Computer Science and Information Engineering
National Chi Nan University

The Principle and Application of Secret Sharing

Dr. Justie Su-Tzu Juan

Lecture 5. Perfect SSS for Graph-Based Structure

§ 5.1 Perfect Secret Sharing Schemes

Slides for a Course Based on

Y.-F. Weng "A Study of Perfect Secret Sharing Scheme", Master Thesis of Department of SCIE, National Chi Nan University, 2006.

§ 5.1 Perfect Secret Sharing Schemes

- **Def:**
  - Let $\mathcal{K}$ be the master key space and $\mathcal{S}_i$ be the share space for participant i. The *information rate* ρ of the secret sharing scheme is defined as $\rho = \min_i \log_2|\mathcal{K}| / \log_2|\mathcal{S}_i|$.
  - A secret sharing scheme is *ideal* if $\rho = 1$.
  - The *minimal access structure* $\Gamma_0 = \{A \in \Gamma: A' \not\subset A \text{ for all } A' \in \Gamma - \{A\}\}$.
  - The *maximal prohibited structure* $\Delta_1 = \{B \in \Delta: B \not\subset B' \text{ for all } B' \in \Gamma - \{B\}\}$.

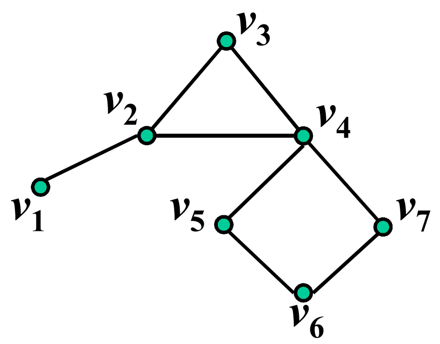
$P = \{P_1, P_2, P_3\}$

$\Gamma = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_2, P_3\}\}$ — Γ_0: $\{P_1, P_2\}, \{P_1, P_3\}$

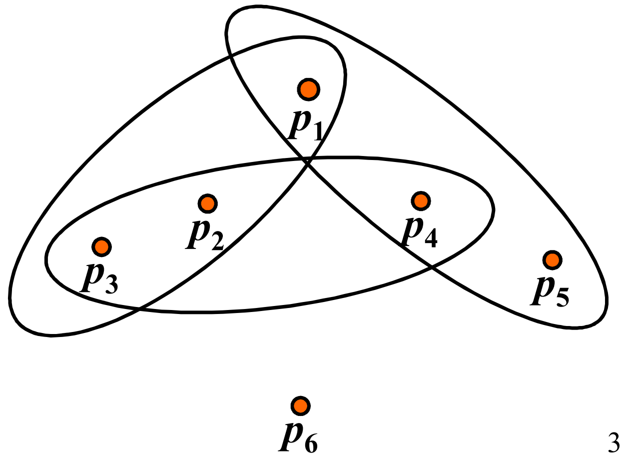
$\Delta = \{\{P_1\}, \{P_2\}, \{P_3\}, \{P_1, P_2\}\}$ — Δ_0: $\{P_3\}, \{P_1, P_2\}$

§ 5.1 Perfect Secret Sharing Schemes

- **Def:**
- Graph $G = (V, E)$
  - $E = \{e_1, e_2, \ldots, e_\varepsilon\}$ and $e_i = \{u, v\}$ where $u, v \in V$, $1 \le i \le \varepsilon$



- Hypergraph $H = (V, E)$
  - $E = \{E_1, E_2, \ldots, E_{|E|}\}$ and $|E_i| \ge 2$, $1 \le i \le |E|$
  - *r*-uniform Hypergraph:
    - $\forall |E_i| = r$, $1 \le i \le |E|$



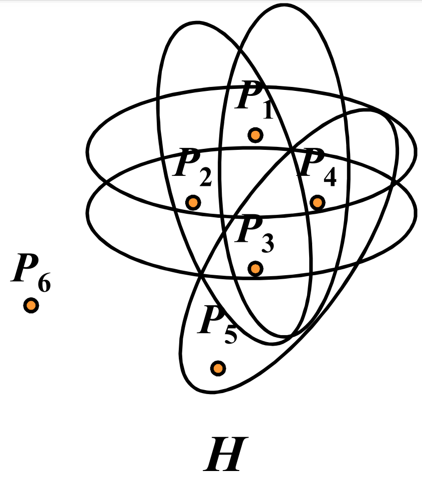
§ 5.1 Perfect Secret Sharing Schemes

- **Related works:**
- Perfect SSS for graph-based prohibited structure (Type II)
  - SS scheme(1997)
    - Sun, Shieh
  - Sun's scheme (1999)

- Perfect SSS for general access structure
  - Tochikubo's scheme (2004) (Type I)
  - TUM scheme (2005) (Type II)
    - Tochikubo, Uyematsu, Matsumoto

§ 5.1 Perfect Secret Sharing Schemes

- ***r*-uniform hypergraph-based prohibited structure**
  - *r*-uniform hypergraph $H = (V, E)$
    - $V(H) = P$ and $|P| = n$
    - $\Delta = \{A: A \subseteq P \text{ and } |A| \leq r - 1\} \cup E(H)$
    - $\Gamma = \{A: A \subseteq P \text{ and } |A| \geq r + 1\} \cup \{A: A \notin E(H) \text{ and } |A| = r\}$



  - Weng and Juan'
  - Weng and Juan
  - Weng, Juan anc

$P = \{p_1, p_2, p_3, p_4, p_5, p_6\}$

$\Delta = \{A: A \subseteq P \text{ and } |A| \leq 2\} \cup E(H)$

$= \{\phi, \{p_1\}, \{p_2\}, \{p_3\}, \{p_4\}, \{p_5\}, \{p_6\}, \{p_1, p_2\}, \{p_1, p_3\}, \{p_1, p_4\}, \{p_1, p_5\}, \{p_1, p_6\}, \{p_2, p_3\}, \{p_2, p_4\}, \{p_2, p_5\}, \{p_2, p_6\}, \{p_3, p_4\}, \{p_3, p_5\}, \{p_3, p_6\}, \{p_4, p_5\}, \{p_4, p_6\}, \{p_5, p_6\}, \{p_1, p_2, p_3\}, \{p_1, p_2, p_4\}, \{p_1, p_3, p_4\}, \{p_2, p_3, p_4\}, \{p_3, p_4, p_5\}\}$

$\Gamma = \{A: A \subseteq P \text{ and } |A| \geq 4\} \cup \{\{p_1, p_2, p_5\}, \{p_1, p_2, p_6\}, \{p_1, p_3, p_5\}, \{p_1, p_3, p_6\}, \{p_1, p_4, p_5\}, \{p_1, p_4, p_6\}, \{p_1, p_5, p_6\}, \{p_2, p_3, p_5\}, \{p_2, p_3, p_6\}, \{p_2, p_4, p_5\}, \{p_2, p_4, p_6\}, \{p_2, p_5, p_6\}, \{p_3, p_4, p_6\}, \{p_3, p_5, p_6\}, \{p_4, p_5, p_6\}\}$

§ 5.1 Perfect Secret Sharing Schemes

- *r*-uniform hypergraph-based prohibited structure

	Sun-Shieh (1997)	Sun (1999)	Tochikubo (2004)	TUM (2005)
extend	*r*-HP1 3-1	*r*-HP2 4-1		I-TUM 6-2
VD	*r*-VDHP1 3-2	*r*-VDHP2 4-2	VDT 5-2	VDTUM
M	*r*-MHP1 3-3	*r*-MHP2 4-3	MT 5-3	MITUM 6-3
VDM	*r*-VDMHP1 3-4	*r*-VDMHP2 4-4	VDMT 5-4	VDMITUM 6-4

Computer Science and Information Engineering
National Chi Nan University

The Principle and Application of Secret Sharing

Dr. Justie Su-Tzu Juan

Lecture 5. Perfect SSS for Graph-Based Structure

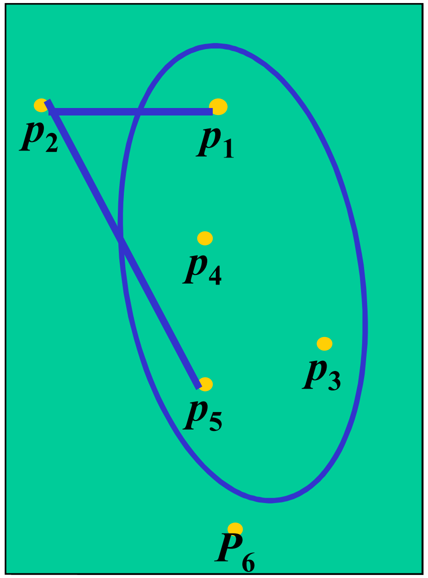
§ 5.2 Hypergraph-based SSS for General Access Structures

Slides for a Course Based on

Y.-C. Wang "Using Hypergraph to Design Perfect Secret Sharing Schemes for General Access Structures", Master Thesis of Department of SCIE, National Chi Nan University, 2007.

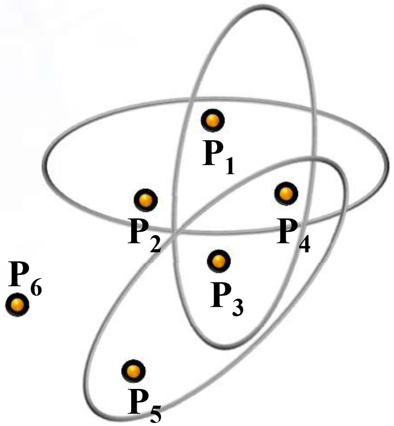
§ 5.2 Hypergraph-based SSS for General Access Structures

- **Hypergraph**
  - r-uniform hypergraph
    - $r = 2$: graph
    - $r > 2$
  - (r_1, r_2)-uniform hypergraph
  - (r_1, r_2, r_3)-uniform hypergraph
  - General hypergraph
- **Hypergraph-based Access structure**
  - $\Gamma = \{A \subseteq P: S \subseteq A \text{ for any } S \in \Delta_0\}$
  - $\Delta = 2^P \setminus \Gamma = \{A \subseteq P: S \not\subset A \text{ for all } S \in \Delta_0\}$.

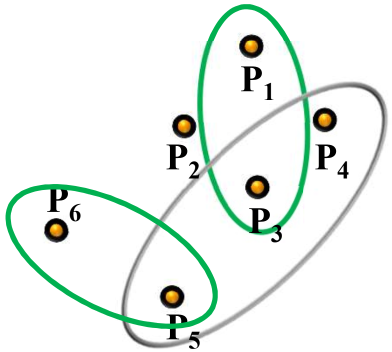


§ 5.2 Hypergraph-based SSS for General Access Structures

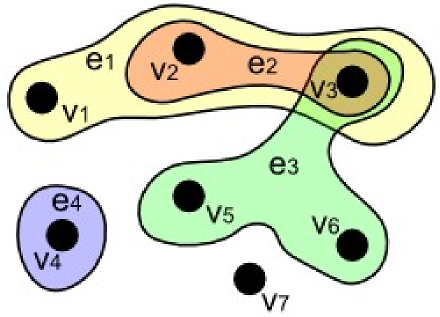
- **Hypergraph $H = (V, E)$**
  - ***r*-Uniform Hypergraph**
  - **(r_1, r_2)-Uniform Hypergraph**
  - **General Hypergraph**



3-Uniform Hypergraph



(2, 3)-Uniform Hypergraph



General Hypergraph

Source: Wikipedia

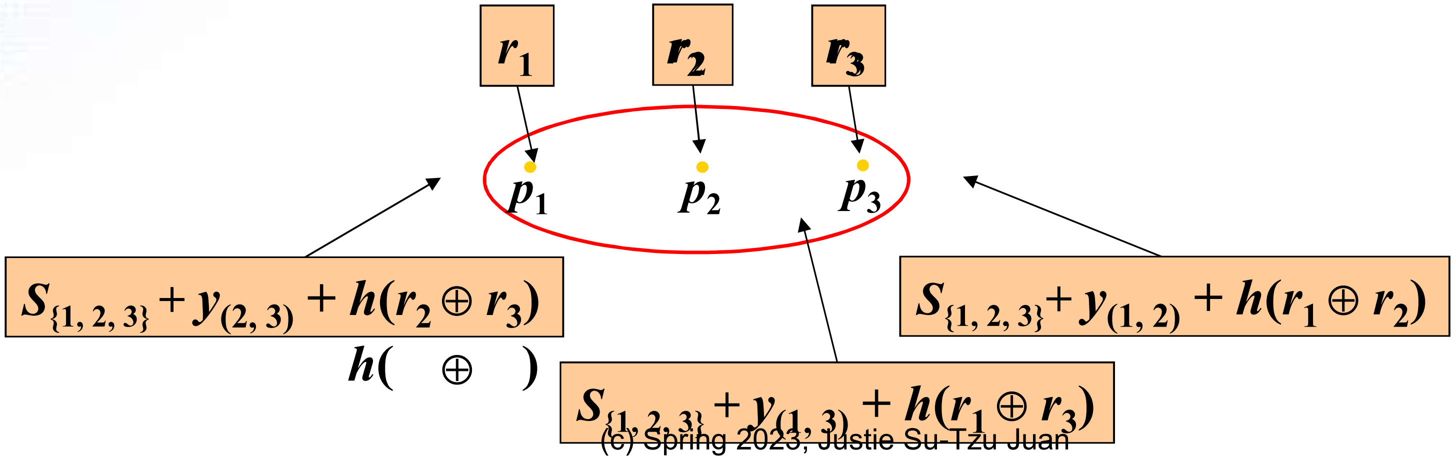
§ 5.2 Hypergraph-based SSS for General Access Structures

- r-HA Scheme (2007)
  Structures
- (r_1, r_2)-HA Scheme (2007)
  Access Structures
- (r_1, r_2, r_3)-HA Scheme
  Based Access Structures
- G-HA Scheme
  - G-VDHA Scheme
  - G-MHA Scheme
  - G-VDMHA Scheme

§ 5.2 Hypergraph-based SSS for General Access Structures

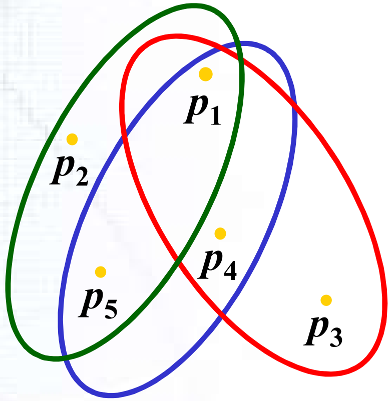
- ***r*-HA Scheme - Idea**
- 3-Uniform Hypergraph
  - $K = (K_1, K_0) \in Z_q \times Z_q$
  - $f(x) = k_2 x^2 + K_1 x + K_0 \pmod{q}$
  - $\boldsymbol{y_{(i,j)} = f(i \cdot n + j)}$
  - h : a one-way hash function

$$S_{\{1,2,3\}} = y_{(1,2)} + h(r_1 \oplus r_2) + y_{(2,3)} + h(r_2 \oplus r_3) + y_{(1,3)} + h(r_1 \oplus r_3)$$



§ 5.2 Hypergraph-based SSS for General Access Structures

- **Ex:**



S_1	S_2
r_1	r_2
$S_{\{1,2,5\}} + y_{(2,5)} + h(r_2 \oplus r_5)$	$S_{\{1,2,5\}} + y_{(1,5)} + h(r_1 \oplus r_5)$
$S_{\{1,3,5\}} + y_{(3,4)} + h(r_3 \oplus r_4)$	–
$S_{\{1,4,5\}} + y_{(4,5)} + h(r_4 \oplus r_5)$	–

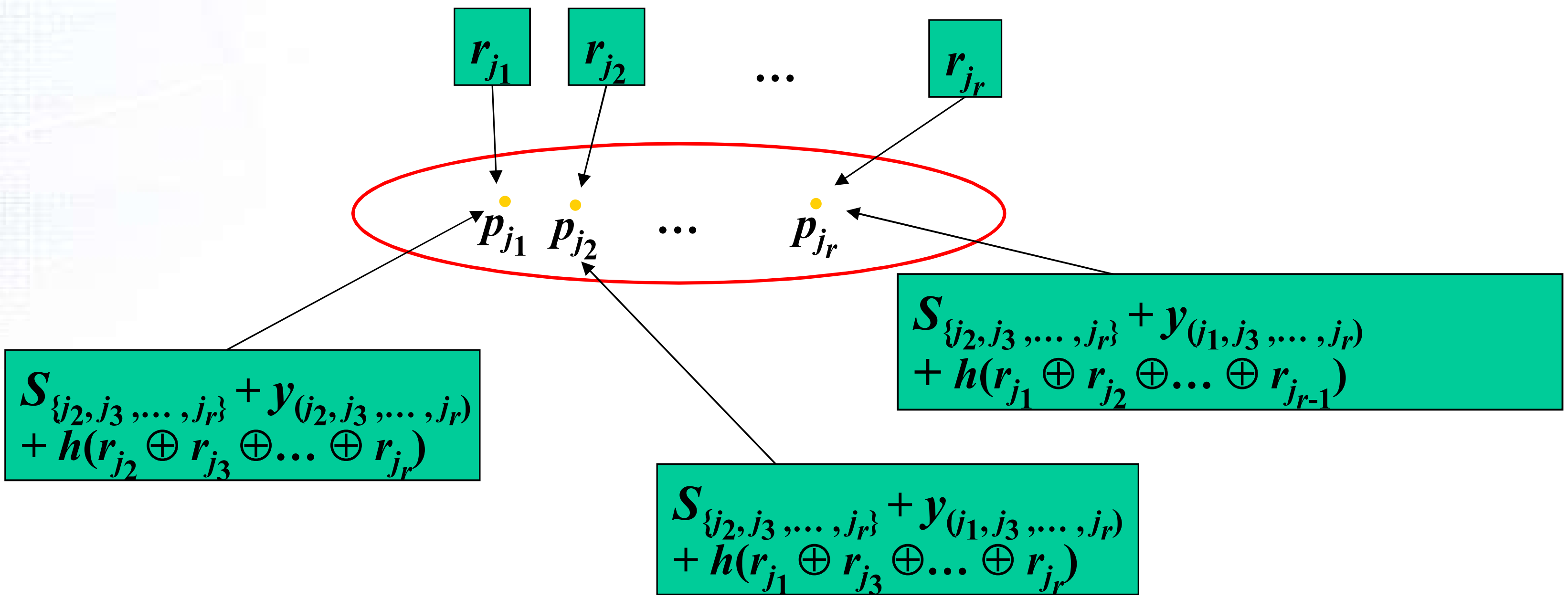
S_3	S_4	S_5
r_3	r_4	r_5
–	–	$S_{\{1,2,5\}} + y_{(1,2)} + h(r_1 \oplus r_2)$
$S_{\{1,3,5\}} + y_{(1,4)} + h(r_1 \oplus r_4)$	$S_{\{1,3,5\}} + y_{(1,3)} + h(r_1 \oplus r_3)$	–
	$S_{\{1,4,5\}} + y_{(1,5)} + h(r_1 \oplus r_5)$	$S_{\{1,4,5\}} + y_{(1,4)} + h(r_1 \oplus r_4)$

$$S_{\{1,2,5\}} = y_{(1,2)} + h(r_1 \oplus r_2) + y_{(2,5)} + h(r_2 \oplus r_5) + y_{(1,5)} + h(r_1 \oplus r_5)$$

…

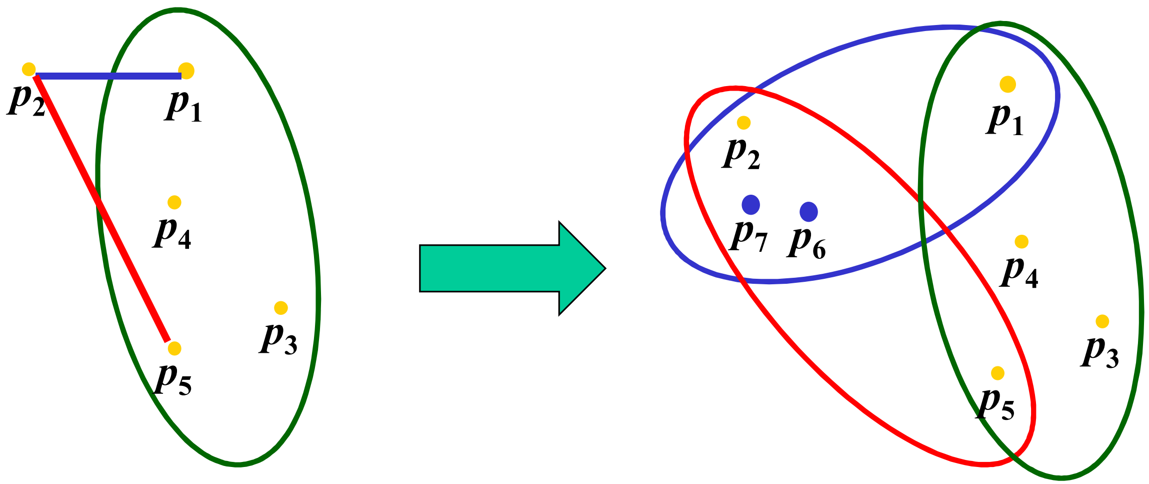
§ 5.2 Hypergraph-based SSS for General Access Structures

- $f(x) = k_{r-1}x^{r-1} + \dots + k_2x^2 + K_1x + K_0 \pmod{q}$
  - $y_{(i_1, i_2, \dots, i_{r-1})} = f\left(\sum_{i=1}^{r-1} i_k\, n^{r-k-1}\right)$

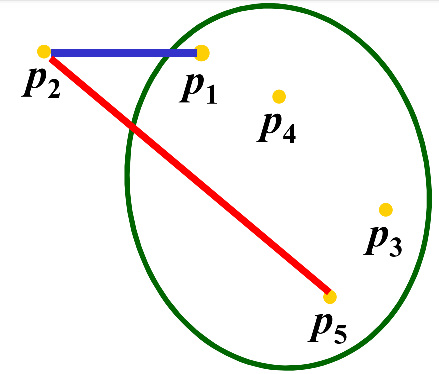


§ 5.2 Hypergraph-based SSS for General Access Structures

- **(r_1, r_2)-HA Scheme – Idea**
  - (2, 4)-HA Scheme

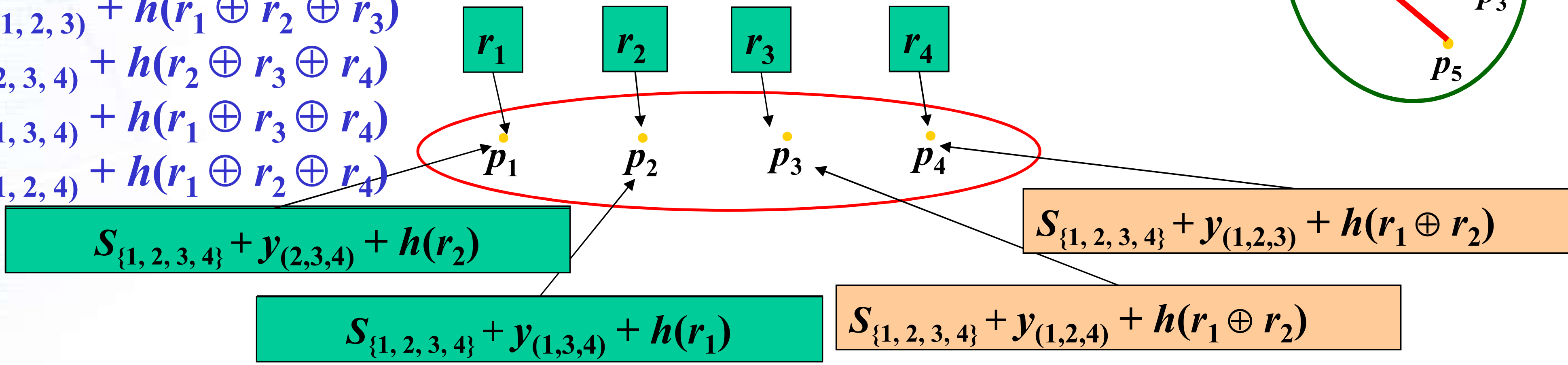


§ 5.2 Hypergraph-based SSS for General Access Structures



- **(r_1, r_2)-HA Scheme**
  - (2, 4)-HA Scheme

$$S_{\{1,2,3,4\}} = y_{(1,2,3)} + h(r_1 \oplus r_2 \oplus r_3) + y_{(2,3,4)} + h(r_2 \oplus r_3 \oplus r_4) + y_{(1,3,4)} + h(r_1 \oplus r_3 \oplus r_4) + y_{(1,2,4)} + h(r_1 \oplus r_2 \oplus r_4)$$

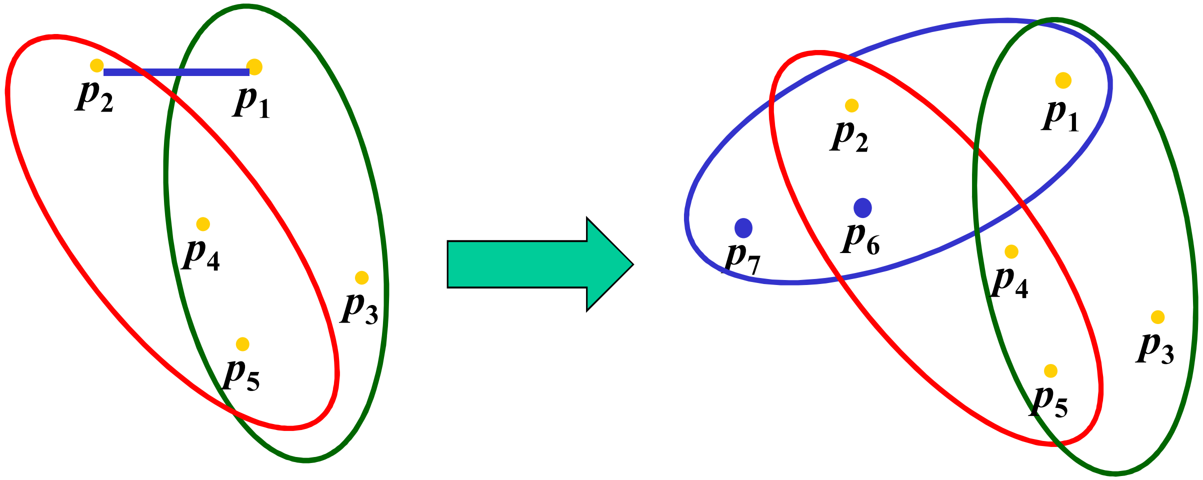


S_1	S_2	S_3	S_4	S_5	S_6	S_7
r_1	r_2	r_3	r_4	r_5	0	0
$S_{\{1,2,3,4\}}+y_{(3,4,5)}+h(r_3 \oplus r_4 \oplus r_5)$	–	$S_{\{1,2,3,4\}}+y_{(1,4,5)}+h()$	$S_{\{1,2,3,4\}}+y_{(1,3,5)}+h()$	$S_{\{1,2,3,4\}}+y_{(1,3,4)}+h()$		
$S_{\{1,2,6,7\}}+y_{(2,6,7)}+h(r_2)$	$S_{\{1,2,6,7\}}+y_{(1,6,7)}+h(r_1)$	–	–	–	$S_{\{1,2,6,7\}}+y_{(1,2,7)}+h(r_1 \oplus r_2)$	$S_{\{1,2,6,7\}}+y_{(1,2,6)}+h(r_1 \oplus r_2)$
–	$S_{\{2,5,6,7\}}+y_{(5,6,7)}+h(r_5)$	–	–	$S_{\{2,5,6,7\}}+y_{(2,6,7)}+h(r_2)$	$S_{\{2,5,6,7\}}+y_{(2,5,7)}+h(r_2 \oplus r_5)$	$S_{\{2,5,6,7\}}+y_{(2,5,6)}+h(r_2 \oplus r_5)$

§ 5.2 Hypergraph-based SSS for General Access Structures

- **(r_1, r_2, r_3)-HA Scheme**
  - (2, 3, 4)-HA Scheme

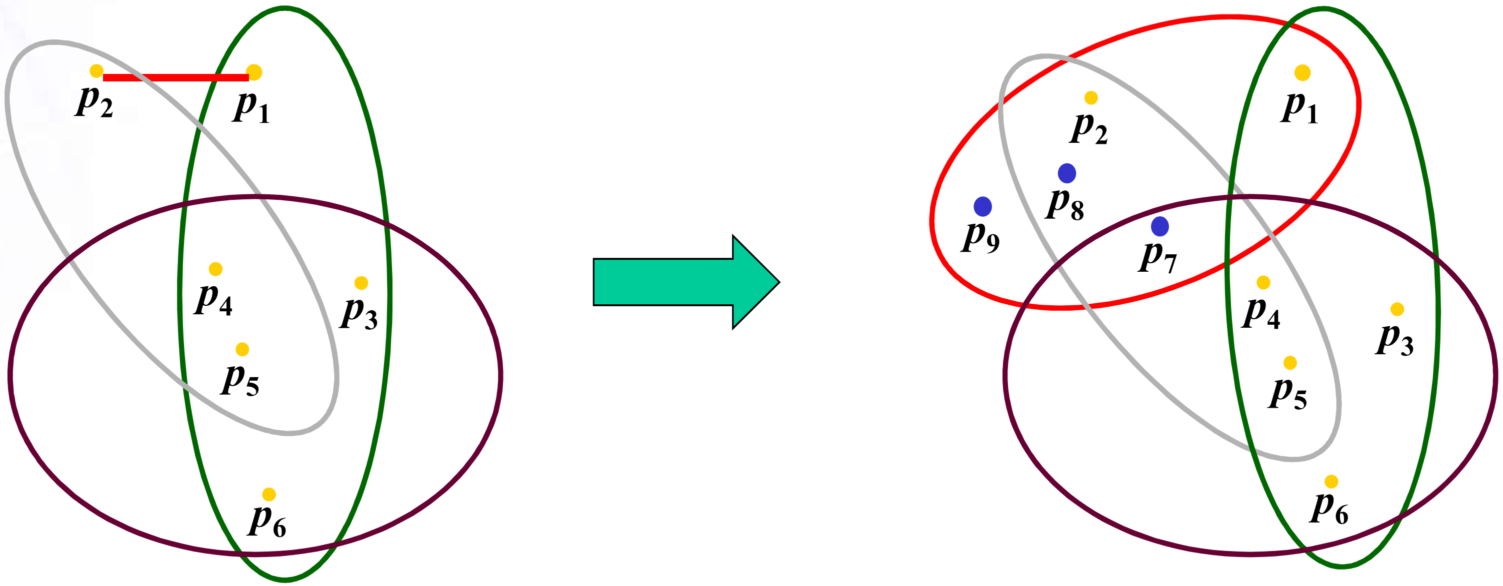
$$
\begin{aligned}
S_{\{1,3,4,5\}} = \; & y_{(1,3,4)} + h(r_1 \oplus r_3 \oplus r_4) \\
& + y_{(1,3,5)} + h(r_1 \oplus r_3 \oplus r_5) \\
& + y_{(1,4,5)} + h(r_1 \oplus r_4 \oplus r_5) \\
& + y_{(3,4,5)} + h(r_3 \oplus r_4 \oplus r_5)
\end{aligned}
$$



S_1	S_2	S_3	S_4	S_5	S_6	S_7
r_1	r_2	r_3	r_4	r_5	0	0
$S_{\{1,3,4,5\}}+y_{(3,4,5)}+h(r_3 \oplus r_4 \oplus r_5)$	–	$S_{\{1,3,4,5\}}+y_{(1,4,5)}+h$	$S_{\{1,3,4,5\}}+y_{(1,3,5)}+h$	$S_{\{1,3,4,5\}}+y_{(1,3,4)}+h$	–	–
–	$S_{\{2,4,5,6\}}+y_{(4,5,6)}+h(r_4 \oplus r_5)$	–	$S_{\{2,4,5,6\}}+y_{(2,5,6)}+h$	$S_{\{2,4,5,6\}}+y_{(2,4,6)}+h$	$S_{\{2,4,5,6\}}+y_{(2,4,5)}+h$	
$S_{\{1,2,6,7\}}+y_{(2,6,7)}+h(r_2)$	$S_{\{1,2,6,7\}}+y_{(1,6,7)}+h(r_1)$	–	–	–	$S_{\{1,2,6,7\}}+y_{(1,2,7)}+h$	$S_{\{1,2,6,7\}}+y_{(1,2,6)}+h$

§ 5.2 Hypergraph-based SSS for General Access Structures

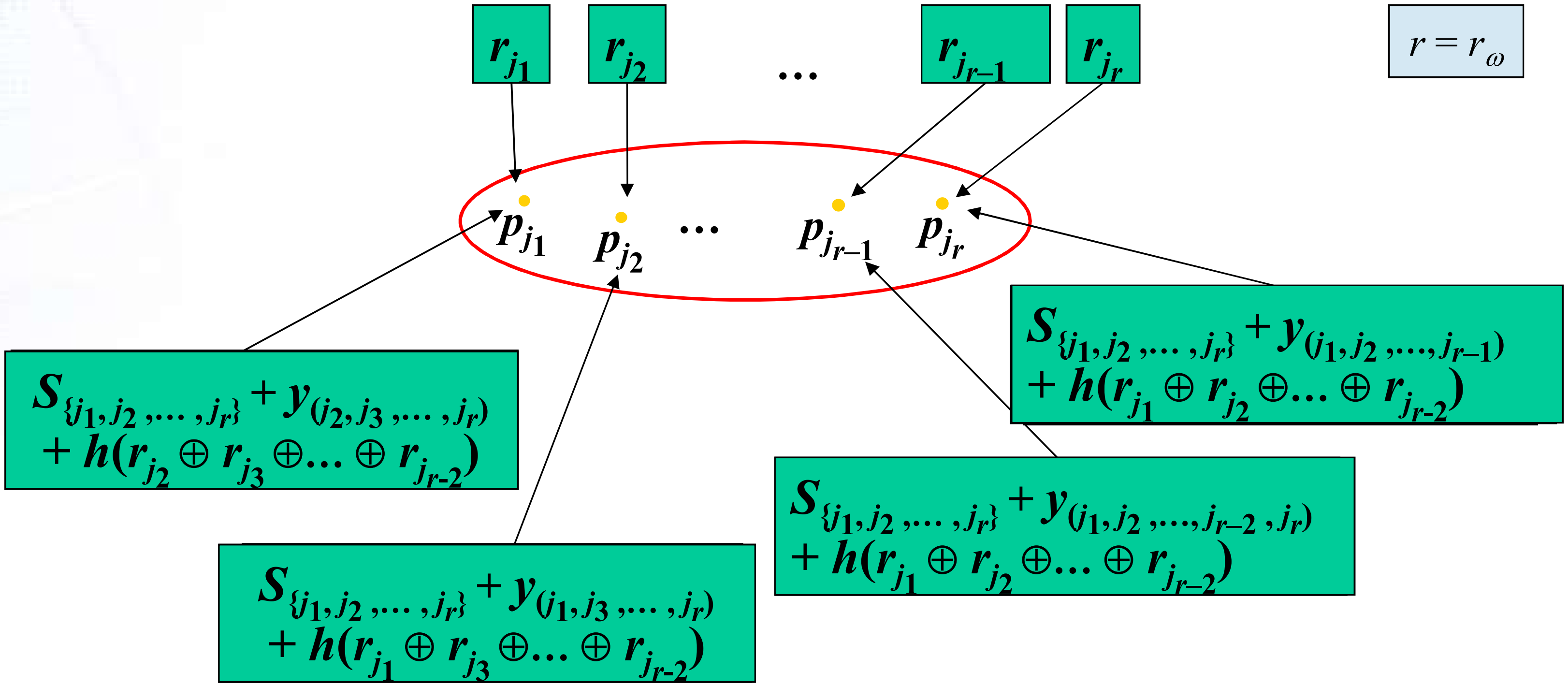
- **G-HA Scheme – Idea**
  - $(r_1, r_2, \ldots, r_\omega)$-HA Scheme
  - (2, 3, 4, 5)-HA Scheme



$|V| = n$ $\quad$ $|V| = n'$

§ 5.2 Hypergraph-based SSS for General Access Structures

- $f(x) = k_{r-1}x^{r-1} + \ldots + k_2x^2 + K_1x + K_0 \pmod{q}$
  - $y_{(i_1,i_2,\ldots,i_{r-1})} = f(\sum_{i=1}^{r-1} i_k (n')^{r-k-1})$



§ 5.2 Hypergraph-based SSS for General Access Structures

- **G-VDHA Scheme**

Publish:

$g, g^{K_0}, g^{K_1}, g^{k_2} \bmod p, g^{S_{\{1,2,3\}}}$

$g^{r_1}, g^{r_2}, g^{h(r_1)}, g^{h(r_2)} \bmod p$ g : generator

To Check p_2:

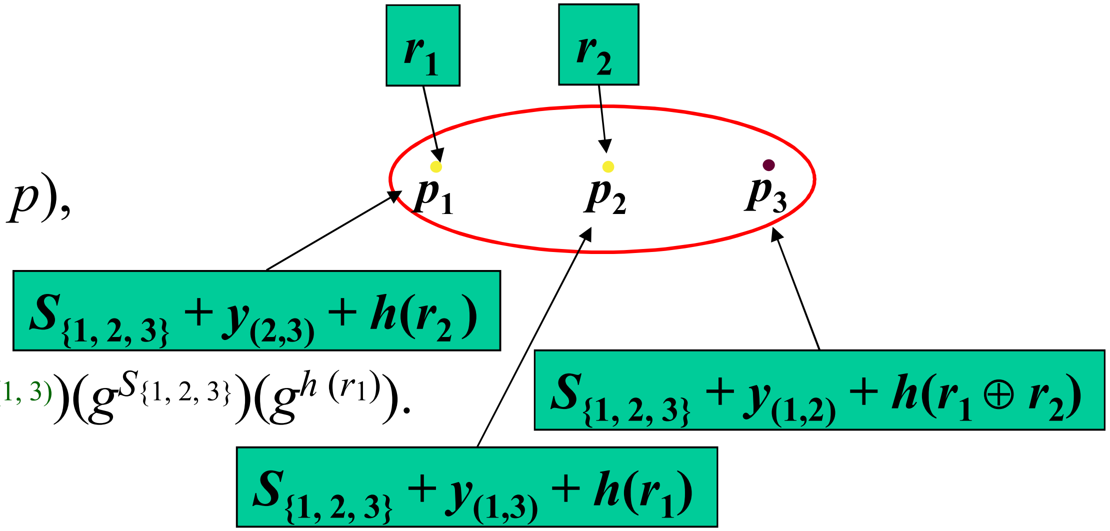
– Calculate

$g^{y_{(1,3)}} = (g^{k_2})^{x^2}(g^{K_1})^{x^1}(g^{K_0}) \pmod p$,

where $x = 1 \cdot 3 + 3$.

– Check $g^{y_{(1,3)}+S_{\{1,2,3\}}+h(r_1)} = (g^{y_{(1,3)}})(g^{S_{\{1,2,3\}}})(g^{h(r_1)})$.

– Check $g^{r_2} = (g)^{r_2}$.



§ 5.2 Hypergraph-based SSS for General Access Structures

- **G-MHA Scheme**

Publish:

F : one way hash function

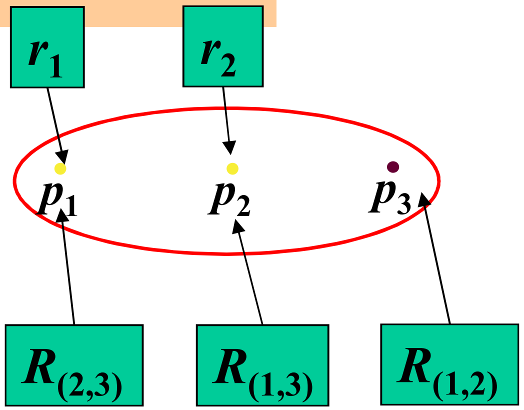
random numbers R over Z_q

$y_{(1,2)} + S_{\{1,2,3\}} + h(F(r_1, R) \oplus F(r_2, R)) + F(R_{(1,3)}, R)$

$y_{(1,3)} + S_{\{1,2,3\}} + h(F(r_1, R)) + F(R_{(1,3)}, R)$

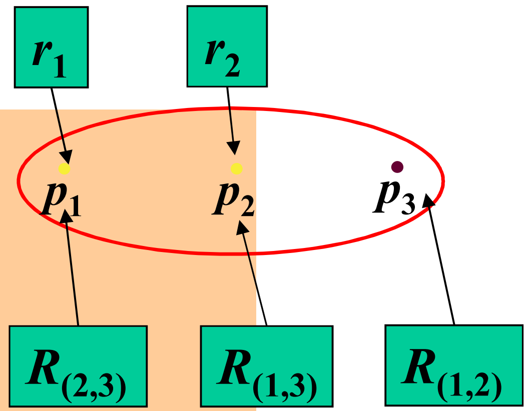
$y_{(2,3)} + S_{\{1,2,3\}} + h(F(r_2, R)) + F(R_{(2,3)}, R)$

- If $\{p_1, p_3, p_3\}$ want to reconstruct the K:
  - p_1: $F(R_{(2,3)}, R)$, $F(r_1, R)$;
  - p_2: $F(R_{(1,3)}, R)$, $F(r_2, R)$;



§ 5.2 Hypergraph-based SSS for General Access Structures

- **G-VDMHA Scheme**



Publish:

random numbers R over Z_q

$y_{(1,2)} + h(F(r_1, R) \oplus F(r_2, R)) + F(R_{(1,2)}, R)$

$y_{(1,3)} + h(F(r_1, R)) + F(R_{(1,3)}, R)$

$y_{(2,3)} + h(F(r_2, R)) + F(R_{(2,3)}, R)$

$g, g^{K_0}, g^{K_1}, g^{k_2}, g^{F(r_1, R)}, g^{F(r_2, R)}, g^{F(r_3, R)},$

$g^{h(F(r_1, R) \oplus F(r_2, R))}, g^{h(F(r_1, R))}, g^{h(F(r_2, R))}.$

p_1: $F(R_{(2,3)}, R), F(r_1, R)$;

p_2: $F(R_{(1,3)}, R), F(r_2, R)$.

Calculate

$g^{y(1,3)} = (g^{k_2})^{x^2}(g^{K_1})^{x^1}(g^{K_0}) \pmod{p}$, where $x = 1 \cdot n' + 3$.

Check

$g^{y(1,3)+h(F(r_1, R))+F(R_{(1,3)}, R)} = (g^{y(1,3)})(g^{h(F(r_1, R))})(g^{F(R_{(1,3)}, R)})$

Check $g^{F(r_1, R)} = (g)^{F(r_1, R)}$.

§ 5.2 Hypergraph-based SSS for General Access Structures

d = the minimum degree of G;
$m_i = \{A: A \in \Gamma_0, |A| = r_i\}$;
$m = \sum_{i=1}^{\omega} m_i$;
$c_i = \max_{A \in \Gamma_0} |A| - r_i$.

- **Performance**

	G-HA scheme (2007)	Tsai et al.'s scheme (1999)	Wang's scheme (2004)
Information rate	$2 / (d + 1)$	1	1
multiple operation	$m \times r_\omega^2 = \sum_{p_i} d_i \times m_i$	$r_i \times m_i$	$\sum_{p_i} (d_i + 2)$
addition operation	$m \times r_\omega^2 = \sum_{p_i} d_i \times m_i$	0	0
power operation	0	$2n + 1$	n
hash function	$\sum_{p_i} d_i$	0	0
exclusive-or	$\sum_{p_i} d_i \times (r_\omega - 1)$	m_i	0
inverse	0	0	$n + m$
Gaussian elimination	0	0	1
#Pseudo-man	$(r_\omega - r_1) / 0$	0	0

§ 5.2 Hypergraph-based SSS for General Access Structures

d = the minimum degree of G;
$m_i = \{A: A \in \Gamma_0, |A| = r_i\}$;
$m = \sum_{i=1}^{\omega} m_i$;
$c_i = \max_{A \in \Gamma_0} |A| - r_i$.

- **Performance**

	TUM Scheme* (2005)	G-HA scheme
information rate	$1 / d$	$2 / (d + 1)$
the number of public share	0	$\sum_{i=1}^{\omega} (m_i \times c_i)$
space complexity	$\sum_{i=1}^{\omega} m_i (r_i - 1) = O(mr_\omega)$	$r_\omega - 1 = O(r_\omega)$
multiple operation	$\sum_{i=1}^{\omega} (m_i \times r_i^2) = O(mr_\omega^2)$	$m \times r_\omega^2 = O(mr_\omega^2)$
addition operation	$\sum_{i=1}^{\omega} (m_i \times r_i^2) = O(mr_\omega^2)$	$m \times r_\omega^2 = O(mr_\omega^2)$
exclusive-or operation	0	$m\, r_\omega (r_\omega - 1) = O(mr_\omega^2)$
hash function	0	$(r_\omega - 1) \times m = O(mr_\omega)$

* The hypergraph is proper.

§ 5.2 Hypergraph-based SSS for General Access Structures

- **Modifilication:**
  - $K = (K_1, K_0) \in Z_q \times Z_q$
    $f(x) = k_{r-1}x^{r-1} + \ldots + k_2x^2 + K_1x + K_0 \pmod q$
  - $K = (K_r, \ldots, K_2, K_1, K_0) \in [Z_q]^r$
    $f(x) = K_rx^{r-1} + \ldots + K_2x^2 + K_1x + K_0 \pmod q$

Non-perfect !