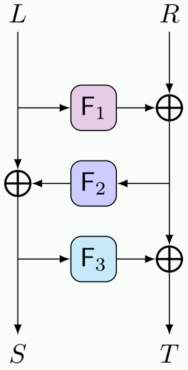
Naor Reingold goes Beyond the Birthday-Bound

Nilanjan Datta

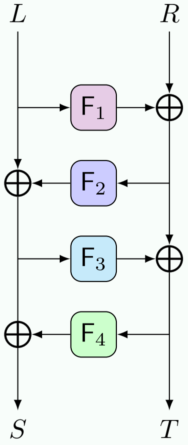
tcg crest
Inventing Harmonious Future

Feistel Construction [Luby and Rackoff, SIAM'86]

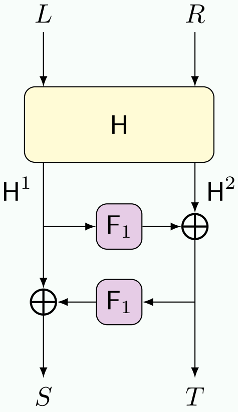


1. F_1, F_2, F_3: Independent Random Function.
2. 3-round LR is PRP Secure up to $2^{n/2}$ queries.
3. 3-round LR Construction is SPRP insecure.

Security of 4 Round Feistel [Patarin, Eurocode'90]

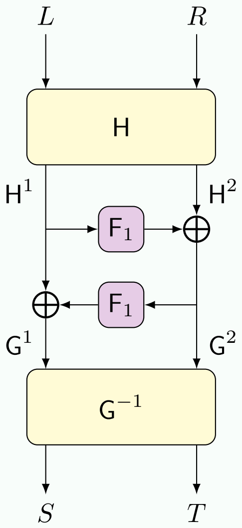


1. F_1, F_2, F_3, F_4: Independent Random Function.
2. 4-round LR is SPRP Secure up to $2^{n/2}$ queries.



1. F_1: Random Function.
2. Achieves PRP Security up to $2^{n/2}$ queries if
   - H^1 is universal
   - H is invertible

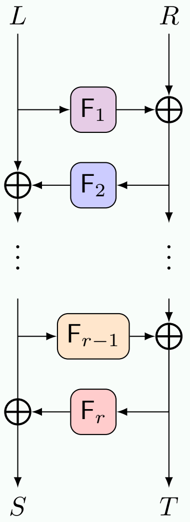
Naor Reingold Construction [Naor and Reingold, JOC'99]



1. F_1: Random Function.
2. Achieves SPRP Security up to $2^{n/2}$ queries if
   - H^1 is universal
   - G^2 is universal
   - Both H and G are invertible

Feistel Constructions: Obtaining BBB Security

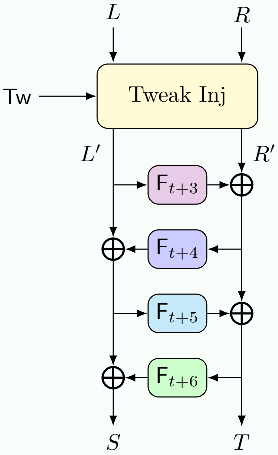
tcg crest
Inventing Harmonious Future



Improving the Security of LR:

# Round	Security	Bound	Ref
6	SPRP	$3n/4$	[Pat, FSE'98]
r $(r \geq 7)$	PRP	$n(r-1)/r$	[MP, EC'03]
r $(r \geq 10)$	SPRP	$n(r-1)/r$	[MP, EC'03]
5	PRP	n	[Pat, CRYPTO'04]
6	SPRP	n	[Pat, CRYPTO'04]

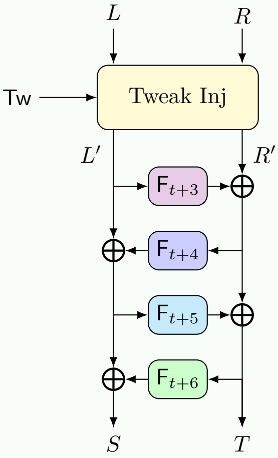
Tweakable LR Constructions [Goldenberg et al., AC'07]

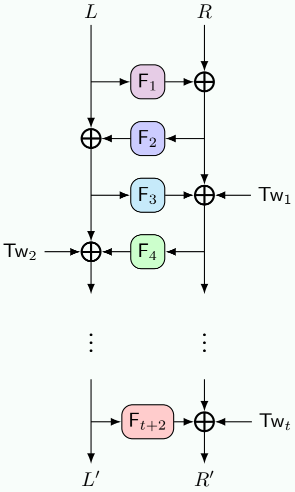


Optimal Security:

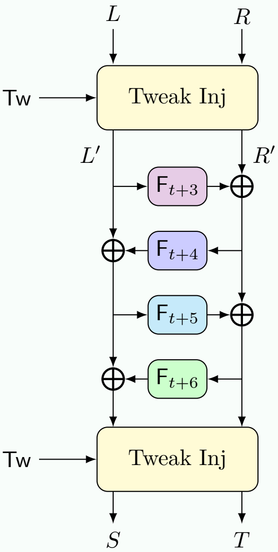
Tweak Size	# RF Call	Security
n	7	TPRP
tn	t+6	TPRP

Tweak Injection used in [Goldenberg et al., AC'07]





Tweakable LR Constructions [Goldenberg et al., AC'07]



Optimal Security:

Tweak Size	# RF Call	Security
n	7	TPRP
tn	t+6	TPRP
n	10	STPRP
tn	2t+8	STPRP

Towards Permutation-based LR Constructions

1. Inner Round functions to be permutations (practical implications).
2. Apply PRP-PRF Switching Lemma: Security only up to Birthday Bound.

Towards Permutation-based LR Constructions

tcg crest
Inventing Harmonious Future

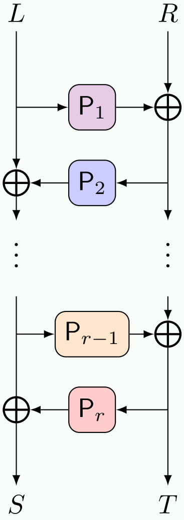
1. Inner Round functions to be permutations (practical implications).

2. Apply PRP-PRF Switching Lemma: Security only up to Birthday Bound.

How many rounds are required to obtain BBB security?

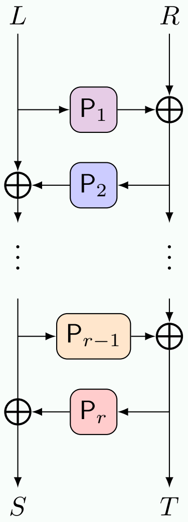
Permutation-based (Tweakable) LR Constructions

Permutation-based LR Constructions [Guo et al., DCC' 21]



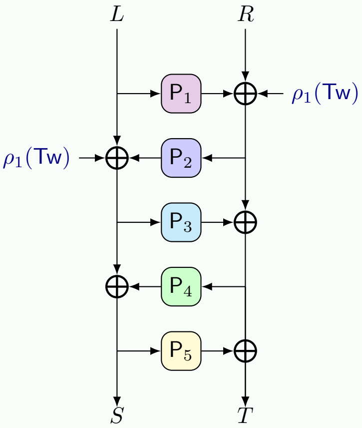
# Round	Security	Bound
3	KPA	$2n/3$
5	CPA	$2n/3$
7	CCA	$2n/3$

Permutation-based LR [Chakraborty et al., CRYPTO' 25]



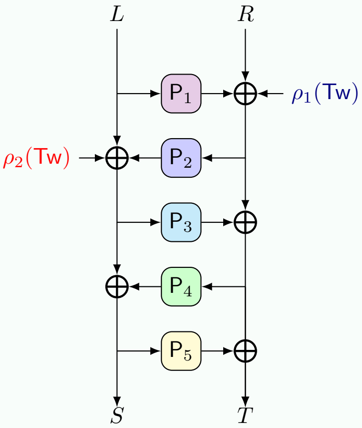
# Round	Security	Bound
5	CPA/PRP	n
7	CCA/SPRP	n

Permutaion-based TLR [Chakraborty et al., CRYPTO' 25]



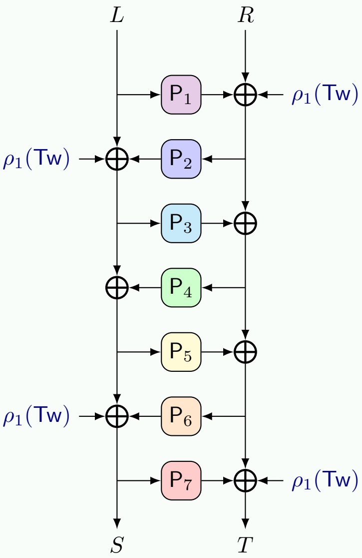
Tweak Size	# RP Call	# AXU Call	Security
n	6	0	TPRP

Permutaion-based TLR [Chakraborty et al., CRYPTO' 25]



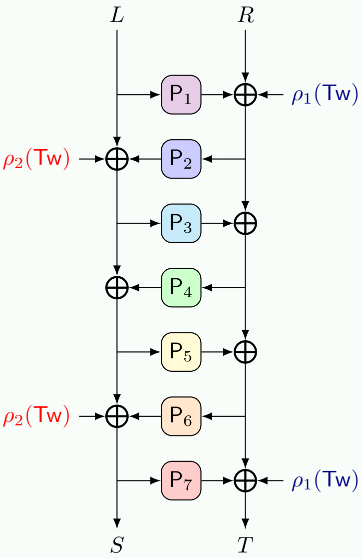
Tweak Size	# RP Call	# AXU Call	Security
n	6	0	TPRP
tn	5	2	TPRP

Permutaion-based TLR [Chakraborty et al., CRYPTO' 25]



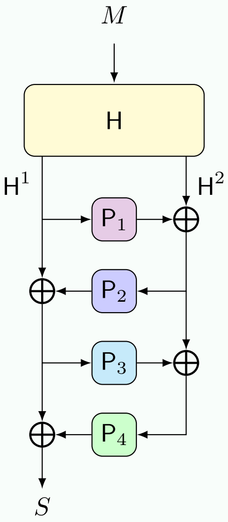
Tweak Size	# RP Call	# AXU Call	Security
n	6	0	TPRP
tn	5	2	TPRP
n	8	0	STPRP

Permutaion-based TLR [Chakraborty et al., CRYPTO' 25]



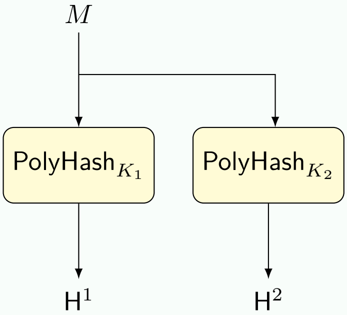
Tweak Size	# RP Call	# AXU Call	Security
n	6	0	TPRP
tn	5	2	TPRP
n	8	0	STPRP
tn	7	2	STPRP

Permutaion-based TLR [Chakraborty et al., ePrint 2025/914]



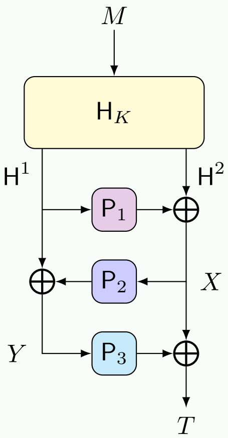
VIL-PRF Construction:

1. PRF Security of $O(q^2\epsilon + \frac{q}{2^n})$ if H is ϵ universal.
2. Instantiation:



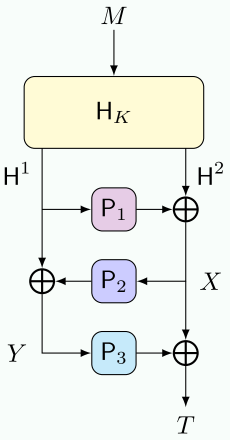
Can you apply Naor-Reingold Technique to reduce the number of (independent) primitive calls?

HF^3: Hash then 3-round Feistel



1. Achieves PRF Security of $O(q^2\epsilon + q\delta)$ queries if
   - H is ϵ universal.
   - H^1 is δ zero-sum universal.

HF^3: Hash then 3-round Feistel



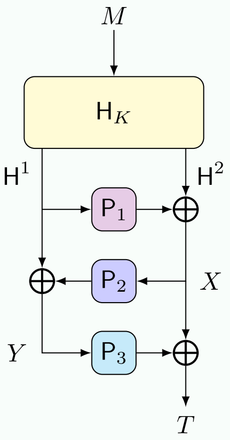
1. Achieves PRF Security of $O(q^2\epsilon + q\delta)$ queries if
   - H is ϵ universal.
   - H^1 is δ zero-sum universal.

Zero-Sum Universal:

H is called an δ zero-sum universal hash function, if $\exists f$ such that for all $\ell \geq 2$ and distinct $M_1, \ldots, M_{\ell-1}$ with $M_\ell \neq f(M_1, \ldots, M_{\ell-1})$,

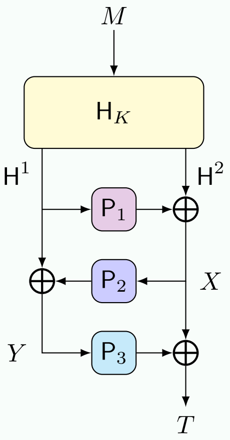
$$\Pr[K \leftarrow_{\$} \mathcal{K}_{\text{hash}} : \mathsf{H}_K(M_1) \oplus \cdots \oplus \mathsf{H}_K(M_\ell) = 0^n] \leq \delta.$$

HF^3: Hash then 3-round Feistel

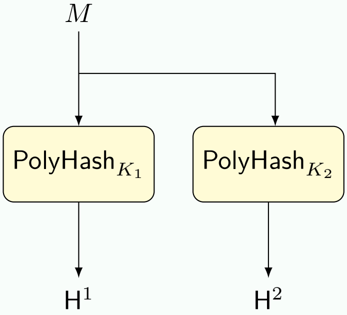


1. Achieves PRF Security of $O(q^2\epsilon + q\delta)$ queries if
   - H is ϵ universal.
   - H^1 is δ zero-sum universal.
2. How costly is this hash function?

HF^3: Hash then 3-round Feistel

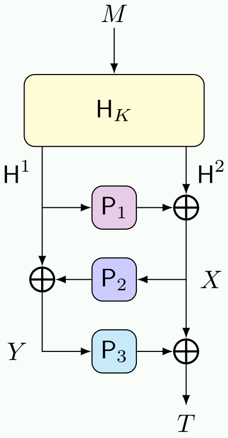


1. Achieves PRF Security of $O(q^2\epsilon + q\delta)$ queries if
   - H is ϵ universal.
   - H^1 is δ zero-sum universal.
2. How costly is this hash function? The same instantiation works..!!



A Brief Proof Overview

Optimal PRF Security of HF^3: Proof Sketch



High Level Proof Idea:

1. Release K and P_1 (real world); sample K and P_1 (ideal world).
2. Extended Transcript:

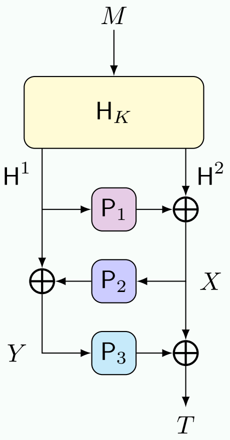
$$\tau = \big((M_1, T_1, \mathsf{H}_1^1, \mathsf{H}_1^2, X_1), \ldots, (M_q, T_q, \mathsf{H}_q^1, \mathsf{H}_q^2, X_q)\big) \,.$$

3. The following must hold:

$$\mathsf{P}_2(X_i) \oplus \mathsf{P}_3^{-1}(X_i \oplus T_i) = \mathsf{H}_i^1, \ \forall i = 1, \ldots, q.$$

4. Define and bound the probability of bad transcripts and apply Mirror Theory to bound the interpolation probability.

Optimal PRF Security of HF^3: Proof Sketch



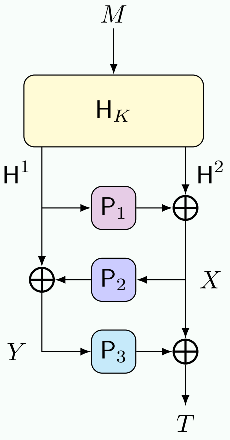
High Level Proof Idea:

1. The following must hold:

$$\mathsf{P}_2(X_i) \oplus \mathsf{P}_3^{-1}(X_i \oplus T_i) = \mathsf{H}_i^1, \ \forall i = 1, \ldots, q.$$

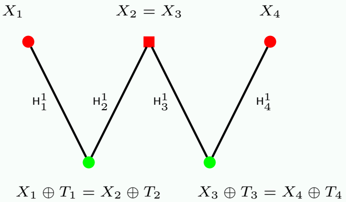
2. Consider the transcript graph:
   - Bi-partite graph with X nodes in one partite and $X \oplus T$ nodes in the other.
   - Edge from X_i to $X_i \oplus T_i$ with level H_i^1.
   - Merge node X_i and X_j if $X_i = X_j$.

Optimal PRF Security of HF^3: Proof Sketch

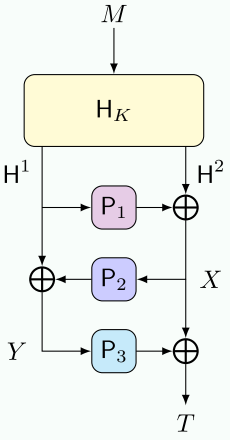


Transcript Graph: An Example

$$
\begin{aligned}
\mathsf{P}_2(X_1) \oplus \mathsf{P}_3^{-1}(X_1 \oplus T_1) &= \mathsf{H}_1^1 \\
\mathsf{P}_2(X_2) \oplus \mathsf{P}_3^{-1}(X_2 \oplus T_2) &= \mathsf{H}_2^1 \\
\mathsf{P}_2(X_3) \oplus \mathsf{P}_3^{-1}(X_3 \oplus T_3) &= \mathsf{H}_3^1 \\
\mathsf{P}_2(X_4) \oplus \mathsf{P}_3^{-1}(X_4 \oplus T_4) &= \mathsf{H}_4^1
\end{aligned}
$$



Optimal PRF Security of HF^3: Proof Sketch



High Level Proof Idea:

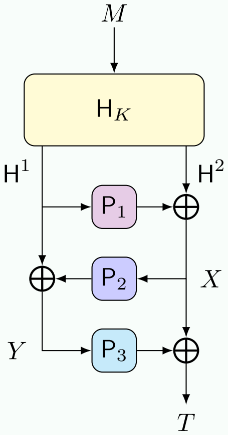
1. The following must hold:

$$\mathsf{P}_2(X_i) \oplus \mathsf{P}_3^{-1}(X_i \oplus T_i) = \mathsf{H}_i^1, \ \forall i = 1, \ldots, q.$$

2. Consider the transcript graph:
   - Bi-partite graph with X nodes in one partite and $X \oplus T$ nodes in the other.
   - Edge from X_i to $X_i \oplus T_i$ with level H_i^1.
   - Merge node X_i and X_j if $X_i = X_j$.

3. Define the bad transcript based on certain properties of the transcript graph so that Mirror Theory can be applied (to lower bound the probability of good transcripts in real world).

Optimal PRF Security of HF^3: Proof Sketch

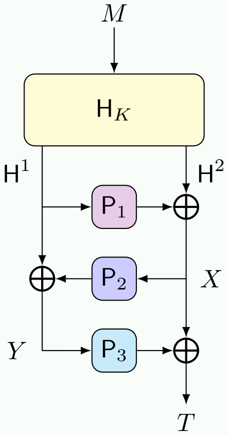


When can you apply Mirror Theory?

If the underlying transcript graph is good, meaning that it does not have

- even-length cycles
- large components (components of size $\geq n$)
- a path with zero label-sum

Optimal PRF Security of HF^3: Proof Sketch



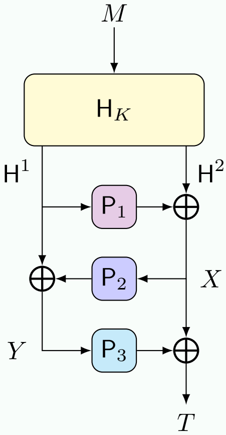
Defining and bounding the Bad Transcript

A transcript is called *bad* if the following occurs

- Universal or Cross-collision Universal
- First Hash Collision
- Zero Hash Sum
- n-multicollision in T values

- We show that the probability of having a bad transcript is bounded by $O(q^2\epsilon + q\delta + nq/2^n)$.

- If bad does not occur then the underlying transcript graph is good with very high probability.



High Interpolation Probability for Good Graphs

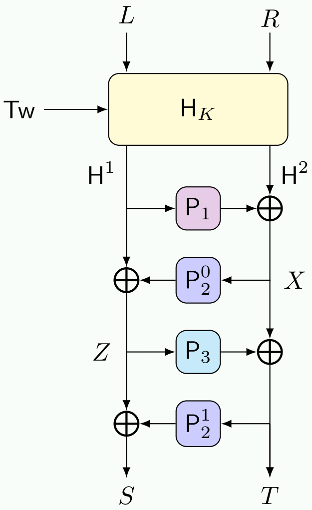
- The Mirror Theory Result: Let $G_{\mathbb{E}} = (V_1 \sqcup V_2, E)$ be the associated edge-labeled bipartite graph for the system of equations $\mathbb{E}$. Let the number of edges in $G_{\mathbb{E}}$ is q and the size of the largest component in $G_{\mathbb{E}}$ is $\xi_{\max}$. If $\xi_{\max}^2 n + \xi_{\max} \leq 2^{n/2}$ and $q\xi_{\max}^2 \leq 2^n/12$, then the number of solutions to $\mathbb{E}$, denoted as $h(\mathbb{E})$ is

$$h(\mathbb{E}) \geq \frac{(2^n - 2)_{|V_1|}(2^n - 2)_{|V_2|}}{2^{nq}}.$$

- We apply this result to show that the interpolation probability is 1.

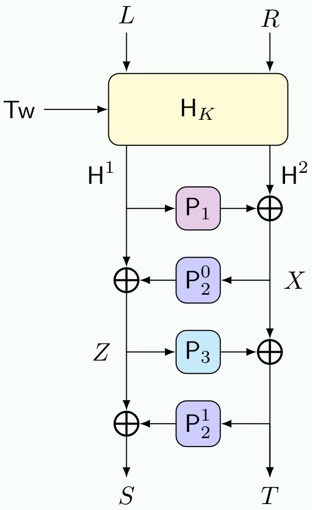
Tweakable LR based TPRP and TSPRP Constructions

HF^4: Hash then 4-round Feistel



1. P_1, P_2, P_3: Independent Random Permutation.
2. $\mathsf{P}_i^b(x) := \mathsf{P}_i(\lfloor x \rfloor \| b)$.
3. Achieves TPRP Security of $O(q^2\epsilon + q\delta + \frac{nq}{2^n})$ if
   - H is ϵ universal.
   - H^1 is δ constant-sum universal.

HF^4: Hash then 4-round Feistel



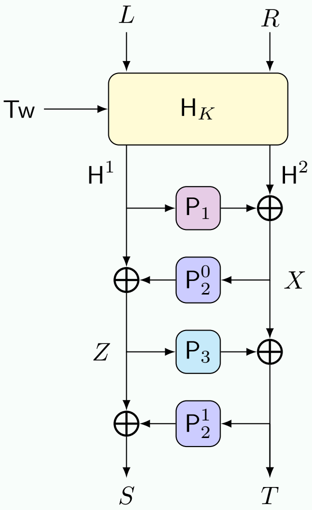
1. Achieves TPRP Security of $O(q^2\epsilon + q\delta + \frac{nq}{2^n})$ if
   - H is ϵ universal.
   - H^1 is δ constant-sum universal.

Constant-Sum Universal:

H is called an δ constant-sum universal hash function, if for any constant c, $\exists f$ such that for all $\ell \geq 2$ and distinct $M_1, \ldots, M_{\ell-1}$ with $M_\ell \neq f(M_1, \ldots, M_{\ell-1})$,

$$\Pr[K \leftarrow_\$ \mathcal{K}_{\text{hash}} : \mathsf{H}_K(M_1) \oplus \cdots \oplus \mathsf{H}_K(M_\ell) = c] \leq \delta.$$

Optimal (T)PRP Security of HF^4: Proof Sketch



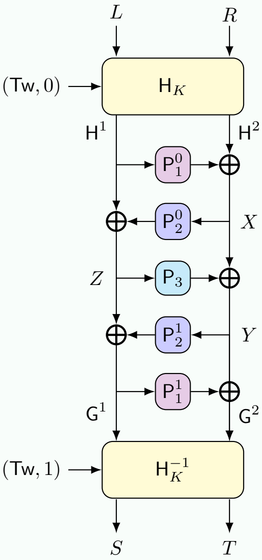
High Level Proof Idea:

1. Release K and P_1 (real world); sample K and P_1 (ideal world).
2. The following must hold:

$$\begin{aligned} \mathsf{P}_2(X'_i) \oplus \mathsf{P}_3^{-1}(X_i \oplus T_i) &= \mathsf{H}^1_i, \ \forall i = 1, \ldots, q. \\ \mathsf{P}_2(T'_i) \oplus \mathsf{P}_3^{-1}(X_i \oplus Y_i) &= S_i, \ \forall i = 1, \ldots, q. \end{aligned}$$

3. Define the bad transcript based on certain properties of the transcript graph so that Mirror Theory can be applied (to lower bound the probability of good transcripts in real world).

$\mathsf{HF}^5\mathsf{H}$: Hash then 5-round Feistel then Hash

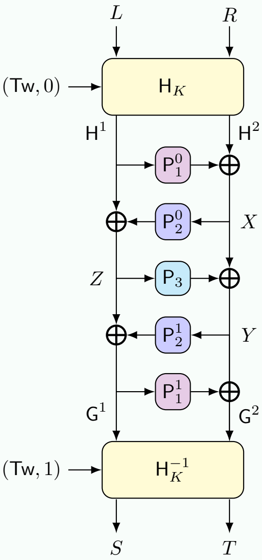


1. P_1, P_2, P_3: Independent Random Permutation.

2. $\mathsf{P}_0^b(x) := \mathsf{P}_0(\lfloor x \rfloor \| b)$.

3. Achieves TSPRP Security of $O(q^2\epsilon + q\delta + \frac{nq}{2^n})$ if
   - H is ϵ universal.
   - H^1 is δ zero-sum universal.

Optimal (T)SPRP Security of $\mathsf{HF}^5\mathsf{H}$: Proof Sketch



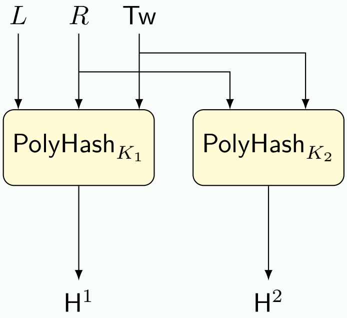
High Level Proof Idea:

1. Release K and P_1 (real world); sample K and P_1 (ideal world).
2. The following must hold:

$$\begin{aligned} \mathsf{P}_2(X_i') \oplus \mathsf{P}_3^{-1}(X_i \oplus Y_i) &= \mathsf{H}_i^1,\ \forall i = 1, \ldots, q. \\ \mathsf{P}_2(Y_i') \oplus \mathsf{P}_3^{-1}(X_i \oplus Y_i) &= \mathsf{G}_i^1,\ \forall i = 1, \ldots, q. \end{aligned}$$

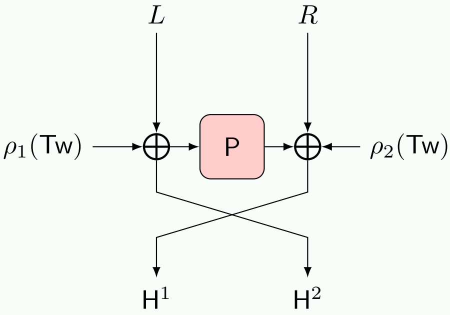
3. Define the bad transcript based on certain properties of the transcript graph so that Mirror Theory can be applied (to lower bound the probability of good transcripts in real world).

Tweakable Hash Instantiation #1



1. $\mathsf{PolyHash}_K(X) := X_{t-1} \cdot K^{t-1} \oplus \cdots \oplus X_1 \cdot K \oplus X_0$
2. $\mathsf{PolyHash}_{K_1}(L, R, \mathsf{Tw}) = L \oplus K_1 \cdot \mathsf{PolyHash}_{K_1}(R, \mathsf{Tw})$
3. $\mathsf{PolyHash}_{K_2}(R, \mathsf{Tw}) = R \oplus K_2 \cdot \mathsf{PolyHash}_{K_2}(\mathsf{Tw})$
4. H is invertible and $\ell^2/2^{2n}$ universal
5. H^1 is and $\ell/2^n$ constant-sum universal

Tweakable Hash Instantiation #2



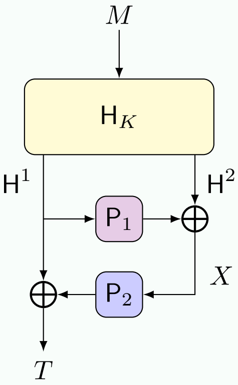
1. $\rho : \{0,1\}^\star \rightarrow \{0,1\}^n$ is ϵ AXU-hash function
2. P is a random permutation
3. H is invertible and ϵ^2 universal
4. H^1 is $\left(\epsilon + \frac{2}{2^n}\right)$ zero-sum universal

Summary When the Hash is Instantiated with RP

Ref	# RP Call	# Indep RP	# AXU Call	Attack Model	Security
CS'25	5	5	2	(T)PRP	n
This Work	5	3	2	(T)PRP	n
CS'25	7	7	2	(T)SPRP	n
This Work	7	4	2	(T)SPRP	n

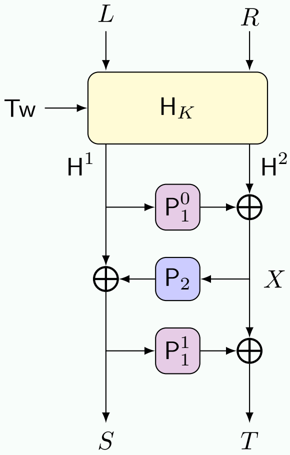
Can you Minimize the Primitive Calls to Obtain BBB TLR?

HF^2: Hash then 2-round Feistel



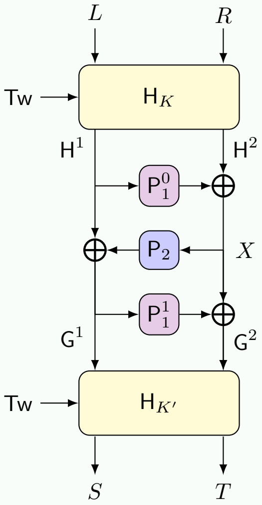
1. P_1, P_2: Independent Random Permutation.
2. Achieves PRF Security of $O(q^2\epsilon + \frac{q\delta}{2^n} + \frac{q}{2^{3n/4}})$ queries if
   - H is ϵ universal.
   - Both H^1 and H^2 are δ universal.

HF^3: Hash then 3-round Feistel



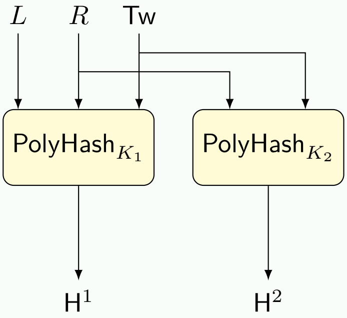
1. $\mathsf{P}_1, \mathsf{P}_2, \mathsf{P}_3$: Independent Random Permutation.
2. $\mathsf{P}_0^b(x) := \mathsf{P}_0(\lfloor x \rfloor \| b)$.
3. Achieves TPRP Security of $O(q^2\epsilon + \frac{q\delta}{2^n} + \frac{q}{2^{3n/4}})$ if
   - H is ϵ universal.
   - Both H^1 and H^2 are δ universal.

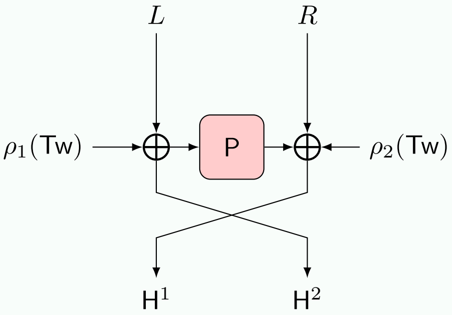
HF^{3}H: Hash then 3-round Feistel then Hash



1. P_1, P_2: Independent Random Permutation.
2. $\mathsf{P}_0^b(x) := \mathsf{P}_0(\lfloor x \rfloor \| b)$.
3. Achieves TSPRP Security of $O(q^2\epsilon + \frac{q\delta}{2^n} + \frac{q}{2^{3n/4}})$ if
   - H is ϵ universal.
   - Both H^1 and H^2 are δ universal.

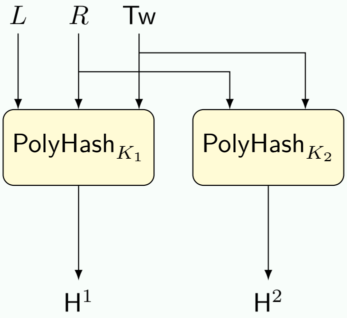
Tweakable Hash Instantiations

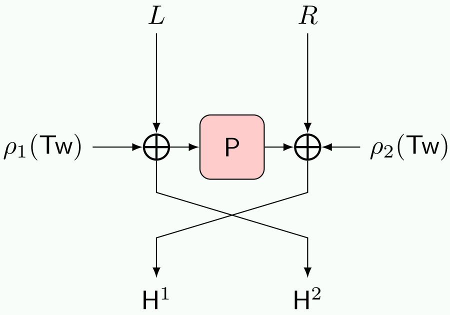




Will the above hash functions work?

Tweakable Hash Instantiations

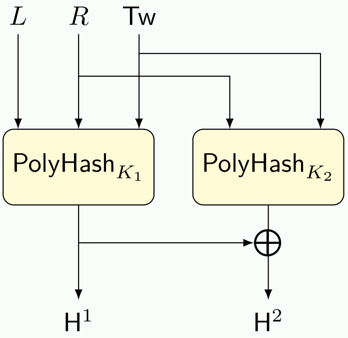


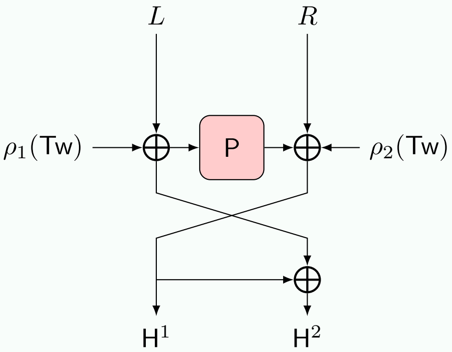


Will the above hash functions work? NO..!!

Tweakable Hash Instantiations

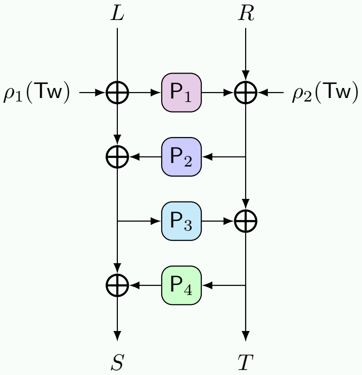
tcg crest
Inventing Harmonious Future



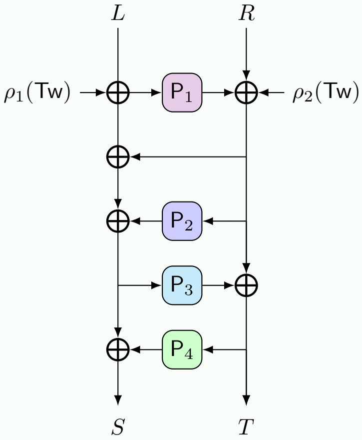


Simple Variant works..!!

TPRP with RP Instantiation

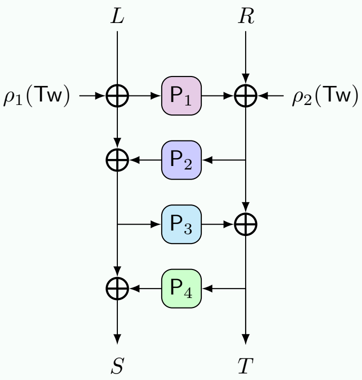


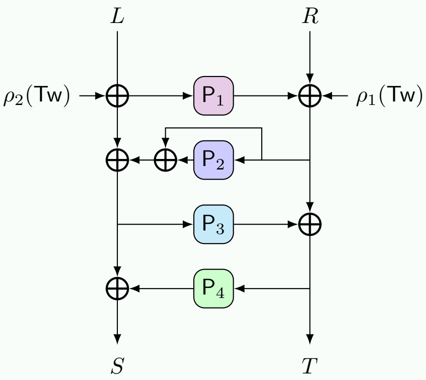
Achieves security at most $2^{n/2}$ queries.



Achieves BBB security up to $2^{3n/4}$ queries.

TPRP with RP Instantiation

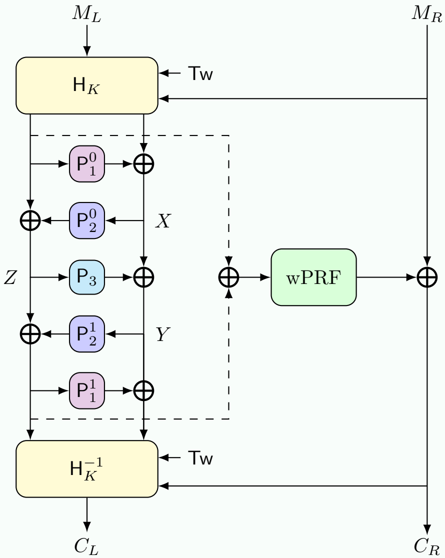




Achieves security at most $2^{n/2}$ queries.

Achieves BBB security up to $2^{3n/4}$ queries.

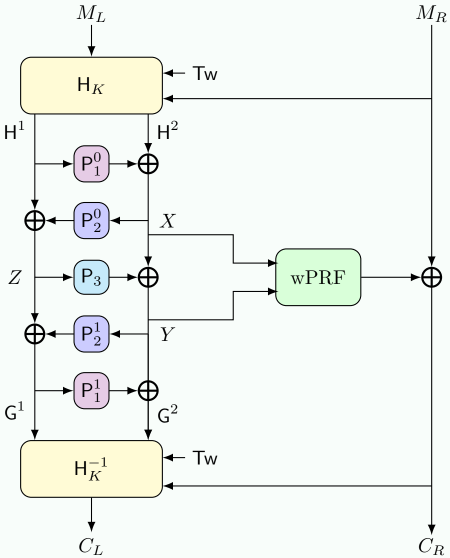
Applications: Optimally Secure Accordion Modes



High Level Idea:

- Employ double-block HCTR style encryption
- Use $\mathsf{HF^5H}$ to instantiate double block optimally secure STPRP.
- Combine with an optimally secure weak PRF, e.g.,
  - Snowflake (Chen et al., EC'25)
  - eCTR [Chung et al., EC'25)

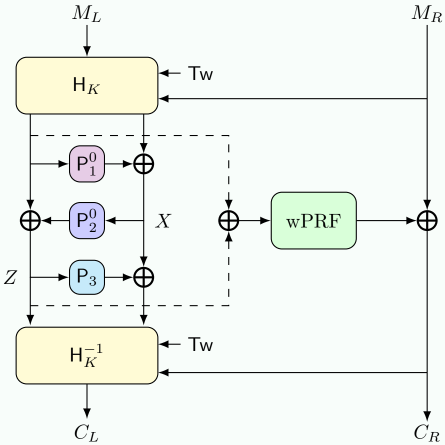
Applications: Optimally Secure Accordion Modes



Ongoing Work (An Efficient Variant):

- Use internal state X and Y in the weak PRF input
- Efficient weak PRF that minimizes the number of primitive invocations
- Efficient Hash Instantiations

Applications: Efficient BBB Secure Accordion Modes

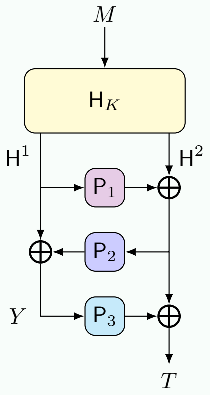


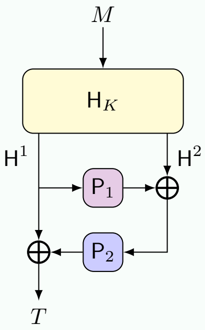
Ongoing Work (An Efficient BBB Variant):

- Efficient BBB-secure weak PRF that minimizes the number of primitive invocations
- Efficient BBB-secure Hash Instantiations

Conclusion and Open Research Avenues

Luby Rackoff Goes BBB - Constructing VIL-PRF

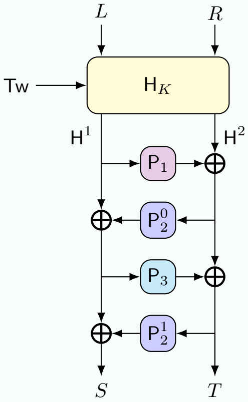


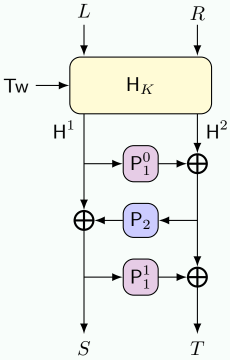


- H: universal, H^1: zero-sum universal.
- Optimal Security

- H, H^1, H^2: universal.
- $3n/4$-bit Security.

Luby Rackoff Goes BBB - Constructing TPRP

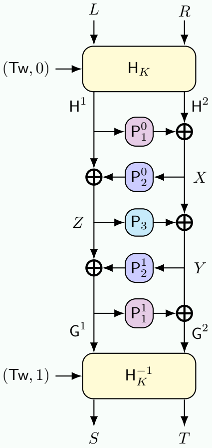




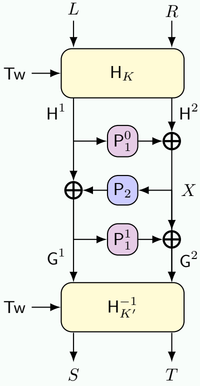
- H: universal, H^1: constant-sum universal.
- Optimal Security.

- H, H^1, H^2: universal.
- $3n/4$-bit Security.

Luby Rackoff Goes BBB - Constructing STPRP



- H: universal, H^1: zero-sum universal.
- Optimal Security

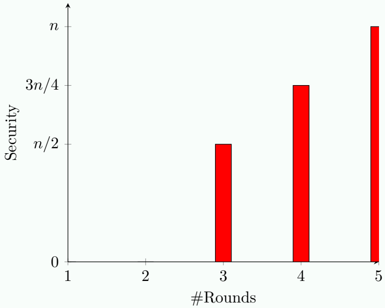


- H, H^1, H^2: universal.
- $3n/4$-bit Security.

Summary When the Hash is Instantiated with RP

Ref	# RP Call	# Indep RP	# AXU Call	Attack Model	Security
CS'25	5	5	2	PRF	n
This Work	4	3	2	PRF	n
This Work	3	2	2	PRF	$3n/4$
CS'25	5	5	2	(T)PRP	n
This Work	5	3	2	(T)PRP	n
This Work	4	3	2	(T)PRP	$3n/4$
CS'25	7	7	2	(T)SPRP	n
This Work	7	4	2	(T)SPRP	n
This Work	5	4	2	(T)SPRP	$3n/4$

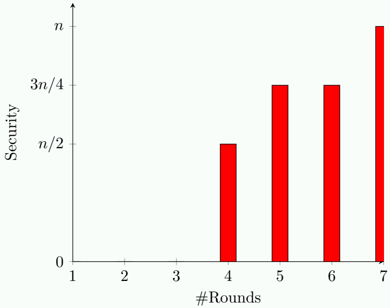
Open Research Avenues



LR-based Double-block (T)PRP

- Minimal # RP calls to obtain BBB security
- Minimal # RP calls to obtain optimal security
- Tight security with 3 and 4 rounds

Open Research Avenues



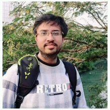
LR-based Double-block (T)SPRP

- Minimal # RP calls to obtain BBB security
- Minimal # RP calls to obtain optimal security
- Tight security with 4, 5 and 6 rounds

For More Details...

tcg crest
Inventing Harmonious Future

https://eprint.iacr.org/2025/1486.pdf



Thank You...

Questions... Comments... Suggestions...