Proof of Mirror Theory for a Wide Range of $\xi_{\max}$

Benoît Cogliati[1] Avijit Dutta[2] Mridul Nandi[2,3]
Jacques Patarin[1,4] Abishanka Saha[3]

Thales DIS France SAS, Meudon, France

Institute for Advancing Intelligence, TCG-CREST, Kolkata, India

Indian Statistical Institute, Kolkata, India

Laboratoire de Mathématiques de Versailles, UVSQ, CNRS, Université Paris-Saclay, Versailles, France

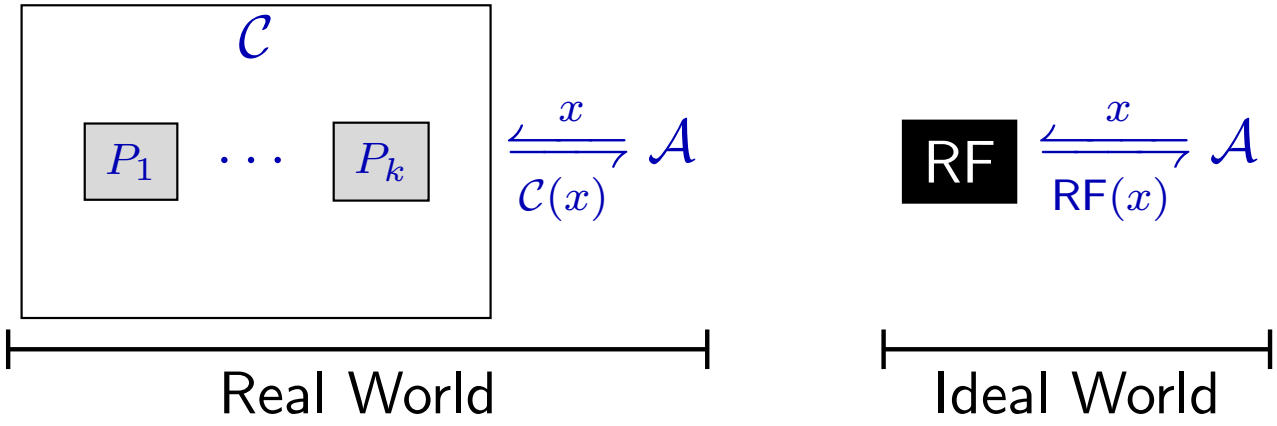
Outline

1. Provable Security using H-Coefficient Technique

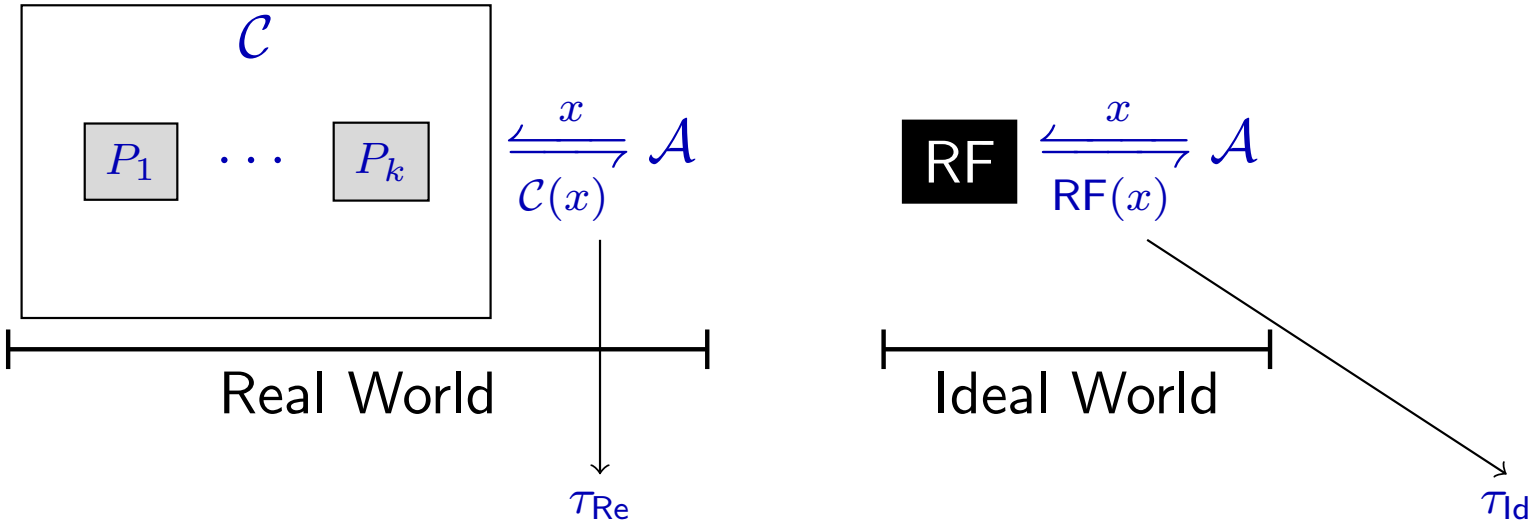
2. Mirror Theory
   - Main Result
   - Proof Strategy
   - Application
   - Future Directions

Outline

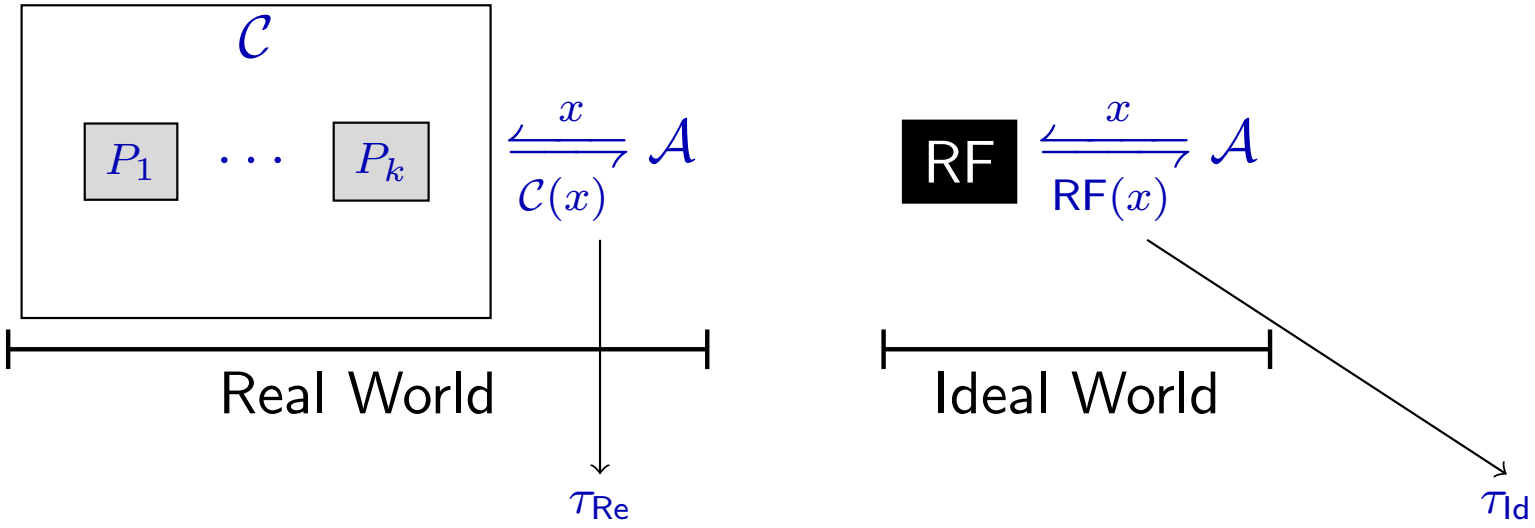
PRF Security using H-coefficient Technique



PRF Security using H-coefficient Technique



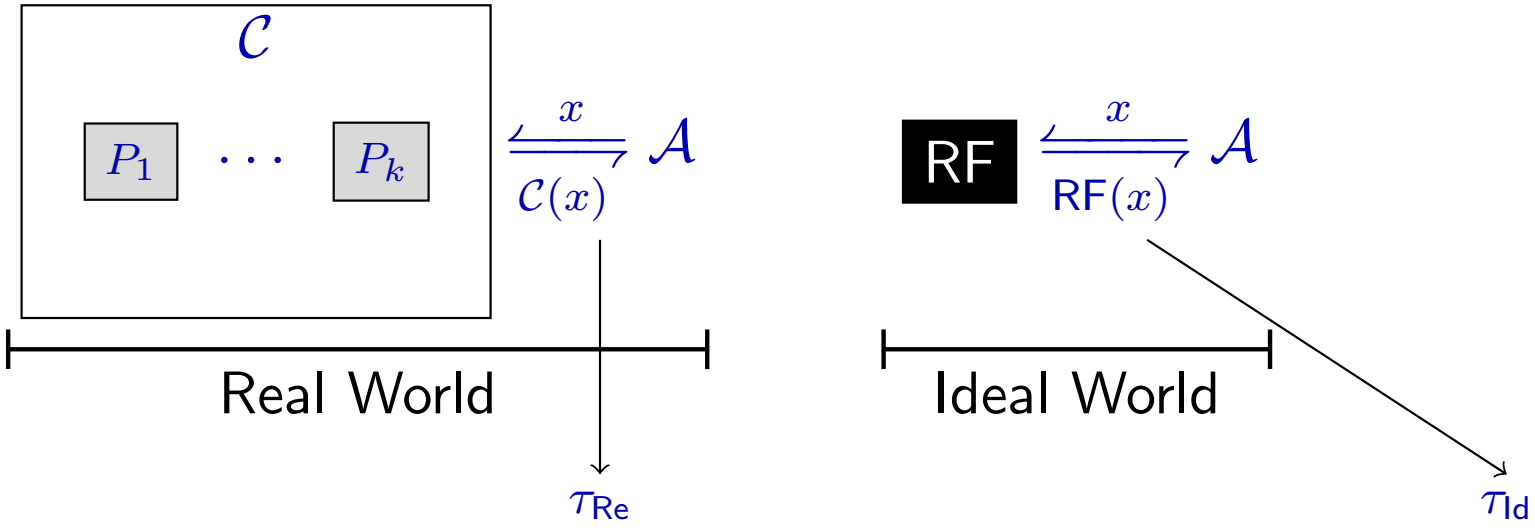
PRF Security using H-coefficient Technique



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

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

PRF Security using H-coefficient Technique

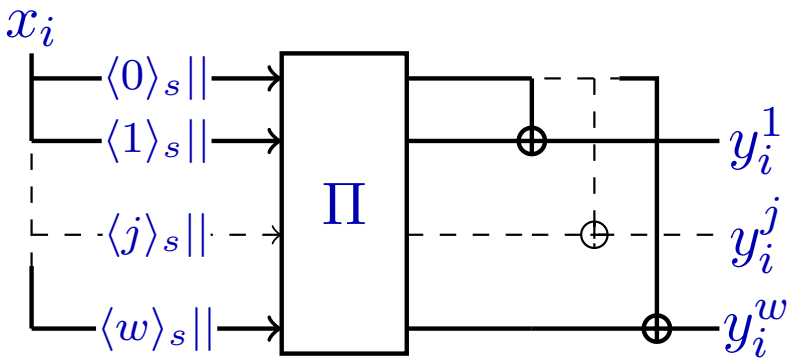


H-Coefficient Technique: For $\mathcal{T}_{\mathsf{good}} \subseteq \mathcal{T}_{\mathsf{Id}}$,

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

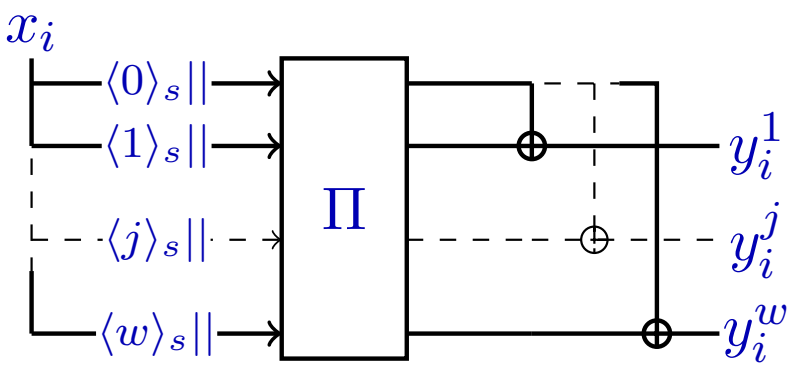
Need a lower bound on: $|\mathcal{T}_{\mathsf{Re}} \cap \mathcal{T}_{\mathsf{good}}|$.

XORP[w]



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

XORP[w]



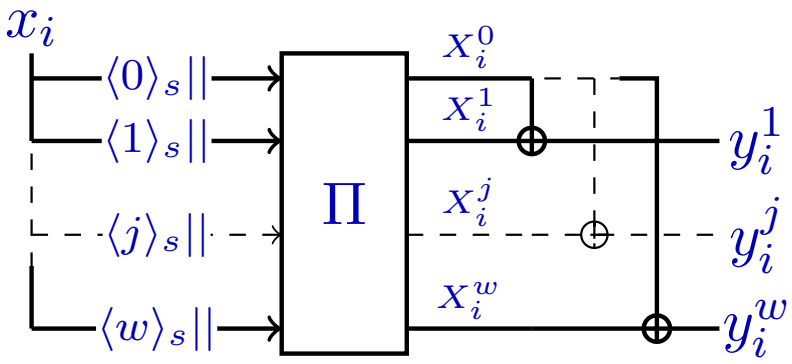
$\tau = ((x_1, y_1), \cdots, (x_q, y_q))$

Goodness Restrictions:

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

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

XORP[w]



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

Goodness Restrictions:

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

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

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

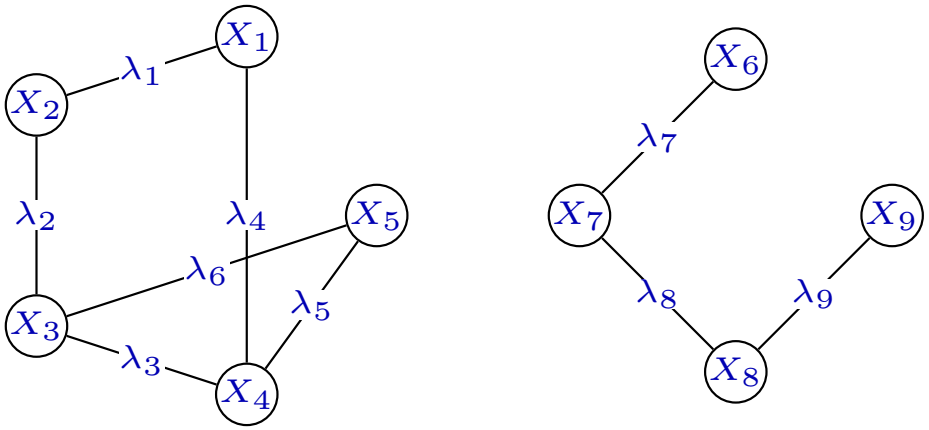
Outline

System of Bivariate Affine Equations

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

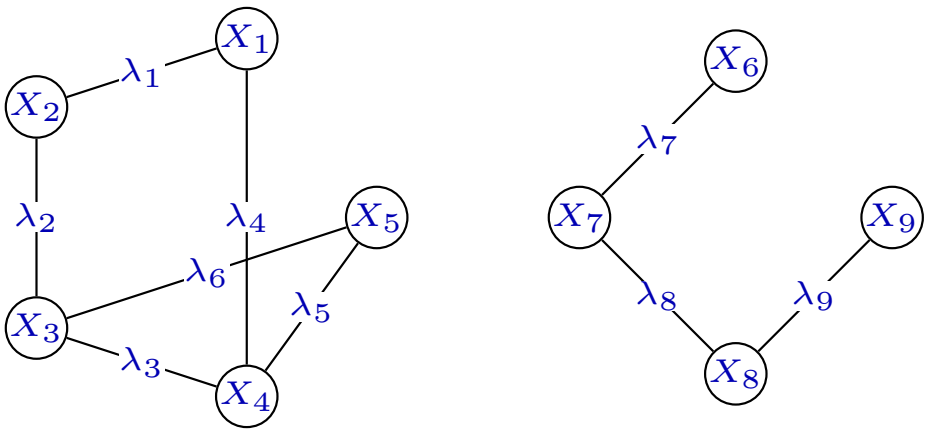
System of Bivariate Affine Equations

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



System of Bivariate Affine Equations

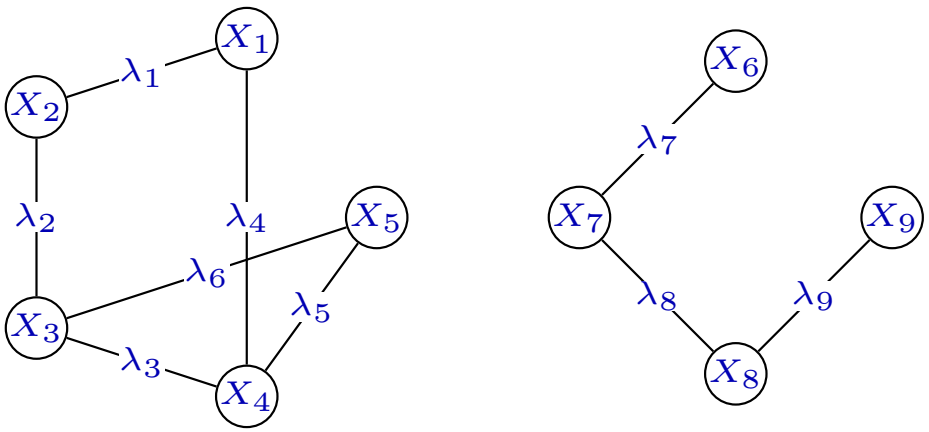
$$X_1 \oplus X_2 = \lambda_1 \quad X_1 \oplus X_4 = \lambda_4 \quad X_6 \oplus X_7 = \lambda_7$$
$$X_2 \oplus X_3 = \lambda_2 \quad X_4 \oplus X_5 = \lambda_5 \quad X_7 \oplus X_8 = \lambda_8$$
$$X_3 \oplus X_4 = \lambda_3 \quad X_3 \oplus X_5 = \lambda_6 \quad X_8 \oplus X_9 = \lambda_9$$



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

System of Bivariate Affine Equations

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

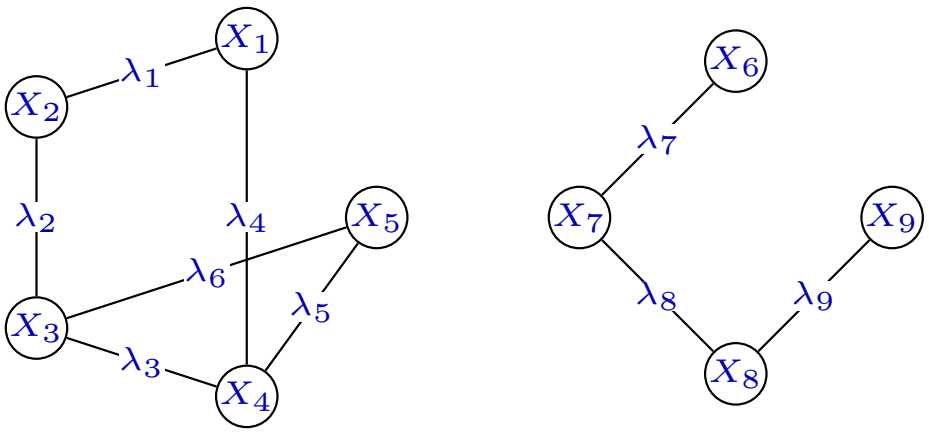


For having a solution, all cycles must have label sum zero.

For pairwise distinctness of a solution, every path must have non-zero label sum.

System of Bivariate Affine Equations

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

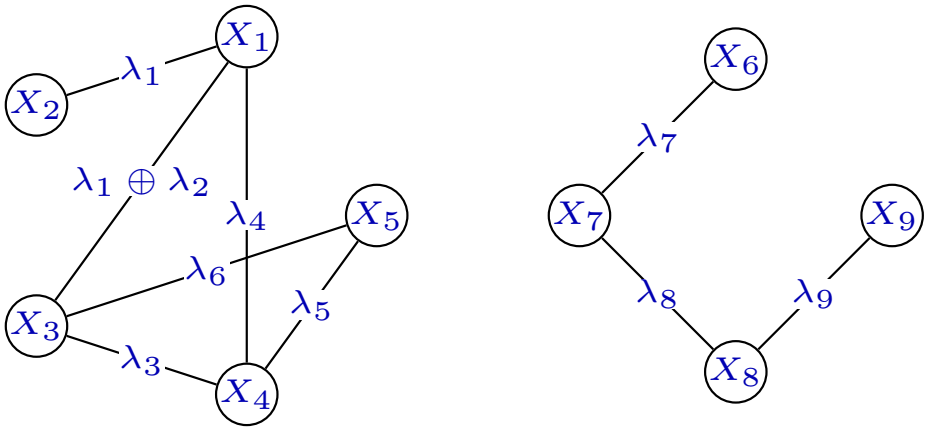


If we assign value to one variable the values of the all the variables in its component gets determined.

$\xi_{\max} :=$ size of largest component

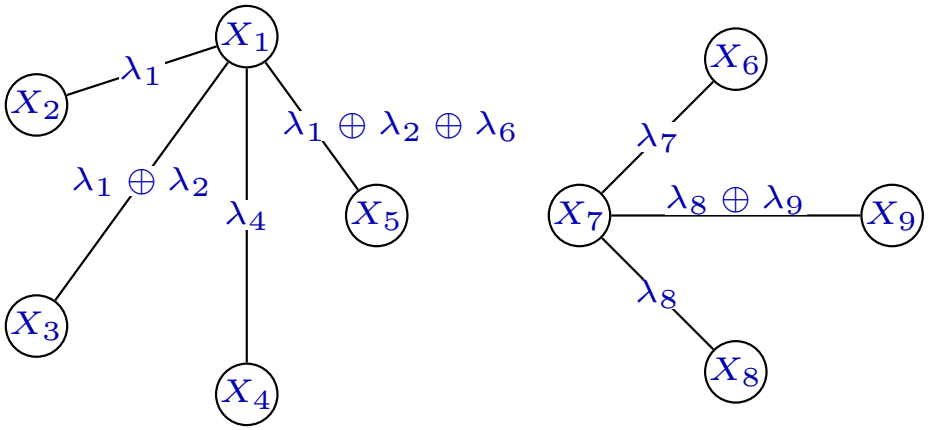
System of Bivariate Affine Equations

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



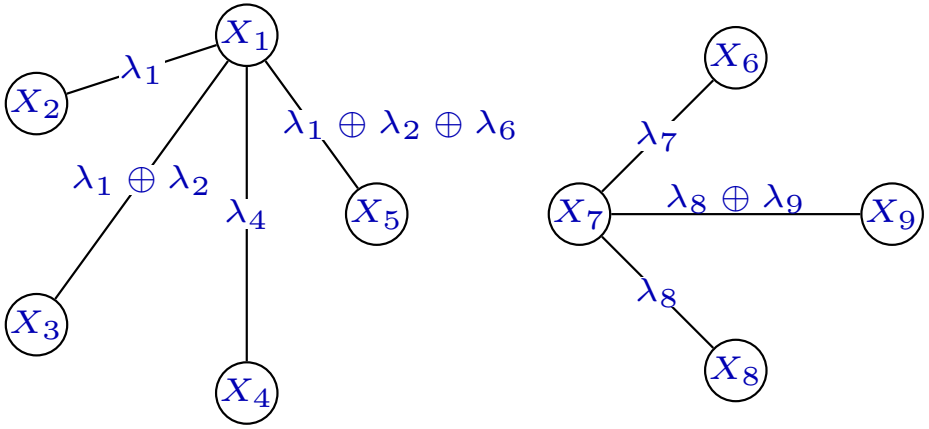
System of Bivariate Affine Equations

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



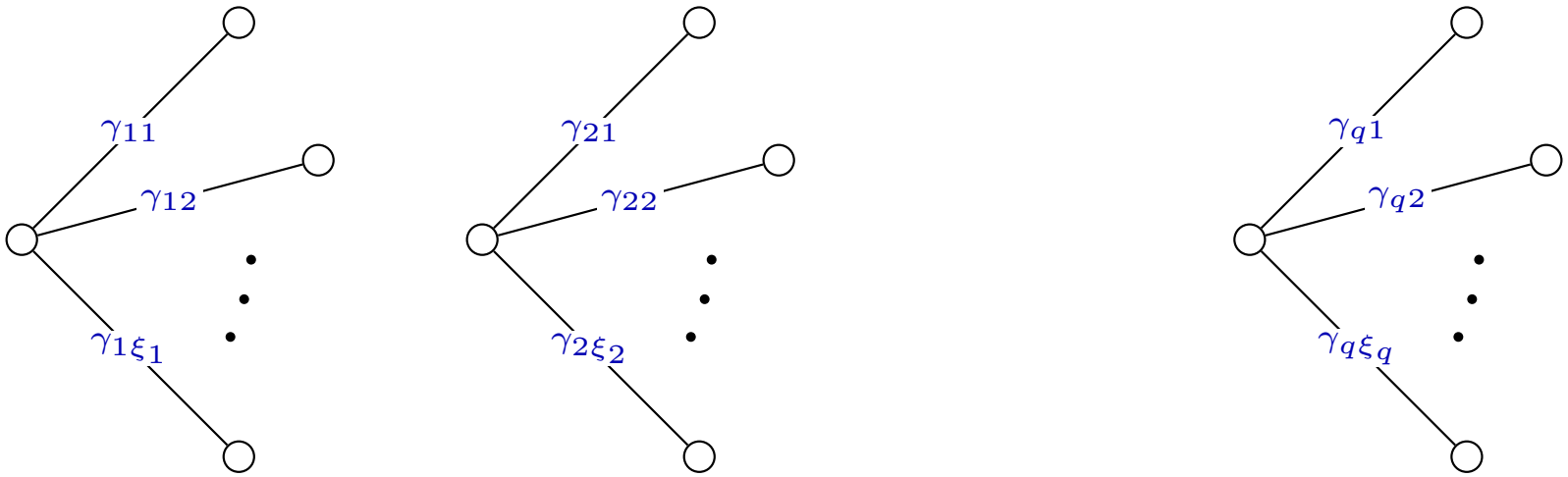
System of Bivariate Affine Equations

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



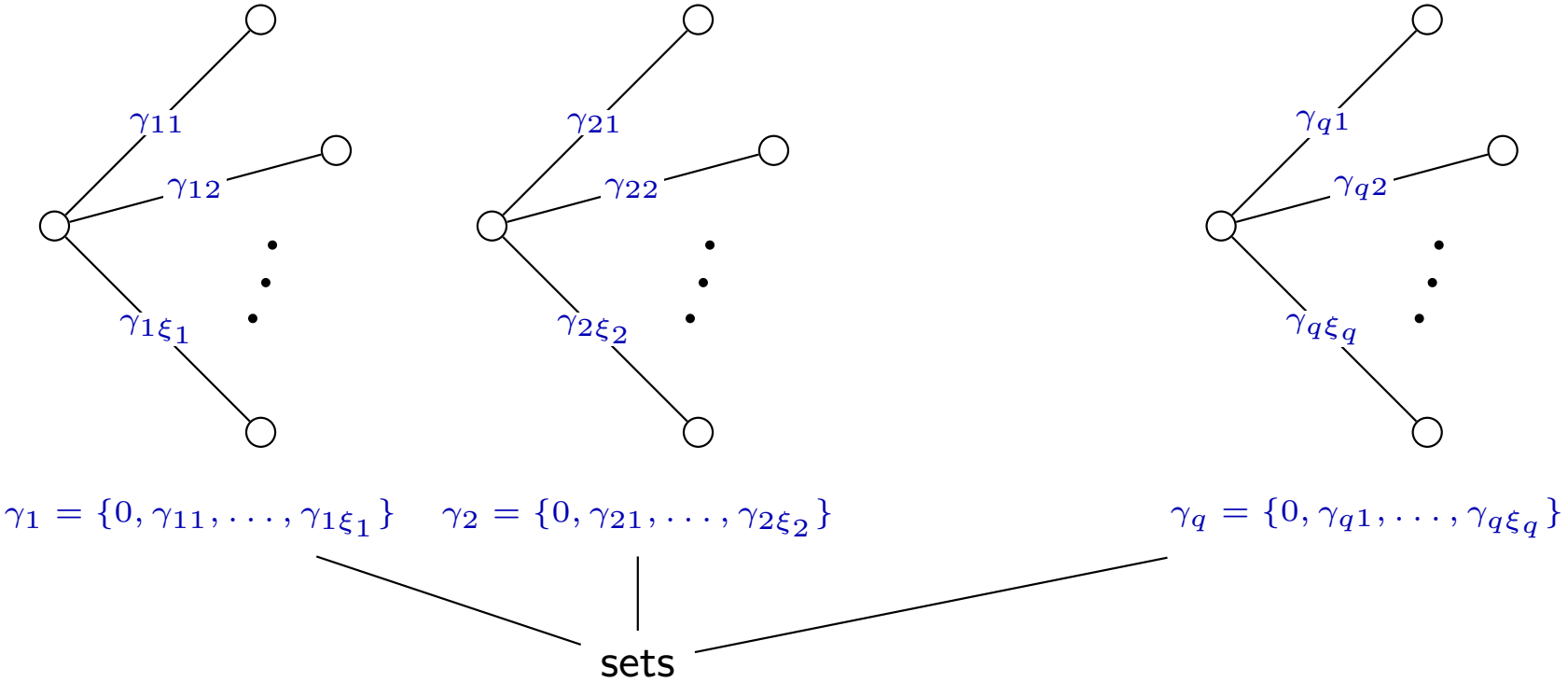
Standard form of the system

Generating Solutions to a System



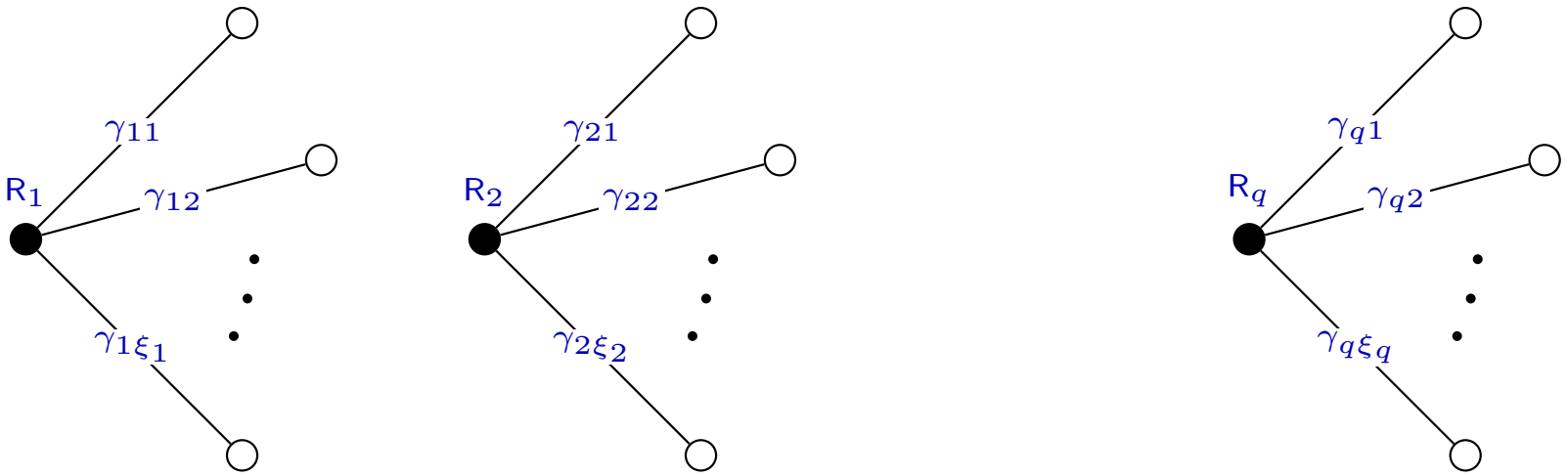
Generating Solutions to a System

$\gamma = (\gamma_1, \ldots, \gamma_q)$ - set system (galaxy of stars)



Generating Solutions to a System

$\gamma = (\gamma_1, \ldots, \gamma_q)$ - set system (galaxy of stars)

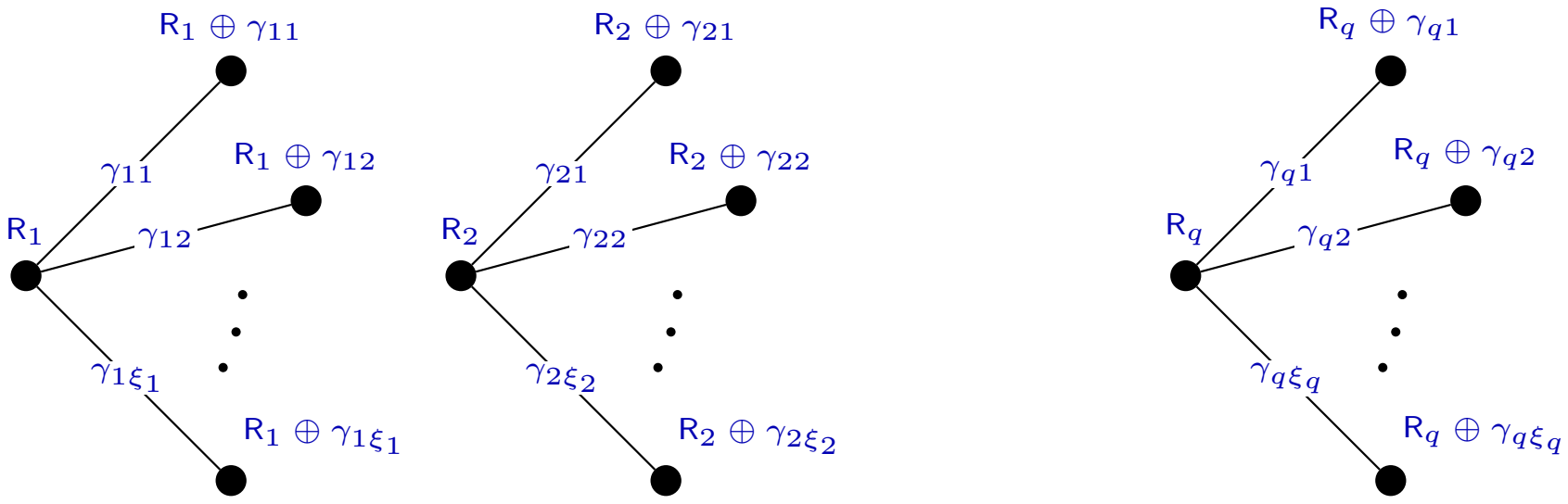


$\gamma_1 = \{0, \gamma_{11}, \ldots, \gamma_{1\xi_1}\}$ $\gamma_2 = \{0, \gamma_{21}, \ldots, \gamma_{2\xi_2}\}$ $\gamma_q = \{0, \gamma_{q1}, \ldots, \gamma_{q\xi_q}\}$

$\mathsf{R}_1, \ldots, \mathsf{R}_q \leftarrow \$ \{0,1\}^n$

Generating Solutions to a System

$\gamma = (\gamma_1, \ldots, \gamma_q)$ - set system (galaxy of stars)



$\gamma_1 = \{0, \gamma_{11}, \ldots, \gamma_{1\xi_1}\}$ $\gamma_2 = \{0, \gamma_{21}, \ldots, \gamma_{2\xi_2}\}$ $\gamma_q = \{0, \gamma_{q1}, \ldots, \gamma_{q\xi_q}\}$

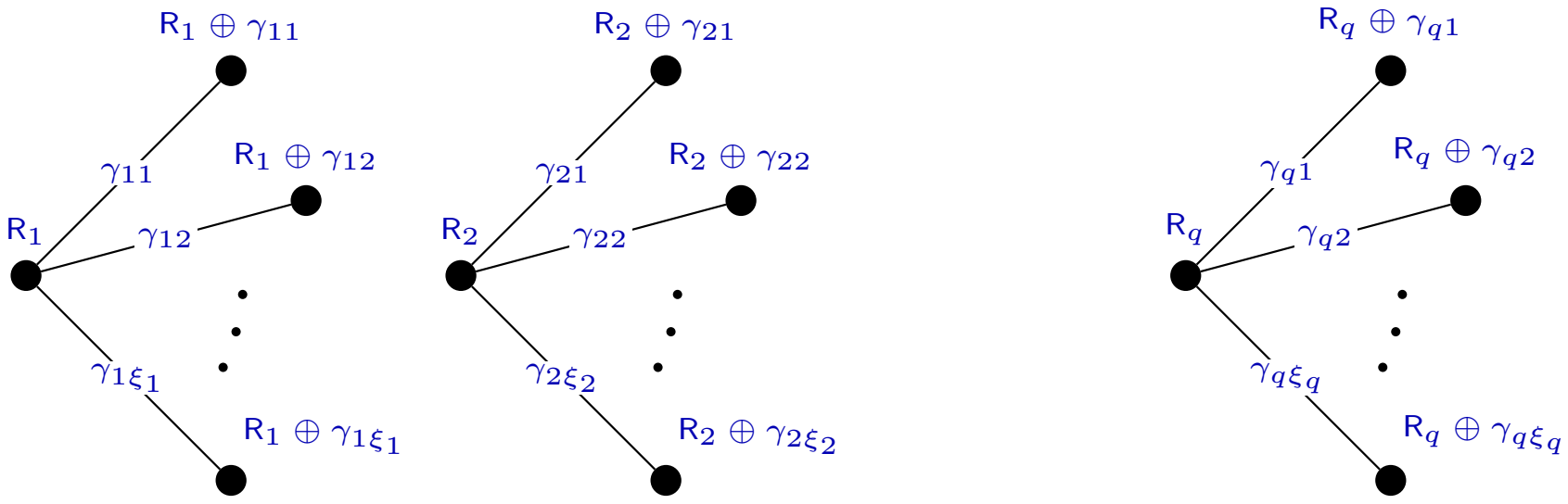
$\mathsf{R}_1, \ldots, \mathsf{R}_q \leftarrow \$ \{0,1\}^n$

The probability that this procedure will yield a particular solution, $(x_{11}, \ldots, x_{1\xi_1}, \ldots, x_{q1}, \ldots, x_{q\xi_q})$, to the above system, is

$$\Pr[\mathsf{R}_1 = x_{11}, \ldots, \mathsf{R}_q = x_{q1}] = 2^{-nq}.$$

Generating Solutions to a System

$\gamma = (\gamma_1, \ldots, \gamma_q)$ - set system (galaxy of stars)



$\gamma_1 = \{0, \gamma_{11}, \ldots, \gamma_{1\xi_1}\}$ $\gamma_2 = \{0, \gamma_{21}, \ldots, \gamma_{2\xi_2}\}$ $\gamma_q = \{0, \gamma_{q1}, \ldots, \gamma_{q\xi_q}\}$

$\mathsf{R}_1, \ldots, \mathsf{R}_q \leftarrow \$ \{0,1\}^n$

Disjointness event -

$$\mathsf{Disj}(\gamma) := \gamma_1 \oplus \mathsf{R}_1, \ldots, \gamma_q \oplus \mathsf{R}_q \text{ are disjoint}$$

$$\mathsf{P}(\gamma) := \Pr_{\mathsf{R}^q}(\mathsf{Disj}(\gamma)) = \frac{\#\text{ p.d. solutions}}{2^{nq}}$$

Main Result

Theorem

Consider a set system $\gamma = (\gamma_1, \ldots, \gamma_q)$, *with* $\|\gamma\| := \sum_i |\gamma_i| = v$ *and* $\|\gamma\|_{\max} := \max_i |\gamma_i| = \xi_{\max}$. *If* $v \leq 2^{n/2}$ *or if* $2^{n/2} \geq \xi_{\max}^2 n + \xi_{\max}$, *and* $1 \leq v \leq 2^n / 12\xi_{\max}^2$, *then*

$$\mathsf{P}(\gamma) \geq \frac{(2^n)_v}{2^{nv}}.$$

Main Result

Theorem

Consider a set system $\gamma = (\gamma_1, \ldots, \gamma_q)$, *with* $\|\gamma\| := \sum_i |\gamma_i| = v$ *and* $\|\gamma\|_{\max} := \max_i |\gamma_i| = \xi_{\max}$. *If* $v \leq 2^{n/2}$ *or if* $\xi_{\max} \sim O(2^{n/4}/\sqrt{n})$, *and* $1 \leq v \leq 2^n/12\xi_{\max}^2$, *then*

$$\mathsf{P}(\gamma) \geq \frac{(2^n)_v}{2^{nv}}.$$

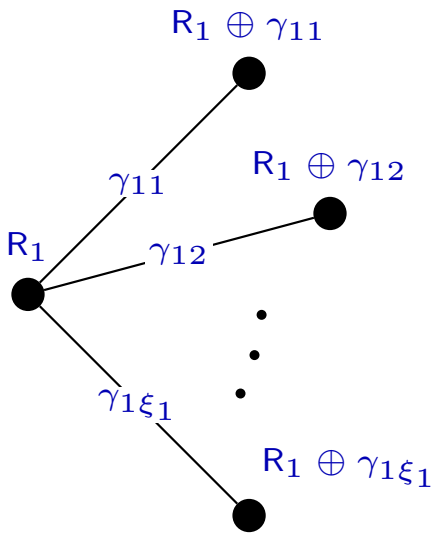
$$\#\text{ p.d. solutions} \geq \frac{(2^n)_v}{2^{nv}} \cdot 2^{nq} = \frac{(2^n)_v}{2^{ne}}$$

$v = \#$ variables

$e = \#$ equations

Proof Strategy

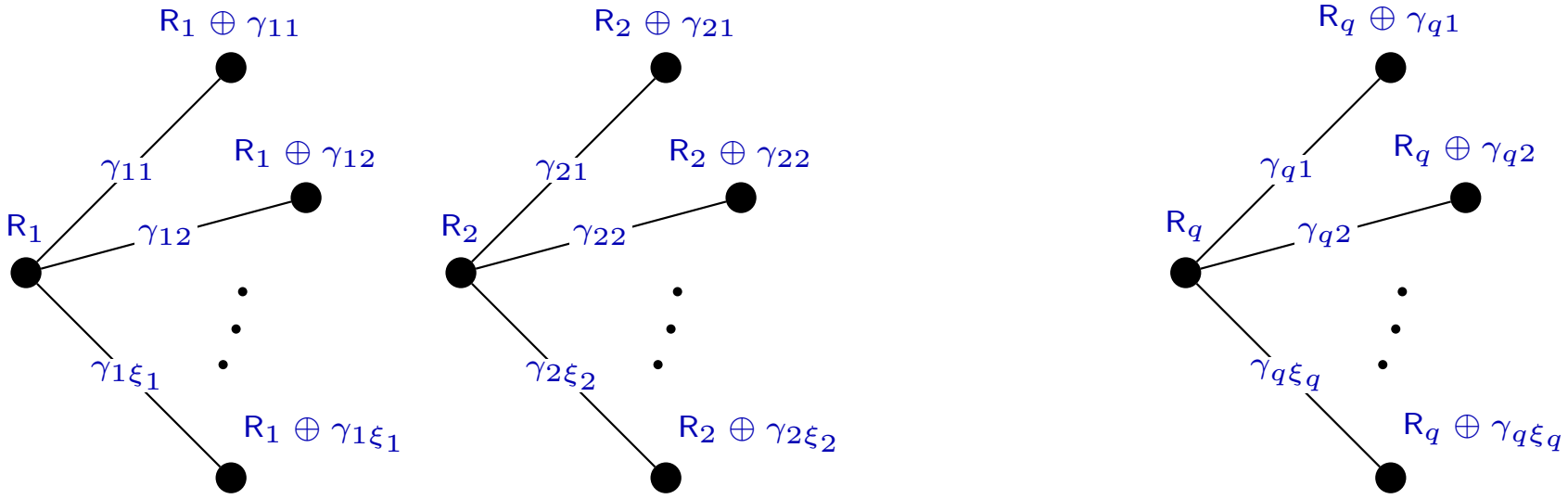
If there is just one star, $\mathsf{P}(\gamma) = 1$



$\gamma_1 = \{0, \gamma_{11}, \ldots, \gamma_{1\xi_1}\}$

Proof Strategy

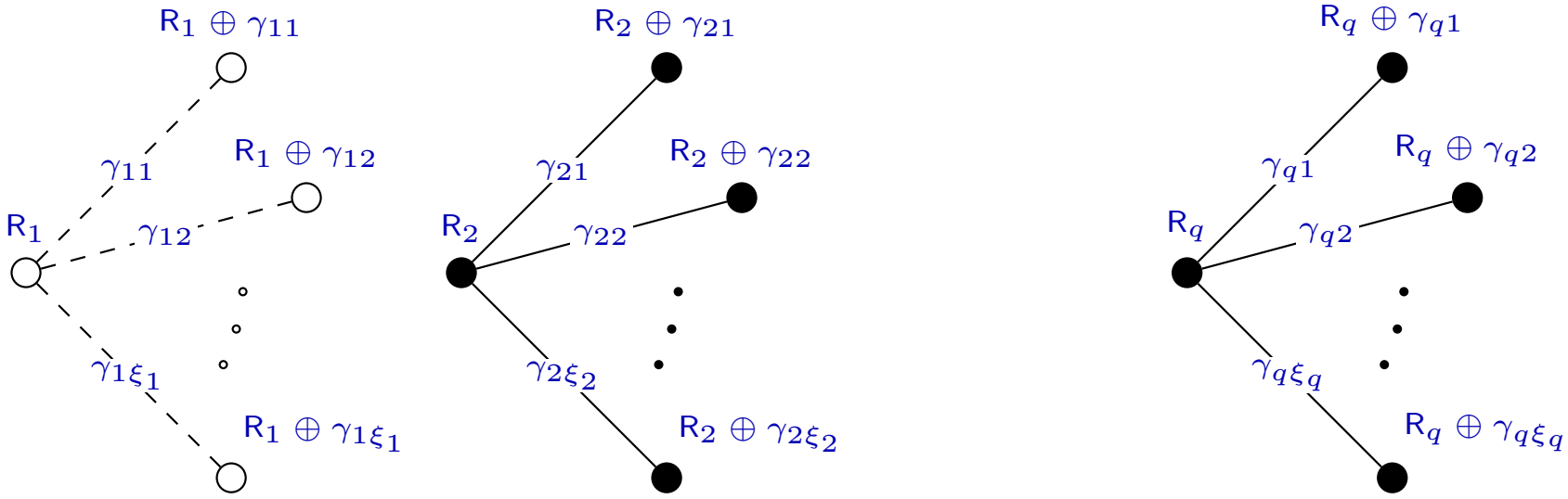
If we remove a star from a galaxy... $\gamma \to \gamma_{-S}$



$\gamma_1 = \{0, \gamma_{11}, \ldots, \gamma_{1\xi_1}\}$ $\gamma_2 = \{0, \gamma_{21}, \ldots, \gamma_{2\xi_2}\}$ $\gamma_q = \{0, \gamma_{q1}, \ldots, \gamma_{q\xi_q}\}$

Proof Strategy

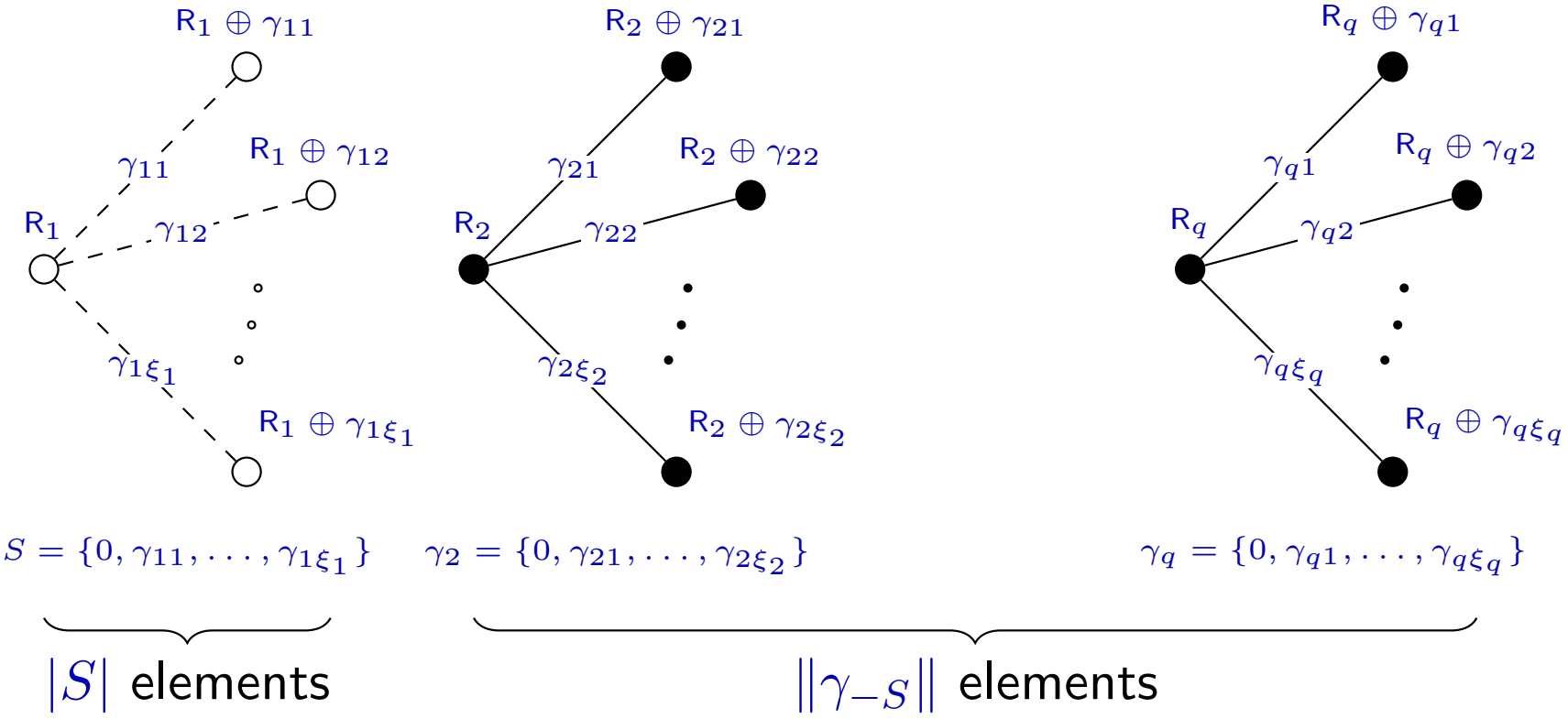
If we remove a star from a galaxy... $\gamma \to \gamma_{-S}$



$S = \{0, \gamma_{11}, \ldots, \gamma_{1\xi_1}\}$ $\gamma_2 = \{0, \gamma_{21}, \ldots, \gamma_{2\xi_2}\}$ $\gamma_q = \{0, \gamma_{q1}, \ldots, \gamma_{q\xi_q}\}$

Proof Strategy

If we remove a star from a galaxy... $\gamma \to \gamma_{-S}$



$$\mathsf{P}(\gamma) \geq \mathsf{P}(\gamma_{-S}) \left(1 - \frac{|S| \cdot \|\gamma_{-S}\|}{2^n}\right)$$ [crude bound]

Proof Strategy

Iterating this inequality, i.e. removing stars from the galaxy one-by-one we get

$$\mathsf{P}(\gamma) \geq \frac{(2^n)_v}{2^{nv}} \left(1 - \frac{q^2 \xi_{\max}^2}{2^n}\right)$$

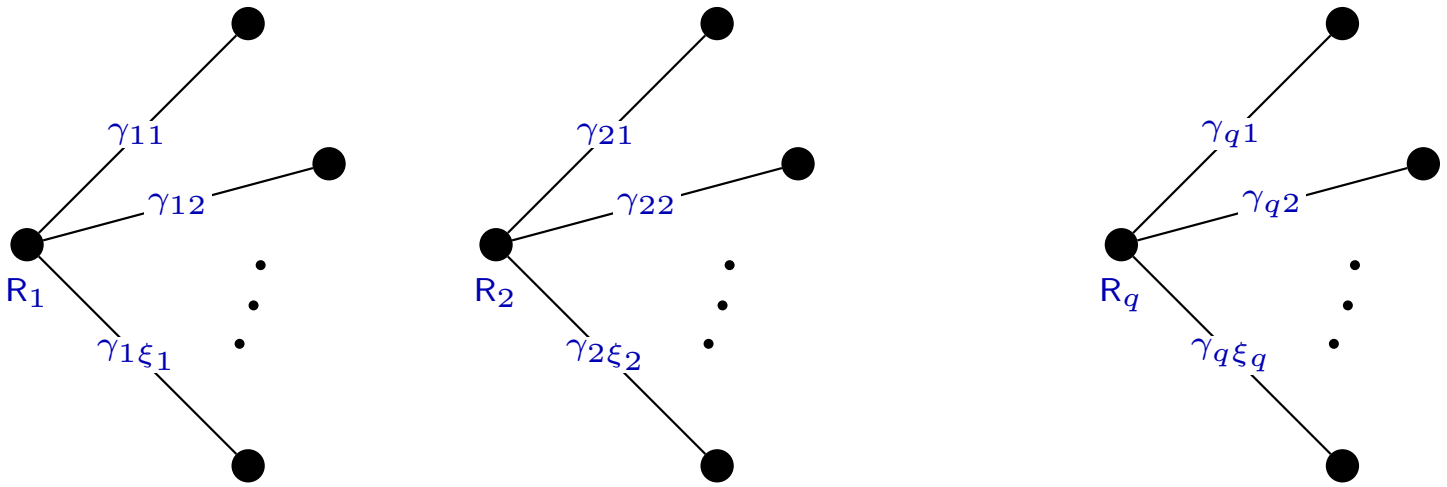
Birthday Bound ✗

However for $v \leq 2^{n/2}$ we can manipulate this inequality to obtain $\mathsf{P}(\gamma) \geq \frac{(2^n)_v}{2^{nv}}$.

Link Deletion Equation

So instead of removing a star, we just remove one link from a star.

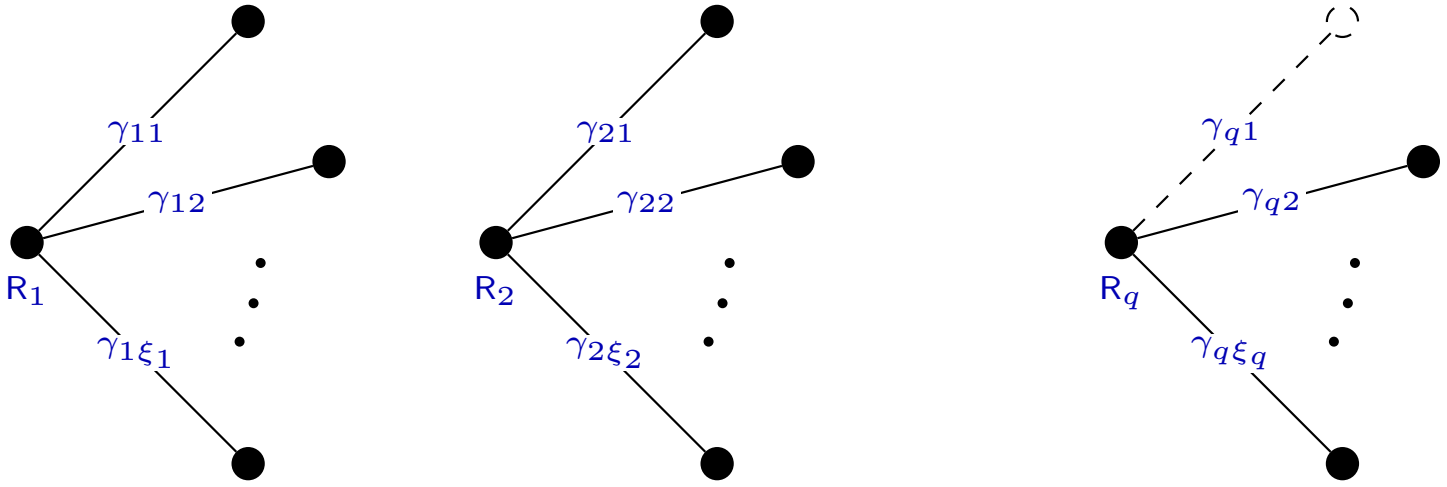
$\boxed{\gamma}$



Link Deletion Equation

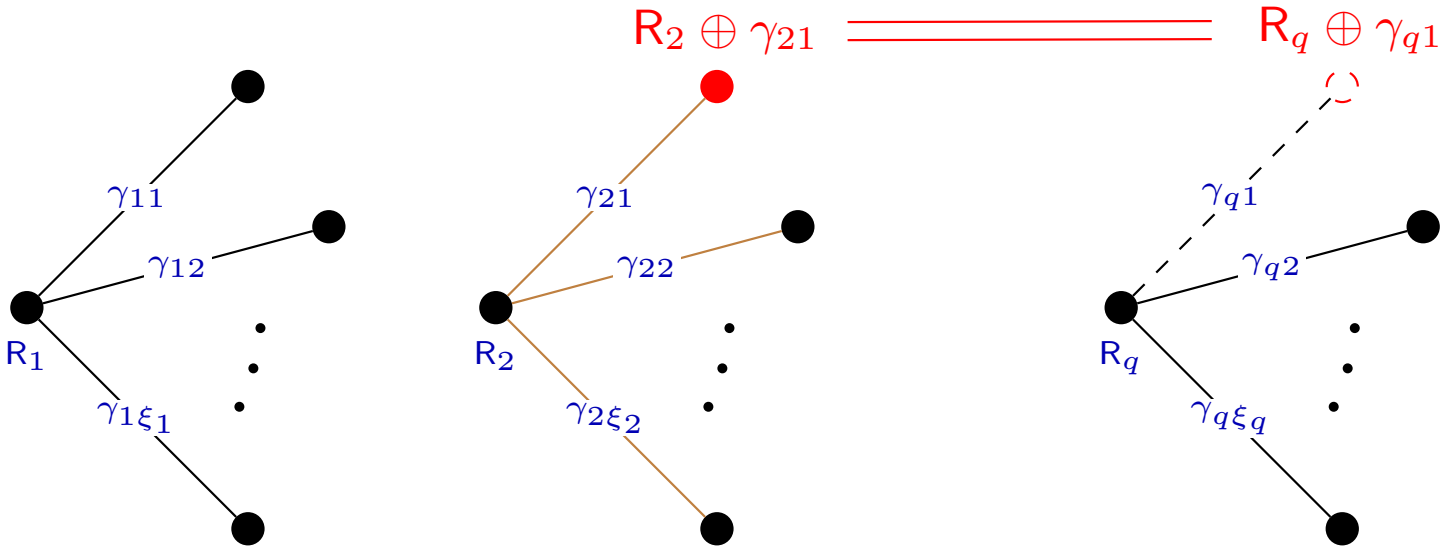
So instead of removing a star, we just remove one link from a star.

$\boxed{\gamma_{-\gamma_{q1}|\gamma_q}}$ *reduced galaxy*



Link Deletion Equation

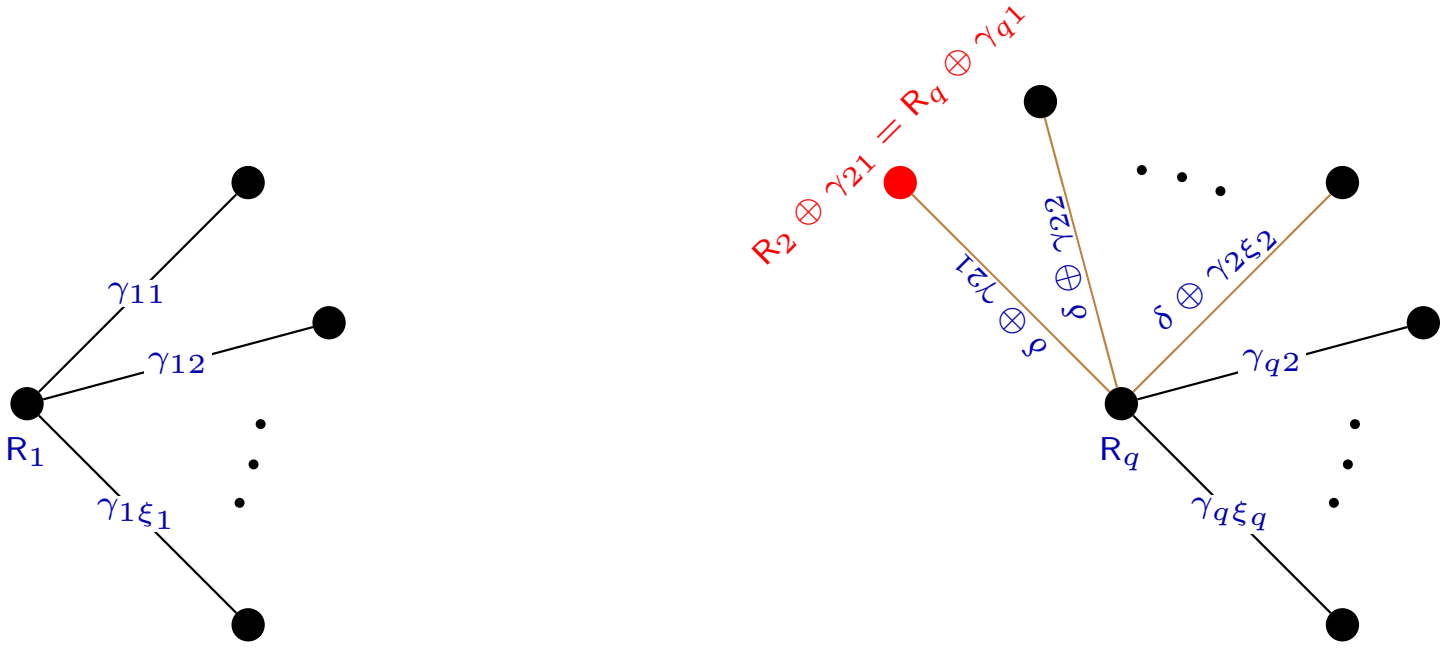
So instead of removing a star, we just remove one link from a star.



Link Deletion Equation

So instead of removing a star, we just remove one link from a star.

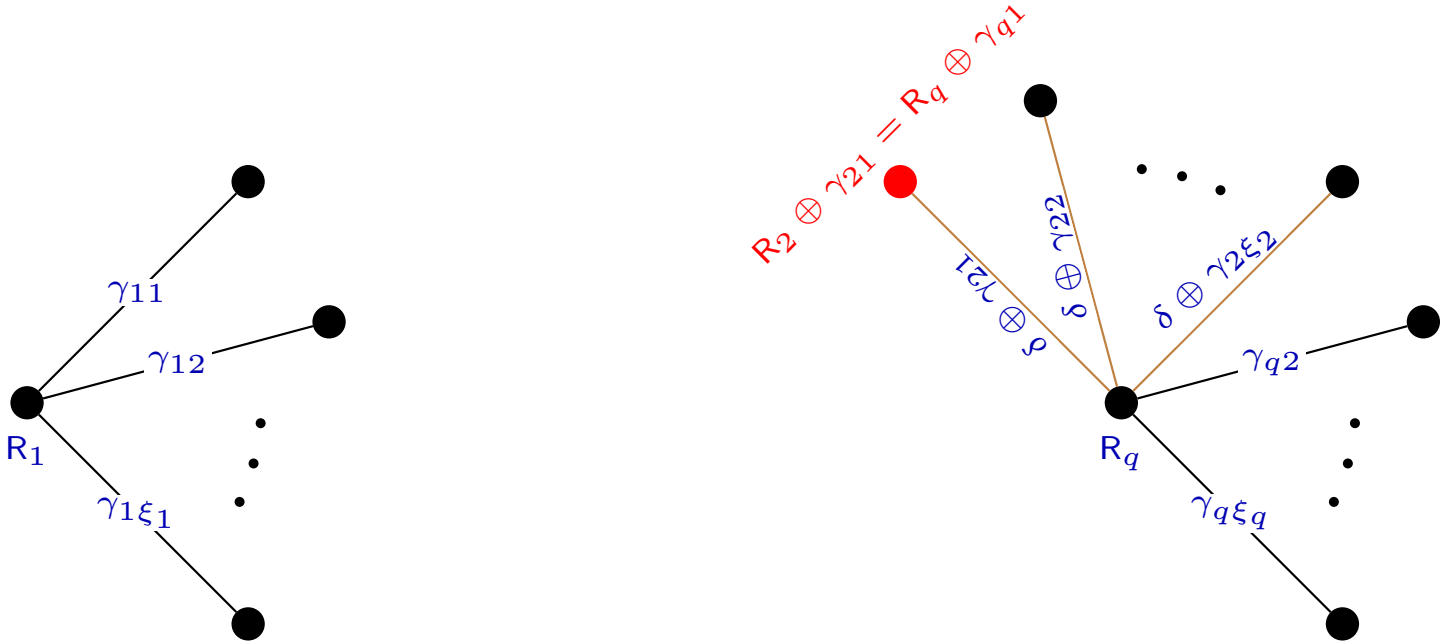
$\boxed{\gamma_{\delta,\gamma_2}}$ where $\delta = \gamma_{q1} \oplus \gamma_{21}$ *merged galaxy*



Link Deletion Equation

So instead of removing a star, we just remove one link from a star.

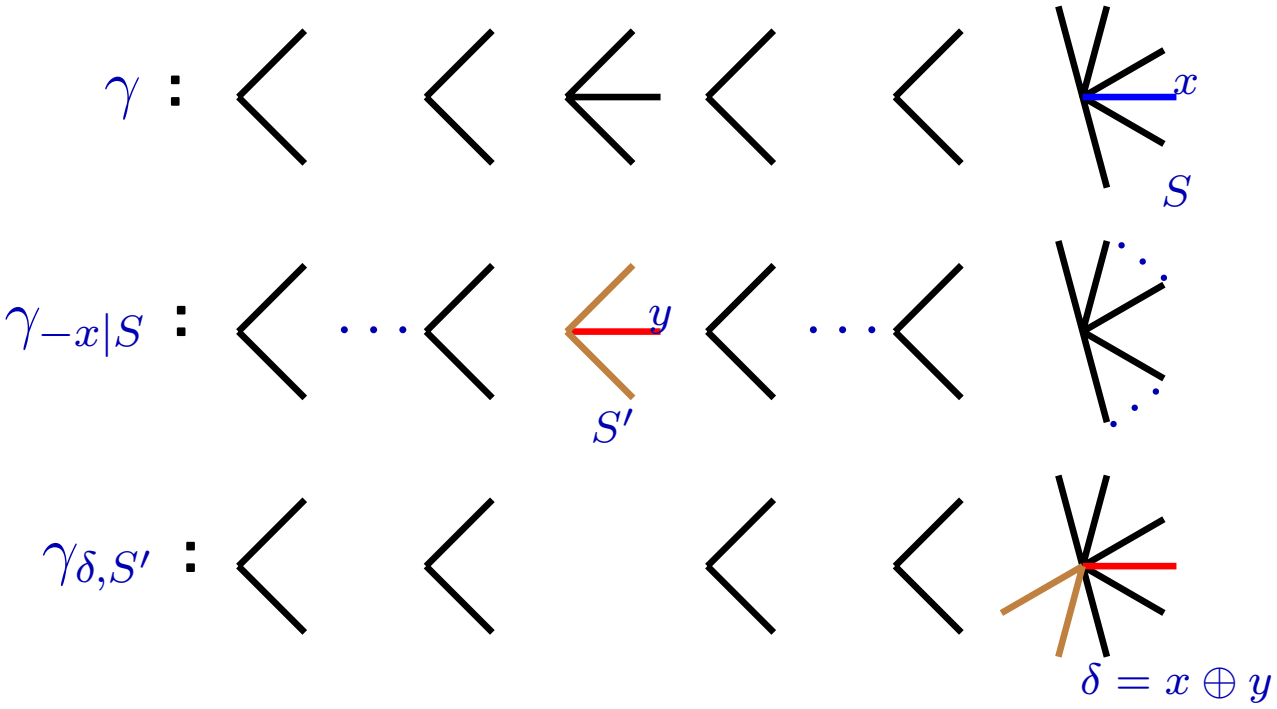
$\boxed{\gamma_{\delta,\gamma_2}}$ where $\delta = \gamma_{q1} \oplus \gamma_{21}$ *merged galaxy*



We must have $(\delta \oplus \gamma_2) \cap (\gamma_q \setminus \{\gamma_{q1}\}) = \emptyset$

Link Deletion Equation

$$\boxed{\mathsf{P}(\gamma) = \mathsf{P}(\gamma_{-x|S}) - \frac{1}{2^n} \sum_{(\delta,S')\in I} \mathsf{P}(\gamma_{\delta,S'})}$$



Link Deletion Equation

$$\boxed{\mathsf{P}(\gamma) = \mathsf{P}(\gamma_{-x|S}) - \frac{1}{2^n} \sum_{(\delta,S')\in I} \mathsf{P}(\gamma_{\delta,S'})}$$

where

$$I := \{(x \oplus y, S') : y \in S' \in \gamma_{-S}, \quad S' \oplus (x \oplus y) \text{ is disjoint with } S \setminus x\}$$

Link Deletion Equation

$$\boxed{\mathsf{P}(\gamma) = \mathsf{P}(\gamma_{-x|S}) - \frac{1}{2^n} \sum_{(\delta,S')\in I} \mathsf{P}(\gamma_{\delta,S'})}$$

where

$$I := \{(x \oplus y, S') : y \in S' \in \gamma_{-S}, \quad S' \oplus (x \oplus y) \text{ is disjoint with } S \setminus x\}$$

$$|I| \leq \|\gamma\| - \Delta_\gamma - |S|/2$$

Here we need that

- the group $(\{0,1\}^n, \oplus)$ is of exponent 2.
- The link removed, x has to be "appropriately" chosen.

Recursive Inequality

$$\mathsf{P}(\gamma) = \mathsf{P}(\underbrace{\gamma_{-x|S}}_{\tau}) - \frac{1}{2^n} \sum_{(\delta,S')\in I} \mathsf{P}(\underbrace{\gamma_{\delta,S'}}_{\tau'})$$

Recursive Inequality

$$\mathsf{P}(\gamma) = \mathsf{P}(\underbrace{\gamma_{-x|S}}_{\tau}) - \frac{1}{2^n} \sum_{(\delta,S')\in I} \mathsf{P}(\underbrace{\gamma_{\delta,S'}}_{\tau'})$$

$$\mathsf{P}(\tau) = \mathsf{P}(\tau_{-z|T}) - \frac{1}{2^n} \sum_{(\delta,T')\in I} \mathsf{P}(\tau_{\delta,T'}) \qquad [\text{where } T = S \setminus x]$$

$$- \left(\mathsf{P}(\tau') = \mathsf{P}(\tau'_{-z|U}) - \frac{1}{2^n} \sum_{(\delta,U')\in I'} \mathsf{P}(\tau'_{\delta,U'})\right) \qquad [\text{where } U = (S \setminus x) \sqcup (\delta \oplus S')]$$

$$\mathsf{P}(\tau) - \mathsf{P}(\tau')| \leq \left|\mathsf{P}(\tau_{-z}) - \mathsf{P}(\tau'_{-z})\right| + \frac{1}{2^n} \sum_{(\delta,U')\in I'} \left|\mathsf{P}(\tau_{\delta,U'}) - \mathsf{P}(\tau'_{\delta,U'})\right|$$

$$+ \frac{1}{2^n} \sum_{(\delta,T')\in I\setminus I'} \mathsf{P}(\tau_{\delta,T'})$$

Recursive Inequality

$$D(\alpha,\ell) = \max_{\substack{\gamma,S,S' \\ |\gamma|=\alpha,|S|=\ell}} |\mathsf{P}(\gamma) - \mathsf{P}(\gamma_{-S-S'+S\sqcup S'})|$$

$$\mathsf{P}(\tau) = \mathsf{P}(\tau_{-z|T}) - \frac{1}{2^n}\sum_{(\delta,T')\in I} \mathsf{P}(\tau_{\delta,T'}) \qquad [\text{where } T = S\setminus x]$$

$$-\left(\mathsf{P}(\tau') = \mathsf{P}(\tau'_{-z|U}) - \frac{1}{2^n}\sum_{(\delta,U')\in I'} \mathsf{P}(\tau'_{\delta,U'})\right) \qquad [\text{where } U = (S\setminus x)\sqcup(\delta\oplus S')]$$

$$D(\alpha,\ell-1) \le D(\alpha,\ell-1) + \frac{\|\gamma'_{-S}\|_{\max}}{2^n}\sum_{S'\in\gamma'_{-S}} D(\alpha-1,\ell+|S'|-1)$$

$$+\frac{2\Delta_{\gamma'}\|\gamma'\|_{\max}\cdot\mathsf{P}(\gamma)}{2^n\left(1-\frac{\|\gamma\setminus\gamma'\|_{\max}\times\|\gamma'\|}{2^n}\right)^{|\gamma\setminus\gamma'|}}$$

Recursive Inequality

$$D(\alpha,\ell) \leq D(\alpha,\ell-1) + \frac{\xi_{\max}}{2^n}\sum_{i=1}^{q} D(\alpha-1,\ell+\xi_i-1) + \frac{2\Delta\xi_{\max}\cdot \mathsf{P}(\gamma)}{2^n\left(1-q\xi_{\max}^2/2^n\right)^{q-\alpha}}$$

Recursive Inequality

$$D(\alpha,\ell) \leq D(\alpha,\ell-1) + \frac{\xi_{\max}}{2^n}\sum_{i=1}^{q} D(\alpha-1,\ell+\xi_i-1) + \frac{2\Delta\xi_{\max}\cdot \mathsf{P}(\gamma)}{2^n\left(1-q\xi_{\max}^2/2^n\right)^{q-\alpha}}$$

This term will vanish after $\ell - 1$ iterations.

Recursive Inequality

$$D(\alpha,\ell) \leq D(\alpha,\ell-1) + \frac{\xi_{\max}}{2^n}\sum_{i=1}^{q} D(\alpha-1,\ell+\xi_i-1) + \frac{2\Delta\xi_{\max}\cdot \mathsf{P}(\gamma)}{2^n\left(1-q\xi_{\max}^2/2^n\right)^{q-\alpha}}$$

The second term is multiplied by $\xi_{\max}/2^n$, so will be geometrically reduced.

Recursive Inequality

$$D(\alpha,\ell) \leq D(\alpha,\ell-1) + \frac{\xi_{\max}}{2^n}\sum_{i=1}^{q} D(\alpha-1,\ell+\xi_i-1) + \frac{2\Delta\xi_{\max}\cdot \mathsf{P}(\gamma)}{2^n\left(1-q\xi_{\max}^2/2^n\right)^{q-\alpha}}$$

This parasite term will not be an issue after a logarithmic number of iterations

Recursive Inequality

$$D(\alpha,\ell) \leq D(\alpha,\ell-1) + \frac{\xi_{\max}}{2^n}\sum_{i=1}^{q} D(\alpha-1,\ell+\xi_i-1) + \frac{2\Delta\xi_{\max}\cdot \mathsf{P}(\gamma)}{2^n\left(1-q\xi_{\max}^2/2^n\right)^{q-\alpha}}$$

Iterating the recursive inequality for $\xi_{\max}\cdot n$ times and then applying the crude bound on the resulting terms gives us

$$D(q,|S|-2) \leq 8\mathsf{P}(\gamma)(\Delta\xi_{\max}^2+1)/2^n$$

Recursive Inequality

$$D(\alpha,\ell) \leq D(\alpha,\ell-1) + \frac{\xi_{\max}}{2^n}\sum_{i=1}^{q} D(\alpha-1,\ell+\xi_i-1) + \frac{2\Delta\xi_{\max}\cdot \mathsf{P}(\gamma)}{2^n\left(1-q\xi_{\max}^2/2^n\right)^{q-\alpha}}$$

Iterating the recursive inequality for $\xi_{\max}\cdot n$ times and then applying the crude bound on the resulting terms gives us

$$D(q,|S|-2) \leq 8\mathsf{P}(\gamma)(\Delta\xi_{\max}^2+1)/2^n$$

This implies

$$\mathsf{P}(\gamma_{\delta,S'}) \leq \mathsf{P}(\gamma_{-x|S})\left(1+\frac{9\Delta(\xi_{\max}^2+1)}{2^n}\right) \qquad (\star\star)$$

Wrapping up the Proof

For an "appropriately" chosen $x \in S \in \gamma$,

$$\boxed{\mathsf{P}(\gamma) \geq \left(1 - \frac{\|\gamma\| - 1}{2^n}\right) \mathsf{P}(\gamma_{-x|S})}$$

Wrapping up the Proof

For an "appropriately" chosen $x \in S \in \gamma$,

$$\boxed{\mathsf{P}(\gamma) \geq \left(1 - \frac{\|\gamma\| - 1}{2^n}\right) \mathsf{P}(\gamma_{-x|S})}$$

$$\gamma \xrightarrow{-x_0|S_0} \gamma^{(1)} \xrightarrow{-x_1|S_1} \gamma^{(2)} \cdots \longrightarrow \gamma^{(i)} \xrightarrow{-x_i|S_i} \gamma^{(i+1)} \cdots \longrightarrow \gamma^{(\sigma)}$$

for "appropriately" chosen $x_i \in S_i \in \gamma^{(i)}$

Wrapping up the Proof

For an "appropriately" chosen $x \in S \in \gamma$,

$$\boxed{\mathsf{P}(\gamma) \geq \left(1 - \frac{\|\gamma\| - 1}{2^n}\right) \mathsf{P}(\gamma_{-x|S})}$$

$$\gamma \xrightarrow{-x_0|S_0} \gamma^{(1)} \xrightarrow{-x_1|S_1} \gamma^{(2)} \cdots \longrightarrow \gamma^{(i)} \xrightarrow{-x_i|S_i} \gamma^{(i+1)} \cdots \longrightarrow \gamma^{(\sigma)}$$

up to $\|\gamma^{(\sigma)}\| \leq 2^{n/2}$

Wrapping up the Proof

For an "appropriately" chosen $x \in S \in \gamma$,

$$\boxed{\mathsf{P}(\gamma) \geq \left(1 - \frac{\|\gamma\| - 1}{2^n}\right) \mathsf{P}(\gamma_{-x|S})}$$

$$\gamma \xrightarrow{-x_0|S_0} \gamma^{(1)} \xrightarrow{-x_1|S_1} \gamma^{(2)} \cdots \longrightarrow \gamma^{(i)} \xrightarrow{-x_i|S_i} \gamma^{(i+1)} \cdots \longrightarrow \gamma^{(\sigma)}$$

Then we have

$$\mathsf{P}(\gamma) \geq \mathsf{P}(\gamma^{(\sigma)}) \prod_{i=1}^{\sigma} \left(1 - \frac{\|\gamma^{(i-1)}\| - 1}{2^n}\right)$$

Wrapping up the Proof

For an "appropriately" chosen $x \in S \in \gamma$,

$$\boxed{\mathsf{P}(\gamma) \geq \left(1 - \frac{\|\gamma\| - 1}{2^n}\right) \mathsf{P}(\gamma_{-x|S})}$$

$$\gamma \xrightarrow{-x_0|S_0} \gamma^{(1)} \xrightarrow{-x_1|S_1} \gamma^{(2)} \cdots \longrightarrow \gamma^{(i)} \xrightarrow{-x_i|S_i} \gamma^{(i+1)} \cdots \longrightarrow \gamma^{(\sigma)}$$

Then we have

$$\mathsf{P}(\gamma) \geq \mathsf{P}(\gamma^{(\sigma)}) \prod_{i=1}^{\sigma} \left(1 - \frac{\|\gamma\| - i}{2^n}\right)$$

Wrapping up the Proof

For an "appropriately" chosen $x \in S \in \gamma$,

$$\boxed{\mathsf{P}(\gamma) \geq \left(1 - \frac{\|\gamma\| - 1}{2^n}\right) \mathsf{P}(\gamma_{-x|S})}$$

$$\gamma \xrightarrow{-x_0|S_0} \gamma^{(1)} \xrightarrow{-x_1|S_1} \gamma^{(2)} \cdots \longrightarrow \gamma^{(i)} \xrightarrow{-x_i|S_i} \gamma^{(i+1)} \cdots \longrightarrow \gamma^{(\sigma)}$$

Then we have

$$\mathsf{P}(\gamma) \geq \frac{(2^n)_{\|\gamma^{(\sigma)}\|}}{2^{n\|\gamma^{(\sigma)}\|}} \prod_{i=1}^{\sigma} \left(1 - \frac{\|\gamma\| - i}{2^n}\right)$$

Wrapping up the Proof

For an "appropriately" chosen $x \in S \in \gamma$,

$$\boxed{\mathsf{P}(\gamma) \geq \left(1 - \frac{\|\gamma\| - 1}{2^n}\right) \mathsf{P}(\gamma_{-x|S})}$$

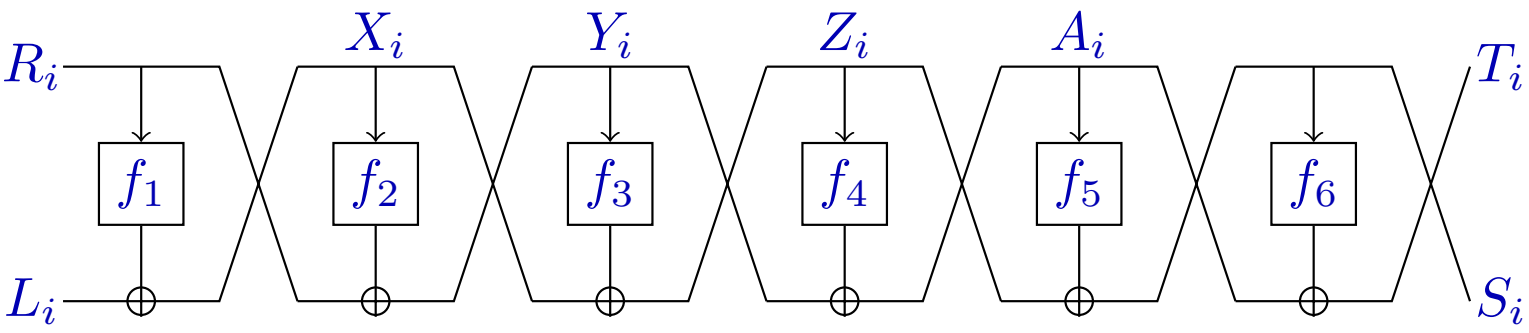
$$\gamma \xrightarrow{-x_0|S_0} \gamma^{(1)} \xrightarrow{-x_1|S_1} \gamma^{(2)} \cdots \longrightarrow \gamma^{(i)} \xrightarrow{-x_i|S_i} \gamma^{(i+1)} \cdots \longrightarrow \gamma^{(\sigma)}$$

Then we have

$$\mathsf{P}(\gamma) \geq \frac{(2^n)_{\|\gamma\|}}{2^{n\|\gamma\|}}$$

Security Analysis of 6-round Feistel

$$\tau = \{([L_i, R_i], [S_i, T_i]) : i \in [q]\}.$$

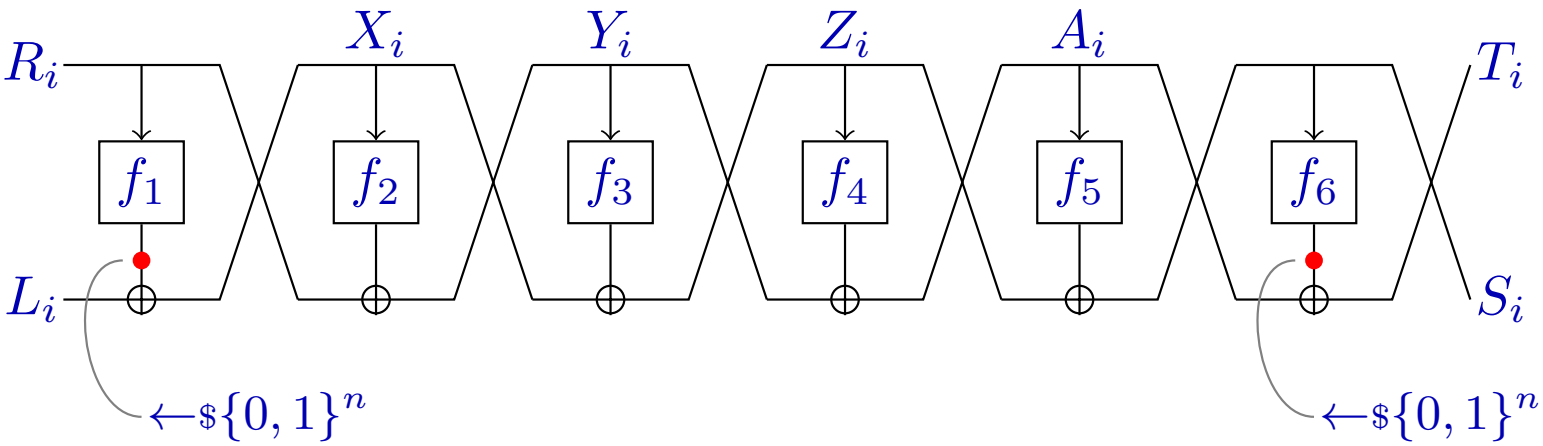


$$\Pr[\boldsymbol{\tau}_{\mathsf{Re}} = \tau] = \frac{N_6(\tau)}{|\mathsf{Func}_n|^6}$$

$$N_6(\tau) := \left|\{(f_1, \cdots, f_6) \in \mathsf{Func}_n^6 : \psi^6(f_1, \cdots, f_6)[L_i, R_i] = [S_i, T_i] \forall i \in [q]\}\right|$$

Security Analysis of 6-round Feistel

$$\tau = \{([L_i, R_i], [S_i, T_i]) : i \in [q]\}.$$

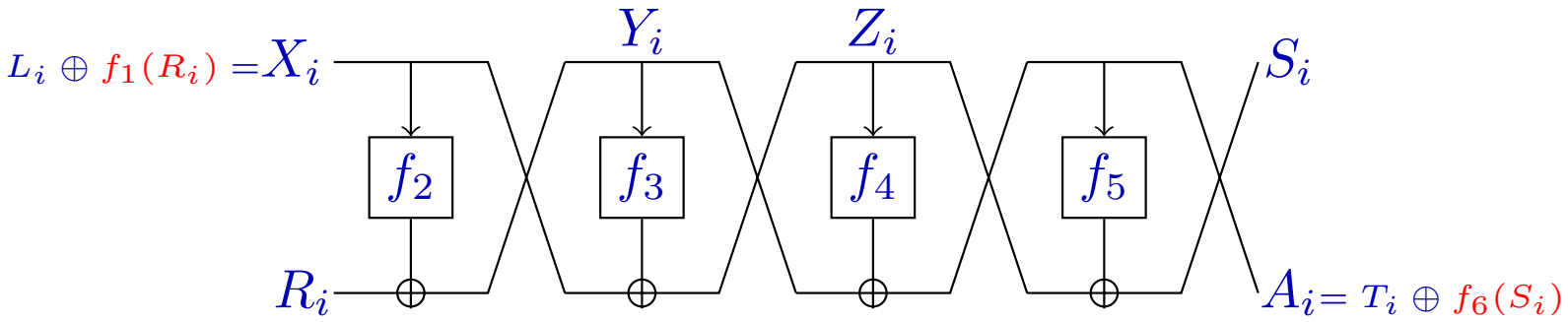


$$\Pr[\boldsymbol{\tau}_{\mathsf{Re}} = \tau] = \frac{N_6(\tau)}{|\mathsf{Func}_n|^6}$$

$$N_6(\tau) := \left|\{(f_1, \cdots, f_6) \in \mathsf{Func}_n^6 : \psi^6(f_1, \cdots, f_6)[L_i, R_i] = [S_i, T_i] \forall i \in [q]\}\right|$$

Security Analysis of 6-round Feistel

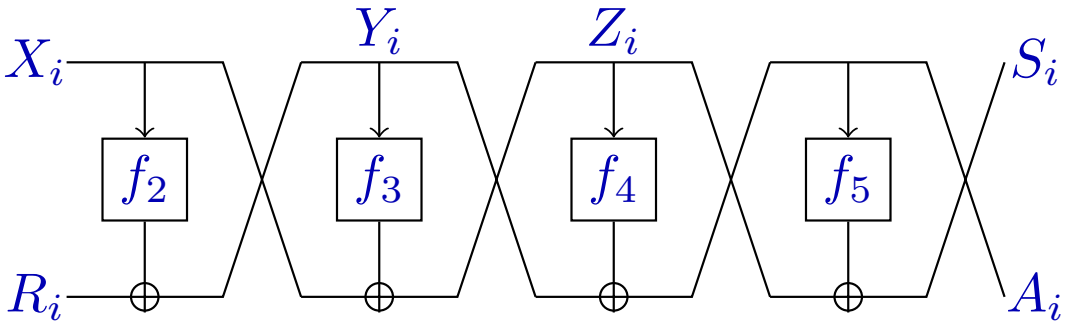
$$\tau' = \{([R_i, X_i], [A_i, S_i]) : i \in [q]\}$$



$$\Pr[\boldsymbol{\tau}_{\mathsf{Re}} = \tau] = \left(\sum_{\substack{f_1, f_6 \\ \leftarrow \$\mathsf{Func}_n}} N_4(\tau') \right) \Big/ |\mathsf{Func}_n|^6$$

$$N_4(\tau') := \left| \{(f_2, \cdots, f_5) \in \mathsf{Func}_n^4 : \psi^4(f_2, \cdots, f_5)[R_i, X_i] = [A_i, S_i] \forall i \in [q]\} \right|$$

Security Analysis of 6-round Feistel



$$\begin{cases} X_i = X_j \implies Y_i \oplus Y_j = R_i \oplus R_j \\ Z_i = Z_j \implies Y_i \oplus Y_j = A_i \oplus A_j \end{cases}$$

$$\begin{cases} A_i = A_j \implies Z_i \oplus Z_j = S_i \oplus S_j \\ Y_i = Y_j \implies Z_i \oplus Z_j = X_i \oplus X_j \end{cases}$$

Security Analysis of 6-round Feistel

Framework $\mathcal{F}$: Collection of equalities on Y and Z variables

$\#(Y^q, Z^q) \in ((\{0,1\}^n)^q)^2$ that satisfy $\mathcal{F} = (2^n)_{q-y_{\mathcal{F}}}(2^n)_{q-z_{\mathcal{F}}} =:$ weight$(\mathcal{F})$.

$$\begin{cases} X_i = X_j \implies Y_i \oplus Y_j = R_i \oplus R_j \\ Z_i = Z_j \in \mathcal{F} \implies Y_i \oplus Y_j = A_i \oplus A_j \\ \text{The only equations } Y_i = Y_j, i < j, \text{ are exactly those implied by } \mathcal{F} \end{cases}$$

$$\begin{cases} A_i = A_j \implies Z_i \oplus Z_j = S_i \oplus S_j \\ Y_i = Y_j \in \mathcal{F} \implies Z_i \oplus Z_j = X_i \oplus X_j \\ \text{The only equations } Z_i = Z_j, i < j, \text{ are exactly those implied by } \mathcal{F} \end{cases}$$

Security Analysis of 6-round Feistel

$$N_4(\tau') = |\mathsf{Func}_n|^4 \sum_{\mathcal{F}} \frac{[\#Y^q \text{ satisfying } (C1)] \cdot [\#Z^q \text{ satisfying } (C2)]}{(2^n)^{4q-x-y_{\mathcal{F}}-z_{\mathcal{F}}-a}}$$

where

$$(C1): \begin{cases} X_i = X_j \implies Y_i \oplus Y_j = R_i \oplus R_j \\ Z_i = Z_j \in \mathcal{F} \implies Y_i \oplus Y_j = A_i \oplus A_j \\ \text{The only equations } Y_i = Y_j, i < j, \text{ are exactly those implied by } \mathcal{F} \end{cases}$$

$$(C2): \begin{cases} A_i = A_j \implies Z_i \oplus Z_j = S_i \oplus S_j \\ Y_i = Y_j \in \mathcal{F} \implies Z_i \oplus Z_j = X_i \oplus X_j \\ \text{The only equations } Z_i = Z_j, i < j, \text{ are exactly those implied by } \mathcal{F} \end{cases}$$

$$x = \#\{i,j\} : X_i = X_j, \ a = \#\{i,j\} : A_i = A_j$$

Security Analysis of 6-round Feistel

$$N_4(\tau') \geq |\mathsf{Func}_n|^4 \sum_{\text{good } \mathcal{F}} \frac{\frac{(2^n)_{q-y_{\mathcal{F}}}}{(2^n)^{x+z_{\mathcal{F}}}} \cdot \frac{(2^n)_{q-z_{\mathcal{F}}}}{(2^n)^{a+y_{\mathcal{F}}}}}{(2^n)^{4q-x-y_{\mathcal{F}}-z_{\mathcal{F}}-a}}$$

where

$$(C1): \begin{cases} X_i = X_j \implies Y_i \oplus Y_j = R_i \oplus R_j \\ Z_i = Z_j \in \mathcal{F} \implies Y_i \oplus Y_j = A_i \oplus A_j \\ \text{The only equations } Y_i = Y_j, i < j, \text{ are exactly those implied by } \mathcal{F} \end{cases}$$

$$(C2): \begin{cases} A_i = A_j \implies Z_i \oplus Z_j = S_i \oplus S_j \\ Y_i = Y_j \in \mathcal{F} \implies Z_i \oplus Z_j = X_i \oplus X_j \\ \text{The only equations } Z_i = Z_j, i < j, \text{ are exactly those implied by } \mathcal{F} \end{cases}$$

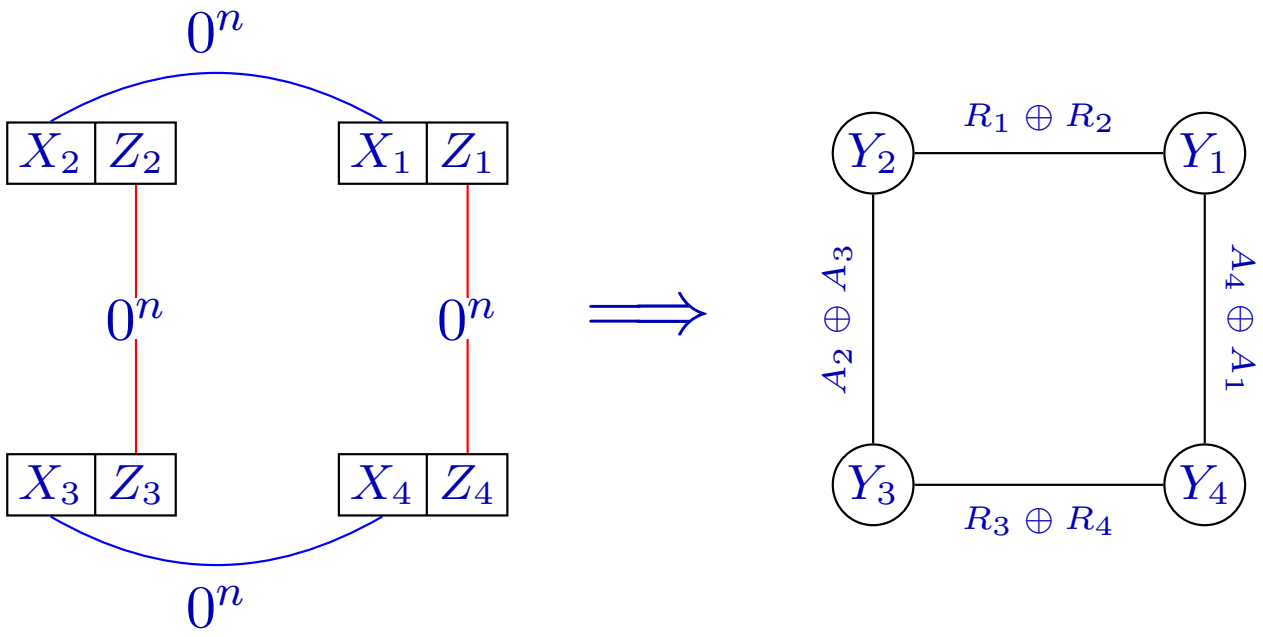
$$x = \#\{i,j\} : X_i = X_j, \ a = \#\{i,j\} : A_i = A_j$$

Security Analysis of 6-round Feistel

$$N_4(\tau') \geq \frac{|\mathsf{Func}_n|^4}{(2^n)^{4q}} \sum_{\text{good } \mathcal{F}} \mathsf{weight}(\mathcal{F})$$

Security Analysis of 6-round Feistel

$$N_4(\tau') \geq \frac{|\mathsf{Func}_n|^4}{(2^n)^{4q}} \Pr[\mathcal{F} \text{ is good}] \sum_{\mathcal{F}} \mathsf{weight}(\mathcal{F})$$



Security Analysis of 6-round Feistel

$$N_4(\tau') \geq \frac{|\mathsf{Func}_n|^4}{(2^n)^{4q}} \left(1 - \frac{8q}{2^n}\right) (2^n)^{2q}$$

Security Analysis of 6-round Feistel

$$\Pr[\boldsymbol{\tau}_{\mathsf{Re}} = \tau] \geq \frac{\sum_{\substack{f_1, f_6 \\ \leftarrow \$ \mathsf{Func}_n}} \frac{|\mathsf{Func}_n|^4}{(2^n)^{2q}} \left(1 - \frac{8q}{2^n}\right)}{|\mathsf{Func}_n^6|}$$

Security Analysis of 6-round Feistel

$$\Pr[\boldsymbol{\tau}_{\mathsf{Re}} = \tau] \geq \frac{1}{(2^n)^{2q}} \left(1 - \frac{8q}{2^n}\right)$$

Security Analysis of 6-round Feistel

$$\frac{\Pr[\boldsymbol{\tau}_{\mathsf{Re}} = \tau]}{\Pr[\boldsymbol{\tau}_{\mathsf{Id}} = \tau]} \geq \frac{\frac{1}{(2^n)^{2q}}\left(1 - \frac{8q}{2^n}\right)}{\frac{1}{\overline{(2^n)_q}}} \geq 1 - \frac{8q}{2^n} - \frac{q^2}{2^{2n}}$$

For $q \leq 2^n/12n^2$,

$$\mathbf{Adv}^{\mathsf{sprp}}_{6LR} \leq \frac{8q}{2^n} + \frac{q^2}{2^{2n}}$$

Open Problems

- non-homogeneous system of non-equations

Open Problems

- non-homogeneous system of non-equations
- groups of exponent $\neq 2$

Open Problems

- non-homogeneous system of non-equations
- groups of exponent $\neq 2$
- $\xi_{\max} > O(2^{n/4}/\sqrt{n})$

Open Problems

- non-homogeneous system of non-equations
- groups of exponent $\neq 2$
- $\xi_{\max} > O(2^{n/4}/\sqrt{n})$
- equations having more than just two variables

Thank You!