On the XOR of Multiple Random Permutations

Bart Mennink and Bart Preneel
KU Leuven (Belgium)

Applied Cryptography and Network Security
June 5, 2015

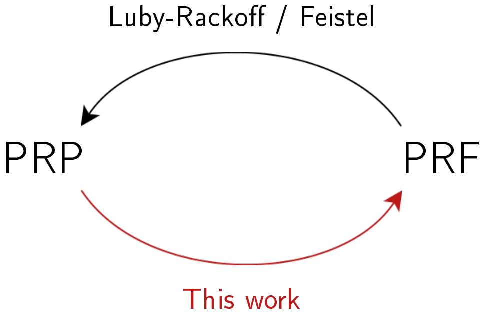
Introduction

PRP PRF

Introduction

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

Introduction



Introduction

$$
\begin{tikzcd}
\mathsf{PRP} \arrow[r, bend right] & \mathsf{PRF}
\end{tikzcd}
$$

Introduction

$$\begin{tikzcd} \text{PRP} \arrow[rr, bend right] & & \text{PRF} \end{tikzcd}$$

- Let E_K be a PRP

Introduction

$$\begin{tikzcd} \text{PRP} \arrow[r, bend right] & \text{PRF} \end{tikzcd}$$

- Let E_K be a PRP
  - $f_K(x) = E_{E_K(x)}(x)$

Introduction

$$\begin{tikzcd} \text{PRP} \arrow[rr, bend right] & & \text{PRF} \end{tikzcd}$$

- Let E_K be a PRP
  - $f_K(x) = E_{E_K(x)}(x)$
  - $f_K(x) = E_K(x) \oplus x$

Introduction

$$\begin{tikzcd} \text{PRP} \arrow[r, bend right] & \text{PRF} \end{tikzcd}$$

- Let E_K be a PRP
  - $f_K(x) = E_{E_K(x)}(x)$
  - $f_K(x) = E_K(x) \oplus x$
  - $f_K(x) = E_K(x)$

Introduction

PRP $\longrightarrow$ PRF

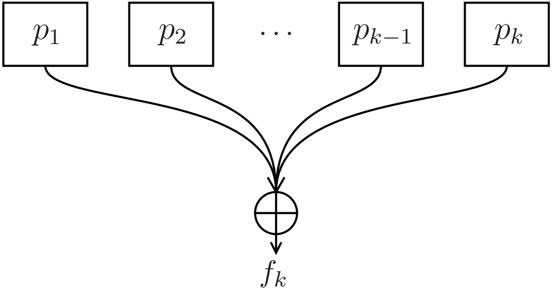
- Let E_K be a PRP
  - $f_K(x) = E_{E_K(x)}(x)$
  - $f_K(x) = E_K(x) \oplus x$
  - $f_K(x) = E_K(x)$
- All: secure PRFs up to birthday bound

Introduction

$$\text{PRP} \longrightarrow \text{PRF}$$

- Let E_K be a PRP
  - $f_K(x) = E_{E_K(x)}(x)$
  - $f_K(x) = E_K(x) \oplus x$
  - $f_K(x) = E_K(x)$
- All: secure PRFs up to birthday bound
- XOR of multiple PRPs: $E_{K_1}(x) \oplus \cdots \oplus E_{K_k}(x)$?

XOR of Multiple Permutations



$$f_k(x) = p_1(x) \oplus \cdots \oplus p_k(x)$$

Instantiations

Secret Permutations

- Based on $E_{K_1}, \ldots, E_{K_k}$
- Adversary can only evaluate f_k

  $\longrightarrow$ indistinguishability

Instantiations

Secret Permutations

- Based on $E_{K_1}, \ldots, E_{K_k}$
- Adversary can only evaluate f_k

$\longrightarrow$ indistinguishability

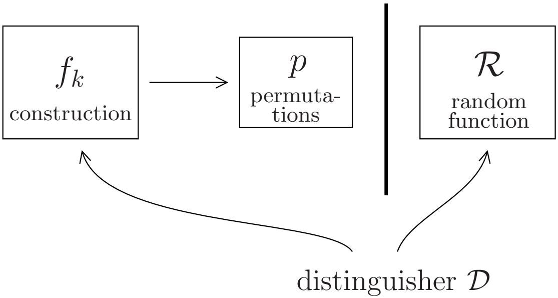
Public Permutations

- Based on stand-alone $p_1, \ldots, p_k$
- Adversary can evaluate f_k and $p_1, \ldots, p_k$

$\longrightarrow$ indifferentiability

Indistinguishability of f_k (p_i secret)

Indistinguishability of f_k: Security Model



- $p = (p_1, \ldots, p_k)$ random n-bit permutations
- $\mathcal{R}$ random n-bit function
- Distinguisher $\mathcal{D}$ computationally unbounded

Indistinguishability of f_k: State of the Art

indistinguishability (p_i secret)	k	bound	reference
	≥ 1	$2^{\frac{k}{k+1}n}$	[Lucks00]
	2	$2^n/n^{2/3}$	[Bellare99]
	2	2^n	[Patarin08]
	≥ 3	$2^{\frac{2k+1}{2k+2}n}$	[CogliatiLP14]

Indistinguishability of f_k: State of the Art

indistinguishability (p_i secret)	k	bound	reference
	≥ 1	$2^{\frac{k}{k+1}n}$	[Lucks00]
	2	$2^n/n^{2/3}$	[Bellare99]
	2	2^n	[Patarin08]
	≥ 3	$2^{\frac{2k+1}{2k+2}n}$	[CogliatiLP14]

Conjectured 2^n

Indistinguishability of f_k: Short Proof

Theorem For all $k \geq 2$, we have $\mathsf{Adv}^{\mathrm{dist}}_{f_{k+1}}(\mathcal{D}) \leq \mathsf{Adv}^{\mathrm{dist}}_{f_k}(\mathcal{D})$

Indistinguishability of f_k: Short Proof

Theorem For all $k \geq 2$, we have $\mathsf{Adv}^{\mathrm{dist}}_{f_{k+1}}(\mathcal{D}) \leq \mathsf{Adv}^{\mathrm{dist}}_{f_k}(\mathcal{D})$

Proof

- Security of f_{k+1}
  $\longrightarrow$ $\mathcal{D}$ queries $p_1 \oplus \cdots \oplus p_{k+1}$ or $\mathcal{R}$

Indistinguishability of f_k: Short Proof

Theorem For all $k \geq 2$, we have $\mathsf{Adv}^{\mathrm{dist}}_{f_{k+1}}(\mathcal{D}) \leq \mathsf{Adv}^{\mathrm{dist}}_{f_k}(\mathcal{D})$

Proof

- Security of f_{k+1}
  $\longrightarrow \mathcal{D}$ queries $p_1 \oplus \cdots \oplus p_{k+1}$ or $\mathcal{R}$
- Reveal output p_{k+1} for every query (in both worlds)

Indistinguishability of f_k: Short Proof

Theorem For all $k \geq 2$, we have $\mathsf{Adv}^{\mathrm{dist}}_{f_{k+1}}(\mathcal{D}) \leq \mathsf{Adv}^{\mathrm{dist}}_{f_k}(\mathcal{D})$

Proof

- Security of f_{k+1}
  $\longrightarrow$ $\mathcal{D}$ queries $p_1 \oplus \cdots \oplus p_{k+1}$ or $\mathcal{R}$
- Reveal output p_{k+1} for every query (in both worlds)
- $\mathcal{D}$ effectively queries $p_1 \oplus \cdots \oplus p_k$ or $\mathcal{R}' := \mathcal{R} \oplus p_{k+1}$

Indistinguishability of f_k: Short Proof

Theorem For all $k \geq 2$, we have $\mathsf{Adv}^{\mathrm{dist}}_{f_{k+1}}(\mathcal{D}) \leq \mathsf{Adv}^{\mathrm{dist}}_{f_k}(\mathcal{D})$

Proof

- Security of f_{k+1}
  $\longrightarrow$ $\mathcal{D}$ queries $p_1 \oplus \cdots \oplus p_{k+1}$ or $\mathcal{R}$
- Reveal output p_{k+1} for every query (in both worlds)
- $\mathcal{D}$ effectively queries $p_1 \oplus \cdots \oplus p_k$ or $\mathcal{R}' := \mathcal{R} \oplus p_{k+1}$
  $\longrightarrow$ Security of f_k

Indistinguishability of f_k: Short Proof

Theorem For all $k \geq 2$, we have $\mathsf{Adv}^{\mathrm{dist}}_{f_{k+1}}(\mathcal{D}) \leq \mathsf{Adv}^{\mathrm{dist}}_{f_k}(\mathcal{D})$

Proof

- Security of f_{k+1}
  $\longrightarrow$ $\mathcal{D}$ queries $p_1 \oplus \cdots \oplus p_{k+1}$ or $\mathcal{R}$
- Reveal output p_{k+1} for every query (in both worlds)
- $\mathcal{D}$ effectively queries $p_1 \oplus \cdots \oplus p_k$ or $\mathcal{R}' := \mathcal{R} \oplus p_{k+1}$
  $\longrightarrow$ Security of f_k

Lemma [Patarin08] We have $\mathsf{Adv}^{\mathrm{dist}}_{f_2}(\mathcal{D}) = \mathcal{O}(q/2^n)$

Indistinguishability of f_k: Short Proof

Theorem For all $k \geq 2$, we have $\mathsf{Adv}^{\mathrm{dist}}_{f_{k+1}}(\mathcal{D}) \leq \mathsf{Adv}^{\mathrm{dist}}_{f_k}(\mathcal{D})$

Proof

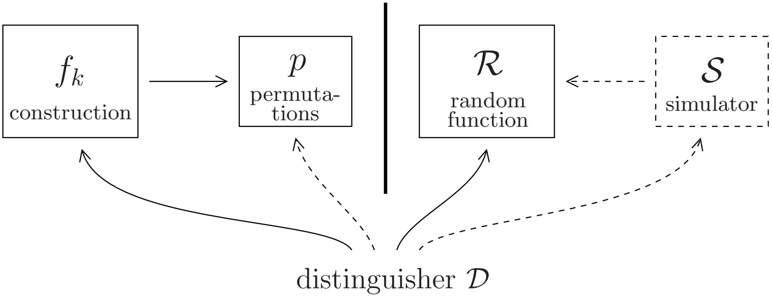
- Security of f_{k+1}
  $\longrightarrow$ $\mathcal{D}$ queries $p_1 \oplus \cdots \oplus p_{k+1}$ or $\mathcal{R}$
- Reveal output p_{k+1} for every query (in both worlds)
- $\mathcal{D}$ effectively queries $p_1 \oplus \cdots \oplus p_k$ or $\mathcal{R}' := \mathcal{R} \oplus p_{k+1}$
  $\longrightarrow$ Security of f_k

Lemma [Patarin08] We have $\mathsf{Adv}^{\mathrm{dist}}_{f_2}(\mathcal{D}) = \mathcal{O}(q/2^n)$

Corollary For all $k \geq 2$, we have $\mathsf{Adv}^{\mathrm{dist}}_{f_k}(\mathcal{D}) = \mathcal{O}(q/2^n)$

Indifferentiability of f_k (p_i public)

Indifferentiability of f_k: Security Model



- Extends indistinguishability: structure of f_k is known
- f_k indifferentiable from $\mathcal{R}$ if $\exists$ simulator $\mathcal{S}$ such that (f_k, p) and $(\mathcal{R}, \mathcal{S})$ are indistinguishable

Indifferentiability of f_k: State of the Art

indifferentiability	k	bound	reference
(p_i public)	2	$2^{n/2}$	[MandalPN10]
	2	$2^{2n/3}$	[MandalPN10]

Our Contribution

-
-

Indifferentiability of f_k: State of the Art

indifferentiability	k	bound	reference
(p_i public)	2	$2^{n/2}$	[MandalPN10]
	$\cancel{2}$	$\cancel{2^{2n/3}}$	~~[MandalPN10]~~

Our Contribution

- Flaw in proof of [MandalPN10]
-

Indifferentiability of f_k: State of the Art

indifferentiability	k	bound	reference
(p_i public)	2	$2^{n/2}$	[MandalPN10]
	$\cancel{2}$	$\cancel{2^{2n/3}}$	~~[MandalPN10]~~
	≥ 2	$2^{2n/3}$	

Our Contribution

- Flaw in proof of [MandalPN10]
- Re-confirmation and generalization of bound

Indifferentiability of f_k: New Result

Theorem For all $k \geq 2$, there exists a simulator $\mathcal{S}$ such that

$$\mathsf{Adv}^{\mathrm{diff}}_{f_k,\mathcal{S}}(\mathcal{D}) \leq \frac{4q^3}{2^{2n}} + \frac{3n^{1/2}q^{3/2}}{2^n} + \frac{2}{2^n}$$

- Old bound: $\frac{96q^3}{2^{2n}} + \frac{1}{2^{11n}}$ [MandalPN10]

Indifferentiability of f_k: New Result

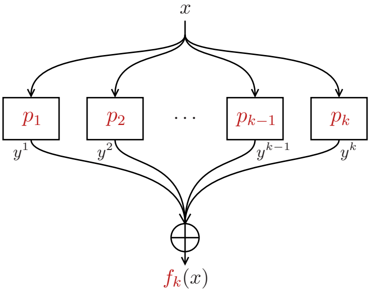
Theorem For all $k \geq 2$, there exists a simulator $\mathcal{S}$ such that

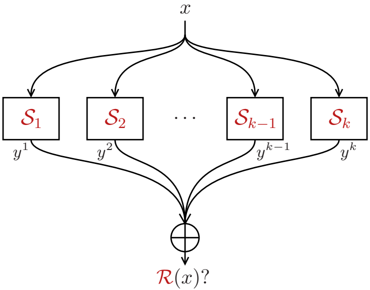
$$\mathsf{Adv}^{\mathrm{diff}}_{f_k,\mathcal{S}}(\mathcal{D}) \leq \frac{4q^3}{2^{2n}} + \frac{3n^{1/2}q^{3/2}}{2^n} + \frac{2}{2^n}$$

- Old bound: $\frac{96q^3}{2^{2n}} + \frac{1}{2^{11n}}$ [MandalPN10]

- Simulator $\mathcal{S}$ and proof similar to the old ones
- Now: high-level intuition

Indifferentiability of f_k: Simulator

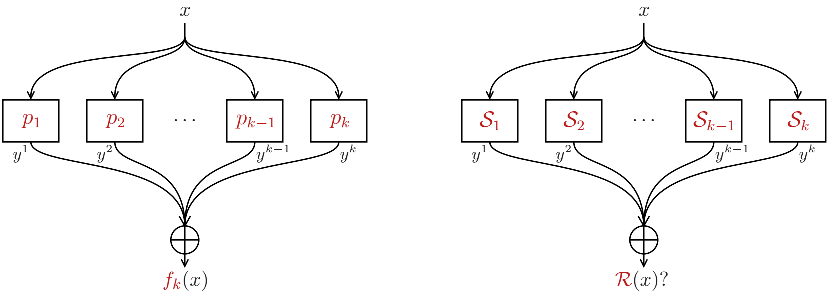




Goal of Simulator

- Tries to answer queries such that $(f_k, p) \approx (\mathcal{R}, \mathcal{S})$

Indifferentiability of f_k: Simulator



Goal of Simulator

- Tries to answer queries such that $(f_k, p) \approx (\mathcal{R}, \mathcal{S})$
- Query-responses $(x, y^1, \ldots, y^k)$ should satisfy
  - $\mathcal{R}(x) = y^1 \oplus \cdots \oplus y^k$
  - x and y^ℓ permutation-wise distinct for all $\ell = 1, \ldots, k$

Indifferentiability of f_k: Proof Idea

Patarin's H-coefficient Technique

- Each conversation defines a transcript
- Define good and bad transcripts

Indifferentiability of f_k: Proof Idea

Patarin's H-coefficient Technique

- Each conversation defines a transcript
- Define good and bad transcripts

$$\mathsf{Adv}^{\mathrm{diff}}_{f_k,\mathcal{S}}(\mathcal{D}) \leq \varepsilon + \mathbf{P}\left(\text{bad transcript for } (f_k, p)\right)$$

$\Lsh$ prob. ratio for good transcripts

Indifferentiability of f_k: Proof Idea

Patarin's H-coefficient Technique

- Each conversation defines a transcript
- Define good and bad transcripts

$$\mathsf{Adv}^{\mathrm{diff}}_{f_k,\mathcal{S}}(\mathcal{D}) \leq \varepsilon + \mathbf{P}\left(\text{bad transcript for } (f_k, p)\right)$$

↰ prob. ratio for good transcripts

- Trade-off: define bad transcripts smartly!

Indifferentiability of f_k: Proof Idea

$$\boxed{N(z) = \{(j, j') \in \{1, \ldots, q\}^2 \mid y_j^1 \oplus y_{j'}^2 = z\}}$$

Indifferentiability of f_k: Proof Idea

$$\boxed{N(z) = \{(j, j') \in \{1, \ldots, q\}^2 \mid y_j^1 \oplus y_{j'}^2 = z\}}$$

Analysis of [MandalPN10]

- Transcript is bad if $|N(z)| \geq \frac{24q^2}{2^n - q}$ for some z

Indifferentiability of f_k: Proof Idea

$$\boxed{N(z) = \{(j, j') \in \{1, \ldots, q\}^2 \mid y^1_j \oplus y^2_{j'} = z\}}$$

Analysis of [MandalPN10]

- Transcript is bad if $|N(z)| \geq \frac{24q^2}{2^n - q}$ for some z
- $\varepsilon \leq 96q^3/2^{2n}$
- $\mathbf{P}\,(\text{bad}) \leq 1/2^{11n}$

Indifferentiability of f_k: Proof Idea

$$\boxed{N(z) = \{(j, j') \in \{1, \ldots, q\}^2 \mid y_j^1 \oplus y_{j'}^2 = z\}}$$

Analysis of [MandalPN10]

- Transcript is bad if $|N(z)| \geq \frac{24q^2}{2^n - q}$ for some z
- $\varepsilon \leq 96q^3/2^{2n}$
- $\mathbf{P}\,(\text{bad}) \leq 1/2^{11n}$

But...

Indifferentiability of f_k: Proof Idea

$$\boxed{N(z) = \{(j, j') \in \{1, \ldots, q\}^2 \mid y_j^1 \oplus y_{j'}^2 = z\}}$$

Analysis of [MandalPN10]

- Transcript is bad if $|N(z)| \geq \frac{24q^2}{2^n - q}$ for some z
- $\varepsilon \leq 96q^3/2^{2n}$
- $\mathbf{P}\,(\text{bad}) \leq 1/2^{11n}$

But...

- Attacker can assure $|N(z)| \geq q/2$ trivially
  $\longrightarrow \mathbf{P}\,(\text{bad}) = 1$

Indifferentiability of f_k: Proof Idea

$$\boxed{N(z) = \{(j, j') \in \{1, \ldots, q\}^2 \mid y_j^1 \oplus y_{j'}^2 = z\}}$$

New Analysis

- Transcript is bad if $\sum_{i=1}^{q} |N(y_i^1 \oplus y_i^2)| > C$

Indifferentiability of f_k: Proof Idea

$$\boxed{N(z) = \{(j, j') \in \{1, \ldots, q\}^2 \mid y_j^1 \oplus y_{j'}^2 = z\}}$$

New Analysis

- Transcript is bad if $\sum_{i=1}^{q} |N(y_i^1 \oplus y_i^2)| > C$
- $\varepsilon \leq C/2^n + q^3/2^{2n}$

Indifferentiability of f_k: Proof Idea

$$\boxed{N(z) = \{(j, j') \in \{1, \ldots, q\}^2 \mid y_j^1 \oplus y_{j'}^2 = z\}}$$

New Analysis

- Transcript is bad if $\sum_{i=1}^{q} |N(y_i^1 \oplus y_i^2)| > C$
- $\varepsilon \leq C/2^n + q^3/2^{2n}$
- $\mathbf{P}$ (bad) reduces to sum-capture problem

Indifferentiability of f_k: Proof Idea

$$\boxed{N(z) = \{(j, j') \in \{1, \ldots, q\}^2 \mid y_j^1 \oplus y_{j'}^2 = z\}}$$

New Analysis

- Transcript is bad if $\sum_{i=1}^{q} |N(y_i^1 \oplus y_i^2)| > C$
- $\varepsilon \leq C/2^n + q^3/2^{2n}$
- $\mathbf{P}$ (bad) reduces to sum-capture problem
  - Given random set Z of size q, find U, V of size q that maximize the number of solutions to $u \oplus v = z$
  - Earlier applications: hashing, signatures, Even-Mansour

Indifferentiability of f_k: Proof Idea

$$\boxed{N(z) = \{(j, j') \in \{1, \ldots, q\}^2 \mid y_j^1 \oplus y_{j'}^2 = z\}}$$

New Analysis

- Transcript is bad if $\sum_{i=1}^{q} |N(y_i^1 \oplus y_i^2)| > C$
- $\varepsilon \leq C/2^n + q^3/2^{2n}$
- $\mathbf{P}$ (bad) reduces to sum-capture problem
  - Given random set Z of size q, find U, V of size q that maximize the number of solutions to $u \oplus v = z$
  - Earlier applications: hashing, signatures, Even-Mansour
  - Using [ChenLL+14]:

$$\mathbf{P}\left(\sum_{i=1}^{q} |N(y_i^1 \oplus y_i^2)| > 3q^3/2^n + 3n^{1/2}q^{3/2}\right) \leq 2/2^n$$

Indifferentiability of f_k: Proof Idea

$$\boxed{N(z) = \{(j, j') \in \{1, \ldots, q\}^2 \mid y_j^1 \oplus y_{j'}^2 = z\}}$$

New Analysis

- Transcript is bad if $\sum_{i=1}^{q} |N(y_i^1 \oplus y_i^2)| > C$
- $\varepsilon \leq C/2^n + q^3/2^{2n}$
- $\mathbf{P}$ (bad) reduces to sum-capture problem
  - Given random set Z of size q, find U, V of size q that maximize the number of solutions to $u \oplus v = z$
  - Earlier applications: hashing, signatures, Even-Mansour
  - Using [ChenLL+14]:

$$\mathbf{P}\left(\sum_{i=1}^{q} |N(y_i^1 \oplus y_i^2)| > \underbrace{3q^3/2^n + 3n^{1/2}q^{3/2}}_{C}\right) \leq 2/2^n$$

Conclusions

indistinguishability (p_i secret)	k	bound	reference
	≥ 1	$2^{\frac{k}{k+1}n}$	[Lucks00]
	2	$2^n/n^{2/3}$	[Bellare99]
	2	2^n	[Patarin08]
	≥ 3	$2^{\frac{2k+1}{2k+2}n}$	[CogliatiLP14]
	≥ 3	2^n	

indifferentiability (p_i public)	k	bound	reference
	2	$2^{n/2}$	[MandalPN10]
	$\cancel{2}$	$\cancel{2^{2n/3}}$	~~[MandalPN10]~~
	≥ 2	$2^{2n/3}$	

Conclusions

XOR of Secret Permutations

- Optimal 2^n security
- Closes the case

XOR of Public Permutations

- Bug in earlier analysis
- New security analysis up to $2^{2n/3}$

Conclusions

XOR of Secret Permutations

- Optimal 2^n security
- Closes the case

XOR of Public Permutations

- Bug in earlier analysis
- New security analysis up to $2^{2n/3}$
- Conjecture: 2^n indifferentiability for $k \geq 2$
  - Bottleneck: bad transcripts
  - Description of simulator thwarted to $k = 2$

Conclusions

XOR of Secret Permutations

- Optimal 2^n security
- Closes the case

XOR of Public Permutations

- Bug in earlier analysis
- New security analysis up to $2^{2n/3}$
- Conjecture: 2^n indifferentiability for $k \geq 2$
  - Bottleneck: bad transcripts
  - Description of simulator thwarted to $k = 2$

Thank you for your attention!

SUPPORTING SLIDES

Indifferentiability of f_k: Simulator

Forward Query $\mathcal{S}(x)$

1. Generate random $y^3, \ldots, y^k$ permutation-wise
2. Query $\mathcal{R}(x)$
3. Generate random y^1, y^2 permutation-wise such that

$$y^1 \oplus y^2 = \mathcal{R}(x) \oplus y^3 \oplus \cdots \oplus y^k$$

Indifferentiability of f_k: Simulator

Forward Query $\mathcal{S}(x)$

1. Generate random $y^3, \ldots, y^k$ permutation-wise
2. Query $\mathcal{R}(x)$
3. Generate random y^1, y^2 permutation-wise such that

$$y^1 \oplus y^2 = \mathcal{R}(x) \oplus y^3 \oplus \cdots \oplus y^k$$

Inverse Query $\mathcal{S}_\ell^{-1}(y^\ell)$ (now: $\ell = 1$)

1. Generate random $y^2, \ldots, y^{k-1}$ permutation-wise
2. Generate random x permutation-wise and query $\mathcal{R}(x)$
3. Set $y^k = \mathcal{R}(x) \oplus y^1 \oplus \cdots \oplus y^{k-1}$

Indifferentiability of f_k: Simulator

Forward Query $\mathcal{S}(x)$

1. Generate random $y^3, \ldots, y^k$ permutation-wise
2. Query $\mathcal{R}(x)$
3. Generate random y^1, y^2 permutation-wise such that

$$y^1 \oplus y^2 = \mathcal{R}(x) \oplus y^3 \oplus \cdots \oplus y^k$$

Inverse Query $\mathcal{S}_\ell^{-1}(y^\ell)$ (now: $\ell = 1$)

1. Generate random $y^2, \ldots, y^{k-1}$ permutation-wise
2. Generate random x permutation-wise and query $\mathcal{R}(x)$
3. Set $y^k = \mathcal{R}(x) \oplus y^1 \oplus \cdots \oplus y^{k-1}$
4. If y^k collides with old value: return to 2.