Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory

Bart Mennink, Samuel Neves

Radboud University (The Netherlands),
University of Coimbra (Portugal)

CRYPTO 2017

August 24, 2017

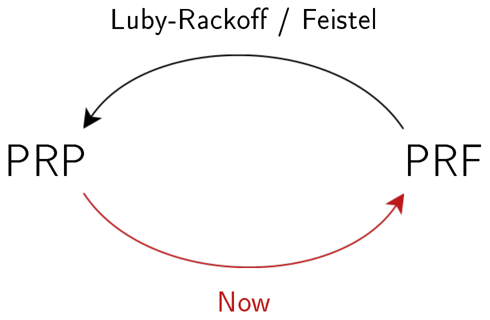
Introduction

PRP PRF

Introduction

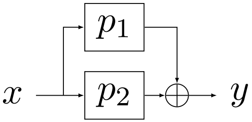
$$\begin{tikzcd} \text{PRP} & \text{PRF} \arrow[l, bend right, "\text{Luby-Rackoff / Feistel}"'] \end{tikzcd}$$

Introduction



Xor of Permutations

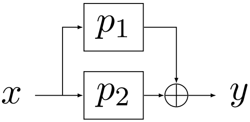
Xor of Permutations



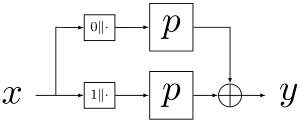
- First suggested by Bellare et al. [BKR98]
- Secure up to 2^n queries [Bl99,Luc00,Pat08]
- Application: CENC, SCT

Xor of Permutations

Xor of Permutations



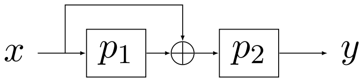
Xor of Single Permutation



- First suggested by Bellare et al. [BKR98]
- Secure up to 2^n queries [Bl99,Luc00,Pat08]
- Application: CENC, SCT
- Single permutation using domain separation

Encrypted (Wegman-Carter) Davies-Meyer

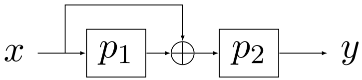
EDM



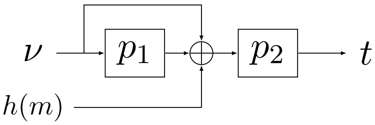
- By Cogliati and Seurin [CS16]
- Secure up to $2^{2n/3}$ queries
- Conjecture: optimal 2^n security

Encrypted (Wegman-Carter) Davies-Meyer

EDM



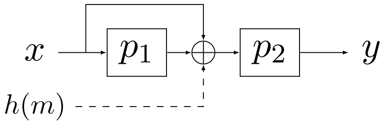
EWCDM



- By Cogliati and Seurin [CS16]
- Secure up to $2^{2n/3}$ queries
- Conjecture: optimal 2^n security
- Message authentication using EWCDM

Our Contribution

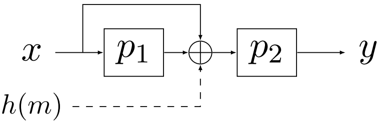
EDM and EWCDM (dashed)



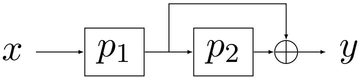
scheme	[CS16]	now
EDM	$2^{2n/3}$	$2^n/n$
EWCDM	$2^{2n/3}$	$2^n/n$

Our Contribution

EDM and EWCDM (dashed)



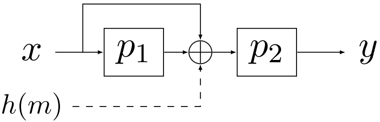
EDMD



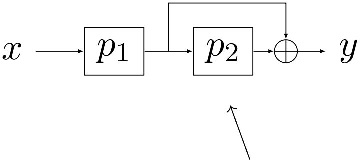
scheme	[CS16]	now
EDM	$2^{2n/3}$	$2^n/n$
EWCDM	$2^{2n/3}$	$2^n/n$
EDMD	——	2^n

Our Contribution

EDM and EWCDM (dashed)



EDMD

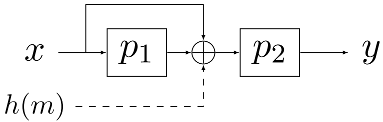


Earlier proposal
EWCDMD removed after
observation by Nandi

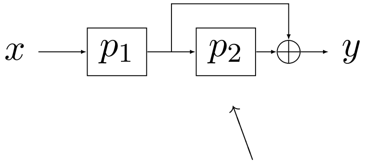
scheme	[CS16]	now
EDM	$2^{2n/3}$	$2^n/n$
EWCDM	$2^{2n/3}$	$2^n/n$
EDMD	——	2^n

Our Contribution

EDM and EWCDM (dashed)



EDMD



Earlier proposal
EWCDMD removed after
observation by Nandi

scheme	[CS16]	now
EDM	$2^{2n/3}$	$2^n/n$
EWCDM	$2^{2n/3}$	$2^n/n$
EDMD	——	2^n

Backbone of analysis: mirror theory

Mirror Theory

System of Equations

- Consider r distinct unknowns $\mathcal{P} = \{P_1, \ldots, P_r\}$
- Consider a system of q equations of the form:

$$\begin{aligned} P_{a_1} \oplus P_{b_1} &= \lambda_1 \\ P_{a_2} \oplus P_{b_2} &= \lambda_2 \\ &\vdots \\ P_{a_q} \oplus P_{b_q} &= \lambda_q \end{aligned}$$

for some surjection $\varphi : \{a_1, b_1, \ldots, a_q, b_q\} \to \{1, \ldots, r\}$

Mirror Theory

System of Equations

- Consider r distinct unknowns $\mathcal{P} = \{P_1, \dots, P_r\}$
- Consider a system of q equations of the form:

$$\begin{aligned} P_{a_1} \oplus P_{b_1} &= \lambda_1 \\ P_{a_2} \oplus P_{b_2} &= \lambda_2 \\ &\vdots \\ P_{a_q} \oplus P_{b_q} &= \lambda_q \end{aligned}$$

for some surjection $\varphi : \{a_1, b_1, \dots, a_q, b_q\} \to \{1, \dots, r\}$

Goal

- Lower bound on the number of solutions to $\mathcal{P}$ such that $P_a \neq P_b$ for all distinct $a, b \in \{1, \dots, r\}$

Mirror Theory

Patarin's Result

- Extremely powerful lower bound

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	
Patarin	ICITS 2008	XoP	

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	
Patarin	ICITS 2008	XoP	
Patarin	AFRICACRYPT 2008	Benes	

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	
Patarin	ICITS 2008	XoP	
Patarin	AFRICACRYPT 2008	Benes	
Patarin	ePrint 2010/287	XoP	Concrete bound

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	
Patarin	ICITS 2008	XoP	
Patarin	AFRICACRYPT 2008	Benes	
Patarin	ePrint 2010/287	XoP	Concrete bound
Patarin	ePrint 2010/293	Feistel	

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	
Patarin	ICITS 2008	XoP	
Patarin	AFRICACRYPT 2008	Benes	
Patarin	ePrint 2010/287	XoP	Concrete bound
Patarin	ePrint 2010/293	Feistel	
Patarin	ePrint 2013/368	XoP	

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	
Patarin	ICITS 2008	XoP	
Patarin	AFRICACRYPT 2008	Benes	
Patarin	ePrint 2010/287	XoP	Concrete bound
Patarin	ePrint 2010/293	Feistel	
Patarin	ePrint 2013/368	XoP	
Cogliati, Lampe, Patarin	FSE 2014	XoP^d	

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	
Patarin	ICITS 2008	XoP	
Patarin	AFRICACRYPT 2008	Benes	
Patarin	ePrint 2010/287	XoP	Concrete bound
Patarin	ePrint 2010/293	Feistel	
Patarin	ePrint 2013/368	XoP	
Cogliati, Lampe, Patarin	FSE 2014	XoP^d	
Volte, Nachef, Marrière	ePrint 2016/136	Feistel	

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

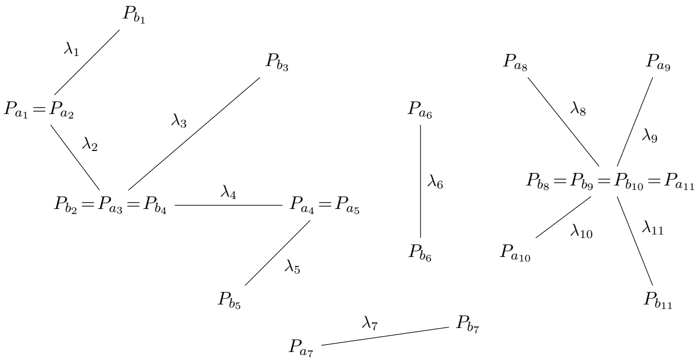
Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	
Patarin	ICITS 2008	XoP	
Patarin	AFRICACRYPT 2008	Benes	
Patarin	ePrint 2010/287	XoP	Concrete bound
Patarin	ePrint 2010/293	Feistel	
Patarin	ePrint 2013/368	XoP	
Cogliati, Lampe, Patarin	FSE 2014	XoP^d	
Volte, Nachef, Marrière	ePrint 2016/136	Feistel	
Iwata, Mennink, Vizár	ePrint 2016/1087	CENC	

Mirror Theory

System of Equations

- r distinct unknowns $\mathcal{P} = \{P_1, \ldots, P_r\}$
- System of equations $P_{a_i} \oplus P_{b_i} = \lambda_i$
- Surjection $\varphi : \{a_1, b_1, \ldots, a_q, b_q\} \to \{1, \ldots, r\}$

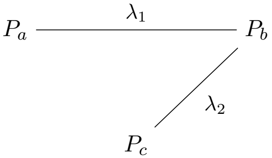
Graph Based View



Mirror Theory: Toy Example 1

- System of equations:

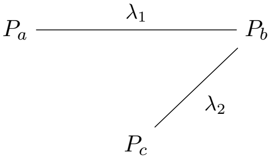
$$P_a \oplus P_b = \lambda_1$$
$$P_b \oplus P_c = \lambda_2$$



Mirror Theory: Toy Example 1

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_b \oplus P_c = \lambda_2$$



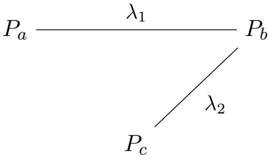
If $\lambda_1 = 0$ or $\lambda_2 = 0$ or $\lambda_1 = \lambda_2$

- Contradiction: $P_a = P_b$ or $P_b = P_c$ or $P_a = P_c$
- Scheme is degenerate

Mirror Theory: Toy Example 1

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_b \oplus P_c = \lambda_2$$



If $\lambda_1 = 0$ or $\lambda_2 = 0$ or $\lambda_1 = \lambda_2$

- Contradiction: $P_a = P_b$ or $P_b = P_c$ or $P_a = P_c$
- Scheme is degenerate

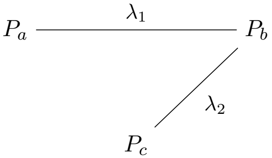
If $\lambda_1, \lambda_2 \neq 0$ and $\lambda_1 \neq \lambda_2$

- 2^n choices for P_a

Mirror Theory: Toy Example 1

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_b \oplus P_c = \lambda_2$$



If $\lambda_1 = 0$ or $\lambda_2 = 0$ or $\lambda_1 = \lambda_2$

- Contradiction: $P_a = P_b$ or $P_b = P_c$ or $P_a = P_c$
- Scheme is degenerate

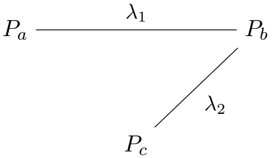
If $\lambda_1, \lambda_2 \neq 0$ and $\lambda_1 \neq \lambda_2$

- 2^n choices for P_a
- Fixes $P_b = \lambda_1 \oplus P_a$ (which is $\neq P_a$ as desired)

Mirror Theory: Toy Example 1

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_b \oplus P_c = \lambda_2$$



If $\lambda_1 = 0$ or $\lambda_2 = 0$ or $\lambda_1 = \lambda_2$

- Contradiction: $P_a = P_b$ or $P_b = P_c$ or $P_a = P_c$
- Scheme is degenerate

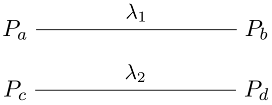
If $\lambda_1, \lambda_2 \neq 0$ and $\lambda_1 \neq \lambda_2$

- 2^n choices for P_a
- Fixes $P_b = \lambda_1 \oplus P_a$ (which is $\neq P_a$ as desired)
- Fixes $P_c = \lambda_2 \oplus P_b$ (which is $\neq P_a, P_b$ as desired)

Mirror Theory: Toy Example 2

- System of equations:

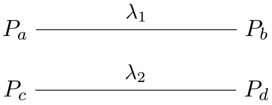
$$P_a \oplus P_b = \lambda_1$$
$$P_c \oplus P_d = \lambda_2$$



Mirror Theory: Toy Example 2

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_c \oplus P_d = \lambda_2$$



If $\boldsymbol{\lambda_1 = 0}$ or $\boldsymbol{\lambda_2 = 0}$

- Contradiction: $P_a = P_b$ or $P_b = P_c$
- Scheme is degenerate

Mirror Theory: Toy Example 2

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_c \oplus P_d = \lambda_2$$

$$\begin{tikzcd} P_a \arrow[rrr, dash, "\lambda_1"] & & & P_b \\ P_c \arrow[rrr, dash, "\lambda_2"] & & & P_d \end{tikzcd}$$

If $\boldsymbol{\lambda_1 = 0}$ or $\boldsymbol{\lambda_2 = 0}$

- Contradiction: $P_a = P_b$ or $P_b = P_c$
- Scheme is degenerate

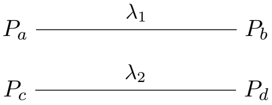
If $\boldsymbol{\lambda_1, \lambda_2 \neq 0}$

- 2^n choices for P_a (which fixes P_b)

Mirror Theory: Toy Example 2

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_c \oplus P_d = \lambda_2$$



If $\lambda_1 = 0$ or $\lambda_2 = 0$

- Contradiction: $P_a = P_b$ or $P_b = P_c$
- Scheme is degenerate

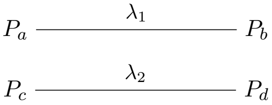
If $\lambda_1, \lambda_2 \neq 0$

- 2^n choices for P_a (which fixes P_b)
- For P_c and P_d we require
  - $P_c \neq P_a, P_b$
  - $P_d = \lambda_2 \oplus P_c \neq P_a, P_b$

Mirror Theory: Toy Example 2

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_c \oplus P_d = \lambda_2$$



If $\lambda_1 = 0$ or $\lambda_2 = 0$

- Contradiction: $P_a = P_b$ or $P_b = P_c$
- Scheme is degenerate

If $\lambda_1, \lambda_2 \neq 0$

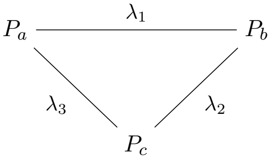
- 2^n choices for P_a (which fixes P_b)
- For P_c and P_d we require
  - $P_c \neq P_a, P_b$
  - $P_d = \lambda_2 \oplus P_c \neq P_a, P_b$
- At least $2^n - 4$ choices for P_c (which fixes P_d)

Mirror Theory: Toy Example 3

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_b \oplus P_c = \lambda_2$$
$$P_c \oplus P_a = \lambda_3$$

- Assume $\lambda_i \neq 0$ and $\lambda_i \neq \lambda_j$

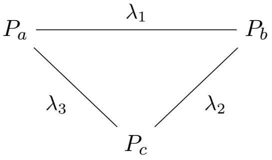


Mirror Theory: Toy Example 3

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_b \oplus P_c = \lambda_2$$
$$P_c \oplus P_a = \lambda_3$$

- Assume $\lambda_i \neq 0$ and $\lambda_i \neq \lambda_j$

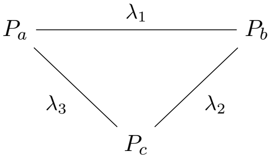


If $\boldsymbol{\lambda_1 \oplus \lambda_2 \oplus \lambda_3 \neq 0}$

- Contradiction: equations sum to $0 = \lambda_1 \oplus \lambda_2 \oplus \lambda_3$
- Scheme contains a circle

Mirror Theory: Toy Example 3

- System of equations:
$$P_a \oplus P_b = \lambda_1$$
$$P_b \oplus P_c = \lambda_2$$
$$P_c \oplus P_a = \lambda_3$$
- Assume $\lambda_i \neq 0$ and $\lambda_i \neq \lambda_j$



If $\boldsymbol{\lambda_1 \oplus \lambda_2 \oplus \lambda_3 \neq 0}$

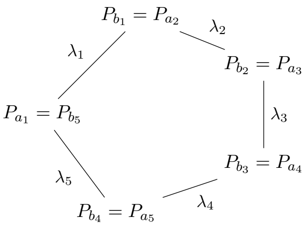
- Contradiction: equations sum to $0 = \lambda_1 \oplus \lambda_2 \oplus \lambda_3$
- Scheme contains a circle

If $\boldsymbol{\lambda_1 \oplus \lambda_2 \oplus \lambda_3 = 0}$

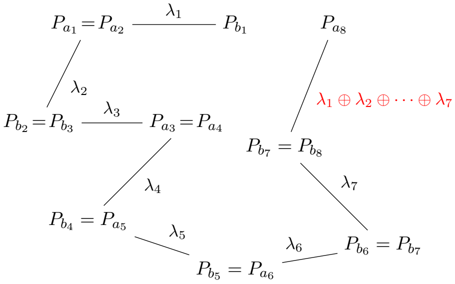
- One redundant equation, no contradiction

Mirror Theory: Two Problematic Cases

Circle



Degeneracy



Mirror Theory: Main Result

System of Equations

- r distinct unknowns $\mathcal{P} = \{P_1, \ldots, P_r\}$
- System of equations $P_{a_i} \oplus P_{b_i} = \lambda_i$
- Surjection $\varphi : \{a_1, b_1, \ldots, a_q, b_q\} \to \{1, \ldots, r\}$

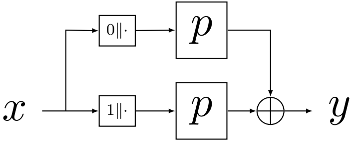
Main Result

If the system of equations is circle-free and non-degenerate, the number of solutions to $\mathcal{P}$ such that $P_a \neq P_b$ for all distinct $a, b \in \{1, \ldots, r\}$ is at least

$$\frac{(2^n)_r}{2^{nq}}$$

provided the maximum tree size ξ satisfies $(\xi - 1)^2 \cdot r \leq 2^n/67$

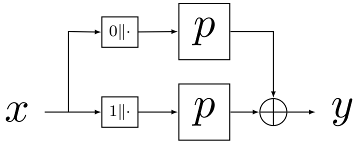
Mirror Theory Applied to XoP



General Setting

- Adversary gets transcript $\tau = \{(x_1, y_1), \ldots, (x_q, y_q)\}$

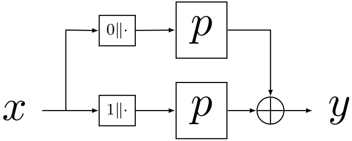
Mirror Theory Applied to XoP



General Setting

- Adversary gets transcript $\tau = \{(x_1, y_1), \ldots, (x_q, y_q)\}$
- Each tuple corresponds to $x_i \mapsto p(0\|x_i) =: P_{a_i}$ and
  $x_i \mapsto p(1\|x_i) =: P_{b_i}$

Mirror Theory Applied to XoP

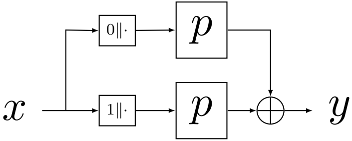


General Setting

- Adversary gets transcript $\tau = \{(x_1, y_1), \ldots, (x_q, y_q)\}$
- Each tuple corresponds to $x_i \mapsto p(0\|x_i) =: P_{a_i}$ and

  $x_i \mapsto p(1\|x_i) =: P_{b_i}$
- System of q equations $P_{a_i} \oplus P_{b_i} = y_i$

Mirror Theory Applied to XoP



General Setting

- Adversary gets transcript $\tau = \{(x_1, y_1), \dots, (x_q, y_q)\}$
- Each tuple corresponds to $x_i \mapsto p(0\|x_i) =: P_{a_i}$ and
  $x_i \mapsto p(1\|x_i) =: P_{b_i}$
- System of q equations $P_{a_i} \oplus P_{b_i} = y_i$
- Inputs to p are all distinct: $2q$ unknowns

Mirror Theory Applied to XoP

$$\begin{tikzcd}
P_{a_1} \arrow[d, dash, "y_1"] & P_{a_2} \arrow[d, dash, "y_2"] & \cdots & P_{a_q} \arrow[d, dash, "y_q"] \\
P_{b_1} & P_{b_2} & & P_{b_q}
\end{tikzcd}$$

Mirror Theory Applied to XoP

$$\begin{tikzcd}
P_{a_1} \arrow[d, dash, "y_1"] & P_{a_2} \arrow[d, dash, "y_2"] & \cdots & P_{a_q} \arrow[d, dash, "y_q"] \\
P_{b_1} & P_{b_2} & & P_{b_q}
\end{tikzcd}$$

Applying Mirror Theory

- Circle-free: no collisions in inputs to p
- Non-degenerate: provided that $y_i \neq 0$ for all i
- Maximum tree size 2

Mirror Theory Applied to XoP

$$\begin{tikzcd} P_{a_1} \arrow[d, dash, "y_1"] & P_{a_2} \arrow[d, dash, "y_2"] & \cdots & P_{a_q} \arrow[d, dash, "y_q"] \\ P_{b_1} & P_{b_2} & & P_{b_q} \end{tikzcd}$$

Applying Mirror Theory

- Circle-free: no collisions in inputs to p
- Non-degenerate: provided that $y_i \neq 0$ for all i
- Maximum tree size 2
- If $2q \leq 2^n/67$: at least $\frac{(2^n)_{2q}}{2^{nq}}$ solutions to unknowns

Mirror Theory Applied to XoP

H-Coefficient Technique [Pat91,Pat08,CS14]

Let $\varepsilon \geq 0$ be such that for all good transcripts τ:

$$\frac{\mathbf{Pr}\left[\text{XoP gives } \tau\right]}{\mathbf{Pr}\left[f \text{ gives } \tau\right]} \geq 1 - \varepsilon$$

Then, $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(q) \leq \varepsilon + \mathbf{Pr}\left[\text{bad transcript for } f\right]$

Mirror Theory Applied to XoP

H-Coefficient Technique [Pat91,Pat08,CS14]

Let $\varepsilon \geq 0$ be such that for all good transcripts τ:

$$\frac{\mathbf{Pr}\left[\text{XoP gives } \tau\right]}{\mathbf{Pr}\left[f \text{ gives } \tau\right]} \geq 1 - \varepsilon$$

Then, $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(q) \leq \varepsilon + \mathbf{Pr}\left[\text{bad transcript for } f\right]$

- Bad transcript: if $y_i = 0$ for some i
  - $\mathbf{Pr}\left[\text{bad transcript for } f\right] = q/2^n$

Mirror Theory Applied to XoP

H-Coefficient Technique [Pat91,Pat08,CS14]

Let $\varepsilon \geq 0$ be such that for all good transcripts τ:

$$\frac{\mathbf{Pr}\left[\text{XoP gives } \tau\right]}{\mathbf{Pr}\left[f \text{ gives } \tau\right]} \geq 1 - \varepsilon$$

Then, $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(q) \leq \varepsilon + \mathbf{Pr}\left[\text{bad transcript for } f\right]$

- Bad transcript: if $y_i = 0$ for some i
  - $\mathbf{Pr}\left[\text{bad transcript for } f\right] = q/2^n$
- For any good transcript:
  - $\mathbf{Pr}\left[\text{XoP gives } \tau\right] \geq \frac{(2^n)_{2q}}{2^{nq}} \cdot \frac{1}{(2^n)_{2q}}$

Mirror Theory Applied to XoP

H-Coefficient Technique [Pat91,Pat08,CS14]

Let $\varepsilon \geq 0$ be such that for all good transcripts τ:

$$\frac{\mathbf{Pr}\left[\text{XoP gives } \tau\right]}{\mathbf{Pr}\left[f \text{ gives } \tau\right]} \geq 1 - \varepsilon$$

Then, $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(q) \leq \varepsilon + \mathbf{Pr}\left[\text{bad transcript for } f\right]$

- Bad transcript: if $y_i = 0$ for some i
  - $\mathbf{Pr}\left[\text{bad transcript for } f\right] = q/2^n$
- For any good transcript:
  - $\mathbf{Pr}\left[\text{XoP gives } \tau\right] \geq \frac{(2^n)_{2q}}{2^{nq}} \cdot \frac{1}{(2^n)_{2q}}$
  - $\mathbf{Pr}\left[f \text{ gives } \tau\right] = \frac{1}{2^{nq}}$

Mirror Theory Applied to XoP

H-Coefficient Technique [Pat91,Pat08,CS14]

Let $\varepsilon \geq 0$ be such that for all good transcripts τ:

$$\frac{\mathbf{Pr}\left[\text{XoP gives } \tau\right]}{\mathbf{Pr}\left[f \text{ gives } \tau\right]} \geq 1 - \varepsilon$$

Then, $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(q) \leq \varepsilon + \mathbf{Pr}\left[\text{bad transcript for } f\right]$

- Bad transcript: if $y_i = 0$ for some i
  - $\mathbf{Pr}\left[\text{bad transcript for } f\right] = q/2^n$
- For any good transcript:

$$\left.\begin{array}{l} \bullet\ \mathbf{Pr}\left[\text{XoP gives } \tau\right] \geq \frac{(2^n)_{2q}}{2^{nq}} \cdot \frac{1}{(2^n)_{2q}} \\ \bullet\ \mathbf{Pr}\left[f \text{ gives } \tau\right] = \frac{1}{2^{nq}} \end{array}\right\} \varepsilon = 0$$

Mirror Theory Applied to XoP

H-Coefficient Technique [Pat91,Pat08,CS14]

Let $\varepsilon \geq 0$ be such that for all good transcripts τ:

$$\frac{\mathbf{Pr}\left[\text{XoP gives } \tau\right]}{\mathbf{Pr}\left[f \text{ gives } \tau\right]} \geq 1 - \varepsilon$$

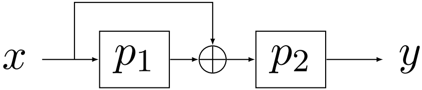
Then, $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(q) \leq \varepsilon + \mathbf{Pr}\left[\text{bad transcript for } f\right]$

- Bad transcript: if $y_i = 0$ for some i
  - $\mathbf{Pr}\left[\text{bad transcript for } f\right] = q/2^n$
- For any good transcript:
  - $\mathbf{Pr}\left[\text{XoP gives } \tau\right] \geq \frac{(2^n)_{2q}}{2^{nq}} \cdot \frac{1}{(2^n)_{2q}}$
  - $\mathbf{Pr}\left[f \text{ gives } \tau\right] = \frac{1}{2^{nq}}$

  $\Big\}\ \varepsilon = 0$

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(q) \leq q/2^n$$

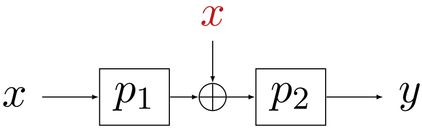
EDM



General Setting

- Adversary gets transcript $\tau = \{(x_1, y_1), \ldots, (x_q, y_q)\}$

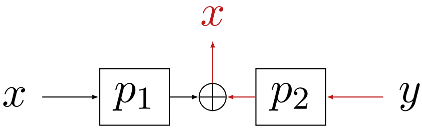
EDM



General Setting

- Adversary gets transcript $\tau = \{(x_1, y_1), \ldots, (x_q, y_q)\}$

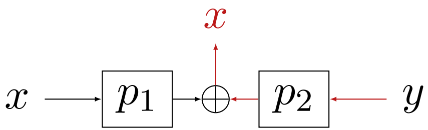
EDM



General Setting

- Adversary gets transcript $\tau = \{(x_1, y_1), \ldots, (x_q, y_q)\}$
- Xor of permutations in the middle

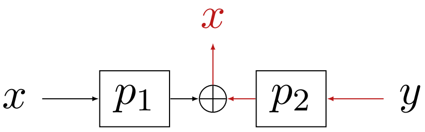
EDM



General Setting

- Adversary gets transcript $\tau = \{(x_1, y_1), \ldots, (x_q, y_q)\}$
- Xor of permutations in the middle
- Each tuple corresponds to $x_i \mapsto p_1(x_i) =: P_{a_i}$ and
  $y_i \mapsto p_2^{-1}(y_i) =: P_{b_i}$

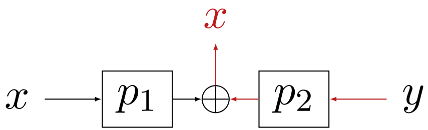
EDM



General Setting

- Adversary gets transcript $\tau = \{(x_1, y_1), \ldots, (x_q, y_q)\}$
- Xor of permutations in the middle
- Each tuple corresponds to $x_i \mapsto p_1(x_i) =: P_{a_i}$ and
  $y_i \mapsto p_2^{-1}(y_i) =: P_{b_i}$
- System of q equations $P_{a_i} \oplus P_{b_i} = x_i$

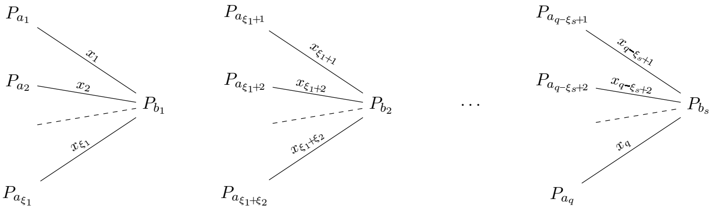
EDM



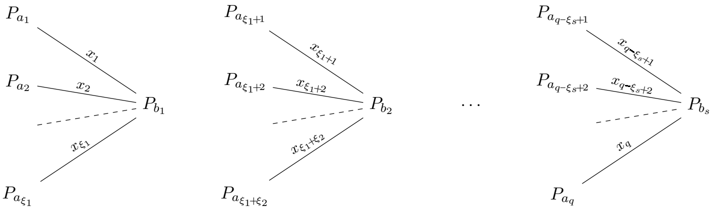
General Setting

- Adversary gets transcript $\tau = \{(x_1, y_1), \ldots, (x_q, y_q)\}$
- Xor of permutations in the middle
- Each tuple corresponds to $x_i \mapsto p_1(x_i) =: P_{a_i}$ and
  $y_i \mapsto p_2^{-1}(y_i) =: P_{b_i}$
- System of q equations $P_{a_i} \oplus P_{b_i} = x_i$
- x_i's all unique, y_i's may collide

EDM


P_{a_1}
x_1
P_{a_2}
x_2
P_{b_1}
x_{ξ_1}
$P_{a_{\xi_1}}$
$P_{a_{\xi_1+1}}$
x_{ξ_1+1}
$P_{a_{\xi_1+2}}$
x_{ξ_1+2}
P_{b_2}
$x_{\xi_1+\xi_2}$
$P_{a_{\xi_1+\xi_2}}$
$\cdots$
$P_{a_{q-\xi_s+1}}$
$x_{q-\xi_s+1}$
$P_{a_{q-\xi_s+2}}$
$x_{q-\xi_s+2}$
P_{b_s}
x_q
P_{a_q}

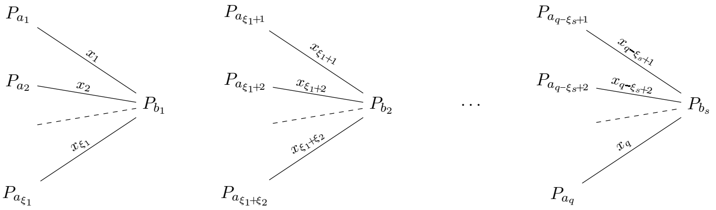
EDM



covers independent permutations

Applying Relaxed Mirror Theory

EDM

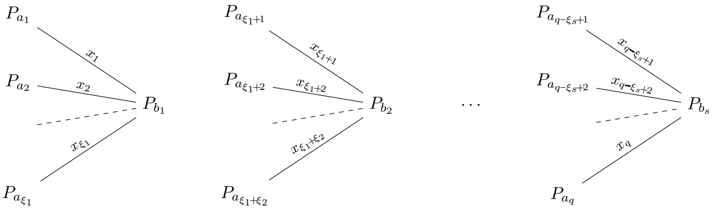


covers independent permutations

Applying Relaxed Mirror Theory

- Circle-free: no collisions in inputs to p_1
- Non-degenerate: as $x_i \neq x_j$ for all $i \neq j$
- Max tree size $\xi + 1$: provided no $(\xi + 1)$-fold collision

EDM

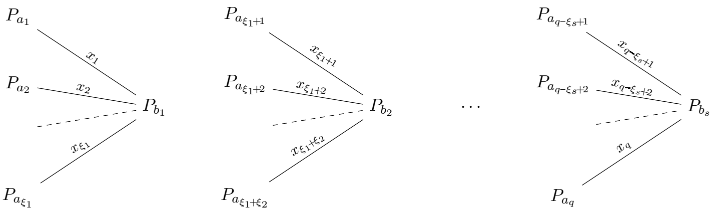


covers independent permutations

Applying Relaxed Mirror Theory

- Circle-free: no collisions in inputs to p_1
- Non-degenerate: as $x_i \neq x_j$ for all $i \neq j$
- Max tree size $\xi + 1$: provided no $(\xi + 1)$-fold collision
- If $\xi^2 q \leq 2^n/67$: at least $\frac{(2^n)_s \cdot (2^n - 1)_q}{2^{nq}}$ solutions to unknowns

EDM

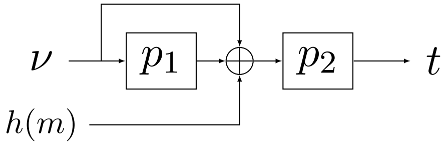


covers independent permutations

Applying Relaxed Mirror Theory

- Circle-free: no collisions in inputs to p_1
- Non-degenerate: as $x_i \neq x_j$ for all $i \neq j$
- Max tree size $\xi + 1$: provided no $(\xi + 1)$-fold collision
- If $\xi^2 q \leq 2^n/67$: at least $\frac{(2^n)_s \cdot (2^n - 1)_q}{2^{nq}}$ solutions to unknowns
- H-coefficient technique: $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{EDM}}(q) \leq q/2^n + \binom{q}{\xi+1}/2^{n\xi}$

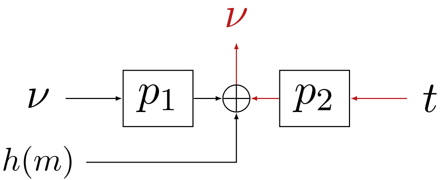
EWCDM



General Setting

- Adversary gets transcript $\tau = \{(\nu_1, m_1, t_1), \ldots, (\nu_q, m_q, t_q)\}$

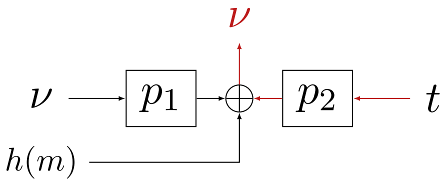
EWCDM



General Setting

- Adversary gets transcript $\tau = \{(\nu_1, m_1, t_1), \ldots, (\nu_q, m_q, t_q)\}$

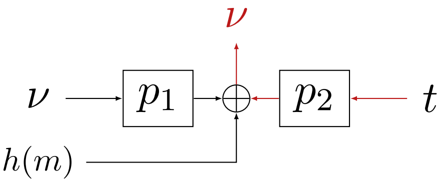
EWCDM



General Setting

- Adversary gets transcript $\tau = \{(\nu_1, m_1, t_1), \ldots, (\nu_q, m_q, t_q)\}$
- Each tuple corresponds to $\nu_i \mapsto p_1(\nu_i) =: P_{a_i}$ and
  $t_i \mapsto p_2^{-1}(t_i) =: P_{b_i}$
- System of q equations $P_{a_i} \oplus P_{b_i} = \nu_i \oplus h(m_i)$

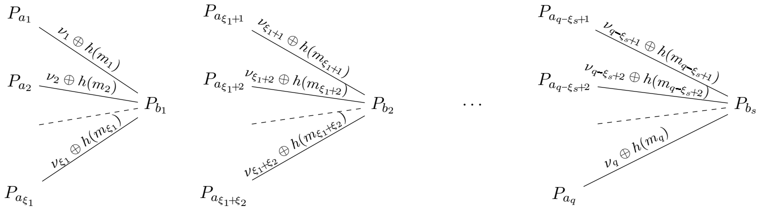
EWCDM



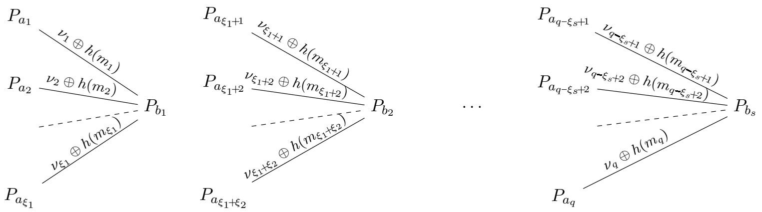
General Setting

- Adversary gets transcript $\tau = \{(\nu_1, m_1, t_1), \ldots, (\nu_q, m_q, t_q)\}$
- Each tuple corresponds to $\nu_i \mapsto p_1(\nu_i) =: P_{a_i}$ and
  $t_i \mapsto p_2^{-1}(t_i) =: P_{b_i}$
- System of q equations $P_{a_i} \oplus P_{b_i} = \nu_i \oplus h(m_i)$
- Extra issue: $\nu_i \oplus h(m_i)$ may collide

EWCDM


P_{a_1}
$\nu_1 \oplus h(m_1)$
P_{a_2}
$\nu_2 \oplus h(m_2)$
P_{b_1}
$\nu_{\xi_1} \oplus h(m_{\xi_1})$
$P_{a_{\xi_1}}$
$P_{a_{\xi_1+1}}$
$\nu_{\xi_1+1} \oplus h(m_{\xi_1+1})$
$P_{a_{\xi_1+2}}$
$\nu_{\xi_1+2} \oplus h(m_{\xi_1+2})$
P_{b_2}
$\nu_{\xi_1+\xi_2} \oplus h(m_{\xi_1+\xi_2})$
$P_{a_{\xi_1+\xi_2}}$
$\cdots$
$P_{a_{q-\xi_s+1}}$
$\nu_{q-\xi_s+1} \oplus h(m_{q-\xi_s+1})$
$P_{a_{q-\xi_s+2}}$
$\nu_{q-\xi_s+2} \oplus h(m_{q-\xi_s+2})$
P_{b_s}
$\nu_q \oplus h(m_q)$
P_{a_q}

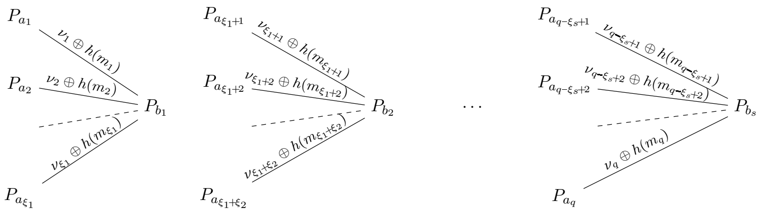
EWCDM



Applying Relaxed Mirror Theory

- Circle-free: no collisions in inputs to p_1
- Non-degenerate: provided $\nu_i \oplus h(m_i) \neq \nu_j \oplus h(m_j)$ in all trees
- Max tree size $\xi + 1$: provided no $(\xi + 1)$-fold collision

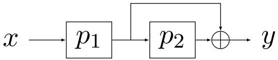
EWCDM



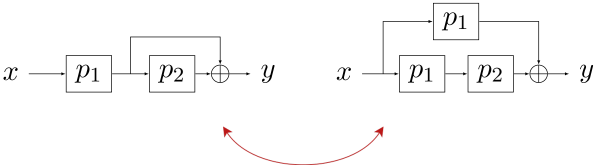
Applying Relaxed Mirror Theory

- Circle-free: no collisions in inputs to p_1
- Non-degenerate: provided $\nu_i \oplus h(m_i) \neq \nu_j \oplus h(m_j)$ in all trees
- Max tree size $\xi + 1$: provided no $(\xi + 1)$-fold collision
- If $\xi^2 q \leq 2^n/67$: $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{EWCDM}}(q) \leq q/2^n + \binom{q}{2}\epsilon/2^n + \binom{q}{\xi+1}/2^{n\xi}$

EDMD

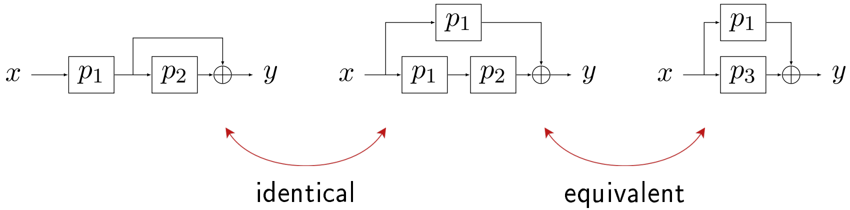


EDMD

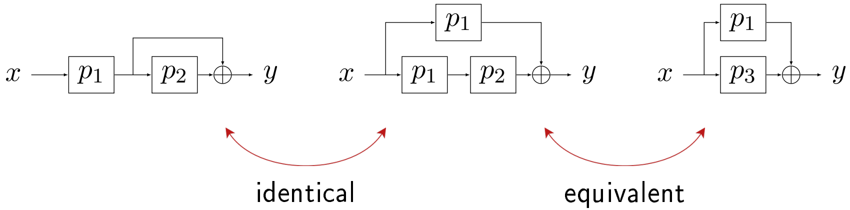


identical

EDMD



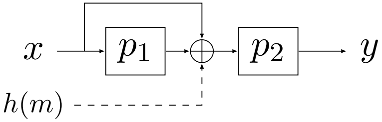
EDMD



- EDMD is at least as secure as XoP
- If $q \leq 2^n/67$: $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{EDMD}}(\mathcal{D}) \leq q/2^n$

Single-Key Variants?

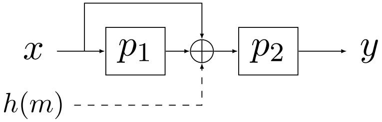
E(WC)DM



- "XoP in the middle" relies on inverting p_2
- Trick fails if $p_1 = p_2$

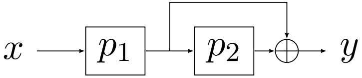
Single-Key Variants?

E(WC)DM



- "XoP in the middle" relies on inverting p_2
- Trick fails if $p_1 = p_2$

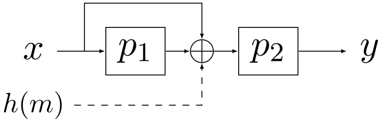
EDMD



- p_1, p_2 independent: cascading has limited influence
- Sliding issues if $p_1 = p_2$

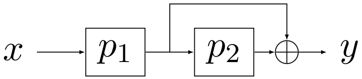
Single-Key Variants?

E(WC)DM



- "XoP in the middle" relies on inverting p_2
- Trick fails if $p_1 = p_2$

EDMD



- p_1, p_2 independent: cascading has limited influence
- Sliding issues if $p_1 = p_2$

Conjecture: optimal 2^n security

Conclusion

Mirror Theory

- Powerful but underestimated technique
- Implies (almost) optimal security of E(WC)DM
- Implies optimal security of EDMD

Conclusion

Mirror Theory

- Powerful but underestimated technique
- Implies (almost) optimal security of E(WC)DM
- Implies optimal security of EDMD

Open Questions

- Single-key variants?
- Dual of EWCDM?
- Further applications

Thank you for your attention!

Supporting Slides

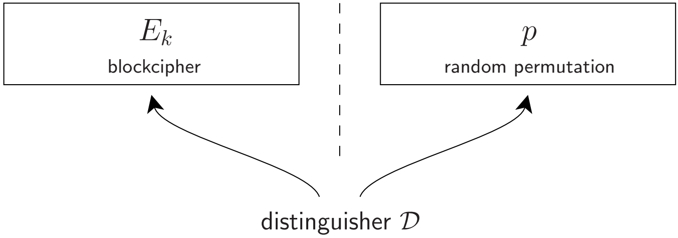
SUPPORTING SLIDES

Pseudorandom Permutation

E_k	p
blockcipher	random permutation

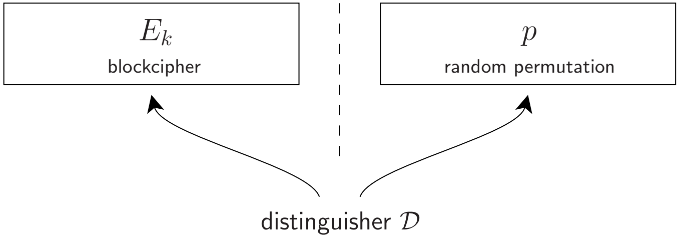
- Two oracles: E_k (for secret random key k) and p

Pseudorandom Permutation



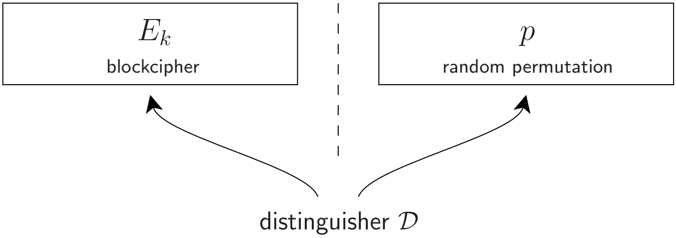
- Two oracles: E_k (for secret random key k) and p
- Distinguisher $\mathcal{D}$ has query access to either E_k or p

Pseudorandom Permutation



- Two oracles: E_k (for secret random key k) and p
- Distinguisher $\mathcal{D}$ has query access to either E_k or p
- $\mathcal{D}$ tries to determine which oracle it communicates with

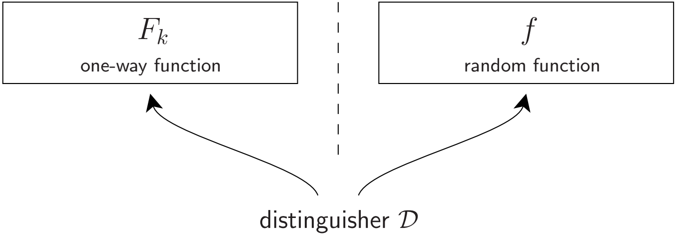
Pseudorandom Permutation



- Two oracles: E_k (for secret random key k) and p
- Distinguisher $\mathcal{D}$ has query access to either E_k or p
- $\mathcal{D}$ tries to determine which oracle it communicates with

$$\mathbf{Adv}_E^{\mathrm{prp}}(\mathcal{D}) = \left|\mathbf{Pr}\left[\mathcal{D}^{E_k} = 1\right] - \mathbf{Pr}\left[\mathcal{D}^{p} = 1\right]\right|$$

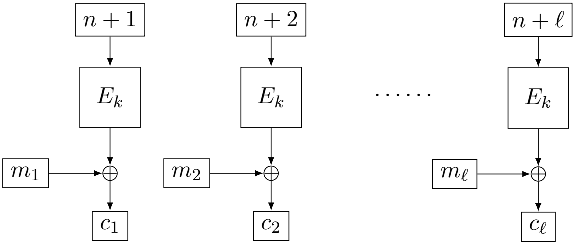
Pseudorandom Function



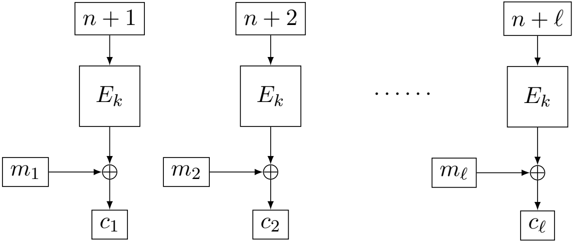
- Two oracles: F_k (for secret random key k) and f
- Distinguisher $\mathcal{D}$ has query access to either F_k or f
- $\mathcal{D}$ tries to determine which oracle it communicates with

$$\mathbf{Adv}_F^{\mathrm{prf}}(\mathcal{D}) = \left| \mathbf{Pr}\left[\mathcal{D}^{F_k} = 1\right] - \mathbf{Pr}\left[\mathcal{D}^{f} = 1\right] \right|$$

Counter Mode Based on Pseudorandom Permutation



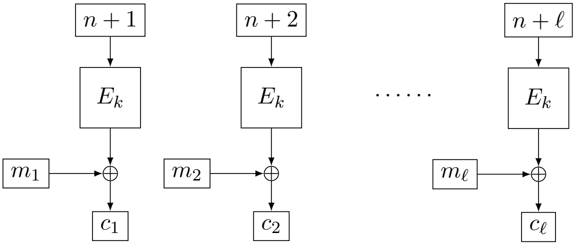
Counter Mode Based on Pseudorandom Permutation



- Security bound:

$$\mathbf{Adv}^{\mathrm{cpa}}_{\mathsf{CTR}[E]}(\sigma) \leq \mathbf{Adv}^{\mathrm{prp}}_{E}(\sigma) + \binom{\sigma}{2}/2^n$$

Counter Mode Based on Pseudorandom Permutation

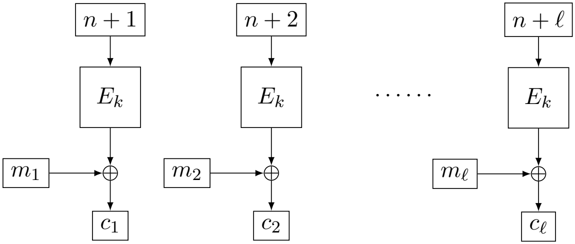


- Security bound:

$$\mathbf{Adv}^{\mathrm{cpa}}_{\mathsf{CTR}[E]}(\sigma) \leq \mathbf{Adv}^{\mathrm{prp}}_{E}(\sigma) + \binom{\sigma}{2}/2^n$$

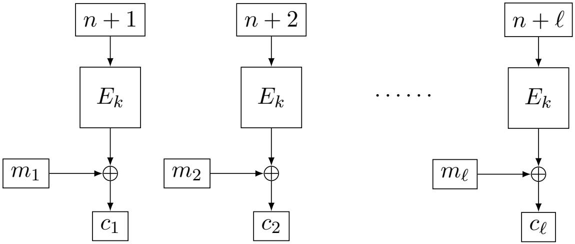
- $\mathsf{CTR}[E]$ is secure as long as:
  - E_k is a secure PRP
  - Number of encrypted blocks $\sigma \ll 2^{n/2}$

Counter Mode Based on Pseudorandom Permutation



- $m_i \oplus c_i$ is distinct for all σ blocks
- Unlikely to happen for random string

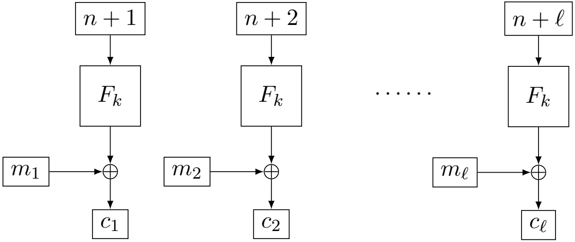
Counter Mode Based on Pseudorandom Permutation



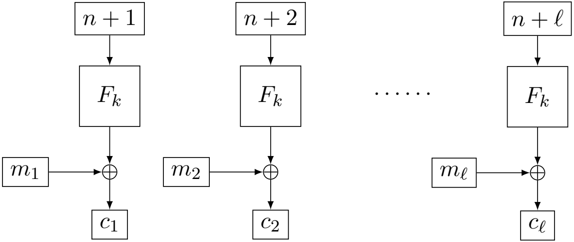
- $m_i \oplus c_i$ is distinct for all σ blocks
- Unlikely to happen for random string
- Distinguishing attack in $\sigma \approx 2^{n/2}$ blocks:

$$\binom{\sigma}{2}/2^n \lesssim \mathbf{Adv}^{\mathrm{cpa}}_{\mathsf{CTR}[E]}(\sigma)$$

Counter Mode Based on Pseudorandom Function



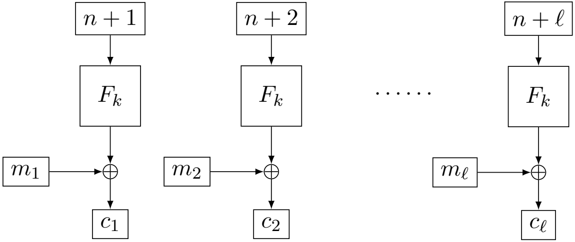
Counter Mode Based on Pseudorandom Function



- Security bound:

$$\mathbf{Adv}^{\mathrm{cpa}}_{\mathsf{CTR}[F]}(\sigma) \leq \mathbf{Adv}^{\mathrm{prf}}_{F}(\sigma)$$

Counter Mode Based on Pseudorandom Function

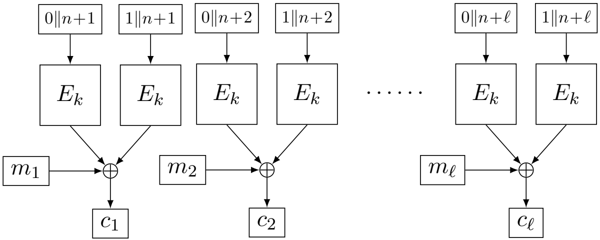


- Security bound:

$$\mathbf{Adv}^{\mathrm{cpa}}_{\mathsf{CTR}[F]}(\sigma) \leq \mathbf{Adv}^{\mathrm{prf}}_{F}(\sigma)$$

- CTR$[F]$ is secure as long as F_k is a secure PRF
- Birthday bound security loss disappeared

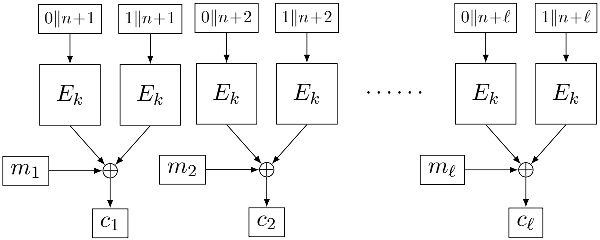
Counter Mode Based on XoP



- Security bound:

$$\mathbf{Adv}^{\mathrm{cpa}}_{\mathsf{CTR[XoP]}}(\sigma) \le \mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(\sigma)$$

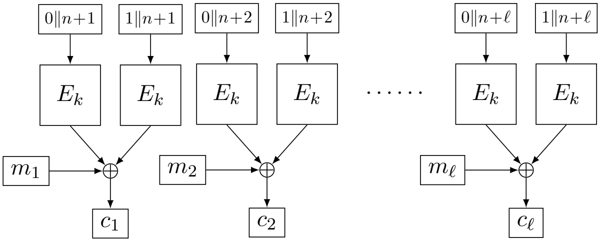
Counter Mode Based on XoP



- Security bound:

$$\begin{aligned}\mathbf{Adv}^{\mathrm{cpa}}_{\mathsf{CTR[XoP]}}(\sigma) &\leq \mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(\sigma) \\ &\leq \mathbf{Adv}^{\mathrm{prp}}_{E}(2\sigma) + \sigma/2^n\end{aligned}$$

Counter Mode Based on XoP

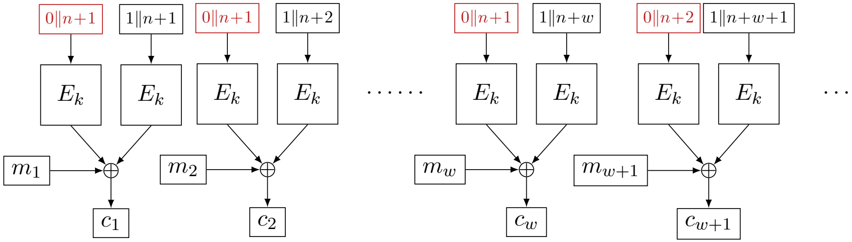


- Security bound:

$$\begin{aligned}\mathbf{Adv}^{\mathrm{cpa}}_{\mathsf{CTR[XoP]}}(\sigma) &\le \mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(\sigma) \\ &\le \mathbf{Adv}^{\mathrm{prp}}_{E}(2\sigma) + \sigma/2^n\end{aligned}$$

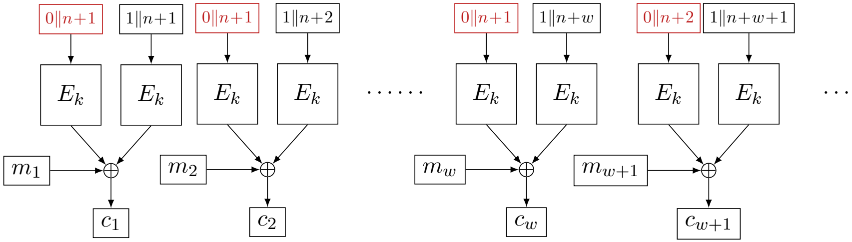
- Beyond birthday-bound but 2x as expensive as CTR$[E]$

CENC by Iwata [Iwa06]



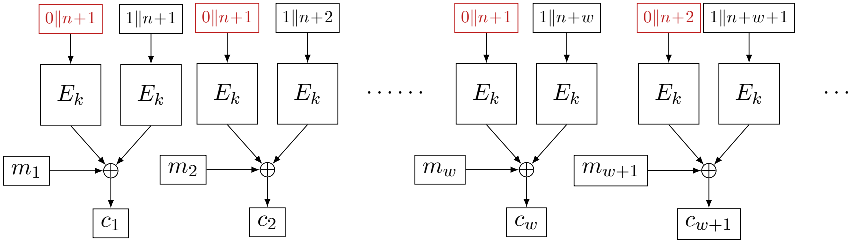
- One subkey used for $w \geq 1$ encryptions

CENC by Iwata [Iwa06]



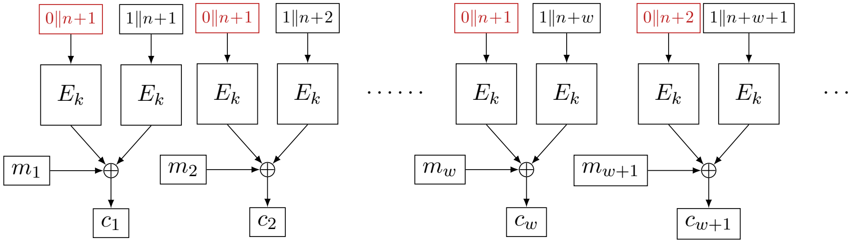
- One subkey used for $w \geq 1$ encryptions
- Almost as expensive as CTR$[E]$

CENC by Iwata [Iwa06]



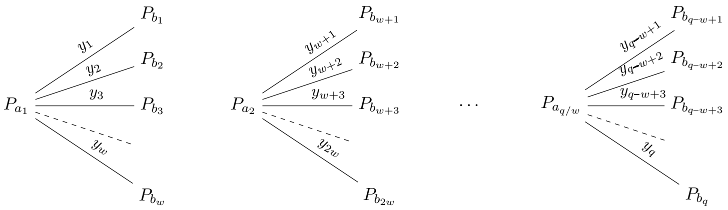
- One subkey used for $w \geq 1$ encryptions
- Almost as expensive as CTR$[E]$
- 2006: $2^{2n/3}$ security, $2^n/w$ conjectured [Iwa06]

CENC by Iwata [Iwa06]

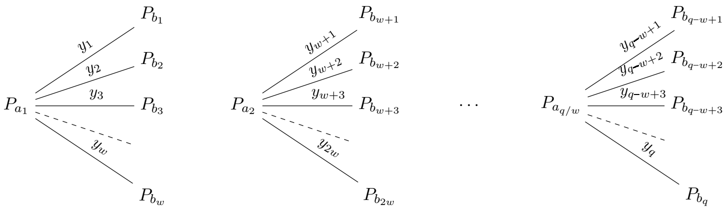


- One subkey used for $w \geq 1$ encryptions
- Almost as expensive as CTR$[E]$
- 2006: $2^{2n/3}$ security, $2^n/w$ conjectured [Iwa06]
- 2016: $2^n/w$ security [IMV16]

Mirror Theory Applied to CENC



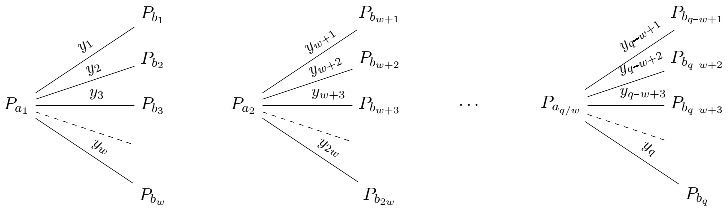
Mirror Theory Applied to CENC



Applying Mirror Theory

- Circle-free: no collisions in inputs to p
- Non-degenerate: provided that $y_i \neq 0$ for all i
  and $y_i \neq y_j$ within all w-blocks
- Maximum tree size $w + 1$

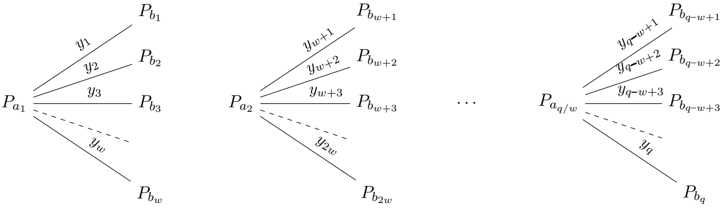
Mirror Theory Applied to CENC



Applying Mirror Theory

- Circle-free: no collisions in inputs to p
- Non-degenerate: provided that $y_i \neq 0$ for all i
  and $y_i \neq y_j$ within all w-blocks
- Maximum tree size $w + 1$
- If $2w^2q \leq 2^n/67$: at least $\frac{(2^n)_r}{2^{nq}}$ solutions to unknowns

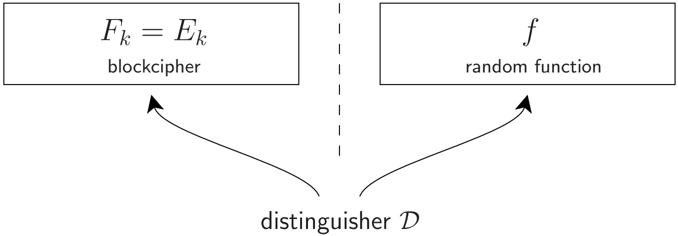
Mirror Theory Applied to CENC



Applying Mirror Theory

- Circle-free: no collisions in inputs to p
- Non-degenerate: provided that $y_i \neq 0$ for all i
  and $y_i \neq y_j$ within all w-blocks
- Maximum tree size $w + 1$
- If $2w^2 q \leq 2^n/67$: at least $\frac{(2^n)_r}{2^{nq}}$ solutions to unknowns
- H-coefficient technique: $\mathbf{Adv}^{\mathrm{cpa}}_{\mathsf{CENC}}(q) \leq q/2^n + wq/2^{n+1}$

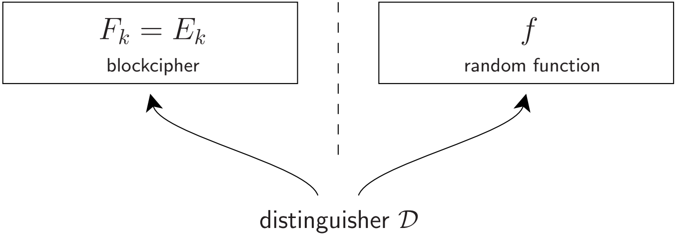
Naive PRP-PRF Conversion



PRP-PRF Switch

- Simply view E_k as a PRF

Naive PRP-PRF Conversion



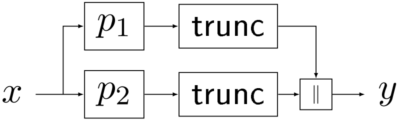
PRP-PRF Switch

- Simply view E_k as a PRF
- E_k does not expose collisions but f does
- E_k can be distinguished from f in $\approx 2^{n/2}$ queries

$$\binom{q}{2}/2^n \lesssim \mathbf{Adv}_E^{\mathrm{prf}}(q) \leq \mathbf{Adv}_E^{\mathrm{prp}}(q) + \binom{q}{2}/2^n$$

Beyond Birthday Bound PRP-PRF Conversion: Truncation

Truncation



- First suggested by Hall et al. [HWKS98]
- Secure up to $2^{3n/4}$ queries [Sta78,BI99,GG16]
- Application: GCM-SIV