Beyond Birthday-Bound Security

Bart Mennink
Radboud University (The Netherlands)

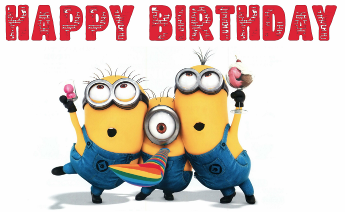
Summer school on real-world crypto and privacy

June 8, 2017

Birthday Paradox

For a random selection of 23 people, with a probability at least 50% two of them share the same birthday

Birthday Paradox



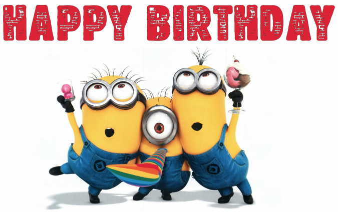
For a random selection of 23 people, with a probability at least 50% two of them share the same birthday

General Birthday Paradox

- Consider space $\mathcal{S} = \{0,1\}^n$
- Randomly draw q elements from $\mathcal{S}$
- Expected number of collisions:

$$\mathbf{Ex}\left[\text{collisions}\right] = \binom{q}{2}/2^n$$

Birthday Paradox



For a random selection of 23 people, with a probability at least 50% two of them share the same birthday

General Birthday Paradox

- Consider space $\mathcal{S} = \{0,1\}^n$
- Randomly draw q elements from $\mathcal{S}$
- Expected number of collisions:

$$\mathbf{Ex}\left[\text{collisions}\right] = \binom{q}{2} / 2^n$$

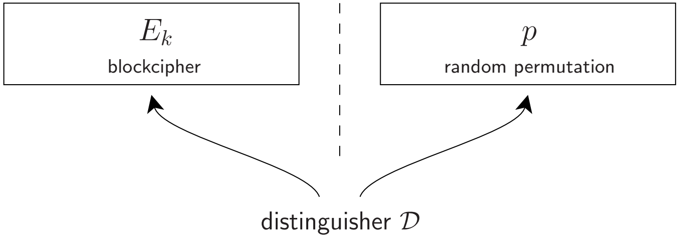
- Important phenomenon in cryptography

Pseudorandom Permutation

E_k blockcipher	p random permutation

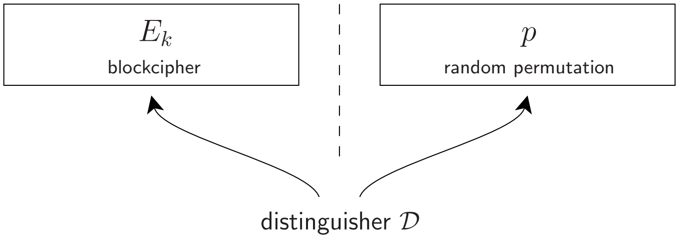
- Two oracles: E_k (for secret random key k) and p

Pseudorandom Permutation



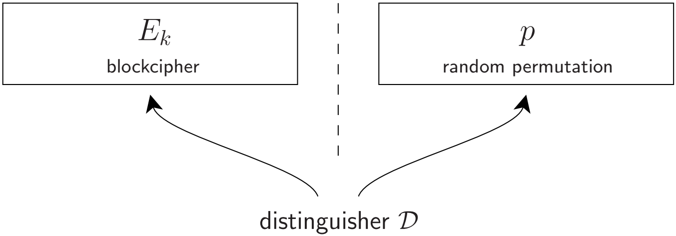
- Two oracles: E_k (for secret random key k) and p
- Distinguisher $\mathcal{D}$ has query access to either E_k or p

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

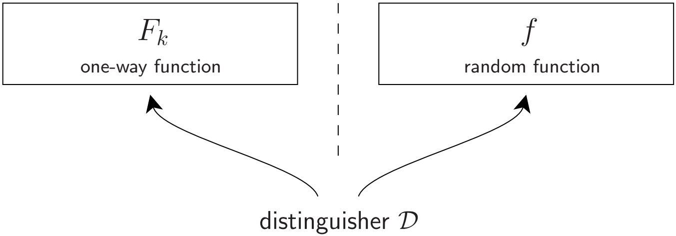
Pseudorandom Permutation



- 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

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

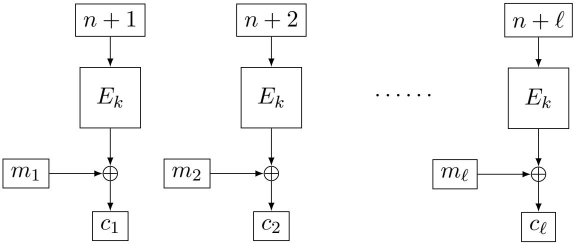
Pseudorandom Function



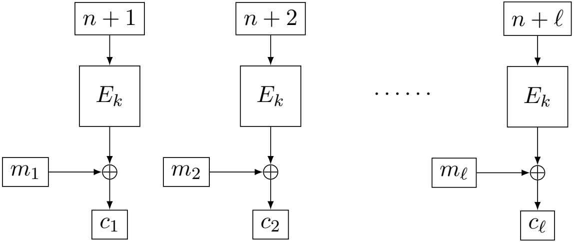
- Two oracles: F_k (for secret random key k) and f
- Distinguisher $\mathcal{D}$ has query access to either F_k or f
- $\mathcal{D}$ tries to determine which oracle it communicates with

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

Counter Mode Based on Pseudorandom Permutation



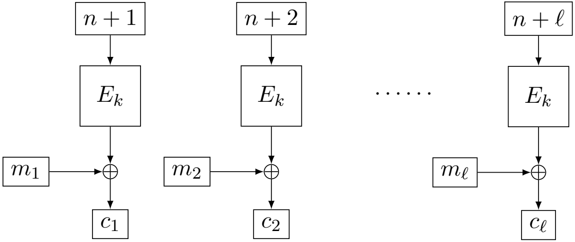
Counter Mode Based on Pseudorandom Permutation



- Security bound:

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

Counter Mode Based on Pseudorandom Permutation

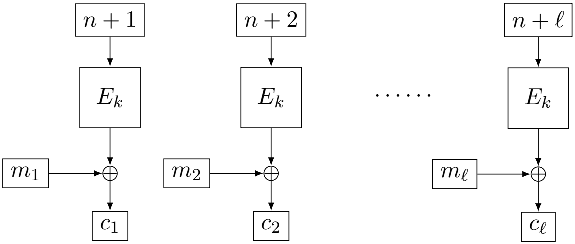


- Security bound:

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

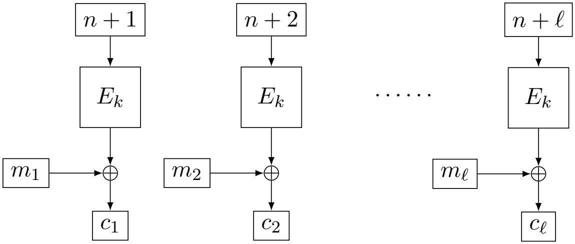
- $\mathsf{CTR}[E]$ is secure as long as:
  - E_k is a secure PRP
  - Number of encrypted blocks $\sigma \ll 2^{n/2}$

Counter Mode Based on Pseudorandom Permutation



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

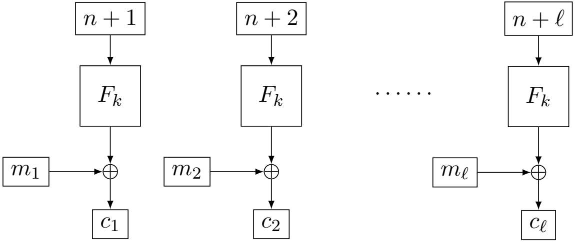
Counter Mode Based on Pseudorandom Permutation



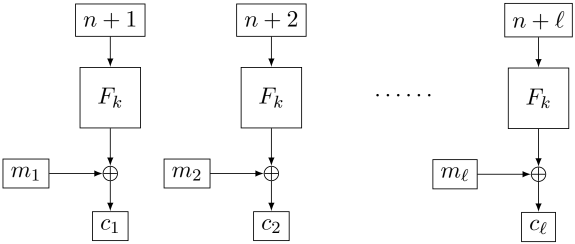
- $m_i \oplus c_i$ is distinct for all σ blocks
- Unlikely to happen for random string
- Distinguishing attack in $\sigma \approx 2^{n/2}$ blocks:

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

Counter Mode Based on Pseudorandom Function



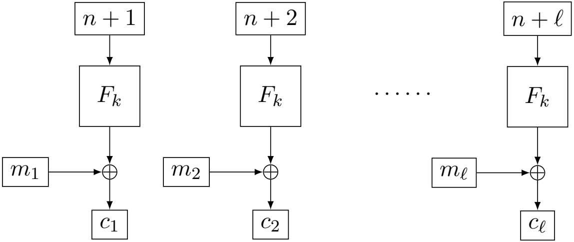
Counter Mode Based on Pseudorandom Function



- Security bound:

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

Counter Mode Based on Pseudorandom Function

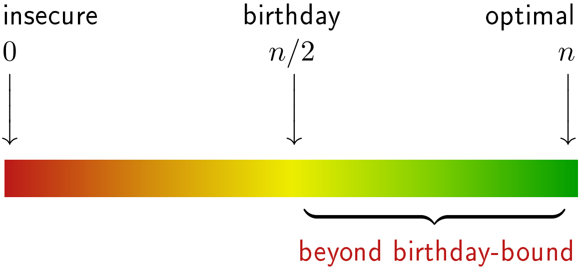


- Security bound:

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

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

Beyond Birthday-Bound Security



Disclaimer

$$\boxed{\text{Beyond birthday-bound} \quad \begin{array}{c}\not\Leftarrow \\ \not\Rightarrow\end{array} \quad \text{Better security}}$$

Disclaimer

$$\boxed{\text{Beyond birthday-bound} \quad \begin{matrix} \not\Leftarrow \\ \not\Rightarrow \end{matrix} \quad \text{Better security}}$$

- n large enough: birthday-bound security is okay
  $\longrightarrow$ Permutation-based constructions
- n too small: birthday-bound security could be bogus
  $\longrightarrow$ Lightweight blockciphers at risk

Disclaimer

$$\boxed{\text{Beyond birthday-bound} \quad \begin{array}{c}\not\Leftarrow \\ \not\Rightarrow\end{array} \quad \text{Better security}}$$

- n large enough: birthday-bound security is okay
  $\longrightarrow$ Permutation-based constructions
- n too small: birthday-bound security could be bogus
  $\longrightarrow$ Lightweight blockciphers at risk

- Beyond birthday-bound: relevant if $n/2$ is on the edge

Sweet32 Attack

On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN

Bhargavan, Leurent, ACM CCS 2016

- TLS supported Triple-DES
- OpenVPN used Blowfish
- Both Blowfish and Triple-DES have 64-bit state
- Practical birthday-bound attack on encryption mode

Outline

PRP-PRF Conversion

Conclusion

Outline

PRP-PRF Conversion

Conclusion

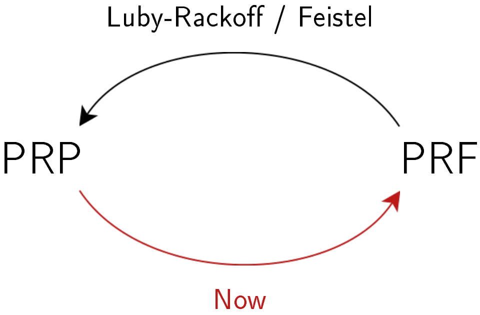
PRP-PRF Conversion

PRP PRF

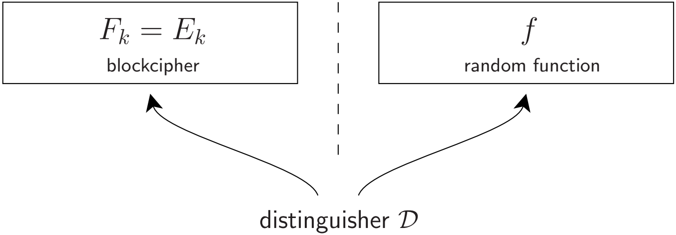
PRP-PRF Conversion

$$\text{PRP} \xleftarrow{\text{Luby-Rackoff / Feistel}} \text{PRF}$$

PRP-PRF Conversion



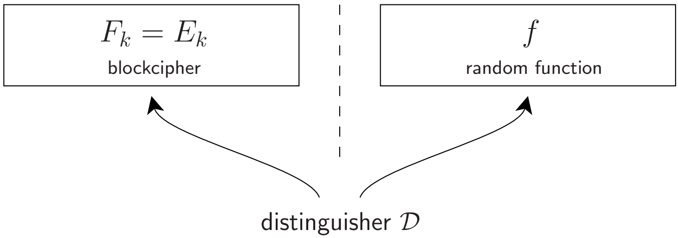
Naive PRP-PRF Conversion



PRP-PRF Switch

- Simply view E_k as a PRF

Naive PRP-PRF Conversion

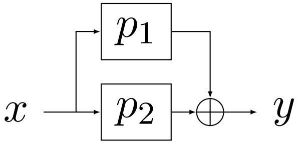


PRP-PRF Switch

- 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

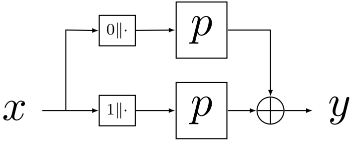
$$\binom{q}{2}/2^n \lesssim \mathbf{Adv}_E^{\mathrm{prf}}(q) \leq \mathbf{Adv}_E^{\mathrm{prp}}(q) + \binom{q}{2}/2^n$$

Xor of Permutations



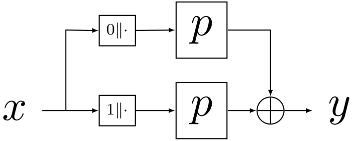
- First suggested by Bellare et al. [BKR98]

Xor of Permutations



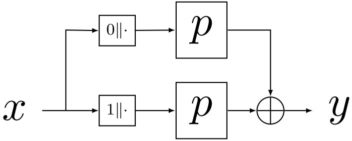
- First suggested by Bellare et al. [BKR98]

Xor of Permutations



- First suggested by Bellare et al. [BKR98]
- Lucks [Luc00]: $2^{2n/3}$
- Bellare and Impagliazzo [BI99]: $2^n/n^{2/3}$
- Patarin [Pat08]: 2^n

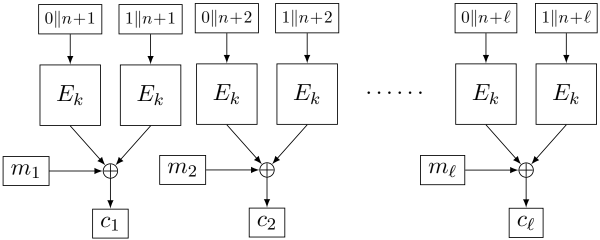
Xor of Permutations



- First suggested by Bellare et al. [BKR98]
- Lucks [Luc00]: $2^{2n/3}$
- Bellare and Impagliazzo [BI99]: $2^n/n^{2/3}$
- Patarin [Pat08]: 2^n

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

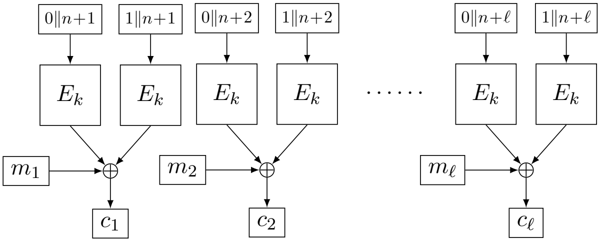
Counter Mode Based on XoP



- Security bound:

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

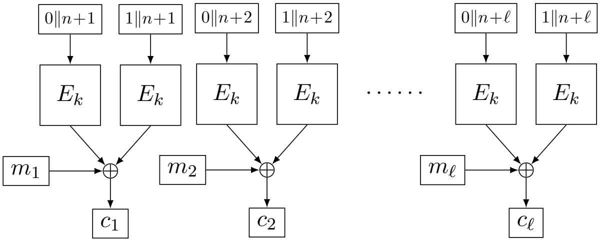
Counter Mode Based on XoP



- Security bound:

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

Counter Mode Based on XoP

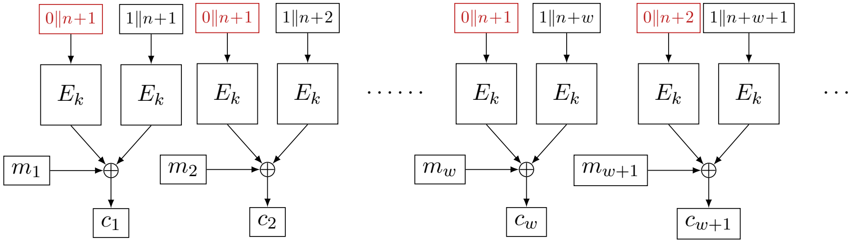


- Security bound:

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

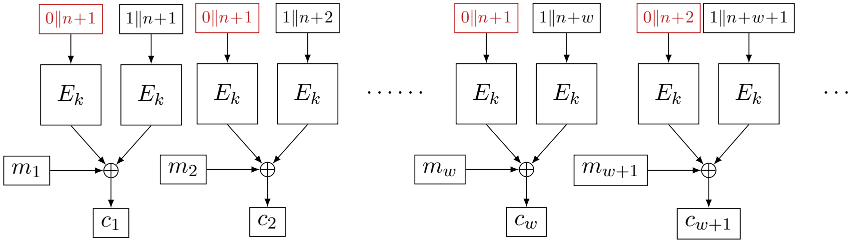
- Beyond birthday-bound but 2x as expensive as CTR$[E]$

CENC by Iwata [Iwa06]



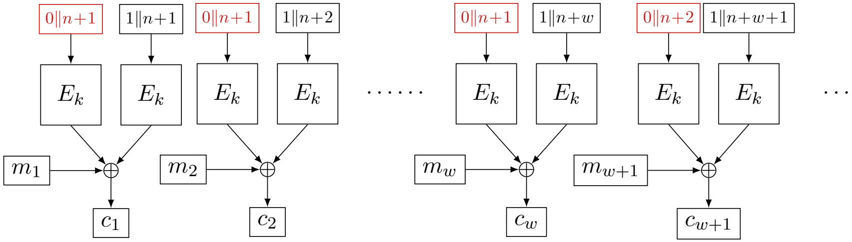
- One subkey used for $w \geq 1$ encryptions

CENC by Iwata [Iwa06]



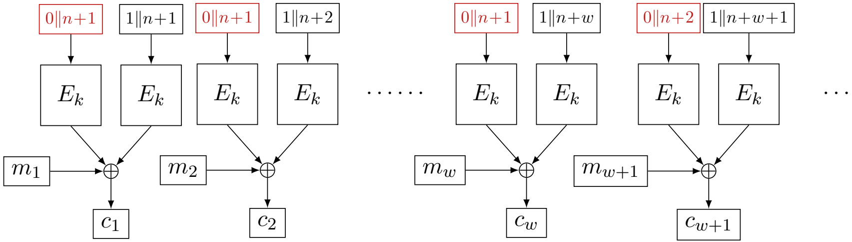
- One subkey used for $w \geq 1$ encryptions
- Almost as expensive as CTR$[E]$

CENC by Iwata [Iwa06]



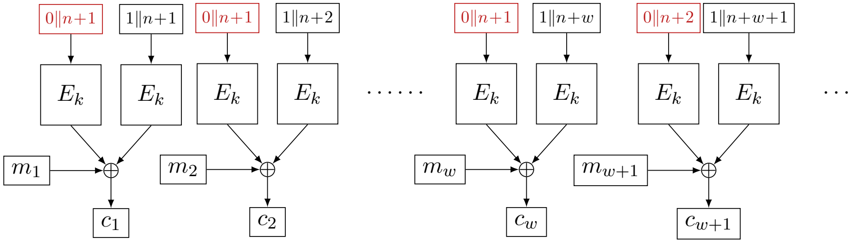
- One subkey used for $w \geq 1$ encryptions
- Almost as expensive as CTR$[E]$
- 2006: $2^{2n/3}$ security, $2^n/w$ conjectured [Iwa06]

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]

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]
  - Well, we did not really prove it ourselves
  - Immediate consequence of mirror theory from 2005

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

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

Goal

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

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
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	
Patarin	ICITS 2008	XoP	
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

Patarin's Result

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

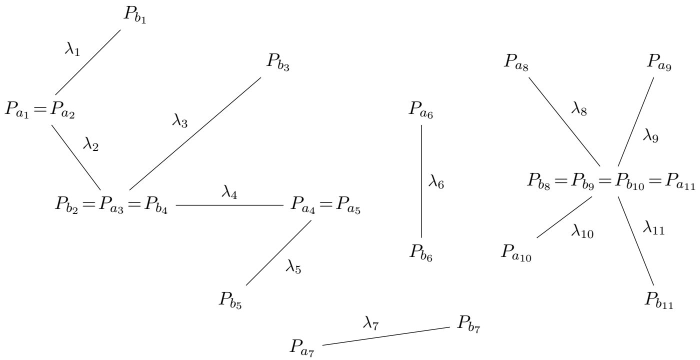
Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	
Patarin	ICITS 2008	XoP	
Patarin	ePrint 2010/287	XoP	concrete bound
Patarin	ePrint 2010/293	Feistel	
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 $\varphi : \{a_1, b_1, \ldots, a_q, b_q\} \to \{1, \ldots, r\}$

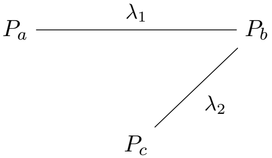
Graph Based View



Mirror Theory: Toy Example 1

- System of equations:

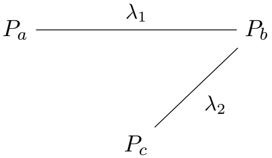
$$P_a \oplus P_b = \lambda_1$$
$$P_b \oplus P_c = \lambda_2$$



Mirror Theory: Toy Example 1

- System of equations:

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



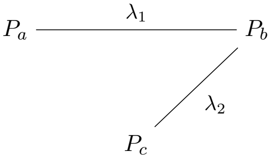
If $\boldsymbol{\lambda_1 = 0}$ or $\boldsymbol{\lambda_2 = 0}$ or $\boldsymbol{\lambda_1 = \lambda_2}$

- 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

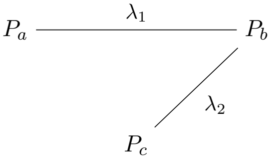
If $\lambda_1, \lambda_2 \neq 0$ and $\lambda_1 \neq \lambda_2$

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

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

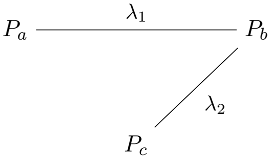
If $\boldsymbol{\lambda_1, \lambda_2 \neq 0}$ and $\boldsymbol{\lambda_1 \neq \lambda_2}$

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

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

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

- 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:

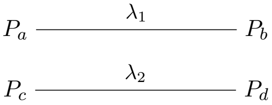
$$P_a \oplus P_b = \lambda_1$$
$$P_c \oplus P_d = \lambda_2$$

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

Mirror Theory: Toy Example 2

- System of equations:

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



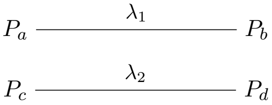
If $\boldsymbol{\lambda_1 = 0}$ or $\boldsymbol{\lambda_2 = 0}$

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

Mirror Theory: Toy Example 2

- System of equations:

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



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:

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

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

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

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

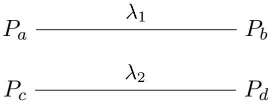
If $\lambda_1, \lambda_2 \neq 0$

- 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 $\lambda_1, \lambda_2 \neq 0$

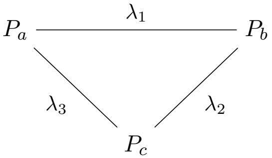
- 2^n choices for P_a (which fixes P_b)
- For P_c and P_d we require
  - $P_c \neq P_a, P_b$
  - $P_d = \lambda_2 \oplus P_c \neq P_a, P_b$
- At least $2^n - 4$ choices for P_c (which fixes P_d)

Mirror Theory: Toy Example 3

- System of equations:

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

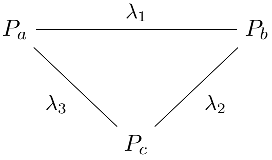
- Assume $\lambda_i \neq 0$ and $\lambda_i \neq \lambda_j$



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

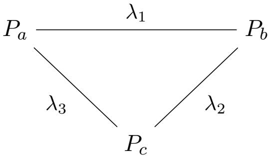
- Contradiction: equations sum to $0 = \lambda_1 \oplus \lambda_2 \oplus \lambda_3$
- Scheme contains a circle

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

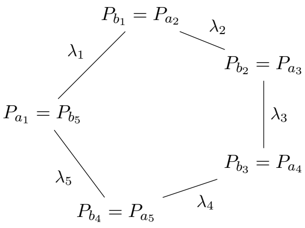
- Contradiction: equations sum to $0 = \lambda_1 \oplus \lambda_2 \oplus \lambda_3$
- Scheme contains a circle

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

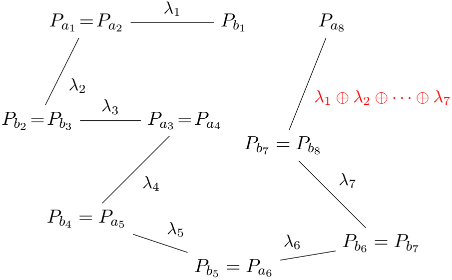
- One redundant equation, no contradiction
- Still counted as circle

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

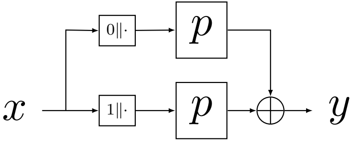
Main Result

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 $(\xi - 1)^2 \cdot r \leq 2^n/67$

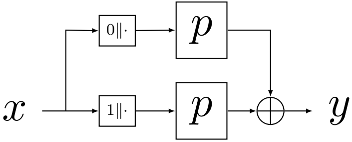
Mirror Theory Applied to XoP



General Setting

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

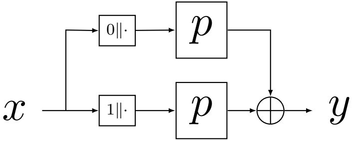
Mirror Theory Applied to XoP



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
  $x_i \mapsto p(1\|x_i) =: P_{b_i}$

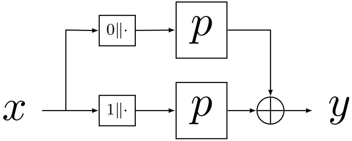
Mirror Theory Applied to XoP



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 $\tau = \{(x_1, y_1), \ldots, (x_q, y_q)\}$
- 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 $P_{a_i} \oplus P_{b_i} = y_i$
- Inputs to p are all distinct: $2q$ unknowns

Mirror Theory Applied to XoP

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

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
  $\longrightarrow$ Call this a bad transcript
- 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
  $\longrightarrow$ Call this a bad transcript
- 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:
  - $\mathbf{Pr}\left[\text{XoP gives } \tau\right] \geq \frac{(2^n)_{2q}}{2^{nq}} \cdot \frac{1}{(2^n)_{2q}}$
  - $\mathbf{Pr}\left[f \text{ gives } \tau\right] = \frac{1}{2^{nq}}$

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

Mirror Theory Applied to XoP

H-Coefficient Technique [Pat91,Pat08,CS14]

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

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

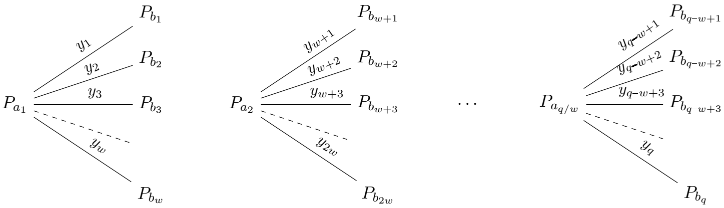
Then, $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(q) \leq \varepsilon + \mathbf{Pr}\left[\text{bad transcript for } f\right]$

- 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:
  - $\mathbf{Pr}\left[\text{XoP gives } \tau\right] \geq \frac{(2^n)_{2q}}{2^{nq}} \cdot \frac{1}{(2^n)_{2q}}$
  - $\mathbf{Pr}\left[f \text{ gives } \tau\right] = \frac{1}{2^{nq}}$

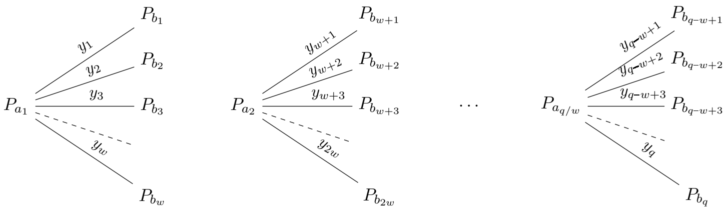
  $\Big\}\ \varepsilon = 0$

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

Mirror Theory Applied to CENC



Mirror Theory Applied to CENC

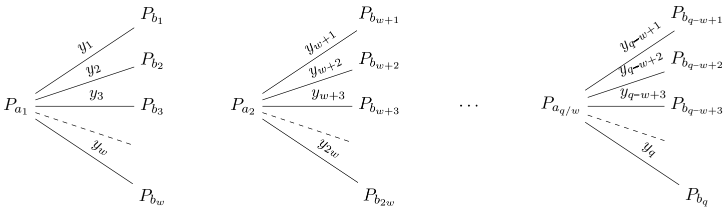


Applying Mirror Theory

- 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

  $\longrightarrow$ Call this a bad transcript
- Maximum tree size $w + 1$

Mirror Theory Applied to CENC

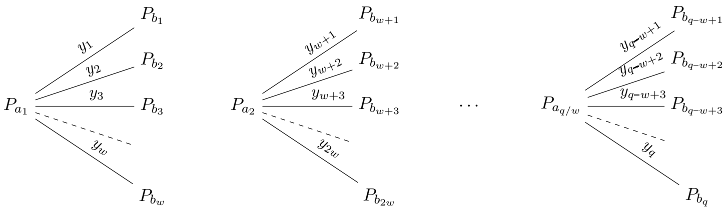


Applying Mirror Theory

- 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

  $\longrightarrow$ Call this a bad transcript
- 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

  $\longrightarrow$ Call this a bad transcript
- Maximum tree size $w + 1$
- If $2w^2q \leq 2^n/67$: at least $\frac{(2^n)_r}{2^{nq}}$ solutions to unknowns
- H-coefficient technique: $\mathbf{Adv}^{\mathrm{cpa}}_{\mathsf{CENC}}(q) \leq q/2^n + wq/2^{n+1}$

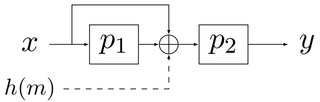
New Look at Mirror Theory

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

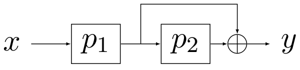
Mennink, Neves, CRYPTO 2017

- Refurbish and modernize mirror theory
- Prove optimal PRF security of:

E(WC)DM [CS16]



EDMD



- Proofs are more involved and beyond scope of presentation

Outline

PRP-PRF Conversion

Conclusion

Conclusion

Beyond Birthday-Bound Security

- Not the holy grail
- Relevant for certain applications
- Often achieved using
  - Extra randomness
  - Extra state size

Challenges

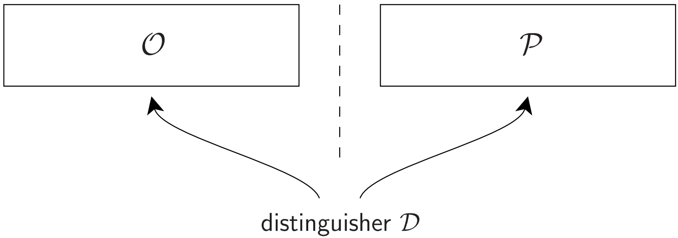
- Trade-off between security and efficiency
- Many open problems in BBB security
  - Existing analyses not always tight

Thank you for your attention!

SUPPORTING SLIDES

Indistinguishability

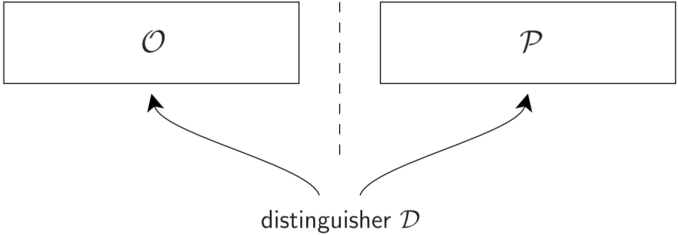
Indistinguishability of Random Systems



$$\mathbf{Adv}^{\mathrm{ind}}(\mathcal{D}) = \left|\mathbf{Pr}\left[\mathcal{D}^{\mathcal{O}} = 1\right] - \mathbf{Pr}\left[\mathcal{D}^{\mathcal{P}} = 1\right]\right| = \Delta_{\mathcal{D}}(\mathcal{O}\ ;\ \mathcal{P})$$

Indistinguishability

Indistinguishability of Random Systems

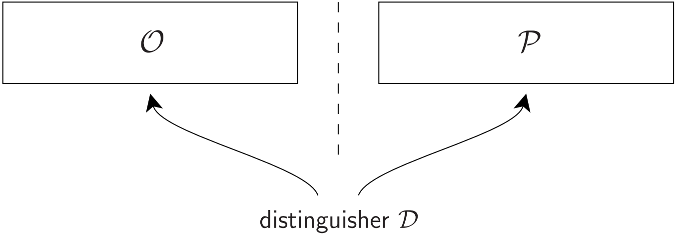


$$\mathbf{Adv}^{\mathrm{ind}}(\mathcal{D}) = \left|\mathbf{Pr}\left[\mathcal{D}^{\mathcal{O}} = 1\right] - \mathbf{Pr}\left[\mathcal{D}^{\mathcal{P}} = 1\right]\right| = \Delta_{\mathcal{D}}(\mathcal{O}\ ;\ \mathcal{P})$$

How to Prove that $\mathbf{Adv}^{\mathrm{ind}}(\mathcal{D})$ is Small?

Indistinguishability

Indistinguishability of Random Systems



$$\mathbf{Adv}^{\mathrm{ind}}(\mathcal{D}) = \left|\mathbf{Pr}\left[\mathcal{D}^{\mathcal{O}} = 1\right] - \mathbf{Pr}\left[\mathcal{D}^{\mathcal{P}} = 1\right]\right| = \Delta_{\mathcal{D}}(\mathcal{O}\ ;\ \mathcal{P})$$

How to Prove that $\mathbf{Adv}^{\mathrm{ind}}(\mathcal{D})$ is Small?

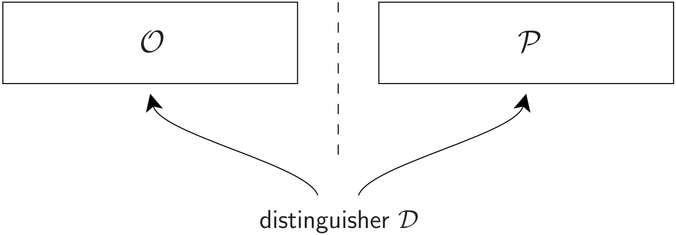
- Game-playing technique
- H-coefficient technique

Game-Playing Technique

- Bellare and Rogaway [BR06]
- Similar to Maurer's methodology [Mau02]

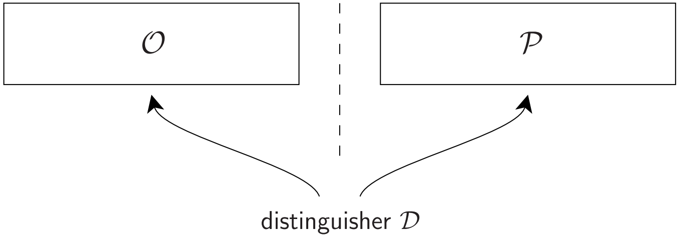
Game-Playing Technique

- Bellare and Rogaway [BR06]
- Similar to Maurer's methodology [Mau02]



Game-Playing Technique

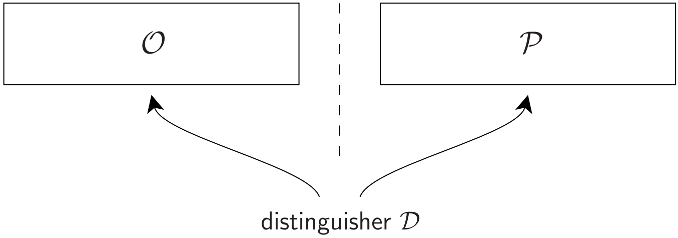
- Bellare and Rogaway [BR06]
- Similar to Maurer's methodology [Mau02]



- Basic idea:
    - From $\mathcal{O}$ to $\mathcal{P}$ in small steps

Game-Playing Technique

- Bellare and Rogaway [BR06]
- Similar to Maurer's methodology [Mau02]



- Basic idea:
  - From $\mathcal{O}$ to $\mathcal{P}$ in small steps
  - Intermediate steps (presumably) easy to analyze

Game-Playing Technique

Triangle Inequality

Fundamental Lemma

Game-Playing Technique

Triangle Inequality

$$\Delta(\mathcal{O};\mathcal{P}) \leq \Delta(\mathcal{O};\mathcal{R}) + \Delta(\mathcal{R};\mathcal{P})$$

Fundamental Lemma

Game-Playing Technique

Triangle Inequality

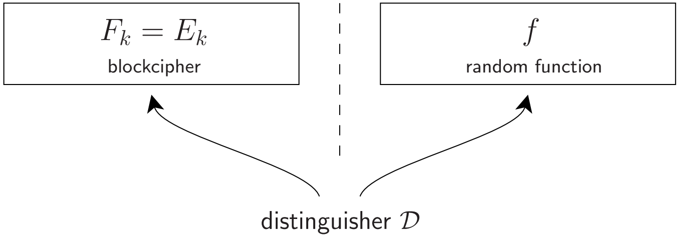
$$\Delta(\mathcal{O}; \mathcal{P}) \leq \Delta(\mathcal{O}; \mathcal{R}) + \Delta(\mathcal{R}; \mathcal{P})$$

Fundamental Lemma

If $\mathcal{O}$ and $\mathcal{P}$ are identical until bad, then:

$$\Delta(\mathcal{O}; \mathcal{P}) \leq \mathbf{Pr}\left[\mathcal{P} \text{ sets bad}\right]$$

Example: PRP-PRF Switch (1/4)



Theorem

For any distinguisher $\mathcal{D}$ making Q queries to E_k/p and T offline evaluations

$$\Delta_{\mathcal{D}}(E_k; f) \leq \mathbf{Adv}_E^{\mathrm{prp}}(\mathcal{D}) + \frac{\binom{Q}{2}}{2^n}$$

Example: PRP-PRF Switch (2/4)

$$\Delta_{\mathcal{D}}(E_k; f)$$

Example: PRP-PRF Switch (2/4)

Step 1. "Replace" E_k by Random Permutation p

$$\Delta_{\mathcal{D}}(E_k; f)$$

Example: PRP-PRF Switch (2/4)

Step 1. "Replace" E_k by Random Permutation p

- Triangle inequality:

$$\Delta_{\mathcal{D}}(E_k; f) \leq \Delta_{\mathcal{D}}(E_k; p) + \Delta_{\mathcal{D}}(p; f)$$

Example: PRP-PRF Switch (2/4)

Step 1. "Replace" E_k by Random Permutation p

- Triangle inequality:

$$\Delta_{\mathcal{D}}(E_k; f) \leq \Delta_{\mathcal{D}}(E_k; p) + \Delta_{\mathcal{D}}(p; f)$$

- $\Delta_{\mathcal{D}}(E_k; p) = \mathbf{Adv}_E^{\mathrm{prp}}(\mathcal{D})$ by definition

Example: PRP-PRF Switch (2/4)

Step 1. "Replace" E_k by Random Permutation p

- Triangle inequality:

$$\Delta_{\mathcal{D}}(E_k; f) \leq \Delta_{\mathcal{D}}(E_k; p) + \Delta_{\mathcal{D}}(p; f)$$

- $\Delta_{\mathcal{D}}(E_k; p) = \mathbf{Adv}_E^{\mathrm{prp}}(\mathcal{D})$ by definition
- $\Delta_{\mathcal{D}}(p; f)$
  - $\mathcal{D}$ is parametrized by Q queries to p/f

Example: PRP-PRF Switch (3/4)

Step 2. Random Permutation to Random Function

- Consider lazily sampled p and f
  - Initially empty list of responses $\mathcal{L}$
  - Randomly generated response for every new query

Example: PRP-PRF Switch (3/4)

Step 2. Random Permutation to Random Function

- Consider lazily sampled p and f
  - Initially empty list of responses $\mathcal{L}$
  - Randomly generated response for every new query

Oracle p
$y \xleftarrow{\$} \{0,1\}^n \backslash \mathcal{L}$ $\mathcal{L} \xleftarrow{\cup} y$ return y

Example: PRP-PRF Switch (3/4)

Step 2. Random Permutation to Random Function

- Consider lazily sampled p and f
  - Initially empty list of responses $\mathcal{L}$
  - Randomly generated response for every new query

Oracle p
$y \xleftarrow{\$} \{0,1\}^n \setminus \mathcal{L}$
$\mathcal{L} \xleftarrow{\cup} y$
return y

Oracle f
$y \xleftarrow{\$} \{0,1\}^n$
return y

Example: PRP-PRF Switch (3/4)

Step 2. Random Permutation to Random Function

- Consider lazily sampled p and f
  - Initially empty list of responses $\mathcal{L}$
  - Randomly generated response for every new query

Oracle p	Oracle p'	Oracle f

$y \xleftarrow{\$} \{0,1\}^n \backslash \mathcal{L}$	$y \xleftarrow{\$} \{0,1\}^n$
	if $y \in \mathcal{L}$
	    $y \xleftarrow{\$} \{0,1\}^n \backslash \mathcal{L}$
	    bad
		$y \xleftarrow{\$} \{0,1\}^n$

$\mathcal{L} \xleftarrow{\cup} y$ return y	$\mathcal{L} \xleftarrow{\cup} y$ return y	return y

Example: PRP-PRF Switch (4/4)

Oracle p	Oracle p'	Oracle f

$y \xleftarrow{\$} \{0,1\}^n \backslash \mathcal{L}$	$y \xleftarrow{\$} \{0,1\}^n$
	if $y \in \mathcal{L}$
	    $y \xleftarrow{\$} \{0,1\}^n \backslash \mathcal{L}$
	    bad
		$y \xleftarrow{\$} \{0,1\}^n$

$\mathcal{L} \xleftarrow{\cup} y$ return y	$\mathcal{L} \xleftarrow{\cup} y$ return y	return y

$$\Delta_{\mathcal{D}}(p; f)$$

Example: PRP-PRF Switch (4/4)

Oracle p	Oracle p'	Oracle f
$y \xleftarrow{\$} \{0,1\}^n \setminus \mathcal{L}$	$y \xleftarrow{\$} \{0,1\}^n$ if $y \in \mathcal{L}$ $y \xleftarrow{\$} \{0,1\}^n \setminus \mathcal{L}$ bad	$y \xleftarrow{\$} \{0,1\}^n$
$\mathcal{L} \xleftarrow{\cup} y$ return y	$\mathcal{L} \xleftarrow{\cup} y$ return y	return y

- Triangle inequality:

$$\Delta_{\mathcal{D}}(p; f) \leq \Delta_{\mathcal{D}}(p; p') + \Delta_{\mathcal{D}}(p'; f)$$

Example: PRP-PRF Switch (4/4)

Oracle p	Oracle p'	Oracle f

$y \xleftarrow{\$} \{0,1\}^n \backslash \mathcal{L}$	$y \xleftarrow{\$} \{0,1\}^n$
	if $y \in \mathcal{L}$
	    $y \xleftarrow{\$} \{0,1\}^n \backslash \mathcal{L}$
	    bad
		$y \xleftarrow{\$} \{0,1\}^n$

$\mathcal{L} \xleftarrow{\cup} y$ return y	$\mathcal{L} \xleftarrow{\cup} y$ return y	return y

identical

- Triangle inequality:

$$\Delta_{\mathcal{D}}(p; f) \leq \Delta_{\mathcal{D}}(p; p') + \Delta_{\mathcal{D}}(p'; f)$$
$$\leq \quad 0 \quad +$$

Example: PRP-PRF Switch (4/4)

Oracle p	Oracle p'	Oracle f
$y \xleftarrow{\$} \{0,1\}^n \backslash \mathcal{L}$	$y \xleftarrow{\$} \{0,1\}^n$	$y \xleftarrow{\$} \{0,1\}^n$
	if $y \in \mathcal{L}$	
	$\quad y \xleftarrow{\$} \{0,1\}^n \backslash \mathcal{L}$	
	$\quad$ bad	
$\mathcal{L} \xleftarrow{\cup} y$	$\mathcal{L} \xleftarrow{\cup} y$	
return y	return y	return y

identical

identical until bad

- Triangle inequality:

$$\begin{aligned}\Delta_{\mathcal{D}}(p; f) &\leq \Delta_{\mathcal{D}}(p; p') + \Delta_{\mathcal{D}}(p'; f) \\ &\leq \quad 0 \quad + \mathbf{Pr}\left[p' \text{ sets bad}\right]\end{aligned}$$

Example: PRP-PRF Switch (4/4)

Oracle p	Oracle p'	Oracle f

$y \xleftarrow{\$} \{0,1\}^n \setminus \mathcal{L}$	$y \xleftarrow{\$} \{0,1\}^n$
	if $y \in \mathcal{L}$
	    $y \xleftarrow{\$} \{0,1\}^n \setminus \mathcal{L}$
	    bad
		$y \xleftarrow{\$} \{0,1\}^n$

$\mathcal{L} \xleftarrow{\cup} y$ return y	$\mathcal{L} \xleftarrow{\cup} y$ return y	return y

identical

identical until bad

- Triangle inequality:

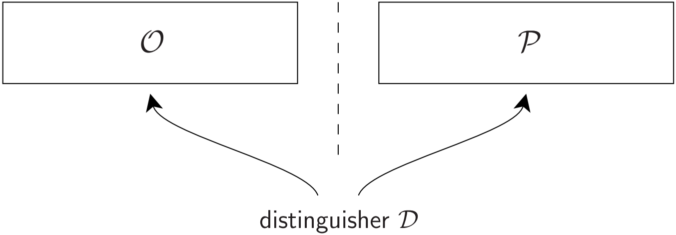
$$
\begin{aligned}
\Delta_{\mathcal{D}}(p; f) &\le \Delta_{\mathcal{D}}(p; p') + \Delta_{\mathcal{D}}(p'; f) \\
&\le \quad 0 \quad + \mathbf{Pr}\left[p' \text{ sets bad}\right] \le \frac{\binom{Q}{2}}{2^n}
\end{aligned}
$$

H-Coefficient Technique

- Patarin [Pat91,Pat08]
- Popularized by Chen and Steinberger [CS14]
- Similar to “Strong Interpolation Technique” [Ber05]

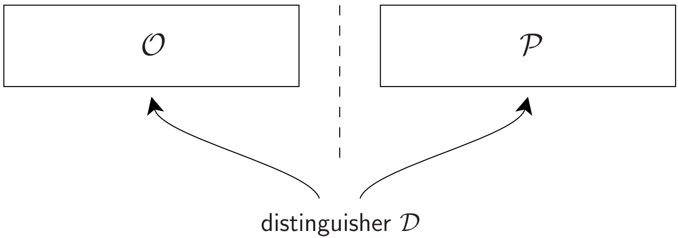
H-Coefficient Technique

- Patarin [Pat91,Pat08]
- Popularized by Chen and Steinberger [CS14]
- Similar to "Strong Interpolation Technique" [Ber05]



H-Coefficient Technique

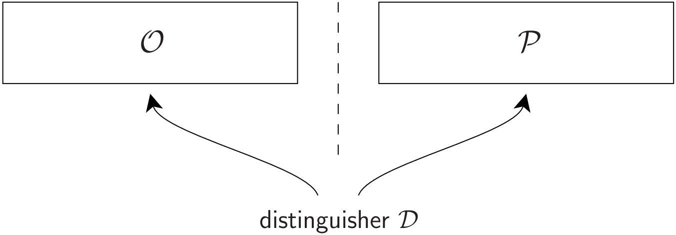
- Patarin [Pat91,Pat08]
- Popularized by Chen and Steinberger [CS14]
- Similar to "Strong Interpolation Technique" [Ber05]



- Basic idea:
  - Each conversation defines a transcript τ

H-Coefficient Technique

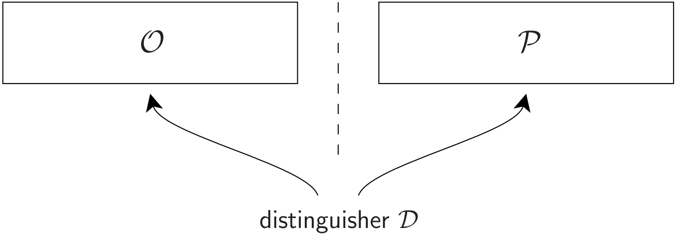
- Patarin [Pat91,Pat08]
- Popularized by Chen and Steinberger [CS14]
- Similar to “Strong Interpolation Technique” [Ber05]



- Basic idea:
  - Each conversation defines a transcript τ
  - $\mathcal{O} \approx \mathcal{P}$ for most of the transcripts

H-Coefficient Technique

- Patarin [Pat91,Pat08]
- Popularized by Chen and Steinberger [CS14]
- Similar to "Strong Interpolation Technique" [Ber05]



- Basic idea:
  - Each conversation defines a transcript τ
  - $\mathcal{O} \approx \mathcal{P}$ for most of the transcripts
  - Remaining transcripts occur with small probability

H-Coefficient Technique

- $\mathcal{D}$ is computationally unbounded and deterministic
- Each conversation defines a transcript τ

H-Coefficient Technique

- $\mathcal{D}$ is computationally unbounded and deterministic
- Each conversation defines a transcript τ
- Consider good and bad transcripts

H-Coefficient Technique

- $\mathcal{D}$ is computationally unbounded and deterministic
- Each conversation defines a transcript τ
- Consider good and bad transcripts

Lemma

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

$$\frac{\mathbf{Pr}\left[\mathcal{O} \text{ gives } \tau\right]}{\mathbf{Pr}\left[\mathcal{P} \text{ gives } \tau\right]} \geq 1 - \varepsilon$$

Then, $\Delta_{\mathcal{D}}(\mathcal{O}; P) \leq \varepsilon + \mathbf{Pr}\left[\text{bad transcript for } \mathcal{P}\right]$

H-Coefficient Technique

- $\mathcal{D}$ is computationally unbounded and deterministic
- Each conversation defines a transcript τ
- Consider good and bad transcripts

Lemma

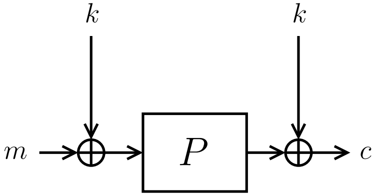
Let $\varepsilon \geq 0$ be such that for all good transcripts τ:

$$\frac{\mathbf{Pr}\left[\mathcal{O} \text{ gives } \tau\right]}{\mathbf{Pr}\left[\mathcal{P} \text{ gives } \tau\right]} \geq 1 - \varepsilon$$

Then, $\Delta_{\mathcal{D}}(\mathcal{O}; P) \leq \varepsilon + \mathbf{Pr}\left[\text{bad transcript for } \mathcal{P}\right]$

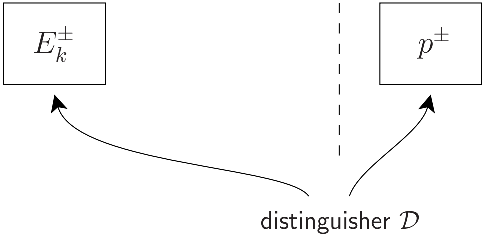
Trade-off: define bad transcripts smartly!

Example: Even-Mansour (1/10)



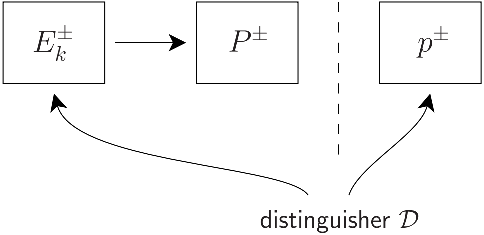
$$E_k(m) = P(m \oplus k) \oplus k$$

Example: Even-Mansour (2/10)



Slightly Different Security Model

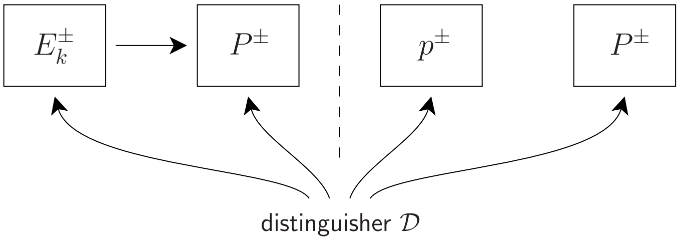
Example: Even-Mansour (2/10)



Slightly Different Security Model

- Underlying permutation

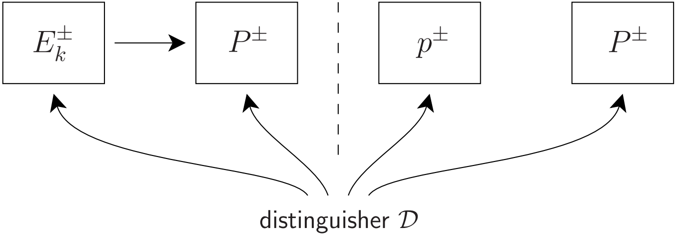
Example: Even-Mansour (2/10)



Slightly Different Security Model

- Underlying permutation randomized
- Information-theoretic distinguisher $\mathcal{D}$
  - Q construction queries
  - T offline evaluations $\approx T$ primitive queries

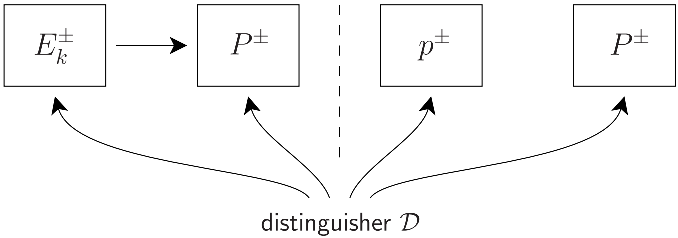
Example: Even-Mansour (2/10)



Slightly Different Security Model

- Underlying permutation randomized
- Information-theoretic distinguisher $\mathcal{D}$
  - Q construction queries
  - T offline evaluations $\approx T$ primitive queries
  - Unbounded computational power

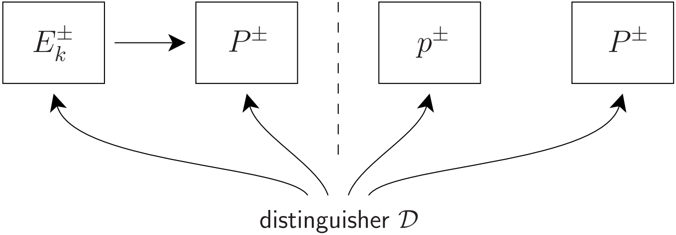
Example: Even-Mansour (3/10)



Slightly Different Security Model

- Without loss of generality, $\mathcal{D}$ is deterministic
  - No random choices

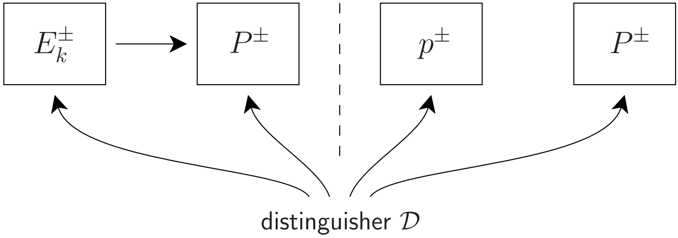
Example: Even-Mansour (3/10)



Slightly Different Security Model

- Without loss of generality, $\mathcal{D}$ is deterministic
  - No random choices
- Reason: at the end we maximize over all distinguishers

Example: Even-Mansour (4/10)



Theorem

For any deterministic distinguisher $\mathcal{D}$ making Q queries to E_k/f and T primitive queries

$$\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{D}) = \Delta_{\mathcal{D}}(E_k^{\pm}, P^{\pm}; p^{\pm}, P^{\pm}) \leq \frac{2QT}{2^n}$$

Example: Even-Mansour (5/10)

Step 1. Define how transcripts look like

Step 2. Define good and bad transcripts

Step 3. Upper bound $\mathbf{Pr}\left[\text{bad transcript for } (p^{\pm}, P^{\pm})\right]$

Step 4. Lower bound $\frac{\mathbf{Pr}\left[(E_k^{\pm},P^{\pm}) \text{ gives } \tau\right]}{\mathbf{Pr}\left[(p^{\pm},P^{\pm}) \text{ gives } \tau\right]} \geq 1 - \varepsilon$ ($\forall$ good τ)

Example: Even-Mansour (6/10)

1. **Define how transcripts look like**
   - Construction queries:
   $$\tau_E = \{(m_1, c_1), \ldots, (m_Q, c_Q)\}$$
   - Primitive queries:
   $$\tau_P = \{(x_1, y_1), \ldots, (x_T, y_T)\}$$

Example: Even-Mansour (6/10)

1. Define how transcripts look like

- Construction queries:

$$\tau_E = \{(m_1, c_1), \ldots, (m_Q, c_Q)\}$$

- Primitive queries:

$$\tau_P = \{(x_1, y_1), \ldots, (x_T, y_T)\}$$

- Unordered lists (ordering not needed in current proof)
- 1-to-1 correspondence between any $\mathcal{D}$ and any (τ_E, τ_P)

Example: Even-Mansour (6/10)

1. Define how transcripts look like

- Construction queries:

$$\tau_E = \{(m_1, c_1), \ldots, (m_Q, c_Q)\}$$

- Primitive queries:

$$\tau_P = \{(x_1, y_1), \ldots, (x_T, y_T)\}$$

- Unordered lists (ordering not needed in current proof)
- 1-to-1 correspondence between any $\mathcal{D}$ and any (τ_E, τ_P)

- Bonus information!
  - After interaction of $\mathcal{D}$ with oracles: reveal the key

Example: Even-Mansour (6/10)

1. Define how transcripts look like

- Construction queries:

$$\tau_E = \{(m_1, c_1), \ldots, (m_Q, c_Q)\}$$

- Primitive queries:

$$\tau_P = \{(x_1, y_1), \ldots, (x_T, y_T)\}$$

- Unordered lists (ordering not needed in current proof)
- 1-to-1 correspondence between any $\mathcal{D}$ and any (τ_E, τ_P)

- Bonus information!
  - After interaction of $\mathcal{D}$ with oracles: reveal the key
  - Real world $(E_k^{\pm}, P^{\pm})$: key used for encryption

Example: Even-Mansour (6/10)

1. Define how transcripts look like

- Construction queries:

$$\tau_E = \{(m_1, c_1), \ldots, (m_Q, c_Q)\}$$

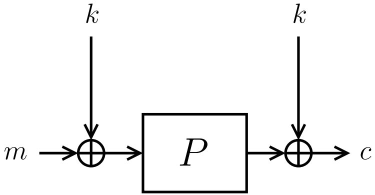
- Primitive queries:

$$\tau_P = \{(x_1, y_1), \ldots, (x_T, y_T)\}$$

- Unordered lists (ordering not needed in current proof)
- 1-to-1 correspondence between any $\mathcal{D}$ and any (τ_E, τ_P)
- Bonus information!

  - After interaction of $\mathcal{D}$ with oracles: reveal the key
  - Real world $(E_k^{\pm}, P^{\pm})$: key used for encryption
  - Ideal world $(p^{\pm}, P^{\pm})$: dummy key $k \xleftarrow{\$} \{0,1\}^n$

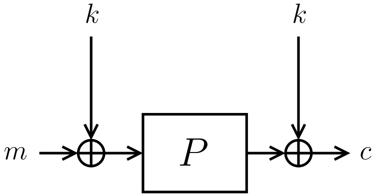
Example: Even-Mansour (7/10)



2. Define good and bad transcripts

- Intuition:

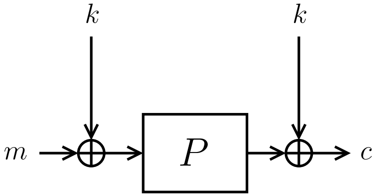
Example: Even-Mansour (7/10)



2. Define good and bad transcripts

- Intuition:
  - $(m, c) \in \tau_E$ "defines" P-query $(m \oplus k, c \oplus k)$

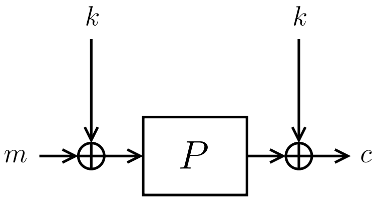
Example: Even-Mansour (7/10)



2. Define good and bad transcripts

- Intuition:
  - $(m, c) \in \tau_E$ "defines" P-query $(m \oplus k, c \oplus k)$
  - Should not collide with any $(x, y) \in \tau_P$

Example: Even-Mansour (7/10)

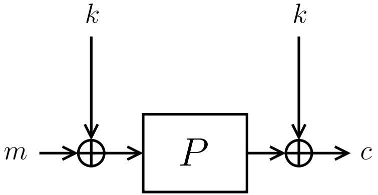


2. Define good and bad transcripts

- Intuition:
  - $(m, c) \in \tau_E$ "defines" P-query $(m \oplus k, c \oplus k)$
  - Should not collide with any $(x, y) \in \tau_P$
- Transcript $\tau = (\tau_E, \tau_P, k)$ is bad if

$\exists (m, c) \in \tau_E, (x, y) \in \tau_P$ such that $m \oplus k = x$ or $c \oplus k = y$

Example: Even-Mansour (7/10)



2. Define good and bad transcripts

- Intuition:
  - $(m, c) \in \tau_E$ "defines" P-query $(m \oplus k, c \oplus k)$
  - Should not collide with any $(x, y) \in \tau_P$
- Transcript $\tau = (\tau_E, \tau_P, k)$ is bad if

$\exists (m, c) \in \tau_E, (x, y) \in \tau_P$ such that $m \oplus k = x$ or $c \oplus k = y$

- Note: no internal collisions in τ_E and τ_P

Example: Even-Mansour (8/10)

3. Upper bound $\mathbf{Pr}\big[$bad transcript for $(\boldsymbol{p}^{\pm}, \boldsymbol{P}^{\pm})\big]$

- Transcript $\tau = (\tau_E, \tau_P, k)$ is bad if

$\exists (m, c) \in \tau_E, (x, y) \in \tau_P$ such that $m \oplus k = x$ or $c \oplus k = y$

Example: Even-Mansour (8/10)

3. Upper bound $\mathbf{Pr}\left[\text{bad transcript for } (p^{\pm}, P^{\pm})\right]$

- Transcript $\tau = (\tau_E, \tau_P, k)$ is bad if

$\exists (m,c) \in \tau_E, (x,y) \in \tau_P$ such that $m \oplus k = x$ or $c \oplus k = y$

$$\Updownarrow$$

$$k \in \{m \oplus x, c \oplus y \mid (m,c) \in \tau_E, (x,y) \in \tau_P\}$$

Example: Even-Mansour (8/10)

3. Upper bound $\mathbf{Pr}\left[\text{bad transcript for } (\boldsymbol{p}^{\pm}, \boldsymbol{P}^{\pm})\right]$

- Transcript $\tau = (\tau_E, \tau_P, k)$ is bad if

$\exists (m, c) \in \tau_E, (x, y) \in \tau_P$ such that $m \oplus k = x$ or $c \oplus k = y$

$$\Updownarrow$$

$$k \in \underbrace{\{m \oplus x, c \oplus y \mid (m, c) \in \tau_E, (x, y) \in \tau_P\}}_{\text{of size } \leq 2QT}$$

Example: Even-Mansour (8/10)

3. Upper bound $\mathbf{Pr}\big[$bad transcript for $(p^{\pm}, P^{\pm})\big]$

- Transcript $\tau = (\tau_E, \tau_P, k)$ is bad if

$$\exists (m,c) \in \tau_E, (x,y) \in \tau_P \text{ such that } m \oplus k = x \text{ or } c \oplus k = y$$

$$\Updownarrow$$

$$\underset{\uparrow}{k} \in \underbrace{\{m \oplus x, c \oplus y \mid (m,c) \in \tau_E, (x,y) \in \tau_P\}}_{\text{of size } \leq 2QT}$$

independently generated n-bit dummy key

Example: Even-Mansour (8/10)

3. Upper bound $\mathbf{Pr}\left[\text{bad transcript for } (p^{\pm}, P^{\pm})\right]$

- Transcript $\tau = (\tau_E, \tau_P, k)$ is bad if

$$\exists (m, c) \in \tau_E, (x, y) \in \tau_P \text{ such that } m \oplus k = x \text{ or } c \oplus k = y$$

$$\Updownarrow$$

$$k \in \underbrace{\{m \oplus x, c \oplus y \mid (m, c) \in \tau_E, (x, y) \in \tau_P\}}_{\text{of size } \leq 2QT}$$

$\uparrow$

independently generated n-bit dummy key

$$\mathbf{Pr}\left[\text{bad transcript for } (p^{\pm}, P^{\pm})\right] \leq \frac{2QT}{2^n}$$

Example: Even-Mansour (9/10)

4. Lower bound $\dfrac{\mathbf{Pr}\left[(E_k^{\pm},P^{\pm}) \text{ gives } \tau\right]}{\mathbf{Pr}\left[(p^{\pm},P^{\pm}) \text{ gives } \tau\right]} \geq 1-\varepsilon$ **($\forall$ good τ)**

Example: Even-Mansour (9/10)

4. Lower bound $\dfrac{\mathbf{Pr}\left[(E_k^{\pm}, P^{\pm}) \text{ gives } \tau\right]}{\mathbf{Pr}\left[(p^{\pm}, P^{\pm}) \text{ gives } \tau\right]} \geq 1 - \varepsilon \ (\forall \text{ good } \tau)$

- Counting "compatible" oracles (modulo details):

$$\mathbf{Pr}\left[\mathcal{O} \text{ gives } \tau\right] = \frac{\left|\text{oracles } \mathcal{O} \text{ that could give } \tau\right|}{\left|\text{oracles } \mathcal{O}\right|}$$

Example: Even-Mansour (9/10)

4. Lower bound $\frac{\mathbf{Pr}\left[(E_k^{\pm},P^{\pm}) \text{ gives } \tau\right]}{\mathbf{Pr}\left[(p^{\pm},P^{\pm}) \text{ gives } \tau\right]} \geq 1-\varepsilon$ **($\forall$ good τ)**

- Counting "compatible" oracles (modulo details):

$$\mathbf{Pr}\left[\mathcal{O} \text{ gives } \tau\right] = \frac{\left|\text{oracles } \mathcal{O} \text{ that could give } \tau\right|}{\left|\text{oracles } \mathcal{O}\right|}$$

- For real world $(E_k^{\pm}, P^{\pm})$:

$$\mathbf{Pr}\left[(E_k^{\pm}, P^{\pm}) \text{ gives } \tau\right] = \rule{4cm}{0.4pt}$$

Example: Even-Mansour (9/10)

4. Lower bound $\frac{\mathbf{Pr}\left[(E_k^{\pm},P^{\pm}) \text{ gives } \tau\right]}{\mathbf{Pr}\left[(p^{\pm},P^{\pm}) \text{ gives } \tau\right]} \geq 1-\varepsilon$ **($\forall$ good τ)**

- Counting "compatible" oracles (modulo details):

$$\mathbf{Pr}\left[\mathcal{O} \text{ gives } \tau\right] = \frac{\left|\text{oracles } \mathcal{O} \text{ that could give } \tau\right|}{\left|\text{oracles } \mathcal{O}\right|}$$

- For real world $(E_k^{\pm}, P^{\pm})$:

$$\mathbf{Pr}\left[(E_k^{\pm}, P^{\pm}) \text{ gives } \tau\right] = \frac{\qquad}{2^n \cdot 2^n!}$$

Example: Even-Mansour (9/10)

4. Lower bound $\dfrac{\mathbf{Pr}\left[(E_k^{\pm}, P^{\pm}) \text{ gives } \tau\right]}{\mathbf{Pr}\left[(p^{\pm}, P^{\pm}) \text{ gives } \tau\right]} \geq 1 - \varepsilon$ **($\forall$ good τ)**

- Counting "compatible" oracles (modulo details):

$$\mathbf{Pr}\left[\mathcal{O} \text{ gives } \tau\right] = \frac{\left|\text{oracles } \mathcal{O} \text{ that could give } \tau\right|}{\left|\text{oracles } \mathcal{O}\right|}$$

- For real world $(E_k^{\pm}, P^{\pm})$:

$$\mathbf{Pr}\left[(E_k^{\pm}, P^{\pm}) \text{ gives } \tau\right] = \frac{(2^n - Q - T)!}{2^n \cdot 2^n!}$$

Example: Even-Mansour (9/10)

4. Lower bound $\frac{\mathbf{Pr}\left[(E_k^\pm, P^\pm) \text{ gives } \tau\right]}{\mathbf{Pr}\left[(p^\pm, P^\pm) \text{ gives } \tau\right]} \geq 1 - \varepsilon$ **($\forall$ good τ)**

- Counting "compatible" oracles (modulo details):

$$\mathbf{Pr}\left[\mathcal{O} \text{ gives } \tau\right] = \frac{\left|\text{oracles } \mathcal{O} \text{ that could give } \tau\right|}{\left|\text{oracles } \mathcal{O}\right|}$$

- For real world $(E_k^\pm, P^\pm)$:

$$\mathbf{Pr}\left[(E_k^\pm, P^\pm) \text{ gives } \tau\right] = \frac{(2^n - Q - T)!}{2^n \cdot 2^n!}$$

- For ideal world $(p^\pm, P^\pm)$:

$$\mathbf{Pr}\left[(p^\pm, P^\pm) \text{ gives } \tau\right] = \frac{(2^n - Q)!(2^n - T)!}{2^n \cdot (2^n!)^2}$$

Example: Even-Mansour (10/10)

4. Lower bound $\dfrac{\mathbf{Pr}\left[(E_k^\pm, P^\pm) \text{ gives } \tau\right]}{\mathbf{Pr}\left[(p^\pm, P^\pm) \text{ gives } \tau\right]} \geq 1 - \varepsilon$ **($\forall$ good τ)**

- Putting things together:

$$\frac{\mathbf{Pr}\left[(E_k^\pm, P^\pm) \text{ gives } \tau\right]}{\mathbf{Pr}\left[(p^\pm, P^\pm) \text{ gives } \tau\right]} = \frac{\frac{(2^n-Q-T)!}{2^n \cdot 2^n!}}{\frac{(2^n-Q)!(2^n-T)!}{2^n \cdot (2^n!)^2}}$$

$$= \frac{(2^n - Q - T)!2^n!}{(2^n - Q)!(2^n - T)!}$$

Example: Even-Mansour (10/10)

4. Lower bound $\dfrac{\mathbf{Pr}\left[(E_k^{\pm}, P^{\pm}) \text{ gives } \tau\right]}{\mathbf{Pr}\left[(p^{\pm}, P^{\pm}) \text{ gives } \tau\right]} \geq 1 - \varepsilon$ **($\forall$ good τ)**

- Putting things together:

$$\frac{\mathbf{Pr}\left[(E_k^{\pm}, P^{\pm}) \text{ gives } \tau\right]}{\mathbf{Pr}\left[(p^{\pm}, P^{\pm}) \text{ gives } \tau\right]} = \frac{\frac{(2^n-Q-T)!}{2^n \cdot 2^n!}}{\frac{(2^n-Q)!(2^n-T)!}{2^n \cdot (2^n!)^2}}$$

$$= \frac{(2^n - Q - T)!2^n!}{(2^n - Q)!(2^n - T)!}$$

$$\geq 1$$

Example: Even-Mansour (10/10)

4. Lower bound $\frac{\mathbf{Pr}\left[(E_k^{\pm},P^{\pm}) \text{ gives } \tau\right]}{\mathbf{Pr}\left[(p^{\pm},P^{\pm}) \text{ gives } \tau\right]} \geq 1-\varepsilon$ **($\forall$ good τ)**

- Putting things together:

$$\frac{\mathbf{Pr}\left[(E_k^{\pm},P^{\pm}) \text{ gives } \tau\right]}{\mathbf{Pr}\left[(p^{\pm},P^{\pm}) \text{ gives } \tau\right]} = \frac{\frac{(2^n-Q-T)!}{2^n\cdot 2^n!}}{\frac{(2^n-Q)!(2^n-T)!}{2^n\cdot(2^n!)^2}}$$

$$= \frac{(2^n-Q-T)!2^n!}{(2^n-Q)!(2^n-T)!}$$

$$\geq 1$$

- We put $\varepsilon = 0$

Example: Even-Mansour (10/10)

4. Lower bound $\frac{\mathbf{Pr}\left[(E_k^{\pm},P^{\pm})\text{ gives }\tau\right]}{\mathbf{Pr}\left[(p^{\pm},P^{\pm})\text{ gives }\tau\right]} \geq 1-\varepsilon$ **($\forall$ good τ)**

- Putting things together:

$$\frac{\mathbf{Pr}\left[(E_k^{\pm},P^{\pm})\text{ gives }\tau\right]}{\mathbf{Pr}\left[(p^{\pm},P^{\pm})\text{ gives }\tau\right]} = \frac{\frac{(2^n-Q-T)!}{2^n\cdot 2^n!}}{\frac{(2^n-Q)!(2^n-T)!}{2^n\cdot(2^n!)^2}}$$
$$= \frac{(2^n-Q-T)!2^n!}{(2^n-Q)!(2^n-T)!}$$
$$\geq 1$$

- We put $\varepsilon = 0$

- Conclusion:

$$\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{D}) = \Delta_{\mathcal{D}}(E_k^{\pm},P^{\pm};p^{\pm},P^{\pm}) \leq \frac{2QT}{2^n} + 0$$