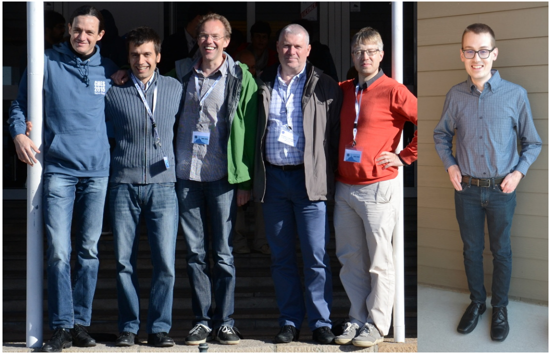
A Modular Approach to the Security Analysis of Two-Permutation Constructions

Yu Long Chen

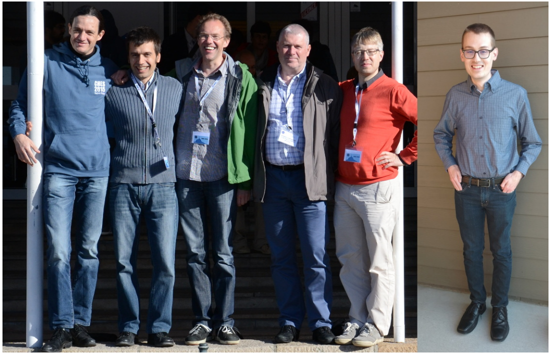
December 7, 2022

SHA-3 and Permutations



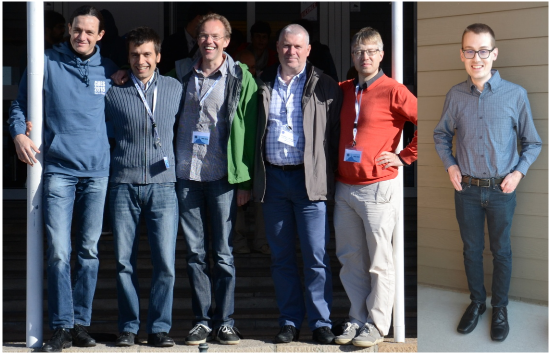
- Announced of SHA-3 competition in 2007

SHA-3 and Permutations



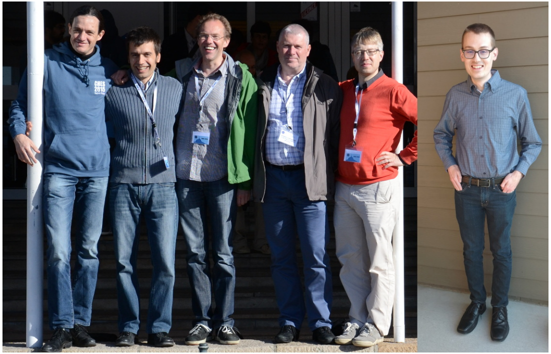
- Announced of SHA-3 competition in 2007
- Keccak was selected as the winner in 2012

SHA-3 and Permutations



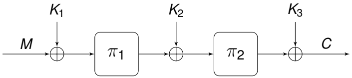
- Announced of SHA-3 competition in 2007
- Keccak was selected as the winner in 2012
- Keccak is permutation based hash function

SHA-3 and Permutations



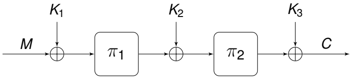
- Announced of SHA-3 competition in 2007
- Keccak was selected as the winner in 2012
- Keccak is permutation based hash function
- Popularization of public permutation based constructions

Two-Calls Permutation-Based Constructions

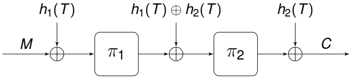


block cipher

Two-Calls Permutation-Based Constructions

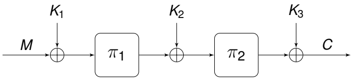


block cipher

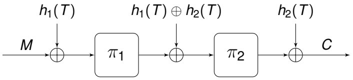


tweakable block cipher

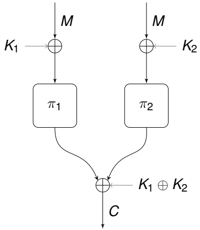
Two-Calls Permutation-Based Constructions



block cipher

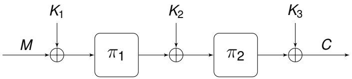


tweakable block cipher

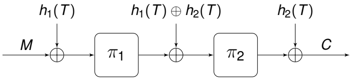


PRF

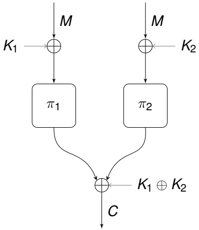
Two-Calls Permutation-Based Constructions



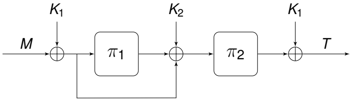
block cipher



tweakable block cipher

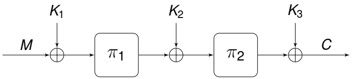


PRF

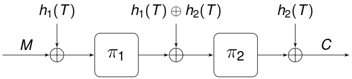


PRF

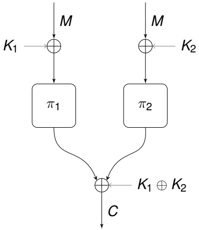
Two-Calls Permutation-Based Constructions



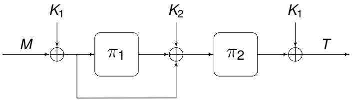
block cipher



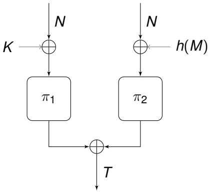
tweakable block cipher



PRF

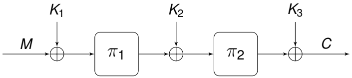


PRF

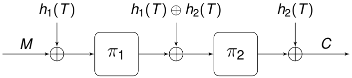


MAC algorithm

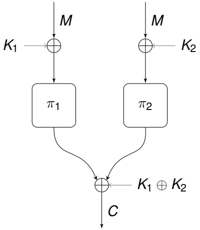
Two-Calls Permutation-Based Constructions



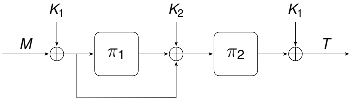
block cipher



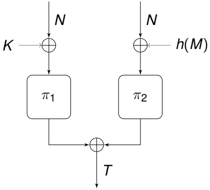
tweakable block cipher



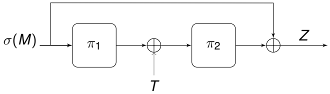
PRF



PRF



MAC algorithm



tccr hash function

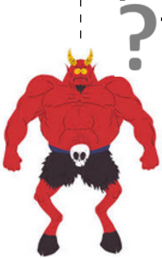
Generic Single-User Security

Our construction $\mathcal{O}$

$\pi_1, \ldots, \pi_r$

Ideal random construction $\mathcal{P}$

$\pi_1, \ldots, \pi_r$



attacker $\mathcal{A}$

- Attacker $\mathcal{A}$ makes q queries to construction oracle ($\mathcal{O}$ or $\mathcal{P}$)

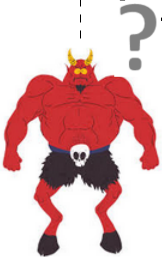
Generic Single-User Security

Our construction $\mathcal{O}$

$\pi_1, \ldots, \pi_r$

Ideal random construction $\mathcal{P}$

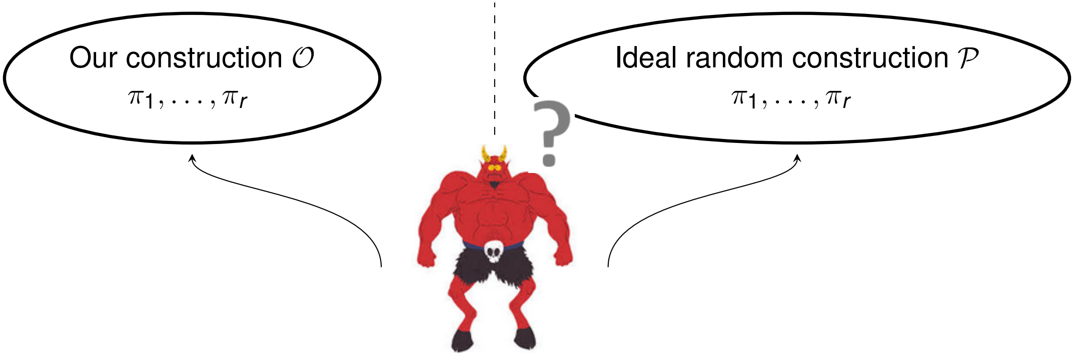
$\pi_1, \ldots, \pi_r$



attacker $\mathcal{A}$

- Attacker $\mathcal{A}$ makes q queries to construction oracle ($\mathcal{O}$ or $\mathcal{P}$)
- Attacker $\mathcal{A}$ makes p queries to each of primitive oracles ($\pi_1, \ldots, \pi_r$)

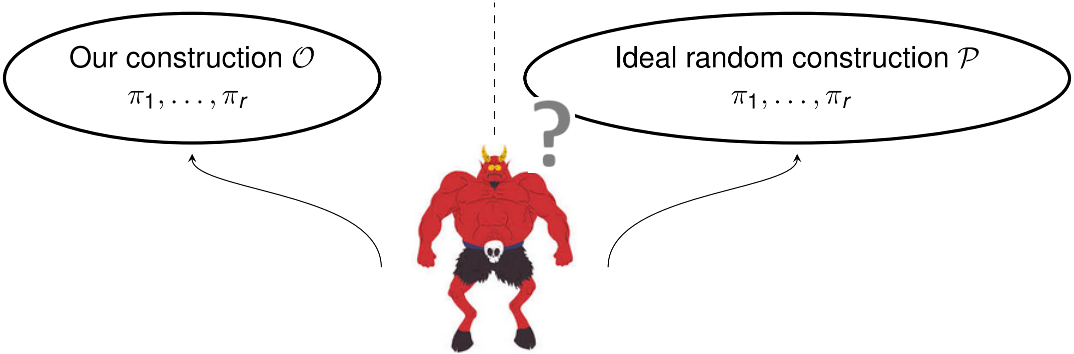
Generic Single-User Security



attacker $\mathcal{A}$

- Attacker $\mathcal{A}$ makes q queries to construction oracle ($\mathcal{O}$ or $\mathcal{P}$)
- Attacker $\mathcal{A}$ makes p queries to each of primitive oracles ($\pi_1, \ldots, \pi_r$)
- Security measured as probability of distinguishing two oracles: $\mathbf{Adv}^{\mathrm{su}}_{\mathcal{O}}(\mathcal{A}) = \text{func(q,p)}$

Generic Single-User Security



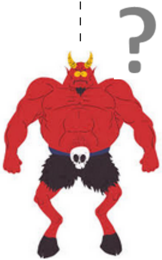
attacker $\mathcal{A}$

- Attacker $\mathcal{A}$ makes q queries to construction oracle ($\mathcal{O}$ or $\mathcal{P}$)
- Attacker $\mathcal{A}$ makes p queries to each of primitive oracles $(\pi_1, \ldots, \pi_r)$
- Security measured as probability of distinguishing two oracles: $\mathbf{Adv}^{\mathrm{su}}_{\mathcal{O}}(\mathcal{A}) = \mathrm{func(q,p)}$
- $\mathcal{O}$ is secure $\Longleftrightarrow$ $\mathbf{Adv}^{\mathrm{su}}_{\mathcal{O}}(\mathcal{A})$ is negligible

Generic Multi-User Security

$\mathcal{O}_{K_1}, \ldots, \mathcal{O}_{K_u}$
$\pi_1, \ldots, \pi_r$

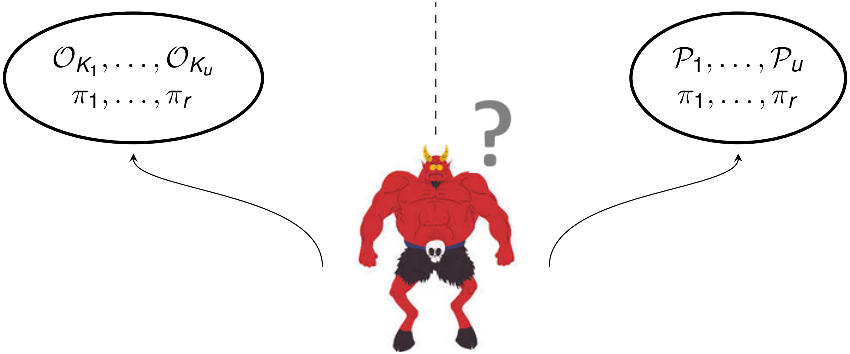
$\mathcal{P}_1, \ldots, \mathcal{P}_u$
$\pi_1, \ldots, \pi_r$



attacker $\mathcal{A}$

- Attacker $\mathcal{A}$ makes q queries to u construction oracles ($\mathcal{O}_{K_1}, \ldots, \mathcal{O}_{K_u}$ or $\mathcal{P}_1, \ldots, \mathcal{P}_u$)

Generic Multi-User Security



attacker $\mathcal{A}$

- Attacker $\mathcal{A}$ makes q queries to u construction oracles ($\mathcal{O}_{K_1}, \ldots, \mathcal{O}_{K_u}$ or $\mathcal{P}_1, \ldots, \mathcal{P}_u$)
- Attacker $\mathcal{A}$ makes p queries to each of primitive oracles ($\pi_1, \ldots, \pi_r$)

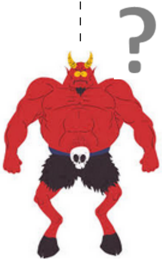
Generic Multi-User Security

$\mathcal{O}_{K_1}, \ldots, \mathcal{O}_{K_u}$

$\pi_1, \ldots, \pi_r$

$\mathcal{P}_1, \ldots, \mathcal{P}_u$

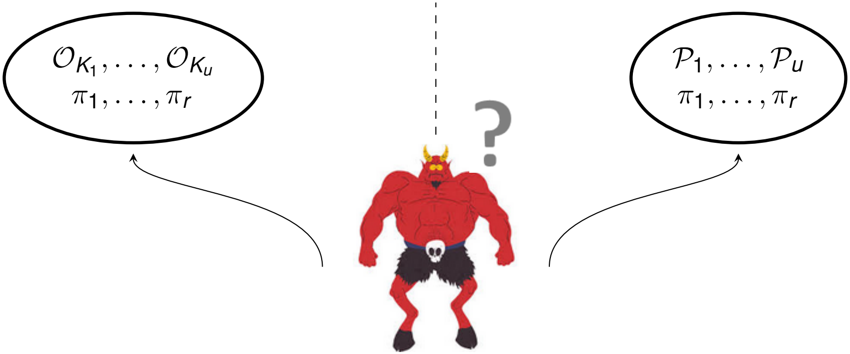
$\pi_1, \ldots, \pi_r$



attacker $\mathcal{A}$

- Attacker $\mathcal{A}$ makes q queries to u construction oracles ($\mathcal{O}_{K_1}, \ldots, \mathcal{O}_{K_u}$ or $\mathcal{P}_1, \ldots, \mathcal{P}_u$)
- Attacker $\mathcal{A}$ makes p queries to each of primitive oracles ($\pi_1, \ldots, \pi_r$)
- Attacker $\mathcal{A}$ succeed as long as it can compromise one user key K_i

Generic Multi-User Security



attacker $\mathcal{A}$

- Attacker $\mathcal{A}$ makes q queries to u construction oracles ($\mathcal{O}_{K_1}, \ldots, \mathcal{O}_{K_u}$ or $\mathcal{P}_1, \ldots, \mathcal{P}_u$)
- Attacker $\mathcal{A}$ makes p queries to each of primitive oracles ($\pi_1, \ldots, \pi_r$)
- Attacker $\mathcal{A}$ succeed as long as it can compromise one user key K_i
- Naive hybrid argument $\mathbf{Adv}^{\mathrm{mu}}_{\mathcal{O}}(\mathcal{A}) = u \cdot \mathbf{Adv}^{\mathrm{su}}_{\mathcal{O}}(\mathcal{A})$

Patarin's H-coefficient Technique

$$\frac{\Pr(X_{\mathcal{O}} = \tau)}{\Pr(X_{\mathcal{P}} = \tau)} \geq 1 - \epsilon$$

$$\mathbf{Adv}(\mathcal{A}) \leq \epsilon + \Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$$

Patarin's H-coefficient Technique

$$\frac{\Pr(X_{\mathcal{O}} = \tau)}{\Pr(X_{\mathcal{P}} = \tau)} \geq 1 - \epsilon$$

$$\mathbf{Adv}(\mathcal{A}) \leq \epsilon + \Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$$

1. $\mathcal{T}_{\text{bad}}$: depends on the construction

Patarin's H-coefficient Technique

$$\frac{\Pr(X_{\mathcal{O}} = \tau)}{\Pr(X_{\mathcal{P}} = \tau)} \geq 1 - \epsilon$$

$$\mathbf{Adv}(\mathcal{A}) \leq \epsilon + \Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$$

1. $\mathcal{T}_{\text{bad}}$: depends on the construction
2. $\Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$: combinatorial problem and relies on the randomness of the keys

Patarin's H-coefficient Technique

$$\frac{\Pr(X_{\mathcal{O}} = \tau)}{\Pr(X_{\mathcal{P}} = \tau)} \geq 1 - \epsilon$$

$$\textbf{Adv}(\mathcal{A}) \leq \epsilon + \Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$$

1. $\mathcal{T}_{\text{bad}}$: depends on the construction
2. $\Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$: combinatorial problem and relies on the randomness of the keys
3. ϵ: depends on the construction

Patarin's H-coefficient Technique

$$\frac{\Pr(X_{\mathcal{O}} = \tau)}{\Pr(X_{\mathcal{P}} = \tau)} \geq 1 - \epsilon$$

$$\mathbf{Adv}(\mathcal{A}) \leq \epsilon + \Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$$

1. $\mathcal{T}_{\text{bad}}$: depends on the construction
2. $\Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$: combinatorial problem and relies on the randomness of the keys
3. ϵ: depends on the construction

Modular approach for Item 1 and Item 3?

System of Equations And Non-Equations

- Two sets of unknown $\mathcal{V} = \{v_1, \ldots, v_{q_V}\}$ and $\mathcal{Y} = \{y_1, \ldots, y_{q_Y}\}$

System of Equations And Non-Equations

- Two sets of unknown $\mathcal{V} = \{v_1, \ldots, v_{q_V}\}$ and $\mathcal{Y} = \{y_1, \ldots, y_{q_Y}\}$
- A system of equations and a system of non-equations

$$\mathcal{E}_m = \begin{cases} v_{I_1} \oplus y_{I_1} = \lambda_1, \\ \vdots \\ v_{I_{qm}} \oplus y_{I_{qm}} = \lambda_{qm}, \end{cases} \qquad \mathcal{E}_a = \begin{cases} v'_{J_1} \oplus y'_{J_1} \neq \lambda'_1, \\ \vdots \\ v'_{J_{qa}} \oplus y'_{J_{qa}} \neq \lambda'_{qa}, \end{cases}$$

with $\lambda_1, \ldots, \lambda_{qm}$ and $\lambda'_1, \ldots, \lambda'_{qa}$ knowns values

System of Equations And Non-Equations

- Two sets of unknown $\mathcal{V} = \{v_1, \ldots, v_{q_V}\}$ and $\mathcal{Y} = \{y_1, \ldots, y_{q_Y}\}$
- A system of equations and a system of non-equations

$$\mathcal{E}_m = \begin{cases} v_{I_1} \oplus y_{I_1} = \lambda_1, \\ \vdots \\ v_{I_{qm}} \oplus y_{I_{qm}} = \lambda_{qm}, \end{cases} \qquad \mathcal{E}_a = \begin{cases} v'_{J_1} \oplus y'_{J_1} \neq \lambda'_1, \\ \vdots \\ v'_{J_{qa}} \oplus y'_{J_{qa}} \neq \lambda'_{qa}, \end{cases}$$

  with $\lambda_1, \ldots, \lambda_{qm}$ and $\lambda'_1, \ldots, \lambda'_{qa}$ knowns values
- Two surjective index mappings:

$$\varphi_V : \{I_1, \ldots, I_{qm}, J_1, \ldots, J_{qa}\} \to \{1, \ldots, q_V\},$$
$$\varphi_Y : \{I_1, \ldots, I_{qm}, J_1, \ldots, J_{qa}\} \to \{1, \ldots, q_Y\},$$

System of Equations And Non-Equations

- Two sets of unknown $\mathcal{V} = \{v_1, \ldots, v_{q_V}\}$ and $\mathcal{Y} = \{y_1, \ldots, y_{q_Y}\}$
- A system of equations and a system of non-equations

$$\mathcal{E}_m = \begin{cases} v_{I_1} \oplus y_{I_1} = \lambda_1, \\ \vdots \\ v_{I_{qm}} \oplus y_{I_{qm}} = \lambda_{qm}, \end{cases} \qquad \mathcal{E}_a = \begin{cases} v'_{J_1} \oplus y'_{J_1} \neq \lambda'_1, \\ \vdots \\ v'_{J_{qa}} \oplus y'_{J_{qa}} \neq \lambda'_{qa}, \end{cases}$$

with $\lambda_1, \ldots, \lambda_{qm}$ and $\lambda'_1, \ldots, \lambda'_{qa}$ knowns values

- Two surjective index mappings:

$$\varphi_V : \{I_1, \ldots, I_{qm}, J_1, \ldots, J_{qa}\} \to \{1, \ldots, q_V\},$$
$$\varphi_Y : \{I_1, \ldots, I_{qm}, J_1, \ldots, J_{qa}\} \to \{1, \ldots, q_Y\},$$

- Our goal is to give a lower bound on the number of solutions of these systems

Patarin's Mirror Theory

- Represents the system of equations and non-equations by a graph

Patarin's Mirror Theory

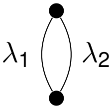
- Represents the system of equations and non-equations by a graph
  - A distinct unknown $\rightarrow$ a vertex with unknown value
  - An equation $\rightarrow$ a λ-labeled edge (normal)
  - A non-equation $\rightarrow$ a λ'-labeled edge (dashed)

Patarin's Mirror Theory

- Represents the system of equations and non-equations by a graph
  - A distinct unknown $\rightarrow$ a vertex with unknown value
  - An equation $\rightarrow$ a λ-labeled edge (normal)
  - A non-equation $\rightarrow$ a λ'-labeled edge (dashed)
- Transcript graph should be

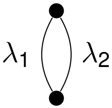
Patarin's Mirror Theory

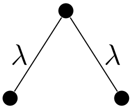
- Represents the system of equations and non-equations by a graph
  - A distinct unknown $\rightarrow$ a vertex with unknown value
  - An equation $\rightarrow$ a λ-labeled edge (normal)
  - A non-equation $\rightarrow$ a λ'-labeled edge (dashed)
- Transcript graph should be
  - acyclic



Patarin's Mirror Theory

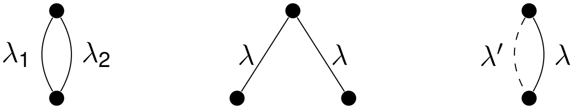
- Represents the system of equations and non-equations by a graph
  - A distinct unknown $\rightarrow$ a vertex with unknown value
  - An equation $\rightarrow$ a λ-labeled edge (normal)
  - A non-equation $\rightarrow$ a λ'-labeled edge (dashed)
- Transcript graph should be
  - acyclic
  - non-zero path label





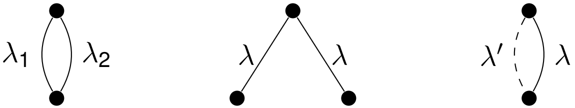
Patarin's Mirror Theory

- Represents the system of equations and non-equations by a graph
  - A distinct unknown $\rightarrow$ a vertex with unknown value
  - An equation $\rightarrow$ a λ-labeled edge (normal)
  - A non-equation $\rightarrow$ a λ'-labeled edge (dashed)
- Transcript graph should be
  - acyclic
  - non-zero path label
  - no cycles with a λ'-labeled edge such that: λ' = sum of the λ-labels



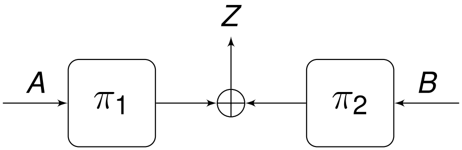
Patarin's Mirror Theory

- Represents the system of equations and non-equations by a graph
  - A distinct unknown $\rightarrow$ a vertex with unknown value
  - An equation $\rightarrow$ a λ-labeled edge (normal)
  - A non-equation $\rightarrow$ a λ'-labeled edge (dashed)
- Transcript graph should be
  - acyclic
  - non-zero path label
  - no cycles with a λ'-labeled edge such that: λ' = sum of the λ-labels
  - these properties define the bad transcripts



Two-Permutation Calls Constructions

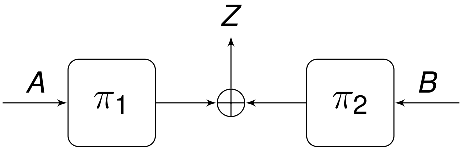
Focus on all constructions that can be viewed as:



A, B, and Z are functions of the secret key, the inputs, and the outputs

Two-Permutation Calls Constructions

Focus on all constructions that can be viewed as:

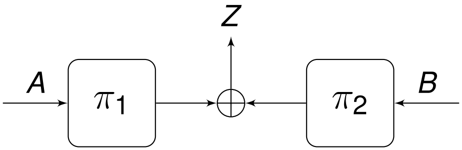


A, B, and Z are functions of the secret key, the inputs, and the outputs

- Security analysis in ideal permutation model

Two-Permutation Calls Constructions

Focus on all constructions that can be viewed as:

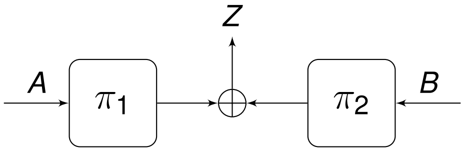


A, B, and Z are functions of the secret key, the inputs, and the outputs

- Security analysis in ideal permutation model
- Query access to the underlying primitives (modeled as random)

Two-Permutation Calls Constructions

Focus on all constructions that can be viewed as:



A, B, and Z are functions of the secret key, the inputs, and the outputs

- Security analysis in ideal permutation model
- Query access to the underlying primitives (modeled as random)
- Primitive queries in the form $\pi_1(u) = v$ and $\pi_2(x) = y$

Include Primitive Queries in The System

$$\mathcal{E}_m^p = \begin{cases} v_{I_1} \oplus y_{I_1} = \lambda_1, \\ \vdots \\ v_{I_{q_m}} \oplus y_{I_{q_m}} = \lambda_{q_m}, \\ v_{I_{q_m+1}} = \lambda_{q_m+1}, \\ \vdots \\ v_{I_{q_m+p}} = \lambda_{q_m+p}, \\ y_{I_{q_m+1}} = \lambda_{q_m+p+1}, \\ \vdots \\ y_{I_{q_m+p}} = \lambda_{q_m+2p}. \end{cases} \qquad \mathcal{E}_a = \begin{cases} v'_{J_1} \oplus y'_{J_1} \neq \lambda'_1, \\ \vdots \\ v'_{J_{q_a}} \oplus y'_{J_{q_a}} \neq \lambda'_{q_a}, \end{cases}$$

Include Primitive Queries in The System

$$\mathcal{E}_m^p = \begin{cases} v_{I_1} \oplus y_{I_1} = \lambda_1, \\ \vdots \\ v_{I_{qm}} \oplus y_{I_{qm}} = \lambda_{qm}, \\ v_{I_{qm+1}} = \lambda_{qm+1}, \\ \vdots \\ v_{I_{qm+p}} = \lambda_{qm+p}, \\ y_{I_{qm+1}} = \lambda_{qm+p+1}, \\ \vdots \\ y_{I_{qm+p}} = \lambda_{qm+2p}. \end{cases} \qquad \mathcal{E}_a = \begin{cases} v'_{J_1} \oplus y'_{J_1} \neq \lambda'_1, \\ \vdots \\ v'_{J_{qa}} \oplus y'_{J_{qa}} \neq \lambda'_{qa}, \end{cases}$$

- Two surjective index mappings:

$$\varphi_V^p \colon \{I_1, \ldots, I_{qm+p}, J_1, \ldots, J_{qa}\} \to \{1, \ldots, q_V\},$$
$$\varphi_Y^p \colon \{I_1, \ldots, I_{qm+p}, J_1, \ldots, J_{qa}\} \to \{1, \ldots, q_Y\},$$

Patarin's Mirror Theory For Permutation-Based Construction

- Represents the system of equations and non-equations by a graph
  - A distinct unknown $\rightarrow$ a vertex with unknown value (black)
  - An equation $\rightarrow$ a λ-labeled edge (normal)
  - A non-equation $\rightarrow$ a λ'-labeled edge (dashed)

Patarin's Mirror Theory For Permutation-Based Construction

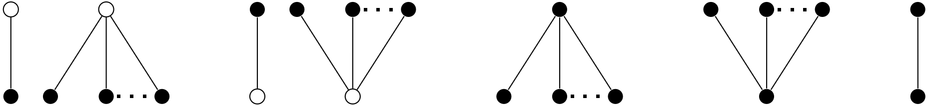
- Represents the system of equations and non-equations by a graph
  - A distinct unknown $\rightarrow$ a vertex with unknown value (black)
  - An equation $\rightarrow$ a λ-labeled edge (normal)
  - A non-equation $\rightarrow$ a λ'-labeled edge (dashed)
  - A primitive query $\rightarrow$ a vertex with known value (white)

Patarin's Mirror Theory For Permutation-Based Construction

- Represents the system of equations and non-equations by a graph
  - A distinct unknown $\rightarrow$ a vertex with unknown value (black)
  - An equation $\rightarrow$ a λ-labeled edge (normal)
  - A non-equation $\rightarrow$ a λ'-labeled edge (dashed)
  - A primitive query $\rightarrow$ a vertex with known value (white)
  - Colliding components: contains a vertex with known value $\rightarrow$ all vertices are defined

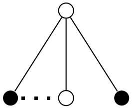
Patarin's Mirror Theory For Permutation-Based Construction

- Represents the system of equations and non-equations by a graph
  - A distinct unknown $\rightarrow$ a vertex with unknown value (black)
  - An equation $\rightarrow$ a λ-labeled edge (normal)
  - A non-equation $\rightarrow$ a λ'-labeled edge (dashed)
  - A primitive query $\rightarrow$ a vertex with known value (white)
  - Colliding components: contains a vertex with known value $\rightarrow$ all vertices are defined
- Simplified the analysis by avoiding components with path of length 3 or higher



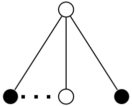
Inconsistency in Transcript Graph

- Each component contains at most one known vertex

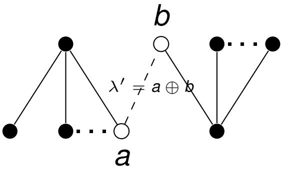


Inconsistency in Transcript Graph

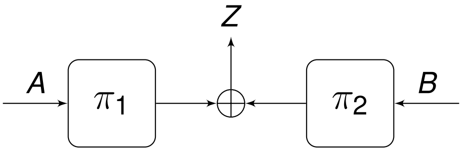
- Each component contains at most one known vertex



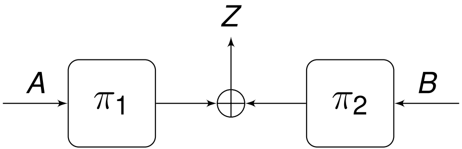
- No λ'-labeled edges that connect two colliding components such that the distance between the two connected vertices is λ'



Framework For Use

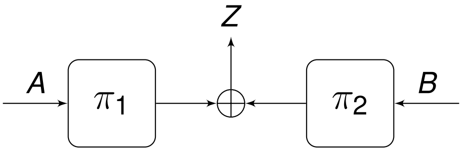


Framework For Use



- Query transcript $\tau = \{(A_1, B_1, Z_1), \ldots, (A_{q_m}, B_{q_m}, Z_{q_m}), \tau_{\pi_1}, \tau_{\pi_2}, K_1, \ldots, K_u\}$

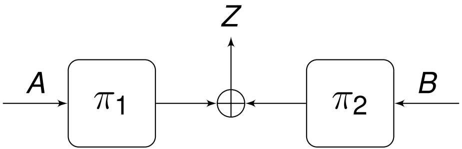
Framework For Use



- Query transcript $\tau = \{(A_1, B_1, Z_1), \ldots, (A_{q_m}, B_{q_m}, Z_{q_m}), \tau_{\pi_1}, \tau_{\pi_2}, K_1, \ldots, K_u\}$
- Each such algorithm consists of an evaluation of π_1 and an evaluation of π_2

$$\mathcal{E}_m^p = \begin{cases} \pi_1(A_1) \oplus \pi_2(B_1) = Z_1, \\ \vdots \\ \pi_1(A_{q_m}) \oplus \pi_2(B_{q_m}) = Z_{q_m}, \\ \pi_1(u) = v \quad \text{for } (u, v) \in \tau_1, \\ \pi_2(x) = y \quad \text{for } (x, y) \in \tau_2, \end{cases} \quad \mathcal{E}_a = \begin{cases} \pi_1(A'_1) \oplus \pi_2(B'_1) \neq Z'_1, \\ \vdots \\ \pi_1(A'_{q_a}) \oplus \pi_2(B'_{q_a}) \neq Z'_{q_a}. \end{cases}$$

Framework For Use

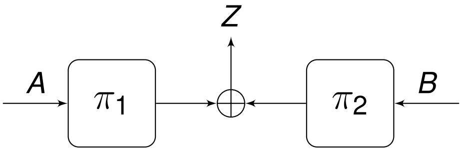


- Query transcript $\tau = \{(A_1, B_1, Z_1), \ldots, (A_{q_m}, B_{q_m}, Z_{q_m}), \tau_{\pi_1}, \tau_{\pi_2}, K_1, \ldots, K_u\}$
- Each such algorithm consists of an evaluation of π_1 and an evaluation of π_2

$$\mathcal{E}_m^p = \begin{cases} \pi_1(A_1) \oplus \pi_2(B_1) = Z_1, \\ \vdots \\ \pi_1(A_{q_m}) \oplus \pi_2(B_{q_m}) = Z_{q_m}, \\ \pi_1(u) = v \quad \text{for } (u, v) \in \tau_1, \\ \pi_2(x) = y \quad \text{for } (x, y) \in \tau_2, \end{cases} \quad \mathcal{E}_a = \begin{cases} \pi_1(A'_1) \oplus \pi_2(B'_1) \neq Z'_1, \\ \vdots \\ \pi_1(A'_{q_a}) \oplus \pi_2(B'_{q_a}) \neq Z'_{q_a}. \end{cases}$$

- Define $\mathcal{T}_{\mathrm{bad}}$ such that the graph is consistent

Framework For Use

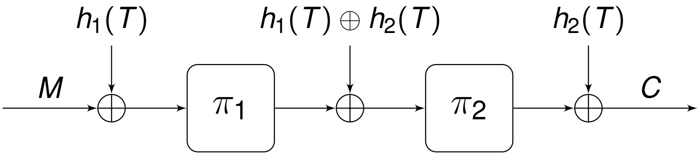


- Query transcript $\tau = \{(A_1, B_1, Z_1), \ldots, (A_{q_m}, B_{q_m}, Z_{q_m}), \tau_{\pi_1}, \tau_{\pi_2}, K_1, \ldots, K_u\}$
- Each such algorithm consists of an evaluation of π_1 and an evaluation of π_2

$$\mathcal{E}_m^p = \begin{cases} \pi_1(A_1) \oplus \pi_2(B_1) = Z_1, \\ \vdots \\ \pi_1(A_{q_m}) \oplus \pi_2(B_{q_m}) = Z_{q_m}, \\ \pi_1(u) = v \quad \text{for } (u, v) \in \tau_1, \\ \pi_2(x) = y \quad \text{for } (x, y) \in \tau_2, \end{cases} \quad \mathcal{E}_a = \begin{cases} \pi_1(A'_1) \oplus \pi_2(B'_1) \neq Z'_1, \\ \vdots \\ \pi_1(A'_{q_a}) \oplus \pi_2(B'_{q_a}) \neq Z'_{q_a}. \end{cases}$$

- Define $\mathcal{T}_{\mathrm{bad}}$ such that the graph is consistent
- Obtain ϵ using permutation-based mirror theory

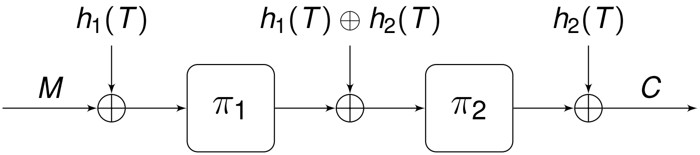
Application on Multi-User Security of TEM



Cogliati et al. 2015

$$\mathbf{Adv}^{\text{mu-tprp}} \leq qp^2/2^{2n} + q^3/2^{2n}$$

Application on Multi-User Security of TEM

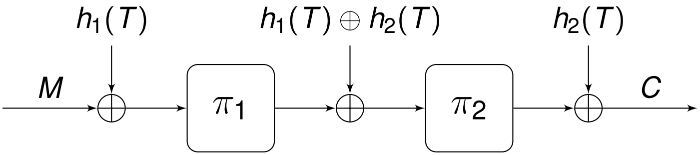


Cogliati et al. 2015

$$\mathbf{Adv}^{\text{mu-tprp}} \leq qp^2/2^{2n} + q^3/2^{2n}$$

- We consider TEM$[\pi_1, \pi_2^{-1}]$ instead of TEM$[\pi_1, \pi_2]$

Application on Multi-User Security of TEM

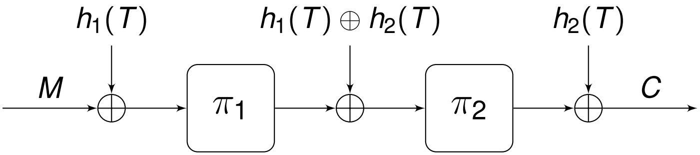


Cogliati et al. 2015

$$\mathbf{Adv}^{\text{mu-tprp}} \leq qp^2/2^{2n} + q^3/2^{2n}$$

- We consider TEM$[\pi_1, \pi_2^{-1}]$ instead of TEM$[\pi_1, \pi_2]$
- View the construction as the xor of two public permutations in the middle with $A = M \oplus h_1(T)$, $B = M \oplus h_2(T)$, and $Z = h_1(T) \oplus h_2(T)$

Application on Multi-User Security of TEM

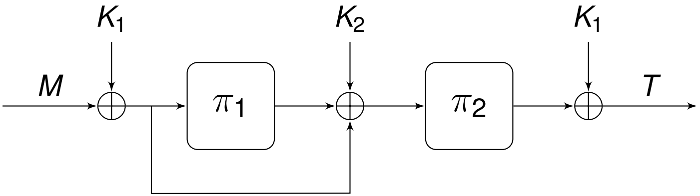


Cogliati et al. 2015

$$\mathbf{Adv}^{\text{mu-tprp}} \leq qp^2/2^{2n} + q^3/2^{2n}$$

- We consider TEM$[\pi_1, \pi_2^{-1}]$ instead of TEM$[\pi_1, \pi_2]$
- View the construction as the xor of two public permutations in the middle with $A = M \oplus h_1(T)$, $B = M \oplus h_2(T)$, and $Z = h_1(T) \oplus h_2(T)$
- Modular security analysis and obtain $2n/3$-bits security as the single-user case

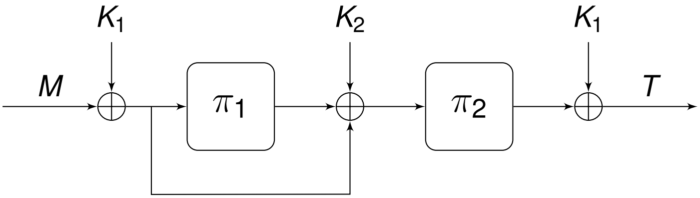
Application on Multi-User Security of EDM$_p$



Dutta et al. 2021

$$\mathbf{Adv}^{\text{mu-prf}} \leq qp^2/2^{2n} + q^3/2^{2n} + \binom{u}{2}/2^n$$

Application on Multi-User Security of EDM_p

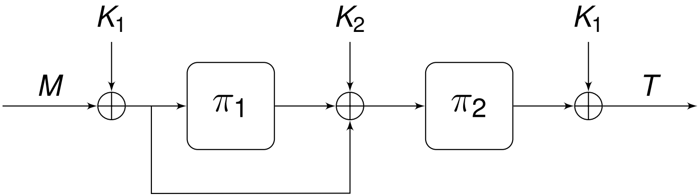


Dutta et al. 2021

$$\mathbf{Adv}^{\text{mu-prf}} \leq qp^2/2^{2n} + q^3/2^{2n} + \binom{u}{2}/2^n$$

- We consider $\mathrm{EDM}_p[\pi_1, \pi_2^{-1}]$ instead of $\mathrm{EDM}_p[\pi_1, \pi_2]$

Application on Multi-User Security of EDM_p

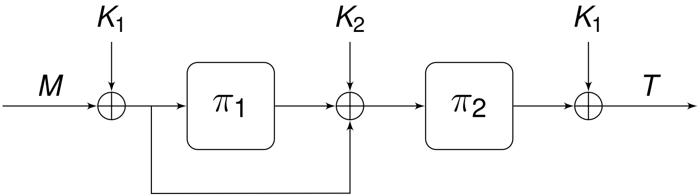


Dutta et al. 2021

$$\mathbf{Adv}^{\text{mu-prf}} \le qp^2/2^{2n} + q^3/2^{2n} + \binom{u}{2}/2^n$$

- We consider $\mathsf{EDM}_p[\pi_1, \pi_2^{-1}]$ instead of $\mathsf{EDM}_p[\pi_1, \pi_2]$
- View the construction as the xor of two public permutations in the middle with $A = M \oplus K_1$, $B = T \oplus K_1$, and $Z = M \oplus K_1 \oplus K_2$

Application on Multi-User Security of EDM_p

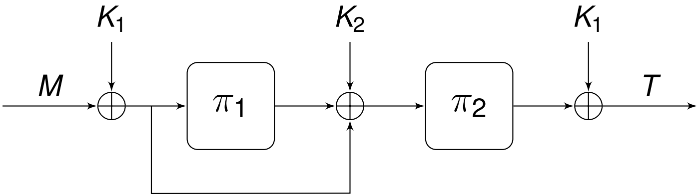


Dutta et al. 2021

$$\mathbf{Adv}^{\text{mu-prf}} \leq qp^2/2^{2n} + q^3/2^{2n} + \binom{u}{2}/2^n$$

- We consider $\mathrm{EDM}_p[\pi_1, \pi_2^{-1}]$ instead of $\mathrm{EDM}_p[\pi_1, \pi_2]$
- View the construction as the xor of two public permutations in the middle with $A = M \oplus K_1$, $B = T \oplus K_1$, and $Z = M \oplus K_1 \oplus K_2$
- Multi-user security analysis is more complex: inputs to π_1 do not need to be fresh

Application on Multi-User Security of EDM_p

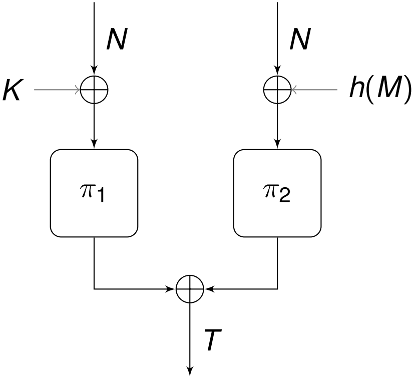


Dutta et al. 2021

$$\mathbf{Adv}^{\text{mu-prf}} \le qp^2/2^{2n} + q^3/2^{2n} + \binom{u}{2}/2^n$$

- We consider $\mathsf{EDM}_p[\pi_1, \pi_2^{-1}]$ instead of $\mathsf{EDM}_p[\pi_1, \pi_2]$
- View the construction as the xor of two public permutations in the middle with $A = M \oplus K_1$, $B = T \oplus K_1$, and $Z = M \oplus K_1 \oplus K_2$
- Multi-user security analysis is more complex: inputs to π_1 do not need to be fresh
- Modular security analysis and obtain $2n/3$-bits security as the single-user case

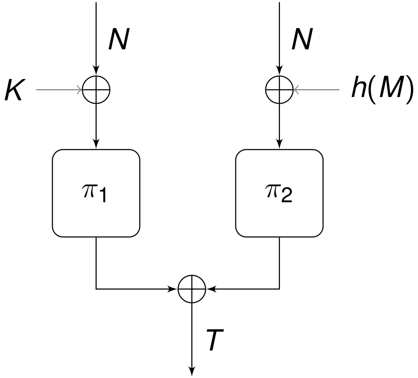
Application on Multi-User Security of nEHTM$_p$ (1)



Dutta and Nandi 2020

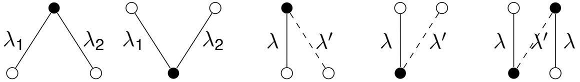
- Proved $2n/3$-bits security

Application on Multi-User Security of nEHTM$_p$ (1)

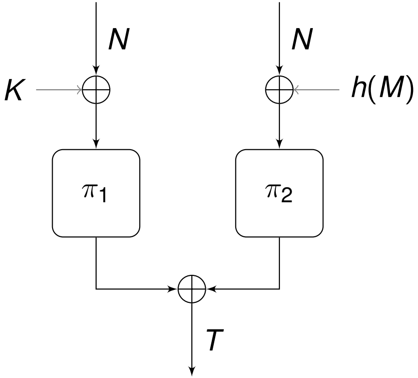


Dutta and Nandi 2020

- Proved $2n/3$-bits security
- Missing bad events in the original security analysis

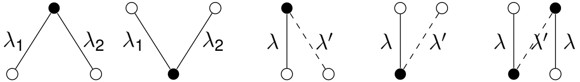


Application on Multi-User Security of nEHTM$_p$ (1)



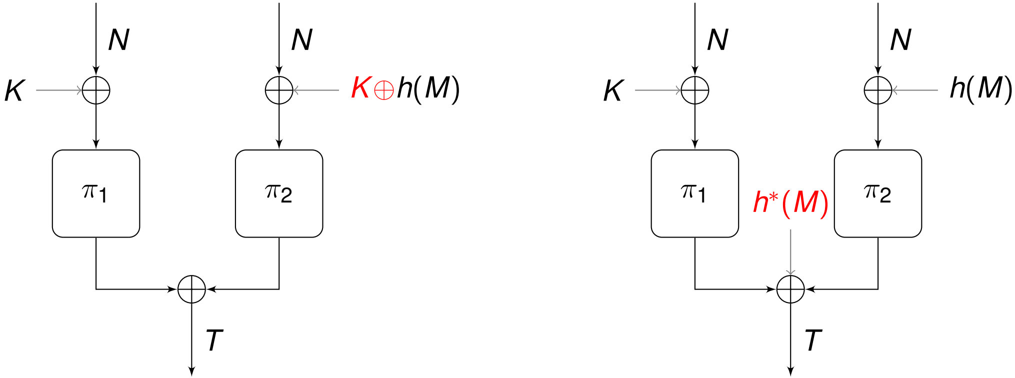
Dutta and Nandi 2020

- Proved $2n/3$-bits security
- Missing bad events in the original security analysis



- Good transcript ratio analysis is also incomplete

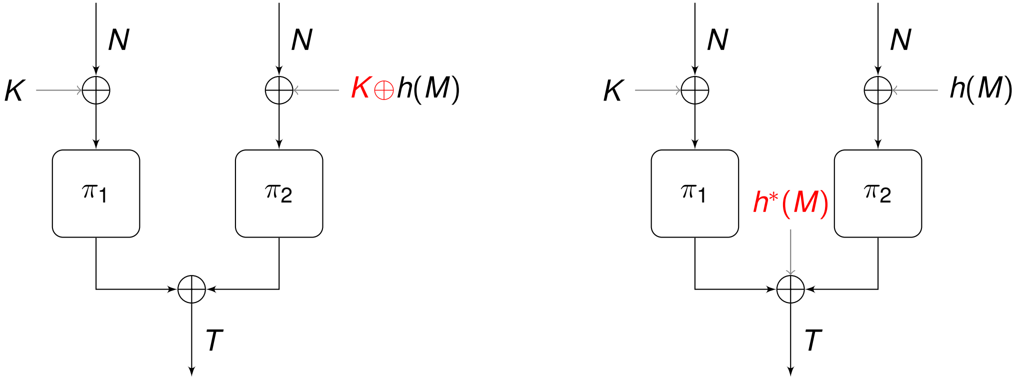
Application on Multi-User Security of nEHTM$_p$ (1)



$$\mathbf{Adv}^{\text{mu-mac}} \leq qp^2/2^{2n} + q^3/2^{2n} + \binom{u}{2}/2^n$$

- Solution by Chen, Dutta, Nandi (left)

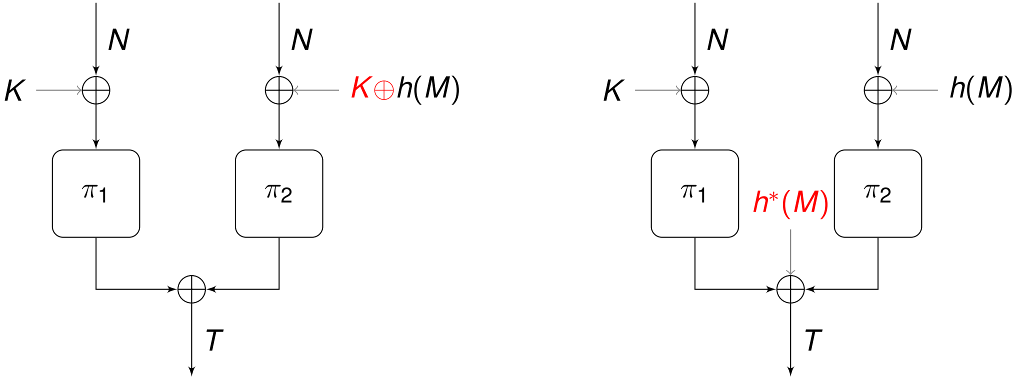
Application on Multi-User Security of nEHTM$_p$ (1)



$$\mathbf{Adv}^{\text{mu-mac}} \leq qp^2/2^{2n} + q^3/2^{2n} + \binom{u}{2}/2^n$$

- Solution by Chen, Dutta, Nandi (left)
- This work focus on modular approach: extra randomness h^* for simplicity (right)

Application on Multi-User Security of nEHTM$_p$ (1)



$$\mathbf{Adv}^{\text{mu-mac}} \le qp^2/2^{2n} + q^3/2^{2n} + \binom{u}{2}/2^n$$

- Solution by Chen, Dutta, Nandi (left)
- This work focus on modular approach: extra randomness h^* for simplicity (right)
- $A = N \oplus K$, $B = N \oplus h(M)$, and $Z = T \oplus h^*(M)$

Conclusion

New results

- Modular proof technique for permutation-based constructions based on mirror theory
- Framework to use this new technique
- Multi-user security of TEM, *p*EDM, and nEHtM$_p$

Conclusion

New results

- Modular proof technique for permutation-based constructions based on mirror theory
- Framework to use this new technique
- Multi-user security of TEM, pEDM, and nEHtM$_p$

Future research

- Design of deterministic MAC and AE schemes using our technique
- Modular approach for multi-user security of block cipher-based constructions
- Generalized modular proof techniques for more difficult constructions

Conclusion

New results

- Modular proof technique for permutation-based constructions based on mirror theory
- Framework to use this new technique
- Multi-user security of TEM, *p*EDM, and nEHtM_p

Future research

- Design of deterministic MAC and AE schemes using our technique
- Modular approach for multi-user security of block cipher-based constructions
- Generalized modular proof techniques for more difficult constructions

Thank you for your attention!