EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC

Benoît Cogliati[1] Yannick Seurin[2]

[1]University of Versailles, France

[2]ANSSI, France

August 15, 2016 — CRYPTO 2016

Summary of our Contribution

We propose a new Wegman-Carter-style MAC, called

Encrypted Wegman Carter with Davies-Meyer,

based on a xor-universal hash function and a block cipher, with the following properties:

1. it is efficient (two block cipher calls, one of which can be computed in parallel to the hash)
2. it is secure beyond the birthday-bound when nonces are not repeated
3. it retains security up to the birthday bound when nonces are reused

Summary of our Contribution

We propose a new Wegman-Carter-style MAC, called

Encrypted Wegman Carter with Davies-Meyer,

based on a xor-universal hash function and a block cipher, with the following properties:

1. it is efficient (two block cipher calls, one of which can be computed in parallel to the hash)
2. it is secure beyond the birthday-bound when nonces are not repeated
3. it retains security up to the birthday bound when nonces are reused

Summary of our Contribution

We propose a new Wegman-Carter-style MAC, called

Encrypted Wegman Carter with Davies-Meyer,

based on a xor-universal hash function and a block cipher, with the following properties:

1. it is efficient (two block cipher calls, one of which can be computed in parallel to the hash)
2. it is secure beyond the birthday-bound when nonces are not repeated
3. it retains security up to the birthday bound when nonces are reused

Summary of our Contribution

We propose a new Wegman-Carter-style MAC, called

Encrypted Wegman Carter with Davies-Meyer,

based on a xor-universal hash function and a block cipher, with the following properties:

1. it is efficient (two block cipher calls, one of which can be computed in parallel to the hash)
2. it is secure beyond the birthday-bound when nonces are not repeated
3. it retains security up to the birthday bound when nonces are reused

Outline

Outline

Background on Wegman-Carter MACs

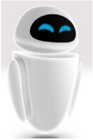
The EWCDM Construction

Security Result and Proof Sketch

Conclusion

(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

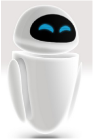
- q_m MAC queries $T = \mathrm{MAC}_K(N, M)$
- q_v verification queries (forgery attempts) (N', M', T')

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) →



(N, M, T) →

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

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

Security Definition

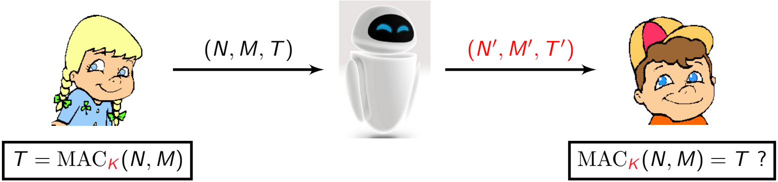
The adversary is allowed

- 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



Security Definition

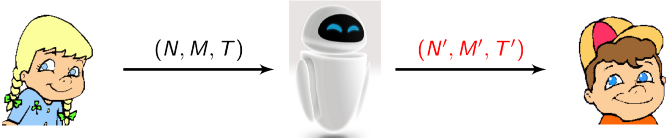
The adversary is allowed

- 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

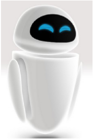
- q_m MAC queries $T = \mathrm{MAC}_K(N, M)$
- q_v verification queries (forgery attempts) (N', M', T')

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

(N, M, T)



(N', M', T')

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

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

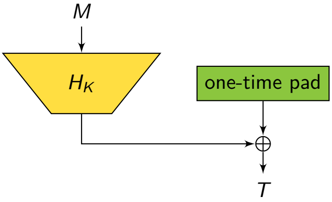
Security Definition

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.

Wegman-Carter MACs [GMS74, WC81]



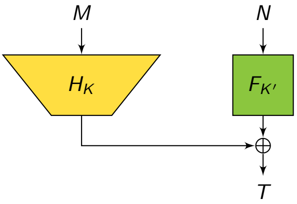
- based on an ε-almost xor-universal (ε-AXU) hash function H:

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

- 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]



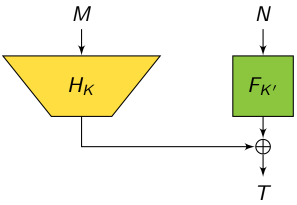
- based on an ε-almost xor-universal (ε-AXU) hash function H:

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

- 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]



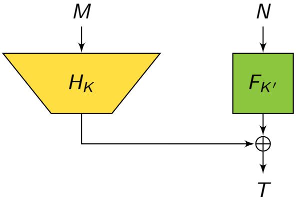
- based on an ε-almost xor-universal (ε-AXU) hash function H:

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

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

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

Wegman-Carter MACs [GMS74, WC81]



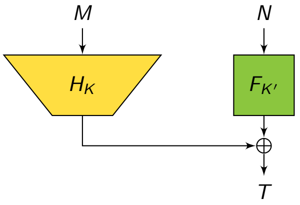
- based on an ε-almost xor-universal (ε-AXU) hash function H:

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

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

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

Implementing the PRF from a Block Cipher

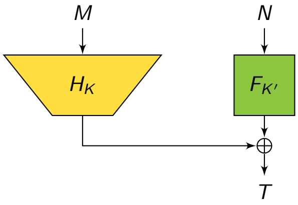


- in practice, F is replaced by a block cipher
- but provable security drops to birthday bound ☹ [Sho96]

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

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

Implementing the PRF from a Block Cipher

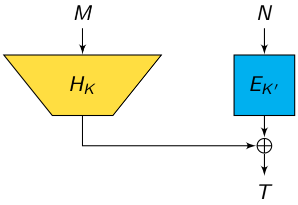


- in practice, F is replaced by a block cipher
- but provable security drops to birthday bound ☹ [Sho96]

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

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

Implementing the PRF from a Block Cipher

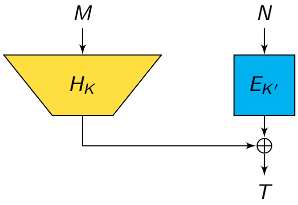


- in practice, F is replaced by a block cipher
- but provable security drops to birthday bound ☹ [Sho96]

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

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

Implementing the PRF from a Block Cipher

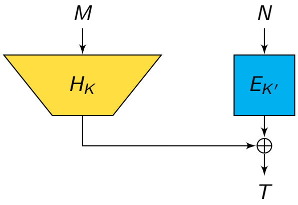


- in practice, F is replaced by a block cipher
- but provable security drops to birthday bound ☹ [Sho96]

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

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

Implementing the PRF from a Block Cipher

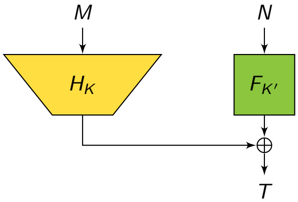


- in practice, F is replaced by a block cipher
- but provable security drops to birthday bound ☹ [Sho96]

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

- a better bound exists [Ber05] but still “birthday-type”
- solution: BBB-secure PRP-to-PRF conversion (more later)

The Nonce-Misuse Problem

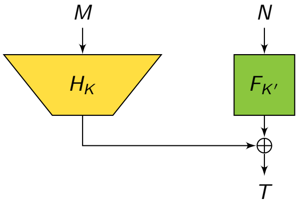


- Wegman-Carter MACs are brittle: a single nonce repetition can completely break security [Jou06, HP08]
- esp. for polynomial-based hashing, i.e., $H_K(M) = P_M(K)$:

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

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

The Nonce-Misuse Problem

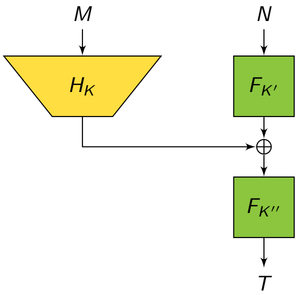


- Wegman-Carter MACs are brittle: a single nonce repetition can completely break security [Jou06, HP08]
- esp. for polynomial-based hashing, i.e., $H_K(M) = P_M(K)$:

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

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

The Nonce-Misuse Problem

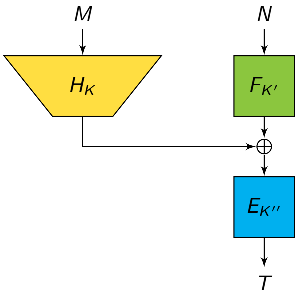


- Wegman-Carter MACs are brittle: a single nonce repetition can completely break security [Jou06, HP08]
- esp. for polynomial-based hashing, i.e., $H_K(M) = P_M(K)$:

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

- 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)

Outline

Our Goal: BBB-security + Nonce-Misuse Resistance

Problem

Design an efficient Wegman-Carter-like MAC:

1. based on a block cipher
2. secure beyond the birthday bound (BBB) in the nonce-respecting case
3. nonce-misuse resistant (at least up to the birthday bound)

State-of-art solution:
Encrypted Wegman-Carter (EWC)
+ PRP-to-PRF conversion

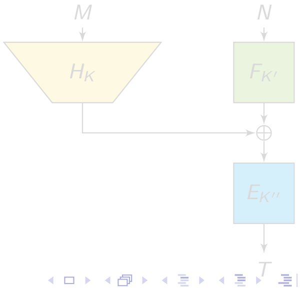
Our Goal: BBB-security + Nonce-Misuse Resistance

Problem

Design an efficient Wegman-Carter-like MAC:

1. based on a block cipher
2. secure beyond the birthday bound (BBB) in the nonce-respecting case
3. nonce-misuse resistant (at least up to the birthday bound)

State-of-art solution:
Encrypted Wegman-Carter (EWC)
+ PRP-to-PRF conversion



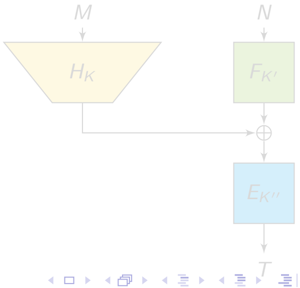
Our Goal: BBB-security + Nonce-Misuse Resistance

Problem

Design an efficient Wegman-Carter-like MAC:

1. based on a block cipher
2. secure beyond the birthday bound (BBB) in the nonce-respecting case
3. nonce-misuse resistant (at least up to the birthday bound)

State-of-art solution:
Encrypted Wegman-Carter (EWC)
+ PRP-to-PRF conversion



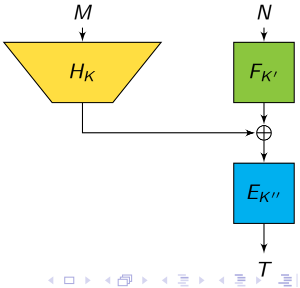
Our Goal: BBB-security + Nonce-Misuse Resistance

Problem

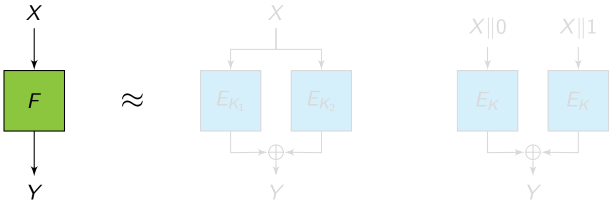
Design an efficient Wegman-Carter-like MAC:

1. based on a block cipher
2. secure beyond the birthday bound (BBB) in the nonce-respecting case
3. nonce-misuse resistant (at least up to the birthday bound)

State-of-art solution:
Encrypted Wegman-Carter (EWC)
+ PRP-to-PRF conversion



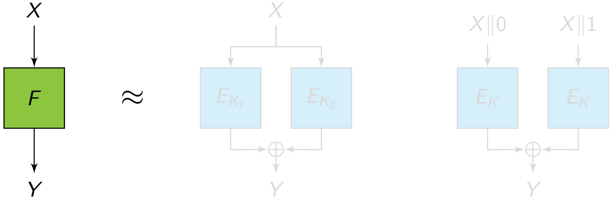
PRP-to-PRF Conversion (Luby-Rackoff Backwards)



A (keyed) n-to-n-bit construction based on a block cipher E is a secure PRP-to-PRF conversion method [BKR98] if it is indist. from a uniformly random function (ideally up to 2^n queries), e.g.:

- E itself is a secure PRF up to $2^{n/2}$ queries
- truncation [HWKS98, BI99]
- XOR construction [Luc00, Pat08a]: $E_{K_1}(X) \oplus E_{K_2}(X)$
- TWIN construction [Luc00]: $E_K(X\|0) \oplus E_K(X\|1)$

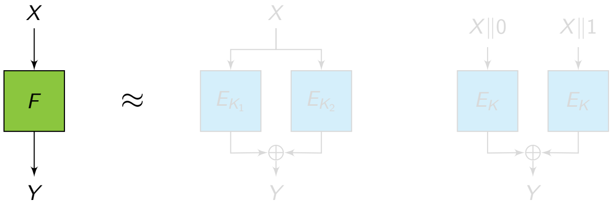
PRP-to-PRF Conversion (Luby-Rackoff Backwards)



A (keyed) n-to-n-bit construction based on a block cipher E is a secure PRP-to-PRF conversion method [BKR98] if it is indist. from a uniformly random function (ideally up to 2^n queries), e.g.:

- E itself is a secure PRF up to $2^{n/2}$ queries
- truncation [HWKS98, BI99]
- XOR construction [Luc00, Pat08a]: $E_{K_1}(X) \oplus E_{K_2}(X)$
- TWIN construction [Luc00]: $E_K(X\|0) \oplus E_K(X\|1)$

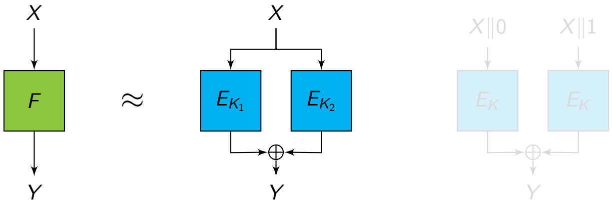
PRP-to-PRF Conversion (Luby-Rackoff Backwards)



A (keyed) n-to-n-bit construction based on a block cipher E is a secure PRP-to-PRF conversion method [BKR98] if it is indist. from a uniformly random function (ideally up to 2^n queries), e.g.:

- E itself is a secure PRF up to $2^{n/2}$ queries
- truncation [HWKS98, BI99]
- XOR construction [Luc00, Pat08a]: $E_{K_1}(X) \oplus E_{K_2}(X)$
- TWIN construction [Luc00]: $E_K(X\|0) \oplus E_K(X\|1)$

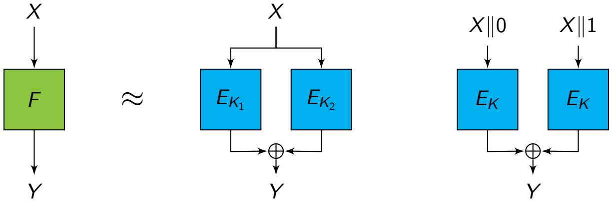
PRP-to-PRF Conversion (Luby-Rackoff Backwards)



A (keyed) n-to-n-bit construction based on a block cipher E is a secure PRP-to-PRF conversion method [BKR98] if it is indist. from a uniformly random function (ideally up to 2^n queries), e.g.:

- E itself is a secure PRF up to $2^{n/2}$ queries
- truncation [HWKS98, BI99]
- XOR construction [Luc00, Pat08a]: $E_{K_1}(X) \oplus E_{K_2}(X)$
- TWIN construction [Luc00]: $E_K(X\|0) \oplus E_K(X\|1)$

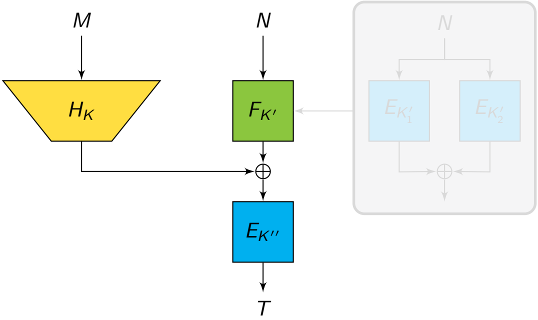
PRP-to-PRF Conversion (Luby-Rackoff Backwards)



A (keyed) n-to-n-bit construction based on a block cipher E is a secure PRP-to-PRF conversion method [BKR98] if it is indist. from a uniformly random function (ideally up to 2^n queries), e.g.:

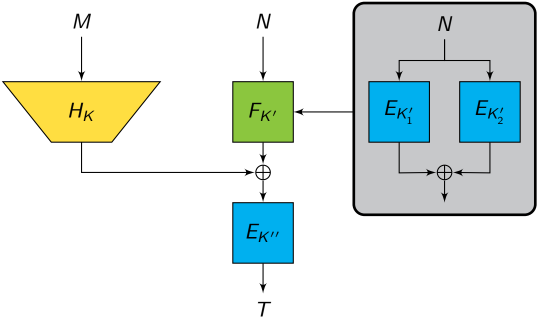
- E itself is a secure PRF up to $2^{n/2}$ queries
- truncation [HWKS98, BI99]
- XOR construction [Luc00, Pat08a]: $E_{K_1}(X) \oplus E_{K_2}(X)$
- TWIN construction [Luc00]: $E_K(X\|0) \oplus E_K(X\|1)$

EWC + PRP-to-PRF Conversion



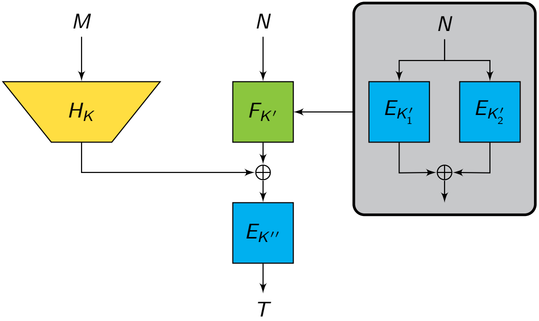
- instantiating F with a BBB-secure PRP-to-PRF construction solves the problem
- but requires at least three BC calls
- is it possible to do better?

EWC + PRP-to-PRF Conversion



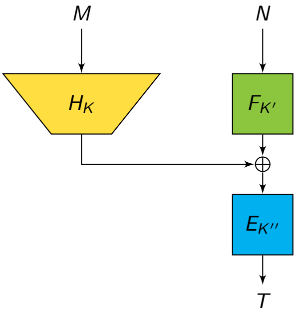
- instantiating F with a BBB-secure PRP-to-PRF construction solves the problem
- but requires at least three BC calls
- is it possible to do better?

EWC + PRP-to-PRF Conversion



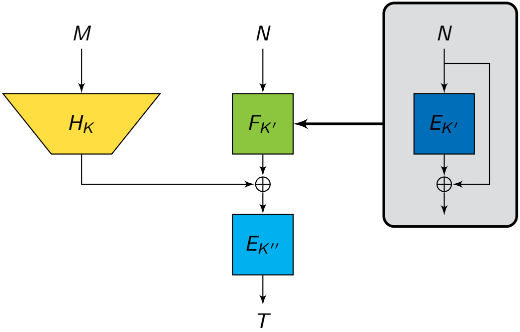
- instantiating F with a BBB-secure PRP-to-PRF construction solves the problem
- but requires at least three BC calls
- is it possible to do better?

Encrypted Wegman-Carter (EWC) + Davies-Meyer (DM)



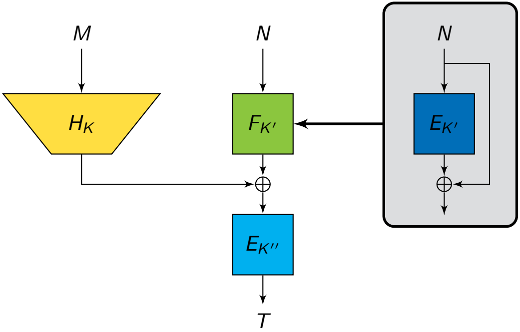
- what if we instantiate $F_{K'}$ with the Davies-Meyer construction $\mathrm{DM}[E]_{K'}(N) = E_{K'}(N) \oplus N$?
- wait! the DM construction is not a BBB-secure PRF: $\mathrm{DM}[E]_{K'}(N) \oplus N = E_{K'}(N)$ is a permutation!
- but here the outer encryption layer prevents this attack

Encrypted Wegman-Carter (EWC) + Davies-Meyer (DM)



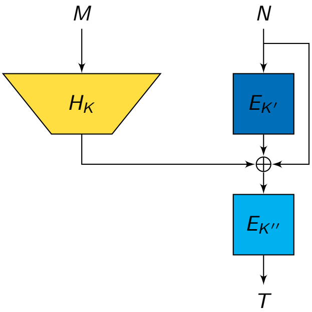
- what if we instantiate $F_{K'}$ with the Davies-Meyer construction $\mathrm{DM}[E]_{K'}(N) = E_{K'}(N) \oplus N$?
- wait! the DM construction is not a BBB-secure PRF: $\mathrm{DM}[E]_{K'}(N) \oplus N = E_{K'}(N)$ is a permutation!
- but here the outer encryption layer prevents this attack

Encrypted Wegman-Carter (EWC) + Davies-Meyer (DM)



- what if we instantiate $F_{K'}$ with the Davies-Meyer construction $\mathrm{DM}[E]_{K'}(N) = E_{K'}(N) \oplus N$?
- wait! the DM construction is not a BBB-secure PRF: $\mathrm{DM}[E]_{K'}(N) \oplus N = E_{K'}(N)$ is a permutation!
- but here the outer encryption layer prevents this attack

Encrypted Wegman-Carter (EWC) + Davies-Meyer (DM)



- what if we instantiate $F_{K'}$ with the Davies-Meyer construction $\mathrm{DM}[E]_{K'}(N) = E_{K'}(N) \oplus N$?
- wait! the DM construction is not a BBB-secure PRF: $\mathrm{DM}[E]_{K'}(N) \oplus N = E_{K'}(N)$ is a permutation!
- but here the outer encryption layer prevents this attack

Outline

Background on Wegman-Carter MACs

The EWCDM Construction

Security Result and Proof Sketch

Conclusion

Security Result for EWCDM

- n = block-length of the BC = tag-length
- L_{max} = maximal message-length (in n bit blocks)

Theorem (Nonce-respecting security of EWCDM)

$$\mathbf{Adv}^{\mathrm{MAC}}_{\mathrm{EWCDM}}(q_m, q_v) \le \frac{5q_m^{3/2}}{2^n} + \frac{\varepsilon q_m}{2} + \frac{6q_v}{2^n} + \varepsilon q_v.$$

(Security up to $q_m \simeq \min\{2^{2n/3}, \varepsilon^{-1}\}$ and $q_v \simeq \varepsilon^{-1} \simeq 2^n/L_{\max}$)

Theorem (Nonce-misusing security of EWCDM)

$$\mathbf{Adv}^{\mathrm{MAC}}_{\mathrm{EWCDM}}(q_m, q_v) \le \frac{2(q_m + q_v)^2}{2^n} + \frac{\varepsilon(q_m + q_v)^2}{2}.$$

(Security up to $q_m, q_v \simeq \varepsilon^{-1/2} \simeq 2^{n/2}/\sqrt{L_{\max}}$)

Security Result for EWCDM

- n = block-length of the BC = tag-length
- L_{max} = maximal message-length (in n bit blocks)

Theorem (Nonce-respecting security of EWCDM)

$$\mathbf{Adv}^{\mathrm{MAC}}_{\mathrm{EWCDM}}(q_m, q_v) \leq \frac{5q_m^{3/2}}{2^n} + \frac{\varepsilon q_m}{2} + \frac{6q_v}{2^n} + \varepsilon q_v.$$

(Security up to $q_m \simeq \min\{2^{2n/3}, \varepsilon^{-1}\}$ and $q_v \simeq \varepsilon^{-1} \simeq 2^n/L_{\max}$)

Theorem (Nonce-misusing security of EWCDM)

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

(Security up to $q_m, q_v \simeq \varepsilon^{-1/2} \simeq 2^{n/2}/\sqrt{L_{\max}}$)

Security Result for EWCDM

- n = block-length of the BC = tag-length
- L_{max} = maximal message-length (in n bit blocks)

Theorem (Nonce-respecting security of EWCDM)

$$\mathbf{Adv}^{\mathrm{MAC}}_{\mathsf{EWCDM}}(q_m, q_v) \leq \frac{5q_m^{3/2}}{2^n} + \frac{\varepsilon q_m}{2} + \frac{6q_v}{2^n} + \varepsilon q_v.$$

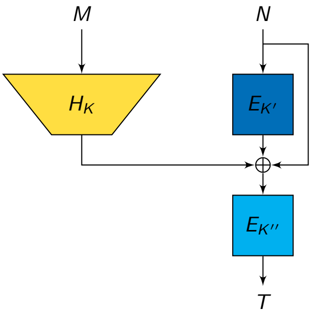
(Security up to $q_m \simeq \min\{2^{2n/3}, \varepsilon^{-1}\}$ and $q_v \simeq \varepsilon^{-1} \simeq 2^n/L_{\max}$)

Theorem (Nonce-misusing security of EWCDM)

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

(Security up to $q_m, q_v \simeq \varepsilon^{-1/2} \simeq 2^{n/2}/\sqrt{L_{\max}}$)

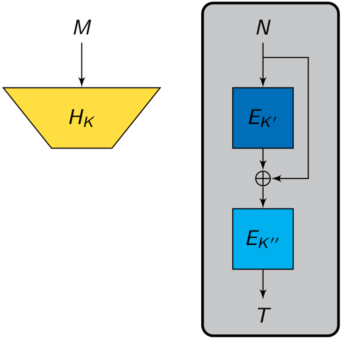
The Encrypted Davies-Meyer PRP-to-PRF Construction



- we can't start by replacing DM[$E_{K'}$] by a random function (⇒ birthday-bound)
- we need to consider directly the PRF-security of

$$N \mapsto E_{K''}(E_{K'}(N) \oplus N)$$

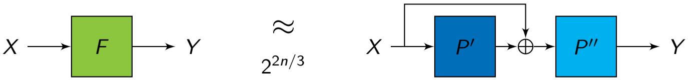
The Encrypted Davies-Meyer PRP-to-PRF Construction



- we can't start by replacing $\mathrm{DM}[E_{K'}]$ by a random function ($\Rightarrow$ birthday-bound)
- we need to consider directly the PRF-security of

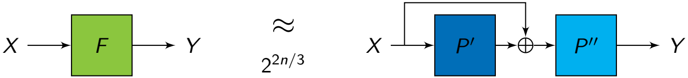
$$N \mapsto E_{K''}(E_{K'}(N) \oplus N)$$

The Encrypted Davies-Meyer PRP-to-PRF Construction



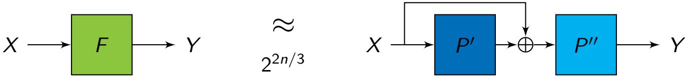
- crux of the proof = prove that $P''(P'(X) \oplus X)$ is a BBB-secure PRP-to-PRF construction
- H-coefficients technique [Pat08b, CS14] (good/bad transcripts)
- bad transcripts: too many collisions
- collisions slightly more likely for $P'(X) \oplus X$ than for $F(X)$
  $\Rightarrow$ lower bound the number of pairs (P', P'') that yield a given good transcript
- we prove security up to $2^{2n/3}$ queries (exact security $\sim 2^n$?)

The Encrypted Davies-Meyer PRP-to-PRF Construction



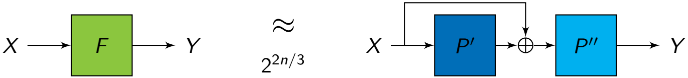
- crux of the proof = prove that $P''(P'(X) \oplus X)$ is a BBB-secure PRP-to-PRF construction
- H-coefficients technique [Pat08b, CS14] (good/bad transcripts)
- bad transcripts: too many collisions
- collisions slightly more likely for $P'(X) \oplus X$ than for $F(X)$ $\Rightarrow$ lower bound the number of pairs (P', P'') that yield a given good transcript
- we prove security up to $2^{2n/3}$ queries (exact security $\sim 2^n$?)

The Encrypted Davies-Meyer PRP-to-PRF Construction



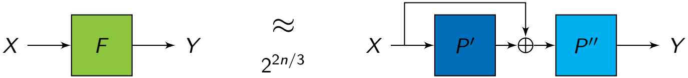
- crux of the proof = prove that $P''(P'(X) \oplus X)$ is a BBB-secure PRP-to-PRF construction
- H-coefficients technique [Pat08b, CS14] (good/bad transcripts)
- bad transcripts: too many collisions
- collisions slightly more likely for $P'(X) \oplus X$ than for $F(X)$
  $\Rightarrow$ lower bound the number of pairs (P', P'') that yield a given good transcript
- we prove security up to $2^{2n/3}$ queries (exact security $\sim 2^n$?)

The Encrypted Davies-Meyer PRP-to-PRF Construction



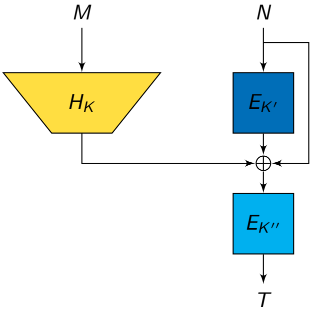
- crux of the proof = prove that $P''(P'(X) \oplus X)$ is a BBB-secure PRP-to-PRF construction
- H-coefficients technique [Pat08b, CS14] (good/bad transcripts)
- bad transcripts: too many collisions
- collisions slightly more likely for $P'(X) \oplus X$ than for $F(X)$
$\Rightarrow$ lower bound the number of pairs (P', P'') that yield a given good transcript
- we prove security up to $2^{2n/3}$ queries (exact security $\sim 2^n$?)

The Encrypted Davies-Meyer PRP-to-PRF Construction



- crux of the proof = prove that $P''(P'(X) \oplus X)$ is a BBB-secure PRP-to-PRF construction
- H-coefficients technique [Pat08b, CS14] (good/bad transcripts)
- bad transcripts: too many collisions
- collisions slightly more likely for $P'(X) \oplus X$ than for $F(X)$
  $\Rightarrow$ lower bound the number of pairs (P', P'') that yield a given good transcript
- we prove security up to $2^{2n/3}$ queries (exact security $\sim 2^n$?)

Handling Verification Queries

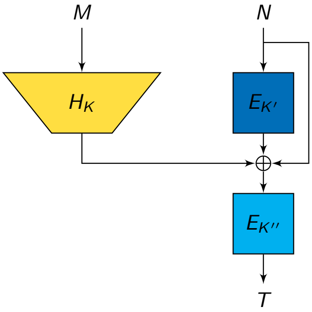


- $H_K(M)$ and the EDM construction are "intermingled"
- the full proof needs to handle verification queries "directly"
- we recast the forgery experiment as *distinguishing* between

$$(\mathrm{MAC}_K(\cdot,\cdot), \mathsf{Verif}_K(\cdot,\cdot,\cdot)) \text{ and } (\mathsf{Rand}(\cdot,\cdot), \mathsf{Reject}(\cdot,\cdot,\cdot))$$

- then we apply the H-coefficients technique [Pat08b, CS14]

Handling Verification Queries

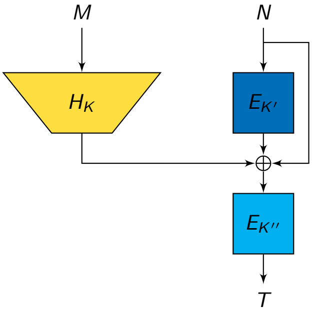


- $H_K(M)$ and the EDM construction are "intermingled"
- the full proof needs to handle verification queries "directly"
- we recast the forgery experiment as *distinguishing* between

$$(\mathrm{MAC}_K(\cdot,\cdot), \mathsf{Verif}_K(\cdot,\cdot,\cdot)) \text{ and } (\mathsf{Rand}(\cdot,\cdot), \mathsf{Reject}(\cdot,\cdot,\cdot))$$

- then we apply the H-coefficients technique [Pat08b, CS14]

Handling Verification Queries

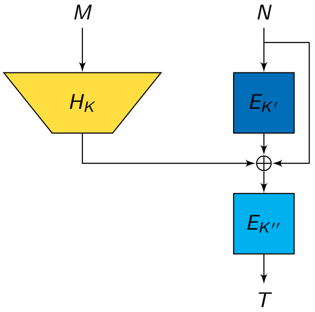


- $H_K(M)$ and the EDM construction are "intermingled"
- the full proof needs to handle verification queries "directly"
- we recast the forgery experiment as *distinguishing* between

$$(\mathrm{MAC}_K(\cdot,\cdot), \mathsf{Verif}_K(\cdot,\cdot,\cdot)) \text{ and } (\mathsf{Rand}(\cdot,\cdot), \mathsf{Reject}(\cdot,\cdot,\cdot))$$

- then we apply the H-coefficients technique [Pat08b, CS14]

Handling Verification Queries



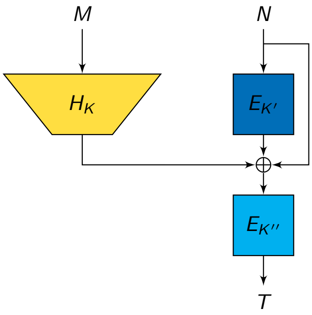
- $H_K(M)$ and the EDM construction are "intermingled"
- the full proof needs to handle verification queries "directly"
- we recast the forgery experiment as *distinguishing* between

$$(\mathrm{MAC}_K(\cdot,\cdot), \mathsf{Verif}_K(\cdot,\cdot,\cdot)) \text{ and } (\mathsf{Rand}(\cdot,\cdot), \mathsf{Reject}(\cdot,\cdot,\cdot))$$

- then we apply the H-coefficients technique [Pat08b, CS14]

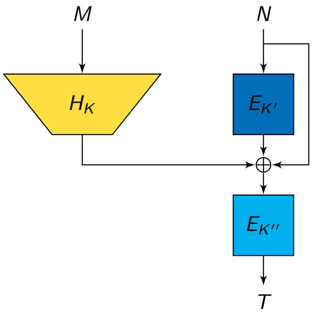
Outline

Final Remarks



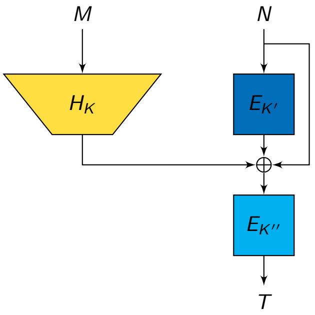
- the outer encryption layer is twice useful:
  1. provides birthday-bound nonce-misuse resistance
  2. provides nonce-respecting BBB-security when combined with the (cheap) feed-forward of the nonce
- easy to implement in a black-box way on top of an existing Wegman-Carter MAC implementation (GCM, Poly1305)

Final Remarks



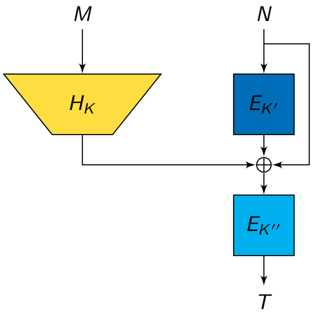
- the outer encryption layer is twice useful:
  1. provides birthday-bound nonce-misuse resistance
  2. provides nonce-respecting BBB-security when combined with the (cheap) feed-forward of the nonce
- easy to implement in a black-box way on top of an existing Wegman-Carter MAC implementation (GCM, Poly1305)

Final Remarks



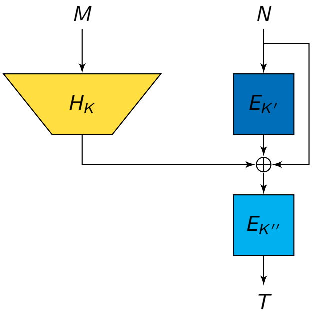
- the outer encryption layer is twice useful:
  1. provides birthday-bound nonce-misuse resistance
  2. provides nonce-respecting BBB-security when combined with the (cheap) feed-forward of the nonce
- easy to implement in a black-box way on top of an existing Wegman-Carter MAC implementation (GCM, Poly1305)

Final Remarks



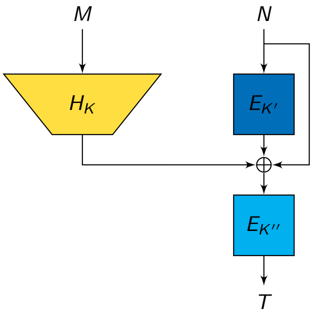
- the outer encryption layer is twice useful:
  1. provides birthday-bound nonce-misuse resistance
  2. provides nonce-respecting BBB-security when combined with the (cheap) feed-forward of the nonce
- easy to implement in a black-box way on top of an existing Wegman-Carter MAC implementation (GCM, Poly1305)

Open Problems



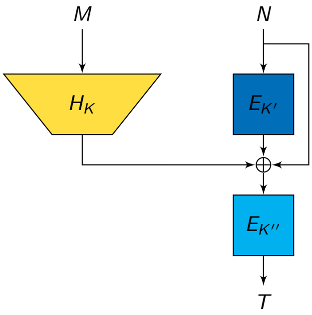
- security beyond $2^{2n/3}$ MAC queries? (no matching attack)
- same key for the two block cipher calls?
- effect of tag truncation?

Open Problems



- security beyond $2^{2n/3}$ MAC queries? (no matching attack)
- same key for the two block cipher calls?
- effect of tag truncation?

Open Problems



- security beyond $2^{2n/3}$ MAC queries? (no matching attack)
- same key for the two block cipher calls?
- effect of tag truncation?

The end...

Thanks for your attention!

Comments or 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.
- Mihir Bellare and Russell Impagliazzo. A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion. IACR Cryptology ePrint Archive, Report 1999/024, 1999. Available at `http://eprint.iacr.org/1999/024`.
- Mihir Bellare, Ted Krovetz, and Phillip Rogaway. Luby-Rackoff Backwards: Increasing Security by Making Block Ciphers Non-invertible. In Kaisa Nyberg, editor, *Advances in Cryptology - EUROCRYPT '98*, volume 1403 of *LNCS*, pages 266–280. Springer, 1998.
- Shan Chen and John Steinberger. Tight Security Bounds for Key-Alternating Ciphers. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 327–350. Springer, 2014. Full version available at `http://eprint.iacr.org/2013/222`.

References II

- 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.

- Chris Hall, David Wagner, John Kelsey, and Bruce Schneier. Building PRFs from PRPs. In Hugo Krawczyk, editor, *Advances in Cryptology - CRYPTO '98*, volume 1462 of *LNCS*, pages 370–389. Springer, 1998.

- 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 III

- Stefan Lucks. The Sum of PRPs Is a Secure PRF. In Bart Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 470–484. Springer, 2000.
- Jacques Patarin. A Proof of Security in $O(2^n)$ for the Xor of Two Random Permutations. In Reihaneh Safavi-Naini, editor, *Information Theoretic Security - ICITS 2008*, volume 5155 of *LNCS*, pages 232–248. Springer, 2008. Full version available at `http://eprint.iacr.org/2008/010`.
- Jacques Patarin. The "Coefficients H" Technique. In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *Selected Areas in Cryptography - SAC 2008*, volume 5381 of *LNCS*, pages 328–345. Springer, 2008.
- 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.

References IV

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.