Computer Science and Information Engineering
National Chi Nan University

The Principle and Application of Secret Sharing

Dr. Justie Su-Tzu Juan

Lecture 4. The Geometric Approach for Sharing Secrets

§ 4.1 A (*k*, *n*)-Threshold Scheme Based on a Hyperspherical Function (HS-TS)

Slides for a Course Based on

T.-C. Wu and W.-H. He, "A geometric approach for sharing secrets", Computer & Security, pp.135-145, 1995

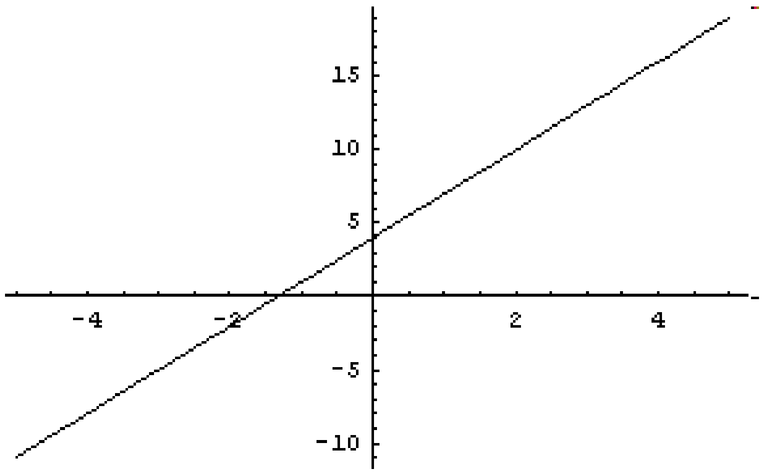
§ 4.1 A (k, n)-Threshold Scheme Based on a Hyperspherical Function (HS-TS)

- **Def:**
  - Let $\mathcal{K}$ be the master key space and $\mathcal{S}$ be the share space. The *information rate* of the secret sharing scheme is defined as $\log_2|\mathcal{K}| / \log_2|\mathcal{S}|$.
  - A secret sharing scheme is *perfect* if any set of participants in the prohibited structure obtains no information regarding the secret.
  - Secret sharing schemes are classified into the following types:
    - Type I: A secret sharing scheme for the *access structure* Γ: $\Delta = 2^P - \Gamma$.
    - Type II: A secret sharing scheme for the *prohibited structure* Δ: $\Gamma = 2^P - \Delta$.
    - Type III: A secret sharing scheme for the *mixed structure* (Γ, Δ): $(\Gamma \cup \Delta) \subseteq 2^P$

§ 4.1 A (k, n)-Threshold Scheme Based on a Hypersphierical Function (HS-TS)

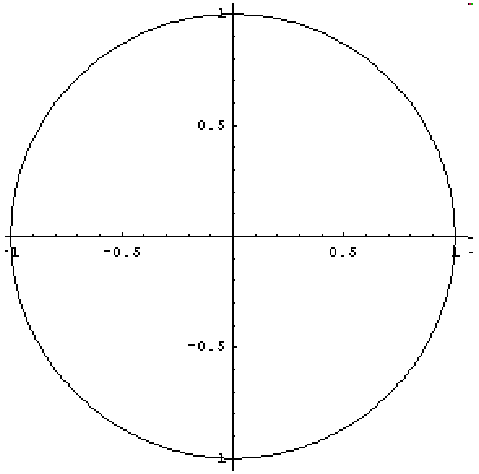
- **Simple geometric properties:**
  - 1. $(x_1, y_1), (x_2, y_2)$ -------------- $y = ax + b$

    a $(2, n)$-threshold scheme.



  - 2. $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ ----- $(x_1 - a_1)^2 + (x_2 - a_2)^2 = s$

    a $(3, n)$ threshold scheme.



§ 4.1 A (k, n)-Threshold Scheme Based on a Hyperspherical Function (HS-TS)

- **Simple geometric properties:**
  - 3. (x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4) ----- $(x_1 - a_1)^2 + (x_2 - a_2)^2 + (x_3 - a_3)^2 = s$

    a (4, n) threshold scheme.

  - 4. Extend 2 and 3 to k items:
    - Given any k points, which don't lie on (k – 2)-dimensional space, can uniquely determine (a_1, a_2, …, $a_{k\text{-}1}$) and s, such that:

$$\sum_{i=1}^{k-1}(x_i - a_i)^2 = s.$$

Device a (k, n) threshold scheme.

§ 4.1 A (k, n)-Threshold Scheme Based on a Hyperspherical Function (HS-TS)

- **Theoretical analysis :**
- **<u>Thm 1 (1/2)</u>:** If k points ($A_1(y_{11}, y_{12}, \ldots, y_{1(k\text{-}1)})$, $A_2(y_{21}, y_{22}, \ldots, y_{2(k\text{-}1)})$, …, $A_k(y_{k1}, y_{k2}, \ldots, y_{k(k\text{-}1)})$) do not lie on in common (k – 2)-dimensional space, then they can uniquely determine the equation $\sum_{i=1}^{k-1}(x_i - a_i)^2 = s$ by

$$\frac{\det\begin{pmatrix} \sum_{i=1}^{k-1} x_i^2 & x_1 & x_2 & \cdots & x_{k-1} & 1 \\ \sum_{i=1}^{k-1} y_{1i}^2 & y_{11} & y_{12} & \cdots & y_{1(k-1)} & 1 \\ \sum_{i=1}^{k-1} y_{2i}^2 & y_{21} & y_{22} & \cdots & y_{2(k-1)} & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \sum_{i=1}^{k-1} y_{ki}^2 & y_{k1} & y_{k2} & \cdots & y_{k(k-1)} & 1 \end{pmatrix}}{\det\begin{pmatrix} y_{11} & y_{12} & \cdots & y_{1(k-1)} & 1 \\ y_{21} & y_{22} & \cdots & y_{2(k-1)} & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ y_{k1} & y_{k2} & \cdots & y_{k(k-1)} & 1 \end{pmatrix}} = 0$$

§ 4.1 A (k, n)-Threshold Scheme Based on a Hyperspherical Function (HS-TS)

- **Theoretical analysis :**
- **<u>Thm 1 (2/2)</u>:** Where and

$$a_i = \frac{\det\begin{pmatrix} \sum_{i=1}^{k-1} y_{1i}^2 & y_{11} & \dots & y_{1(i-1)} & y_{1(i+1)} & \dots & y_{1(k-1)} & 1 \\ \sum_{i=1}^{k-1} y_{2i}^2 & y_{21} & \dots & y_{2(i-1)} & y_{2(i+1)} & \dots & y_{2(k-1)} & 1 \\ & . & . & . & . & . & . & . \\ \sum_{i=1}^{k-1} y_{ki}^2 & y_{k1} & \dots & y_{k(i-1)} & y_{k(i+1)} & \dots & y_{k(k-1)} & 1 \end{pmatrix}}{\det\begin{pmatrix} y_{11} & y_{12} & \dots & y_{1(k-1)} & 1 \\ y_{21} & y_{22} & \dots & y_{2(k-1)} & 1 \\ & . & . & . & . \\ y_{k1} & y_{k2} & \dots & y_{k(k-1)} & 1 \end{pmatrix}} \times \frac{1}{2} \times (-1)^{(i+1)}$$

$$s = \frac{\det\begin{pmatrix} \sum_{i=1}^{k-1} y_{1i}^2 & y_{11} & y_{12} & \dots & y_{1(k-1)} \\ \sum_{i=1}^{k-1} y_{2i}^2 & y_{21} & y_{22} & \dots & y_{2(k-1)} \\ & . & . & . & . \\ \sum_{i=1}^{k-1} y_{ki}^2 & y_{k1} & y_{k2} & \dots & y_{k(k-1)} \end{pmatrix}}{\det\begin{pmatrix} y_{11} & y_{12} & \dots & y_{1(k-1)} & 1 \\ y_{21} & y_{22} & \dots & y_{2(k-1)} & 1 \\ & . & . & . & . \\ y_{k1} & y_{k2} & \dots & y_{k(k-1)} & 1 \end{pmatrix}} \times (-1)^{(k+1)} + \sum_{i=1}^{k-1} a_i^2$$

§ 4.1 A (k, n)-Threshold Scheme Based on a Hyperspherical Function (HS-TS)

- **Theoretical analysis :**

- **Ex:** (5, 3), (2, 6), (2, 0) do not lie on in common 2-dimensional space (line), $(x_1 - 2)^2 + (x_2 - 3)^2 = 9$ (i.e. $x_1^2 - 4x_1 + x_2^2 - 6x_2 + 4 = 0$) can be determined by

$$\frac{\det\begin{pmatrix} x_1^2 + x_2^2 & x_1 & x_2 & 1 \\ 34 & 5 & 3 & 1 \\ 40 & 2 & 6 & 1 \\ 4 & 2 & 0 & 1 \end{pmatrix}}{\det\begin{pmatrix} 5 & 3 & 1 \\ 2 & 6 & 1 \\ 2 & 0 & 1 \end{pmatrix}} = x_1^2 - 4x_1 + x_2^2 - 6x_2 + 4 = 0$$

where

$$a_2 = \frac{\det\begin{pmatrix} 34 & 5 & 1 \\ 40 & 2 & 1 \\ 4 & 2 & 1 \end{pmatrix}}{\det\begin{pmatrix} 5 & 3 & 1 \\ 2 & 6 & 1 \\ 2 & 0 & 1 \end{pmatrix}} \times \frac{1}{2} \times (-1)^{(2+1)} = 3$$

$$a_1 = \frac{\det\begin{pmatrix} 34 & 3 & 1 \\ 40 & 6 & 1 \\ 4 & 0 & 1 \end{pmatrix}}{\det\begin{pmatrix} 5 & 3 & 1 \\ 2 & 6 & 1 \\ 2 & 0 & 1 \end{pmatrix}} \times \frac{1}{2} \times (-1)^{(1+1)} = 2$$

§ 4.1 A (k, n)-Threshold Scheme Based on a Hyperspherical Function (HS-TS)

- **Theoretical analysis :**
- **Def:** Let p be an odd prime and gcd(a, p) = 1. If the quadratic congruence (二次同餘) $x^2 = a \pmod{p}$ has a solution, then a is said to be a quadratic residue (二次剩餘) of p.

- **Ex:** For p = 13, find x in Z_p^* such that $x^2 = a \pmod{13}$.

  Sol. $1^2 = 12^2 = 1 \pmod{13}$; $4^2 = 9^2 = 3 \pmod{13}$; $2^2 = 11^2 = 4 \pmod{13}$;

  $5^2 = 8^2 = 12 \pmod{13}$; $3^2 = 10^2 = 9 \pmod{13}$; $6^2 = 7^2 = 10 \pmod{13}$.

  The quadratic residues of 13 are 1, 3, 4, 9, 10, 12,

  while the non-residues are 2, 5, 6, 7, 8, 11.

§ 4.1 A (k, n)-Threshold Scheme Based on a Hyperspherical Function (HS-TS)

- **Theoretical analysis :**
- **Ex:** Let p = 19, 2 is a quadratic non-residue modulo 19.

  Sol. $1^2 = 18^2 = 1 \pmod{19}$; $2^2 = 17^2 = 4 \pmod{19}$; $3^2 = 16^2 = 9 \pmod{19}$;

  $4^2 = 15^2 = 16 \pmod{19}$; $5^2 = 14^2 = 6 \pmod{19}$; $6^2 = 13^2 = 17 \pmod{19}$;

  $7^2 = 12^2 = 11 \pmod{19}$; $8^2 = 11^2 = 7 \pmod{19}$; $9^2 = 10^2 = 5 \pmod{19}$.

  The quadratic residues of 19 are 1, 4, 5, 6, 7, 9, 11, 16, 17

  while the non-residues are 2, 3, 8, 10, 12, 13, 14, 15, 18.

- **Thm 4:** Let p be an odd prime number. If 2 is a quadratic non-residue modulo p, then every integer $r \in [0, p)$ can be expressed in the form

  $r = x^2 + y^2 \pmod{p}$ with integer $x, y \in [0, p)$.

§ 4.1 A (k, n)-Th
Hypersph

$1^2 = 18^2 = 1 \pmod{19}$; $2^2 = 17^2 = 4 \pmod{19}$; $3^2 = 16^2 = 9 \pmod{19}$;
$4^2 = 15^2 = 16 \pmod{19}$; $5^2 = 14^2 = 6 \pmod{19}$; $6^2 = 13^2 = 17 \pmod{19}$;
$7^2 = 12^2 = 11 \pmod{19}$; $8^2 = 11^2 = 7 \pmod{19}$; $9^2 = 10^2 = 5 \pmod{19}$.

- **Theoretical analysis :**
- **Ex:** An example of Thm 4, let p = 19, 2 is a quadratic non-residue modulo 19.

Sol. $0 = 0^2 + 0^2 \pmod{19}$; $1 = 0^2 + 1^2 \pmod{19}$; $2 = 1^2 + 1^2 \pmod{19}$; $3 = 4^2 + 5^2 \pmod{19}$;
$4 = 0^2 + 2^2 \pmod{19}$; $5 = 1^2 + 2^2 \pmod{19}$; $6 = 0^2 + 5^2 \pmod{19}$; $7 = 5^2 + 1^2 \pmod{19}$;
$8 = 2^2 + 2^2 \pmod{19}$; $9 = 0^2 + 3^2 \pmod{19}$; $10 = 1^2 + 3^2 \pmod{19}$;
$11 = 5^2 + 9^2 \pmod{19}$; $12 = 5^2 + 5^2 \pmod{19}$; $13 = 5^2 + 8^2 \pmod{19}$;
$14 = 8^2 + 7^2 \pmod{19}$; $15 = 2^2 + 7^2 \pmod{19}$; $16 = 4^2 + 0^2 \pmod{19}$;
$17 = 0^2 + 6^2 \pmod{19}$; $18 = 7^2 + 8^2 \pmod{19}$.

- **Corollary 2:** Let p be an odd prime number. If 2 is not a quadratic residue modulo p, any integer $z \in [0, p)$ can be expressed as the sum of k ($k \geq 2$) integer squares (modulo p).

§ 4.1 A (k, n)-Threshold Scheme Based on a Hyperspherical Function (HS-TS)

- **Wu & He's (k, n)-TS Based on a Hyperspherical Function HS-TS (1995)**
  - **Initial Phase**

    Step 1. For $i = 0, 1, 2, ..., (p-1)/2$, compute $z_i = i^2 \pmod p$.

    Put the pair (z_i, i) in the directory file.

    Step 2. Publish the directory file.
  - **Distribution (secret $K = (a_1, a_2, \ldots, a_{k-1})$) 1/2:**

    For $i = 1, 2, ..., n$, do the following :

    Step 1. For $j = 1, 2, ..., k-3$, do the following:

    (1.1) Randomly choose a pair in the directory file and let it be (r_{ij}, w_{ij}).

    (1.2) Set x_{ij} to be either $w_{ij} + a_j \pmod p$ or $p - w_{ij} + a_j \pmod p$.

§ 4.1 A (k, n)-Threshold Scheme Based on a Hyperspherical Function (HS-TS)

- **Wu & He's (k, n)-TS Based on a Hyperspherical Function HS-TS (1995)**
  - **Distribution (secret $K = (a_1, a_2, \ldots, a_{k-1})$) 2/2:**

    For $i = 1, 2, ..., n$, do the following :

    Step 2. Choose two pairs $(r_{i(k-2)}, w_{i(k-2)})$ and $(r_{i(k-1)}, w_{i(k-1)})$ from the directory file, such that $r_{i(k-2)} + r_{i(k-1)} = s - \Sigma_{j=1,k-3}\, r_{ij} \pmod p$.

    Step 3. Set $x_{i(k-2)}$ to be either $w_{i(k-2)} + a_{k-2} \pmod p$ or $p - w_{i(k-2)} + a_{k-2} \pmod p$.
    Set $x_{i(k-1)}$ to be either $w_{i(k-1)} + a_{k-1} \pmod p$ or $p - w_{i(k-1)} + a_{k-1} \pmod p$.

    Step 4. Let $E_i = (x_{i1}, x_{i2}, ..., x_{i(k-1)})$ and $E_i' = (x_{i1}, x_{i2}, ..., x_{i(k-1)}, 1)$.

    Step 5. If $i \le k$ and $E_1', E_2', ..., E_i'$ are linear dependent, then repeat Step 1 to 4.
    If $i > k$ and any k of $E_1', E_2', ..., E_i'$ are linear dependent, then repeat Step 1 to 4.

    Step 6. Output E_i.
  - **Reconstruction (secret $K = (a_1, a_2, \ldots, a_{k-1})$): By Thm 1.**

$0 = 0^2 + 0^2 \pmod{19}$; $1 = 0^2 + 1^2 \pmod{19}$; $2 = 1^2 + 1^2 \pmod{19}$; $3 = 4^2 + 5^2 \pmod{19}$; $4 = 0^2 + 2^2 \pmod{19}$; $5 = 1^2 + 2^2 \pmod{19}$; $6 = 0^2 + 5^2 \pmod{19}$; $7 = 5^2 + 1^2 \pmod{19}$; $8 = 2^2 + 2^2 \pmod{19}$; $9 = 0^2 + 3^2 \pmod{19}$; $10 = 1^2 + 3^2 \pmod{19}$; $11 = 5^2 + 9^2 \pmod{19}$; $12 = 5^2 + 5^2 \pmod{19}$; $13 = 5^2 + 8^2 \pmod{19}$; $14 = 8^2 + 8^2 \pmod{19}$; $15 = 2^2 + 7^2 \pmod{19}$; $16 = 4^2 + 0^2 \pmod{19}$; $17 = 0^2 + 6^2 \pmod{19}$; $18 = 7^2 + 8^2 \pmod{19}$.

- **Wu & He's (k, n)-TS Based on a Hyperspherical Function HS-TS (1995)**
  - **Ex (1/3):** $p = 19$, $n = 4$, $k = 4$ and $s = 6$, The secret $K = (5, 3, 2)$.The equation is

$$(x_1 - 5)^2 + (x_2 - 3)^2 + (x_3 - 2)^2 = 6 \pmod{19}.$$

  - **Initial Phase:** The pairs in the corresponding directory file are

    (0, 0), (1, 1), (4, 2), (5, 9), (6, 5), (7, 8), (9, 3), (11, 7), (16, 4),and (17, 6).
  - **Distribution:**

    (1) Randomly choose a pair $(r_{11}, w_{11}) = (1,1)$ and let $r_{11} = 1$.

    (2) Set $x_{11} = w_{11} + a_1 = 1 + 5 \pmod{19} = 6$.

    (3) Choose two pairs (r_{12}, w_{12}) and (r_{13}, w_{13}) from the directory file, such that

$$r_{12} + r_{13} \pmod{19} = 6 - \Sigma_{j = 1, 4-3}\, r_{1j} \pmod{19} = 6 - 1 = 5.$$

    Set $r_{12} = 1$ and $r_{13} = 4$. The pairs in the directory file are (1, 1) and (4, 2)

§ 4.1

$0 = 0^2 + 0^2 \pmod{19}$; $1 = 0^2 + 1^2 \pmod{19}$; $2 = 1^2 + 1^2 \pmod{19}$; $3 = 4^2 + 5^2 \pmod{19}$;
$4 = 0^2 + 2^2 \pmod{19}$; $5 = 1^2 + 2^2 \pmod{19}$; $6 = 0^2 + 5^2 \pmod{19}$; $7 = 5^2 + 1^2 \pmod{19}$;
$8 = 2^2 + 2^2 \pmod{19}$; $9 = 0^2 + 3^2 \pmod{19}$; $10 = 1^2 + 3^2 \pmod{19}$; $11 = 5^2 + 9^2 \pmod{19}$;
$12 = 5^2 + 5^2 \pmod{19}$; $13 = 5^2 + 8^2 \pmod{19}$; $14 = 8^2 + 8^2 \pmod{19}$; $15 = 2^2 + 7^2 \pmod{19}$;
$16 = 4^2 + 0^2 \pmod{19}$; $17 = 0^2 + 6^2 \pmod{19}$; $18 = 7^2 + 8^2 \pmod{19}$.

- **Wu & He's (k, n)-TS Based on a Hyperspherical Function HS-TS (1995)**
  - **Ex (2/3):** $p = 19$, $n = 4$, $k = 4$ and $s = 6$, The secret $K = (5, 3, 2)$.The equation is

$$(x_1 - 5)^2 + (x_2 - 3)^2 + (x_3 - 2)^2 = 6 \pmod{19}.$$

  - **Initial Phase:** The pairs in the corresponding directory file are

    (0, 0), (1, 1), (4, 2), (5, 9), (6, 5), (7, 8), (9, 3), (11, 7), (16, 4),and (17, 6).

  - **Distribution:**

    (4) Set $x_{12} = 1 + 3 \pmod{19} = 4$ and $x_{13} = 2 + 2 \pmod{19} = 4$.

    (5) Since (6, 4, 4, 1) is linearly independent, we have $E_1 = (6, 4, 4)$.

    (6) Similarly, we can obtain

$$E_2 = (7, 4, 3),\ E_3 = (6, 5, 3), \text{ and } E_4 = (8, 3, 6).$$

§ 4.1 A (*k*, *n*)-Threshold Scheme Based on a Hyperspherical Function (HS-TS)

- **Wu & He's (*k*, *n*)-TS Based on a Hyperspherical Function HS-TS (1995)**
  - **Ex (3/3):** p =19, n = 4, k = 4 and s = 6, The secret K = (5, 3, 2).The equation is

    $$(x_1 - 5)^2 + (x_2 - 3)^2 + (x_3 - 2)^2 = 6 \pmod{19}.$$

  - **Reconstruction:**

    (1) Let E_1' = (6, 4, 4, 1), E_2' = (7, 4, 3, 1), E_3' = (6, 5, 3, 1), and E_4' = (8, 3, 6, 1)

    (2) Then

    $$\det\begin{pmatrix} 6 & 4 & 4 & 1 \\ 7 & 4 & 3 & 1 \\ 6 & 5 & 3 & 1 \\ 8 & 3 & 6 & 1 \end{pmatrix} (\bmod 19) = 16$$

    (3) Over Z_{19}^*, the inverse of 16 (mod 19) is 6 and the inverse of 2 (mod 19) is 10.

    (4) Compute

    $$a_1 = \det\begin{pmatrix} 11 & 4 & 4 & 1 \\ 17 & 4 & 3 & 1 \\ 13 & 5 & 3 & 1 \\ 14 & 3 & 6 & 1 \end{pmatrix} \times \frac{1}{16} \times \frac{1}{2} \times (-1)^{1+1} (\bmod 19) = 8 \times 6 \times 10 \times 1 (\bmod 19) = 5$$

    (5) Similar way to find a_2 and a_3.

§ 4.1 A (k, n)-Threshold Scheme Based on a Hyperspherical Function (HS-TS)

- **Wu & He's (k, n)-TS Based on a Hyperspherical Function HS-TS (1995)**
- **Discussion.**
  - The equation $\sum_{i=1}^{k-1}(x_i - a_i)^2 = s$ contains k unknown variables.
  - The probabilistic algorithm for evaluating the determinant of a $k \times k$ matrix required an expected $O(k(w + k \log k))$ field operations (where w is approximate to the number of field operations needed to apply the matrix to a test vector).
  - The secret $K = (a_1, a_2, \ldots, a_{k-1})$ needs to compute k determinants.
  - So the time complexity for recovering the secret is about $O(k^2(w + k \log k))$ field operations.
  - The information rate of the HS-TS is $\log_2|\mathcal{K}| / \log_2|\mathcal{S}| = \log_2 p^{k-1} / \log_2 p^{k-1} = 1$.

§ 4.1 A (k, n)-Threshold Scheme Based on a Hyperspherical Function (HS-TS)

- HW2: (5/2)
  - (1) Refer to Feldman's scheme, design an verifiable and detectable secret sharing scheme (VDSSS) that can verify and detect the authenticity of the shares of HS-TS.
  - (2) Refer to Yang et al.'s scheme, design an online (t, n) multi-secret sharing scheme (OSSS) based on HS-TS.

Computer Science and Information Engineering
National Chi Nan University

The Principle and Application of Secret Sharing

Dr. Justie Su-Tzu Juan

Lecture 4. The Geometric Approach for Sharing Secrets

§ 4.2 A (k, n) Multi-secret Sharing Scheme Based on a Hyperelliptic Function (HE-TS)

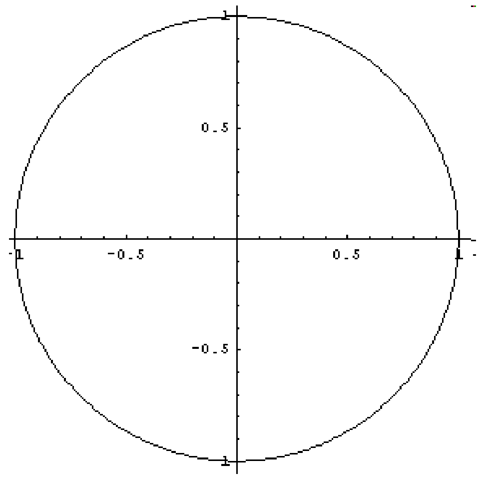
Slides for a Course Based on

Y.-L. Chuang "A Study on Secret Sharing Scheme", Master Thesis of Department of SCIE, National Chi Nan University, 2005.

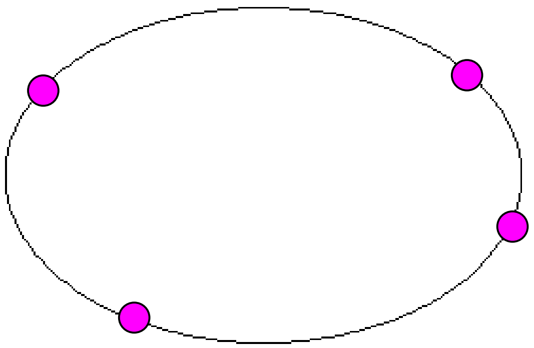
§ 4.2 A (k, n) Multi-secret Sharing Scheme Based on a Hyperelliptic Function (HE-TS)

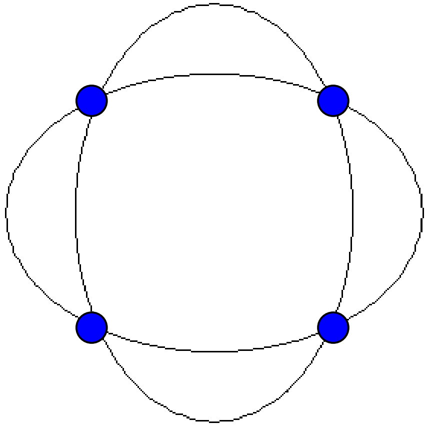
- **Simple geometric properties:**
  - 1. (x_1, y_1), (x_2, y_2), (x_3, y_3) ----- $(x_1 - a_1)^2 + (x_2 - a_2)^2 = s$

    a (3, n) threshold scheme.



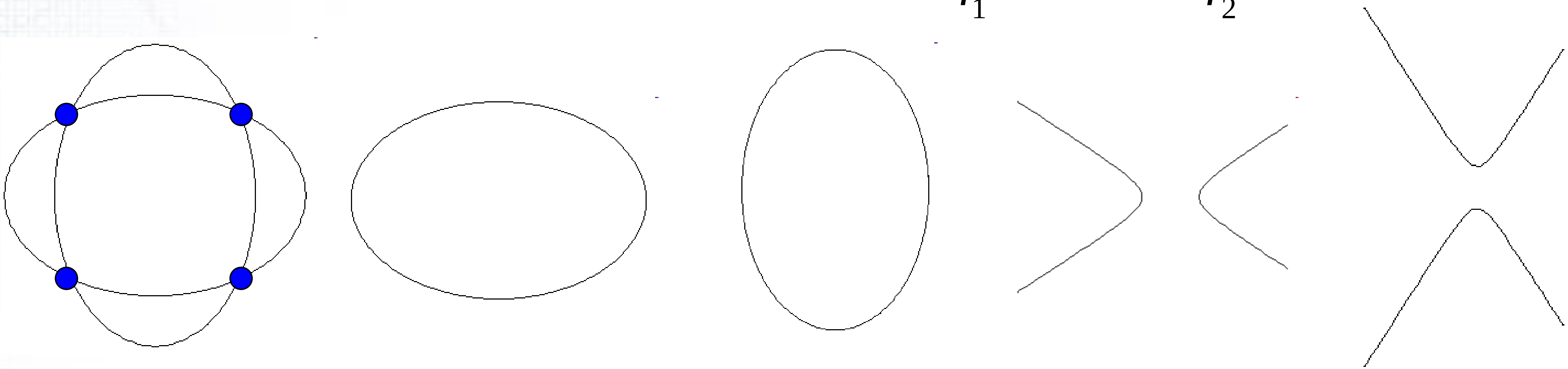
  - 2. (x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4) ----- $(\frac{x_1 - a_1}{r_1})^2 + (\frac{x_2 - a_2}{r_2})^2 = 1$





§ 4.2 A (k, n) Multi-secret Sharing Scheme Based on a Hyperelliptic Function (HE-TS)

- **Simple geometric properties:**
  - 2. (x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4) ----- $(\frac{x_1 - a_1}{r_1})^2 + (\frac{x_2 - a_2}{r_2})^2 = 1$



- $\sum_{i=1}^{k} b_i^2 (x_i - a_i)^2 = 1 \pmod p$ ---- A ($2k$, n)-threshold scheme
- For ($2k - 1$, n)-threshold scheme: Publish b_1.

§ 4.2 A (k, n) Multi-secret Sharing Scheme Based on a Hyperelliptic Function (HE-TS)

- **Algorithm - (2k, n) HE-TS**
  - **Initial Phase**

    Step 1. For $i = 0, 1, 2, ..., (p - 1)/2$, compute $z_i = i^2 \pmod{p}$.

    Put the pair (z_i, i) in the directory file.

    Step 2. Publish the directory file.

  - **Distribution (secret $K = (a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k)$) 1/2:**

    For $i = 1, 2, ..., n$, do the following :

    Step 1. For $j = 1, 2, ..., k - 2$, do the following:

    (1.1) Randomly choose a pair in the directory file and let it be (r_{ij}, w_{ij}).

    (1.2) Set x_{ij} to be either $b_j^{-1}w_{ij} + a_j \pmod{p}$ or $p - b_j^{-1}w_{ij} + a_j \pmod{p}$.

§ 4.2 A (k, n) Multi-secret Sharing Scheme Based on a Hyperelliptic Function (HE-TS)

- **Algorithm**
  - **Distribution (secret $K = (a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k)$) 2/2:**

For $i = 1, 2, \ldots, n$, do the following :

Step 2. Choose two pairs $(r_{i(k-1)}, w_{i(k-1)})$ and (r_{ik}, w_{ik}) from the directory file, such that $r_{i(k-1)} + r_{ik} = 1 - \Sigma_{j=1,k-2}\, r_{ij} \pmod p$.

Step 3. Set $x_{i(k-1)}$ to be either $b_{k-1}^{-1} w_{i(k-1)} + a_{k-1} \pmod p$ or $p - b_{k-1}^{-1} w_{i(k-1)} + a_{k-1} \pmod p$. Set x_{ik} to be either $b_k^{-1} w_{ik} + a_k \pmod p$ or $p - b_k^{-1} w_{ik} + a_k \pmod p$.

Step 4. Let $E_i = (x_{i1}, x_{i2}, \ldots, x_{ik})$ and $E_i' = (x_{i1}^2, x_{i1}, x_{i2}^2, x_{i2}, \ldots, x_{ik}^2, x_{ik})$.

Step 5. If $i \le 2k$ and $E_1', E_2', \ldots, E_i'$ are l. d., then repeat Step 1 to 4. If $i > 2k$ and any $2k$ of $E_1', E_2', \ldots, E_i'$ are l. d., then repeat Step 1 to 4.

Step 6. Output E_i.

§ 4.2 A (k, n) Multi-secret Sharing Scheme Based on a Hyperelliptic Function (HE-TS)

- **Algorithm**
  - **Reconstruction (secret $K = (a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k)$) 1/3:** Any $2k$ of n shares E_i can determine the secret K. WLOG, let the $2k$ shares be $E_1, E_2, \ldots, E_{2k}$,

    Step 1. let equation $\sum_{i=1}^{k} b_i^2 (x_i - a_i)^2 = 1 \pmod p$ be $\sum_{i=1}^{k} x_i^2 c_{2i-1} + x_i c_{2i} = 1 \pmod p$.

    Step 2. Using Cramer's Rule, determine all c_i as:

    $c_i = \Delta_{c_i}/\Delta$, where

$$\Delta = \det\begin{pmatrix} x_{11}^2 & x_{11} & x_{21}^2 & x_{21} & \cdots & x_{1k}^2 & x_{1k} \\ x_{21}^2 & x_{21} & x_{22}^2 & x_{22} & \cdots & x_{2k}^2 & x_{2k} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{(2k)1}^2 & x_{(2k)1} & x_{(2k)2}^2 & x_{(2k)2} & \cdots & x_{(2k)k}^2 & x_{(2k)k} \end{pmatrix} \bmod p$$

§ 4.2 A (k, n) Multi-secret Sharing Scheme Based on a Hyperelliptic Function (HE-TS)

- **Algorithm**
  - **Reconstruction (secret $K = (a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k)$) 2/3:**

Step 2. Using Cramer's Rule, determine all c_i as:

$$\Delta_{c_i} = \det\begin{pmatrix} x_{11}^2 & x_{11} & \cdots & x_{1\left(\frac{i-1}{2}\right)} & 1 & x_{1\left(\frac{i+1}{2}\right)} & \cdots & x_{1k}^2 & x_{1k} \\ x_{21}^2 & x_{21} & \cdots & x_{2\left(\frac{i-1}{2}\right)} & 1 & x_{2\left(\frac{i+1}{2}\right)} & \cdots & x_{2k}^2 & x_{2k} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{(2k)1}^2 & x_{(2k)1} & \cdots & x_{(2k)\left(\frac{i-1}{2}\right)} & 1 & x_{(2k)\left(\frac{i+1}{2}\right)} & \cdots & x_{(2k)k}^2 & x_{(2k)k} \end{pmatrix} \bmod p \text{ if } i \text{ is odd;}$$

$$\Delta_{c_i} = \det\begin{pmatrix} x_{11}^2 & x_{11} & \cdots & x^2_{1\left(\frac{i}{2}\right)} & 1 & x^2_{1\left(\frac{i}{2}+1\right)} & \cdots & x_{1k}^2 & x_{1k} \\ x_{21}^2 & x_{21} & \cdots & x^2_{2\left(\frac{i}{2}\right)} & 1 & x^2_{2\left(\frac{i}{2}+1\right)} & \cdots & x_{2k}^2 & x_{2k} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{(2k)1}^2 & x_{(2k)1} & \cdots & x^2_{(2k)\left(\frac{i}{2}\right)} & 1 & x^2_{(2k)\left(\frac{i}{2}+1\right)} & \cdots & x_{(2k)k}^2 & x_{(2k)k} \end{pmatrix} \bmod p \text{ if } i \text{ is even;}$$

§ 4.2 A (k, n) Multi-secret Sharing Scheme Based on a Hyperelliptic Function (HE-TS)

- **Algorithm**
  - **Reconstruction (secret $K = (a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k)$) 3/3:**

Step 3. determine a_i and b_i^2 by using c_j for all $1 \le i \le k$, $1 \le j \le 2k$:

$$a_i = -(c_{2i} / 2c_{2i-1}) \bmod p$$
$$= -(\Delta c_{2i} / 2\Delta_{2i-1}) \bmod p$$

$$b_i^2 = c_i / \left(1 + \sum_{i=1}^{k} \frac{c_{2i}^2}{4c_{2i-1}}\right)$$

$$b_i^2 = \frac{\det \begin{pmatrix} 1+\frac{c_2^2}{4c_1} & \cdots & \frac{c_1 c_{2i-2}^2}{4c_{2i-3}} & c_1 & \frac{c_1 c_{2i+2}^2}{4c_{2i+1}} & \cdots & \frac{c_1 c_{2k}^2}{4c_{2k-1}} \\ \frac{c_3 c_2^2}{4c_1^2} & \cdots & \frac{c_3 c_{2i-2}^2}{4c_{2i-3}} & c_3 & \frac{c_3 c_{2i+2}^2}{4c_{2i+1}} & \cdots & \frac{c_3 c_{2k}^2}{4c_{2k-1}} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{c_{2t-1} c_2^2}{4c_1^2} & \cdots & \frac{c_{2t-1} c_{2i-2}^2}{4c_{2i-3}} & c_{2t-1} & \frac{c_{2t-1} c_{2i+2}^2}{4c_{2i+1}} & \cdots & 1+\frac{c_{2k-1} c_{2k}^2}{4c_{2k-1}} \end{pmatrix}_{(k \times k)}}{\det \begin{pmatrix} 1+\frac{c_2^2}{4c_1} & \frac{c_1 c_4^2}{4c_3} & \cdots & \frac{c_1 c_{2k}^2}{4c_{2k-1}} \\ \frac{c_3 c_2^2}{4c_1^2} & 1+\frac{c_4^2}{4c_3} & \cdots & \frac{c_3 c_{2k}^2}{4c_{2k-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{c_{2t-1} c_2^2}{4c_1^2} & \frac{c_{2t-1} c_4^2}{4c_3^2} & \cdots & 1+\frac{c_{2k-1} c_{2k}^2}{4c_{2k-1}} \end{pmatrix}_{(k \times k)}}$$

§ 4.2 ... Base...

$0 = 0^2 + 0^2 \pmod{19}$; $1 = 0^2 + 1^2 \pmod{19}$; $2 = 1^2 + 1^2 \pmod{19}$; $3 = 4^2 + 5^2 \pmod{19}$;
$4 = 0^2 + 2^2 \pmod{19}$; $5 = 1^2 + 2^2 \pmod{19}$; $6 = 0^2 + 5^2 \pmod{19}$; $7 = 5^2 + 1^2 \pmod{19}$;
$8 = 2^2 + 2^2 \pmod{19}$; $9 = 0^2 + 3^2 \pmod{19}$; $10 = 1^2 + 3^2 \pmod{19}$; $11 = 5^2 + 9^2 \pmod{19}$;
$12 = 5^2 + 5^2 \pmod{19}$; $13 = 5^2 + 8^2 \pmod{19}$; $14 = 8^2 + 8^2 \pmod{19}$; $15 = 2^2 + 7^2 \pmod{19}$;
$16 = 4^2 + 0^2 \pmod{19}$; $17 = 0^2 + 6^2 \pmod{19}$; $18 = 7^2 + 8^2 \pmod{19}$.

- **Ex (1/4):** p =19, n = 4, and $2k$ = 4, The secret K = (5, 3, 2, 4).The equation is

$$2^2(x_1 - 5)^2 + 4^2(x_2 - 3)^2 = 1 \pmod{19}.$$

$$\Rightarrow (x_1 - 5)^2 / 10^2 + (x_2 - 2)^2 / 5^2 = 1 \pmod{19}. \ (b_1^{-1} = 10, b_2^{-1} = 5)$$

  - **Initial Phase:** The pairs in the corresponding directory file are

    (0, 0), (1, 1), (4, 2), (5, 9), (6, 5), (7, 8), (9, 3), (11, 7), (16, 4),and (17, 6).

  - **Distribution:**

    (1) Skip Step 1

    (3) Choose two pairs (r_{11}, w_{11}) and (r_{12}, w_{12}) from the directory file, such that

$$r_{11} + r_{12} \pmod{19} = 1 - \Sigma_{j = 1, 2-2}\, r_{1j} \pmod{19} = 1.$$

    Set $r_{11} = 0$ and $r_{12} = 1$. The pairs in the directory file are (0, 0) and (1, 1)

§ 4.2 ... Base...

$0 = 0^2 + 0^2 \pmod{19}$; $1 = 0^2 + 1^2 \pmod{19}$; $2 = 1^2 + 1^2 \pmod{19}$; $3 = 4^2 + 5^2 \pmod{19}$; $4 = 0^2 + 2^2 \pmod{19}$; $5 = 1^2 + 2^2 \pmod{19}$; $6 = 0^2 + 5^2 \pmod{19}$; $7 = 5^2 + 1^2 \pmod{19}$; $8 = 2^2 + 2^2 \pmod{19}$; $9 = 0^2 + 3^2 \pmod{19}$; $10 = 1^2 + 3^2 \pmod{19}$; $11 = 5^2 + 9^2 \pmod{19}$; $12 = 5^2 + 5^2 \pmod{19}$; $13 = 5^2 + 8^2 \pmod{19}$; $14 = 8^2 + 8^2 \pmod{19}$; $15 = 2^2 + 7^2 \pmod{19}$; $16 = 4^2 + 0^2 \pmod{19}$; $17 = 0^2 + 6^2 \pmod{19}$; $18 = 7^2 + 8^2 \pmod{19}$.

- **Ex (2/4):** $p = 19$, $n = 4$, and $2k = 4$, The secret $K = (5, 3, 2, 4)$.The equation is

$$2^2(x_1 - 5)^2 + 4^2(x_2 - 3)^2 = 1 \pmod{19}.$$

  - **Initial Phase:** The pairs in the corresponding directory file are
    (0, 0), (1, 1), (4, 2), (5, 9), (6, 5), (7, 8), (9, 3), (11, 7), (16, 4),and (17, 6).
  - **Distribution:**
    (4) Set $x_{11} = 10 \cdot 0 + 5 \pmod{19} = 5$ and $x_{12} = 5 \cdot 1 + 3 \pmod{19} = 8$.
    $(b_1^{-1} = 10, b_2^{-1} = 5)$
    (5) Since $(25, 5, 64, 8) = (6, 5, 7, 8)$ is linearly independent, we have $E_1 = (5, 8)$.
    (6) Similarly, we can obtain
    $E_2 = (4, 4)$, $E_3 = (16, 0)$, and $E_4 = (5, 17)$.

§ 4.2 A (k, n) Multi-secret Sharing Scheme Based on a Hyperelliptic Function (HE-TS)

- **Ex (3/4):** p =19, n = 4, and $2k$ = 4, The secret K = (5, 3, 2, 4).The equation is

$$2^2(x_1 - 5)^2 + 4^2(x_2 - 3)^2 = 1 \pmod{19}.$$

  - **Reconstruction:**

    (1) Let E_1' = (5, 8), E_2' = (4, 4), E_3' = (16, 0), and E_4' = (5, 17)

    (2) Let $x_1^2c_1 + x_1c_2 + x_2^2c_3 + x_2c_4 = 1 \pmod{19}$

    (3) Then

$$\Delta = \det\begin{pmatrix} 25 & 5 & 64 & 8 \\ 16 & 4 & 16 & 4 \\ 256 & 16 & 0 & 0 \\ 25 & 5 & 289 & 17 \end{pmatrix} \pmod{19} = \det\begin{pmatrix} 6 & 5 & 7 & 8 \\ 16 & 4 & 16 & 4 \\ 9 & 16 & 0 & 0 \\ 6 & 5 & 4 & 17 \end{pmatrix} \pmod{19} = 7$$

    Over Z_{19}^*, the inverse of 7 (mod 19) is 11.

    (4)

$$\Delta_{c_1} = \det\begin{pmatrix} 1 & 5 & 7 & 8 \\ 1 & 4 & 16 & 4 \\ 1 & 16 & 0 & 0 \\ 1 & 5 & 4 & 17 \end{pmatrix} \pmod{19} = 12 \qquad \Delta_{c_2} = \det\begin{pmatrix} 6 & 1 & 7 & 8 \\ 16 & 1 & 16 & 4 \\ 9 & 1 & 0 & 0 \\ 6 & 1 & 4 & 17 \end{pmatrix} \pmod{19} = 13$$

(c) Spring 2023, Justie Su-Tzu Juan

§ 4.2 A (k, n) Multi-secret Sharing Scheme Based on a Hyperelliptic Function (HE-TS)

- **Ex (4/4):** p =19, n = 4, and $2k$ = 4, The secret K = (5, 3, 2, 4).The equation is

$$2^2(x_1 - 5)^2 + 4^2(x_2 - 3)^2 = 1 \pmod{19}.$$

  - **Reconstruction:**

    (5) $c_1 = \Delta_{c_1}/\Delta = 12 / 7 \pmod{19} = 12 \cdot 11 \pmod{19} = 18$;

    $c_2 = \Delta_{c_2}/\Delta = 13 / 7 \pmod{19} = 13 \cdot 11 \pmod{19} = 10$.

    (6) Compute $a_1 = -(c_2 / 2c_1) \pmod{p} = -(10 / 17) \pmod{19} = -(10 \cdot 9) \pmod{19} = 5$.

    (7) Similar way to find a_2, b_1 and b_2.

§ 4.2 A (k, n) Multi-secret Sharing Scheme Based on a Hyperelliptic Function (HE-TS)

- **Discussion.**
  - The equation $\sum_{i=1}^{k} b_i^2 (x_i - a_i)^2 = 1 \pmod{p}$ contains $2k$ unknown variables.
  - The computing time of Reconstruction Phase in HE-TS is equal to the time complexity of HS-TS when the secret $K = a_i$ for some i in both scheme (perfect).
  - The length of the share that each participant be distributed is $(2k - 1)|K|$ in HS-TS. And the length of the share that each participant be distributed is $k|K|$ in HE-TS.
  - The information rate of the HE-TS is $\log_2|\mathcal{K}| / \log_2|\mathcal{S}| = \log_2 p^{2k} / \log_2 p^k = 2$.
  - When the secret $K = a_i$ for some i (in ($2k$, n)-threshold scheme):
    - The information rate of the HS-TS is $\log_2|\mathcal{K}| / \log_2|\mathcal{S}| = \log_2 p / \log_2 p^{2k-1} = 1/(2k - 1)$.
    - The information rate of the HE-TS is $\log_2|\mathcal{K}| / \log_2|\mathcal{S}| = \log_2 p / \log_2 p^k = 1/k$.