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

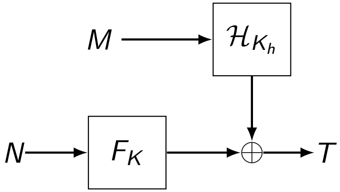
Nilanjan Datta [1], Avijit Dutta [2], Mridul Nandi [2] and Kan Yasuda [3]

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

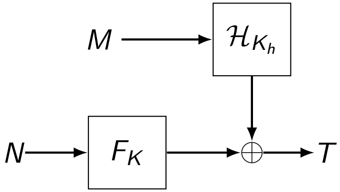
CRYPTO, 2018

August 22, 2018

WC MAC [Wegman and Carter, JCSS 1981]

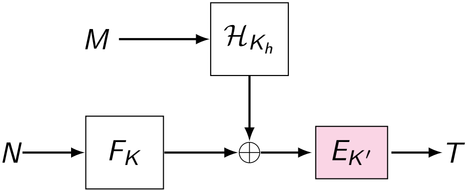


WC MAC [Wegman and Carter, JCSS 1981]

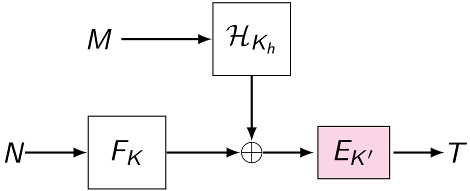


- Nonce Respecting (NR): $O(\epsilon q_v)$ security (Beyond the Birthday Bound)
- Nonce Misuse (NM): No security !!

EWC MAC [Cogliati and Seurin, CRYPTO 2016]

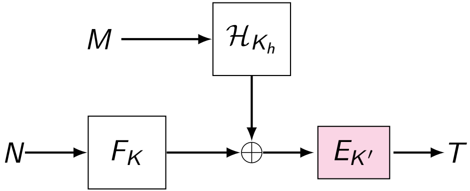


EWC MAC [Cogliati and Seurin, CRYPTO 2016]



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

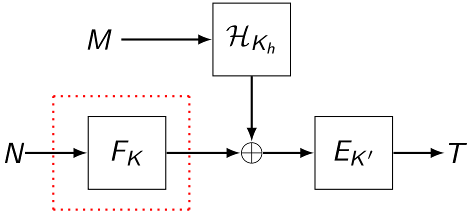
EWC MAC [Cogliati and Seurin, CRYPTO 2016]



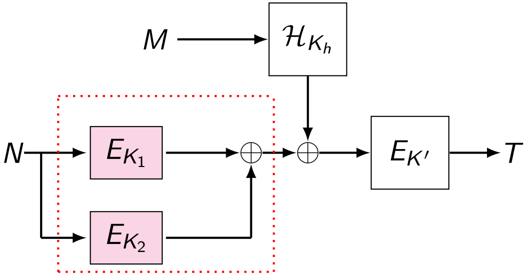
- Nonce Respecting (NR): Same security (Beyond the Birthday Bound)
- Nonce Misuse (NM): Birthday Bound security

$F_K \rightarrow E_K$: NR security drops to Birthday Bound!!

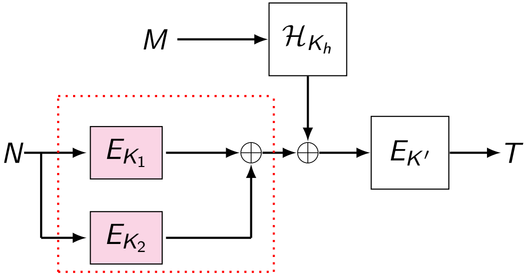
Towards Beyond Birthday Security



Towards Beyond Birthday Security

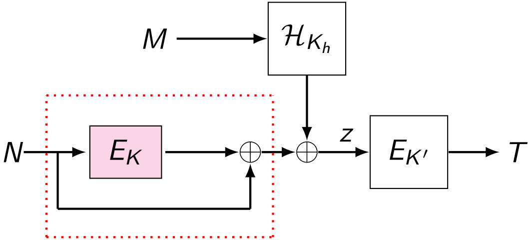


Towards Beyond Birthday Security



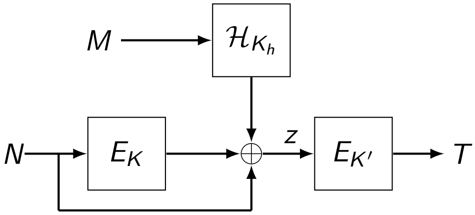
Can we reduce the number of BC calls?

EWCDM MAC [Cogliati and Seurin, CRYPTO 2016]



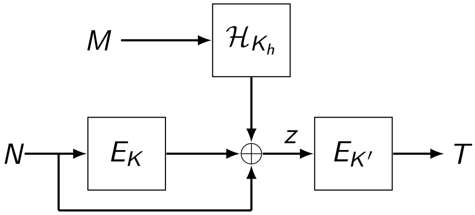
Instantiation of F_K by Keyed Davies-Meyer Construction

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]

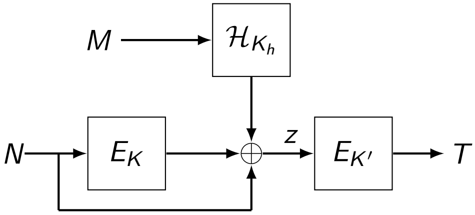


MAC security: $2n/3$-bit (NR setting), $n/2$-bit (NM setting)

Conjecture of Cogliati and Seurin

- EWCDM is secure upto $\approx n$-bit (NR setting).

EWCDM MAC [Cogliati and Seurin, CRYPTO 2016]



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.

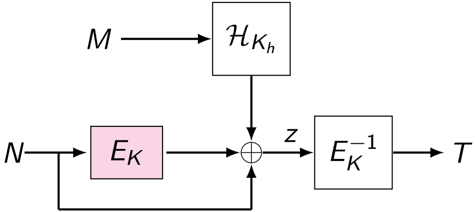
Current Results on EWCDM

- [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 wth 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)

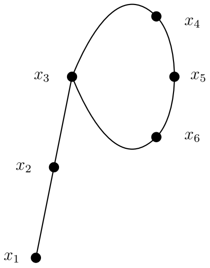


- Single Keyed Nonce Based MAC (Nonce Space: $2n/3$ bits)
- MAC security: $2n/3$-bit (NR setting), $n/2$-bit (NM setting)

Assumptions on $\mathcal{H}$

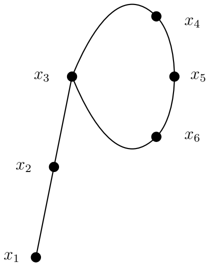
- Regular, Almost XOR Universal
- 3-way regular (i.e., $\mathcal{H}(X_1) \oplus \mathcal{H}(X_2) \oplus \mathcal{H}(X_3) = Y(\neq 0)$)

Necessity of Nonce-space Reduction



$$
\begin{aligned}
\Pi(x_1) \oplus \Pi(x_2) &= H_k(m) + x_1 \\
\Pi(x_2) \oplus \Pi(x_3) &= H_k(m) + x_2 \\
\Pi(x_3) \oplus \Pi(x_4) &= H_k(m) + x_3 \\
\Pi(x_4) \oplus \Pi(x_5) &= H_k(m) + x_4 \\
\Pi(x_5) \oplus \Pi(x_6) &= H_k(m) + x_5 \\
\Pi(x_6) \oplus \Pi(x_3) &= H_k(m) + x_6
\end{aligned}
$$

Necessity of Nonce-space Reduction

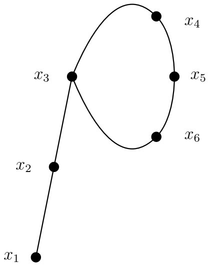


$$
\begin{aligned}
\Pi(x_1) \oplus \Pi(x_2) &= H_k(m) + x_1\\
\Pi(x_2) \oplus \Pi(x_3) &= H_k(m) + x_2\\
\Pi(x_3) \oplus \Pi(x_4) &= H_k(m) + x_3\\
\Pi(x_4) \oplus \Pi(x_5) &= H_k(m) + x_4\\
\Pi(x_5) \oplus \Pi(x_6) &= H_k(m) + x_5\\
\Pi(x_6) \oplus \Pi(x_3) &= H_k(m) + x_6
\end{aligned}
$$

$$\Updownarrow$$

$$\boxed{x_3 + x_4 + x_5 + x_6 = 0}$$

Necessity of Nonce-space Reduction



$$
\begin{aligned}
\Pi(x_1) \oplus \Pi(x_2) &= H_k(m) + x_1 \\
\Pi(x_2) \oplus \Pi(x_3) &= H_k(m) + x_2 \\
\Pi(x_3) \oplus \Pi(x_4) &= H_k(m) + x_3 \\
\Pi(x_4) \oplus \Pi(x_5) &= H_k(m) + x_4 \\
\Pi(x_5) \oplus \Pi(x_6) &= H_k(m) + x_5 \\
\Pi(x_6) \oplus \Pi(x_3) &= H_k(m) + x_6
\end{aligned}
$$

$$\Updownarrow$$

$$\boxed{x_3 + x_4 + x_5 + x_6 = 0}$$

Forging 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

$$
\begin{aligned}
P_{n_1} \oplus P_{t_1} &= \lambda_1 \\
P_{n_2} \oplus P_{t_2} &= \lambda_2 \\
&\vdots \\
P_{n_q} \oplus P_{t_q} &= \lambda_q
\end{aligned}
$$

Patarin's Mirror Theory

A system of q equations

$$
\begin{aligned}
P_{n_1} \oplus P_{t_1} &= \lambda_1 \\
P_{n_2} \oplus P_{t_2} &= \lambda_2 \\
&\vdots \\
P_{n_q} \oplus P_{t_q} &= \lambda_q
\end{aligned}
$$

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

Patarin's Mirror Theory

Equivalent reduced system of q equations

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

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

Patarin's Mirror Theory

Equivalent reduced system of q equations

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

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 $\phi : \{n_1, t_1, \ldots, n_q, t_q\} \to \{1, \ldots, r\}$

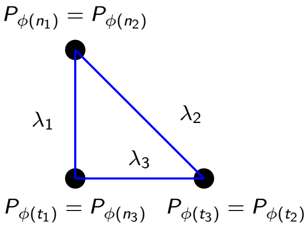
Patarin's Mirror Theory

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



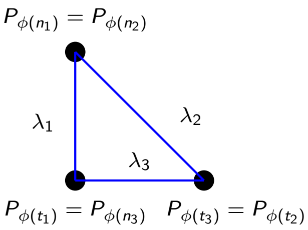
Patarin's Mirror Theory

System of Equations

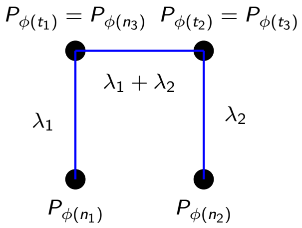
- r distinct unknowns
- System of equations: $P_{n_i} \oplus P_{t_i} = \lambda_i, i \in \{1, \ldots, q\}$
- Index mapping function $\phi : \{n_1, t_1, \ldots, n_q, t_q\} \rightarrow \{1, \ldots, r\}$

Graph Based View

Circle



Degenerate



Patarin's Mirror Theory

Main result (Mirror Theory)

If $G[\phi, \lambda]$ is (i) circle-free and (ii) non-degenerate for a fixed ϕ 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 $\xi_{\max}$ of $G[\phi, \lambda]$ satisfies $(\xi_{\max} - 1)^2 \cdot r \leq 2^n/67$.

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

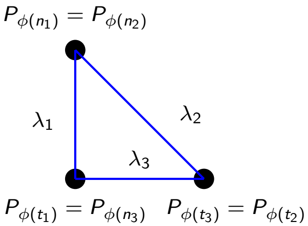
Extended Mirror Theory

System of Equations and Non-Equations

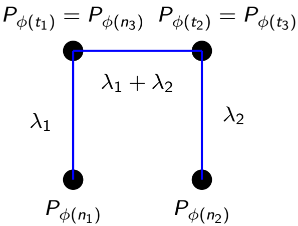
- $\mathcal{P} = \{P_1, \ldots, P_r\}$
- $P_{n_i} \oplus P_{t_i} = \lambda_i, i \in \{1, \ldots, q\}; P_{n_j} \oplus P_{t_j} \neq \widetilde{\lambda}_j, j \in \{q+1, \ldots, q+v\}$
- $\phi : \{n_1, t_1, \ldots, n_q, t_q, n_{q+1}, t_{q+1}, \ldots, n_{q+v}, t_{q+v}\} \rightarrow \{1, \ldots, r\}$

Circle, Degeneracy

Circle



Degenerate



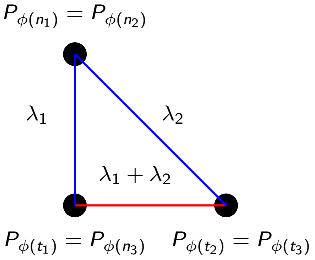
Extended Mirror Theory

System of Equations and Non-Equations

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

Degeneracy-II

$$\begin{aligned} P_{\phi(n_1)} \oplus P_{\phi_{t_1}} &= \lambda_1 \\ P_{\phi(n_2)} \oplus P_{\phi_{t_2}} &= \lambda_2 \\ P_{\phi(n_3)} \oplus P_{\phi_{t_3}} &\neq \lambda_1 + \lambda_2 \end{aligned}$$



Extended Mirror Theory

System of Equations and Non-Equations

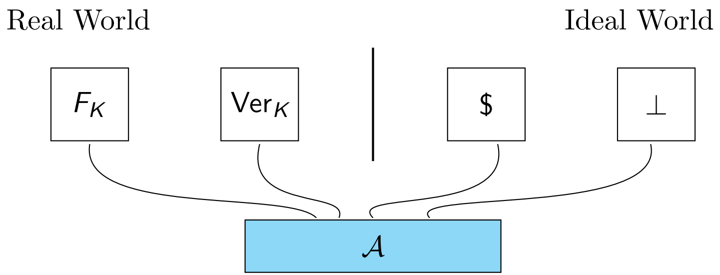
- $\mathcal{P} = \{P_1, \ldots, P_r\}$
- $P_{n_i} \oplus P_{t_i} = \lambda_i, i \in \{1, \ldots, q\}; P_{n_j} \oplus P_{t_j} \neq \widetilde{\lambda}_j, j \in \{q+1, \ldots, q+v\}$
- $\phi : \{n_1, t_1, \ldots, n_q, t_q, n_{q+1}, t_{q+1}, \ldots, n_{q+v}, t_{q+v}\} \to \{1, \ldots, r\}$

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 ϕ and $\lambda' = (\lambda_1, \ldots, \lambda_q, \widetilde{\lambda_{q+1}}, \ldots, \widetilde{\lambda_{q+v}})$, then the distinct number of solutions with $\xi_{\max} = 3$, is at least

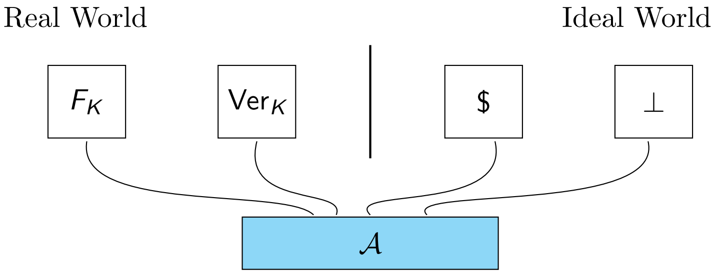
$$\frac{(2^n)_{3q/2}}{2^{nq}}(1 - \frac{5q^3}{2^{2n}} - \frac{v}{2^n}).$$

H-Coefficient Technique



$$\mathbf{Adv}^{\mathrm{real}}_{\mathrm{ideal}}(\mathcal{A}) = \mid \ \Pr[\mathcal{A}^{F_K, \mathsf{Ver}_K} = 1] - \Pr[\mathcal{A}^{\$, \perp} = 1] \mid$$

H-Coefficient Technique



$$\mathbf{Adv}^{\mathrm{real}}_{\mathrm{ideal}}(\mathcal{A}) = \mid \Pr[\mathcal{A}^{F_K, \mathsf{Ver}_K} = 1] - \Pr[\mathcal{A}^{\$, \perp} = 1] \mid$$

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

H-Coefficient Technique

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

Main Theorm (H-Coefficient Technique)

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

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

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

then

$$\mathbf{Adv}^{\mathrm{real}}_{\mathrm{ideal}}(\mathcal{A}) \leq \epsilon_{\mathrm{ratio}} + \epsilon_{\mathrm{bad}}$$

An Overview of the Security Proof of DWCDM

MAC Equations

$$(\mathcal{E}_m) = \begin{cases} \Pi(N_1) \oplus \Pi(T_1) = \lambda_1 \\ \Pi(N_2) \oplus \Pi(T_2) = \lambda_2 \\ \vdots \\ \Pi(N_{q_m}) \oplus \Pi(T_{q_m}) = \lambda_{q_m} \end{cases}$$

Ver Equations

$$(\mathcal{E}_v) = \begin{cases} \Pi(N'_1) \oplus \Pi(T'_1) \neq \lambda'_1 \\ \Pi(N'_2) \oplus \Pi(T'_2) \neq \lambda_2 \\ \vdots \\ \Pi(N'_{q_v}) \oplus \Pi(T'_{q_v}) \neq \lambda'_{q_v} \end{cases}$$

$$\boxed{\lambda_i = N_i \oplus H_k(M_i), \quad \lambda'_i = N'_i \oplus H_k(M'_i)}$$

An Overview of the Security Proof of DWCDM

MAC Equations

$$(\mathcal{E}_m) = \begin{cases} \Pi(N_1) \oplus \Pi(T_1) = \lambda_1 \\ \Pi(N_2) \oplus \Pi(T_2) = \lambda_2 \\ \vdots \\ \Pi(N_{q_m}) \oplus \Pi(T_{q_m}) = \lambda_{q_m} \end{cases}$$

Ver Equations

$$(\mathcal{E}_v) = \begin{cases} \Pi(N'_1) \oplus \Pi(T'_1) \neq \lambda'_1 \\ \Pi(N'_2) \oplus \Pi(T'_2) \neq \lambda_2 \\ \vdots \\ \Pi(N'_{q_v}) \oplus \Pi(T'_{q_v}) \neq \lambda'_{q_v} \end{cases}$$

$$\boxed{\lambda_i = N_i \oplus H_k(M_i), \quad \lambda'_i = N'_i \oplus H_k(M'_i)}$$

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

$\Pr[C.1] \leq q_m \epsilon_{\mathrm{reg}}$

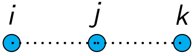
$\Pr[C.2] \leq q_m^2 \epsilon_{\mathrm{axu}}/2^n$

$\Pr[C.3] \leq q_m \epsilon_{\mathrm{axu}}/2^{n/3}$

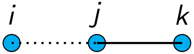
$\Pr[C.4] \leq q_m/2^n$

An Overview of the Security Proof of DWCDM

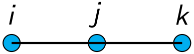
(C.5) Component Size of MAC Graph is 3



$$T_i = T_j = T_k$$



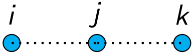
$$T_i = T_j = N_k$$



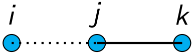
$$N_i = T_j, N_j = T_k$$

An Overview of the Security Proof of DWCDM

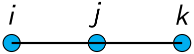
(C.5) Component Size of MAC Graph is 3



$T_i = T_j = T_k$



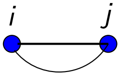
$T_i = T_j = N_k$



$N_i = T_j, N_j = T_k$

(C.6) Circle in MAC Graph

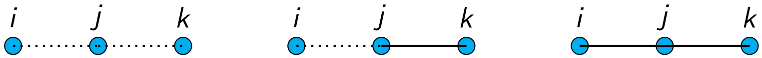
(Self Loop)



(Parallel Edge)

An Overview of the Security Proof of DWCDM

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



$T_i = T_j = T_k$ $\qquad$ $T_i = T_j = N_k$ $\qquad$ $N_i = T_j, N_j = T_k$

(C.6) Circle in MAC Graph

(Self Loop) $\qquad$ (Parallel Edge)

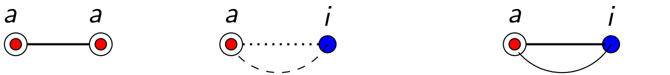
Bounds $\qquad \Pr[C.5] \leq q_m/2^{2n/3} \qquad \Pr[C.6] \leq q_m/2^{2n/3}$

 Security Proof of DWCDM

An Overview of the Security Proof of DWCDM

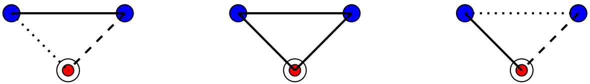
(C.7) Circle in Verification Graph:

(A) Cycle of length two



$N'_a = T_a$ $\qquad$ $N'_a = N_i,\ T'_a = T_i$ $\qquad$ $N'_a = T_i,\ T'_a = N_i$

(B) Cycle of length three



Bound $\qquad \Pr[\text{C.7}] \le \max\{2q_v\epsilon_{\text{3-reg}}, 2q_v\epsilon_{\text{axu}}, q_v\epsilon_{\text{reg}}, q_m/2^{2n/3}\}$

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

$$\mathbf{Adv}(\mathcal{A}) \leq O(q_m/2^{2n/3}) + q_v/2^n$$

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

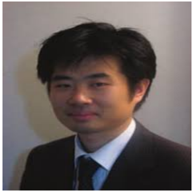
A Glimpse of Pure 1K-DWCDM

- 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..!!!