Beyond-Birthday-Bound Secure MACs

Yannick Seurin

ANSSI, France

January 2018, Dagstuhl Seminar

Introduction

- we survey recent results on MAC constructions which are
  - based on a block cipher (BC) or a tweakable block cipher (TBC)
  - secure beyond the birthday bound (BBB-secure)
- most (T)BC-based MACs are secure only up to the birthday-bound w.r.t. to the block size n: they become insecure when $\sim 2^{n/2}$ (blocks of) messages have been treated
- BBB-security is important for lightweight crypto (small blocks, inconvenient re-keying,...)
- we highlight some open problems along the way

Introduction

- we survey recent results on MAC constructions which are
  - based on a block cipher (BC) or a tweakable block cipher (TBC)
  - secure beyond the birthday bound (BBB-secure)
- most (T)BC-based MACs are secure only up to the birthday-bound w.r.t. to the block size n: they become insecure when $\sim 2^{n/2}$ (blocks of) messages have been treated
- BBB-security is important for lightweight crypto (small blocks, inconvenient re-keying, ...)
- we highlight some open problems along the way

Introduction

- we survey recent results on MAC constructions which are
  - based on a block cipher (BC) or a tweakable block cipher (TBC)
  - secure beyond the birthday bound (BBB-secure)
- most (T)BC-based MACs are secure only up to the birthday-bound w.r.t. to the block size n: they become insecure when $\sim 2^{n/2}$ (blocks of) messages have been treated
- BBB-security is important for lightweight crypto (small blocks, inconvenient re-keying,...)
- we highlight some open problems along the way

Introduction

- we survey recent results on MAC constructions which are
  - based on a block cipher (BC) or a tweakable block cipher (TBC)
  - secure beyond the birthday bound (BBB-secure)
- most (T)BC-based MACs are secure only up to the birthday-bound w.r.t. to the block size n: they become insecure when $\sim 2^{n/2}$ (blocks of) messages have been treated
- BBB-security is important for lightweight crypto (small blocks, inconvenient re-keying,...)
- we highlight some open problems along the way

Introduction

- we survey recent results on MAC constructions which are
  - based on a block cipher (BC) or a tweakable block cipher (TBC)
  - secure beyond the birthday bound (BBB-secure)
- most (T)BC-based MACs are secure only up to the birthday-bound w.r.t. to the block size n: they become insecure when $\sim 2^{n/2}$ (blocks of) messages have been treated
- BBB-security is important for lightweight crypto (small blocks, inconvenient re-keying, . . .)
- we highlight some open problems along the way

Introduction

- we survey recent results on MAC constructions which are
  - based on a block cipher (BC) or a tweakable block cipher (TBC)
  - secure beyond the birthday bound (BBB-secure)
- most (T)BC-based MACs are secure only up to the birthday-bound w.r.t. to the block size n: they become insecure when $\sim 2^{n/2}$ (blocks of) messages have been treated
- BBB-security is important for lightweight crypto (small blocks, inconvenient re-keying, . . .)
- we highlight some open problems along the way

Outline

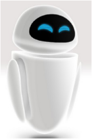
Outline

Generalities

Stateless Deterministic MACs
- The UHF-then-PRF Paradigm
- Constructing BBB-Secure Output Functions from (T)BCs
- Constructing BBB-Secure UHFs from (T)BCs

Nonce-Based MACs
- State of Art
- Open Problems

MAC Definition



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

$\mathrm{MAC}_K(N', M') = T'$?

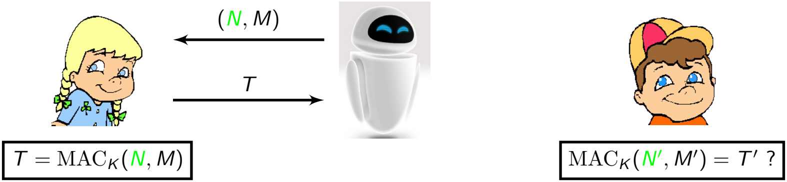
Security Definition

The adversary is allowed

- q MAC queries $T = \mathrm{MAC}_K(N, M)$
- 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'.

MAC Definition



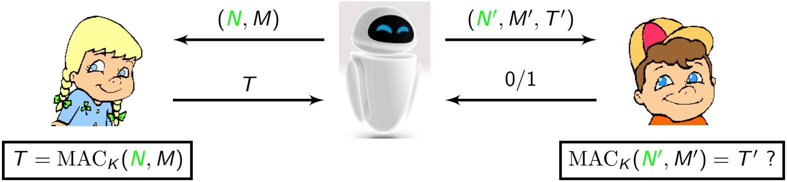
Security Definition

The adversary is allowed

- q MAC queries $T = \mathrm{MAC}_K(N, M)$
- 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'.

MAC Definition



Security Definition

The adversary is allowed

- q MAC queries $T = \mathrm{MAC}_K(N, M)$
- 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'.

Three types of MAC

- stateless and deterministic: MAC function only takes the key and the message as input
  (Variable-input-length PRF $\Rightarrow$ stateless deterministic MAC)
- nonce-based:
  - MAC function takes as input a non-repeating nonce N in addition to the key and the message M
  - sec. model: the nonce is chosen by the adversary
  - the adversary is said nonce-respecting if it does not repeat nonces in MAC queries and nonce-misusing otherwise
- randomized: MAC function takes as input random coins R (generated by the sender) in addition to the key and the message

Three types of MAC

- stateless and deterministic: MAC function only takes the key and the message as input
  (Variable-input-length PRF $\Rightarrow$ stateless deterministic MAC)
- nonce-based:
  - MAC function takes as input a non-repeating nonce N in addition to the key and the message M
  - sec. model: the nonce is chosen by the adversary
  - the adversary is said nonce-respecting if it does not repeat nonces in MAC queries and nonce-misusing otherwise
- randomized: MAC function takes as input random coins R (generated by the sender) in addition to the key and the message

Three types of MAC

- stateless and deterministic: MAC function only takes the key and the message as input
  (Variable-input-length PRF $\Rightarrow$ stateless deterministic MAC)
- nonce-based:
  - MAC function takes as input a non-repeating nonce N in addition to the key and the message M
  - sec. model: the nonce is chosen by the adversary
  - the adversary is said nonce-respecting if it does not repeat nonces in MAC queries and nonce-misusing otherwise
- randomized: MAC function takes as input random coins R (generated by the sender) in addition to the key and the message

Graceful Nonce-Misuse Security Degradation

- the security of some nonce-based MACs collapses if a single nonce is repeated (e.g. GMAC)
- ideally, security should degrade gracefully in case nonces are repeated
- any BBB-secure nonce-based MAC with graceful security degradation can be turned into a BBB-secure randomized MAC by choosing n-bit nonces uniformly at random:

$$\mathbf{Adv}_F^{\text{rand-MAC}}(q,v) \le \underbrace{\frac{q^{\mu+1}}{2^{\mu(n+1)}}}_{\substack{\mu\text{-multicoll.}\\ \text{proba.}}} + \mathbf{Adv}_F^{\text{nonce-MAC}}(q,v,\mu)$$

where μ is the maximal number of nonce repetitions.

Graceful Nonce-Misuse Security Degradation

- the security of some nonce-based MACs collapses if a single nonce is repeated (e.g. GMAC)
- ideally, security should degrade gracefully in case nonces are repeated
- any BBB-secure nonce-based MAC with graceful security degradation can be turned into a BBB-secure randomized MAC by choosing n-bit nonces uniformly at random:

$$\mathbf{Adv}_F^{\text{rand-MAC}}(q,v) \leq \underbrace{\frac{q^{\mu+1}}{2^{\mu(n+1)}}}_{\substack{\mu\text{-multicoll.}\\ \text{proba.}}} + \mathbf{Adv}_F^{\text{nonce-MAC}}(q,v,\mu)$$

where μ is the maximal number of nonce repetitions.

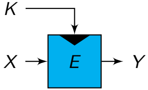
Graceful Nonce-Misuse Security Degradation

- the security of some nonce-based MACs collapses if a single nonce is repeated (e.g. GMAC)
- ideally, security should degrade gracefully in case nonces are repeated
- any BBB-secure nonce-based MAC with graceful security degradation can be turned into a BBB-secure randomized MAC by choosing n-bit nonces uniformly at random:

$$\mathbf{Adv}_F^{\text{rand-MAC}}(q, v) \leq \underbrace{\frac{q^{\mu+1}}{2^{\mu(n+1)}}}_{\substack{\mu\text{-multicoll.}\\ \text{proba.}}} + \mathbf{Adv}_F^{\text{nonce-MAC}}(q, v, \mu)$$

where μ is the maximal number of nonce repetitions.

Building Blocks: BCs and TBCs



n = block size
t = tweak size

- block cipher E: for each key K, $X \mapsto E(K, X)$ is a permutation
- tweakable block cipher $\widetilde{E}$: for each key K and each tweak W, $X \mapsto \widetilde{E}(K, W, X)$ is a permutation
- one can think of a keyed TBC $\widetilde{E}_K$ as an "imperfect" $(n+t)$-to-n-bit PRF
- if any tweak W is used at most "a few" times, $\widetilde{E}_K$ is close to a random $(n+t)$-to-n-bit function

Building Blocks: BCs and TBCs

n = block size
t = tweak size

- block cipher E: for each key K, $X \mapsto E(K, X)$ is a permutation
- tweakable block cipher $\widetilde{E}$: for each key K and each tweak W, $X \mapsto \widetilde{E}(K, W, X)$ is a permutation
- one can think of a keyed TBC $\widetilde{E}_K$ as an "imperfect" $(n + t)$-to-n-bit PRF
- if any tweak W is used at most "a few" times, $\widetilde{E}_K$ is close to a random $(n + t)$-to-n-bit function

Building Blocks: BCs and TBCs

n = block size

t = tweak size

- block cipher E: for each key K, $X \mapsto E(K, X)$ is a permutation
- tweakable block cipher $\widetilde{E}$: for each key K and each tweak W, $X \mapsto \widetilde{E}(K, W, X)$ is a permutation
- one can think of a keyed TBC $\widetilde{E}_K$ as an "imperfect" $(n + t)$-to-n-bit PRF
- if any tweak W is used at most "a few" times, $\widetilde{E}_K$ is close to a random $(n + t)$-to-n-bit function

Building Blocks: BCs and TBCs

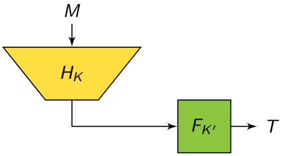
n = block size
t = tweak size

- block cipher E: for each key K, $X \mapsto E(K, X)$ is a permutation
- tweakable block cipher $\widetilde{E}$: for each key K and each tweak W, $X \mapsto \widetilde{E}(K, W, X)$ is a permutation
- one can think of a keyed TBC $\widetilde{E}_K$ as an "imperfect" $(n + t)$-to-n-bit PRF
- if any tweak W is used at most "a few" times, $\widetilde{E}_K$ is close to a random $(n + t)$-to-n-bit function

Outline

Outline

The UHF-then-PRF Construction

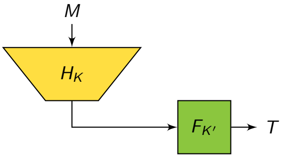


- based on a fixed-input-length PRF F and an ε-almost universal (ε-AU) hash function H:

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

- H can be statistically secure (polynomial evaluation) or computationally secure (BC/TBC-based)
- most MACs are (variants of) this construction (UMAC, EMAC, OMAC, CMAC, PMAC, NMAC)

The UHF-then-PRF Construction

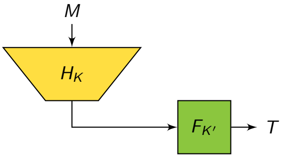


- based on a fixed-input-length PRF F and an ε-almost universal (ε-AU) hash function H:

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

- H can be statistically secure (polynomial evaluation) or computationally secure (BC/TBC-based)
- most MACs are (variants of) this construction (UMAC, EMAC, OMAC, CMAC, PMAC, NMAC)

The UHF-then-PRF Construction

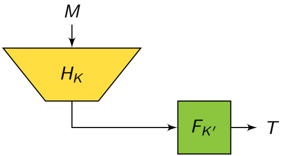


- based on a fixed-input-length PRF F and an ε-almost universal (ε-AU) hash function H:

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

- H can be statistically secure (polynomial evaluation) or computationally secure (BC/TBC-based)
- most MACs are (variants of) this construction (UMAC, EMAC, OMAC, CMAC, PMAC, NMAC)

Security of UHF-then-PRF



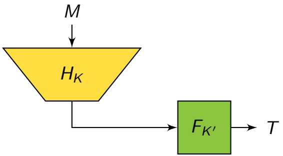
- birthday-bound-secure w.r.t. H collision probability ε

$$\mathbf{Adv}^{\mathrm{PRF}}_{F \circ H}(q) \leq \frac{q^2 \varepsilon}{2} + \mathbf{Adv}^{\mathrm{PRF}}_{F}(q)$$

- typical instantiation from a block cipher E:
  - $H \leftarrow \mathrm{CBC}[E]$ or $\mathrm{PMAC}[E]$ ($\varepsilon \simeq 2^{-n}$)
  - $F \leftarrow E$

$\Rightarrow$ BB-security

Security of UHF-then-PRF



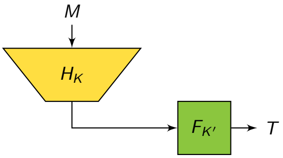
- birthday-bound-secure w.r.t. H collision probability ε

$$\mathbf{Adv}_{F\circ H}^{\mathrm{PRF}}(q) \leq \frac{q^2\varepsilon}{2} + \mathbf{Adv}_{F}^{\mathrm{PRF}}(q)$$

- typical instantiation from a block cipher E:
  - $H \leftarrow \mathrm{CBC}[E]$ or $\mathrm{PMAC}[E]$ ($\varepsilon \simeq 2^{-n}$)
  - $F \leftarrow E$

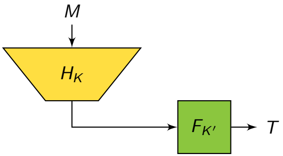
$\Rightarrow$ BB-security

BBB-Security of UHF-then-PRF



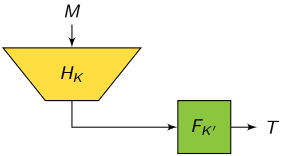
- for BBB-security, we need a $2n$-bit output UHF with $\varepsilon \simeq 2^{-2n}$ and a BBB-secure $2n$-to-n-bit PRF
- constructing a BBB-secure $2n$-to-n-bit PRF from an n-bit block cipher seems inconvenient
(e.g. XOR2 construction [Luc00, Pat08, DHT17] + 5-round Feistel [Pat04])
- however, PRF-security seems like an overkill (the adversary does not control F inputs)

BBB-Security of UHF-then-PRF



- for BBB-security, we need a $2n$-bit output UHF with $\varepsilon \simeq 2^{-2n}$ and a BBB-secure $2n$-to-n-bit PRF
- constructing a BBB-secure $2n$-to-n-bit PRF from an n-bit block cipher seems inconvenient
(e.g. XOR2 construction [Luc00, Pat08, DHT17] + 5-round Feistel [Pat04])
- however, PRF-security seems like an overkill (the adversary does not control F inputs)

BBB-Security of UHF-then-PRF



- for BBB-security, we need a $2n$-bit output UHF with $\varepsilon \simeq 2^{-2n}$ and a BBB-secure $2n$-to-n-bit PRF
- constructing a BBB-secure $2n$-to-n-bit PRF from an n-bit block cipher seems inconvenient
  (e.g. XOR2 construction [Luc00, Pat08, DHT17] + 5-round Feistel [Pat04])
- however, PRF-security seems like an overkill (the adversary does not control F inputs)

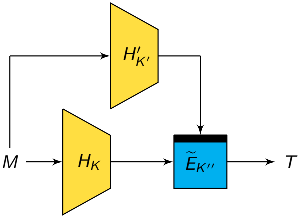
Outline

Generalities

Stateless Deterministic MACs
- The UHF-then-PRF Paradigm
- Constructing BBB-Secure Output Functions from (T)BCs
- Constructing BBB-Secure UHFs from (T)BCs

Nonce-Based MACs
- State of Art
- Open Problems

TBC-Based Constructions [CLS17, LN17]

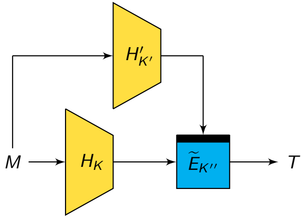


Hash as Tweak (HaT) [CLS17]

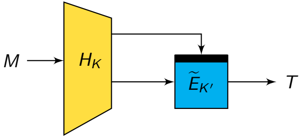
Hash-then-TBC [LN17]

- HaT construction BBB-secure assuming H and H' are ε-AU secure
- Hash-then-TBC construction BBB-secure under more complex UHF-type properties of H

TBC-Based Constructions [CLS17, LN17]



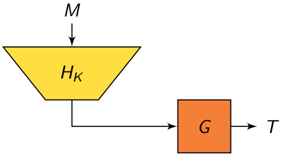
Hash as Tweak (HaT) [CLS17]



Hash-then-TBC [LN17]

- HaT construction BBB-secure assuming H and H' are ε-AU secure
- Hash-then-TBC construction BBB-secure under more complex UHF-type properties of H

The UHF-then-RO Construction [CLS17]

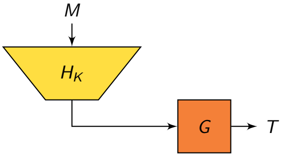


- the output function need not be keyed
- modeling G as a RO, the construction is secure if H is ε-AU and ε'-uniform:

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

- security proof under a standard assumption on G?

The UHF-then-RO Construction [CLS17]

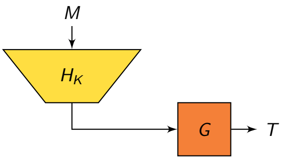


- the output function need not be keyed
- modeling G as a RO, the construction is secure if H is ε-AU and ε'-uniform:

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

- security proof under a standard assumption on G?

The UHF-then-RO Construction [CLS17]

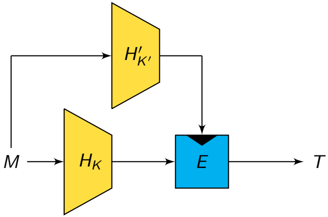


- the output function need not be keyed
- modeling G as a RO, the construction is secure if H is ε-AU and ε'-uniform:

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

- security proof under a standard assumption on G?

BBB-Secure Instantiation from an Ideal BC [CLS17]

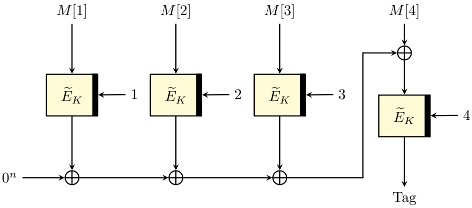


Hash as Key (HaK)

- the HaK construction is BBB-secure in the ideal cipher model assuming H and H' are ε-AU and ε'-uniform

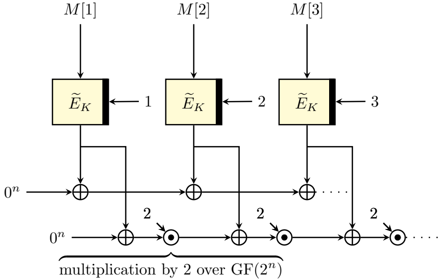
Outline

PMAC/PMAC1 [BR02, Rog04]



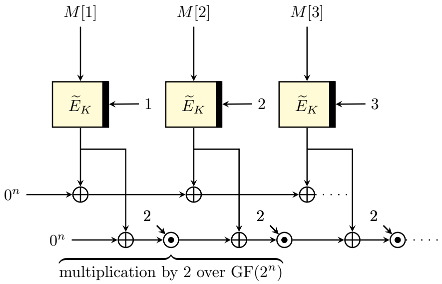
- most existing constructions are variants of PMAC [BR02] (BC-based) and PMAC1 [Rog04] (TBC-based)
- the underlying hash function (omitting final $\widetilde{E}$ call) is ε-AU for $\varepsilon \simeq 2^{-n}$

PMAC_TBC [Nai15]



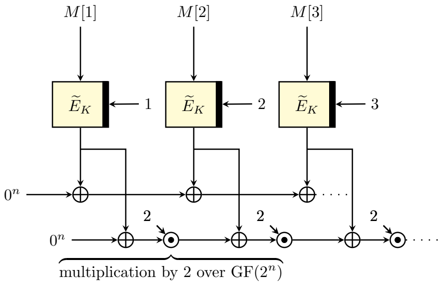
- PMAC_TBC = TBC-based variant of PMAC_Plus [Yas11]
- combined with an output function weaker than a $2n$-bit PRF
- achieves n-bit security
- but each TBC call processes only n bits of message

PMAC_TBC [Nai15]



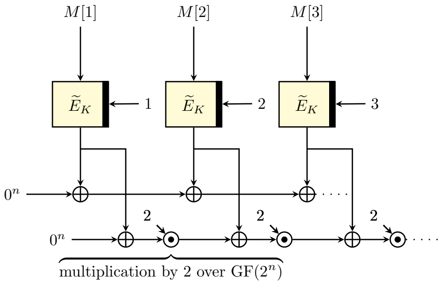
- PMAC_TBC = TBC-based variant of PMAC_Plus [Yas11]
- combined with an output function weaker than a $2n$-bit PRF
- achieves n-bit security
- but each TBC call processes only n bits of message

PMAC_TBC [Nai15]



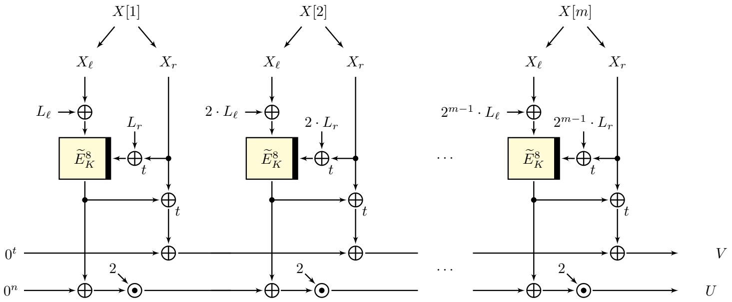
- PMAC_TBC = TBC-based variant of PMAC_Plus [Yas11]
- combined with an output function weaker than a $2n$-bit PRF
- achieves n-bit security
- but each TBC call processes only n bits of message

PMAC_TBC [Nai15]



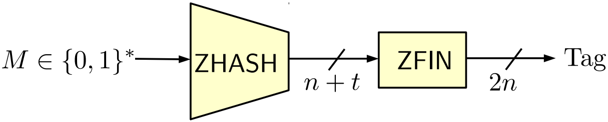
- PMAC_TBC = TBC-based variant of PMAC_Plus [Yas11]
- combined with an output function weaker than a $2n$-bit PRF
- achieves n-bit security
- but each TBC call processes only n bits of message

ZHASH [IMPS17]



- each TBC call processes $(n + t)$ bits of message
- uses a variant of the XTX construction [MI15] to extend the tweak space and incorporate the block counter
- ZHASH is ε-AU for $\varepsilon = 4/2^{n+\min\{n,t\}}$

ZMAC [IMPS17] and ZMAC+ [LN17]



- ZMAC [IMPS17] combines ZHASH and an $(n + t)$-to-n-bit PRF constructed from the TBC using the UHF-then-PRF paradigm
- ZMAC+ [LN17] improves the efficiency of the output function using the Hash-then-TBC construction

Open Problems

- alternative to UHF-then-PRF:
  - finalization function in PMAC_Plus: $(U, V) \mapsto E_{K_1}(U) \oplus E_{K_2}(V)$ $\Rightarrow$ not a PRF
  - find a generic composition theorem capturing the security proofs of PMAC_Plus and PMAC_TBC
- exact security of PMAC_Plus?
- efficient BC-based constructions with n-bit security? (F_t construction [IM16] and LightMAC_Plus2 [Nai17] achieve $kn/(k+1)$-bit security with a kn bit state)

Open Problems

- alternative to UHF-then-PRF:
  - finalization function in PMAC_Plus: $(U, V) \mapsto E_{K_1}(U) \oplus E_{K_2}(V)$ $\Rightarrow$ not a PRF
  - find a generic composition theorem capturing the security proofs of PMAC_Plus and PMAC_TBC
- exact security of PMAC_Plus?
- efficient BC-based constructions with n-bit security? (F_t construction [IM16] and LightMAC_Plus2 [Nai17] achieve $kn/(k+1)$-bit security with a kn bit state)

Open Problems

- alternative to UHF-then-PRF:
  - finalization function in PMAC_Plus: $(U, V) \mapsto E_{K_1}(U) \oplus E_{K_2}(V)$ $\Rightarrow$ not a PRF
  - find a generic composition theorem capturing the security proofs of PMAC_Plus and PMAC_TBC
- exact security of PMAC_Plus?
- efficient BC-based constructions with n-bit security? (F_t construction [IM16] and LightMAC_Plus2 [Nai17] achieve $kn/(k+1)$-bit security with a kn bit state)

Outline

Generalities

Stateless Deterministic MACs

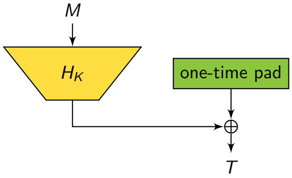
- The UHF-then-PRF Paradigm
- Constructing BBB-Secure Output Functions from (T)BCs
- Constructing BBB-Secure UHFs from (T)BCs

Nonce-Based MACs

- State of Art
- Open Problems

Outline

The Wegman-Carter Construction [GMS74, WC81]



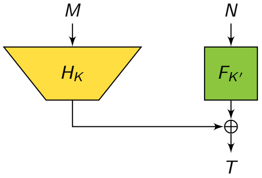
- based on an ε-almost xor-universal (ε-AXU) hash function H:

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

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

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

The Wegman-Carter Construction [GMS74, WC81]



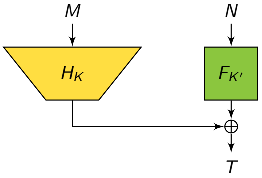
- based on an ε-almost xor-universal (ε-AXU) hash function H:

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

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

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

The Wegman-Carter Construction [GMS74, WC81]



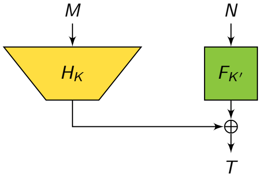
- based on an ε-almost xor-universal (ε-AXU) hash function H:

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

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

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

The Wegman-Carter Construction [GMS74, WC81]



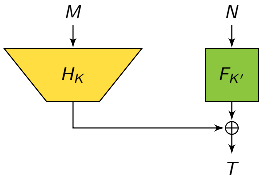
- based on an ε-almost xor-universal (ε-AXU) hash function H:

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

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

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

Implementing the PRF from a Block Cipher

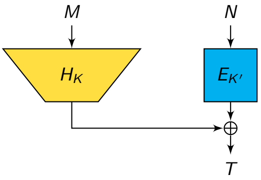


- in practice, F is replaced by a block cipher
  $\rightarrow$ Wegman-Carter-Shoup (WCS) construction
- provable security drops to birthday bound ☹ [Sho96]

$$\mathbf{Adv}^{\mathrm{MAC}}_{\mathrm{WCS}}(q, v) \leq v\varepsilon + \frac{(q+v)^2}{2 \cdot 2^n} + \mathbf{Adv}^{\mathrm{PRP}}_{E}(q+v)$$

- a better bound exists [Ber05] but still "birthday-type"
- easy solution: PRP-to-PRF conversion (e.g. xor of PRPs)

Implementing the PRF from a Block Cipher

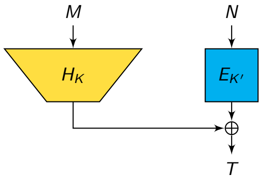


- in practice, F is replaced by a block cipher
  $\rightarrow$ Wegman-Carter-Shoup (WCS) construction
- provable security drops to birthday bound ☹ [Sho96]

$$\mathbf{Adv}^{\mathrm{MAC}}_{\mathsf{WCS}}(q,v) \leq v\varepsilon + \frac{(q+v)^2}{2 \cdot 2^n} + \mathbf{Adv}^{\mathrm{PRP}}_{E}(q+v)$$

- a better bound exists [Ber05] but still "birthday-type"
- easy solution: PRP-to-PRF conversion (e.g. xor of PRPs)

Implementing the PRF from a Block Cipher

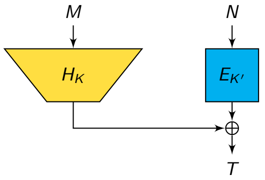


- in practice, F is replaced by a block cipher
  $\rightarrow$ Wegman-Carter-Shoup (WCS) construction
- provable security drops to birthday bound ☹ [Sho96]

$$\mathbf{Adv}^{\mathrm{MAC}}_{\mathsf{WCS}}(q,v) \leq v\varepsilon + \frac{(q+v)^2}{2 \cdot 2^n} + \mathbf{Adv}^{\mathrm{PRP}}_{E}(q+v)$$

- a better bound exists [Ber05] but still "birthday-type"
- easy solution: PRP-to-PRF conversion (e.g. xor of PRPs)

Implementing the PRF from a Block Cipher

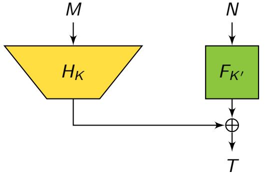


- in practice, F is replaced by a block cipher
  $\rightarrow$ Wegman-Carter-Shoup (WCS) construction
- provable security drops to birthday bound ☹ [Sho96]

$$\mathbf{Adv}^{\mathrm{MAC}}_{\mathsf{WCS}}(q,v) \leq v\varepsilon + \frac{(q+v)^2}{2\cdot 2^n} + \mathbf{Adv}^{\mathrm{PRP}}_{E}(q+v)$$

- a better bound exists [Ber05] but still “birthday-type”
- easy solution: PRP-to-PRF conversion (e.g. xor of PRPs)

The Nonce-Misuse Problem

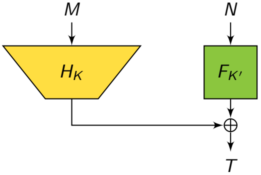


- Wegman-Carter MACs are brittle: a single nonce repetition can completely break security [Jou06, HP08]
- esp. for polynomial-based hashing, i.e., $H_K(M) = P_M(K)$:

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

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

The Nonce-Misuse Problem

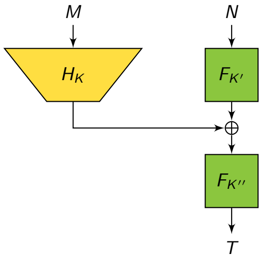


- Wegman-Carter MACs are brittle: a single nonce repetition can completely break security [Jou06, HP08]
- esp. for polynomial-based hashing, i.e., $H_K(M) = P_M(K)$:

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

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

The Nonce-Misuse Problem

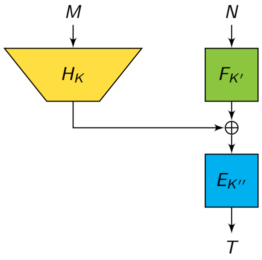


- Wegman-Carter MACs are brittle: a single nonce repetition can completely break security [Jou06, HP08]
- esp. for polynomial-based hashing, i.e., $H_K(M) = P_M(K)$:

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

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

The Nonce-Misuse Problem

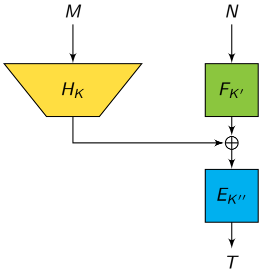


- Wegman-Carter MACs are brittle: a single nonce repetition can completely break security [Jou06, HP08]
- esp. for polynomial-based hashing, i.e., $H_K(M) = P_M(K)$:

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

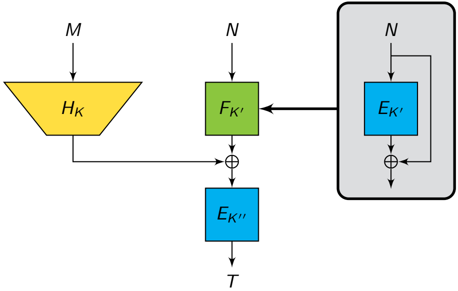
- solution: extra PRF call (in fact, OK to use a PRP here)
- Encrypted Wegman-Carter (EWC)

EWCDM: BBB-security + Nonce-Misuse Resistance [CS16]



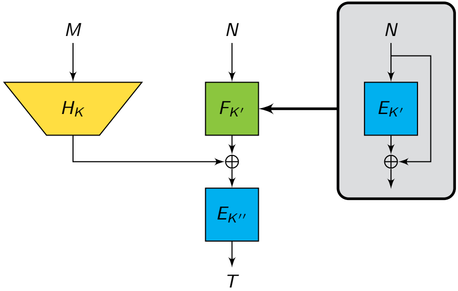
- what if we instantiate $F_{K'}$ with the Davies-Meyer construction $\mathrm{DM}[E]_{K'}(N) = E_{K'}(N) \oplus N$?
- the DM construction is not a BBB-secure PRF: $\mathrm{DM}[E]_{K'}(N) \oplus N = E_{K'}(N)$ is a permutation!
- but here the outer encryption layer prevents this attack
- Encrypted Wegman-Carter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

EWCDM: BBB-security + Nonce-Misuse Resistance [CS16]



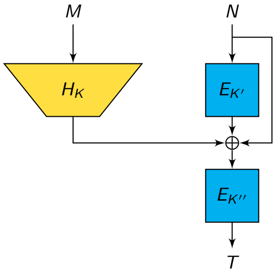
- what if we instantiate $F_{K'}$ with the Davies-Meyer construction $\mathrm{DM}[E]_{K'}(N) = E_{K'}(N) \oplus N$?
- the DM construction is not a BBB-secure PRF: $\mathrm{DM}[E]_{K'}(N) \oplus N = E_{K'}(N)$ is a permutation!
- but here the outer encryption layer prevents this attack
- Encrypted Wegman-Carter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

EWCDM: BBB-security + Nonce-Misuse Resistance [CS16]



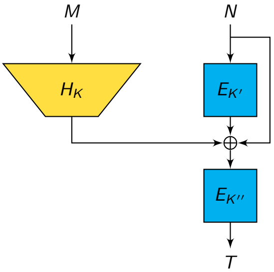
- what if we instantiate $F_{K'}$ with the Davies-Meyer construction $\mathrm{DM}[E]_{K'}(N) = E_{K'}(N) \oplus N$?
- the DM construction is not a BBB-secure PRF: $\mathrm{DM}[E]_{K'}(N) \oplus N = E_{K'}(N)$ is a permutation!
- but here the outer encryption layer prevents this attack
- Encrypted Wegman-Carter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

EWCDM: BBB-security + Nonce-Misuse Resistance [CS16]



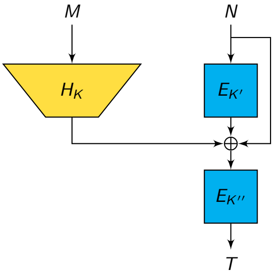
- what if we instantiate $F_{K'}$ with the Davies-Meyer construction $\mathrm{DM}[E]_{K'}(N) = E_{K'}(N) \oplus N$?
- the DM construction is not a BBB-secure PRF: $\mathrm{DM}[E]_{K'}(N) \oplus N = E_{K'}(N)$ is a permutation!
- but here the outer encryption layer prevents this attack
- Encrypted Wegman-Carter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

EWCDM: BBB-security + Nonce-Misuse Resistance [CS16]



- what if we instantiate $F_{K'}$ with the Davies-Meyer construction $\mathrm{DM}[E]_{K'}(N) = E_{K'}(N) \oplus N$?
- 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 with Davies-Meyer (EWCDM)

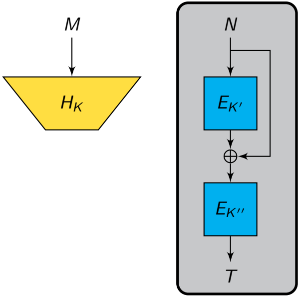
The Encrypted Davies-Meyer PRP-to-PRF Construction



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

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

Security Results for EDM and EWCDM

EDM is a secure PRF up to:

- $2^{2n/3}$ queries (H-coefficients) [CS16]
- $2^{3n/4}$ queries (Chi-squared method) [DHT17]
- $2^n/n$ queries (Mirror Theory) [MN17]

EWCDM is a secure MAC up to

- $2^{2n/3}$ MAC and 2^n verif. queries (H-coefficients) [CS16]
- $2^n/n$ MAC and verif. queries (Mirror Theory) [MN17]

Security Results for EDM and EWCDM

EDM is a secure PRF up to:

- $2^{2n/3}$ queries (H-coefficients) [CS16]
- $2^{3n/4}$ queries (Chi-squared method) [DHT17]
- $2^n/n$ queries (Mirror Theory) [MN17]

EWCDM is a secure MAC up to

- $2^{2n/3}$ MAC and 2^n verif. queries (H-coefficients) [CS16]
- $2^n/n$ MAC and verif. queries (Mirror Theory) [MN17]

Security Results for EDM and EWCDM

EDM is a secure PRF up to:

- $2^{2n/3}$ queries (H-coefficients) [CS16]
- $2^{3n/4}$ queries (Chi-squared method) [DHT17]
- $2^n/n$ queries (Mirror Theory) [MN17]

EWCDM is a secure MAC up to

- $2^{2n/3}$ MAC and 2^n verif. queries (H-coefficients) [CS16]
- $2^n/n$ MAC and verif. queries (Mirror Theory) [MN17]

Security Results for EDM and EWCDM

EDM is a secure PRF up to:

- $2^{2n/3}$ queries (H-coefficients) [CS16]
- $2^{3n/4}$ queries (Chi-squared method) [DHT17]
- $2^n/n$ queries (Mirror Theory) [MN17]

EWCDM is a secure MAC up to

- $2^{2n/3}$ MAC and 2^n verif. queries (H-coefficients) [CS16]
- $2^n/n$ MAC and verif. queries (Mirror Theory) [MN17]

Security Results for EDM and EWCDM

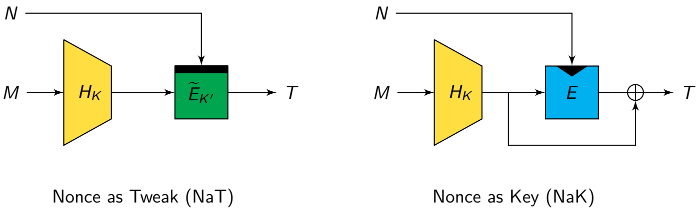
EDM is a secure PRF up to:

- $2^{2n/3}$ queries (H-coefficients) [CS16]
- $2^{3n/4}$ queries (Chi-squared method) [DHT17]
- $2^n/n$ queries (Mirror Theory) [MN17]

EWCDM is a secure MAC up to

- $2^{2n/3}$ MAC and 2^n verif. queries (H-coefficients) [CS16]
- $2^n/n$ MAC and verif. queries (Mirror Theory) [MN17]

TBC and IC-Based Finalization [CLS17]

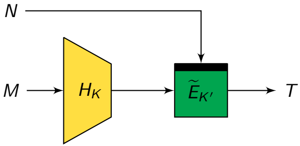


- both constructions enjoy graceful security degradation with maximal nonce multiplicity μ

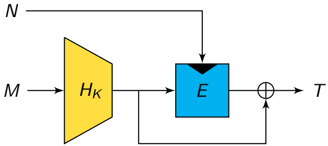
$$\mathbf{Adv}^{\text{nonce-MAC}}_{\text{NaT/NaK}}(q, v) \leq \mu q \varepsilon + (\dots)$$

- NaK construction provably secure in the ideal cipher model, assuming H is ε-AXU and uniform (Davies-Meyer mode required to make the output function non-invertible!)

TBC and IC-Based Finalization [CLS17]



Nonce as Tweak (NaT)



Nonce as Key (NaK)

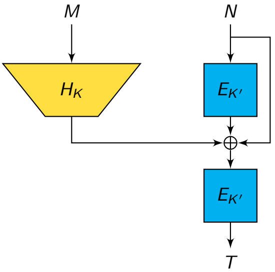
- both constructions enjoy graceful security degradation with maximal nonce multiplicity μ

$$\mathbf{Adv}^{\text{nonce-MAC}}_{\text{NaT/NaK}}(q, v) \leq \mu q \varepsilon + (\ldots)$$

- NaK construction provably secure in the ideal cipher model, assuming H is ε-AXU and uniform (Davies-Meyer mode required to make the output function non-invertible!)

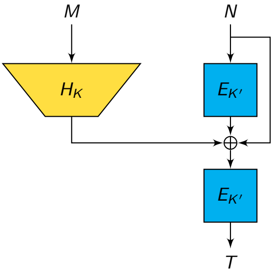
Outline

Optimizing and Instantiating EWCDM



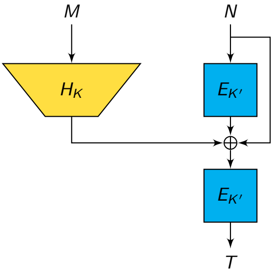
- can we use the same key for the two BC calls?
- preliminary result: single-key EDM is a secure PRF up to $2^{2n/3}$ queries [CS18]
- can we instantiate H_K with e.g. CBC[E_K] or PMAC[E_K]? (same key for hashing and finalization)

Optimizing and Instantiating EWCDM



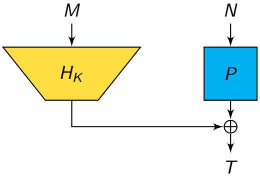
- can we use the same key for the two BC calls?
- preliminary result: single-key EDM is a secure PRF up to $2^{2n/3}$ queries [CS18]
- can we instantiate H_K with e.g. CBC[E_K] or PMAC[E_K]? (same key for hashing and finalization)

Optimizing and Instantiating EWCDM



- can we use the same key for the two BC calls?
- preliminary result: single-key EDM is a secure PRF up to $2^{2n/3}$ queries [CS18]
- can we instantiate H_K with e.g. CBC[E_K] or PMAC[E_K]? (same key for hashing and finalization)

Back to the Wegman-Carter-Shoup Construction

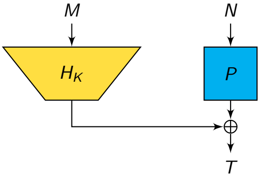


- consider a forgery attempt (N', M', T') after q MAC queries:
  - if N' is fresh, forgery valid with proba. at most $1/(2^n - q)$
  - if N' appeared in a MAC queries $(N', M) \rightarrow T$, forgery valid if

$$H_K(M) \oplus H_K(M') = T \oplus T'$$

- problem: K is not uniformly random after second MAC query
  $\Rightarrow$ cannot use UHF property of H

Back to the Wegman-Carter-Shoup Construction

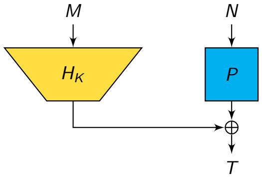


- consider a forgery attempt (N', M', T') after q MAC queries:
  - if N' is fresh, forgery valid with proba. at most $1/(2^n - q)$
  - if N' appeared in a MAC queries $(N', M) \rightarrow T$, forgery valid if

$$H_K(M) \oplus H_K(M') = T \oplus T'$$

- problem: K is not uniformly random after second MAC query
  $\Rightarrow$ cannot use UHF property of H

Back to the Wegman-Carter-Shoup Construction

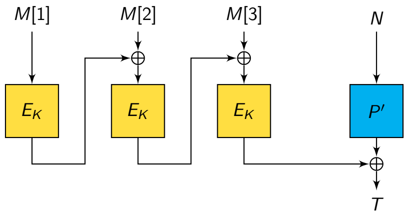


- security bound (one forgery attempt):

$$\mathbf{Adv}_{\mathrm{WC}}^{\mathrm{MAC}}(q,1) \leq v\varepsilon + \frac{(q+1)^2}{2 \cdot 2^n}$$

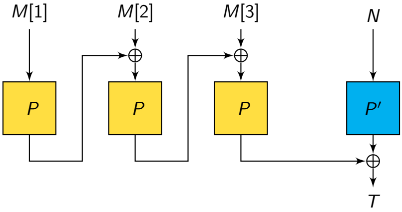
- matching attack when $H_K(M) = K \cdot M$:
  - make $q \sim 2^{n/2}$ MAC queries $(N_i, M_i) \to T_i$
  - for each pair (i,j), $K \cdot (M_i \oplus M_j) \neq T_i \oplus T_j$
  - $\Rightarrow$ discard $\sim 2^n$ bad keys
- security bound is tight (number of queries)

WCS with a Computational BC-based UHF



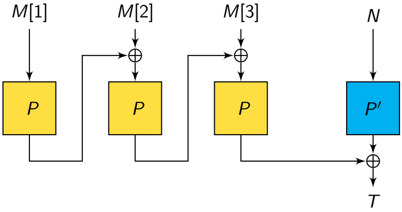
- instantiate H_K with e.g. CBC$[E_K]$
- replace E_K by a random permutation P (PRP term)
  $\Rightarrow$ previous information-theoretic attack does not work anymore
- very similar to CCM authentication
  $\rightarrow$ conjectured BBB-secure by Jonsson [Jon02]

WCS with a Computational BC-based UHF



- instantiate H_K with e.g. CBC$[E_K]$
- replace E_K by a random permutation P (PRP term)
  $\Rightarrow$ previous information-theoretic attack does not work anymore
- very similar to CCM authentication
  $\rightarrow$ conjectured BBB-secure by Jonsson [Jon02]

WCS with a Computational BC-based UHF



- instantiate H_K with e.g. $\mathrm{CBC}[E_K]$
- replace E_K by a random permutation P (PRP term)
  $\Rightarrow$ previous information-theoretic attack does not work anymore
- very similar to CCM authentication
  $\rightarrow$ conjectured BBB-secure by Jonsson [Jon02]

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.

John Black and Phillip Rogaway. A Block-Cipher Mode of Operation for Parallelizable Message Authentication. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 384–397. Springer, 2002.

Benoît Cogliati, Jooyoung Lee, and Yannick Seurin. New Constructions of MACs from (Tweakable) Block Ciphers. *IACR Trans. Symmetric Cryptol.*, 2017(2):27–58, 2017.

Benoît Cogliati and Yannick Seurin. EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 (Proceedings, Part I)*, volume 9814 of *LNCS*, pages 121–149. Springer, 2016.

References II

- Benoît Cogliati and Yannick Seurin. Analysis of the Single-Permutation Encrypted Davies-Meyer Construction. *Des. Codes Cryptography*, 2018.
- Wei Dai, Viet Tung Hoang, and Stefano Tessaro. Information-theoretic Indistinguishability via the Chi-squared Method. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 (Proceedings, Part III)*, volume 10403 of *LNCS*, pages 497–523. Springer, 2017. Full version at `http://eprint.iacr.org/2017/537`.
- 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.
- Tetsu Iwata and Kazuhiko Minematsu. Stronger Security Variants of GCM-SIV. *IACR Trans. Symmetric Cryptol.*, 2016(1):134–157, 2016.

References III

Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, and Yannick Seurin. ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 (Proceedings, Part III)*, volume 10403 of *LNCS*, pages 34–65. Springer, 2017.

Jakob Jonsson. On the Security of CTR + CBC-MAC. In Kaisa Nyberg and Howard M. Heys, editors, *Selected Areas in Cryptography - SAC 2002*, volume 2595 of *LNCS*, pages 76–93. Springer, 2002.

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.

Eik List and Mridul Nandi. ZMAC+ - An Efficient Variable-output-length Variant of ZMAC. *IACR Trans. Symmetric Cryptol.*, 2017(4):306–325, 2017.

References IV

- 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.
- Kazuhiko Minematsu and Tetsu Iwata. Tweak-Length Extension for Tweakable Blockciphers. In Jens Groth, editor, *Cryptography and Coding - IMACC 2015*, volume 9496 of *LNCS*, pages 77–93. Springer, 2015.
- Bart Mennink and Samuel Neves. Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 (Proceedings, Part III)*, volume 10403 of *LNCS*, pages 556–583. Springer, 2017. Full version at `http://eprint.iacr.org/2017/473`.
- Yusuke Naito. Full PRF-Secure Message Authentication Code Based on Tweakable Block Cipher. In Man Ho Au and Atsuko Miyaji, editors, *ProvSec 2015*, volume 9451 of *LNCS*, pages 167–182. Springer, 2015.

References V

- Yusuke Naito. Blockcipher-Based MACs: Beyond the Birthday Bound Without Message Length. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 (Proceedings, Part III)*, volume 10626 of *LNCS*, pages 446–470. Springer, 2017.
- Jacques Patarin. Security of Random Feistel Schemes with 5 or More Rounds. In Matthew K. Franklin, editor, *Advances in Cryptology - CRYPTO 2004*, volume 3152 of *LNCS*, pages 106–122. Springer, 2004.
- 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`.
- Phillip Rogaway. Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. In Pil Joong Lee, editor, *Advances in Cryptology - ASIACRYPT 2004*, volume 3329 of *LNCS*, pages 16–31. Springer, 2004.

References VI

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.

Kan Yasuda. A New Variant of PMAC: Beyond the Birthday Bound. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011*, volume 6841 of *LNCS*, pages 596–609. Springer, 2011.