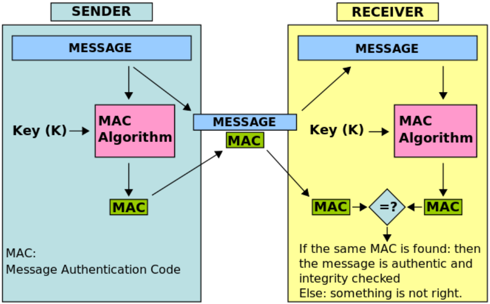
Wegman-Carter Style MACs from TBCs

Jooyoung Lee

School of Computing(GSIS), KAIST

Message Authentication Codes



http://en.wikipedia.org/wiki/File:MAC.svg

- Block cipher-based: CMAC, OMAC etc.
- Hash-based: HMAC
  - $HMAC_K(M) = H((K' \oplus \text{opad})||H(K' \oplus \text{ipad})||M)$
- Universal hashing-based

Security of MACs

MAC Queries

If (N, M) queried, then $T = MAC_{\mathbf{K}}(N, M)$ is returned

- Nonce-respecting: All the nonces are different in the MAC queries
- Nonce-misuse: Nonces might be repreated

Verification Queries

If (N, M, T) is queried, then 1(accept) or 0(reject) is returned

- The adversarial goal is to find at least one successful forgery

The two phases might be separated.

Viewed as a Distinguishing Game

Real World

- A key $\mathbf{K}$ is chosen uniformly at random
- A mac query (N, M) is faithfully answered with $T = MAC_{\mathbf{K}}(N, M)$
- A verification query (N, M, T) is faithfully answered by checking

$$MAC_{\mathbf{K}}(N, M) \stackrel{?}{=} T$$

- At the end of the interaction, the real key $\mathbf{K}$ is given for free

Ideal World

- A mac query (N, M) is answered with the evaluation of an ideal primitive at (N, M)
- A verification query (N, M, T) is always answered with 0(=reject)
- At the end of the interaction, an independent random key $\mathbf{K}$ is given to the distinguisher

Universal Hash Family

Definition

Let $\mathcal{K}$, $\mathcal{X}$, $\mathcal{Y}$ be non-empty sets and let $\varepsilon > 0$. A keyed function

$$H : \mathcal{K} \times \mathcal{X} \longrightarrow \mathcal{Y}$$

is said to be ε-almost xor universal (AXU) if for any distinct $X, X' \in \mathcal{X}$ and $Y \in \mathcal{Y}$,

$$\Pr\left[K \leftarrow_{\$} \mathcal{K} : H_K(X) \oplus H_K(X') = Y\right] \leq \varepsilon.$$

Example

For $M = (M_1, \ldots, M_l) \in \mathbb{F}_{2^n}^l$, and a key $K \in \mathbb{F}_{2^n}$,

$$H_K(M) = M_l K^l + M_{l-1} K^{l-1} + \cdots + M_1 K.$$

Obtained by computing $H \leftarrow (H \oplus M_i)K$ for $i = 1, \ldots, l$, where H is initialized as 0.

Wegman-Carter MAC

- Given an ε-AXU hash family H and a pseudorandom function F, then the tag of a message M is defined as

$$T = H_{K_h}(M) \oplus F_K(N)$$

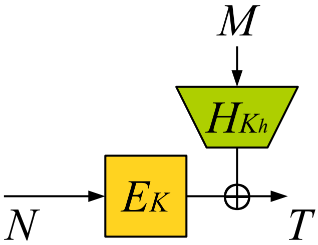
  where N is a nonce.

- Forging probability is upper bounded by $(\frac{1}{2^n} + \varepsilon)q_v$ where
  - $\varepsilon \approx 1/2^n$ and q_v is the number of verification queries
  - F is assumed to be truly random
- Nonces should not be repeated.
  - If nonces are repeated, then one might obtain

$$T \oplus T' = H_{K_h}(M) \oplus H_{K_h}(M')$$

    for T, T', M and M', revealing the secret key K_h

Wegman-Carter MACs based on Block Ciphers



- Typically, F is instantiated with a block cipher E
  - A random permutation is distinguished from a random function with $2^{n/2}$ queries
  - Forging probability is upper bounded by $(\frac{1}{2^n} + \varepsilon)q_v + \frac{(q_m+q_v)^2}{2^n}$
  - Birthday bound is tight?
- Vulnurable to nonce misuse(repetition)

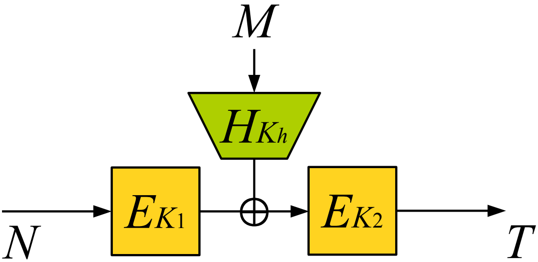
Key Recovery Attack

1. Obtain
$$T_i = MAC_{K,K_h}(N_i, M) = H_{K_h}(M) \oplus E_K(N_i),$$
for a fixed message M and all different nonces N_i, $i = 1, \ldots, 2^{\frac{n}{2}}$.
2. For each candidate key K^*, compute
$$T_i \oplus H_{K^*}(M)$$
for $i = 1, \ldots, 2^{\frac{n}{2}}$.
3. If there exists a collision, then discard K^*. Otherwise, check it using another set of $2^{\frac{n}{2}}$ tags.

Analysis

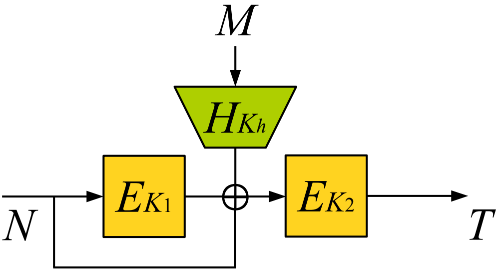
If $K^* = K_h$, then we would have $T_i \oplus H_{K^*}(M) = E_K(N_i)$, which are all different.

Nonce Misuse Resistance



- Resistant to nonce misuse(repetition) up to $2^{n/2}$ queries
- Secure only up to $2^{n/2}$ queries even in the nonce-respecting scenario

Recent Result: EWCDM (Crypto 2016)

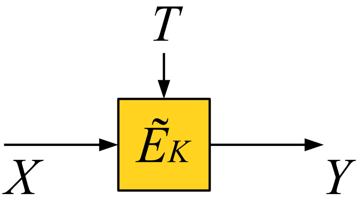


- Secure up to $2^{2n/3}$ queries in the nonce-respecting scenario
- Resistant to nonce misuse(repetition) up to $2^{n/2}$ queries

Open Problems

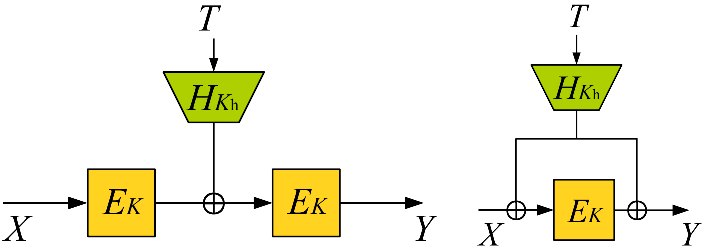
- What if $K_1 = K_2$?
- How truncation affects the security?

Tweakable Block Ciphers



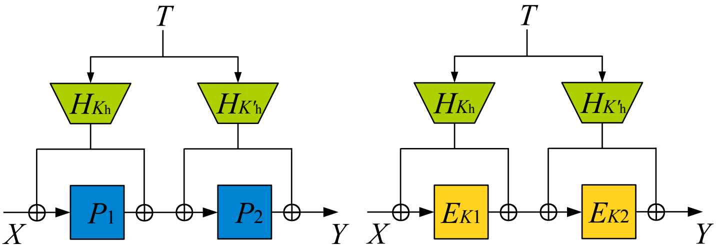
- Additional inputs called tweaks provide variability to the block cipher encryption
- Changing tweaks should be efficient without rekeying
- For a secret random key K, a tweakable block cipher $\widetilde{E}$ should behave like an ideal block cipher
  - A distinguisher adaptively makes forward and backward queries in order to distinguish the construction using a secret random key from the ideal cipher

LRW Constructions (Liskov, Rivest, Wagner: Crypto 2002)



- H is an almost xor universal hash family
- The CMT (left) is secure up to $2^{\frac{n}{2}}$ forward queries
- The LRW (right) is secure up to $2^{\frac{n}{2}}$ forward and backward queries

Tweakable Even-Mansour Ciphers (Cogliati, et al.: Crypto 2015)

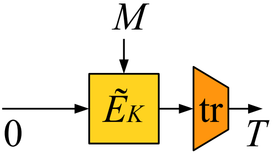


- P_1 and P_2 are public random permutations
- Distinguishing advantages are upper bounded as follows:

$$\mathbf{Adv}_{TEM2}(q_c, q_p) \leq \frac{29\sqrt{q_c}q_p}{2^n} + \varepsilon\sqrt{q_c}q_p + 4\varepsilon q_c^{3/2} + \frac{30q_c^{3/2}}{2^n}$$

$$\mathbf{Adv}_{LRW2}(q_c) \leq 4\varepsilon q_c^{3/2} + \frac{30q_c^{3/2}}{2^n}$$

WC-MACs from Weakly Secure TBCs



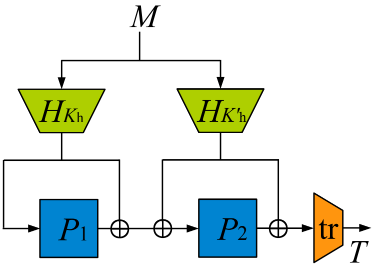
- Plaintext $\rightarrow$ Constant
- Tweak $\rightarrow$ Message (of a variable length)
- Ciphertext $\rightarrow$ Tag

MAC-Security of a (Truncated) Ideal Block Cipher

The forging probability is upper bounded by $q_v/2^\tau$.

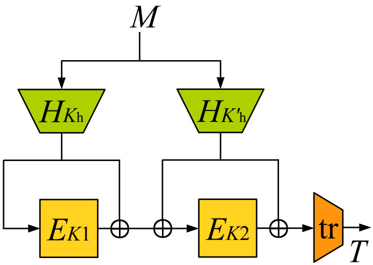
1. No matter how many MAC queries are made, $\tilde{E}_K(M, 0)$ is truly random as long as M has not been queried before.
2. The success probability is $\frac{1}{2^\tau}$ for any verification query (M, T).
3. The tag length can be extended: $T = \tilde{E}_K(M, 0) || \tilde{E}_K(M, 1)$

WC-MAC from the Two-round TEM



- Deterministic (stateless)
- Secure up to $2^{\frac{2n}{3}}$ queries (ignoring the truncation)
- Based on public primitives
- Security analyzed for truncated variants
- But two evaluations of H needed
  - Still faster than block cipher-based ones?

WC-MAC from the Two-round LRW



- Deterministic (stateless)
- Using four keys
- The adversarial forging probability is upper bounded by

$$(q_m + q_v)^{3/2} + \frac{30(q_m + q_v)^{3/2}}{2^n} + \frac{q_v}{2^\tau}$$

Ongoing Research: Using Fully Secure Tweakable Block Ciphers

- Wang et. al. found 32 constructions for TBCs that achieve 2^n security and make two calls to the underlying block cipher
  - $\widetilde{E4}^T_K(X) = E_{T \oplus Y}(X \oplus K) \oplus K$ for $Y = E_K(0)$
  - Only n-bit tweaks accepted (if E is an n-bit key block cipher)
  - Security proved in the ideal cipher model
- Minematsu and Iwata proposed a method of extending tweak lengths:
  - $XTX^T_{K,L}(X) = \tilde{E}^V_K(X \oplus W) \oplus W$ where $H_L(T) = W||V$
  - Let $H_L(T) = H_{K_h}(T)||H_{K'_h}(T)$ for $L = K_h||K'_h$
- Combining the above two construction and viewing Y as an additional key (denoted K') results in...

Ongoing Research: Using Fully Secure Tweakable Block Ciphers

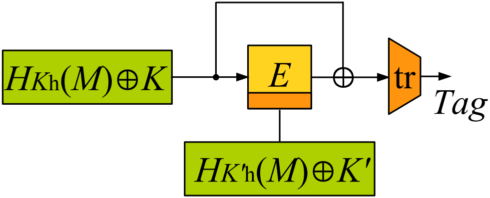
- A new TBC

$$TBC_{\mathbf{K}}^{T}(X) = E_{H_{K_h'}(T)\oplus K'}(X \oplus K \oplus H_{K_h}(T)) \oplus K \oplus H_{K_h}(T).$$

- A new deterministic MAC

$$MAC_{\mathbf{K}}^{T}(X) = E_{H_{K_h'}(M)\oplus K'}(K \oplus H_{K_h}(M)) \oplus K \oplus H_{K_h}(T).$$

  - Using $\mathbf{K} = (K_h, K_h', K, K')$ as a key
  - Single call to the underlying block cipher
  - Fully secure in the ideal cipher model
  - Truncation allowed



Thank You!