Attacking Cryptographic Systems* (2009), p. 105.

Anne Canteaut et al. “Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression”. In: *Fast Software Encryption - 23rd International Conference, FSE 2016*. 2016, pp. 313–333.

Thai Duong and Juliano Rizzo. “Cryptography in the Web: The Case of Cryptographic Design Flaws in ASP.NET”. In: *32nd IEEE Symposium on Security and Privacy, S&P 2011*. 2011, pp. 481–489.

Hidenori Kuwakado and Masakatu Morii. “Security on the quantum-type Even-Mansour cipher”. In: *Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012*. 2012, pp. 312–316.

Marc Kaplan et al. "Breaking Symmetric Cryptosystems Using Quantum Period Finding". In: *Advances in Cryptology - CRYPTO 2016*. 2016, pp. 207–237.

Stefan Kölbl et al. "Haraka v2 - Efficient Short-Input Hashing for Post-Quantum Applications". In: *IACR Trans. Symmetric Cryptol.* 2016 ().

Pierrick Méaux et al. "Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts". In: *Advances in Cryptology - EUROCRYPT 2016*. 2016, pp. 311–343.

Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin. *Breaking 104 bit WEP in less than 60 seconds*. Cryptology ePrint Archive, Report 2007/120. `http://eprint.iacr.org/2007/120`. 2007.