# Indifferentiability of the Sum of Random Permutations Towards Optimal Security

Jooyoung Lee

School of Computing (GSIS), KAIST

# Motivation

- A Feistel cipher securely transforms a set of random functions into a random permutation.
- How can we transform a set of random permutations into a random function? (Called “Luby-Rackoff Backwards".)
- The counter mode of operation turns a block cipher into a stream cipher: using a nonce $N$ and counters, a key stream

$$E_k(N||0)||E_k(N||1)||E_k(N||2)\cdots$$

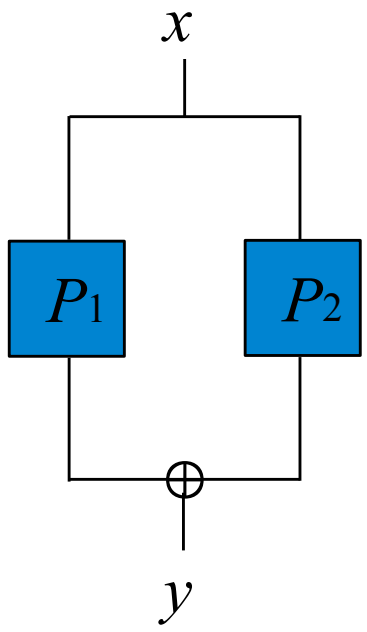
  is generated and then xored to the message.
  - The keyed permutation $E_k$ can be assume to be a truly random permutation.
  - With $q \approx 2^{\frac{n}{2}}$ blocks, a key stream from the CTR mode can be distinguished from a truly random key stream, where $n$ is the block size.

# Xor of Multiple Random Permutations

- A random permutation $P$ can be viewed as a random function up to the birthday bound. (PRP/PRF Switching Lemma)
- Can we do better than PRP/PRF switching? We might consider the construction

$$F_l(x) = P_1(x) \oplus \cdots \oplus P_l(x)$$

where $P_i$'s are independent random permutations.



# Indistinguishability vs. Indifferentiability

## Indistinguishability

- In a black box, there is either $F_l$ or a truly random function $\mathcal{R}$ with the same probability.
- An adversary is allowed to make oracle queries to a black box, and tries to find out what is inside the black box.

## Indifferentiability

- An adversary is allowed to have oracle access to each of $P_1, \ldots, P_l$.
- To prove that $F_l$ is indifferentiable from a public random function $\mathcal{R}$, one should present a simulator $\mathcal{S}$ that emulates $P = (P_1, \ldots, P_l)$ having access to $\mathcal{R}$ so that it is infeasible to distinguish two systems $(\mathcal{R}, \mathcal{S}[\mathcal{R}])$ and $(F_l[P], P)$.
- In an information-theoretic sense, $F_l$ is $(q, \epsilon)$-indifferentiable from the ideal primitive $\mathcal{R}$ if there exists a simulator $\mathcal{S}$ with oracle access to $\mathcal{R}$ such that for any distinguisher $\mathcal{D}$ making at most $q$ queries, it holds that

$$\mathsf{Adv}_{F_l,\mathcal{S}}(\mathcal{D}) \stackrel{\text{def}}{=} \left| \Pr\left[\mathcal{D}^{F_l[P],P} = 1\right] - \Pr\left[\mathcal{D}^{\mathcal{R},\mathcal{S}[\mathcal{R}]} = 1\right] \right| < \epsilon.$$

# History and Our Result

## Indistinguishability

| Thres. num. queries | Technique | Reference |
|---|---|---|
| $2^{\frac{ln}{l+1}}$ | | Lucks |
| $2^{\frac{(2l+1)n}{2l+2}}$ | Coefficient-$H$ | Cogliati et. al. |
| $2^{\frac{(l+1)n}{l+2}}$ | Coefficient-$H_\sigma$ | |

Even $F_2$ has been proved to be secure up to $O(2^n)$ queries (Patarin), but the exact coefficients are not clear.

## Indifferentiability

| Range for $l$ | Thres. num. queries | Reference |
|---|---|---|
| 2 | $2^{\frac{2n}{3}}$ | Mandal et. al. |
| $\geq 2$ | $2^{\frac{2n}{3}}$ | Mennink et. al |
| $\geq 4$ | $2^{\left(2\lfloor\frac{l}{2}\rfloor-1\right)n/2\lfloor\frac{l}{2}\rfloor}$ ($= 2^{\frac{(l-1)n}{l}}$ if $l$ is even) | This work |

# Our Result

## Theorem

*For an even integer $l \geq 4$, there exists a simulator $\mathcal{S}$ such that for any distinguisher $\mathcal{D}$ making $q$ oracle queries,*

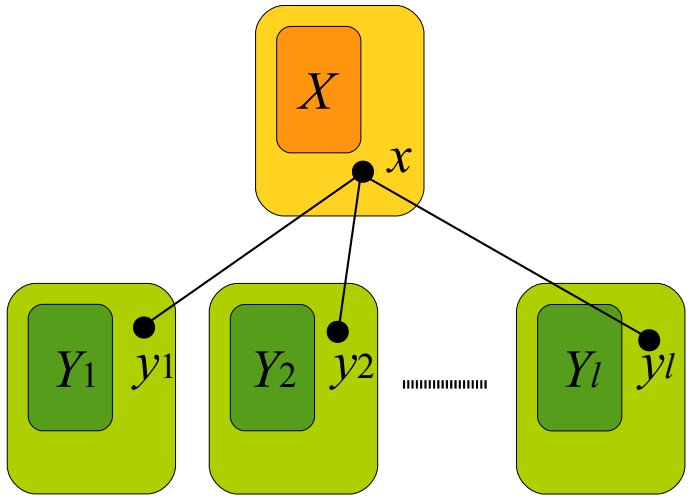
$$\mathsf{Adv}_{F_l,\mathcal{S}}(\mathcal{D}) \leq \frac{(2q)^l}{2^{(l-1)n}}.$$

*The simulator makes at most $q$ queries to $\mathcal{R}$.*

## Remark

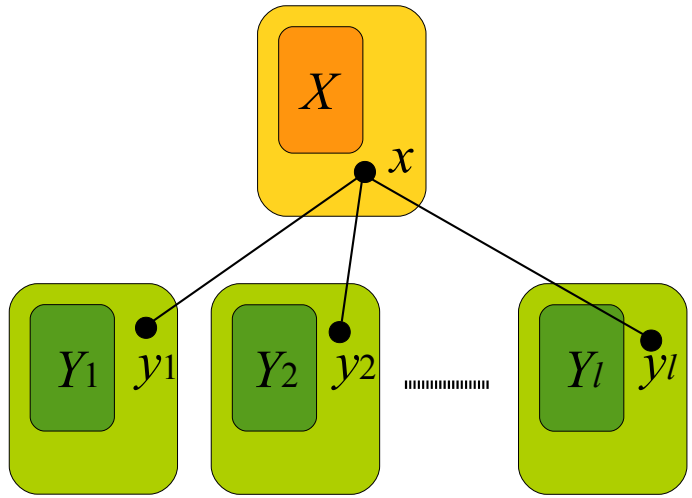
*If $m > l$, then $F_m$ is at least as secure as $F_l$.*

# Description of the Simulator




- Simulator $\mathcal{S}$ keeps the domain $X$ and the ranges $Y_1, \ldots, Y_l$ of evaluations of $P_i$ that already have been determined.
- When a forward query $P_j(x)$ is made for some $j = 1, \ldots, l$, $\mathcal{S}$ do:
  1. Obtain $z = \mathcal{R}(x)$ via an oracle query to $\mathcal{R}$.
  2. Choose an $l$-tuple $\mathbf{y} = (y_1, y_2, \ldots, y_l)$ uniformly at random from the set
$$\Pi^z \stackrel{\text{def}}{=} \left\{ (y_1, \ldots, y_l) \in \prod_{j=1}^{l} \overline{Y_j} : \bigoplus_{j=1}^{l} y_j = z \right\}.$$
  3. Assign $y_1, \ldots, y_l$ to $P_1(x), \ldots, P_l(x)$, respectively.
  4. Update: $X \leftarrow X \cup \{x\}$ and $Y_j \leftarrow Y_j \cup \{y_j\}$ for $j = 1, \ldots, l$.
  5. Answer the query as assigned to the corresponding variable.

# Description of the Simulator

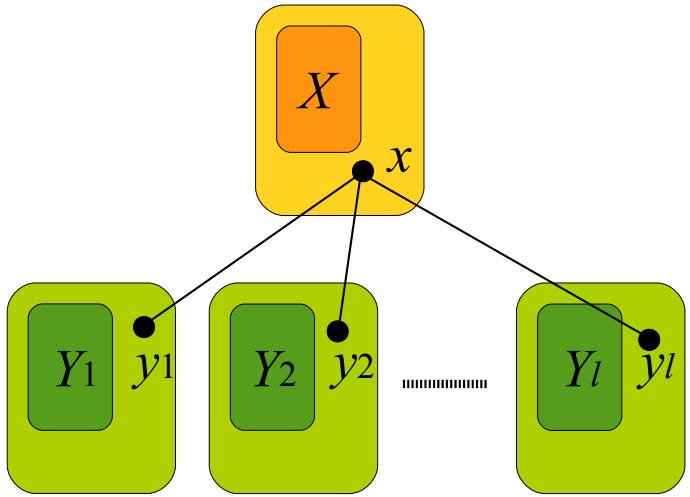



- When a backward query $P_{j^*}^{-1}(y_{j^*})$ is made for some $j^* = 1, \ldots, l$, $\mathcal{S}$ do:
  1. Choose $x$ uniformly at random from $\{0,1\}^n \setminus X$.
  2. Obtain $z = \mathcal{R}(x)$ via an oracle query to $\mathcal{R}$.
  3. Choose an $(l-1)$-tuple $\hat{\mathbf{y}} = (y_1, \ldots, y_{j^*-1}, y_{j^*+1}, \ldots, y_l)$ uniformly at random from the set

$$\Pi_{j^*}^{z \oplus y_{j^*}} \stackrel{\text{def}}{=} \left\{ \hat{\mathbf{y}} \in \prod_{\substack{1 \le j \le l \\ j \ne j^*}} \overline{Y_j} : \bigoplus_{\substack{1 \le j \le l \\ j \ne j^*}} y_j = z \oplus y \right\}.$$

  4. Assign $y_1, \ldots, y_l$ to $P_1(x), \ldots, P_l(x)$, respectively.
  5. Update: $X \leftarrow X \cup \{x\}$ and $Y_j \leftarrow Y_j \cup \{y_j\}$ for $j = 1, \ldots, l$.
  6. Answer the query with $x$.

# Giving Free Queries to the Distinguisher

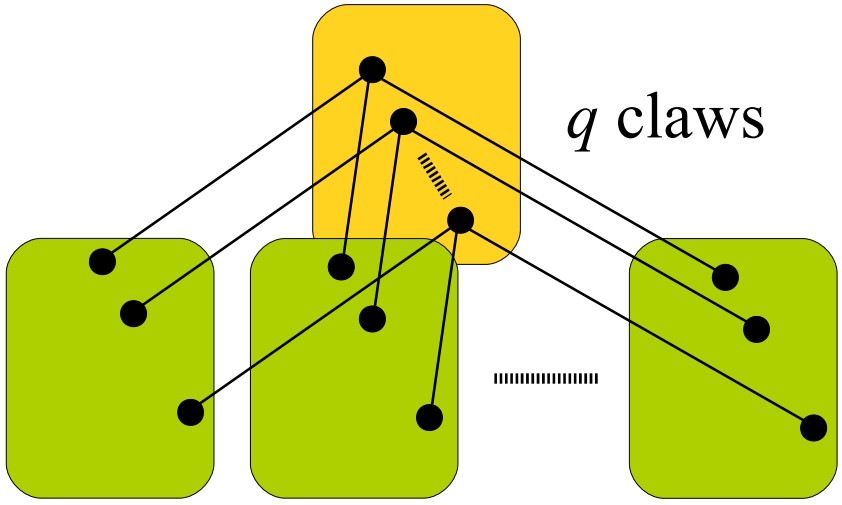



- At the end of the interaction, distinguisher $\mathcal{D}$ will be given additional queries (primitive evaluations) for free:
  - If a forward query $F_l(x)$ or $P_j(x)$ has been made for some $j$, then $\mathcal{D}$ will be given $P_{j'}(x)$ for all unqueried indices $j'$ if any.
  - If a backward query $P_j^{-1}(y)$ has been made and answered with $x$ for some $j$, then $\mathcal{D}$ will be given $P_{j'}(x)$ for all unqueried indices $j'$ if any.
- In this way, by making a single query, $\mathcal{D}$ is able to obtain a tuple

$$(x, y_1, \ldots, y_l)$$

such that $P_j(x) = y_j$ for $j = 1, \ldots, l$.

# H-coefficient Technique




If $\mathcal{D}$ makes total $q$ oracle queries, then we can assume that $\mathcal{D}$ obtains a transcript of the following form.

$$\tau = ((x_1, y_{11}, \ldots, y_{l1}), \ldots, (x_q, y_{1q}, \ldots, y_{lq})) .$$

## Lemma

*Fix a distinguisher $\mathcal{D}$. If there exists $\varepsilon$ such that*

$$\frac{\Pr[T_{\mathrm{si}} = \tau]}{\Pr[T_{\mathrm{re}} = \tau]} \geq 1 - \varepsilon.$$

*for any attainable transcript $\tau \in \mathcal{T}$, then one has*

$$\mathrm{Adv}_{F_l, \mathcal{S}}(\mathcal{D}) \leq \varepsilon.$$

# Security Proof

- For any transcript

$$\tau = ((x_1, y_{11}, \ldots, y_{l1}), \ldots, (x_q, y_{1q}, \ldots, y_{lq}))$$

  it is easy to show

$$\Pr[T_{\mathrm{re}} = \tau] = \frac{1}{(N)_q^l} = \prod_{i=0}^{q-1} \frac{1}{(N-i)^l}.$$

- In order to estimate $\Pr[T_{\mathrm{si}} = \tau]$, one has to upper bound the size of

$$\Pi^z = \left\{ (y_1, \ldots, y_l) \in \prod_{j=1}^{l} \overline{Y_j} : \bigoplus_{j=1}^{l} y_j = z \right\}$$

  at each sampling of the responses.

# Security Proof

- Let

$$A_j = \left\{ (y_1, \ldots, y_l) \in \left(\{0,1\}^n\right)^l : \bigoplus_{j=1}^{l} y_j = z \bigwedge y_j \in Y_j \right\}$$

  for $j = 1, \ldots, l$.

- Then one has

$$\begin{aligned} \Pi^z &= \left\{ (y_1, \ldots, y_l) \in \prod_{j=1}^{l} \overline{Y_j} : \bigoplus_{j=1}^{l} y_j = z \right\} \\ &= \left\{ (y_1, \ldots, y_l) \in \left(\{0,1\}^n\right)^l : \bigoplus_{j=1}^{l} y_j = z \right\} \setminus \bigcup_{j=1}^{l} A_j. \end{aligned}$$

- By the inclusion-exclusion principle, one has

$$\left| \bigcup_{i=1}^{l} A_i \right| = \sum_{k=1}^{l} (-1)^{k+1} \left( \sum_{1 \le j_1 < \cdots < j_k \le l} |A_{j_1} \cap \cdots \cap A_{j_k}| \right).$$

# Security Proof

- For $k < l$ and for any set of $k$ indices

$$1 \leq j_1 < j_2 < \cdots < j_k \leq l,$$

one has

$$|A_{j_1} \cap A_{j_2} \cap \cdots \cap A_{j_k}| = i^k N^{l-k-1},$$

while

$$|A_1 \cap A_2 \cap \cdots \cap A_l| \leq i^{l-1}.$$

- With this estimation, one has

$$\left|\Pi^z\right| \leq \frac{(N-i)^l}{N} + \left(i^{l-1} - \frac{i^l}{N}\right)$$

when $\mathcal{A}$ makes the $i$-th query.

- This upper bound leads to

$$\frac{\Pr[T_{\mathrm{si}} = \tau]}{\Pr[T_{\mathrm{re}} = \tau]} \geq 1 - \frac{(2q)^l}{N^{l-1}}.$$

# Conclusion

- The indifferentiability of the sum of public random permutations has been proved only up to

$$2^{\frac{(l-1)n}{l}}$$

  queries for an even integer $l \geq 4$.

- This is the first result that shows the indifferentiablity of the sum of random permutations is strengthened towards the optimal bound $2^n$ as the number of summands increases.