



A Compilation of Mirror Theory Concepts

Suprita Talnikar

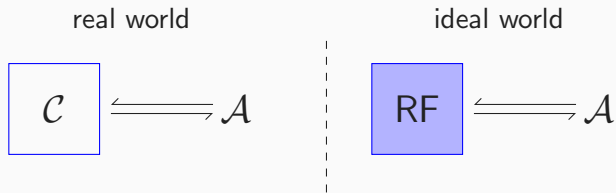
Radboud University (The Netherlands)

August 28, 2024

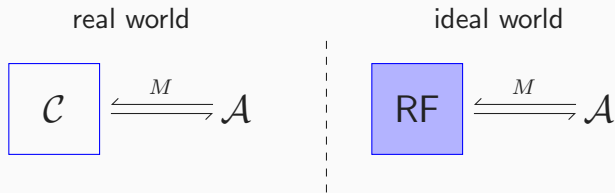


Introduction

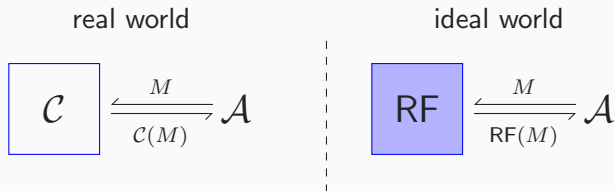
Patarin's Technique:



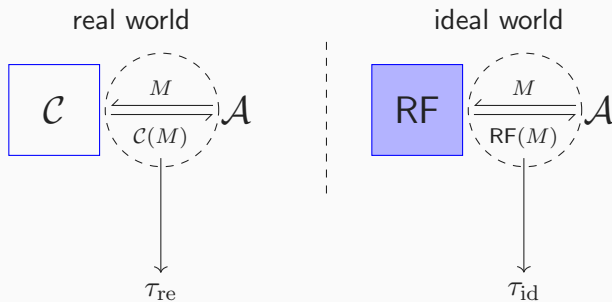
Patarin's Technique:



Patarin's Technique:



Patarin's Technique:



H-Coefficients formula:

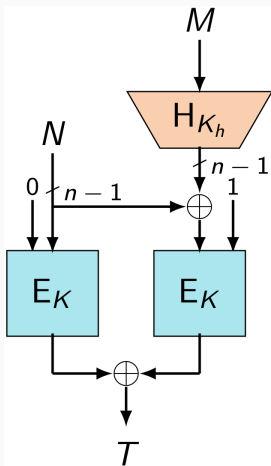
$$\text{For } \mathcal{T}_{\text{good}} \subseteq \mathcal{T}_{\text{id}}, \Delta(\tau_{\text{id}}, \tau_{\text{re}}) \leq \max_{\tau \in \mathcal{T}_{\text{good}}} \frac{\Pr_{\text{re}}[\tau_{\text{re}} = \tau]}{\Pr_{\text{id}}[\tau_{\text{id}} = \tau]}$$

Need a lower bound on $\mathcal{T}_{\text{re}} \cap \mathcal{T}_{\text{good}}$.

It is very convenient to use Mirror Theory for computing the probabilities in this formula!

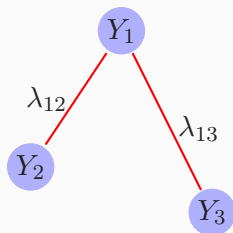
Extending Mirror Theory - I

Nonce-Based Enhanced Hash-then-Mask



- Single-keyed nonce-based variant of EHtM (FSE 2010)
- **MAC security:** $2n/3$ -bit (NR setting)
- Tight $3n/4$ -bit security proved by Choi et. al. in Asiacrypt 2020.
- Security degrades gracefully with repetition of nonce

Mirror Theory: Equations-Inducing Graphs



The system of equations induced by this graph $\mathcal{G} = (V, E, \mathcal{L})$ is:

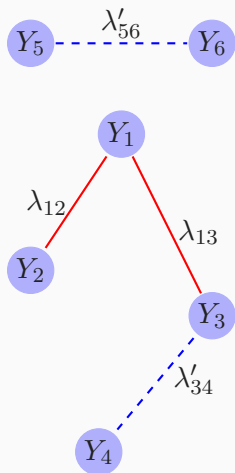
$$Y_1 \oplus Y_2 = \lambda_{12}$$

$$Y_1 \oplus Y_3 = \lambda_{13}$$

Definition

With respect to this system of equations $\mathcal{E}_{\mathcal{G}}$, an injective function $\Phi : V \rightarrow \{0, 1\}^n$ is said to be an *injective solution* if $\Phi(Y_i) \oplus \Phi(Y_j) = \lambda_{ij}$ for all $Y_i, Y_j \in \mathcal{S}$.

Mirror Theory: Equations-and-Non-Equations-Inducing Graphs



The system of equations and non-equations induced by this graph $\mathcal{G} = (V, E_{\text{eq}} \sqcup E_{\text{neq}}, \mathcal{L})$ is:

$$Y_1 \oplus Y_2 = \lambda_{12}$$

$$Y_1 \oplus Y_3 = \lambda_{13}$$

$$Y_3 \oplus Y_4 \neq \lambda'_{34}$$

$$Y_5 \oplus Y_6 \neq \lambda'_{56}$$

Definition

For this system $\mathcal{E}_{\mathcal{G}}$, $\Phi : V \rightarrow \{0, 1\}^n$ is said to be an *injective solution function* if Φ is an injective function such that $\Phi(Y_i) \oplus \Phi(Y_j) = \lambda_{ij}$ for all $Y_i, Y_j \in \mathcal{S}$ and $\Phi(Y_i) \oplus \Phi(Y_j) \neq \lambda'_{ij}$ for all $Y_i, Y_j \in \mathcal{S}'$.

Solutions must be consistent

No restrictions on edge-labels that induce equations

Path Label: The sum of all labels in a path P , denoted $\mathcal{L}(P)$.

Cycle Label: The sum of all labels in a cycle $\mathcal{C}$, denoted $\mathcal{L}(\mathcal{C})$.

Solutions must be consistent

No restrictions on edge-labels that induce equations

Path Label: The sum of all labels in a path P , denoted $\mathcal{L}(P)$.

Cycle Label: The sum of all labels in a cycle $\mathcal{C}$, denoted $\mathcal{L}(\mathcal{C})$.

Good Graph:

- **NC.** The subgraph of $\mathcal{G}$ that induces equations is acyclic

Solutions must be consistent

No restrictions on edge-labels that induce equations

Path Label: The sum of all labels in a path P , denoted $\mathcal{L}(P)$.

Cycle Label: The sum of all labels in a cycle $\mathcal{C}$, denoted $\mathcal{L}(\mathcal{C})$.

Good Graph:

- **NC.** The subgraph of $\mathcal{G}$ that induces equations is acyclic
- **NPL.** for all paths p in graph $\mathcal{G}$, $\mathcal{L}(P) \neq 0$, and

Solutions must be consistent

No restrictions on edge-labels that induce equations

Path Label: The sum of all labels in a path P , denoted $\mathcal{L}(P)$.

Cycle Label: The sum of all labels in a cycle $\mathcal{C}$, denoted $\mathcal{L}(\mathcal{C})$.

Good Graph:

- **NC.** The subgraph of $\mathcal{G}$ that induces equations is acyclic
- **NPL.** for all paths p in graph $\mathcal{G}$, $\mathcal{L}(P) \neq 0$, and
- **NCL.** for all cycles in $\mathcal{G}$ whose edge-set contains exactly one non-equation (dashed) edge $e' \in \mathcal{S}'$, $\mathcal{L}(\mathcal{C}) \neq 0$.

A Theorem on Extended Mirror Theory

- Let $\mathcal{G}$ be a good graph with α vertices.
- Out of the α vertices, q_m vertices induce equations and q_v vertices induce non-equations ($q_m + q_v \geq \alpha$).

A Theorem on Extended Mirror Theory

- Let $\mathcal{G}$ be a good graph with α vertices.
- Out of the α vertices, q_m vertices induce equations and q_v vertices induce non-equations ($q_m + q_v \geq \alpha$).
- The subgraph of $\mathcal{G}$ that induces the *system of equations* has k connected components, the i^{th} component having size w_i .
 $\sigma_i := (w_1 + \dots + w_i)$.

A Theorem on Extended Mirror Theory

- Let $\mathcal{G}$ be a good graph with α vertices.
- Out of the α vertices, q_m vertices induce equations and q_v vertices induce non-equations ($q_m + q_v \geq \alpha$).
- The subgraph of $\mathcal{G}$ that induces the *system of equations* has k connected components, the i^{th} component having size w_i .
 $\sigma_i := (w_1 + \dots + w_i)$.
- **Required:** The minimum number of injective solutions to the induced systems of equations and non-equations from a set of size $2^n - c$.

This number is: $(2^n)_\alpha \left(1 - \sum_{i=1}^k \frac{6\sigma_{i-1}^2 \binom{w_i}{2}}{2^{2n}} - \frac{2(q_v + c\alpha)}{2^n} \right),$
provided $\sigma_k w_{\max} \leq 2^n/4$.

**The real world system of authentication equations $\mathcal{E}_m$
and verification non-equations $\mathcal{E}_v$ are:**

$$\begin{array}{ll} \pi(\hat{N}_1) \oplus \pi(\hat{X}_1) = T_1 & \pi(\hat{N}'_1) \oplus \pi(\hat{X}'_1) \neq T'_1 \\ \pi(\hat{N}_2) \oplus \pi(\hat{X}_2) = T_2 & \pi(\hat{N}'_2) \oplus \pi(\hat{X}'_2) \neq T'_2 \\ & \vdots \\ \pi(\hat{N}_{q_m}) \oplus \pi(\hat{X}_{q_m}) = T_{q_m} & \pi(\hat{N}'_{q_m}) \oplus \pi(\hat{X}'_{q_m}) \neq T'_{q_m} \end{array}$$

Here, the $\hat{}$ symbol is used as shorthand notation for indicating an injective function mapping the variable N or X to $\Phi(N)$ or $\Phi(X)$ (respectively).

Choi et al., Asiacrypt 2020:

- For positive integers m, q_m and nonnegative integers v, q_v , let $\mathcal{G} = (V, E_{\text{eq}} \sqcup E_{\text{neq}}, \mathcal{L})$ be a good graph such that $|E_{\text{eq}}| = m$ involving q_m vertices and $|E_{\text{neq}}| = v$ involving q_v vertices (hence, $\alpha \leq q_m + q_v$).
- Let $\mathcal{G}_{\text{eq}}$ be divided into four subgraphs,
 - $\mathcal{G}_0 := (V_0, E_0)$ being the set of isolated vertices,
 - $\mathcal{G}_1 := (V_1, E_1)$ being the union of components of size two (i.e. trails of length one),
 - $\mathcal{G}_2 := (V_2, E_2)$ being the union of components containing at least one trail of length two, but not a trail of length three, and
 - $\mathcal{G}_3 := (V_3, E_3)$ being the union of components containing at least one trail of length three.
- Suppose that $\mathcal{G}_2$ can be decomposed into k components $\mathcal{C}_1, \dots, \mathcal{C}_k$.

Choi et al., Asiacrypt 2020:

Then number of solutions to $\mathcal{G}$, denoted $h(\mathcal{G})$, satisfies:

$$\begin{aligned} \frac{h(\mathcal{G})2^{nq_m}}{(2^n)^{|\mathbf{V}|}} &\geq 1 - \frac{|\mathbf{V}_3|^4}{2^{2n}} - \frac{(|\mathbf{V}_3| + |\mathbf{V}_2|)^2}{2^{2n}} \sum_{i=1}^k |\mathcal{C}_i|^2 \\ &\quad - \frac{8(|\mathbf{V}_3| + |\mathbf{V}_2|)q_m^2}{2^{2n}} \\ &\quad - \frac{18q_m^2}{2^{2n}} - \frac{16q_m^4}{2^{3n}} - \frac{2q_v}{2^n} - \frac{16q_mq_v}{2^{2n}}, \end{aligned}$$

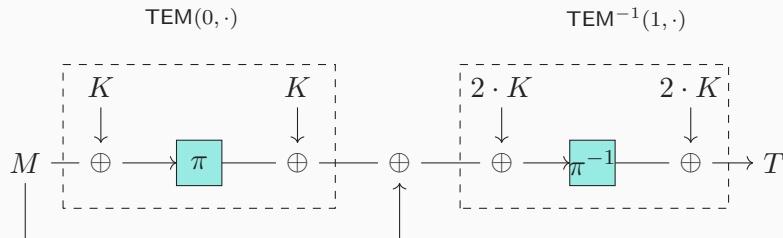
provided that $q_m \leq 2^{n-3}$.

Thus, the bound is improved to $3n/4$ bits.

Also, $\xi_{\max}$ increased to 4.

Extending Mirror Theory - II

Permutation-Based Davies-Meyer MAC



- Single-keyed, single permutation-based MAC
- Variable-length messages incorporated through a hash function, in PDM*MAC
- Uses Tweakable Evan-Mansour (TEM).
- **PRF security:** $2n/3$ -bits.
- Inverse-free instantiation in pEDM, ToSC 2021.

A Corollary on Extended Mirror Theory

- Let $\mathcal{G}_{\text{eq,neq}} = (V, E_{\text{eq}} \sqcup E_{\text{neq}}, \mathcal{L})$ be a good graph.
- Suppose the subgraph $\mathcal{G}_{\text{eq}}$ (inducing equations) only has components of size 2 or 3 (therefore, $\xi_i = 2$ or $\xi_i = 3 \ \forall i$).
- If the number of vertices involved in only non-equations is $|V \setminus V_{\text{eq}}| = q_v$ and
- $\lambda_i (i \in [q_m])$ are edge-labels of the edges in the equations-inducing subgraph E_{eq} in the same order as the components,
- **then** the probability of the induced systems of equations and non-equations attaining any solution
- from a set $S' \subseteq \{0,1\}^n$ of size $(2^n - p')$ for all the variables represented only by the vertices in V_{eq} is bounded by-

$$\frac{1}{2^{nq_m}} \left(1 - \frac{1200q_m^3 + 312(p' + 3q_v)q_m^2 + 2(p' + 3q_v)^2q_m}{2^{2n}} \right) \left(1 - \frac{q_v}{2^n} \right).$$

The real world system of equations is:

Construction equations:

$$\pi(M_1 \oplus K) \oplus \pi(T_1 \oplus 2K) = 3K \oplus M_1$$

$$\vdots$$

$$\pi(M_q \oplus K) \oplus \pi(T_q \oplus 2K) = 3K \oplus M_q$$

Queries to primitive π :

$$\pi(\tilde{u}_1) = \tilde{v}_1$$

$$\vdots$$

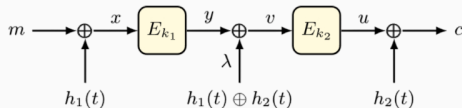
$$\pi(\tilde{u}_p) = \tilde{v}_p$$

Thus, $M_i \oplus K$ or $T_i \oplus 2K$ is mapped (injectively) to $\Phi(M_i)$ or $\Phi(T_i)$, respectively.

The security bound for PDMMAC (and its variants)
is therefore of the order of $2n/3$ bits.

Extending Mirror Theory - III

Towards Tight Security of Cascaded LRW2, Mennink (TCC 2018), Tight Security of Cascaded LRW2, Jha et al. (JoC 2020)



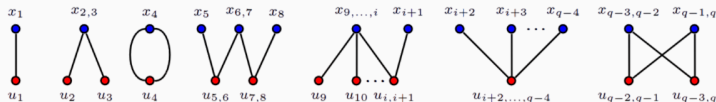
System of Equations:

$$Y_1 \oplus V_1 = \lambda_1$$

$$Y_2 \oplus V_2 = \lambda_2$$

$\vdots$

$$Y_q \oplus V_q = \lambda_q$$



Bipartite graphs induce transcripts for a 2-round instantiation of CLRW2.

Jha et al. prove a tight security bound of up to $q \approx 2^{\frac{3n}{4} - 1.43}$ queries. using the following theorem on Mirror Theory:

- Consider a system of linear equations as described in the previous slide with $q < 2^{n-2}$ and $\xi_{\max} q \leq 2^{n-1}$, and the graph $\mathcal{G}$ inducing it.
- Partition the components of $\mathcal{G}$ as
 - c_1 isolated vertices, corresponding to $q_1 (= c_1)$ equations in the system,
 - c_2 *stars* with centers corresponding to the variables Y_i , corresponding to q_2 equations in the system, and
 - c_3 *stars* with centers corresponding to the variables V_i , corresponding to q_3 equations in the system.
- Then the number of tuples $(Y_1, Y_2, \dots, Y_q, V_1, V_2, \dots, V_q)$ such that $Y_i \neq Y_j$ and $V_i \neq V_j$ for $i \neq j$
- that satisfy this system of equations, denoted h_q , is at least:

$$\left(1 - \frac{13q^4}{2^{3n}} - \frac{2q^2}{2^{2n}} - \left(\sum_{i=1}^{c_2+c_3} \frac{4q^2}{2^{2n}}\right)\right) \times \frac{(2^n)_{q_1+c_2+q_3} (2^n)_{q_1+q_2+c_3}}{\prod_{\lambda' \in \hat{\lambda}^q} (2^n)_{\mu(\lambda^q, \lambda')}} \quad (1)$$

Extending Mirror Theory - IV

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

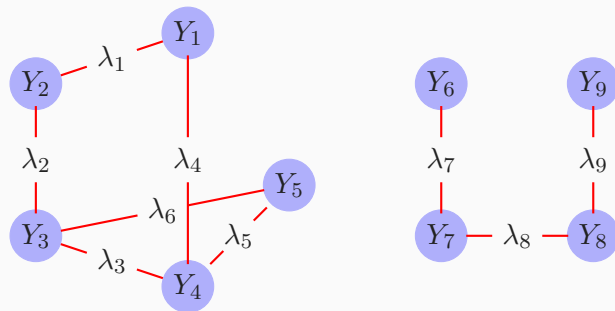
- Cogliati et al., Eurocrypt 2024.

Revisiting Systems of Bivariate Affine Equations

$$Y_1 \oplus Y_2 = \lambda_1 \quad Y_1 \oplus Y_4 = \lambda_4 \quad Y_6 \oplus Y_7 = \lambda_7$$

$$Y_2 \oplus Y_3 = \lambda_2 \quad Y_4 \oplus Y_5 = \lambda_5 \quad Y_7 \oplus Y_8 = \lambda_8$$

$$Y_3 \oplus Y_4 = \lambda_3 \quad Y_3 \oplus Y_5 = \lambda_6 \quad Y_8 \oplus Y_9 = \lambda_9$$

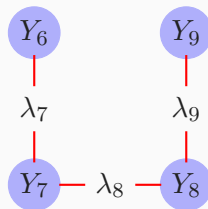
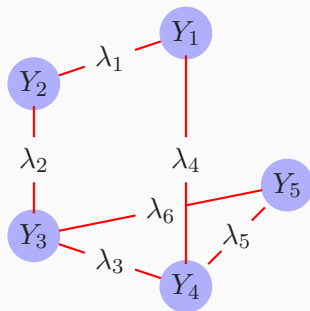


Revisiting Systems of Bivariate Affine Equations

$$Y_1 \oplus Y_2 = \lambda_1 \quad Y_1 \oplus Y_4 = \lambda_4 \quad Y_6 \oplus Y_7 = \lambda_7$$

$$Y_2 \oplus Y_3 = \lambda_2 \quad Y_4 \oplus Y_5 = \lambda_5 \quad Y_7 \oplus Y_8 = \lambda_8$$

$$Y_3 \oplus Y_4 = \lambda_3 \quad Y_3 \oplus Y_5 = \lambda_6 \quad Y_8 \oplus Y_9 = \lambda_9$$

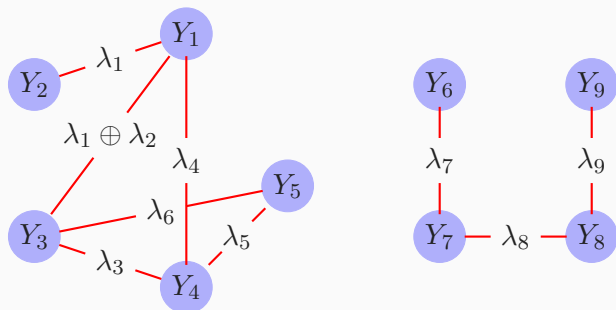


If we assign a value to one variable, the values of all the variables in its component get determined.

The size of largest component is denoted $\xi_{\max}$.

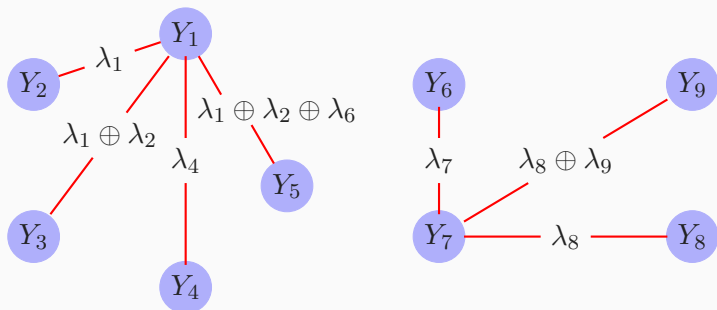
Simplifying:

$$\begin{array}{lll} Y_1 \oplus Y_2 = \lambda_1 & Y_1 \oplus Y_4 = \lambda_4 & Y_6 \oplus Y_7 = \lambda_7 \\ Y_1 \oplus Y_3 = \lambda_1 \oplus \lambda_2 & Y_4 \oplus Y_5 = \lambda_5 & Y_7 \oplus Y_8 = \lambda_8 \\ Y_3 \oplus Y_4 = \lambda_3 & Y_3 \oplus Y_5 = \lambda_6 & Y_8 \oplus Y_9 = \lambda_9 \end{array}$$

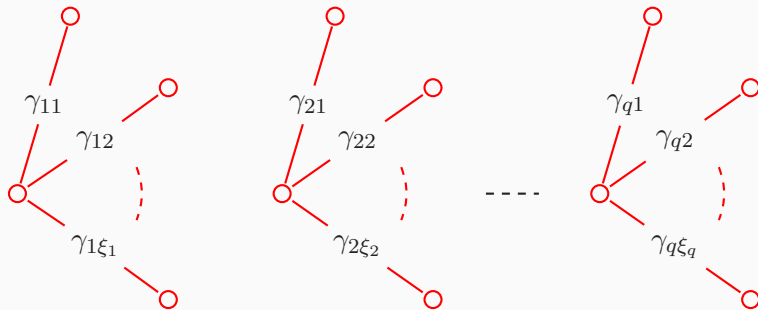


Standard form of the system:

$$\begin{array}{lll} Y_1 \oplus Y_2 = \lambda_1 & Y_1 \oplus Y_4 = \lambda_4 & Y_6 \oplus Y_7 = \lambda_7 \\ Y_1 \oplus Y_3 = \lambda_1 \oplus \lambda_2 & Y_1 \oplus Y_5 = \lambda_1 \oplus \lambda_2 \oplus \lambda_6 & Y_7 \oplus Y_8 = \lambda_8 \\ & & Y_7 \oplus Y_9 = \lambda_8 \oplus \lambda_9 \end{array}$$

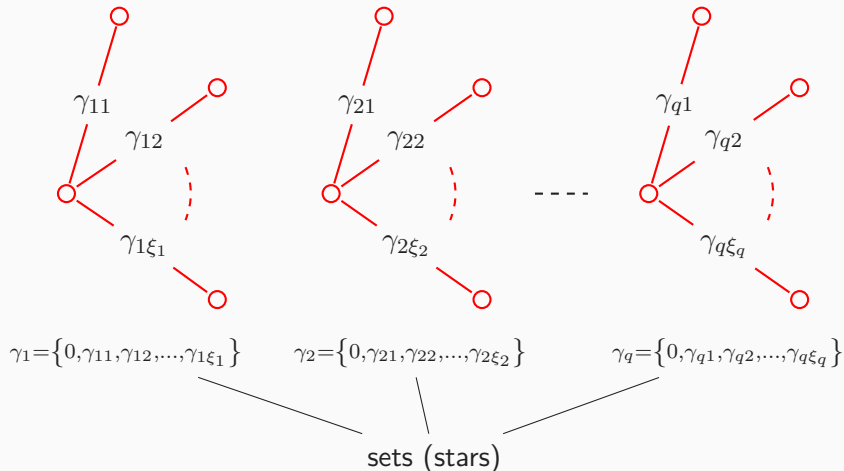


Generating Solutions for a System of Equations



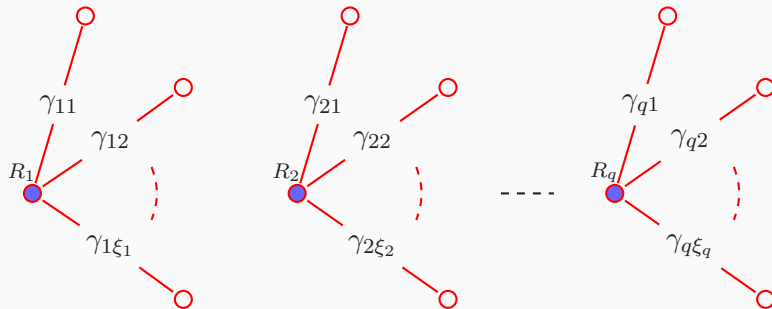
Generating Solutions for a System of Equations

$\gamma = \{\gamma_1, \gamma_2, \dots, \gamma_q\}$ – set system (galaxy of stars)



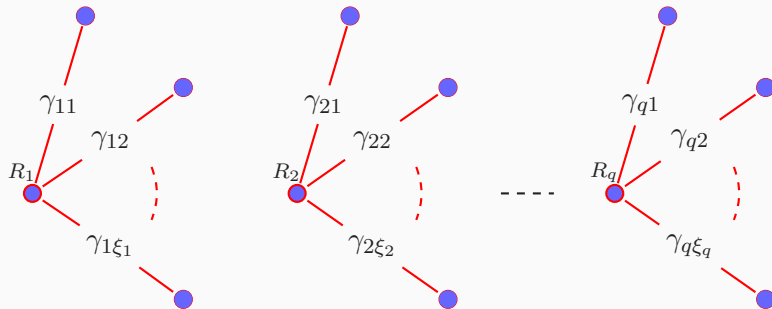
Generating Solutions for a System of Equations

$$R_1, R_2, \dots, R_q \stackrel{\$}{\leftarrow} \{0, 1\}^n$$



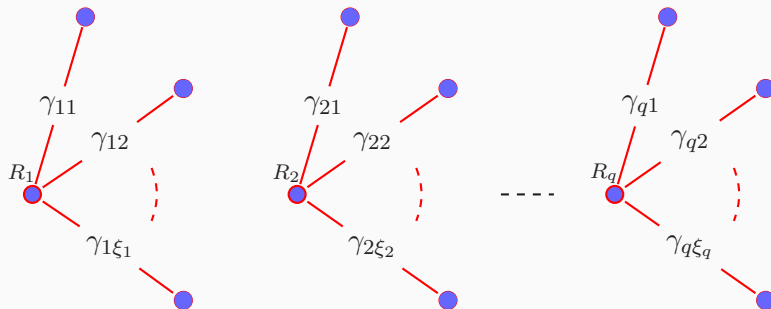
Generating Solutions for a System of Equations

$$R_1, R_2, \dots, R_q \stackrel{\$}{\leftarrow} \{0, 1\}^n$$



Generating Solutions for a System of Equations

$$R_1, R_2, \dots, R_q \stackrel{\$}{\leftarrow} \{0, 1\}^n$$



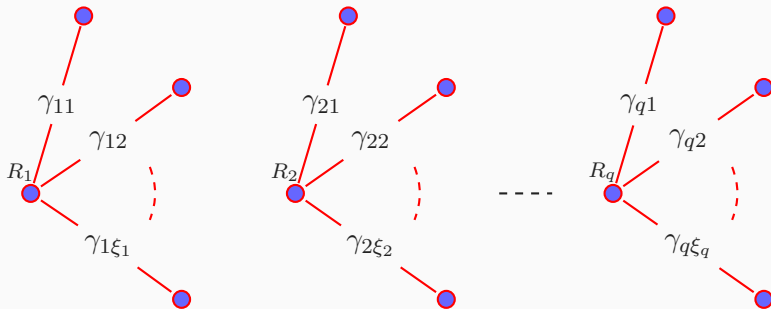
The probability of obtaining a particular solution

$(x_{11}, \dots, x_{1\xi_1}, x_{21}, \dots, x_{2\xi_2}, \dots, x_{q1}, \dots, x_{q\xi_q})$ to the system of equations is

$$\Pr[R_1=x_{11}, R_2=x_{21}, \dots, R_q=x_{q1}] = 2^{-nq}.$$

Generating Solutions for a System of Equations

$$R_1, R_2, \dots, R_q \stackrel{\$}{\leftarrow} \{0, 1\}^n$$

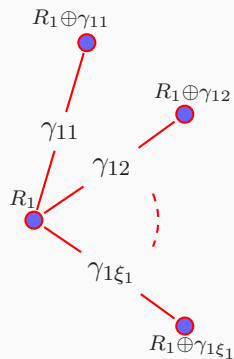


Disjointness Event:

$\text{Disj}(\gamma) := \gamma_1 \oplus R_1, \gamma_2 \oplus R_2, \dots, \gamma_q \oplus R_q$ are disjoint

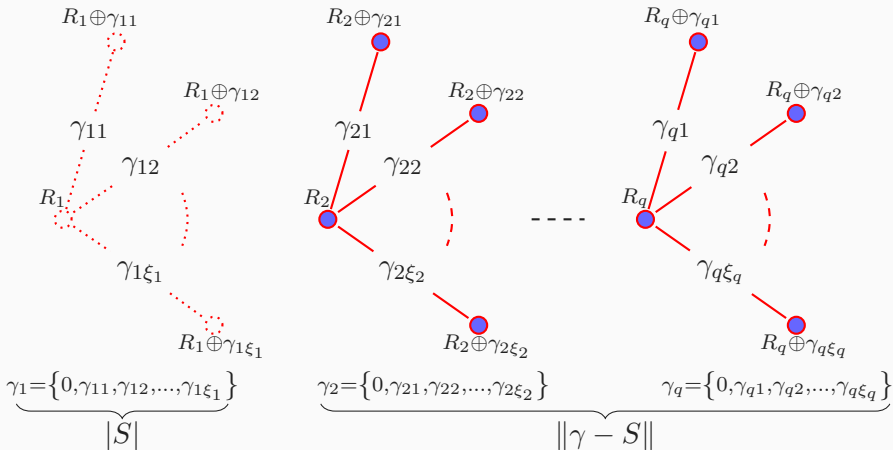
$$P(\gamma) = \frac{\# \text{ pairwise distinct solutions}}{2^{nq}}$$

If there is just one star, $P(\gamma) = 1$:



Removing star S from a galaxy: $\gamma \rightarrow \gamma - S$

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

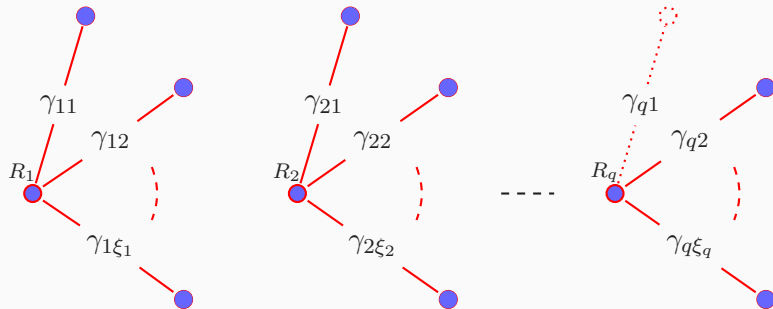


Iterating this inequality
i.e. removing stars from the galaxy one-by-one, we get

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

Birthday Bound!!

So instead of removing an entire star, we only remove one link.



Theorem

- Consider a set system $\gamma = (\gamma_1, \gamma_2, \dots, \gamma_q)$,
- with $\|\gamma\| := \sum_i |\gamma_i| = v$ and $\|\gamma\|_{\max} := \max_i |\gamma_i| = \xi_{\max}$.
- If $v \leq 2^{n/2}$ or $\xi_{\max} + n\xi_{\max}^2 \leq 2^{n/2}$,
- and $1 \leq v \leq \frac{2^n}{12\xi_{\max}^2}$,
- then $P(\gamma) \geq \frac{(2^n)_v}{2^{nv}}$.

$$\text{Therefore, } \# \text{ pairwise distinct solutions } \geq \frac{(2^n)_v}{2^{nv}} \cdot 2^{nq} = \frac{(2^n)_v}{2^{ne}}.$$

Here, v is the number of vertices (i.e. the number of variables), and e the number of edges (i.e. the number of equations) in the graph (system of equations).

Thank you for your attention!