Categorization of Faulty Nonce Misuse Resistant Message Authentication

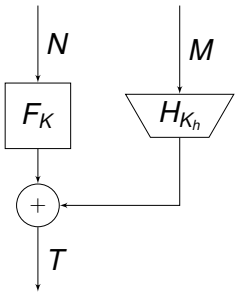
Yu Long Chen[1] Bart Mennink[2] Bart Preneel[1]

imec-COSIC, KU Leuven

Digital Security Group, Radboud University

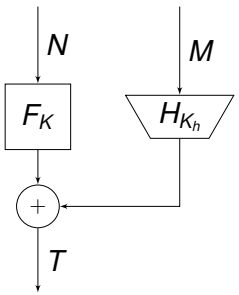
December, 2021

Nonce-Based MAC Algorithms and Wegman-Carter



Wegman and Carter (1981)

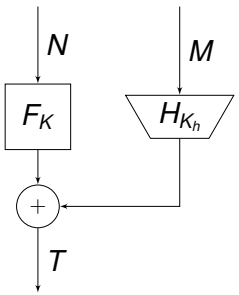
Nonce-Based MAC Algorithms and Wegman-Carter



Wegman and Carter (1981)

- Based on work of Gilbert, MacWilliams, and Sloane (1974)

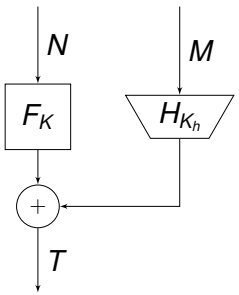
Nonce-Based MAC Algorithms and Wegman-Carter



Wegman and Carter (1981)

- Based on work of Gilbert, MacWilliams, and Sloane (1974)
- F = PRF: n-bit security

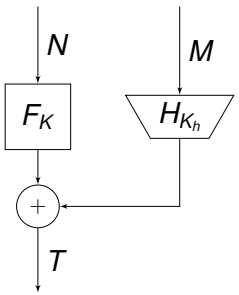
Nonce-Based MAC Algorithms and Wegman-Carter



Wegman and Carter (1981)

- Based on work of Gilbert, MacWilliams, and Sloane (1974)
- F = PRF: n-bit security
- F = block cipher: $n/2$-bit security (Wegman-Carter-Shoup)

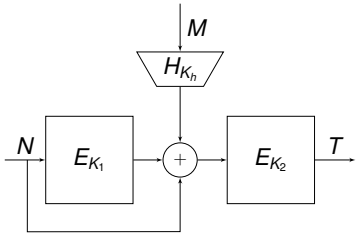
Nonce-Based MAC Algorithms and Wegman-Carter



Wegman and Carter (1981)

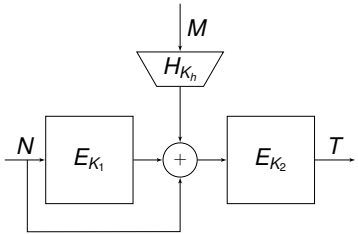
- Based on work of Gilbert, MacWilliams, and Sloane (1974)
- F = PRF: n-bit security
- F = block cipher: $n/2$-bit security (Wegman-Carter-Shoup)
- Broken by nonce repetition

Encrypted Wegman-Carter with Davies-Meyer



Cogliati and Seurin (2016)

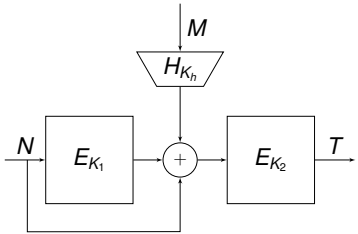
Encrypted Wegman-Carter with Davies-Meyer



Cogliati and Seurin (2016)

- $2n/3$-bit security in nonce-respecting scenario

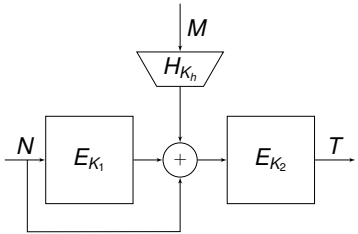
Encrypted Wegman-Carter with Davies-Meyer



Cogliati and Seurin (2016)

- $2n/3$-bit security in nonce-respecting scenario
- $n/2$-bit security in nonce-misuse scenario

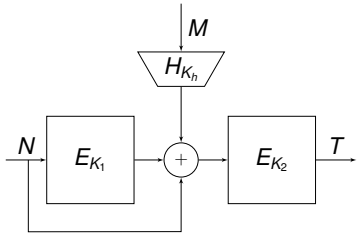
Encrypted Wegman-Carter with Davies-Meyer



Cogliati and Seurin (2016)

- $2n/3$-bit security in nonce-respecting scenario
- $n/2$-bit security in nonce-misuse scenario
- Mennink and Neves (2017): n-bit security in nonce-respecting scenario using unverified mirror theory

Encrypted Wegman-Carter with Davies-Meyer

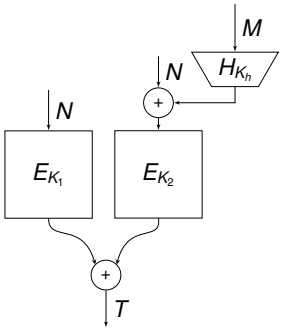


Cogliati and Seurin (2016)

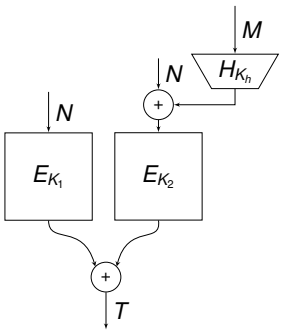
- $2n/3$-bit security in nonce-respecting scenario
- $n/2$-bit security in nonce-misuse scenario
- Mennink and Neves (2017): n-bit security in nonce-respecting scenario using unverified mirror theory
- Datta et al. (2018): DWCDM using one block cipher call with its inverse

Nonce-Based Enhanced Hash-then-Mask

Dutta et al. (2019)



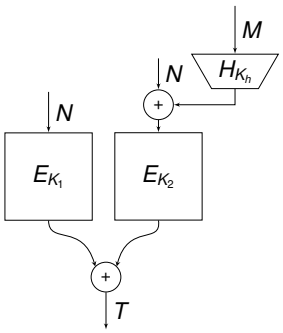
Nonce-Based Enhanced Hash-then-Mask



Dutta et al. (2019)

- Nonce-based variant of EHtM (Minematsu 2010)

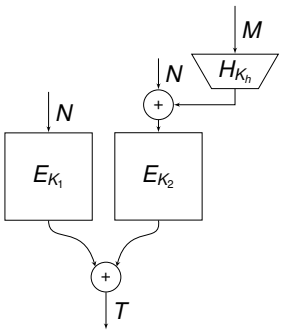
Nonce-Based Enhanced Hash-then-Mask



Dutta et al. (2019)

- Nonce-based variant of EHtM (Minematsu 2010)
- Faulty nonce model: “faulty” query = MAC query with repeated nonce

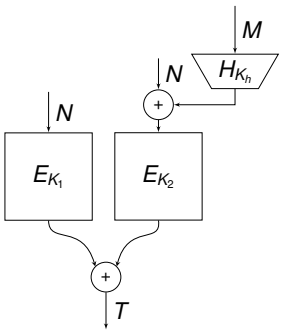
Nonce-Based Enhanced Hash-then-Mask



Dutta et al. (2019)

- Nonce-based variant of EHtM (Minematsu 2010)
- Faulty nonce model: “faulty” query = MAC query with repeated nonce
- Graceful security degradation

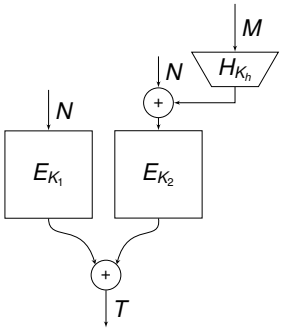
Nonce-Based Enhanced Hash-then-Mask



Dutta et al. (2019)

- Nonce-based variant of EHtM (Minematsu 2010)
- Faulty nonce model: “faulty” query = MAC query with repeated nonce
- Graceful security degradation
- $2n/3$-bit security if number of faulty queries $\leq 2^{n/3}$

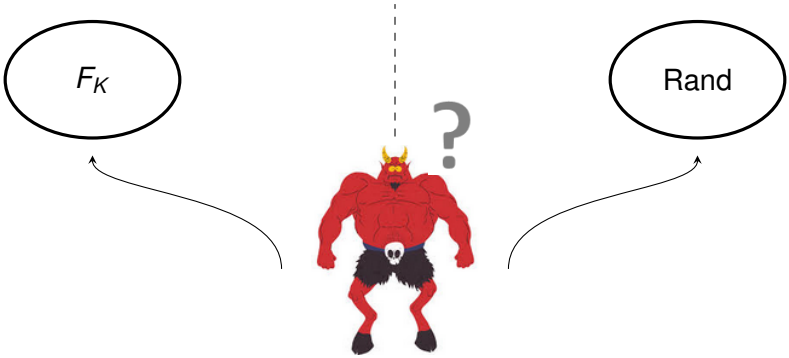
Nonce-Based Enhanced Hash-then-Mask



Dutta et al. (2019)

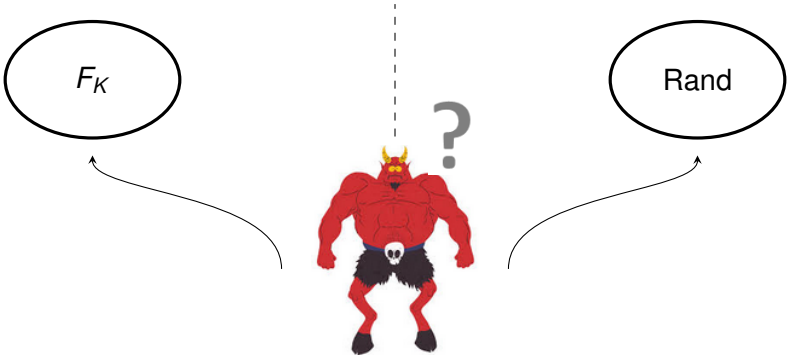
- Nonce-based variant of EHtM (Minematsu 2010)
- Faulty nonce model: “faulty” query = MAC query with repeated nonce
- Graceful security degradation
- $2n/3$-bit security if number of faulty queries $\leq 2^{n/3}$
- Choi et al. (2020): $3n/4$-bit security if number of faulty queries $\leq 2^{3n/8}$

Security Definition



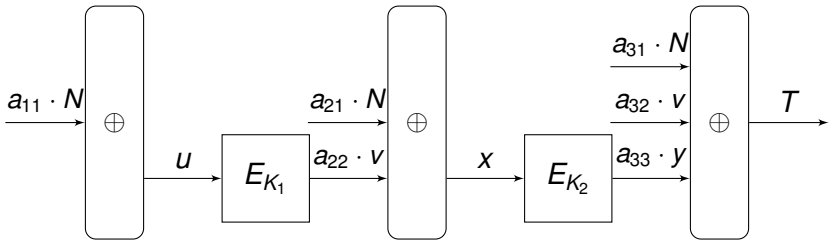
- Adversary $\mathcal{A}$ makes q queries to oracle (F_K or Rand)

Security Definition



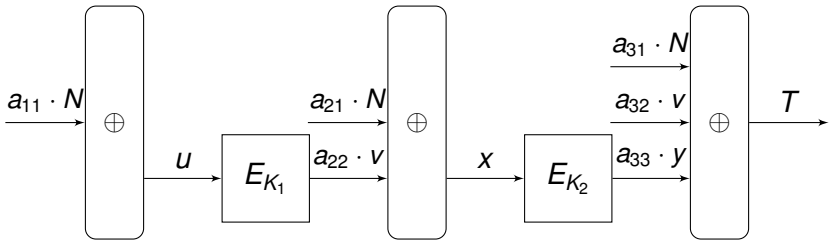
- Adversary $\mathcal{A}$ makes q queries to oracle (F_K or Rand)
- Good PRF $\iff$ $\mathcal{A}$ cannot determine which world it is interacting with

Generalized Fixed-Input-Length PRF Construction



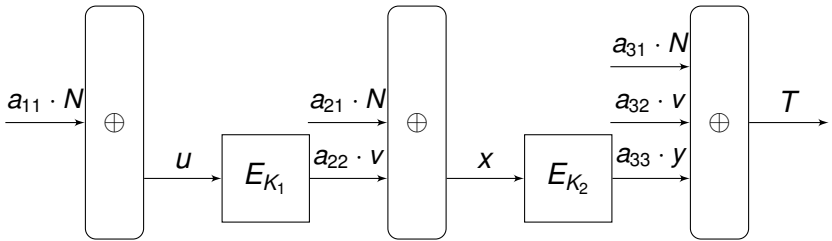
- Fixed input-length PRFs from two block cipher calls

Generalized Fixed-Input-Length PRF Construction



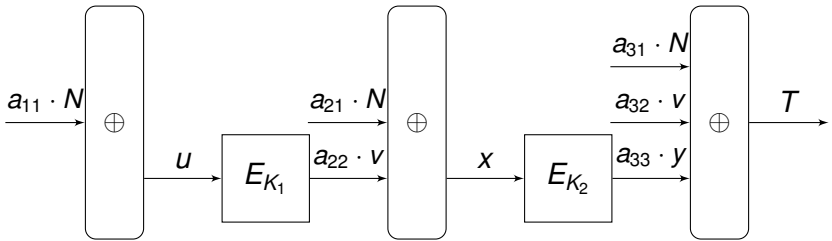
- Fixed input-length PRFs from two block cipher calls
- In total 2^6 schemes, but many trivially insecure

Generalized Fixed-Input-Length PRF Construction



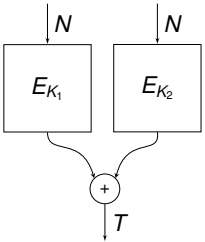
- Fixed input-length PRFs from two block cipher calls
- In total 2^6 schemes, but many trivially insecure
- $a_{11} = 1$, $a_{33} = 1$, $a_{22} + a_{32} \geq 1$, $a_{21} + a_{22} \geq 1$

Generalized Fixed-Input-Length PRF Construction

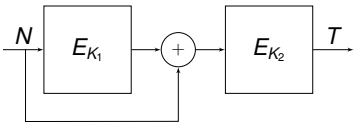


- Fixed input-length PRFs from two block cipher calls
- In total 2^6 schemes, but many trivially insecure
- $a_{11} = 1$, $a_{33} = 1$, $a_{22} + a_{32} \geq 1$, $a_{21} + a_{22} \geq 1$
- We are only interested in beyond birthday bound secure PRFs

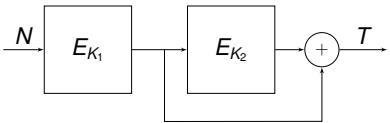
SoP, EDM, and EDMD



Sum of Permutations
(Bellare et al. 1998)

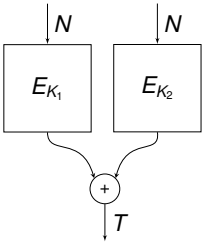


Encrypted Davies-Meyer
(Cogliati and Seurin 2016)

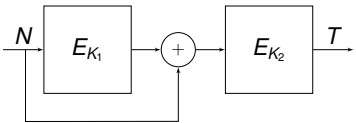


Encrypted Davies-Meyer Dual
(Mennink and Neves 2017)

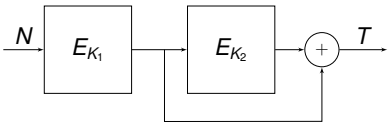
SoP, EDM, and EDMD



Sum of Permutations
(Bellare et al. 1998)



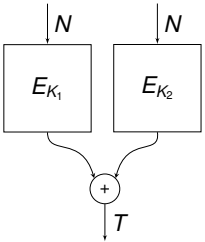
Encrypted Davies-Meyer
(Cogliati and Seurin 2016)



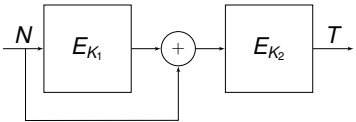
Encrypted Davies-Meyer Dual
(Mennink and Neves 2017)

n-bit security

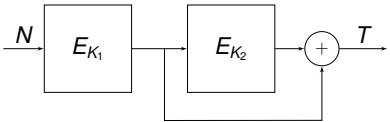
SoP, EDM, and EDMD



Sum of Permutations
(Bellare et al. 1998)



Encrypted Davies-Meyer
(Cogliati and Seurin 2016)

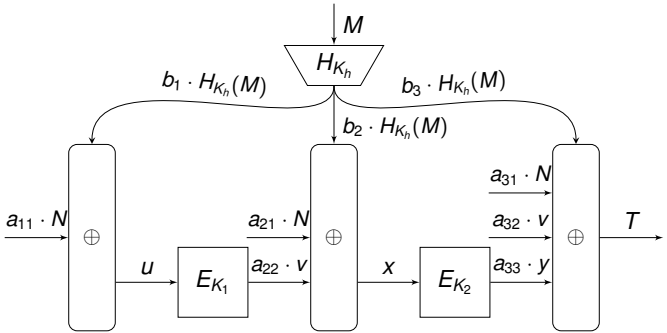


Encrypted Davies-Meyer Dual
(Mennink and Neves 2017)

n-bit security

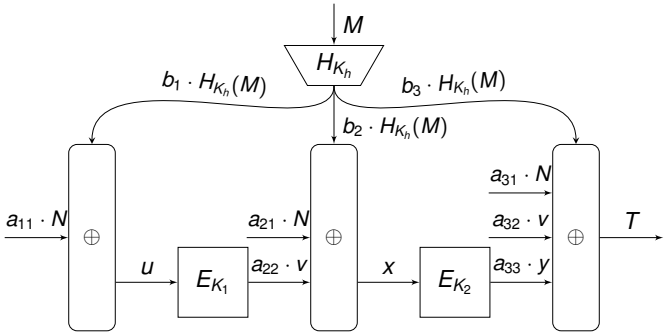
+ natural siblings of these 3 PRFs consist of XORing the input to the output

Generalized Nonce-Based MAC Algorithms



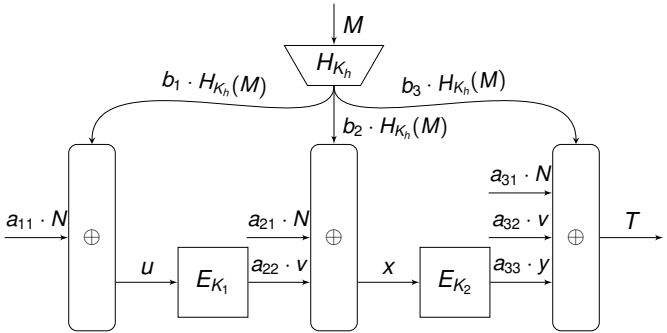
- Nonce-based PRFs from two block cipher calls and one universal hash function call

Generalized Nonce-Based MAC Algorithms



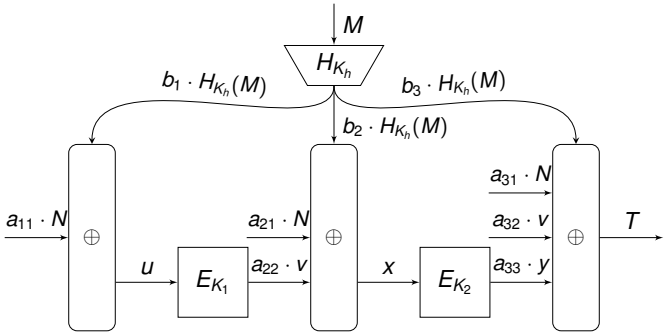
- Nonce-based PRFs from two block cipher calls and one universal hash function call
- In total 2^9 schemes, but many trivially insecure

Generalized Nonce-Based MAC Algorithms



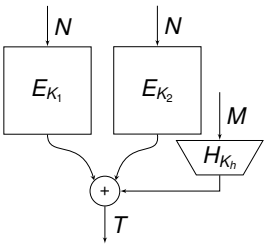
- Nonce-based PRFs from two block cipher calls and one universal hash function call
- In total 2^9 schemes, but many trivially insecure
- $a_{11} = 1$, $a_{33} = 1$, $a_{22} + a_{32} \geq 1$, $a_{21} + a_{22} \geq 1$, $b_1 + b_2 + b_3 \geq 1$

Generalized Nonce-Based MAC Algorithms

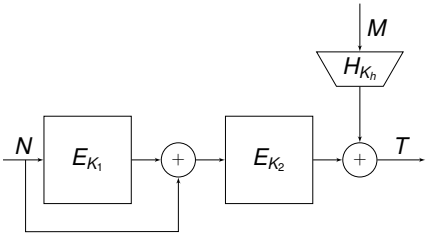


- Nonce-based PRFs from two block cipher calls and one universal hash function call
- In total 2^9 schemes, but many trivially insecure
- $a_{11} = 1$, $a_{33} = 1$, $a_{22} + a_{32} \geq 1$, $a_{21} + a_{22} \geq 1$, $b_1 + b_2 + b_3 \geq 1$
- In total 10 interesting constructions
  (5 based on EDM, 3 based on SoP, and 2 based on EDMD)

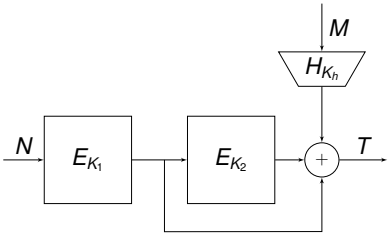
SoP, EDM, and EDMD Based Wegman-Carter



SoP Wegman-Carter

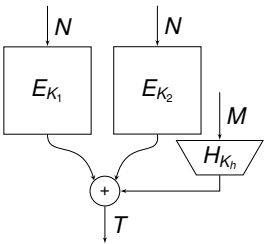


EDM Wegman-Carter

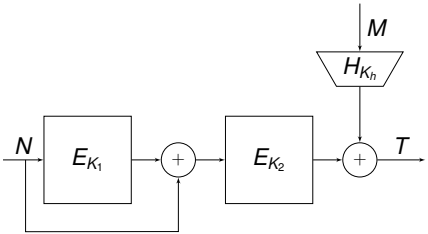


EDMD Wegman-Carter

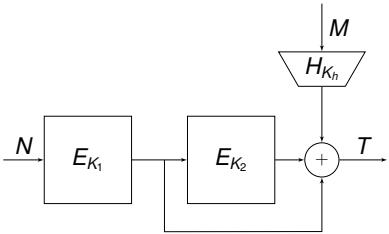
SoP, EDM, and EDMD Based Wegman-Carter



SoP Wegman-Carter



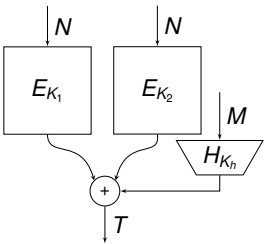
EDM Wegman-Carter



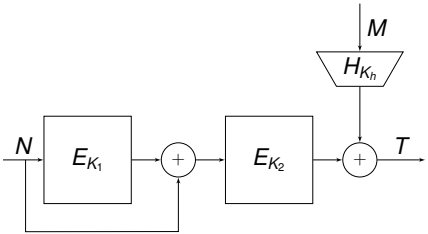
EDMD Wegman-Carter

n-bit security in nonce-respecting scenario

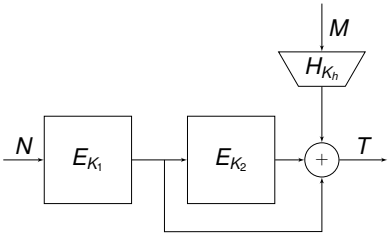
SoP, EDM, and EDMD Based Wegman-Carter



SoP Wegman-Carter



EDM Wegman-Carter

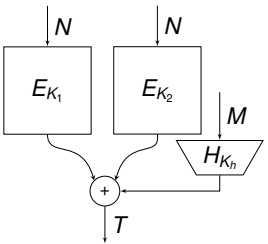


EDMD Wegman-Carter

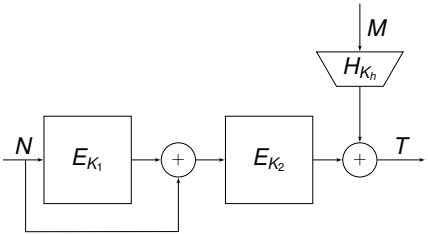
n-bit security in nonce-respecting scenario

Totally broken if a single nonce is re-used

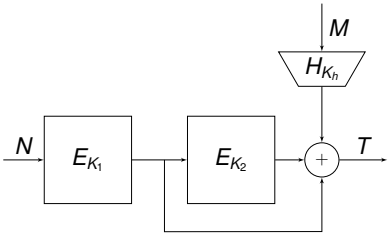
SoP, EDM, and EDMD Based Wegman-Carter



SoP Wegman-Carter



EDM Wegman-Carter



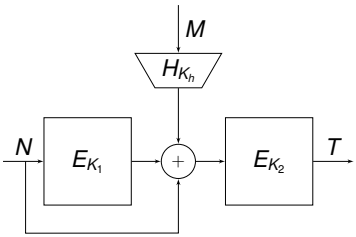
EDMD Wegman-Carter

n-bit security in nonce-respecting scenario

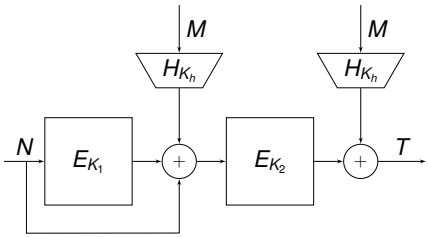
Totally broken if a single nonce is re-used

Schemes left: 4 based on EDM, 2 based on SoP, and 1 based on EDMD

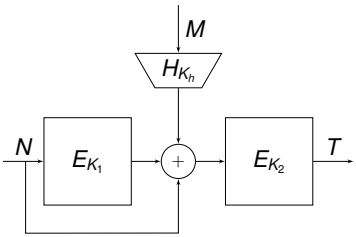
Nonce-Based MAC Algorithms Based on EDM (1)



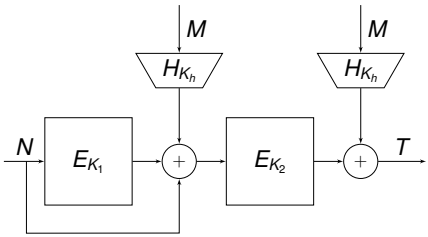
EWCDM



Nonce-Based MAC Algorithms Based on EDM (1)

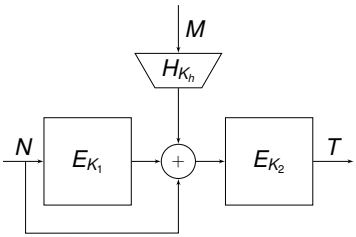


EWCDM

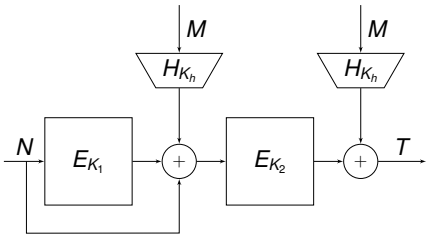


$3n/4$-bit security with concrete proof in nonce-respecting scenario

Nonce-Based MAC Algorithms Based on EDM (1)



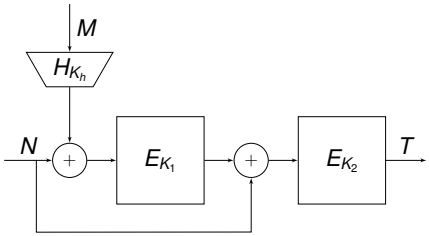
EWCDM

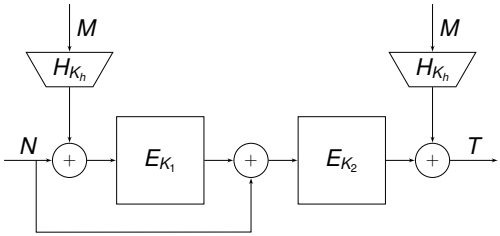


$3n/4$-bit security with concrete proof in nonce-respecting scenario

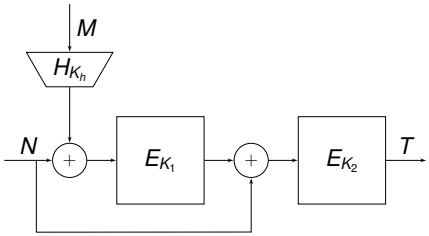
No graceful security degradation, $n/2$-bit security if a single nonce is re-used

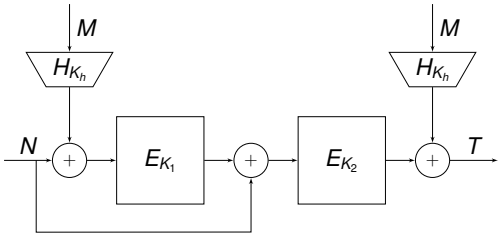
Nonce-Based MAC Algorithms Based on EDM (2)





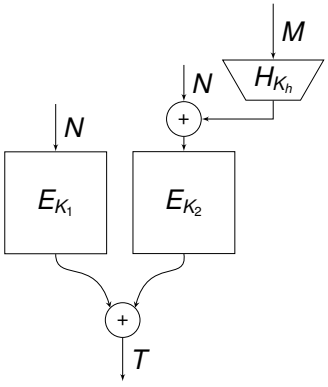
Nonce-Based MAC Algorithms Based on EDM (2)



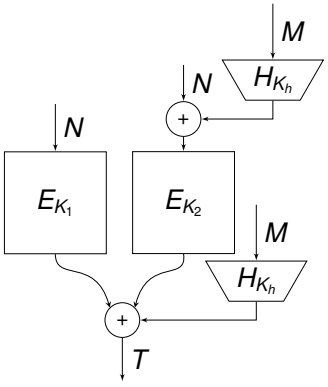


$3n/4$-bit security if number of faulty queries $\leq 2^{n/2}$

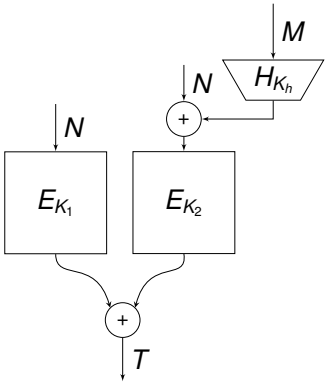
Nonce-Based MAC Algorithms Based on SoP



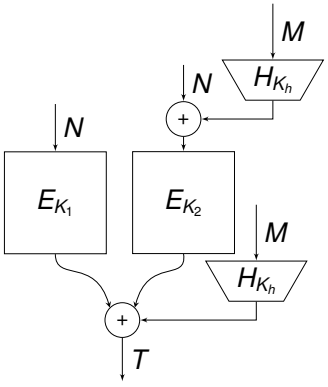
nEHtM



Nonce-Based MAC Algorithms Based on SoP

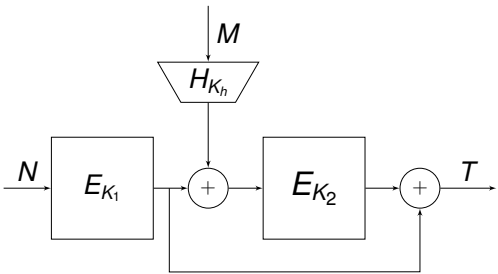


nEHtM

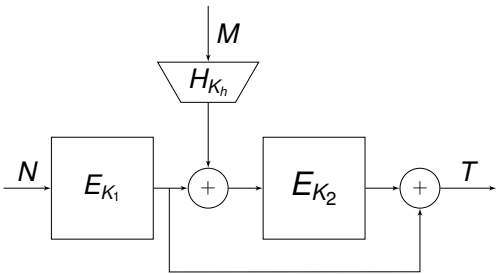


$3n/4$-bit security if number of faulty queries $\leq 2^{3n/8}$

Nonce-Based MAC Algorithm Based on EDMD

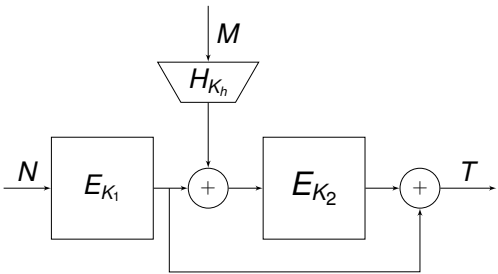


Nonce-Based MAC Algorithm Based on EDMD



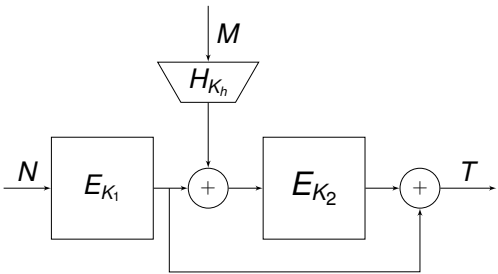
- Outputs of E_{K_1} are not known

Nonce-Based MAC Algorithm Based on EDMD



- Outputs of E_{K_1} are not known
- Outputs of E_{K_2} are also not known due to feed-forward (we only know T)

Nonce-Based MAC Algorithm Based on EDMD



- Outputs of E_{K_1} are not known
- Outputs of E_{K_2} are also not known due to feed-forward (we only know T)
- Impossible to apply any other currently known technique

Security Analysis

- Patarin's H-coefficient technique

$$\frac{\Pr(X_{\mathcal{O}} = \tau)}{\Pr(X_{\mathcal{P}} = \tau)} \geq 1 - \epsilon$$

$$\mathbf{Adv}(\mathcal{A}) \leq \epsilon + \Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$$

Security Analysis

- Patarin's H-coefficient technique

$$\frac{\Pr(X_{\mathcal{O}} = \tau)}{\Pr(X_{\mathcal{P}} = \tau)} \geq 1 - \epsilon$$

$$\mathbf{Adv}(\mathcal{A}) \leq \epsilon + \Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$$

- Patarin's mirror theory to obtain ϵ, transcript graph should be

Security Analysis

- Patarin's H-coefficient technique

$$\frac{\Pr(X_{\mathcal{O}} = \tau)}{\Pr(X_{\mathcal{P}} = \tau)} \geq 1 - \epsilon$$

$$\mathbf{Adv}(\mathcal{A}) \leq \epsilon + \Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$$

- Patarin's mirror theory to obtain ϵ, transcript graph should be
  - acyclic

Security Analysis

- Patarin's H-coefficient technique

$$\frac{\Pr(X_{\mathcal{O}} = \tau)}{\Pr(X_{\mathcal{P}} = \tau)} \geq 1 - \epsilon$$

$$\mathbf{Adv}(\mathcal{A}) \leq \epsilon + \Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$$

- Patarin's mirror theory to obtain ϵ, transcript graph should be
  - acyclic
  - non-zero path label

Security Analysis

- Patarin's H-coefficient technique

$$\frac{\Pr(X_{\mathcal{O}} = \tau)}{\Pr(X_{\mathcal{P}} = \tau)} \geq 1 - \epsilon$$

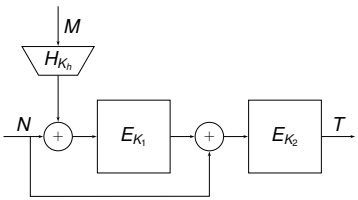
$$\mathbf{Adv}(\mathcal{A}) \leq \epsilon + \Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$$

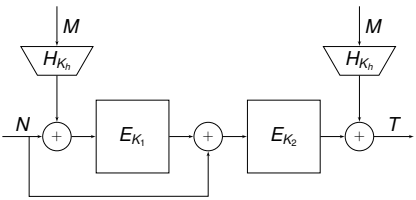
- Patarin's mirror theory to obtain ϵ, transcript graph should be
  - acyclic
  - non-zero path label
  - these two properties define $\Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$

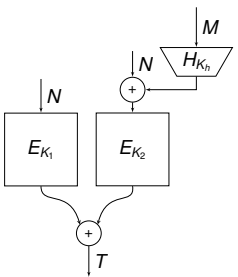
Comparison

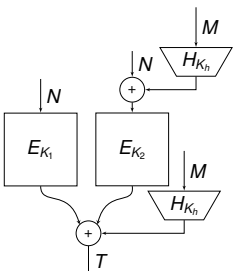
MAC	nonce-resp. security ($\log_2$)	nonce-misuse security ($\log_2$)	computing E_{K_1} without M	sequential/ parallel	security tightness	note
$F_{B_1}^{\mathrm{EDM}}$	n	0	✓	S	tight	WC-with-EDM
$F_{B_1}^{\mathrm{SoP}}$	n	0	✓	P	tight	WC-with-SoP
$F_{B_1}^{\mathrm{EDMD}}$	n	0	✓	S	tight	WC-with-EDMD
$F_{B_2}^{\mathrm{EDM}}$	$3n/4$ (n)	$n/2$	✓	S	not (tight)	EWCDM
$F_{B_3}^{\mathrm{EDM}}$	$3n/4$	$n/2$	✓	S	not	this work
$F_{B_4}^{\mathrm{EDM}}$	$3n/4$	$3n/4$ ($\mu < 2^{n/2}$)	—	S	?	this work
$F_{B_5}^{\mathrm{EDM}}$	$3n/4$	$3n/4$ ($\mu < 2^{n/2}$)	—	S	?	this work
$F_{B_2}^{\mathrm{SoP}}$	$3n/4$	$3n/4$ ($\mu \leq 2^{n/4}$)	✓	P	?	nEHtM
$F_{B_3}^{\mathrm{SoP}}$	$3n/4$	$3n/4$ ($\mu \leq 2^{n/4}$)	✓	P	?	this work
$F_{B_2}^{\mathrm{EDMD}}$	?	?	✓	S	—	—

Four MAC Algorithms with Graceful Security Degradation









Conclusion

New results

- All PRFs based on two block cipher calls
- All MAC algorithms based on one universal hash function and two block cipher calls
- Beyond birthday bound security in faulty nonce model

Conclusion

New results

- All PRFs based on two block cipher calls
- All MAC algorithms based on one universal hash function and two block cipher calls
- Beyond birthday bound security in faulty nonce model

Further research

- Tightness of security bounds
- Beyond birthday bound security of the tenth MAC algorithm
- MAC security

Conclusion

New results

- All PRFs based on two block cipher calls
- All MAC algorithms based on one universal hash function and two block cipher calls
- Beyond birthday bound security in faulty nonce model

Further research

- Tightness of security bounds
- Beyond birthday bound security of the tenth MAC algorithm
- MAC security

Thank you for your attention!