Tweakable, Permutation-based Luby-Rackoff Constructions

Bishwajit Chakraborty[1] Abishanka Saha[2]

Nanyang Technological University, Singapore

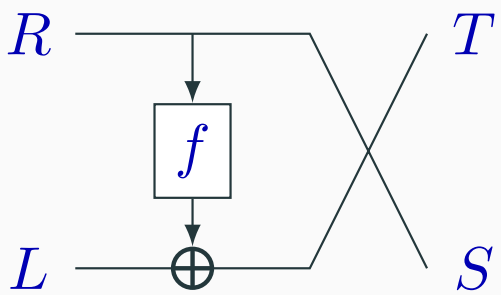
Eindhoven University of Technology, The Netherlands

The Luby-Rackoff construction

The Luby-Rackoff construction

The Luby-Rackoff transformation converts a n-bit function, $f : \{0,1\}^n \to \{0,1\}^n$, to a $2n$-bit permutation,

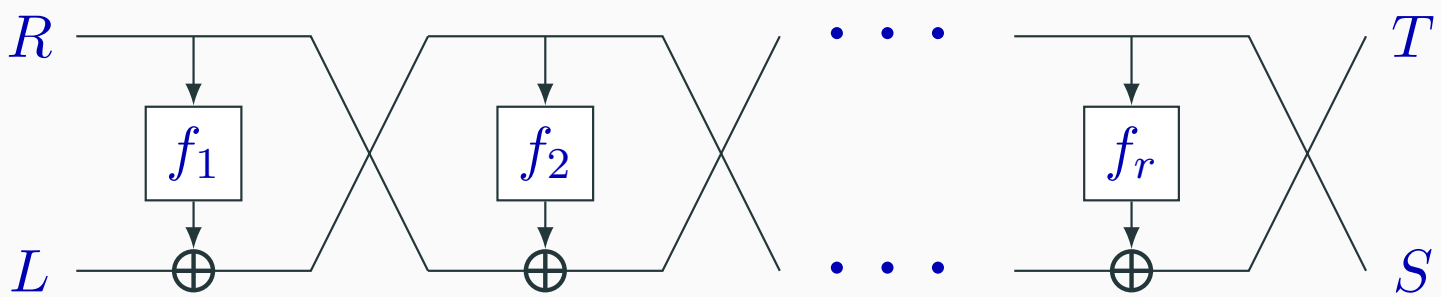
$$\Psi^f : \{0,1\}^{2n} \to \{0,1\}^{2n}$$
$$(L, R) \mapsto (S, T)$$



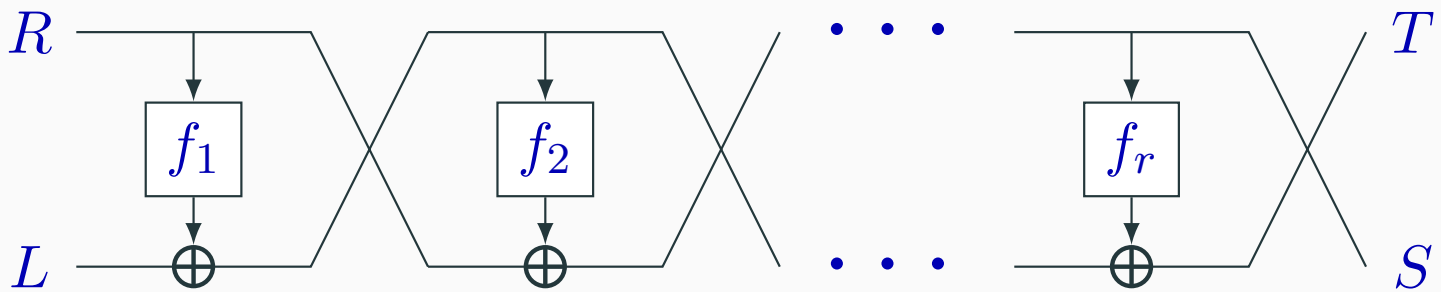
The Luby-Rackoff construction

Given r n-bit functions $f_1, \ldots, f_r : \{0,1\}^n \to \{0,1\}^n$ we can extend this to the r-round Luby-Rackoff construction

$$\Psi^{(f_1,\ldots,f_r)} : \{0,1\}^{2n} \to \{0,1\}^{2n}$$



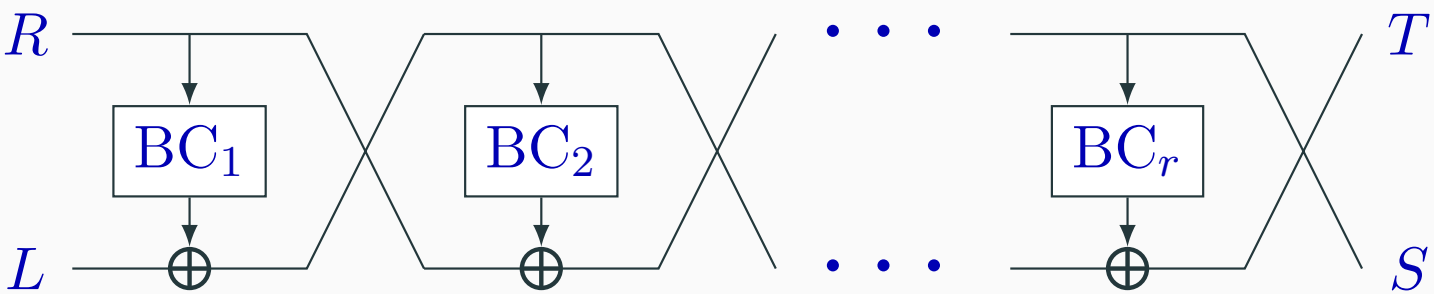
The Luby-Rackoff construction



Most security analyses are done in Random Oracle model: for $F_1, \ldots, F_r \leftarrow\!\!\$ \mathsf{Func}(n)$,

$$\mathbf{Adv}^{\mathrm{prp}}_{\Psi(f_1,\ldots,f_r)} \leq \mathbf{Adv}^{\mathrm{prp}}_{\Psi(F_1,\ldots,F_r)} + \sum_{i=1}^{r} \mathbf{Adv}^{\mathrm{prf}}_{f_i}$$

The Luby-Rackoff construction



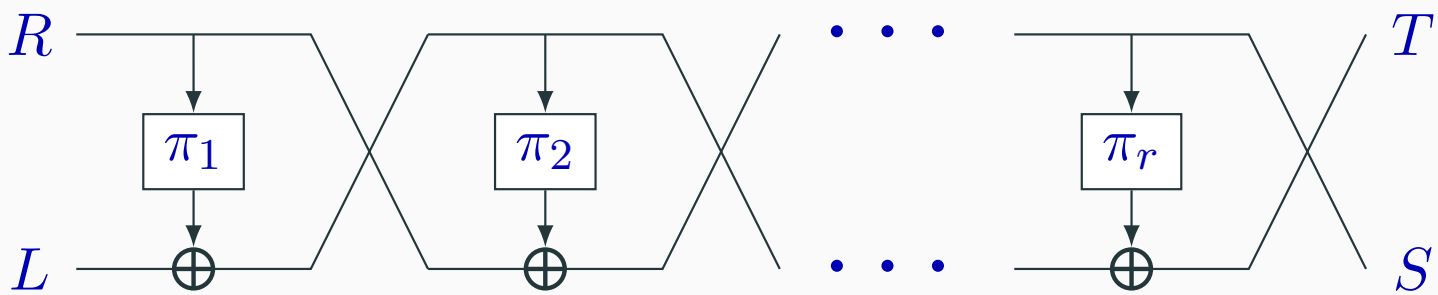
$F_1, \ldots, F_r \leftarrow\!\!\$ \mathsf{Func}(n)$,

$$\mathbf{Adv}^{\mathrm{prp}}_{\Psi(f_1,\ldots,f_r)} \leq \mathbf{Adv}^{\mathrm{prp}}_{\Psi(F_1,\ldots,F_r)} + \sum_{i=1}^{r} \mathbf{Adv}^{\mathrm{prf}}_{\mathrm{BC}_i}$$

⚠ Birthday Bound due to PRP-PRF switching lemma.

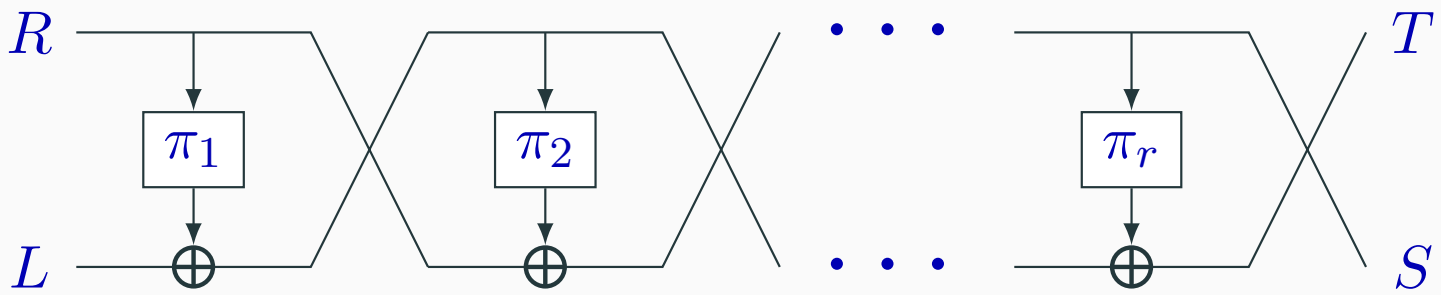
Permutation-based Luby-Rackoff (pLR)

Instead we can analyze the security of Luby-Rackoff when the internal primitives are indeed permutations, i.e., for $\pi_1, \ldots, \pi_r \in \mathsf{Perm}(n)$,



Permutation-based Luby-Rackoff (pLR)

$\pi_1, \ldots, \pi_r \in \mathsf{Perm}(n)$,



Previous BBB results: Guo et al.[1] showed

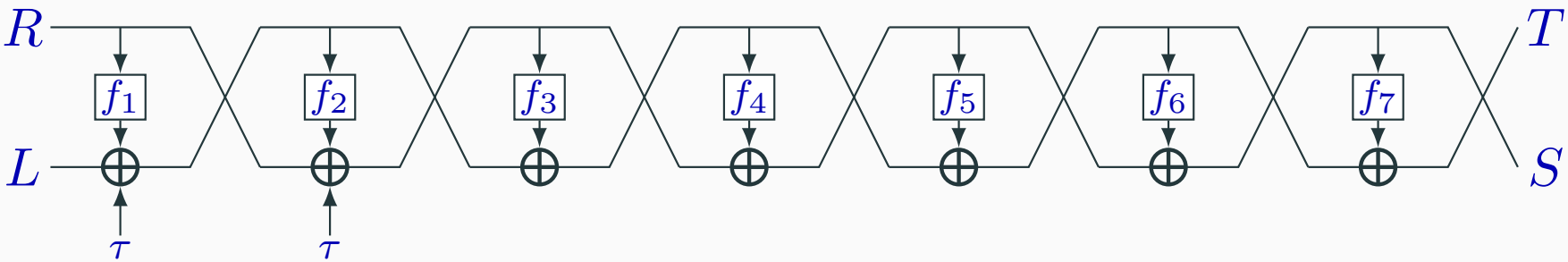
- 5-rounds of pLR is a $\frac{2}{3}n$-bit secure PRP.
- 7-rounds of pLR is a $\frac{2}{3}n$-bit secure SPRP.

[1] Guo, C., Zhang, G.: *Beyond-birthday security for permutation-based feistel networks.* Designs, Codes and Cryptography 89, 407–440 (2021)

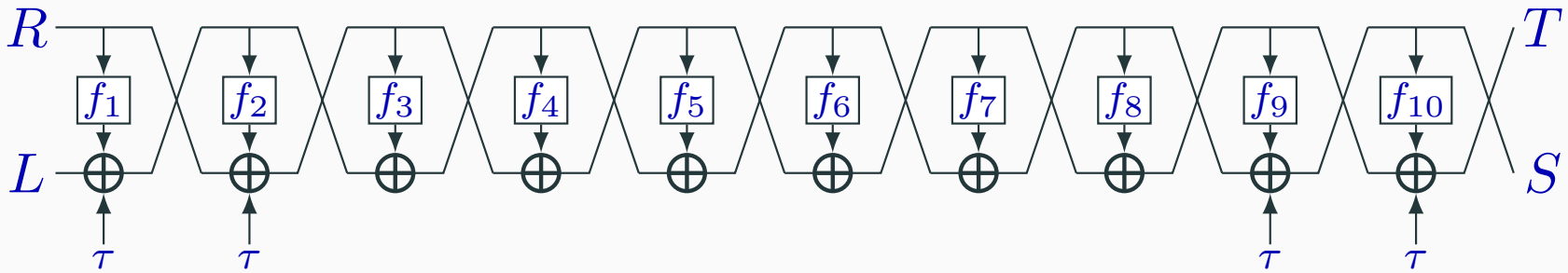
Tweaking Luby-Rackoff

Tweakable Luby-Rackoff construction

Goldenberg et al.[2] showed that



is a n-bit secure TPRP, and

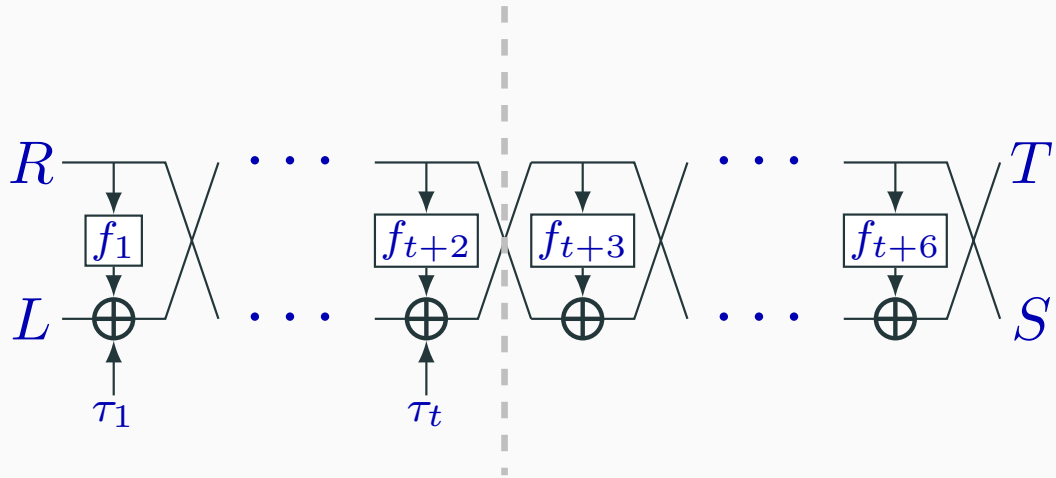


is a n-bit secure TSPRP.

[2] Goldenberg, D., Hohenberger, S., Liskov, M., Schwartz, E.C., Seyalioglu, H. *On Tweaking Luby-Rackoff Blockciphers.* In: Kurosawa, K. (eds) Advances in Cryptology – ASIACRYPT 2007.

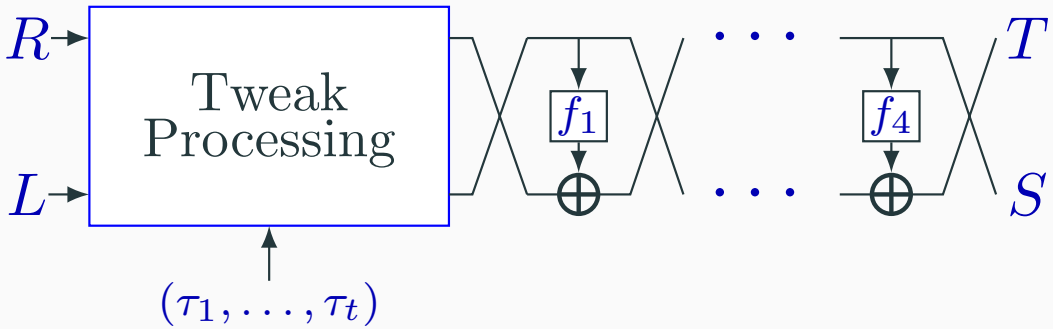
For longer tweaks...

n-bit CPA/TPRP security



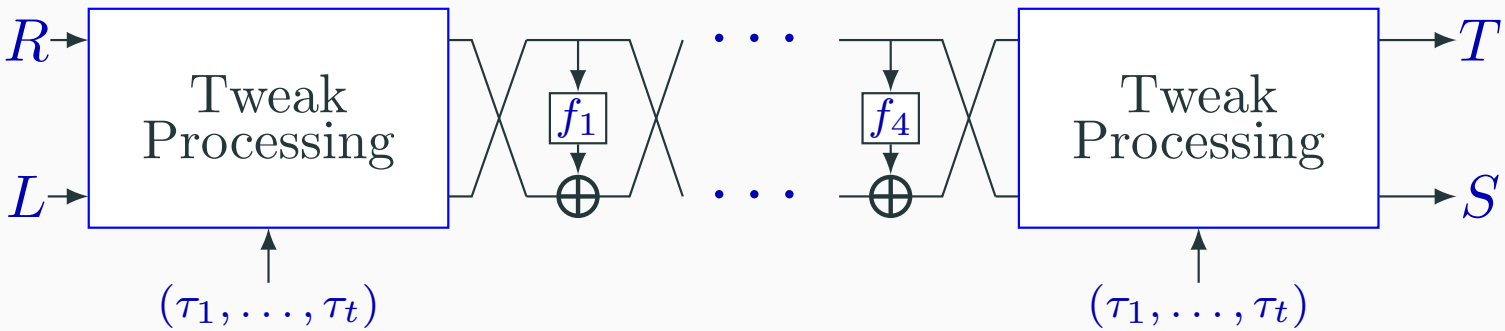
For longer tweaks...

n-bit CPA/TPRP security



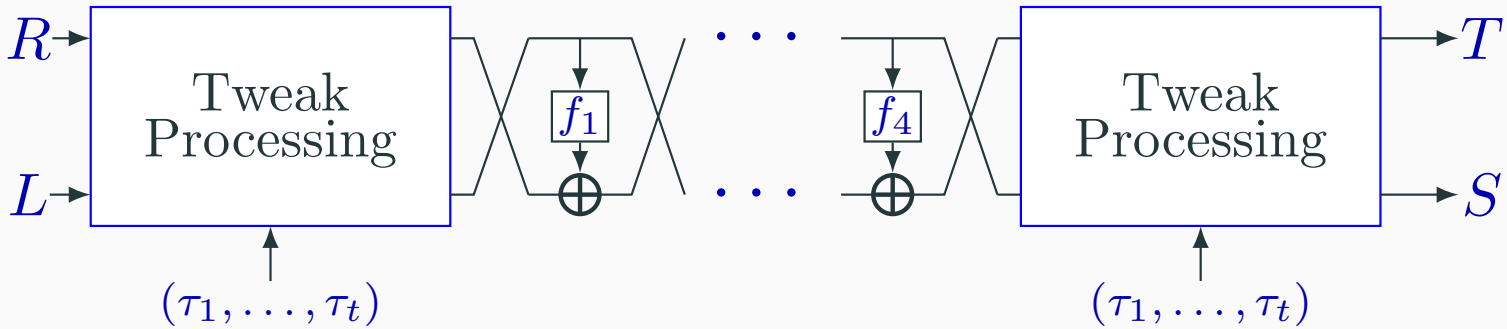
For longer tweaks...

n-bit CCA/TSPRP security



For longer tweaks...

n-bit CCA/TSPRP security



- Tweak Processing : $(t+2)$-LR rounds.

Our Contributions

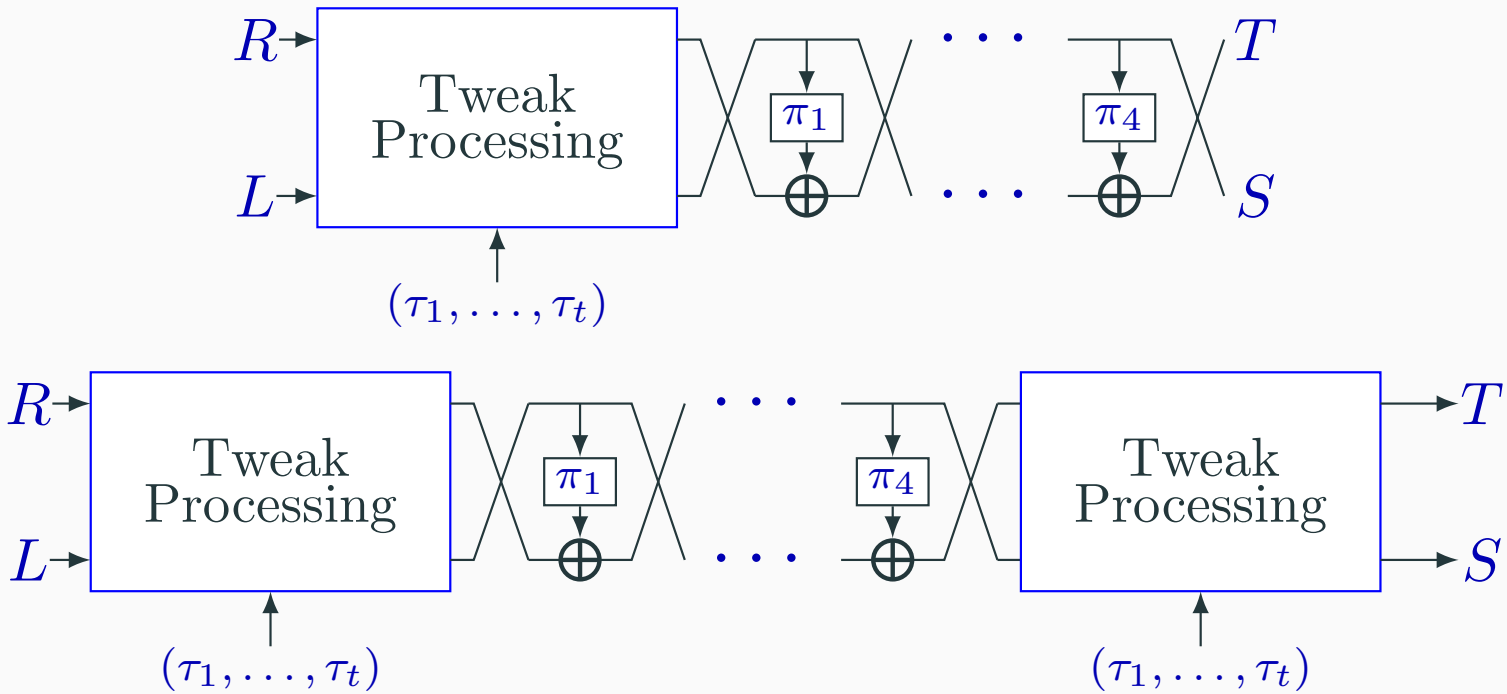
Outline

Our Contributions

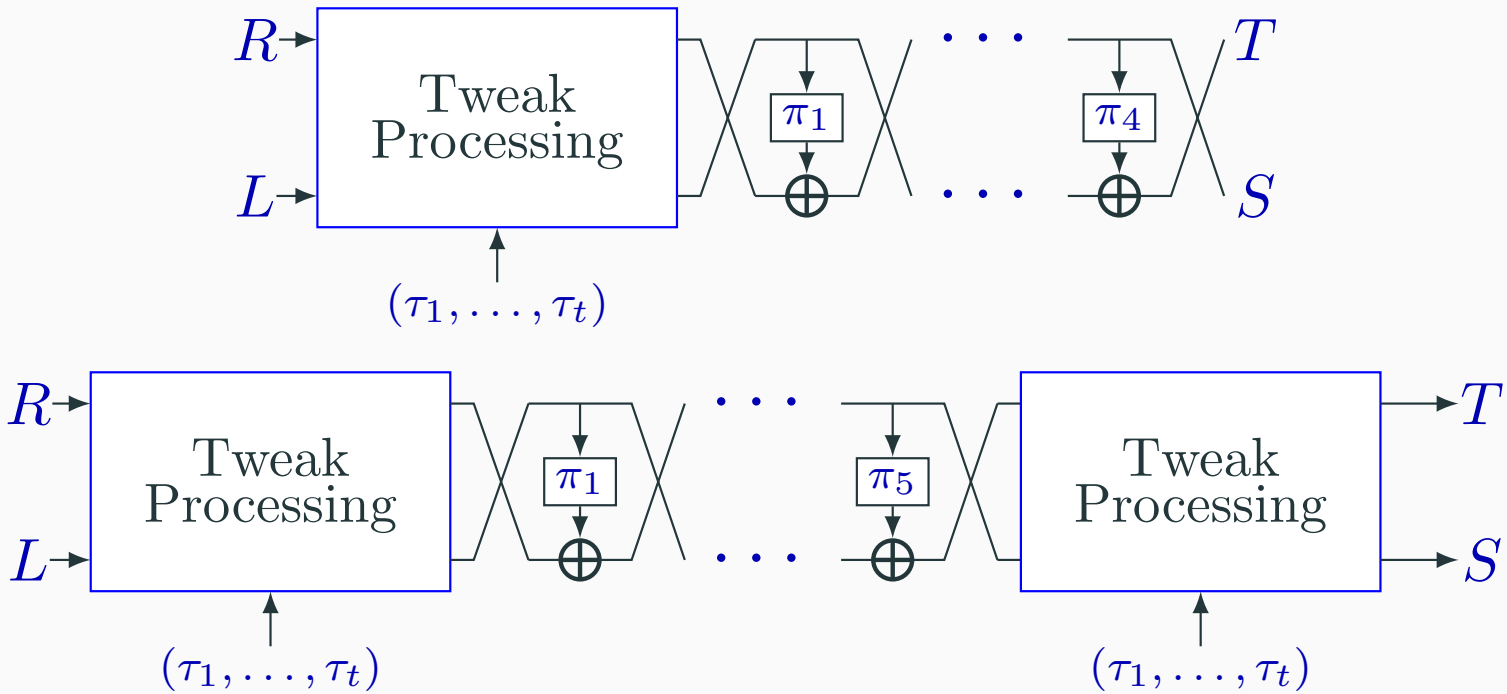
Two motivating questions for this work:

- Can the results of Goldenberg et al. be extended to *permutation-based* LR constructions?
- Can the number of rounds required in tweak processing be reduced?

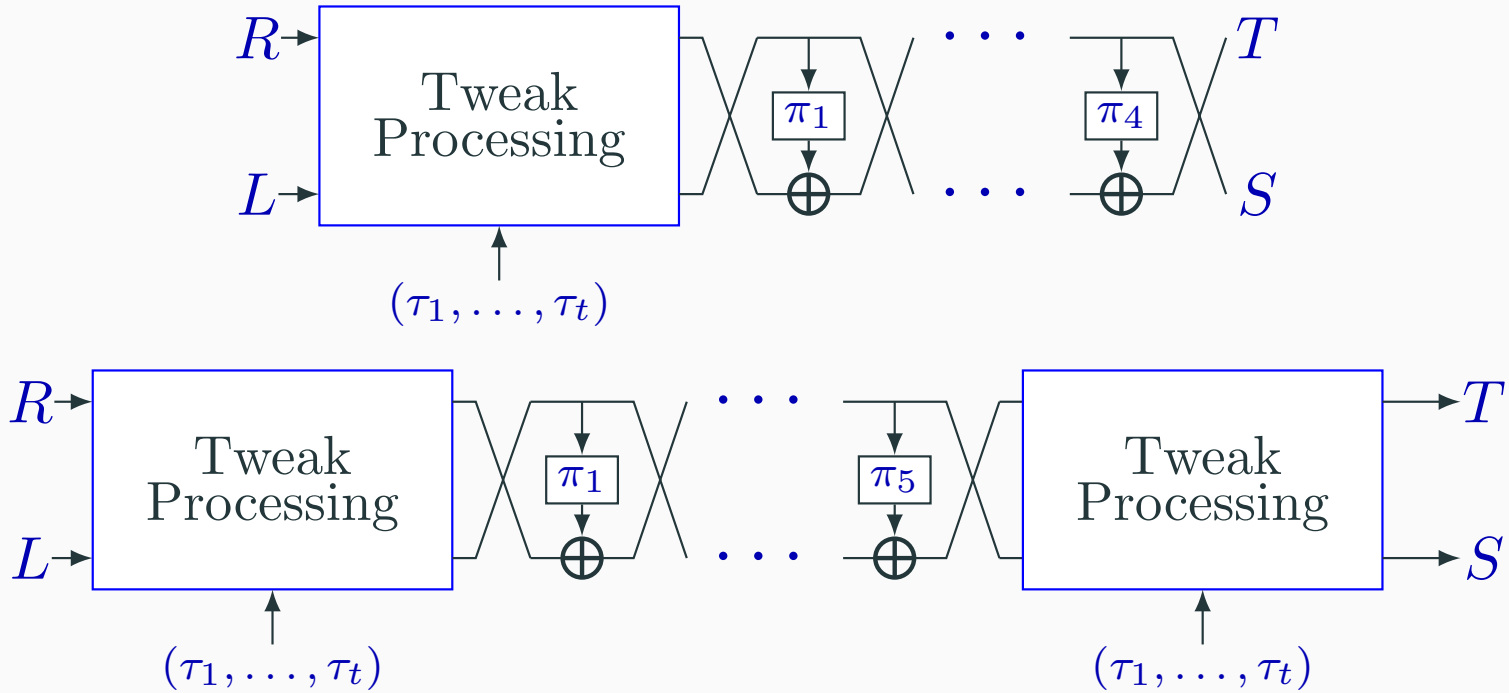
Our Contributions



Our Contributions

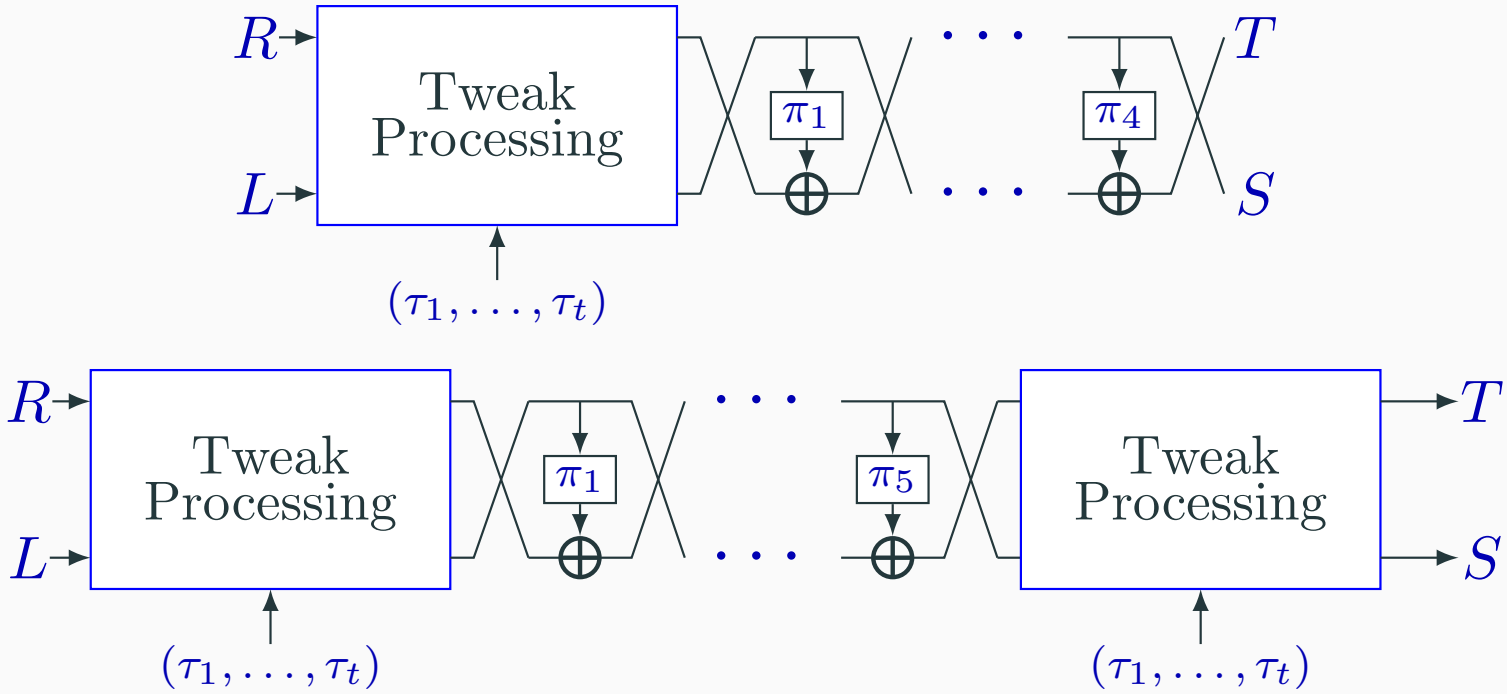


Our Contributions



Find the probabilistic requirements from the $2n$-bit-to-$2n$-bit maps Processing t blocks of n-bit tweaks.

Our Contributions



TLR-Compatible Function Family

Outline

Our Contributions

- Motivation
- TLR-compatible family
- Our candidates
- Proof sketch
- Mirror theory
- Corollary: (S)PRP

TLR-compatible family

$\mathcal{F} \subseteq \mathsf{TPerm}(tn, 2n)$ is *TLR-compatible* if:

For $(T_1, X_1) \neq (T_2, X_2) \in \{0,1\}^{tn} \times \{0,1\}^{2n}$,

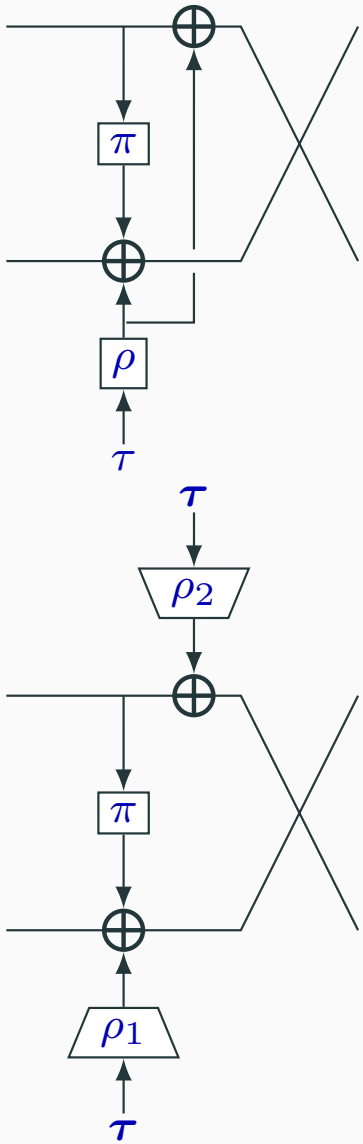
- probability of full collision is negligible,

$$\Pr_{F \leftarrow\$ \mathcal{F}}[F(T_1, X_1) = F(T_2, X_2)] \leq \frac{4}{2^{2n}}.$$

- probability of collision in the right half of the output is negligible,

$$\Pr_{F \leftarrow\$ \mathcal{F}}[F(T_1, X_1)_R = F(T_2, X_2)_R] \leq \frac{2}{2^{n}}.$$

TLR compatible family from 1-round pLR



For n-bit tweak:

$\rho \leftarrow\!\!\$ \mathsf{Perm}(n)$

For b blocks of n-bit tweaks:

$\rho_1, \rho_2 \leftarrow\!\!\$$ AXU Hash function family

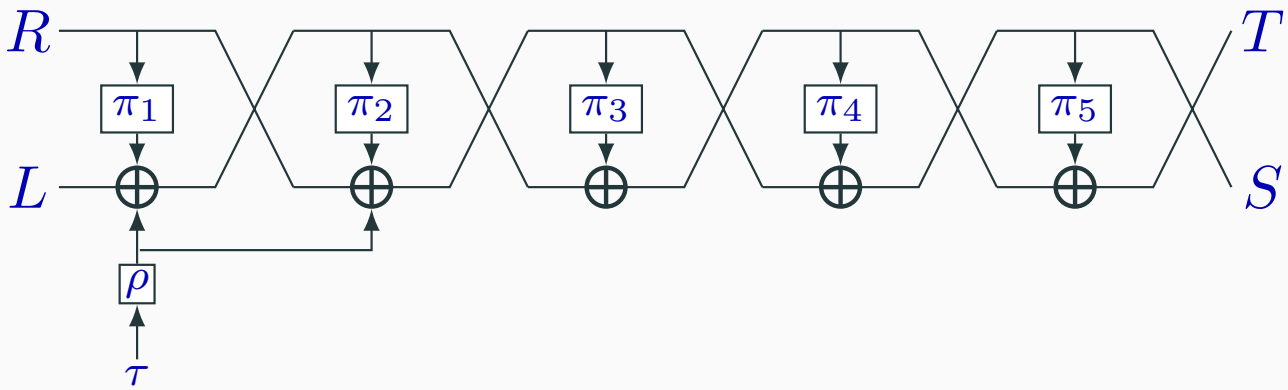
$\Big($for any $x \neq x' \in \{0,1\}^*, a \in \{0,1\}^n$,

$\Pr_{H \leftarrow\!\!\$ \mathcal{H}}[H(x) \oplus H(x') = a] \leq \frac{2}{2^n}.\Big)$

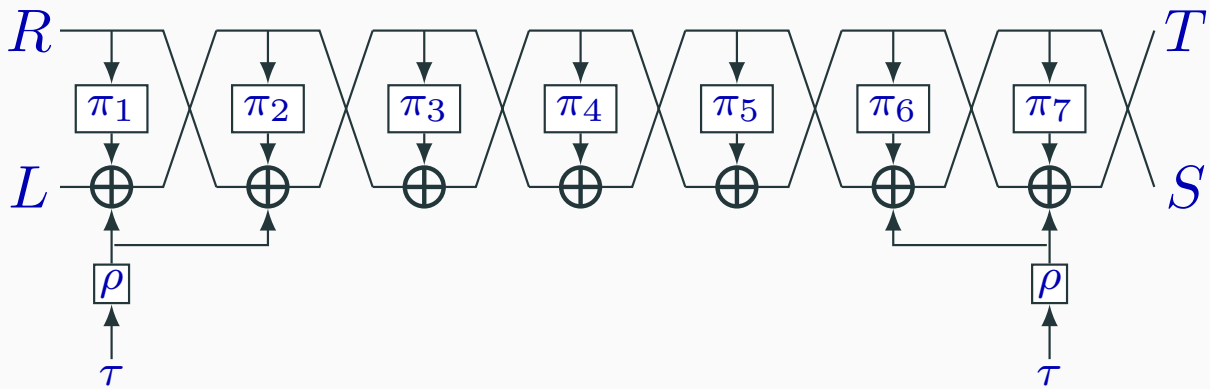
Outline

Instantiations

For n-bit tweaks



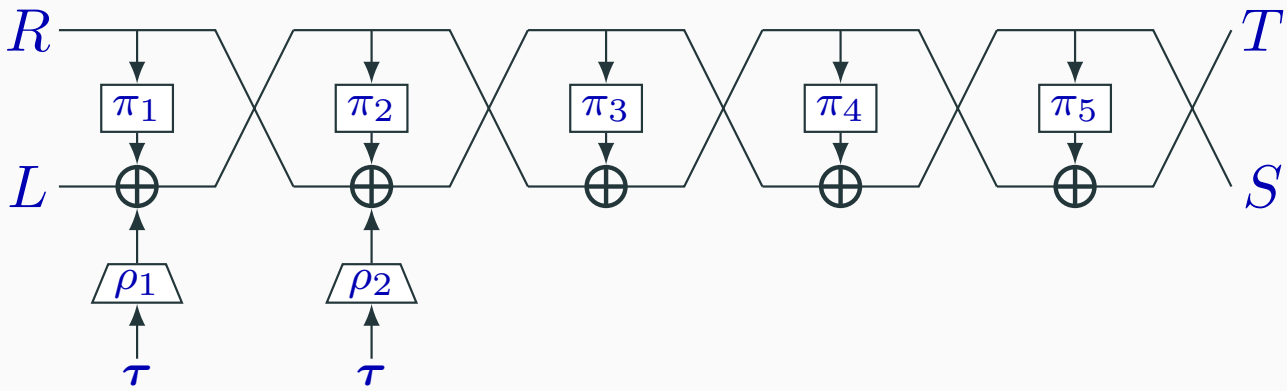
n-bit secure TPRP candidate: TLRP5.



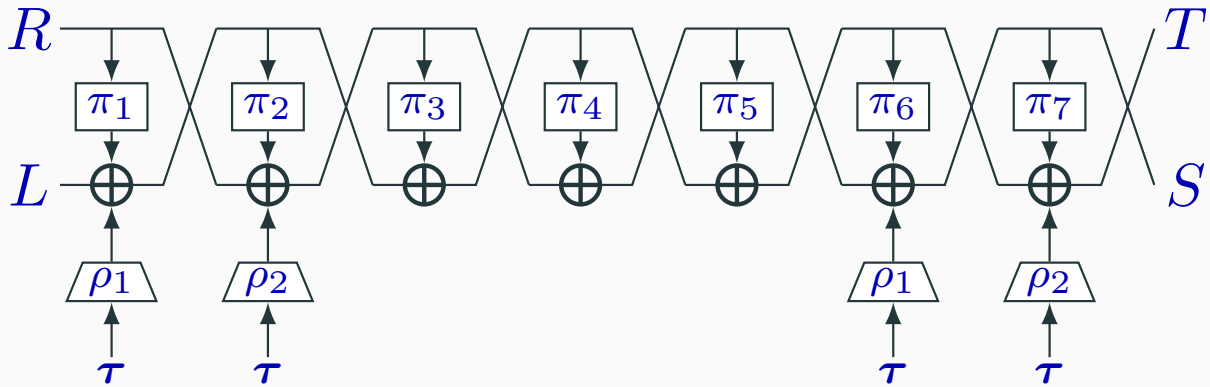
n-bit secure TSPRP candidate: TLRP7.

Instantiations

For b-blocks of n-bit tweaks



n-bit secure TPRP candidate: TLRP5+.



n-bit secure TSPRP candidate: TLRP7+.

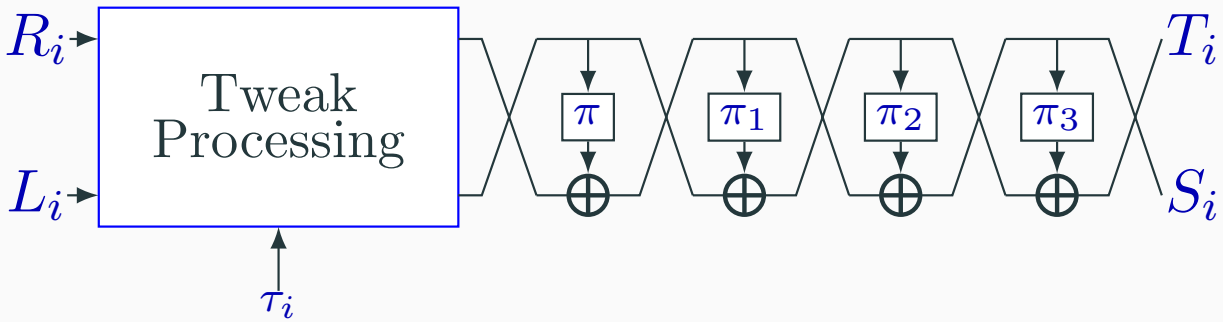
Outline

Our Contributions

- Motivation
- TLR-compatible family
- Our candidates
- Proof sketch
- Mirror theory
- Corollary: (S)PRP

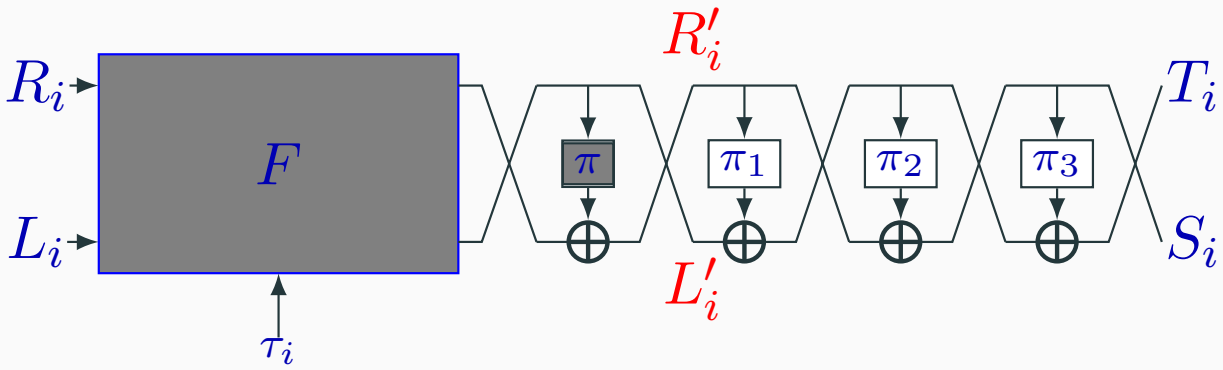
Proof sketch

transcript: $\{((\tau_i, L_i, R_i), (S_i, T_i))\}$



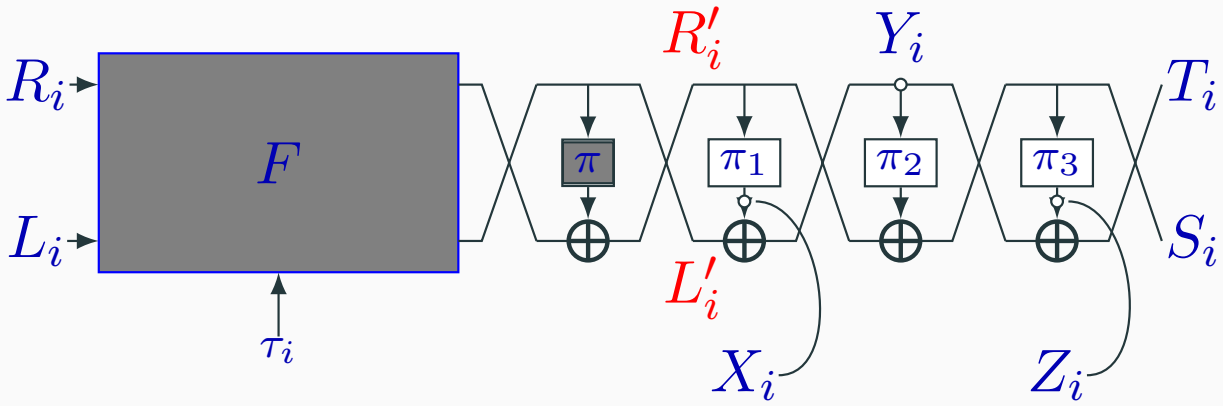
Proof sketch

extended transcript: $\{((\tau_i, L_i, R_i), L'_i, R'_i, (S_i, T_i))\}$



Proof sketch

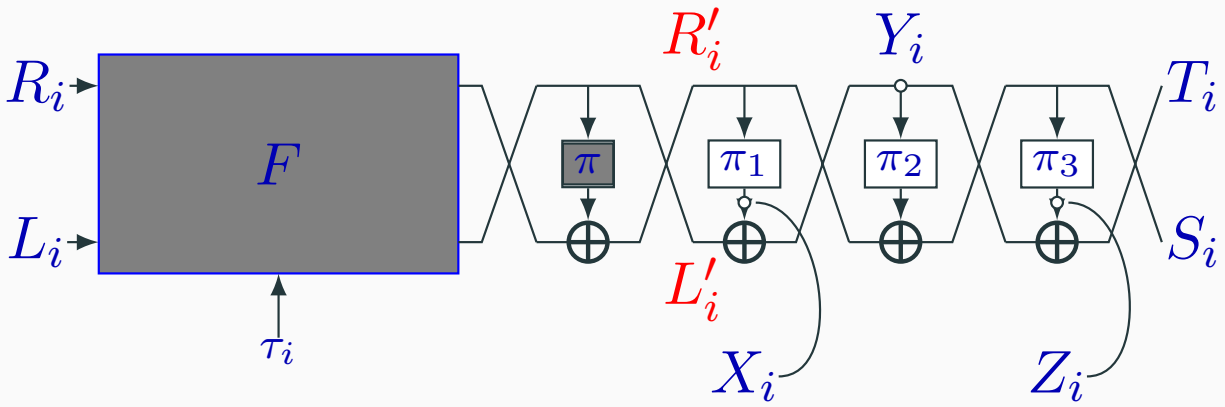
extended transcript: $\{((\tau_i, L_i, R_i), L'_i, R'_i, (S_i, T_i))\}$



$$X_i \oplus Y_i = L'_i, \quad Y_i \oplus Z_i = T_i, \qquad i \in [q]$$

Proof sketch

extended transcript: $\{((\tau_i, L_i, R_i), L'_i, R'_i, (S_i, T_i))\}$

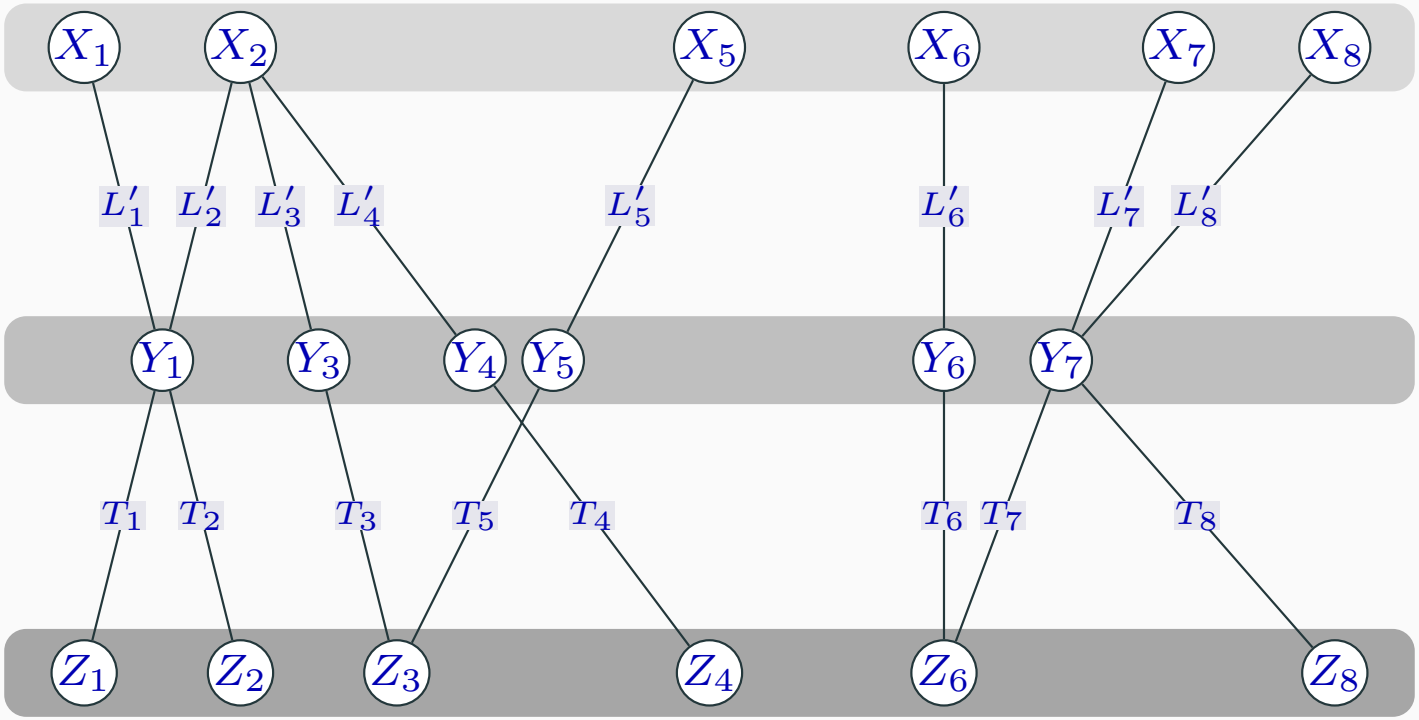


$$X_i \oplus Y_i = L'_i, \quad Y_i \oplus Z_i = T_i, \qquad i \in [q]$$

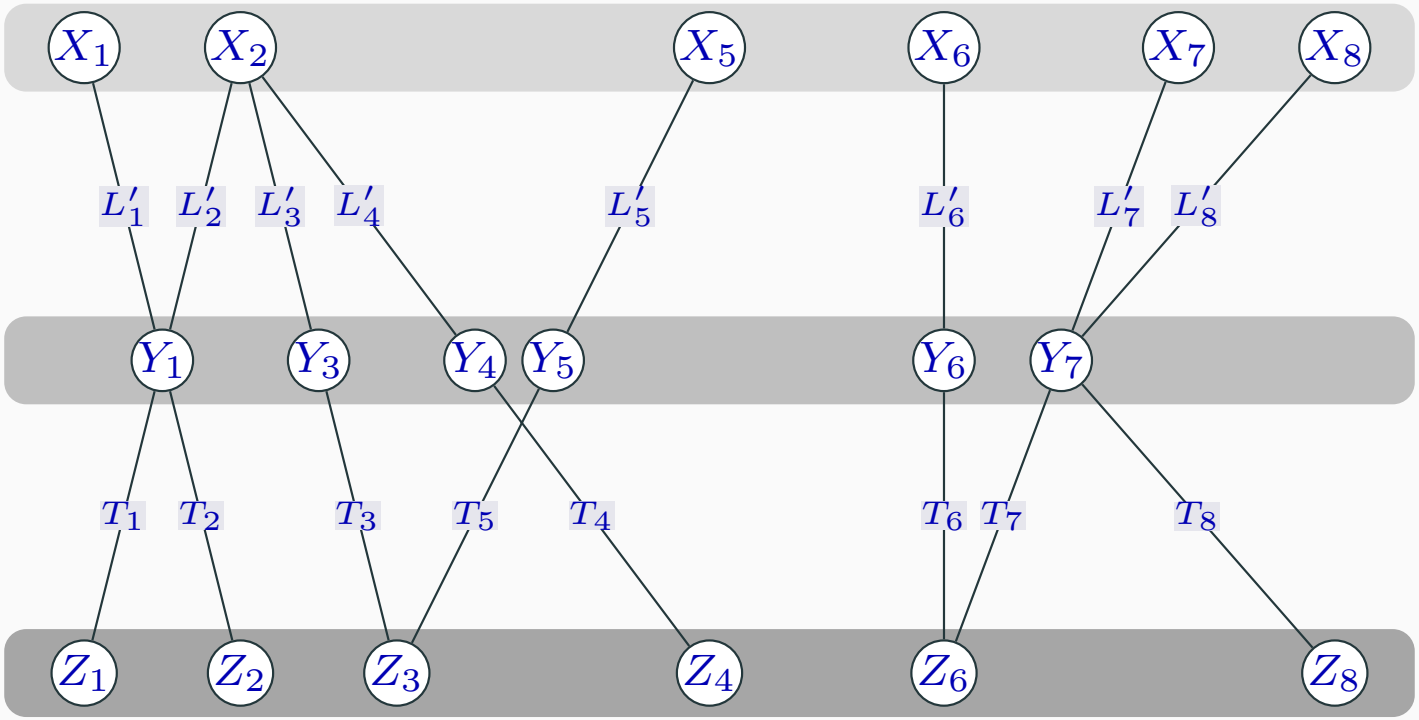
Note that $R'_i = R'_j \iff X_i = X_j, \qquad S_i = S_j \iff Z_i = Z_j$

$$R'_i \oplus S_i = R'_j \oplus S_j \iff Y_i = Y_j$$

Proof sketch

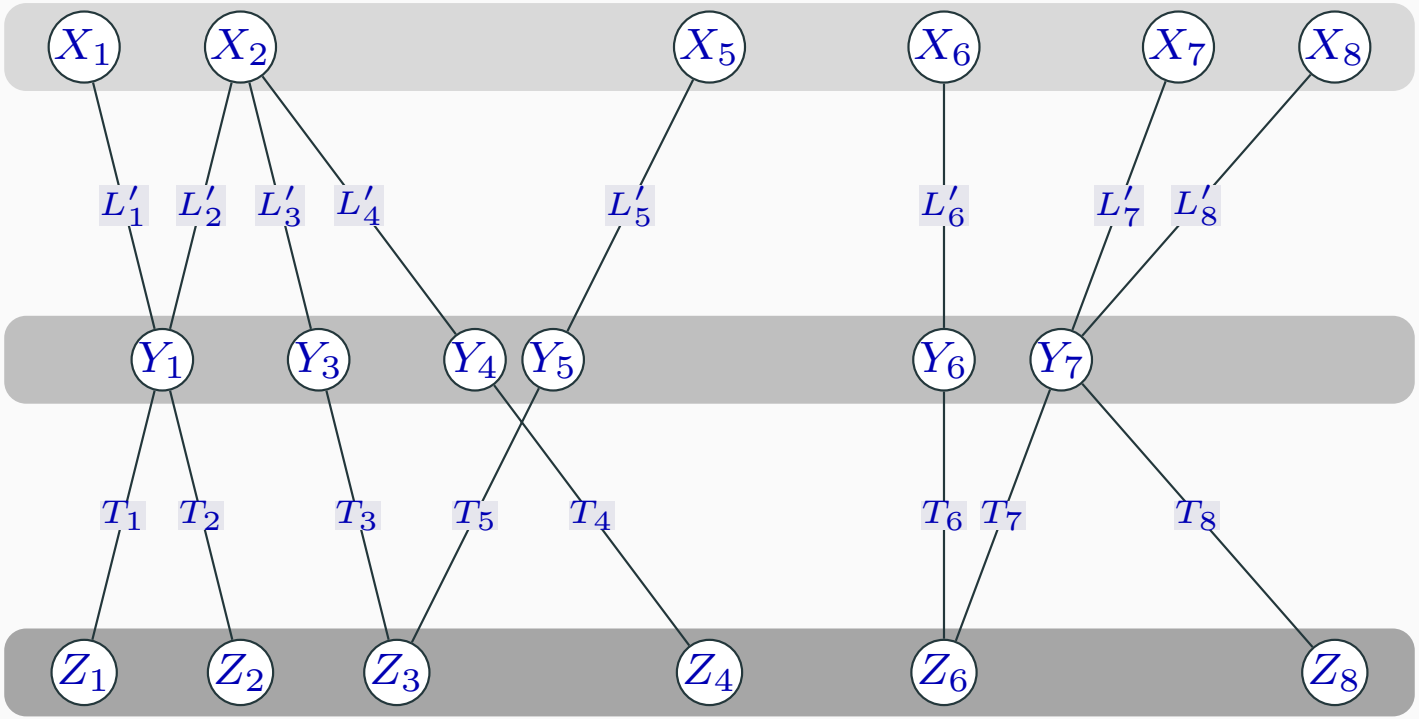


Proof sketch



Bad events: • cycles, • component size too large, • path between two $X/Y/Z$-vertices has label sum zero - w.p. $\mathcal{O}(q/2^n)$ due to TLR-compatibility.

Proof sketch



$\#(X, Y, Z)$-respecting solutions

$=\#$ permutation-triples (π_1, π_2, π_3): $\Psi^{(\pi_1,\pi_2,\pi_3)}(L'_i, R'_i) = (S_i, T_i)$.

Outline

Mirror Theory for three independent permutations

Theorem

Good system of equations: $\#$ *equations* $= e$,
partition of variables $= V_1 \sqcup V_2 \sqcup V_3$.
largest component size $= \xi$

If $q \leq \frac{2^n}{48\xi^2}$ *and* $2^{n/2} > n\xi^2 + n$,

$$\#(V_1, V_2, V_3)\text{-respecting solutions} \geq \frac{(2^n - 2)_{|V_1|}(2^n - 2)_{|V_2|}(2^n - 2)_{|V_3|}}{2^{ne}}.$$

Mirror Theory for three independent permutations

Theorem

Good system of equations: $\#$ *equations* $= e$,
partition of variables $= V_1 \sqcup V_2 \sqcup V_3$.
largest component size $= \xi$

If $q \leq \frac{2^n}{48\xi^2}$ *and* $2^{n/2} > n\xi^2 + n$,

$$\#(V_1, V_2, V_3)\text{-respecting solutions} \geq \frac{(2^n - 2)_{|V_1|}(2^n - 2)_{|V_2|}(2^n - 2)_{|V_3|}}{2^{ne}}.$$

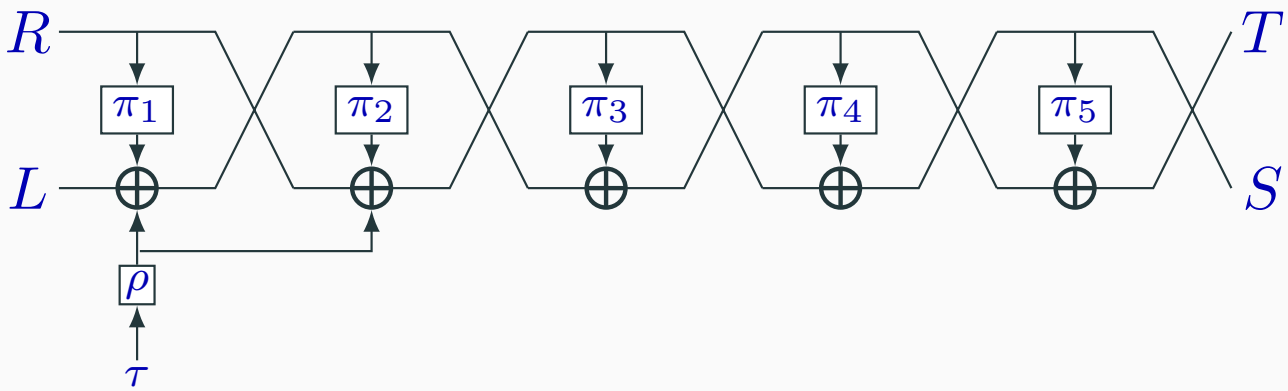
expected $\#(V_1, V_2, V_3)$-respecting solutions $= \dfrac{(2^n)_{|V_1|}(2^n)_{|V_2|}(2^n)_{|V_3|}}{2^{ne}}$.

Outline

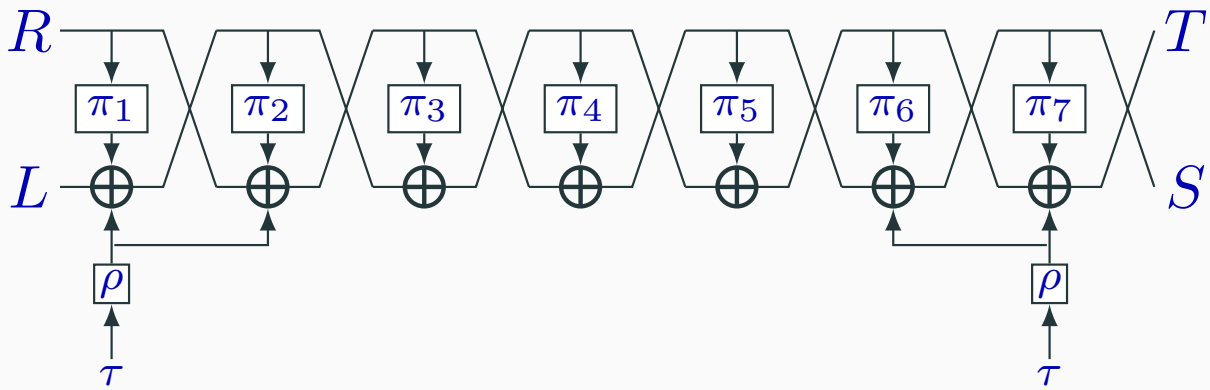
Our Contributions

- Motivation
- TLR-compatible family
- Our candidates
- Proof sketch
- Mirror theory
- Corollary: (S)PRP

5/7-rounds pLR is optimally secure PRP/SPRP

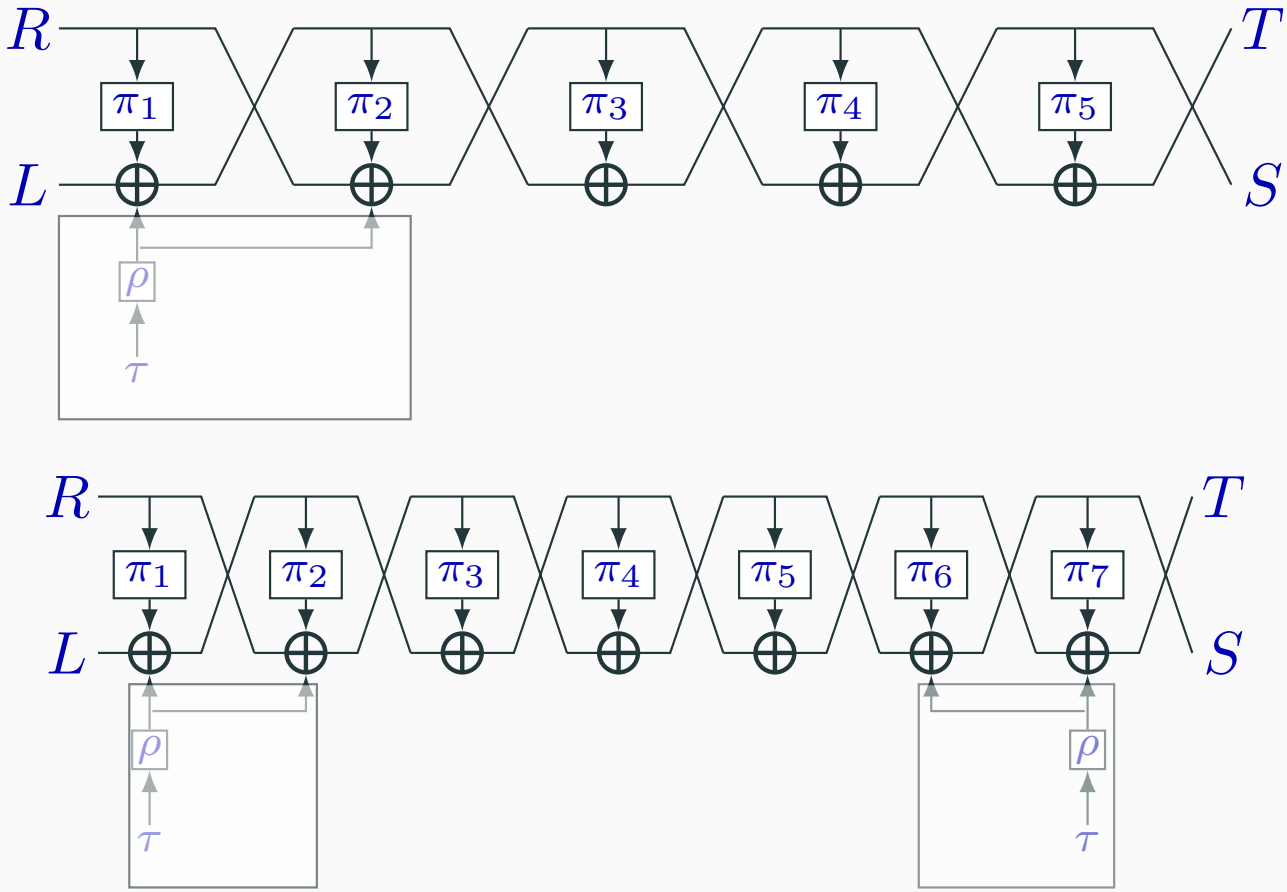


n-bit secure TPRP candidate: TLRP5.

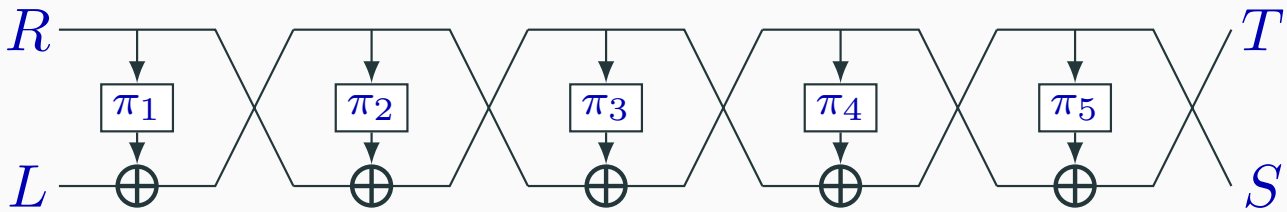


n-bit secure TSPRP candidate: TLRP7.

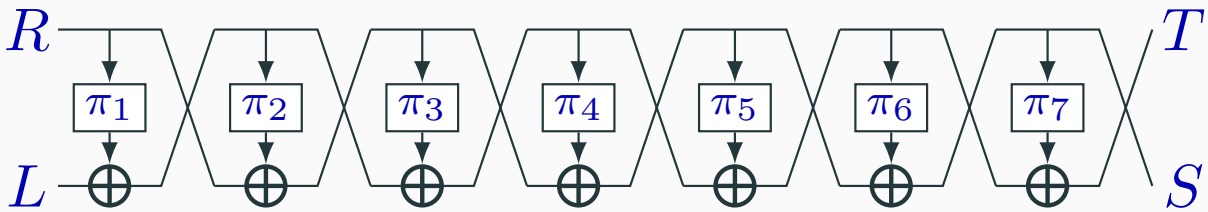
5/7-rounds pLR is optimally secure PRP/SPRP



5/7-rounds pLR is optimally secure PRP/SPRP



n-bit secure PRP: 5-pLR.



n-bit secure SPRP: 7-pLR.

Future Directions

Future Directions

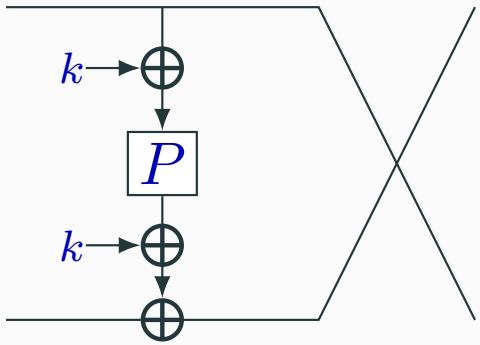
- minimal number of blockcipher calls for optimally secure (T)PRP.

In this work:

- PRP: 5 calls, SPRP: 7 calls
- TPRP: 7 calls, TSPRP: 11 calls

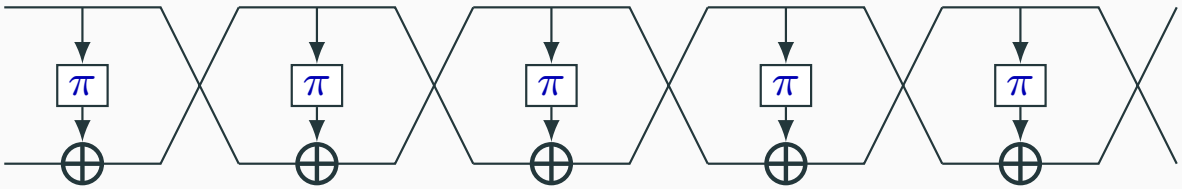
Future Directions

- Luby-Rackoff with public-permutation-based key-alternating ciphers.



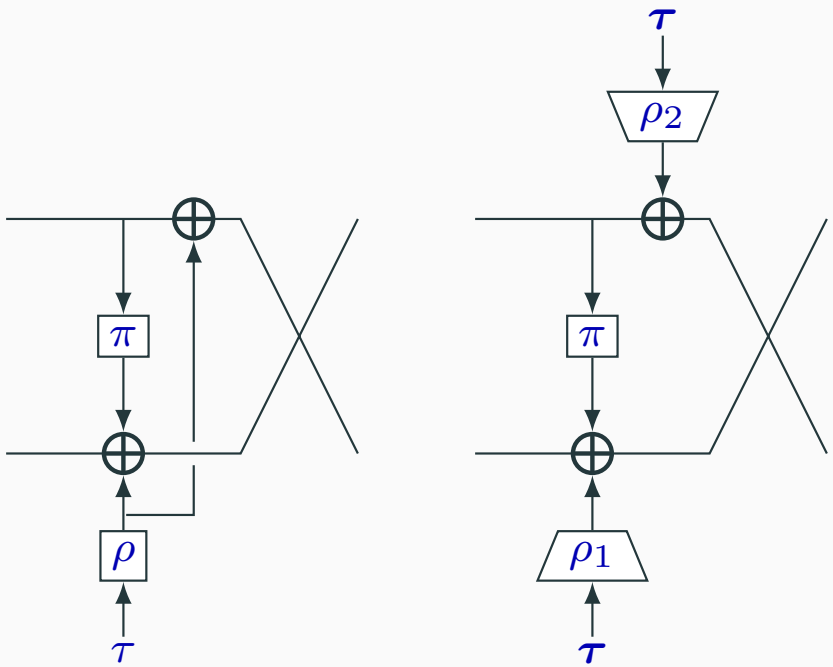
Future Directions

- single-keyed version of our candidates.



Future Directions

- optimizing TLR-compatible constructions.



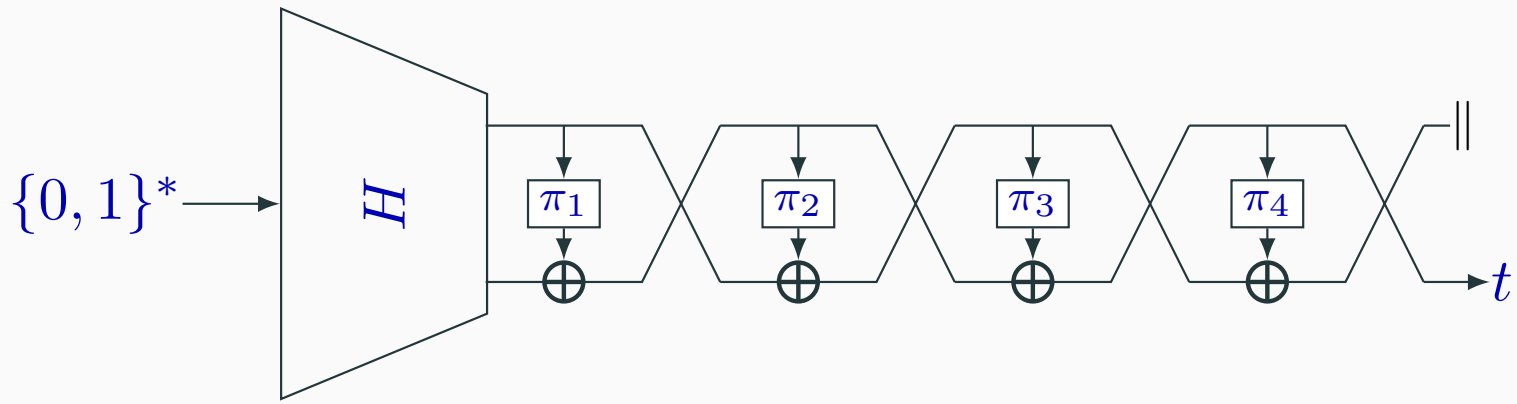
Future Directions

- minimal number of blockcipher calls for optimally secure (T)PRP.
- Luby-Rackoff with public-permutation-based key-alternating ciphers.
- single-keyed version of our candidates.
- optimizing TLR-compatible constructions.

ePrint paper

Check out the extended version at ia.cr/2025/914

Additional consequences: Optimally-secure MAC construction from pLR: DbHtF MAC family.



Thank You!