Encrypt or Decrypt? To Make a Single-Key BBB Secure Nonce-Based MAC

Nilanjan Datta\textsuperscript{1}, Avijit Dutta\textsuperscript{2}, Mridul Nandi\textsuperscript{2} and Kan Yasuda\textsuperscript{3}

1. Indian Institute of Technology, Kharagpur, India
2. Indian Statistical Institute, Kolkata, India
3. NTT Secure Platform Laboratories, NTT Corporation, Japan

CRYPTO, 2018
August 22, 2018
WC MAC [Wegman and Carter, JCSS 1981]
WC MAC [Wegman and Carter, JCSS 1981]

- Nonce Respecting (NR): $O(\epsilon q_v)$ security (Beyond the Birthday Bound)
- Nonce Misuse (NM): No security!!
EWC MAC [Cogliati and Seurin, CRYPTO 2016]

\[ M \rightarrow \mathcal{H}_{K_h} \]

\[ N \rightarrow F_K \rightarrow \oplus \rightarrow E_{K'} \rightarrow T \]
EWC MAC [Cogliati and Seurin, CRYPTO 2016]

**Nonce Respecting (NR):** Same security (Beyond the Birthday Bound)

**Nonce Misuse (NM):** Birthday Bound security
EWC MAC [Cogliati and Seurin, CRYPTO 2016]

- Nonce Respecting (NR): Same security (Beyond the Birthday Bound)
- Nonce Misuse (NM): Birthday Bound security

\[ F_K \rightarrow E_K \]: NR security drops to Birthday Bound!!
Towards Beyond Birthday Security
Towards Beyond Birthday Security

Can we reduce the number of BC calls?

N. Datta, A. Dutta, M. Nandi and K. Yasuda
Can we reduce the number of BC calls?
EWCDM MAC [Cogliati and Seurin, CRYPTO 2016]

Instantiation of $F_K$ by Keyed Davies-Meyer Construction
EWCDM MAC [Cogliati and Seurin, CRYPTO 2016]

MAC security: $2n/3$-bit (NR setting), $n/2$-bit (NM setting)
EWCDM MAC [Cogliati and Seurin, CRYPTO 2016]

$M \rightarrow \mathcal{H}_{K_h}$

$N \rightarrow E_K$

$E_K \rightarrow z \rightarrow E_{K'}$

$T$

**MAC security:** $2n/3$-bit (NR setting), $n/2$-bit (NM setting)

Conjecture of Cogliati and Seurin

- EWCDM is secure upto $\approx n$-bit (NR setting).
**EWCDM MAC [Cogliati and Seurin, CRYPTO 2016]**

\[
M \xrightarrow{H_{K_h}} \quad N \xrightarrow{E_K} \quad z \xrightarrow{E_{K'}} \quad T
\]

**MAC security**: $2n/3$-bit (NR setting), $n/2$-bit (NM setting)

**Conjecture of Cogliati and Seurin**

- Single keyed EWCDM (i.e. $K = K'$) is BBB Secure against NR adversaries.
Current Results on EWCDM

- [Mennink and Neves, CRYPTO 2016]: Optimal PRF security of EWCDM (NR setting)
- $n$-bit security of Mirror Theory: Unverifiable!!
- [Cogliati and Seurin, DCC 2018]: Difficulty of proving the security of single-keyed EWCDM
Outline

- Decrypted Wegman-Carter with Davies-Meyer (DWCDM)
  - Specification
  - Necessity of Nonce-space Reduction
- (Extended) Mirror Theory
  - Mirror Theory
  - Extended Mirror Theory
- Security of DWCDM
  - H-Coefficient Technique
  - Proof Approach
- 1K-DWCDM
Decrypted Wegman-Carter with Davies-Meyer (DWCDM)

- Single Keyed Nonce Based MAC (Nonce Space: $2n/3$ bits)
- MAC security: $2n/3$-bit (NR setting), $n/2$-bit (NM setting)

Assumptions on $\mathcal{H}$
- Regular, Almost XOR Universal
- 3-way regular (i.e., $\mathcal{H}(X_1) \oplus \mathcal{H}(X_2) \oplus \mathcal{H}(X_3) = Y (\neq 0)$)
Necessity of Nonce-space Reduction

\[ \begin{align*}
\Pi(x_1) \oplus \Pi(x_2) &= H_k(m) + x_1 \\
\Pi(x_2) \oplus \Pi(x_3) &= H_k(m) + x_2 \\
\Pi(x_3) \oplus \Pi(x_4) &= H_k(m) + x_3 \\
\Pi(x_4) \oplus \Pi(x_5) &= H_k(m) + x_4 \\
\Pi(x_5) \oplus \Pi(x_6) &= H_k(m) + x_5 \\
\Pi(x_6) \oplus \Pi(x_3) &= H_k(m) + x_6
\end{align*} \]
Necessity of Nonce-space Reduction

\[ \Pi(x_1) \oplus \Pi(x_2) = H_k(m) + x_1 \]
\[ \Pi(x_2) \oplus \Pi(x_3) = H_k(m) + x_2 \]
\[ \Pi(x_3) \oplus \Pi(x_4) = H_k(m) + x_3 \]
\[ \Pi(x_4) \oplus \Pi(x_5) = H_k(m) + x_4 \]
\[ \Pi(x_5) \oplus \Pi(x_6) = H_k(m) + x_5 \]
\[ \Pi(x_6) \oplus \Pi(x_3) = H_k(m) + x_6 \]

\[ x_3 + x_4 + x_5 + x_6 = 0 \]
Necessity of Nonce-space Reduction

\[
\begin{align*}
\Pi(x_1) \oplus \Pi(x_2) &= H_k(m) + x_1 \\
\Pi(x_2) \oplus \Pi(x_3) &= H_k(m) + x_2 \\
\Pi(x_3) \oplus \Pi(x_4) &= H_k(m) + x_3 \\
\Pi(x_4) \oplus \Pi(x_5) &= H_k(m) + x_4 \\
\Pi(x_5) \oplus \Pi(x_6) &= H_k(m) + x_5 \\
\Pi(x_6) \oplus \Pi(x_3) &= H_k(m) + x_6 \\
\end{align*}
\]

\[x_3 + x_4 + x_5 + x_6 = 0\]

Forcing Event

\((x_i + x_{i+1} + \cdots + x_j = 0) \Rightarrow (x_j, m, x_i)\) is a valid forgery.
Patarin’s Mirror Theory

A system of $q$ equations

\[ P_{n_1} \oplus P_{t_1} = \lambda_1 \]
\[ P_{n_2} \oplus P_{t_2} = \lambda_2 \]
\[ \vdots \]
\[ P_{n_q} \oplus P_{t_q} = \lambda_q \]
Patarin’s Mirror Theory

A system of $q$ equations

\[
P_{n_1} \oplus P_{t_1} = \lambda_1 \\
P_{n_2} \oplus P_{t_2} = \lambda_2 \\
\vdots \\
P_{n_q} \oplus P_{t_q} = \lambda_q
\]

$\phi : \{n_1, t_1, \ldots, n_q, t_q\} \rightarrow \{1, \ldots, r\}$ be a surjective index mapping function.
Patarin’s Mirror Theory

Equivalent reduced system of $q$ equations

\[
P_{\phi(n_1)} \oplus P_{\phi(t_1)} = \lambda_1 \\
P_{\phi(n_2)} \oplus P_{\phi(t_2)} = \lambda_2 \\
\vdots \\
P_{\phi(n_q)} \oplus P_{\phi(t_q)} = \lambda_q
\]

System of $q$ equations over $\mathcal{P} = \{P_1, \ldots, P_r\}$ variables.
Patarin’s Mirror Theory

Equivalent reduced system of $q$ equations

$$P_{\phi(n_1)} \oplus P_{\phi(t_1)} = \lambda_1$$
$$P_{\phi(n_2)} \oplus P_{\phi(t_2)} = \lambda_2$$
$$\vdots$$
$$P_{\phi(n_q)} \oplus P_{\phi(t_q)} = \lambda_q$$

System of $q$ equations over $\mathcal{P} = \{P_1, \ldots, P_r\}$ variables.

Goal of Mirror Theory

- Lower bound the number of solutions to $\mathcal{P}$ such that $P_a \neq P_b$ for $a \neq b \in \{1, \ldots, r\}$. 
Patarin’s Mirror Theory

System of Equations

- $r$ distinct unknowns
- System of equations: $P_{n_i} \oplus P_{t_i} = \lambda_i, i \in \{1, \ldots, q\}$
- Index mapping function $\phi : \{n_1, t_1, \ldots, n_q, t_q\} \rightarrow \{1, \ldots, r\}$
Patarin’s Mirror Theory

System of Equations

- $r$ distinct unknowns
- System of equations: $P_{n_i} \oplus P_{t_i} = \lambda_i, i \in \{1, \ldots, q\}$
- Index mapping function $\phi : \{n_1, t_1, \ldots, n_q, t_q\} \rightarrow \{1, \ldots, r\}$

Graph Based View

Circle

$P_{\phi(n_1)} = P_{\phi(n_2)}$

$P_{\phi(t_1)} = P_{\phi(n_3)}$  $P_{\phi(t_3)} = P_{\phi(t_2)}$
Patarin’s Mirror Theory

System of Equations

- $r$ distinct unknowns
- System of equations: $P_{n_i} \oplus P_{t_i} = \lambda_i, i \in \{1, \ldots, q\}$
- Index mapping function $\phi : \{n_1, t_1, \ldots, n_q, t_q\} \rightarrow \{1, \ldots, r\}$

Graph Based View

Circle

\[ P_{\phi(n_1)} = P_{\phi(n_2)} \]
\[ P_{\phi(t_1)} = P_{\phi(n_3)} \quad P_{\phi(t_3)} = P_{\phi(t_2)} \]

Degenerate

\[ P_{\phi(t_1)} = P_{\phi(n_3)} \quad P_{\phi(t_2)} = P_{\phi(t_3)} \]
\[ \lambda_1 + \lambda_2 \]
\[ \lambda_1 \]
\[ \lambda_2 \]
Main result (Mirror Theory)

If $G[\phi, \lambda]$ is (i) circle-free and (ii) non-degenerate for a fixed $\phi$ and $\lambda = (\lambda_1, \ldots, \lambda_q)$, then the distinct number of solutions is at least

$$\frac{(2^n)^r}{2^{nq}},$$

provided the maximum component size $\xi_{\text{max}}$ of $G[\phi, \lambda]$ satisfies $(\xi_{\text{max}} - 1)^2 \cdot r \leq 2^n / 67.$
Extended Mirror Theory

- Proof of Mirror theory: An inductive proof on the number of components
- Verifiable upto $3n/4$ bit security
- By definition, Mirror theory deals with a general system of equations and non-equations, however the treatment of non-equations has nowhere been found till date!!
Extended Mirror Theory

- Proof of Mirror theory: An inductive proof on the number of components
- Verifiable upto $3n/4$ bit security
- By definition, Mirror theory deals with a general system of equations and non-equations, however the treatment of non-equations has nowhere been found till date!!

Goal of Extended Mirror Theory

Lower bound on the distinct number of solutions of a system of bivariate affine equations with bivariate affine non-equations
Extended Mirror Theory

System of Equations and Non-Equations

- \( \mathcal{P} = \{P_1, \ldots, P_r\} \)
- \( P_{n_i} \oplus P_{t_i} = \lambda_i, \ i \in \{1, \ldots, q\}; \ P_{n_j} \oplus P_{t_j} = \tilde{\lambda}_j, j \in \{q+1, \ldots, q + v\} \)
- \( \phi : \{n_1, t_1, \ldots, n_q, t_q, n_{q+1}, t_{q+1}, \ldots, n_{q+v}, t_{q+v}\} \rightarrow \{1, \ldots, r\} \)

Circle, Degeneracy

Circle

\[ P_{\phi(n_1)} = P_{\phi(n_2)} \]

\[ P_{\phi(t_1)} = P_{\phi(n_3)} \quad P_{\phi(t_2)} = P_{\phi(t_3)} \]

Degenerate

\[ P_{\phi(n_1)} = P_{\phi(n_2)} \]

\[ P_{\phi(t_1)} = P_{\phi(n_3)} \quad P_{\phi(t_2)} = P_{\phi(t_3)} \]

\[ \lambda_1 + \lambda_2 \]

\[ \lambda_1 \quad \lambda_2 \]
Extended Mirror Theory

System of Equations and Non-Equations

- $\mathcal{P} = \{P_1, \ldots, P_r\}$
- $P_{n_i} \oplus P_{t_i} = \lambda_i, \ i \in \{1, \ldots, q\}; \ P_{n_j} \oplus P_{t_j} \neq \tilde{\lambda}_j, \ j \in \{q + 1, \ldots, q + v\}$
- $\phi : \{n_1, t_1, \ldots, n_q, t_q, n_{q+1}, t_{q+1}, \ldots, n_{q+v}, t_{q+v}\} \rightarrow \{1, \ldots, r\}$

Degeneracy-II

\[
\begin{align*}
P_{\phi(n_1)} \oplus P_{\phi(t_1)} &= \lambda_1 \\
P_{\phi(n_2)} \oplus P_{\phi(t_2)} &= \lambda_2 \\
P_{\phi(n_3)} \oplus P_{\phi(t_3)} &\neq \lambda_1 + \lambda_2
\end{align*}
\]
Extended Mirror Theory

System of Equations and Non-Equations

- $\mathcal{P} = \{P_1, \ldots, P_r\}$
- $P_{n_i} \oplus P_{t_i} = \lambda_i, i \in \{1, \ldots, q\}$; $P_{n_j} \oplus P_{t_j} \neq \tilde{\lambda}_j, j \in \{q+1, \ldots, q+v\}$
- $\phi : \{n_1, t_1, \ldots, n_q, t_q, n_{q+1}, t_{q+1}, \ldots, n_{q+v}, t_{q+v}\} \rightarrow \{1, \ldots, r\}$

Main result (Extended Mirror Theory)

If $G[\phi, \lambda']$ is (i) circle-free and (ii) non-degenerate of type-I and II for a fixed $\phi$ and $\lambda' = (\lambda_1, \ldots, \lambda_q, \lambda_{q+1}, \ldots, \lambda_{q+v})$, then the distinct number of solutions with $\xi_{\max} = 3$, is at least

$$\frac{(2^n)^{3q/2}}{2^{nq}} \left(1 - \frac{5q^3}{2^n} - \frac{v}{2^n}\right).$$
H-Coefficient Technique

\[ \text{Adv}_{\text{real}}(A) = | \Pr[A^{F_K, Ver_K} = 1] - \Pr[A^\$, \bot = 1] | \]
H-Coefficient Technique

\[ \text{Adv}_{\text{ideal}}(A) = | \Pr[A^{F_K, \text{Ver}_K} = 1] - \Pr[A^{\$, \bot} = 1] | \]

- Transcript: \( \tau = \tau_m \cup \tau_v \)
  - \( \tau_m = (((N_1, M_1, T_1), \ldots, (N_{q_m}, M_{q_m}, T_{q_m})) \)
  - \( \tau_v = (((N'_1, M'_1, T'_1, b_1), \ldots, (N'_{q_v}, M'_{q_v}, T'_{q_v}, b_{q_v})) \)

Real World

\( F_K \)

\( \text{Ver}_K \)

Ideal World

\( \$ \)

\( \bot \)

Diagram showing the relationship between the real and ideal worlds with the adversary \( A \).
H-Coefficient Technique

- $X_{re} :=$ probability distribution of transcript in real world.
- $X_{id} :=$ probability distribution of transcript in ideal world.
- $\mathcal{V} = \text{GoodT} \sqcup \text{BadT}$

Main Theorem (H-Coefficient Technique)

If there exists $\epsilon_{\text{ratio}}, \epsilon_{\text{bad}} \geq 0$ such that

(i) for all $\tau \in \text{GoodT}$, \[
\frac{\Pr[X_{re} = \tau]}{\Pr[X_{id} = \tau]} \geq 1 - \epsilon_{\text{ratio}}
\]

(ii) $\Pr[X_{id} \in \text{BadT}] \leq \epsilon_{\text{bad}}$,

then

$$\text{Adv}_{\text{ideal}}^\text{real}(A) \leq \epsilon_{\text{ratio}} + \epsilon_{\text{bad}}$$
An Overview of the Security Proof of DWCDM

MAC Equations

\[(E_m) = \begin{cases} 
\pi(N_1) \oplus \pi(T_1) = \lambda_1 \\
\pi(N_2) \oplus \pi(T_2) = \lambda_2 \\
\vdots \\
\pi(N_{qm}) \oplus \pi(T_{qm}) = \lambda_{qm} 
\end{cases}\]

Ver Equations

\[(E_v) = \begin{cases} 
\pi(N'_1) \oplus \pi(T'_1) \neq \lambda'_1 \\
\pi(N'_2) \oplus \pi(T'_2) \neq \lambda'_2 \\
\vdots \\
\pi(N'_{qv}) \oplus \pi(T'_{qv}) \neq \lambda'_{qv} 
\end{cases}\]

\[\lambda_i = N_i \oplus H_k(M_i), \quad \lambda'_i = N'_i \oplus H_k(M'_i)\]
An Overview of the Security Proof of DWCDM

MAC Equations

\[(E_m) = \begin{cases}
\prod(N_1) \oplus \prod(T_1) = \lambda_1 \\
\prod(N_2) \oplus \prod(T_2) = \lambda_2 \\
\vdots \\
\prod(N_{qm}) \oplus \prod(T_{qm}) = \lambda_{qm}
\end{cases}\]

Ver Equations

\[(E_v) = \begin{cases}
\prod(N'_1) \oplus \prod(T'_1) \neq \lambda'_1 \\
\prod(N'_2) \oplus \prod(T'_2) \neq \lambda'_2 \\
\vdots \\
\prod(N'_{qv}) \oplus \prod(T'_{qv}) \neq \lambda'_{qv}
\end{cases}\]

Bad Events

- (C.1) \( \lambda_i = 0 \)
- (C.2) \( \lambda_i = \lambda_j, T_i = T_j \) (Degeneracy-I)
- (C.3) \( N_i = T_j, \lambda_i = \lambda_j \) (Degeneracy-I)
- (C.4) \( T_i = 0 \)

### Bounds

- \( \Pr[C.1] \leq q_m \epsilon_{reg} \)
- \( \Pr[C.2] \leq q_m^2 \epsilon_{axu}/2^n \)
- \( \Pr[C.3] \leq q_m \epsilon_{axu}/2^{n/3} \)
- \( \Pr[C.4] \leq q_m/2^n \)
An Overview of the Security Proof of DWCDM

(C.5) Component Size of MAC Graph is 3

\[ T_i = T_j = T_k \]

\[ T_i = T_j = N_k \]

\[ N_i = T_j, N_j = T_k \]
An Overview of the Security Proof of DWCDM

(C.5) Component Size of MAC Graph is 3

\[ T_i = T_j = T_k \]

(C.6) Circle in MAC Graph

(Self Loop) (Parallel Edge)
An Overview of the Security Proof of DWCDM

(C.5) Component Size of MAC Graph is 3

\[ T_i = T_j = T_k \]

(C.6) Circle in MAC Graph

\[ N_i = T_j, N_j = T_k \]

Bounds

\[ \Pr[C.5] \leq \frac{q_m}{2^{2n/3}} \]
\[ \Pr[C.6] \leq \frac{q_m}{2^{2n/3}} \]
An Overview of the Security Proof of DWCDM

(C.7) Circle in Verification Graph:

(A) Cycle of length two

\[ N'_a = T_a \quad N'_a = N_i, \quad T'_a = T_i \quad N'_a = T_i, \quad T'_a = N_i \]

(B) Cycle of length three

Bound \( \Pr[C.7] \leq \max\{2q_v \epsilon_{3\text{-reg}}, 2q_v \epsilon_{axu}, q_v \epsilon_{\text{reg}}, q_m/2^{2n/3}\} \)
An Overview of the Security Proof of DWCDM

Summarize

- $\epsilon_{\text{bad}} \approx O(q_m/2^{2n/3})$
- $\epsilon_{\text{good}} = \frac{5q_m^3}{2^{2n}} + \frac{q_v}{2^n}$ (From Extended Mirror Theory)

MAC security of DWCDM

\[
\text{Adv}(A) \leq O(q_m/2^{2n/3}) + q_v/2^n
\]
A Glimpse of Pure 1K-DWCDM

- Derive the hash key as $E_K(0^{n-1} 1)$
- Security proof: Consider uni-variate non-equations as well
- Provides same level of security of DWCDM
A Glimpse of Pure 1K-DWCDM

- Derive the hash key as $E_K(0^{n-1}1)$
- Security proof: Consider uni-variate non-equations as well
- Provides same level of security of DWCDM

Our Conjecture

DWCDM can be proven secured upto $3n/4$ bit with $n - 1$ bits of nonce space
Thank You..!!!