Sequential Indifferentiability of STH and EDM

Hrithik Nandi

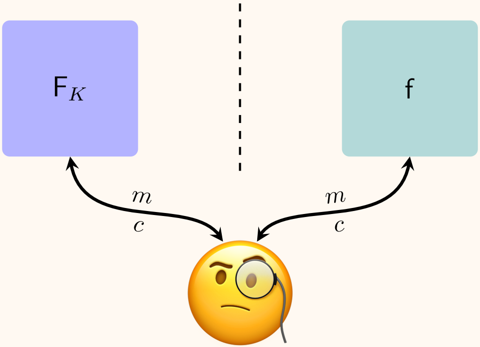
Institute for Advancing Intelligence, TCG CREST
&
Ramakrishna Mission Vivekananda Educational and Research Institute

Crypto Winter School 2025, IIT Bhilai

December 11, 2025

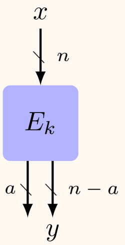
PRF Security: Indistinguishability

- $\mathsf{F}\colon \mathcal{M} \times \mathcal{K} \to \mathcal{C}$, where $\mathcal{M} := \{0,1\}^m, \mathcal{K} := \{0,1\}^k$ and $\mathcal{C} := \{0,1\}^n$
- $\mathsf{f} \xleftarrow{\$} \mathrm{Func}[\mathcal{M}, \mathcal{C}]$, where $\mathrm{Func}[\mathcal{M}, \mathcal{C}]$ is the set of all functions from $\mathcal{M}$ to $\mathcal{C}$

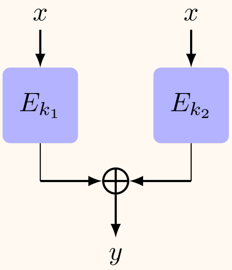


$$\boxed{\mathsf{Adv}^{\mathrm{PRF}}_{\mathcal{A},\mathsf{F}}(q) := \left|\Pr[K \xleftarrow{\$} \mathcal{K}\colon \mathcal{A}^{\mathsf{F}_K(\cdot)} \to 1] - \Pr[\mathsf{f} \xleftarrow{\$} \mathrm{Func}(n)\colon \mathcal{A}^{\mathsf{f}(\cdot)} \to 1]\right|}$$

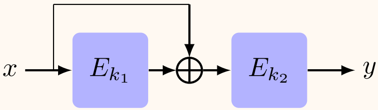
PRP based PRF



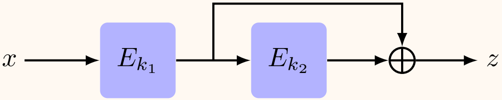
Truncation



Xor of Permutations

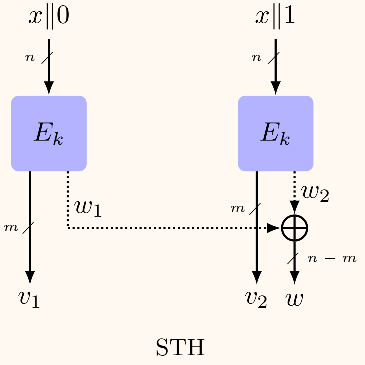


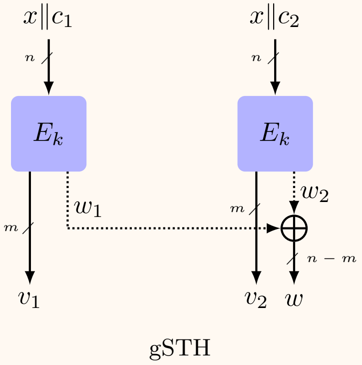
EDM



EDMD

PRP BASED PRF



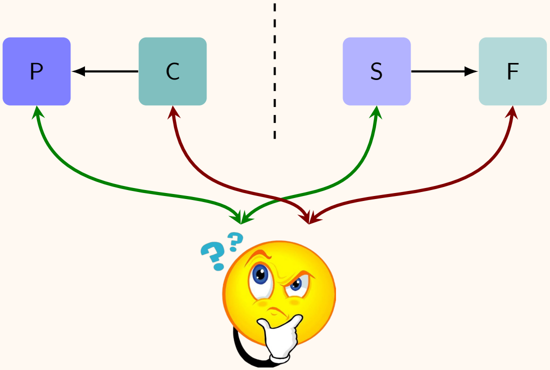


- In this work we have proposed gSTH construction, which takes an $(n-l)$-bit input and produces $(n+m)$-bit outputs and $c_1 \neq c_2 \in \{0,1\}^l$ are two constants.

Moving from Secret to Public Permutation

- In PRF security (indistinguishability) setting underlying primitives remain secret.
- Motivation behind making the permutations public:
    - Sometimes block ciphers are instantiated with fixed keys,
    - Many unkeyed permutations are designed as an underlying primitive of encryption, MAC, hash functions.
- Now the question is to what degree the constructions behave like random function when they are instantiated with public permutations.
- Moves to indifferentiability setting.

Indifferentiable Security Notion



$$\boxed{\mathrm{Adv}^{\mathrm{indiff}}_{\mathsf{C}^{\mathsf{P}},\mathsf{F}^{\mathsf{S}}}(\mathcal{A}) := \left|\Pr[\mathcal{A}^{\mathsf{C},\mathsf{P}} \to 1] - \Pr[\mathcal{A}^{\mathsf{F},\mathsf{S}} \to 1]\right|}$$

$\exists$ S s.t. $\mathrm{Adv}^{\mathrm{indiff}}_{\mathsf{C}^{\mathsf{P}},\mathsf{F}^{\mathsf{S}}}(\mathcal{A})$ is negligible $\forall$ adversary $\mathcal{A}$

$\Longrightarrow$

C is indifferentiable from F

Indifferentiable Security Notion

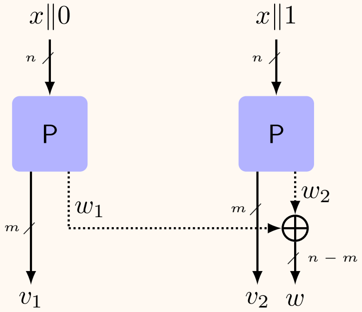
Sequential Indifferentiability

A construction C with oracle access to an ideal primitive P is said to be sequentially (q, σ, ϵ)-indifferentiable from an ideal primitive F if there exists a simulator $\mathcal{S}$ with oracle access to F such that for any distinguisher $\mathcal{D}$ making exactly q queries to the primitive and the simulator makes a total of σ queries to the ideal primitive F such that the distinguisher is restricted in first making its primitive queries and then making its construction queries, it holds that

$$\mathbf{Adv}_{\mathsf{C},\mathcal{S}}^{\text{seq-indiff}}(\mathcal{D}) = \left| \Pr\left[\mathcal{D}^{\mathsf{C}^{\mathsf{P}},\mathsf{P}} \to 1\right] - \Pr\left[\mathcal{D}^{\mathsf{F},\mathcal{S}^{\mathsf{F}}} \to 1\right] \right| < \epsilon.$$

- Sequential Indifferentiability is a weaker notion of Indifferentiability,
- In this model, the distinguisher must make all its queries to the ideal primitive P (or the simulator $\mathcal{S}$) before querying the construction C^{P} (or the ideal primitive F).

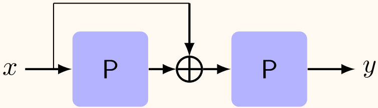
Indifferentiable Attack on STH



1. Make inverse primitive query with 0^n;
2. Let u be the response;
3. Make construction query with $\mathrm{left}_{n-1}(u)$;
4. Let $v_1\|v_2\|w$ be the response;
5. If $(\mathrm{right}_1(u) = 0 \wedge v_1 = 0^m) \vee (\mathrm{right}_1(u) = 1 \wedge v_2 = 0^m)$
   Return 1;
6. Else
   Return 0;

$$\begin{aligned}\mathrm{Adv}^{\text{seq-indiff}}_{\mathrm{STH},\mathsf{S}}(\mathcal{A}) &:= \left|\Pr[\mathcal{A}^{\mathrm{STH},\mathsf{P}} \to 1] - \Pr[\mathcal{A}^{\mathsf{RF},\mathsf{S}} \to 1]\right| \\ &\geq \left|1 - \frac{2p(n)}{2^m}\right|\end{aligned}$$

Indifferentiable Attack on P-EDM



1. Make inverse primitive query with 0^n;
2. Let x be the response;
3. Make construction query with x;
4. Let z be the response;
5. If $z = 0^n$

   Return 1;
6. Else

   Return 0;

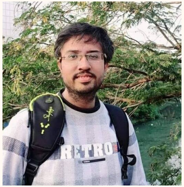
$$\begin{aligned}\mathrm{Adv}^{\text{seq-indiff}}_{\text{P-EDM},\mathsf{S}}(\mathcal{A}) &:= \left|\Pr[\mathcal{A}^{\text{P-EDM},\mathsf{P}} \rightarrow 1] - \Pr[\mathcal{A}^{\mathsf{RF},\mathsf{S}} \rightarrow 1]\right| \\ &\geq \left|1 - \frac{2p(n)}{2^m}\right|\end{aligned}$$

Our Contribution

Construction	Sequential	Regular	Reference
TRP	$\min\{2^{(n+m)/3}, 2^m, 2^l\}$	$\min\{2^{(n+m)/3}, 2^m, 2^l\}$	Choi et. al'19
SUMPIP	$2^{n/2}$	?	Dodis et. al'08
SoP	$2^{2n/3-\log n}$	$2^{2n/3-\log n}$	Gunsing et. al'23
STH	$\times$	$\times$	Our work
STH2	$\times$	$\times$	Our work
gSTH	2^l ($\dagger$)	?	Our work
EDM	$2^{n/2}$	?	Our work
P-EDM	$\times$	$\times$	Our work

Table: Sequential and Regular Indifferentiability Results of PRP-based PRFs. The symbols "?" and "$\times$" mean Not known and insecure, respectively. We use the symbol ($\dagger$) to denote that the bound is tight.

For More Details




https://eprint.iacr.org/2025/1518

Thank You!

Questions?