New Constructions of MACs from (Tweakable) Block Ciphers

Benoît Cogliati$^1$ Jooyoung Lee$^2$ Yannick Seurin$^3$

$^1$UL, Luxembourg
$^2$KAIST, Korea
$^3$ANSSI, France

March 6, 2018 — FSE 2018
Summary of the contribution

- we propose four new MAC constructions based on a (tweakable) block cipher:

<table>
<thead>
<tr>
<th></th>
<th>stateless and deterministic</th>
<th>nonce-based/randomized</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBC-based</td>
<td>Hash-as-Tweak (HaT)</td>
<td>Nonce-as-Tweak (NaT)</td>
</tr>
<tr>
<td>BC-based</td>
<td>Hash-as-Key (HaK)</td>
<td>Nonce-as-Key (NaK)</td>
</tr>
</tbody>
</table>

- all four constructions are secure beyond the birthday bound
- TBC-based constructions are provably secure in the standard model
- BC-based constructions are provably secure in the ideal cipher model
- nonce-based constructions provide graceful security degradation with the maximal number of nonce repetitions
Summary of the contribution

- we propose four new MAC constructions based on a (tweakable) block cipher:

<table>
<thead>
<tr>
<th></th>
<th>stateless and deterministic</th>
<th>nonce-based/randomized</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBC-based</td>
<td>Hash-as-Tweak (HaT)</td>
<td>Nonce-as-Tweak (NaT)</td>
</tr>
<tr>
<td>BC-based</td>
<td>Hash-as-Key (HaK)</td>
<td>Nonce-as-Key (NaK)</td>
</tr>
</tbody>
</table>

- all four constructions are **secure beyond the birthday bound**
  - TBC-based constructions are provably secure in the standard model
  - BC-based constructions are provably secure in the ideal cipher model
  - nonce-based constructions provide graceful security degradation with the maximal number of nonce repetitions
Summary of the contribution

- we propose four new MAC constructions based on a (tweakable) block cipher:

<table>
<thead>
<tr>
<th></th>
<th>stateless and deterministic</th>
<th>nonce-based/randomized</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBC-based</td>
<td>Hash-as-Tweak (HaT)</td>
<td>Nonce-as-Tweak (NaT)</td>
</tr>
<tr>
<td>BC-based</td>
<td>Hash-as-Key (HaK)</td>
<td>Nonce-as-Key (NaK)</td>
</tr>
</tbody>
</table>

- all four constructions are secure beyond the birthday bound
- TBC-based constructions are provably secure in the standard model
- BC-based constructions are provably secure in the ideal cipher model
- nonce-based constructions provide graceful security degradation with the maximal number of nonce repetitions
Summary of the contribution

- we propose four new MAC constructions based on a (tweakable) block cipher:

<table>
<thead>
<tr>
<th></th>
<th>stateless and deterministic</th>
<th>nonce-based/randomized</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBC-based</td>
<td>Hash-as-Tweak (HaT)</td>
<td>Nonce-as-Tweak (NaT)</td>
</tr>
<tr>
<td>BC-based</td>
<td>Hash-as-Key (HaK)</td>
<td>Nonce-as-Key (NaK)</td>
</tr>
</tbody>
</table>

- all four constructions are **secure beyond the birthday bound**
- TBC-based constructions are provably secure in the **standard model**
- BC-based constructions are provably secure in the **ideal cipher model**
- nonce-based constructions provide **graceful security degradation** with the maximal number of nonce repetitions
Outline

Generalities

Stateless Deterministic MACs

Nonce-Based MACs
Outline

Generalities

Stateless Deterministic MACs

Nonce-Based MACs
MAC definition

\[ T = \text{MAC}_K(N, M) \]

\[ \text{MAC}_K(N', M') = T' ? \]

Security Definition

The adversary is allowed

- \( q \) MAC queries \( T = \text{MAC}_K(N, M) \)
- \( v \) 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 $T = \text{MAC}_K(N, M)$
- $v$ 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

\[ T = \text{MAC}_K(N, M) \]

Security Definition

The adversary is allowed

- \( q \) MAC queries \( T = \text{MAC}_K(N, M) \)
- \( v \) 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

\[ T = \text{MAC}_K(N, M) \]

\[ \text{MAC}_K(N', M') = T' \]

Security Definition

The adversary is allowed

- \( q \) MAC queries \( T = \text{MAC}_K(N, M) \)
- \( v \) 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 $M$
  - security model: nonces are chosen by the adversary, any nonce can be used at most $\mu$ times in MAC queries
    - $\mu = 1$: nonce-respecting adversary
    - $\mu > 1$: nonce-misusing adversary

- **randomized**: MAC function takes as input random coins (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 \( M \)
  - security model: nonces are chosen by the adversary, any nonce can be used at most \( \mu \) times in MAC queries
    - \( \mu = 1 \): nonce-respecting adversary
    - \( \mu > 1 \): nonce-misusing adversary
- **randomized**: MAC function takes as input random coins (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 $M$
  - security model: nonces are chosen by the adversary, any nonce can be used at most $\mu$ times in MAC queries
  - $\mu = 1$: nonce-respecting adversary
  - $\mu > 1$: nonce-misusing adversary

- **randomized**: MAC function takes as input random coins (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 used twice (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:

$$\text{Adv}_{\text{F}}^{\text{rand-MAC}}(q, v) \leq \frac{q^\mu + 1}{2\mu(n+1)} + \text{Adv}_{\text{F}}^{\text{nonce-MAC}}(q, v, \mu)$$

small for $\mu > 1$

for any value of $\mu =$ maximal number of nonce repetitions.
Graceful nonce-misuse security degradation

- the security of some nonce-based MACs collapses if a single nonce is used twice (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:

$$\text{Adv}^{\text{rand-MAC}}_F(q, v) \leq \frac{q^{\mu+1}}{2^{\mu(n+1)}} + \text{Adv}^{\text{nonce-MAC}}_F(q, v, \mu)$$

small for $\mu > 1$

for any value of $\mu = \text{maximal number of nonce repetitions}$.
Graceful nonce-misuse security degradation

- the security of some nonce-based MACs collapses if a single nonce is used twice (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:

$$\text{Adv}_{F}^{\text{rand-MAC}}(q, v) \leq \frac{q^{\mu+1}}{2^{\mu(n+1)}} + \text{Adv}_{F}^{\text{nonce-MAC}}(q, v, \mu)$$

- $\mu$-multicoll. proba.
- small for $\mu > 1$

for any value of $\mu = \text{maximal number of nonce repetitions}$. 

B. Cogliati, J. Lee, Y. Seurin  
New Constructions of MACs from (T)BCs  
FSE 2018
Building blocks: BCs and TBCs

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

$n = \text{block size}$
$t = \text{tweak size}$
Building blocks: BCs and TBCs

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

$n = \text{block size}$
$t = \text{tweak size}$
Building blocks: BCs and TBCs

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

$n = \text{block size}$
$t = \text{tweak size}$
Building blocks: BCs and TBCs

- Block cipher $E$: for each key $K$, $X \mapsto E(K, X)$ is a permutation.
- Tweakeable block cipher $\tilde{E}$: for each key $K$ and each tweak $W$, $X \mapsto \tilde{E}(K, W, X)$ is a permutation.
- One can think of a keyed TBC $\tilde{E}_K$ as an “imperfect” PRF from $(n + t)$ bits to $n$ bits.
- If any tweak $W$ is used at most “a few” times, $\tilde{E}_K$ is close to a random $(n + t)$-to-$n$-bit function.
Outline

Generalities

Stateless Deterministic MACs

Nonce-Based MACs

Conclusion
The “standard” UHF-then-PRF Construction

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

  $$\forall M \neq M', \Pr[K \leftarrow K : H_K(M) = H_K(M')] \leq \varepsilon$$

- $H$ 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 “standard” UHF-then-PRF Construction

- based on a fixed-input-length PRF $F$ and an $\varepsilon$-almost universal ($\varepsilon$-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 “standard” UHF-then-PRF Construction

- based on a fixed-input-length PRF $F$ and an $\varepsilon$-almost universal ($\varepsilon$-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 $\varepsilon$

\[ \text{Adv}_{F \circ H}^{\text{PRF}}(q) \leq \frac{q^2 \varepsilon}{2} + \text{Adv}_{F}^{\text{PRF}}(q) \]

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

\[ \Rightarrow \text{BB-security} \]
Security of UHF-then-PRF

- birthday-bound-secure w.r.t. $H$ collision probability $\varepsilon$

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

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

$\Rightarrow$ BB-security
Construction 1: Hash-as-Tweak (HaT)

- BBB-secure assuming $H$ and $H'$ are $\varepsilon$-AU secure:

$$\text{Adv}^{\text{MAC}}_{\text{HaT}}(q, \nu) \leq q^2\varepsilon^2 + q\nu\varepsilon^2 + (\ldots)$$

- follow-up work: Hash-then-TBC construction [LN17], BBB-secure under more complex UHF-type properties of $H$
Construction 1: Hash-as-Tweak (HaT)

- BBB-secure assuming $H$ and $H'$ are $\varepsilon$-AU secure:
  \[
  \text{Adv}^{\text{MAC}}_{\text{HaT}}(q, v) \leq q^2 \varepsilon^2 + qv\varepsilon^2 + (\ldots)
  \]

- follow-up work: Hash-then-TBC construction [LN17], BBB-secure under more complex UHF-type properties of $H$
Construction 2: Hash-as-Key (HaK)

• output transformation unkeyed \( \Rightarrow H \) and \( H' \) must be \( \varepsilon' \)-uniform:

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

• BBB-secure in the ideal cipher model assuming \( H \) and \( H' \) are \( \varepsilon \)-AU and \( \varepsilon' \)-uniform:

\[
\text{Adv}^{\text{MAC}}_{\text{HaK}}(q, v) \leq q^2 \varepsilon^2 + qv \varepsilon^2 + (\ldots)
\]
The UHF-then-RO construction

- Hash-as-Key (HaK) is a special case of the “UHF-then-RO” construction
  - modeling $G$ as a random function oracle ($q_G$ queries), the construction is secure if $H$ is $\varepsilon$-AU and $\varepsilon'$-uniform:
    \[
    \text{Adv}_{G \circ H}^{\text{PRF}}(q, q_G) \leq \frac{q^2 \varepsilon}{2} + q q_G \varepsilon'
    \]
  - security proof under a standard assumption on $G$? 
The UHF-then-RO construction

- Hash-as-Key (HaK) is a special case of the “UHF-then-RO” construction
- modeling $G$ as a random function oracle ($q_G$ queries), the construction is secure if $H$ is $\varepsilon$-AU and $\varepsilon'$-uniform:

$$\text{Adv}^{\text{PRF}}_{G \circ H}(q, q_G) \leq \frac{q^2 \varepsilon}{2} + qq_G\varepsilon'$$

- security proof under a standard assumption on $G$?
The UHF-then-RO construction

- Hash-as-Key (HaK) is a special case of the “UHF-then-RO” construction
- modeling $G$ as a random function oracle ($q_G$ queries), the construction is secure if $H$ is $\varepsilon$-AU and $\varepsilon'$-uniform:

$$\text{Adv}^{\text{PRF}}_{G \circ H}(q, q_G) \leq \frac{q^2 \varepsilon}{2} + q q_G \varepsilon'$$

- security proof under a standard assumption on $G$?
Outline

Generalities

Stateless Deterministic MACs

Nonce-Based MACs

B. Cogliati, J. Lee, Y. Seurin

New Constructions of MACs from (T)BCs
The Wegman-Carter construction \([\text{GMS74, WC81}]\)

- based on an \(\varepsilon\)-almost xor-universal (\(\varepsilon\)-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 (GHASH, Poly1305)
- “optimal” security:
  \[
  \text{Adv}_{\text{WC}}^{\text{nonce-MAC}}(q, v) \leq v\varepsilon + \text{Adv}_{F}^{\text{PRF}}(q + v)
  \]
The Wegman-Carter construction [GMS74, WC81]

- based on an $\epsilon$-almost xor-universal ($\epsilon$-AXU) hash function $H$:
  \[ \forall M \neq M', \forall Y, \Pr[K \leftarrow \mathcal{K} : H_K(M) \oplus H_K(M') = Y] \leq \epsilon \]
- in practice, OTPs are replaced by a PRF applied to a nonce $N$
- $H$ usually based on polynomial evaluation (GHASH, Poly1305)
- “optimal” security:
  \[ \text{Adv}^{\text{nonce-MAC}}_{\text{WC}}(q, v) \leq v\epsilon + \text{Adv}^{\text{PRF}}_{F}(q + v) \]
The Wegman-Carter construction \[ \text{[GMS74, WC81]} \]

- based on an \( \varepsilon \)-almost xor-universal (\( \varepsilon \)-AXU) hash function \( H \):
  \[
  \forall M \neq M', \forall Y, \Pr[K \leftarrow K : H_K(M) \oplus H_K(M') = Y] \leq \varepsilon
  \]
- in practice, OTPs are replaced by a PRF applied to a nonce \( N \)
- \( H \) usually based on polynomial evaluation (GHASH, Poly1305)
- “optimal” security:
  \[
  \text{Adv}_{\text{WC}}^{\text{nonce-MAC}}(q, v) \leq v\varepsilon + \text{Adv}_F^{\text{PRF}}(q + v)
  \]
The Wegman-Carter construction \([GMS74, WC81]\)

- based on an \(\varepsilon\)-almost xor-universal (\(\varepsilon\)-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 (GHASH, Poly1305)
- “optimal” security:
  \[
  \text{Adv}^{\text{nonce-MAC}}_{\text{WC}}(q, v) \leq v \varepsilon + \text{Adv}^{\text{PRF}}_{F}(q + v)
  \]
Wegman-Carter weaknesses

- in practice, \( F \) is replaced by a block cipher
  \( \rightarrow \) Wegman-Carter-Shoup (WCS) construction

- provable security drops to birthday bound [Sho96, Ber05]

\[
\text{Adv}_{\text{WCS}}^{\text{nonce-MAC}}(q, \nu) \leq \nu \varepsilon + \frac{(q + \nu)^2}{2 \cdot 2^n} + \text{Adv}^P_{\text{PRP}}(q + \nu)
\]

- nonce-misuse problem: a single nonce repetition can completely break security [Jou06, HP08] (esp. for polynomial hashing)
Wegman-Carter weaknesses

- in practice, $F$ is replaced by a block cipher
  $\rightarrow$ Wegman-Carter-Shoup (WCS) construction
- provable security drops to birthday bound [Sho96, Ber05]

\[
\text{Adv}_{\text{WCS}}^{\text{nonce-MAC}}(q, v) \leq v\varepsilon + \frac{(q + v)^2}{2 \cdot 2^n} + \text{Adv}_E^{\text{PRP}}(q + v)
\]

- nonce-misuse problem: a single nonce repetition can completely break security [Jou06, HP08] (esp. for polynomial hashing)
Wegman-Carter weaknesses

- in practice, $F$ is replaced by a block cipher
  $\rightarrow$ Wegman-Carter-Shoup (WCS) construction
- provable security drops to birthday bound [Sho96, Ber05]

\[
\text{Adv}_{\text{WCS}}^{\text{nonce-MAC}}(q, v) \leq v\varepsilon + \frac{(q + v)^2}{2 \cdot 2^n} + \text{Adv}_E^{\text{PRP}}(q + v)
\]

- nonce-misuse problem: a single nonce repetition can completely break security [Jou06, HP08] (esp. for polynomial hashing)
Construction 3: Nonce-as-Tweak (NaT)

- if nonces don’t repeat to often, $\tilde{E}_{K'}$ is close to a perfect PRF
- graceful security degradation with maximal nonce multiplicity $\mu$

$$\text{Adv}_{\text{NaT}}^{\text{nonce-MAC}}(q, v) \leq 2(\mu - 1)q\varepsilon + \mu v\varepsilon + (\ldots)$$

- can be seen as a special case of the (PRF-based) WMAC construction [BC09]
Construction 3: Nonce-as-Tweak (NaT)

- if nonces don’t repeat too often, $\tilde{E}_{K'}$ is close to a perfect PRF
- graceful security degradation with maximal nonce multiplicity $\mu$

$$\text{Adv}_{\text{NaT}}^{\text{nonce-MAC}}(q, v) \leq 2(\mu - 1)q\epsilon + \mu v\epsilon + (\ldots)$$

- can be seen as a special case of the (PRF-based) WMAC construction [BC09]
Construction 3: Nonce-as-Tweak (NaT)

- if nonces don’t repeat too often, $\tilde{E}_{K'}$ is close to a perfect PRF
- graceful security degradation with maximal nonce multiplicity $\mu$

$$\text{Adv}_{\text{NaT}}^{\text{nonce-MAC}}(q, v) \leq 2(\mu - 1)q\varepsilon + \mu v\varepsilon + (\ldots)$$

- can be seen as a special case of the (PRF-based) WMAC construction [BC09]
Construction 4: Nonce-as-Key (NaK)

- provably secure in the ideal cipher model, assuming \( H \) is \( \epsilon \)-AXU and \( \epsilon' \)-uniform
  
  \[
  \text{Adv}_{\text{NaK}}^{\text{nonce-MAC}}(q, v) \leq \mu q \epsilon + (\ldots)
  \]

- graceful security degradation with maximal nonce multiplicity \( \mu \)

- Davies-Meyer mode required to make the output function non-invertible!
Construction 4: Nonce-as-Key (NaK)

- provably secure in the ideal cipher model, assuming $H$ is $\varepsilon$-AXU and $\varepsilon'$-uniform

\[
\text{Adv}_{\text{NaK}}^{\text{nonce-MAC}}(q, v) \leq \mu q \varepsilon + (\ldots)
\]

- graceful security degradation with maximal nonce multiplicity $\mu$
- Davies-Meyer mode required to make the output function non-invertible!
Construction 4: Nonce-as-Key (NaK)

- provably secure in the ideal cipher model, assuming $H$ is $\varepsilon$-AXU and $\varepsilon'$-uniform

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

- graceful security degradation with maximal nonce multiplicity $\mu$
- Davies-Meyer mode required to make the output function non-invertible!
Conclusion

• we proposed four new MAC constructions secure beyond the birthday bound:

<table>
<thead>
<tr>
<th></th>
<th>Stateless and Deterministic</th>
<th>Nonce-Based/Randomized</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBC-based</td>
<td>Hash-as-Tweak (HaT)</td>
<td>Nonce-as-Tweak (NaT)</td>
</tr>
<tr>
<td>BC-based</td>
<td>Hash-as-Key (HaK)</td>
<td>Nonce-as-Key (NaK)</td>
</tr>
</tbody>
</table>

• all security proofs rely on the standard H-coefficients technique [Pat08, CS14]

• our work does not address how to construct the UHF from a BC or TBC but many existing constructions can be used (PMAC/PMAC1 [BR02, Rog04], ZHASH [IMPSh17], etc.)

• Nonce-as-Tweak (NaT) used in CAESAR candidate Deoxys v1.4
Conclusion

- we proposed four new MAC constructions secure beyond the birthday bound:

<table>
<thead>
<tr>
<th>Stateless and Deterministic</th>
<th>Nonce-Based/Randomized</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBC-based</td>
<td>Hash-as-Tweak (HaT)</td>
</tr>
<tr>
<td>BC-based</td>
<td>Hash-as-Key (HaK)</td>
</tr>
<tr>
<td>Nonce-as-Tweak (NaT)</td>
<td></td>
</tr>
<tr>
<td>Nonce-as-Key (NaK)</td>
<td></td>
</tr>
</tbody>
</table>

- all security proofs rely on the standard H-coefficients technique \[Pat08, CS14\]
- our work does not address how to construct the UHF from a BC or TBC but many existing constructions can be used (PMAC/PMAC1 \[BR02, Rog04\], ZHASH \[IMPS17\], etc.)
- Nonce-as-Tweak (NaT) used in CAESAR candidate Deoxys v1.4
Conclusion

- we proposed four new MAC constructions secure beyond the birthday bound:

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stateless</td>
<td>Hash-as-Tweak (HaT)</td>
</tr>
<tr>
<td>Deterministic</td>
<td>Hash-as-Key (HaK)</td>
</tr>
<tr>
<td>Nonce-Based</td>
<td>Nonce-as-Tweak (NaT)</td>
</tr>
<tr>
<td>Randomized</td>
<td>Nonce-as-Key (NaK)</td>
</tr>
</tbody>
</table>

- all security proofs rely on the standard H-coefficients technique [Pat08, CS14]

- our work does not address how to construct the UHF from a BC or TBC but many existing constructions can be used (PMAC/PMAC1 [BR02, Rog04], ZHASH [IMPS17], etc.)

- Nonce-as-Tweak (NaT) used in CAESAR candidate Deoxys v1.4
Conclusion

- we proposed four new MAC constructions secure beyond the birthday bound:

<table>
<thead>
<tr>
<th></th>
<th>stateless and deterministic</th>
<th>nonce-based/randomized</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBC-based</td>
<td>Hash-as-Tweak (HaT)</td>
<td>Nonce-as-Tweak (NaT)</td>
</tr>
<tr>
<td>BC-based</td>
<td>Hash-as-Key (HaK)</td>
<td>Nonce-as-Key (NaK)</td>
</tr>
</tbody>
</table>

- all security proofs rely on the standard H-coefficients technique [Pat08, CS14]

- our work does not address how to construct the UHF from a BC or TBC but many existing constructions can be used (PMAC/PMAC1 [BR02, Rog04], ZHASH [IMPS17], etc.)

- Nonce-as-Tweak (NaT) used in CAESAR candidate Deoxys v1.4
The end...

Thanks for your attention!

Comments or questions?


References


