New Constructions of MACs from Tweakable Block Ciphers

Benoît Cogliati[1] Yannick Seurin[2] Jooyoung Lee[3]

[1]UL, Luxembourg

[2]ANSSI, France

[3]KAIST, Korea

January , 2017 — Early Symmetric Crypto

Outline

A quick overview of our results

We propose two Nonce-based, two Randomized, and two Deterministic MAC constructions based on a $\varepsilon-$AXU and uniform hash function and a Block Cipher or a Tweakable Block Cipher which are:

- efficient (1 call to the underlying cipher and 1 or 2 calls to the hash function),
- provably (very) secure, in the Ideal Cipher model for BC-based constructions and in the Standard Model for TBC-based ones.

A quick overview of our results

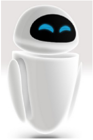
We propose two Nonce-based, two Randomized, and two Deterministic MAC constructions based on a $\varepsilon-$AXU and uniform hash function and a Block Cipher or a Tweakable Block Cipher which are:

- efficient (1 call to the underlying cipher and 1 or 2 calls to the hash function),
- provably (very) secure, in the Ideal Cipher model for BC-based constructions and in the Standard Model for TBC-based ones.

Outline

Nonce-Based Message Authentication Codes

(N, M, T) →



$T = \mathrm{MAC}_K(N, M)$

$\mathrm{MAC}_K(N, M) = T\ ?$

Security Definition

The adversary is allowed

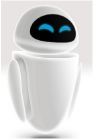
- q_m MAC queries $T = \mathrm{MAC}_K(N, M)$
- q_v verification queries (forgery attempts) (N', M', T')

and is successful if one of the verification queries (N', M', T') passes and no previous MAC query (N', M') returned T'.

The adversary is said nonce-respecting if it does not repeat nonces in MAC queries.

Nonce-Based Message Authentication Codes

$(N, M, T) \longrightarrow$



$(N, M, T) \longrightarrow$

$T = \mathrm{MAC}_K(N, M)$

$\mathrm{MAC}_K(N, M) = T$?

Security Definition

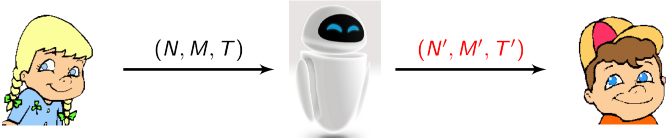
The adversary is allowed

- q_m MAC queries $T = \mathrm{MAC}_K(N, M)$
- q_v verification queries (forgery attempts) (N', M', T')

and is successful if one of the verification queries (N', M', T') passes and no previous MAC query (N', M') returned T'.

The adversary is said nonce-respecting if it does not repeat nonces in MAC queries.

Nonce-Based Message Authentication Codes



$T = \mathrm{MAC}_K(N, M)$

$\mathrm{MAC}_K(N, M) = T$?

Security Definition

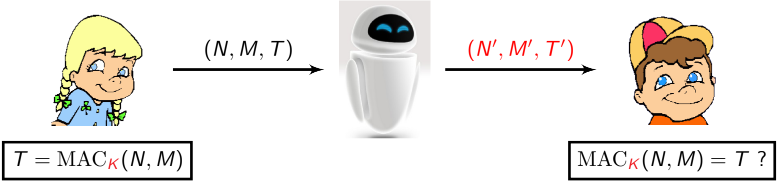
The adversary is allowed

- q_m MAC queries $T = \mathrm{MAC}_K(N, M)$
- q_v verification queries (forgery attempts) (N', M', T')

and is successful if one of the verification queries (N', M', T') passes and no previous MAC query (N', M') returned T'.

The adversary is said nonce-respecting if it does not repeat nonces in MAC queries.

Nonce-Based Message Authentication Codes



Security Definition

The adversary is allowed

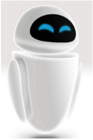
- q_m MAC queries $T = \mathrm{MAC}_K(N, M)$
- q_v verification queries (forgery attempts) (N', M', T')

and is successful if one of the verification queries (N', M', T') passes and no previous MAC query (N', M') returned T'.

The adversary is said nonce-respecting if it does not repeat nonces in MAC queries.

Nonce-Based Message Authentication Codes

(N, M, T) →



(N', M', T') →

$T = \mathrm{MAC}_K(N, M)$

$\mathrm{MAC}_K(N, M) = T$?

Security Definition

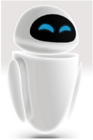
The adversary is allowed

- q_m MAC queries $T = \mathrm{MAC}_K(N, M)$
- q_v verification queries (forgery attempts) (N', M', T')

and is successful if one of the verification queries (N', M', T') passes and no previous MAC query (N', M') returned T'.
The adversary is said nonce-respecting if it does not repeat nonces in MAC queries.

Deterministic Message Authentication Codes

(M, T) →



$T = \mathrm{MAC}_K(M)$

$\mathrm{MAC}_K(M) = T$?

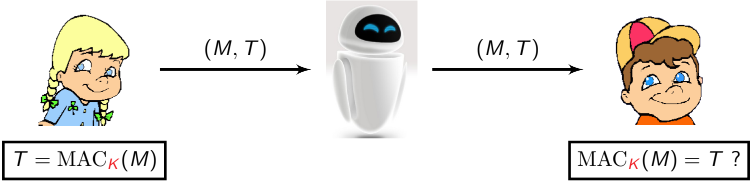
Security Definition

The adversary is allowed

- q_m MAC queries $T = \mathrm{MAC}_K(M)$
- q_v verification queries (forgery attempts) (M', T')

and is successful if one of the verification queries (M', T') passes and no previous MAC query M' returned T'.

Deterministic Message Authentication Codes



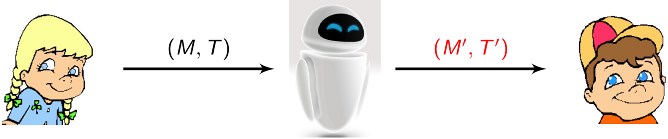
Security Definition

The adversary is allowed

- q_m MAC queries $T = \mathrm{MAC}_K(M)$
- q_v verification queries (forgery attempts) (M', T')

and is successful if one of the verification queries (M', T') passes and no previous MAC query M' returned T'.

Deterministic Message Authentication Codes



$T = \mathrm{MAC}_K(M)$

$\mathrm{MAC}_K(M) = T$?

Security Definition

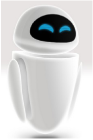
The adversary is allowed

- q_m MAC queries $T = \mathrm{MAC}_K(M)$
- q_v verification queries (forgery attempts) (M', T')

and is successful if one of the verification queries (M', T') passes and no previous MAC query M' returned T'.

Deterministic Message Authentication Codes

(M, T) →



(M', T') →

$T = \mathrm{MAC}_K(M)$

$\mathrm{MAC}_K(M) = T$?

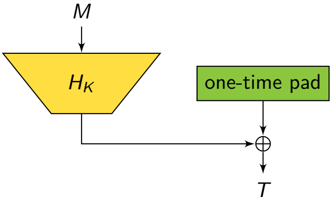
Security Definition

The adversary is allowed

- q_m MAC queries $T = \mathrm{MAC}_K(M)$
- q_v verification queries (forgery attempts) (M', T')

and is successful if one of the verification queries (M', T') passes and no previous MAC query M' returned T'.

Wegman-Carter MACs [GMS74, WC81]



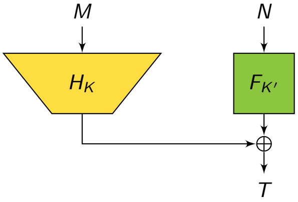
- based on an ε-almost xor-universal (ε-AXU) hash function H:

$$\forall M \neq M', \forall Y, \Pr[K \leftarrow_\$ \mathcal{K} : H_K(M) \oplus H_K(M') = Y] \leq \varepsilon$$

- in practice, OTPs are replaced by a PRF applied to a nonce N
- H usually based on polynomial evaluation (GCM, Poly1305)
- "optimal" security:

$$\mathbf{Adv}_{\mathrm{WC}}^{\mathrm{MAC}}(q_m, q_v) \leq \varepsilon q_v + \mathbf{Adv}_F^{\mathrm{PRF}}(q_m + q_v)$$

Wegman-Carter MACs [GMS74, WC81]



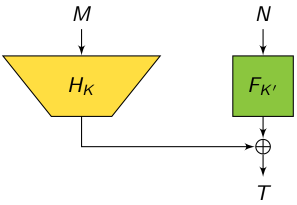
- based on an ε-almost xor-universal (ε-AXU) hash function H:

$$\forall M \neq M', \forall Y, \Pr[K \leftarrow_{\$} \mathcal{K} : H_K(M) \oplus H_K(M') = Y] \leq \varepsilon$$

- in practice, OTPs are replaced by a PRF applied to a nonce N
- H usually based on polynomial evaluation (GCM, Poly1305)
- "optimal" security:

$$\mathbf{Adv}_{\mathrm{WC}}^{\mathrm{MAC}}(q_m, q_v) \leq \varepsilon q_v + \mathbf{Adv}_F^{\mathrm{PRF}}(q_m + q_v)$$

Wegman-Carter MACs [GMS74, WC81]



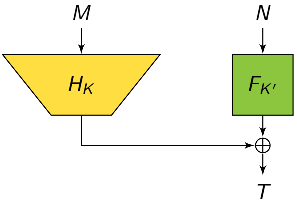
- based on an ε-almost xor-universal (ε-AXU) hash function H:

$$\forall M \neq M', \forall Y, \Pr[K \leftarrow_\$ \mathcal{K} : H_K(M) \oplus H_K(M') = Y] \leq \varepsilon$$

- in practice, OTPs are replaced by a PRF applied to a nonce N
- H usually based on polynomial evaluation (GCM, Poly1305)
- "optimal" security:

$$\mathbf{Adv}^{\mathrm{MAC}}_{\mathrm{WC}}(q_m, q_v) \leq \varepsilon q_v + \mathbf{Adv}^{\mathrm{PRF}}_{F}(q_m + q_v)$$

Wegman-Carter MACs [GMS74, WC81]



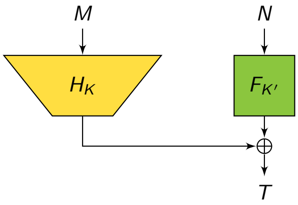
- based on an ε-almost xor-universal (ε-AXU) hash function H:

$$\forall M \neq M', \forall Y, \Pr[K \leftarrow_\$ \mathcal{K} : H_K(M) \oplus H_K(M') = Y] \leq \varepsilon$$

- in practice, OTPs are replaced by a PRF applied to a nonce N
- H usually based on polynomial evaluation (GCM, Poly1305)
- "optimal" security:

$$\mathbf{Adv}^{\mathrm{MAC}}_{\mathsf{WC}}(q_m, q_v) \leq \varepsilon q_v + \mathbf{Adv}^{\mathrm{PRF}}_F(q_m + q_v)$$

Implementing the PRF from a Block Cipher

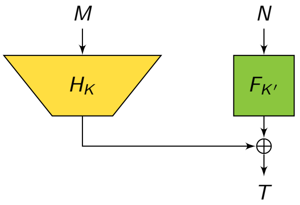


- in practice, F is replaced by a block cipher
- but provable security drops to birthday bound ☹ [Sho96]

$$\mathbf{Adv}^{\mathrm{MAC}}_{\mathrm{WC}}(q_m, q_v) \leq \varepsilon q_v \quad + \mathbf{Adv}^{\mathrm{PRF}}_{F}(q_m + q_v)$$

- a better bound exists [Ber05] but still "birthday-type"
- solution: BBB-secure PRP-to-PRF conversion

Implementing the PRF from a Block Cipher

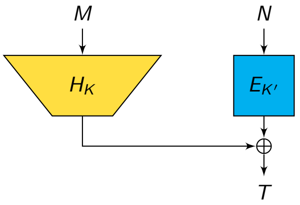


- in practice, F is replaced by a block cipher
- but provable security drops to birthday bound ☹ [Sho96]

$$\mathbf{Adv}^{\mathrm{MAC}}_{\mathrm{WC}}(q_m, q_v) \le \varepsilon q_v \quad + \mathbf{Adv}^{\mathrm{PRF}}_{F}(q_m + q_v)$$

- a better bound exists [Ber05] but still "birthday-type"
- solution: BBB-secure PRP-to-PRF conversion

Implementing the PRF from a Block Cipher

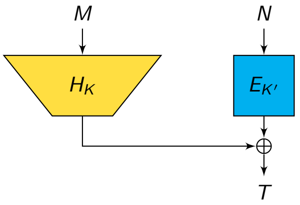


- in practice, F is replaced by a block cipher
- but provable security drops to birthday bound ☹ [Sho96]

$$\mathbf{Adv}_{\mathrm{WC}}^{\mathrm{MAC}}(q_m, q_v) \leq \varepsilon q_v \quad + \frac{(q_m+q_v)^2}{2 \cdot 2^n}$$

- a better bound exists [Ber05] but still "birthday-type"
- solution: BBB-secure PRP-to-PRF conversion

Implementing the PRF from a Block Cipher

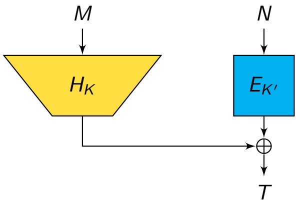


- in practice, F is replaced by a block cipher
- but provable security drops to birthday bound ☹ [Sho96]

$$\mathbf{Adv}^{\mathrm{MAC}}_{\mathsf{WC}}(q_m, q_v) \leq \varepsilon q_v \quad + \frac{(q_m+q_v)^2}{2 \cdot 2^n}$$

- a better bound exists [Ber05] but still "birthday-type"
- solution: BBB-secure PRP-to-PRF conversion

Implementing the PRF from a Block Cipher

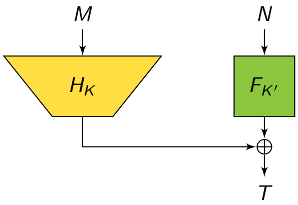


- in practice, F is replaced by a block cipher
- but provable security drops to birthday bound ☹ [Sho96]

$$\mathbf{Adv}^{\mathrm{MAC}}_{\mathrm{WC}}(q_m, q_v) \leq \varepsilon q_v \quad + \frac{(q_m+q_v)^2}{2 \cdot 2^n}$$

- a better bound exists [Ber05] but still "birthday-type"
- solution: BBB-secure PRP-to-PRF conversion

The Nonce-Misuse Problem

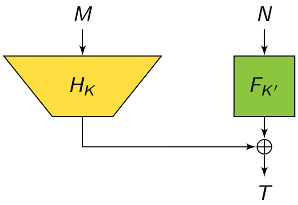


- Wegman-Carter MACs are brittle: a single nonce repetition can completely break security [Jou06, HP08]
- esp. for polynomial-based hashing, i.e., $H_K(M) = P_M(K)$:

$$\begin{cases} P_M(K) \oplus F_{K'}(N) = T \\ P_{M'}(K) \oplus F_{K'}(N) = T' \end{cases} \Rightarrow P_M(K) \oplus P_{M'}(K) = T \oplus T'$$

- solution: extra PRF call (in fact, OK to use a PRP here)

The Nonce-Misuse Problem

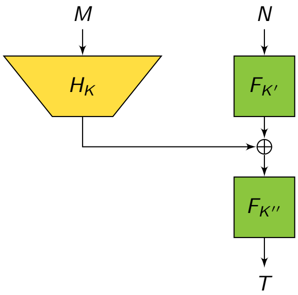


- Wegman-Carter MACs are brittle: a single nonce repetition can completely break security [Jou06, HP08]
- esp. for polynomial-based hashing, i.e., $H_K(M) = P_M(K)$:

$$\begin{cases} P_M(K) \oplus F_{K'}(N) = T \\ P_{M'}(K) \oplus F_{K'}(N) = T' \end{cases} \Rightarrow P_M(K) \oplus P_{M'}(K) = T \oplus T'$$

- solution: extra PRF call (in fact, OK to use a PRP here)

The Nonce-Misuse Problem

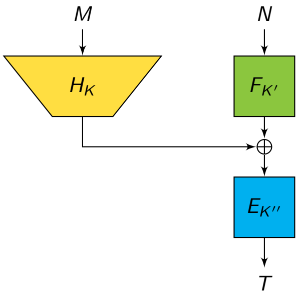


- Wegman-Carter MACs are brittle: a single nonce repetition can completely break security [Jou06, HP08]
- esp. for polynomial-based hashing, i.e., $H_K(M) = P_M(K)$:

$$\begin{cases} P_M(K) \oplus F_{K'}(N) = T \\ P_{M'}(K) \oplus F_{K'}(N) = T' \end{cases} \Rightarrow P_M(K) \oplus P_{M'}(K) = T \oplus T'$$

- solution: extra PRF call (in fact, OK to use a PRP here)

The Nonce-Misuse Problem

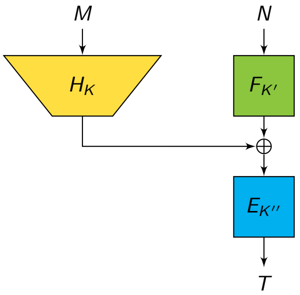


- Wegman-Carter MACs are brittle: a single nonce repetition can completely break security [Jou06, HP08]
- esp. for polynomial-based hashing, i.e., $H_K(M) = P_M(K)$:

$$\begin{cases} P_M(K) \oplus F_{K'}(N) = T \\ P_{M'}(K) \oplus F_{K'}(N) = T' \end{cases} \Rightarrow P_M(K) \oplus P_{M'}(K) = T \oplus T'$$

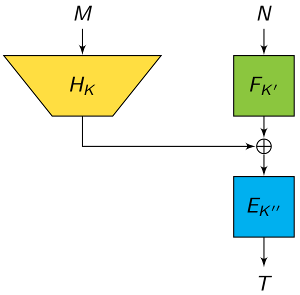
- solution: extra PRF call (in fact, OK to use a PRP here)

The Nonce-Misuse Problem



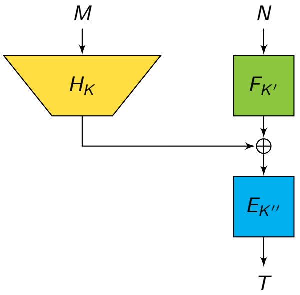
- good security against *nonce-respecting* adversaries ;
- BUT security drops to the birthday bound when a nonce is used twice ;
- same problem when implementing F from a Block Cipher ;
- too simple mixing of the nonce and the hash of the message...

The Nonce-Misuse Problem



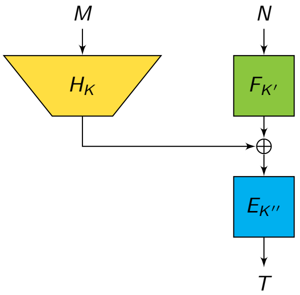
- good security against *nonce-respecting* adversaries ;
- BUT security drops to the birthday bound when a nonce is used twice ;
- same problem when implementing F from a Block Cipher ;
- too simple mixing of the nonce and the hash of the message...

The Nonce-Misuse Problem



- good security against *nonce-respecting* adversaries ;
- BUT security drops to the birthday bound when a nonce is used twice ;
- same problem when implementing F from a Block Cipher ;
- too simple mixing of the nonce and the hash of the message...

The Nonce-Misuse Problem



- good security against *nonce-respecting* adversaries ;
- BUT security drops to the birthday bound when a nonce is used twice ;
- same problem when implementing F from a Block Cipher ;
- too simple mixing of the nonce and the hash of the message...

A Useful Remark

- Take any two sets S, T and a set of triples $\tau = \{(s, t_1, t_1'), \dots, (s, t_q, t_q')\}$ such that

$$\forall 1 \leq i \neq j \leq q,\ s_i = s_j \implies t_i \neq t_j \text{ and } t_i' \neq t_j'.$$

- Take an additional triple $(s, t, t') \notin \tau$.
- Then, the probability that a uniformly random family of permutations $(P_s)_{s \in S} \in \mathrm{Perm}\{T\}^S$ satisfies

$$\forall 1 \leq i \leq q,\ P_{s_i}(t_i) = t_i', \qquad P_s(t) = t'$$

is greater than

$$\left(1 - \frac{1}{2^n - \max(q_1, \dots, q_r)}\right) \prod_{i=1}^{r} \frac{(2^n - q_i)!}{(2^n)!} \qquad (1)$$

where r is the number distinct $s \in S$ in τ, and q_i is the number of occurences of tweak s_i.

A Useful Remark

- Take any two sets S, T and a set of triples $\tau = \{(s, t_1, t'_1), \ldots, (s, t_q, t'_q)\}$ such that

$$\forall 1 \leq i \neq j \leq q,\ s_i = s_j \implies t_i \neq t_j \text{ and } t'_i \neq t'_j.$$

- Take an additional triple $(s, t, t') \notin \tau$.
- Then, the probability that a uniformly random family of permutations $(P_s)_{s \in S} \in \mathrm{Perm}\{T\}^S$ satisfies

$$\forall 1 \leq i \leq q,\ P_{s_i}(t_i) = t'_i, \qquad P_s(t) = t'$$

is greater than

$$\left(1 - \frac{1}{2^n - \max(q_1, \ldots, q_r)}\right) \prod_{i=1}^{r} \frac{(2^n - q_i)!}{(2^n)!} \qquad (1)$$

where r is the number distinct $s \in S$ in τ, and q_i is the number of occurences of tweak s_i.

A Useful Remark

- Take any two sets S, T and a set of triples $\tau = \{(s, t_1, t'_1), \ldots, (s, t_q, t'_q)\}$ such that

$$\forall 1 \leq i \neq j \leq q,\ s_i = s_j \implies t_i \neq t_j \text{ and } t'_i \neq t'_j.$$

- Take an additional triple $(s, t, t') \notin \tau$.
- Then, the probability that a uniformly random family of permutations $(P_s)_{s \in S} \in \text{Perm}\{T\}^S$ satisfies

$$\forall 1 \leq i \leq q,\ P_{s_i}(t_i) = t'_i, \qquad P_s(t) = t'$$

is greater than

$$\left(1 - \frac{1}{2^n - \max(q_1, \ldots, q_r)}\right) \prod_{i=1}^{r} \frac{(2^n - q_i)!}{(2^n)!} \qquad (1)$$

where r is the number distinct $s \in S$ in τ, and q_i is the number of occurences of tweak s_i.

A Useful Remark (continued)

- An Ideal Cipher is exactly a uniformly random family of permutations ;

A Useful Remark (continued)

- An Ideal Cipher is exactly a uniformly random family of permutations ;
- A secure Tweakable Block Cipher instantiated with a random key must behave as uniformly random family of permutations ;

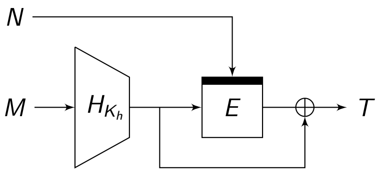
A Useful Remark (continued)

- An Ideal Cipher is exactly a uniformly random family of permutations ;
- A secure Tweakable Block Cipher instantiated with a random key must behave as uniformly random family of permutations ;

It is possible to build secure MACs using previous remark by ensuring that r remains low !

Outline

A Nonce-Based MAC

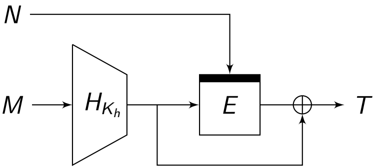


- Dubbed the HENK construction (*Hash-then-Encrypt with Nonce as Key*).
- Based on a BC E and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the BC and 1 call to H.
- Secure: probability of forgery for a (μ, q_m, q_e, q_v)−adversary is lower than

$$\frac{(\mu-1)q_m}{2^n}+(\mu-1)\varepsilon q_m+\frac{q_v}{2^n-\mu-q_e}+(3\mu+n)\varepsilon q_v+\frac{q_e}{2^n-q_e}.$$

- Proof in the Ideal Cipher Model.

A Nonce-Based MAC

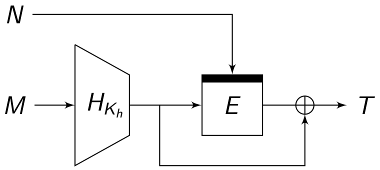


- Dubbed the HENK construction (*Hash-then-Encrypt with Nonce as Key*).
- Based on a BC E and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the BC and 1 call to H.
- Secure: probability of forgery for a $(\mu, q_m, q_e, q_v)-$adversary is lower than

$$\frac{(\mu-1)q_m}{2^n}+(\mu-1)\varepsilon q_m+\frac{q_v}{2^n-\mu-q_e}+(3\mu+n)\varepsilon q_v+\frac{q_e}{2^n-q_e}.$$

- Proof in the Ideal Cipher Model.

A Nonce-Based MAC

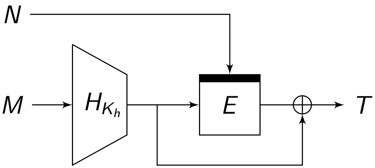


- Dubbed the HENK construction (*Hash-then-Encrypt with Nonce as Key*).
- Based on a BC E and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the BC and 1 call to H.
- Secure: probability of forgery for a $(\mu, q_m, q_e, q_v)-$adversary is lower than

$$\frac{(\mu-1)q_m}{2^n}+(\mu-1)\varepsilon q_m+\frac{q_v}{2^n-\mu-q_e}+(3\mu+n)\varepsilon q_v+\frac{q_e}{2^n-q_e}.$$

- Proof in the Ideal Cipher Model.

A Nonce-Based MAC

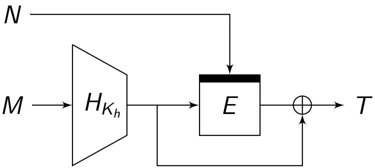


- Dubbed the HENK construction (*Hash-then-Encrypt with Nonce as Key*).
- Based on a BC E and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the BC and 1 call to H.
- Secure: probability of forgery for a (μ, q_m, q_e, q_v)−adversary is lower than

$$\frac{(\mu-1)q_m}{2^n}+(\mu-1)\varepsilon q_m+\frac{q_v}{2^n-\mu-q_e}+(3\mu+n)\varepsilon q_v+\frac{q_e}{2^n-q_e}.$$

- Proof in the Ideal Cipher Model.

A Nonce-Based MAC



- Dubbed the HENK construction (*Hash-then-Encrypt with Nonce as Key*).
- Based on a BC E and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the BC and 1 call to H.
- Secure: probability of forgery for a $(\mu, q_m, q_e, q_v)-$adversary is lower than

$$\frac{(\mu-1)q_m}{2^n} + (\mu-1)\varepsilon q_m + \frac{q_v}{2^n-\mu-q_e} + (3\mu+n)\varepsilon q_v + \frac{q_e}{2^n-q_e}.$$

- Proof in the Ideal Cipher Model.

A Nonce-Based MAC (proof)

Before applying Eq 1, we need to make sure that none of the following holds:

- there exists a block cipher query $(K, X, Y) \in \tau_e$ and a verification query $(N', M', T', b) \in \tau_v$ such that
$$K = N',\ Y = T' \oplus H_{K_h}(M'),\ X = H_{K_h}(M'),$$
- there exists a MAC query $(N, M, T) \in \tau_m$ and a verification query $(N', M', T', b) \in \tau_v$ such that
$$N = N',\ T = T',\ H_{K_h}(M) = H_{K_h}(M'),$$
- there exists two distinct MAC queries (N, M, T) and (N', M', T') such that $N = N'$ and either $H_{K_h}(M) = H_{K_h}(M')$ or $T \oplus H_{K_h}(M) = T' \oplus H_{K_h}(M')$,
- there exists a block cipher query $(K, X, Y) \in \tau_e$ and a MAC query $(N, M, T) \in \tau_m$ such that $K = N$ and either $X = H_{K_h}(M)$ or $Y = T \oplus H_{K_h}(M)$.

A Nonce-Based MAC (proof)

Before applying Eq 1, we need to make sure that none of the following holds:

- there exists a block cipher query $(K, X, Y) \in \tau_e$ and a verification query $(N', M', T', b) \in \tau_v$ such that

$$K = N',\ Y = T' \oplus H_{K_h}(M'),\ X = H_{K_h}(M'),$$

- there exists a MAC query $(N, M, T) \in \tau_m$ and a verification query $(N', M', T', b) \in \tau_v$ such that

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

- there exists two distinct MAC queries (N, M, T) and (N', M', T') such that $N = N'$ and either $H_{K_h}(M) = H_{K_h}(M')$ or $T \oplus H_{K_h}(M) = T' \oplus H_{K_h}(M')$,
- there exists a block cipher query $(K, X, Y) \in \tau_e$ and a MAC query $(N, M, T) \in \tau_m$ such that $K = N$ and either $X = H_{K_h}(M)$ or $Y = T \oplus H_{K_h}(M)$.

A Nonce-Based MAC (proof)

Before applying Eq 1, we need to make sure that none of the following holds:

- there exists a block cipher query $(K, X, Y) \in \tau_e$ and a verification query $(N', M', T', b) \in \tau_v$ such that

$$K = N',\ Y = T' \oplus H_{K_h}(M'),\ X = H_{K_h}(M'),$$

- there exists a MAC query $(N, M, T) \in \tau_m$ and a verification query $(N', M', T', b) \in \tau_v$ such that

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

- there exists two distinct MAC queries (N, M, T) and (N', M', T') such that $N = N'$ and either $H_{K_h}(M) = H_{K_h}(M')$ or $T \oplus H_{K_h}(M) = T' \oplus H_{K_h}(M')$,
- there exists a block cipher query $(K, X, Y) \in \tau_e$ and a MAC query $(N, M, T) \in \tau_m$ such that $K = N$ and either $X = H_{K_h}(M)$ or $Y = T \oplus H_{K_h}(M)$.

A Nonce-Based MAC (proof)

Before applying Eq 1, we need to make sure that none of the following holds:

- there exists a block cipher query $(K, X, Y) \in \tau_e$ and a verification query $(N', M', T', b) \in \tau_v$ such that
$$K = N',\ Y = T' \oplus H_{K_h}(M'),\ X = H_{K_h}(M'),$$
- there exists a MAC query $(N, M, T) \in \tau_m$ and a verification query $(N', M', T', b) \in \tau_v$ such that
$$N = N',\ T = T',\ H_{K_h}(M) = H_{K_h}(M'),$$
- there exists two distinct MAC queries (N, M, T) and (N', M', T') such that $N = N'$ and either $H_{K_h}(M) = H_{K_h}(M')$ or $T \oplus H_{K_h}(M) = T' \oplus H_{K_h}(M')$,
- there exists a block cipher query $(K, X, Y) \in \tau_e$ and a MAC query $(N, M, T) \in \tau_m$ such that $K = N$ and either $X = H_{K_h}(M)$ or $Y = T \oplus H_{K_h}(M)$.

A Randomized Variant

- Dubbed the HERK construction (*Hash-then-Encrypt with Random Key*).
- Based HENK, but instead of a nonce we use a random key.
- Efficient: 1 call to the BC and 1 call to H.
- Secure: probability of forgery for a $(q_m, q_e, q_v)-$adversary is lower than

$$\frac{(n-1)q_m}{2^n} + (n-1)\varepsilon q_m + \frac{q_v}{2^n - n - q_e} + 4n\varepsilon q_v + \frac{q_e}{2^n - q_e}.$$

- Proof in the Ideal Cipher Model.

A Randomized Variant

- Dubbed the HERK construction (*Hash-then-Encrypt with Random Key*).
- Based HENK, but instead of a nonce we use a random key.
- Efficient: 1 call to the BC and 1 call to H.
- Secure: probability of forgery for a (q_m, q_e, q_v)−adversary is lower than

$$\frac{(n-1)q_m}{2^n} + (n-1)\varepsilon q_m + \frac{q_v}{2^n - n - q_e} + 4n\varepsilon q_v + \frac{q_e}{2^n - q_e}.$$

- Proof in the Ideal Cipher Model.

A Randomized Variant

- Dubbed the HERK construction (*Hash-then-Encrypt with Random Key*).
- Based HENK, but instead of a nonce we use a random key.
- Efficient: 1 call to the BC and 1 call to H.
- Secure: probability of forgery for a $(q_m, q_e, q_v)-$adversary is lower than

$$\frac{(n-1)q_m}{2^n} + (n-1)\varepsilon q_m + \frac{q_v}{2^n - n - q_e} + 4n\varepsilon q_v + \frac{q_e}{2^n - q_e}.$$

- Proof in the Ideal Cipher Model.

A Randomized Variant

- Dubbed the HERK construction (*Hash-then-Encrypt with Random Key*).
- Based HENK, but instead of a nonce we use a random key.
- Efficient: 1 call to the BC and 1 call to H.
- Secure: probability of forgery for a $(q_m, q_e, q_v)-$adversary is lower than

$$\frac{(n-1)q_m}{2^n} + (n-1)\varepsilon q_m + \frac{q_v}{2^n - n - q_e} + 4n\varepsilon q_v + \frac{q_e}{2^n - q_e}.$$

- Proof in the Ideal Cipher Model.

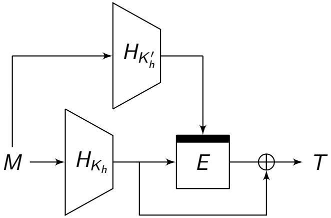
A Randomized Variant

- Dubbed the HERK construction (*Hash-then-Encrypt with Random Key*).
- Based HENK, but instead of a nonce we use a random key.
- Efficient: 1 call to the BC and 1 call to H.
- Secure: probability of forgery for a $(q_m, q_e, q_v)-$adversary is lower than

$$\frac{(n-1)q_m}{2^n} + (n-1)\varepsilon q_m + \frac{q_v}{2^n - n - q_e} + 4n\varepsilon q_v + \frac{q_e}{2^n - q_e}.$$

- Proof in the Ideal Cipher Model.

A Standard MAC

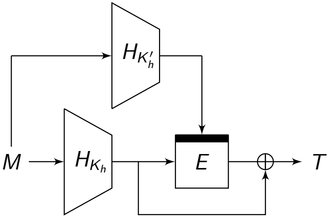


- Dubbed the HEHK construction (*Hash-then-Encrypt with Hash as Key*).
- Based on a BC E and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the BC and 2 calls to H.
- Secure: probability of forgery for a $(q_m, q_e, q_v)-$adversary is lower than

$$2\varepsilon^2 q_m(q_m + q_e) + \varepsilon^2(q_m + q_e)q_v + \frac{q_v}{2^n - q_m - q_e}$$

- Proof in the Ideal Cipher Model.

A Standard MAC

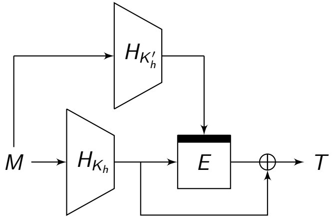


- Dubbed the HEHK construction (*Hash-then-Encrypt with Hash as Key*).
- Based on a BC E and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the BC and 2 calls to H.
- Secure: probability of forgery for a (q_m, q_e, q_v)−adversary is lower than

$$2\varepsilon^2 q_m(q_m + q_e) + \varepsilon^2(q_m + q_e)q_v + \frac{q_v}{2^n - q_m - q_e}$$

- Proof in the Ideal Cipher Model.

A Standard MAC

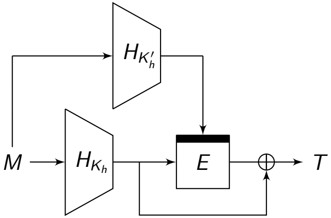


- Dubbed the HEHK construction (*Hash-then-Encrypt with Hash as Key*).
- Based on a BC E and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the BC and 2 calls to H.
- Secure: probability of forgery for a (q_m, q_e, q_v)−adversary is lower than

$$2\varepsilon^2 q_m(q_m + q_e) + \varepsilon^2(q_m + q_e)q_v + \frac{q_v}{2^n - q_m - q_e}$$

- Proof in the Ideal Cipher Model.

A Standard MAC

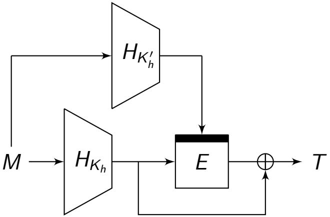


- Dubbed the HEHK construction (*Hash-then-Encrypt with Hash as Key*).
- Based on a BC E and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the BC and 2 calls to H.
- Secure: probability of forgery for a $(q_m, q_e, q_v)-$adversary is lower than

$$2\varepsilon^2 q_m(q_m + q_e) + \varepsilon^2(q_m + q_e)q_v + \frac{q_v}{2^n - q_m - q_e}$$

- Proof in the Ideal Cipher Model.

A Standard MAC



- Dubbed the HEHK construction (*Hash-then-Encrypt with Hash as Key*).
- Based on a BC E and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the BC and 2 calls to H.
- Secure: probability of forgery for a $(q_m, q_e, q_v)-$adversary is lower than

$$2\varepsilon^2 q_m(q_m + q_e) + \varepsilon^2(q_m + q_e)q_v + \frac{q_v}{2^n - q_m - q_e}$$

- Proof in the Ideal Cipher Model.

A Standard MAC (proof)

Before applying Eq 1, we need to make sure that none of the following holds:

- there exist a block cipher query $(K, X, Y) \in \tau_e$ and a verification query $(M', T', b) \in \tau_v$ such that $K = H_{K'_h}(M')$ and $X = H_{K_h}(M')$ and $Y = T' \oplus H_{K_h}(M')$,
- there exist a MAC query $(M, T) \in \tau_m$ and a verification query $(M', T', b) \in \tau_v$ such that $H_{K'_h}(M) = H_{K'_h}(M')$ and $H_{K_h}(M) = H_{K_h}(M')$ and $T = T'$,
- there exists two distinct MAC queries (M, T) and (M', T') such that $H_{K'_h}(M) = H_{K'_h}(M')$ and either $H_{K_h}(M) = H_{K_h}(M')$ or $T \oplus H_{K_h}(M) = T' \oplus H_{K_h}(M')$,
- there exists a block cipher query $(K, X, Y) \in \tau_e$ and a MAC query $(M, T) \in \tau_m$ such that $K = H_{K'_h}(M)$ and either $X = H_{K_h}(M)$ or $Y = T \oplus H_{K_h}(M)$.

A Standard MAC (proof)

Before applying Eq 1, we need to make sure that none of the following holds:

- there exist a block cipher query $(K, X, Y) \in \tau_e$ and a verification query $(M', T', b) \in \tau_v$ such that $K = H_{K_h'}(M')$ and $X = H_{K_h}(M')$ and $Y = T' \oplus H_{K_h}(M')$,
- there exist a MAC query $(M, T) \in \tau_m$ and a verification query $(M', T', b) \in \tau_v$ such that $H_{K_h'}(M) = H_{K_h'}(M')$ and $H_{K_h}(M) = H_{K_h}(M')$ and $T = T'$,
- there exists two distinct MAC queries (M, T) and (M', T') such that $H_{K_h'}(M) = H_{K_h'}(M')$ and either $H_{K_h}(M) = H_{K_h}(M')$ or $T \oplus H_{K_h}(M) = T' \oplus H_{K_h}(M')$,
- there exists a block cipher query $(K, X, Y) \in \tau_e$ and a MAC query $(M, T) \in \tau_m$ such that $K = H_{K_h'}(M)$ and either $X = H_{K_h}(M)$ or $Y = T \oplus H_{K_h}(M)$.

A Standard MAC (proof)

Before applying Eq 1, we need to make sure that none of the following holds:

- there exist a block cipher query $(K, X, Y) \in \tau_e$ and a verification query $(M', T', b) \in \tau_v$ such that $K = H_{K_h'}(M')$ and $X = H_{K_h}(M')$ and $Y = T' \oplus H_{K_h}(M')$,
- there exist a MAC query $(M, T) \in \tau_m$ and a verification query $(M', T', b) \in \tau_v$ such that $H_{K_h'}(M) = H_{K_h'}(M')$ and $H_{K_h}(M) = H_{K_h}(M')$ and $T = T'$,
- there exists two distinct MAC queries (M, T) and (M', T') such that $H_{K_h'}(M) = H_{K_h'}(M')$ and either $H_{K_h}(M) = H_{K_h}(M')$ or $T \oplus H_{K_h}(M) = T' \oplus H_{K_h}(M')$,
- there exists a block cipher query $(K, X, Y) \in \tau_e$ and a MAC query $(M, T) \in \tau_m$ such that $K = H_{K_h'}(M)$ and either $X = H_{K_h}(M)$ or $Y = T \oplus H_{K_h}(M)$.

A Standard MAC (proof)

Before applying Eq 1, we need to make sure that none of the following holds:

- there exist a block cipher query $(K, X, Y) \in \tau_e$ and a verification query $(M', T', b) \in \tau_v$ such that $K = H_{K'_h}(M')$ and $X = H_{K_h}(M')$ and $Y = T' \oplus H_{K_h}(M')$,
- there exist a MAC query $(M, T) \in \tau_m$ and a verification query $(M', T', b) \in \tau_v$ such that $H_{K'_h}(M) = H_{K'_h}(M')$ and $H_{K_h}(M) = H_{K_h}(M')$ and $T = T'$,
- there exists two distinct MAC queries (M, T) and (M', T') such that $H_{K'_h}(M) = H_{K'_h}(M')$ and either $H_{K_h}(M) = H_{K_h}(M')$ or $T \oplus H_{K_h}(M) = T' \oplus H_{K_h}(M')$,
- there exists a block cipher query $(K, X, Y) \in \tau_e$ and a MAC query $(M, T) \in \tau_m$ such that $K = H_{K'_h}(M)$ and either $X = H_{K_h}(M)$ or $Y = T \oplus H_{K_h}(M)$.

Outline

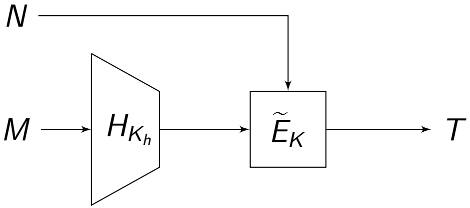
Context

Block Cipher Based Constructions

Tweakable Block Cipher Based Constructions

Security of Truncated MACs

A Nonce-Based MAC

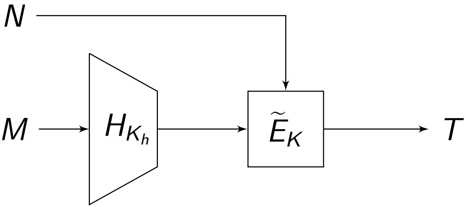


- Dubbed the HENT construction (*Hash-then-Encrypt with Nonce as Tweak*).
- Based on a TBC $\widetilde{E}$ and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the TBC and 1 call to H.
- Secure: probability of forgery for a $(\mu, q_m, q_v)-$adversary is lower than

$$\mathbf{Adv}_{\widetilde{E}}^{\mathrm{TPRP}}(\mathrm{A}') + \frac{(\mu-1)q_m}{2^n} + (\mu-1)q_m\varepsilon + \frac{q_v}{2^n-\mu} + \mu q_v \varepsilon$$

- Proof in the Standard Model!

A Nonce-Based MAC

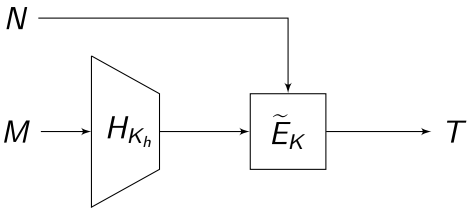


- Dubbed the HENT construction (*Hash-then-Encrypt with Nonce as Tweak*).
- Based on a TBC $\widetilde{E}$ and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the TBC and 1 call to H.
- Secure: probability of forgery for a $(\mu, q_m, q_v)-$adversary is lower than

$$\mathbf{Adv}_{\widetilde{E}}^{\mathrm{TPRP}}(\mathrm{A}') + \frac{(\mu-1)q_m}{2^n} + (\mu-1)q_m\varepsilon + \frac{q_v}{2^n-\mu} + \mu q_v \varepsilon$$

- Proof in the Standard Model!

A Nonce-Based MAC

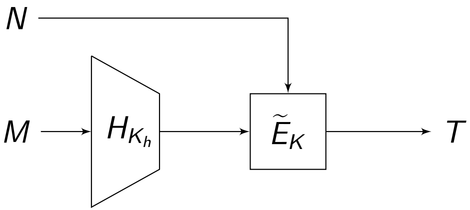


- Dubbed the HENT construction (*Hash-then-Encrypt with Nonce as Tweak*).
- Based on a TBC $\widetilde{E}$ and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the TBC and 1 call to H.
- Secure: probability of forgery for a (μ, q_m, q_v)−adversary is lower than

$$\mathbf{Adv}^{\mathrm{TPRP}}_{\widetilde{E}}(\mathrm{A}') + \frac{(\mu-1)q_m}{2^n} + (\mu-1)q_m\varepsilon + \frac{q_v}{2^n-\mu} + \mu q_v \varepsilon$$

- Proof in the Standard Model!

A Nonce-Based MAC

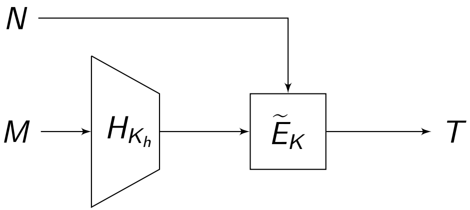


- Dubbed the HENT construction (*Hash-then-Encrypt with Nonce as Tweak*).
- Based on a TBC $\widetilde{E}$ and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the TBC and 1 call to H.
- Secure: probability of forgery for a $(\mu, q_m, q_v)-$adversary is lower than

$$\mathbf{Adv}_{\widetilde{E}}^{\mathrm{TPRP}}(\mathrm{A}') + \frac{(\mu-1)q_m}{2^n} + (\mu-1)q_m\varepsilon + \frac{q_v}{2^n-\mu} + \mu q_v \varepsilon$$

- Proof in the Standard Model!

A Nonce-Based MAC



- Dubbed the HENT construction (*Hash-then-Encrypt with Nonce as Tweak*).
- Based on a TBC $\widetilde{E}$ and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the TBC and 1 call to H.
- Secure: probability of forgery for a $(\mu, q_m, q_v)-$adversary is lower than

$$\mathbf{Adv}_{\widetilde{E}}^{\mathrm{TPRP}}(\mathsf{A}') + \frac{(\mu-1)q_m}{2^n} + (\mu-1)q_m\varepsilon + \frac{q_v}{2^n-\mu} + \mu q_v \varepsilon$$

- Proof in the Standard Model!

A Nonce-Based MAC (proof)

Before applying Eq 1, we need to make sure that none of the following holds:

- there exists a MAC query $(N_i, M_i, T_i) \in \tau_m$ and a verification query $(N'_j, M'_j, T'_j, b_j) \in \tau_v$ such that

$$\begin{cases} N_i = N'_j \\ T_i = T'_j \\ H_{K_h}(M_i) = H_{K_h}(M'_j), \end{cases}$$

- there exists two distinct MAC queries (N, M, T) and (N', M', T') such that $N = N'$ and either $H_{K_h}(M) = H_{K_h}(M')$ or $T = T'$.

A Nonce-Based MAC (proof)

Before applying Eq 1, we need to make sure that none of the following holds:

- there exists a MAC query $(N_i, M_i, T_i) \in \tau_m$ and a verification query $(N_j', M_j', T_j', b_j) \in \tau_v$ such that

$$\begin{cases} N_i = N_j' \\ T_i = T_j' \\ H_{K_h}(M_i) = H_{K_h}(M_j'), \end{cases}$$

- there exists two distinct MAC queries (N, M, T) and (N', M', T') such that $N = N'$ and either $H_{K_h}(M) = H_{K_h}(M')$ or $T = T'$.

A Randomized Variant

- Dubbed the HERT construction (*Hash-then-Encrypt with Random Tweak*).
- Based on the HERT construction.
- Efficient: 1 call to the TBC and 1 call to H.
- Secure: probability of forgery for a $(q_m, q_v)-$adversary is lower than

$$\mathbf{Adv}_{\widetilde{E}}^{\mathrm{TPRP}}(\mathrm{A}') + \frac{(n-1)q_m}{2^n} + (n-1)q_m\varepsilon + \frac{q_v}{2^n - n} + nq_v\varepsilon$$

- Proof in the Standard Model!

A Randomized Variant

- Dubbed the HERT construction (*Hash-then-Encrypt with Random Tweak*).
- Based on the HERT construction.
- Efficient: 1 call to the TBC and 1 call to H.
- Secure: probability of forgery for a $(q_m, q_v)-$adversary is lower than

$$\mathbf{Adv}_{\widetilde{E}}^{\mathrm{TPRP}}(\mathsf{A}') + \frac{(n-1)q_m}{2^n} + (n-1)q_m\varepsilon + \frac{q_v}{2^n - n} + nq_v\varepsilon$$

- Proof in the Standard Model!

A Randomized Variant

- Dubbed the HERT construction (*Hash-then-Encrypt with Random Tweak*).
- Based on the HERT construction.
- Efficient: 1 call to the TBC and 1 call to H.
- Secure: probability of forgery for a (q_m, q_v)−adversary is lower than

$$\mathbf{Adv}_{\widetilde{E}}^{\mathrm{TPRP}}(\mathrm{A}') + \frac{(n-1)q_m}{2^n} + (n-1)q_m\varepsilon + \frac{q_v}{2^n - n} + nq_v\varepsilon$$

- Proof in the Standard Model!

A Randomized Variant

- Dubbed the HERT construction (*Hash-then-Encrypt with Random Tweak*).
- Based on the HERT construction.
- Efficient: 1 call to the TBC and 1 call to H.
- Secure: probability of forgery for a $(q_m, q_v)-$adversary is lower than

$$\mathbf{Adv}_{\widetilde{E}}^{\mathrm{TPRP}}(\mathsf{A}') + \frac{(n-1)q_m}{2^n} + (n-1)q_m\varepsilon + \frac{q_v}{2^n - n} + nq_v\varepsilon$$

- Proof in the Standard Model!

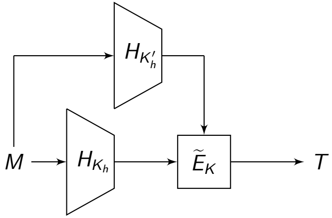
A Randomized Variant

- Dubbed the HERT construction (*Hash-then-Encrypt with Random Tweak*).
- Based on the HERT construction.
- Efficient: 1 call to the TBC and 1 call to H.
- Secure: probability of forgery for a $(q_m, q_v)-$adversary is lower than

$$\mathbf{Adv}_{\widetilde{E}}^{\mathrm{TPRP}}(\mathsf{A}') + \frac{(n-1)q_m}{2^n} + (n-1)q_m\varepsilon + \frac{q_v}{2^n - n} + nq_v\varepsilon$$

- Proof in the Standard Model!

A Standard MAC

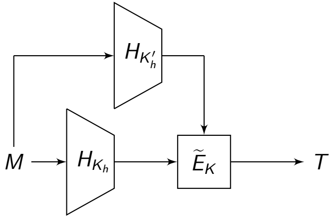


- Dubbed the HEHT construction (*Hash-then-Encrypt with Hash as Tweak*).
- Based on a TBC $\widetilde{E}$ and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the TBC and 2 calls to H.
- Secure: probability of forgery for a $(q_m, q_v)-$adversary is lower than

$$\mathbf{Adv}_{\widetilde{E}}^{\mathrm{TPRP}}(\mathrm{A}') + 2\varepsilon^2 q_m^2 + \varepsilon^2 q_m q_v + \frac{q_v}{2^n - q_m}$$

- Proof in the Standard Model!

A Standard MAC

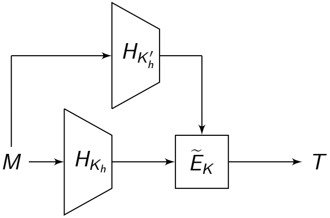


- Dubbed the HEHT construction (*Hash-then-Encrypt with Hash as Tweak*).
- Based on a TBC $\widetilde{E}$ and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the TBC and 2 calls to H.
- Secure: probability of forgery for a $(q_m, q_v)-$adversary is lower than

$$\mathbf{Adv}_{\widetilde{E}}^{\mathrm{TPRP}}(\mathrm{A}') + 2\varepsilon^2 q_m^2 + \varepsilon^2 q_m q_v + \frac{q_v}{2^n - q_m}$$

- Proof in the Standard Model!

A Standard MAC

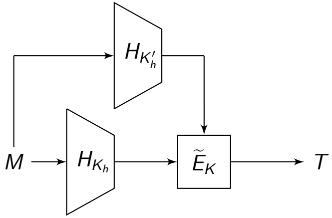


- Dubbed the HEHT construction (*Hash-then-Encrypt with Hash as Tweak*).
- Based on a TBC $\widetilde{E}$ and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the TBC and 2 calls to H.
- Secure: probability of forgery for a (q_m, q_v)−adversary is lower than

$$\mathbf{Adv}_{\widetilde{E}}^{\mathrm{TPRP}}(\mathrm{A}') + 2\varepsilon^2 q_m^2 + \varepsilon^2 q_m q_v + \frac{q_v}{2^n - q_m}$$

- Proof in the Standard Model!

A Standard MAC

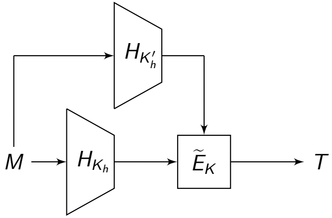


- Dubbed the HEHT construction (*Hash-then-Encrypt with Hash as Tweak*).
- Based on a TBC $\widetilde{E}$ and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the TBC and 2 calls to H.
- Secure: probability of forgery for a $(q_m, q_v)-$adversary is lower than

$$\mathbf{Adv}_{\widetilde{E}}^{\mathrm{TPRP}}(\mathrm{A}') + 2\varepsilon^2 q_m^2 + \varepsilon^2 q_m q_v + \frac{q_v}{2^n - q_m}$$

- Proof in the Standard Model!

A Standard MAC



- Dubbed the HEHT construction (*Hash-then-Encrypt with Hash as Tweak*).
- Based on a TBC $\widetilde{E}$ and a ε-AXU and uniform hash function H.
- Efficient: 1 call to the TBC and 2 calls to H.
- Secure: probability of forgery for a $(q_m, q_v)-$adversary is lower than

$$\mathbf{Adv}_{\widetilde{E}}^{\mathrm{TPRP}}(\mathrm{A}') + 2\varepsilon^2 q_m^2 + \varepsilon^2 q_m q_v + \frac{q_v}{2^n - q_m}$$

- Proof in the Standard Model!

A Standard MAC (proof)

Before applying Eq 1, we need to make sure that none of the following holds:

- there exist a MAC query $(M, T) \in \tau_m$ and a verification query $(M', T', b) \in \tau_v$ such that $H_{K'_h}(M) = H_{K'_h}(M')$ and $H_{K_h}(M) = H_{K_h}(M')$ and $T = T'$,
- there exists two distinct MAC queries (M, T) and (M', T') such that $H_{K'_h}(M) = H_{K'_h}(M')$ and either $H_{K_h}(M) = H_{K_h}(M')$.

A Standard MAC (proof)

Before applying Eq 1, we need to make sure that none of the following holds:

- there exist a MAC query $(M, T) \in \tau_m$ and a verification query $(M', T', b) \in \tau_v$ such that $H_{K'_h}(M) = H_{K'_h}(M')$ and $H_{K_h}(M) = H_{K_h}(M')$ and $T = T'$,
- there exists two distinct MAC queries (M, T) and (M', T') such that $H_{K'_h}(M) = H_{K'_h}(M')$ and either $H_{K_h}(M) = H_{K_h}(M')$.

Outline

Context

Block Cipher Based Constructions

Tweakable Block Cipher Based Constructions

Security of Truncated MACs

What about truncated variations of our constructions ?

Our construction compose well with truncation.

What about truncated variations of our constructions ?

Our construction compose well with truncation.
E.g., if one takes the first s bits of the outputs of the HEHT construction, the probability of forgery of a $(q_m, q_v)-$adversary is lower than

$$\mathbf{Adv}_{\widetilde{E}}^{\mathrm{TPRP}}(\mathsf{A}') + 2\varepsilon^2 q_m^2 + 2^{n-s}\varepsilon^2 q_m q_v + \frac{2^{n-s} q_v}{2^n - q_m}.$$

The end...

Thanks for your attention !

Any questions ?

References I

- Daniel J. Bernstein. Stronger Security Bounds for Wegman-Carter-Shoup Authenticators. In Ronald Cramer, editor, *Advances in Cryptology - EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 164–180. Springer, 2005.

- Edgar N. Gilbert, F. Jessie MacWilliams, and Neil J. A. Sloane. Codes which detect deception. *Bell System Technical Journal*, 53(3):405–424, 1974.

- Helena Handschuh and Bart Preneel. Key-Recovery Attacks on Universal Hash Function Based MAC Algorithms. In David Wagner, editor, *Advances in Cryptology - CRYPTO 2008*, volume 5157 of *LNCS*, pages 144–161. Springer, 2008.

- Antoine Joux. Authentication Failures in NIST Version of GCM. Comments submitted to NIST Modes of Operation Process, 2006. Available at http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/comments/800-38_Series-Drafts/GCM/Joux_comments.pdf.

References II

- Victor Shoup. On Fast and Provably Secure Message Authentication Based on Universal Hashing. In Neal Koblitz, editor, *Advances in Cryptology - CRYPTO '96*, volume 1109 of *LNCS*, pages 313–328. Springer, 1996.

- Mark N. Wegman and Larry Carter. New Hash Functions and Their Use in Authentication and Set Equality. *J. Comput. Syst. Sci.*, 22(3):265–279, 1981.