Mirror Theory: Proof Techniques and Applications

Abisshanka Saha

Eindhoven University of Technology, The Netherlands

a.saha1@tue.nl, sahaa.1993@gmail.com

Outline

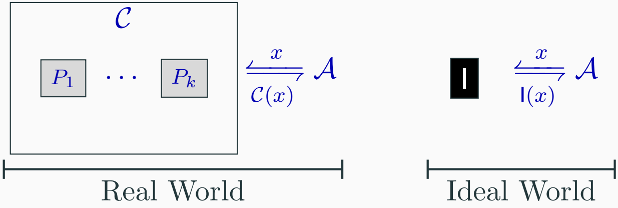
Provable Security using H-Coefficient Technique

Graphical representation of Bivariate Equations and Non-Equations

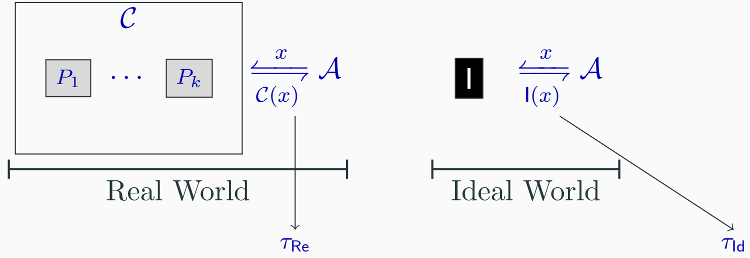
Different Variants of Mirror Theory

Provable Security using H-Coefficient Technique

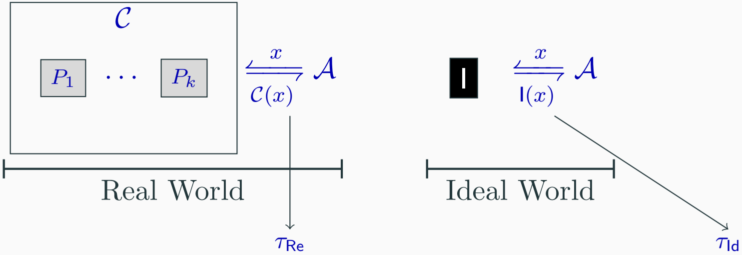
H-coefficient Technique



H-coefficient Technique



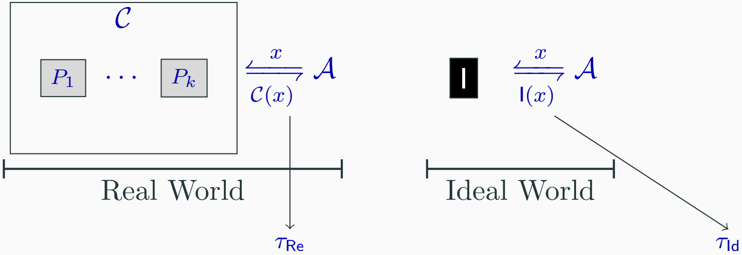
H-coefficient Technique



H-Coefficient Technique: For $\mathcal{T}_{\mathsf{good}} \subseteq \mathcal{T}_{\mathsf{Id}}$,

$$\Delta(\tau_{\mathsf{Id}}, \tau_{\mathsf{Re}}) \leq 1 - \frac{\Pr_{\mathsf{Re}}(\tau_{\mathsf{Re}} = \tau | \tau \in \mathcal{T}_{\mathsf{good}})}{\Pr_{\mathsf{Id}}(\tau_{\mathsf{Id}} = \tau | \tau \in \mathcal{T}_{\mathsf{good}})} + \Pr_{\mathsf{Id}}(\tau \notin \mathcal{T}_{\mathsf{good}})$$

H-coefficient Technique



H-Coefficient Technique: For $\mathcal{T}_{\mathsf{good}} \subseteq \mathcal{T}_{\mathsf{Id}}$,

$$\Delta(\tau_{\mathsf{Id}}, \tau_{\mathsf{Re}}) \leq 1 - \frac{\Pr_{\mathsf{Re}}(\tau_{\mathsf{Re}} = \tau | \tau \in \mathcal{T}_{\mathsf{good}})}{\Pr_{\mathsf{Id}}(\tau_{\mathsf{Id}} = \tau | \tau \in \mathcal{T}_{\mathsf{good}})} + \Pr_{\mathsf{Id}}(\tau \notin \mathcal{T}_{\mathsf{good}})$$

Need to count: $|\mathcal{T}_{\mathsf{Re}} \cap \mathcal{T}_{\mathsf{good}}|$.

System of Equations and Non-Equations from Transcripts

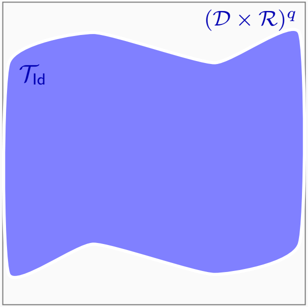
$\tau \in \mathcal{T}_{\mathsf{Re}} \cap \mathcal{T}_{\mathsf{good}}$ satisfies three kinds of restrictions:

$(\mathcal{D} \times \mathcal{R})^q$

System of Equations and Non-Equations from Transcripts

$\tau \in \mathcal{T}_{\mathsf{Re}} \cap \mathcal{T}_{\mathsf{good}}$ satisfies three kinds of restrictions:

Attainability restrictions

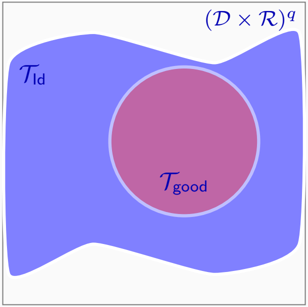


System of Equations and Non-Equations from Transcripts

$\tau \in \mathcal{T}_{\mathsf{Re}} \cap \mathcal{T}_{\mathsf{good}}$ satisfies three kinds of restrictions:

Attainability restrictions

$+$ Goodness restrictions



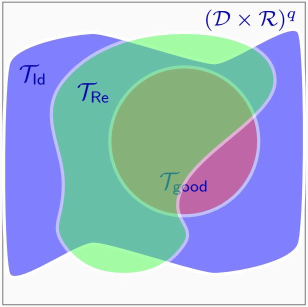
System of Equations and Non-Equations from Transcripts

$\tau \in \mathcal{T}_{\mathsf{Re}} \cap \mathcal{T}_{\mathsf{good}}$ satisfies three kinds of restrictions:

Attainability restrictions

$+$ Goodness restrictions

$+$ Real world-realizability restrictions



System of Equations and Non-Equations from Transcripts

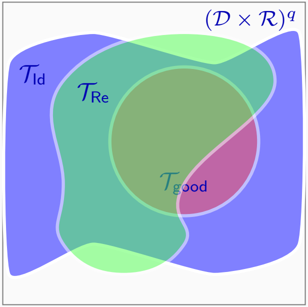
$\tau \in \mathcal{T}_{\mathsf{Re}} \cap \mathcal{T}_{\mathsf{good}}$ satisfies three kinds of restrictions:

Attainability restrictions

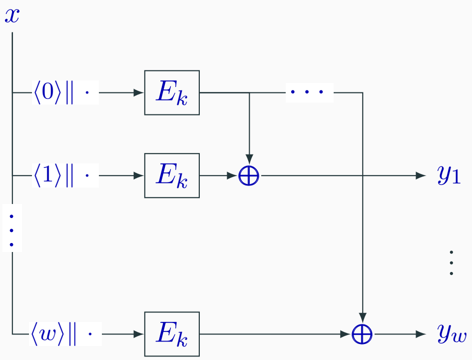
$+$ Goodness restrictions

$+$ Real world-realizability restrictions

Restrictions $\equiv$ System of **Equations** and **Non-Equations**,
where the **variables** are **outputs of the primitives** used in the construction.

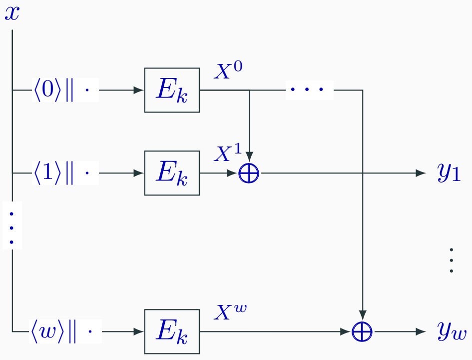


Example 1: XORP[w]



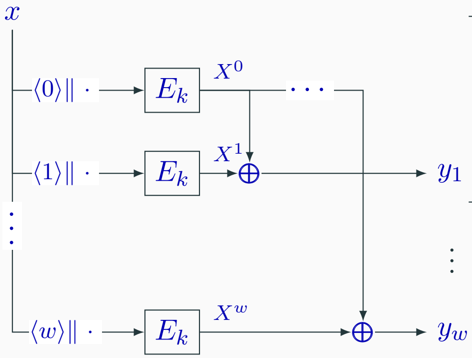
$$\tau = ((x_1, y_1), \cdots, (x_q, y_q))$$

Example 1: XORP[w]



$$\tau = ((x_1, y_1), \cdots, (x_q, y_q))$$

Example 1: XORP[w]



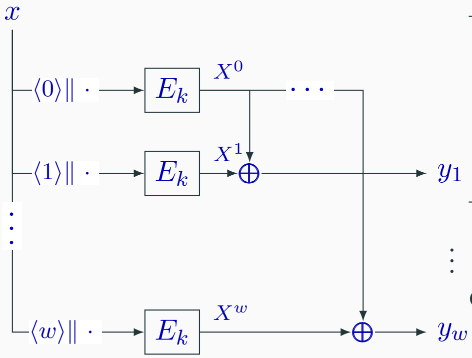
$$\tau = ((x_1, y_1), \cdots, (x_q, y_q))$$

Real World Realizability Restrictions:

Equations	
$X_i^0 \oplus X_i^1 = y_i^1$	
$\vdots$	$i \in [q]$
$X_i^0 \oplus X_i^w = y_i^w$	

Non-Equations
$X_i^j \oplus X_{i'}^{j'} \neq 0^n, \quad (i,j) \neq (i',j')$

Example 1: XORP[w]



$$\tau = ((x_1, y_1), \cdots, (x_q, y_q))$$

Real World Realizability Restrictions:

Equations	
$X_i^0 \oplus X_i^1 = y_i^1$	
$\vdots$	$i \in [q]$
$X_i^0 \oplus X_i^w = y_i^w$	

Non-Equations	
$X_i^j \oplus X_{i'}^{j'} \neq 0^n,$	$(i,j) \neq (i',j')$

Goodness Restrictions:

$y_i^j \neq 0^n \qquad (i,j) \in [q] \times [w]$

$y_i^j \neq y_i^{j'} \qquad i \in [q], j \neq j' \in [w]$

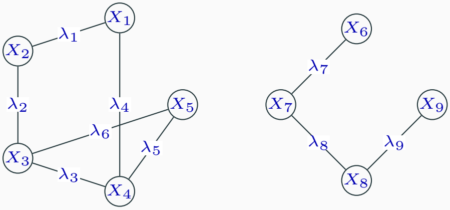
Graphical representation of Bivariate Equations and Non-Equations

System of Bivariate Affine Equations

$$\begin{array}{lll} X_1 \oplus X_2 = \lambda_1 & X_1 \oplus X_4 = \lambda_4 & X_6 \oplus X_7 = \lambda_7 \\ X_2 \oplus X_3 = \lambda_2 & X_4 \oplus X_5 = \lambda_5 & X_7 \oplus X_8 = \lambda_8 \\ X_3 \oplus X_4 = \lambda_3 & X_3 \oplus X_5 = \lambda_6 & X_8 \oplus X_9 = \lambda_9 \end{array}$$

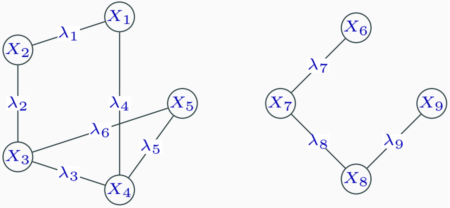
System of Bivariate Affine Equations

$$X_1 \oplus X_2 = \lambda_1 \quad X_1 \oplus X_4 = \lambda_4 \quad X_6 \oplus X_7 = \lambda_7$$
$$X_2 \oplus X_3 = \lambda_2 \quad X_4 \oplus X_5 = \lambda_5 \quad X_7 \oplus X_8 = \lambda_8$$
$$X_3 \oplus X_4 = \lambda_3 \quad X_3 \oplus X_5 = \lambda_6 \quad X_8 \oplus X_9 = \lambda_9$$



System of Bivariate Affine Equations

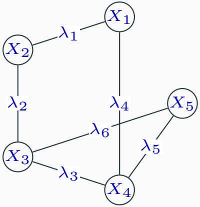
$$
\begin{array}{lll}
X_1 \oplus X_2 = \lambda_1 & X_1 \oplus X_4 = \lambda_4 & X_6 \oplus X_7 = \lambda_7 \\
X_2 \oplus X_3 = \lambda_2 & X_4 \oplus X_5 = \lambda_5 & X_7 \oplus X_8 = \lambda_8 \\
X_3 \oplus X_4 = \lambda_3 & X_3 \oplus X_5 = \lambda_6 & X_8 \oplus X_9 = \lambda_9
\end{array}
$$

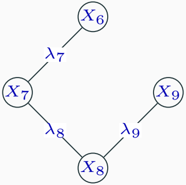


For having a solution, all cycles must have label sum zero.

System of Bivariate Affine Equations

$$\begin{array}{lll} X_1 \oplus X_2 = \lambda_1 & X_1 \oplus X_4 = \lambda_4 & X_6 \oplus X_7 = \lambda_7 \\ X_2 \oplus X_3 = \lambda_2 & X_4 \oplus X_5 = \lambda_5 & X_7 \oplus X_8 = \lambda_8 \\ X_3 \oplus X_4 = \lambda_3 & X_3 \oplus X_5 = \lambda_6 & X_8 \oplus X_9 = \lambda_9 \end{array}$$

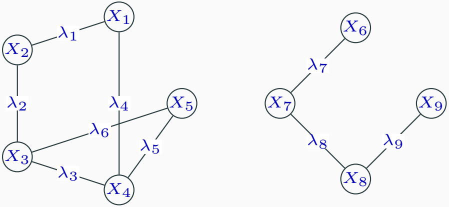




For having a solution, all cycles must have label sum zero.

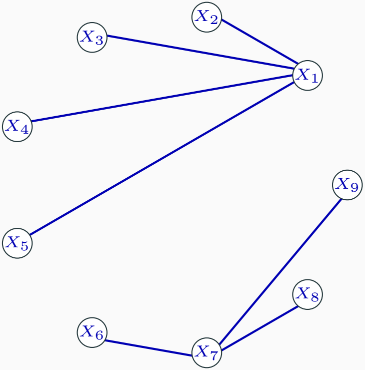
System of Bivariate Affine Equations

$$
\begin{array}{lll}
X_1 \oplus X_2 = \lambda_1 & X_1 \oplus X_4 = \lambda_4 & X_6 \oplus X_7 = \lambda_7 \\
X_2 \oplus X_3 = \lambda_2 & X_4 \oplus X_5 = \lambda_5 & X_7 \oplus X_8 = \lambda_8 \\
X_3 \oplus X_4 = \lambda_3 & X_3 \oplus X_5 = \lambda_6 & X_8 \oplus X_9 = \lambda_9
\end{array}
$$



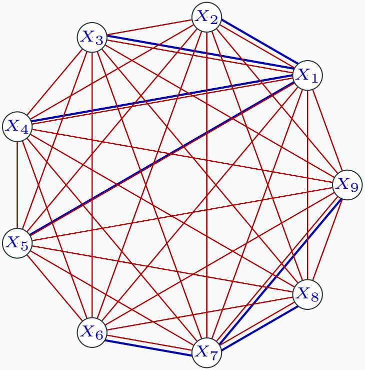
If we assign value to one variable the values of the all the variables in its component gets determined. $\xi_{\max} :=$ size of largest component

Adding Non-Equations



$$X_1 \oplus X_2 = \lambda'_1 \qquad X_7 \oplus X_6 = \lambda'_5$$
$$X_1 \oplus X_3 = \lambda'_2 \qquad X_7 \oplus X_8 = \lambda'_6$$
$$X_1 \oplus X_4 = \lambda'_3 \qquad X_7 \oplus X_9 = \lambda'_7$$
$$X_1 \oplus X_5 = \lambda'_4$$

Adding Non-Equations



$X_1 \oplus X_2 = \lambda'_1$ $\quad$ $X_7 \oplus X_6 = \lambda'_5$

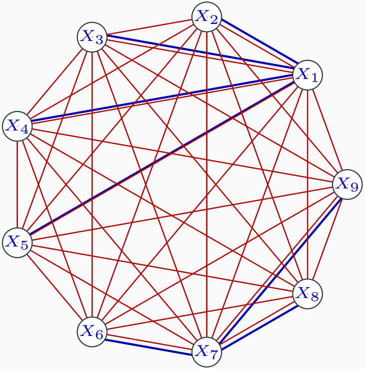
$X_1 \oplus X_3 = \lambda'_2$ $\quad$ $X_7 \oplus X_8 = \lambda'_6$

$X_1 \oplus X_4 = \lambda'_3$ $\quad$ $X_7 \oplus X_9 = \lambda'_7$

$X_1 \oplus X_5 = \lambda'_4$

$X_i \oplus X_j \neq 0^n \qquad i, j \in [9]$

Adding Non-Equations



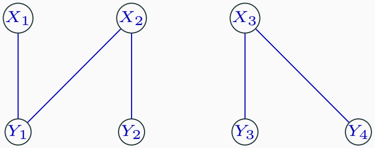
$$X_1 \oplus X_2 = \lambda'_1 \qquad X_7 \oplus X_6 = \lambda'_5$$
$$X_1 \oplus X_3 = \lambda'_2 \qquad X_7 \oplus X_8 = \lambda'_6$$
$$X_1 \oplus X_4 = \lambda'_3 \qquad X_7 \oplus X_9 = \lambda'_7$$
$$X_1 \oplus X_5 = \lambda'_4$$

$$X_i \oplus X_j \neq 0^n \qquad i, j \in [9]$$

No blue path has label sum 0^n

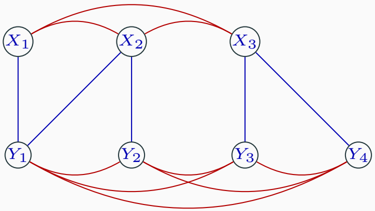
Complete Mirror Theory Problem (CMTP)

Adding Non-Equations



$$
\begin{aligned}
X_1 \oplus Y_1 &= \lambda_1 \qquad & X_3 \oplus Y_3 &= \lambda_4 \\
X_2 \oplus Y_1 &= \lambda_2 \qquad & X_3 \oplus Y_4 &= \lambda_5 \\
X_2 \oplus Y_2 &= \lambda_3
\end{aligned}
$$

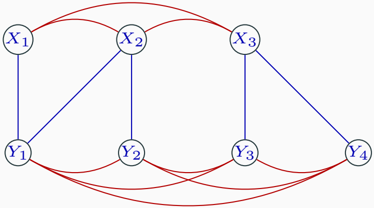
Adding Non-Equations



$$X_1 \oplus Y_1 = \lambda_1 \qquad X_3 \oplus Y_3 = \lambda_4$$
$$X_2 \oplus Y_1 = \lambda_2 \qquad X_3 \oplus Y_4 = \lambda_5$$
$$X_2 \oplus Y_2 = \lambda_3$$

$$X_i \oplus X_j \neq 0^n \qquad i, j \in [3]$$
$$Y_i \oplus Y_j \neq 0^n \qquad i, j \in [4]$$

Adding Non-Equations



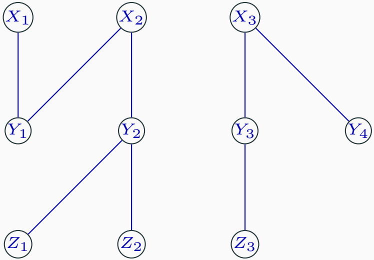
Biclique Mirror Theory Problem (BMTP)

$$X_1 \oplus Y_1 = \lambda_1 \qquad X_3 \oplus Y_3 = \lambda_4$$
$$X_2 \oplus Y_1 = \lambda_2 \qquad X_3 \oplus Y_4 = \lambda_5$$
$$X_2 \oplus Y_2 = \lambda_3$$

$$X_i \oplus X_j \neq 0^n \qquad i, j \in [3]$$
$$Y_i \oplus Y_j \neq 0^n \qquad i, j \in [4]$$

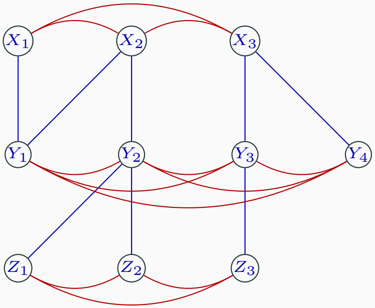
No even-length blue path has label sum 0^n

Adding Non-Equations



$$
\begin{array}{ll}
X_1 \oplus Y_1 = \lambda_1 & X_3 \oplus Y_3 = \lambda_4 \\
X_2 \oplus Y_1 = \lambda_2 & X_3 \oplus Y_4 = \lambda_5 \\
X_2 \oplus Y_2 = \lambda_3 & Y_2 \oplus Z_1 = \lambda_6 \\
Y_2 \oplus Z_2 = \lambda_7 & Y_3 \oplus Z_3 = \lambda_8
\end{array}
$$

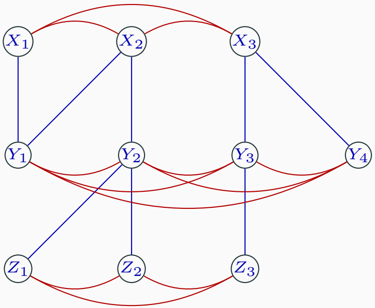
Adding Non-Equations



$$X_1 \oplus Y_1 = \lambda_1 \qquad X_3 \oplus Y_3 = \lambda_4$$
$$X_2 \oplus Y_1 = \lambda_2 \qquad X_3 \oplus Y_4 = \lambda_5$$
$$X_2 \oplus Y_2 = \lambda_3 \qquad Y_2 \oplus Z_1 = \lambda_6$$
$$Y_2 \oplus Z_2 = \lambda_7 \qquad Y_3 \oplus Z_3 = \lambda_8$$

$$X_i \oplus X_j \neq 0^n \qquad i, j \in [3]$$
$$Y_i \oplus Y_j \neq 0^n \qquad i, j \in [4]$$
$$Z_i \oplus Z_j \neq 0^n \qquad i, j \in [3]$$

Adding Non-Equations



$$X_1 \oplus Y_1 = \lambda_1 \qquad X_3 \oplus Y_3 = \lambda_4$$
$$X_2 \oplus Y_1 = \lambda_2 \qquad X_3 \oplus Y_4 = \lambda_5$$
$$X_2 \oplus Y_2 = \lambda_3 \qquad Y_2 \oplus Z_1 = \lambda_6$$
$$Y_2 \oplus Z_2 = \lambda_7 \qquad Y_3 \oplus Z_3 = \lambda_8$$

$$X_i \oplus X_j \neq 0^n \qquad i, j \in [3]$$
$$Y_i \oplus Y_j \neq 0^n \qquad i, j \in [4]$$
$$Z_i \oplus Z_j \neq 0^n \qquad i, j \in [3]$$

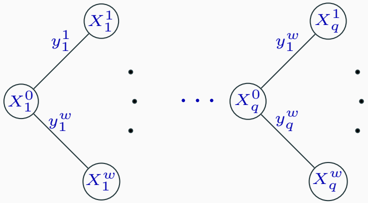
Triclique Mirror Theory Problem (TMTP)

Different Variants of Mirror Theory

Example 1: XORP[w] (contd.)

Equations	
$X_i^0 \oplus X_i^1 = y_i^1$	
$\vdots$	$i \in [q]$
$X_i^0 \oplus X_i^w = y_i^w$	

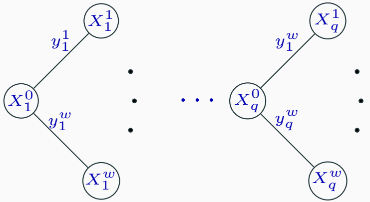
Non-Equations
$X_i^j \oplus X_{i'}^{j'} \neq 0^n, \quad (i,j) \neq (i',j')$



Example 1: XORP[w] (contd.)

Equations

$$\left.\begin{array}{c} X_i^0 \oplus X_i^1 = y_i^1 \\ \vdots \\ X_i^0 \oplus X_i^w = y_i^w \end{array}\right. \qquad i \in [q]$$



Non-Equations

$$X_i^j \oplus X_{i'}^{j'} \neq 0^n, \quad (i,j) \neq (i',j')$$

Goodness Restrictions:

$$y_i^j \neq 0^n \qquad (i,j) \in [q] \times [w]$$

$$y_i^j \neq y_i^{j'} \qquad i \in [q], j \neq j' \in [w]$$

$$\frac{\Pr_{\mathsf{Re}}(\tau_{\mathsf{Re}} = \tau)}{\Pr_{\mathsf{Id}}(\tau_{\mathsf{Id}} = \tau)} = \frac{\mathcal{N}/(2^n)_{(w+1)q}}{2^{nw}}$$

Complete Mirror Theory [CDNPS23]

Theorem

Consider a system of e *equations*
involving v *variables*
largest component size $= \xi_{\max}$.
If $\sqrt{N} \geq \xi_{\max}^2 \log_2 N + \xi_{\max}$, *and* $1 \leq v \leq N/12\xi_{\max}^2$, *then the number of solutions of the system of equations and complete set of non-equations is at least*

$$\frac{(2^n)_v}{2^{ne}}.$$

Complete Mirror Theory [CDNPS23]

Theorem

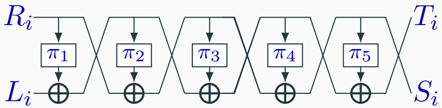
Consider a system of e *equations*
involving v *variables*
largest component size $= \xi_{\max}$.
If $\sqrt{N} \geq \xi_{\max}^2 \log_2 N + \xi_{\max}$, *and* $1 \leq v \leq N/12\xi_{\max}^2$, *then the number of solutions of the system of equations and complete set of non-equations is at least*

$$\frac{(2^n)_v}{2^{ne}}.$$

$\implies$ n-bit security for XORP[w]

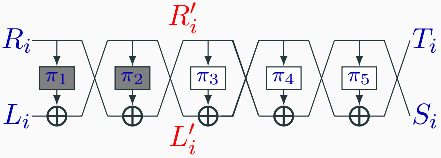
Example 2: 5 round permutation-based Luby-Rackoff

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



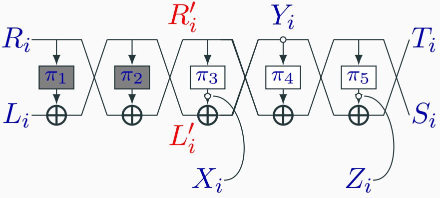
Example 2: 5 round permutation-based Luby-Rackoff

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



Example 2: 5 round permutation-based Luby-Rackoff

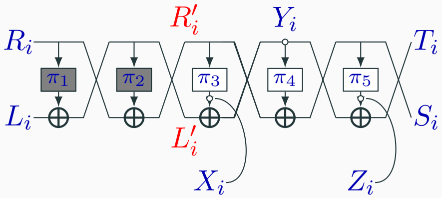
extended transcript: $\{((L_i, R_i), L'_i, R'_i, (S_i, T_i))\}$



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

Example 2: 5 round permutation-based Luby-Rackoff

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

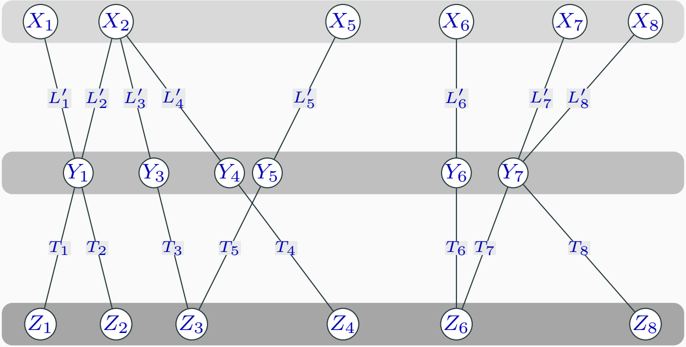


$$X_i \oplus Y_i = L'_i, \quad Y_i \oplus Z_i = T_i, \qquad i \in [q]$$

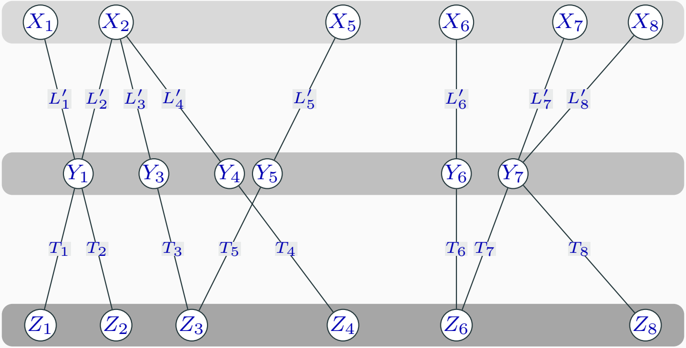
Note that $R'_i = R'_j \iff X_i = X_j, \qquad S_i = S_j \iff Z_i = Z_j$

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

Triclique Mirror Theory

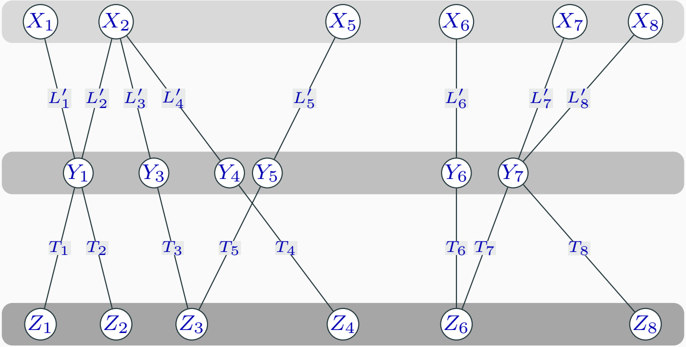


Triclique Mirror Theory



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 randomness of π_1, π_2

Triclique Mirror Theory



#(X, Y, Z)-respecting solutions

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

Triclique Mirror Theory

Theorem ([CS25])

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* $2^{n/2} > n\xi^2 + n$,

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

The extends the result for biclique mirror theory by [CLL24]

Triclique Mirror Theory

Theorem ([CS25])

Good system of equations: $\#$ *equations* $= e$,

partition of variables $= V_1 \sqcup V_2 \sqcup V_3$.

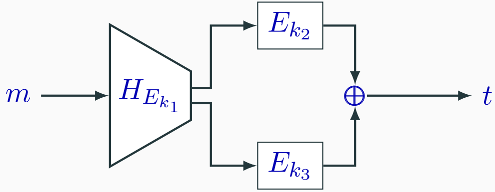
largest component size $= \xi$

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

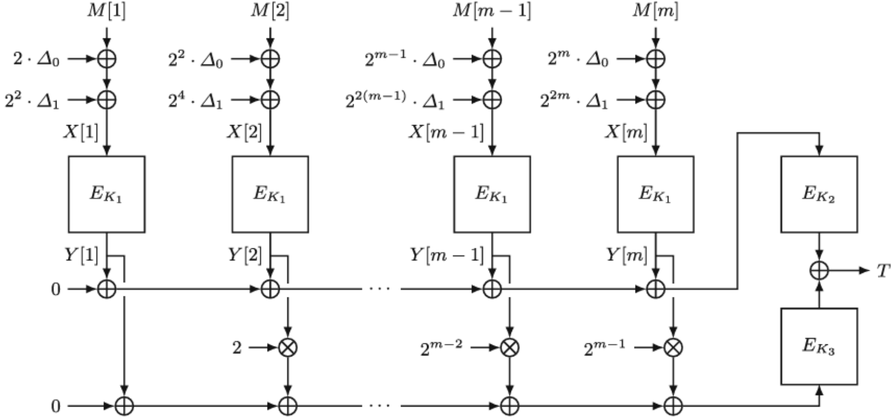
$$\#(V_1, V_2, V_3)\text{-}\textit{respecting solutions} \geq \frac{(2^n-2)_{|V_1|}(2^n-2)_{|V_2|}(2^n-2)_{|V_3|}}{2^{ne}}.$$

$\Longrightarrow$ n-bit CPA security of 5-pLR

Example 3: 1k-DbHtS [DDNP18]

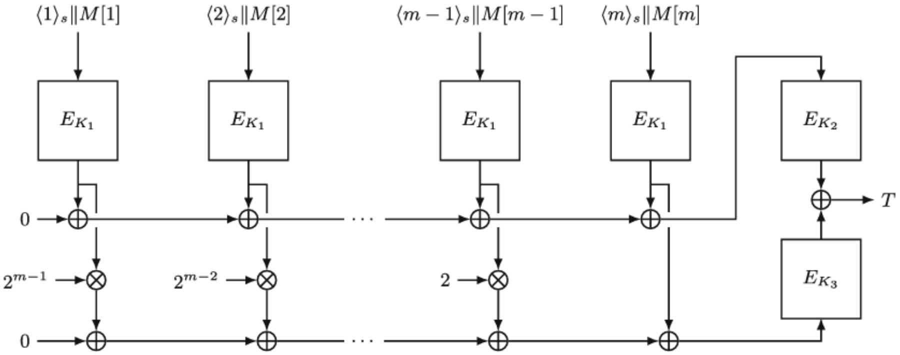


Instantiations : PMAC+



PMAC-Plus based on a block cipher E using three keys K_1, K_2, K_3, where $\Delta_0 = E_{K_1}(0)$ and $\Delta_1 = E_{K_1}(1)$.

Instantiations : LightMAC+



LightMAC-Plus based on a block cipher E using three keys K_1, K_2, K_3.

Restricted Mirror Theory Problem [CEJNS24]

Theorem

For a full row rank system, $\mathbb{E}$*, of* e *bivariate equations in* v *variables, in standard form, let* $\mathbb{E}_i$ *be the sub-system comprising of the equations of the* i*-th component. Then* $\mathbb{E}_i$ *has at least*

$$\frac{(2^n - |\mathcal{F}_i|)}{2^n}\left(1 - 2\left|\mu(\boldsymbol{\lambda}_i, \mathcal{F}_i) - \frac{(|\mathcal{R}| + e)^2}{2^n}\right| - \frac{4}{2^n}\right),$$

pairwise disjoint solutions with no variable assigned a value from the forbidden set $\mathcal{R}$*. Here* $\mathcal{F}_i := x_{\leq i-1} \cup \mathcal{R}$ *and*
$\mu(\boldsymbol{\lambda}_i, \mathcal{F}_i) = |\{(\phi_1, \phi_2) \in \mathcal{F}_i^{[2]} : \phi_1 \oplus \phi_2 \in \boldsymbol{\lambda}_i\}|$

Example 4: The LRW+ Paradigm [JKNS24]

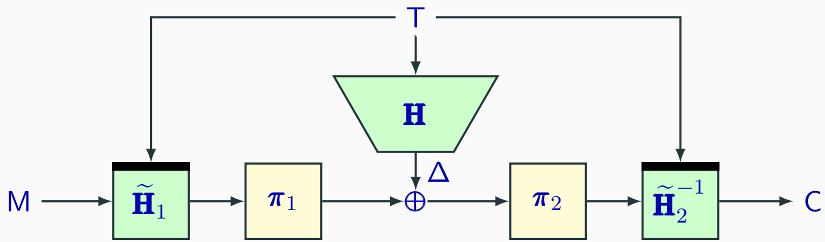


Figure 1: The LRW+ construction.

$$\Pr\left(\widetilde{\mathbf{H}} \leftarrow_{\$} \widetilde{\mathcal{H}} \ : \ \widetilde{\mathbf{H}}(t, m) = \widetilde{\mathbf{H}}(t', m')\right) \le \epsilon_1 \qquad \widetilde{\mathcal{H}} \text{ is } \epsilon_1\text{-AUTPF}$$

$$\Pr\left(\mathbf{H} \leftarrow_{\$} \mathcal{H} \ : \ \mathbf{H}(t) = \mathbf{H}(t')\right) \le \epsilon_2 \qquad \mathcal{H} \text{ is } \epsilon_2\text{-AUHF}$$

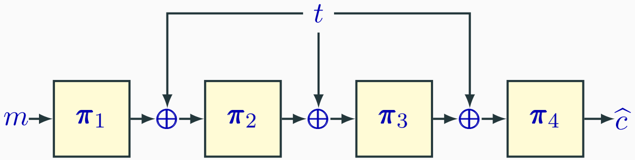
Instantiations

$\widetilde{\mathbf{H}}_1(t, m) = \boldsymbol{\pi}_1(m) \oplus t$

$\widetilde{\mathbf{H}}_2^{-1}(t, c) = \boldsymbol{\pi}_2^{-1}(c) \oplus t$

$\mathbf{H}(t) = t$

4LRW1

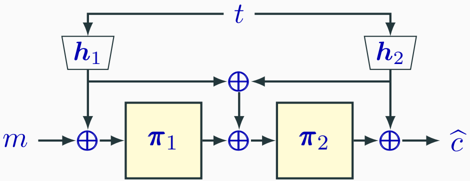


$\widetilde{\mathbf{H}}_1(t, m) = m \oplus \boldsymbol{h}_1(t)$

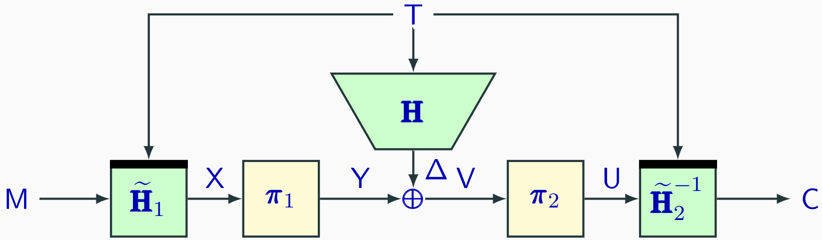
$\widetilde{\mathbf{H}}_2^{-1}(t, c) = c \oplus \boldsymbol{h}_2(t)$

$\mathbf{H}(t) = \boldsymbol{h}_1(t) \oplus \boldsymbol{h}_2(t)$

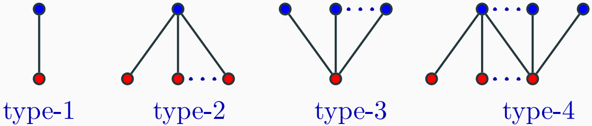
CLRW2



The LRW+ Paradigm



Good transcripts are such that the graph of equations $\mathsf{Y}_i \oplus \mathsf{V}_i = \Delta_i$ has only the following components:



Bipartite Mirror Theory for Tweakable Permutations [JKNS23]

Theorem (Bipartite Mirror Theory for general $\xi_{\max}$ [JN20])

Suppose for a consistent system of equations, the corresponding graph structure contains only type-1, type-2, type-3, type-4 components, in total $q \leq 2^n/4$ *edges, and maximum component size* $\xi_{\max} q \leq 2^n/2$

$$\left(1 - \frac{13q^4}{2^{3n}} - \frac{2q^2}{2^{2n}} - \left(\sum_{i=1}^{c_2+c_3} \eta_{c_1+i}^2\right) \frac{4q^2}{2^{2n}}\right) \times \frac{(2^n)_{q_1+c_2+q_3}(2^n)_{q_1+q_2+c_3}}{\prod_{i\in[s]}(2^n)_{\nu_i}}$$

solutions satisfying $\mathsf{Y}_i \neq \mathsf{Y}_j \wedge \mathsf{V}_i \neq \mathsf{V}_j$

- c_1, c_2, c_3 - the number of components of type-1, type-2, type-3 categories, respectively.
- q_1, q_2, q_3 - the number of edges of isolated, type-1, type-2, type-3 components, respectively.
- ν_i - multiplicity of Δ_i.