# Cryptography

**Cunsheng DING**

**HKUST, Hong Kong**

**COMP3631**

# Lecture 22: Secret Sharing Schemes

## Main Topics of This Lecture

1. A brief introduction to secret sharing.
2. An $(n, n)$-threshold scheme.
3. The Shamir $(t, n)$-threshold scheme.
4. A modified version of the Shamir $(t, n)$-threshold scheme.
5. Some references and other information on secret sharing.

# A Brief Introduction to Secret Sharing

# The Idea of Secret Sharing

**The problem:** A **dealer** has a secret $s \in \mathcal{S}$ to be shared by **a group of** $n$ **participants** in such a way that some subgroups of them can recover the secret, while other subgroups cannot do so.

**Solution:** The idea of secret sharing
The dealer designs $n$ functions $f_1, \cdots, f_n$. The dealer then computes

$$s_i = f_i(s),$$

and distributes it to one participant as his/her **share** of the secret $s$.

When some subgroup of participants meet together with their shares, they are able to compute $s$ from their shares with a **secret recovering function**.

# The Building Blocks of a Secret Sharing Scheme

**A secret space $\mathcal{S}$**: We assume that this space has equal probability distribution.

**A dealer:** A special participant who chooses a secret $s$ randomly from $\mathcal{S}$ and then computes a share of $s$ for each participant.

**A group of participants $P_i$:** they are going to share the secret designed by the dealer.

**A share computing procedure:** The dealer will follow this procedure to compute a share of $s$ for each participant.

**A secret recovering procedure:** When "some" subgroup of participants meet together with their shares, they can recover the secret $s$ by following this procedure.

# $(t, n)$-Threshold Schemes

**Definition:** Let $t$ and $n$ be positive integers, where $2 \leq t \leq n$.
A $(t, n)$**-threshold scheme** is a method of sharing a secret $s$ among a set of $n$ participants in such a way that any $t$ participants can determine $s$, but any group of $t - 1$ or fewer participants gets no information about $s$ from their shares.

**Remark:** $t$ is called the threshold value of a $(t, n)$-threshold scheme.

**Comment:** $(t, n)$-threshold schemes are a special type of secret sharing schemes.

# Scenarios Requiring Secret Sharing

**Scenario I:** A bank has a vault (a secure room) which must be opened every day. The bank employs four tellers, but the bank does not trust the combination of any two individual tellers. The bank wants to design a system whereby any three tellers can gain access to the vault, but no two of them can do so. This problem can be solved by means of **secret sharing schemes**.

**Scenario II:** According to *Time Magazine* (p. 13, May 4, 1992), the control of nuclear weapons in Russia involves a similar "2-out-of-3" access mechanism. The three parties involved are the President, the Defense Minister and the Defense Ministry.

# An $(n, n)$-Threshold Scheme

# An $(n, n)$-Threshold Scheme

**Secret:** a random binary string $s$ of $w$ bits, that is, the secret space is $\{0,1\}^w$.

**Participants:** $P_1, P_2, \cdots, P_n$.

**Computing the shares:** A dealer first chooses $n-1$ random binary strings $s_1, s_2, \cdots, s_{n-1}$ of $w$ bits, and then computes

$$s_n = s \oplus s_1 \oplus s_2 \oplus \cdots \oplus s_{n-1}.$$

The dealer finally distributes $s_i$ to $P_i$ as the share of the secret $s$.

**Recovering the secret:** When all the participants meet together with their shares, they compute the secret as

$$s = s_1 \oplus s_2 \oplus \cdots \oplus s_n.$$

**Conclusion:** This is an $(n, n)$-threshold scheme.

# The Shamir $(t, n)$-Threshold Scheme

# The Shamir $(t, n)$-Threshold Scheme

**System parameters:** A prime $p$, two positive integers $t$ and $n$, where $2 \leq t \leq n$.

**Secret space:** $\mathbf{Z}_p = \{0, 1, 2, \ldots, p-1\}$.

**Designing a secret $s$:** A dealer randomly chooses an element of $\mathbf{Z}_p$ as the secret $s$.

**Participants:** $P_1, P_2, \cdots, P_n$.

# The Shamir $(t, n)$-Threshold Scheme

**Computing and distributing the shares:** The dealer first chooses $n$ pairwise distinct nonzero elements of $\mathbf{Z}_p$, denoted by $x_i$, $1 \leq i \leq n$. The condition is that $n + 1 \leq p$.

The dealer then chooses (independently at random) $t - 1$ elements of $\mathbf{Z}_p$, $a_1, a_2, \cdots, a_{t-1}$. For each $1 \leq i \leq n$, the dealer computes $y_i = a(x_i)$, where

$$a(x) = s + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$$

and all the operations are the modulo-$p$ operations in $\mathbf{Z}_p$.

The dealer then gives $(x_i, y_i)$ to participant $P_i$ as his/her share of $s$.

**Remark:** Only the dealer knows $s$ and $a_1, \cdots, a_{t-1}$.

**Question:** Why the constants $x_i$ cannot be zero?

**Questions:** Which subgroups of participants can recover $s$? How?

# The Shamir $(t, n)$-Threshold Scheme

**Lemma:** Let $i_1, i_2, \cdots, i_t$ be $t$ distinct integers in the set $\{1, 2, \cdots, n\}$. Then the following **Vandermonde matrix**

$$A = \begin{bmatrix} 1 & x_{i_1} & x_{i_1}^2 & \cdots & x_{i_1}^{t-1} \\ 1 & x_{i_2} & x_{i_2}^2 & \cdots & x_{i_2}^{t-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{i_t} & x_{i_t}^2 & \cdots & x_{i_t}^{t-1} \end{bmatrix}$$

is invertible over the finite field $\mathbf{Z}_p$.

**Remark:** It is known that

$$\det(A) = \prod_{1 \le j < k \le t} (x_{i_k} - x_{i_j}).$$

**Attention:** All the operations are the modulo-$p$ operations in $\mathbf{Z}_p$.

# The Shamir $(t, n)$-Threshold Scheme

**Recovering the secret:** Suppose that participants $P_{i_1}, P_{i_2}, \cdots, P_{i_t}$ want to determine $s$ with their shares $(x_{i_j}, y_{i_j})$. They know that

$$y_{i_j} = a(x_{i_j}), \quad j = 1, 2, \cdots, t$$

and $a(x)$ is the (secret) polynomial chosen by the dealer. So they have

$$\begin{bmatrix} 1 & x_{i_1} & x_{i_1}^2 & \cdots & x_{i_1}^{t-1} \\ 1 & x_{i_2} & x_{i_2}^2 & \cdots & x_{i_2}^{t-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{i_t} & x_{i_t}^2 & \cdots & x_{i_t}^{t-1} \end{bmatrix} \begin{bmatrix} s \\ a_1 \\ \vdots \\ a_{t-1} \end{bmatrix} = \begin{bmatrix} y_{i_1} \\ y_{i_2} \\ \vdots \\ y_{i_t} \end{bmatrix}.$$

Since $A$ is invertible, solving this equation gives $s$.

**Conclusion:** Any subgroup of $t$ participants can recover the secret $s$.

# The Shamir $(t, n)$-Threshold Scheme

**Theorem:** Suppose the participants $P_{i_1}, P_{i_2}, \cdots, P_{i_{t-1}}$ want to determine $s$ with their shares $(x_{i_j}, y_{i_j})$. They know that

$$y_{i_j} = a(x_{i_j}), \quad j = 1, 2, \cdots, t-1$$

and $a(x)$ is the (secret) polynomial chosen by the dealer. But these $t-1$ shares $(x_{i_j}, y_{i_j})$ give no information on $s$.

**Proof:** These $t-1$ participants have

$$\begin{bmatrix} 1 & x_{i_1} & x_{i_1}^2 & \cdots & x_{i_1}^{t-1} \\ 1 & x_{i_2} & x_{i_2}^2 & \cdots & x_{i_2}^{t-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{i_{t-1}} & x_{i_{t-1}}^2 & \cdots & x_{i_{t-1}}^{t-1} \end{bmatrix} \begin{bmatrix} s \\ a_1 \\ \vdots \\ a_{t-1} \end{bmatrix} = \begin{bmatrix} y_{i_1} \\ y_{i_2} \\ \vdots \\ y_{i_{t-1}} \end{bmatrix}.$$

# Proof of the Theorem - ctd.

It follows that

$$\begin{aligned} s + a_1 x_{i_1} + a_2 x_{i_1}^2 + \cdots + a_{t-1} x_{i_1}^{t-1} &= y_{i_1} \\ s + a_1 x_{i_2} + a_2 x_{i_2}^2 + \cdots + a_{t-1} x_{i_2}^{t-1} &= y_{i_2} \\ \vdots &= \vdots \\ s + a_1 x_{i_{t-1}} + a_2 x_{i_{t-1}}^2 + \cdots + a_{t-1} x_{i_{t-1}}^{t-1} &= y_{i_{t-1}} \end{aligned}$$

# Proof of the Theorem - ctd.

Thus

$$\begin{aligned} a_1 x_{i_1} + a_2 x_{i_1}^2 + \cdots + a_{t-1} x_{i_1}^{t-1} &= y_{i_1} - s \\ a_1 x_{i_2} + a_2 x_{i_2}^2 + \cdots + a_{t-1} x_{i_2}^{t-1} &= y_{i_2} - s \\ \vdots &= \vdots \\ a_1 x_{i_{t-1}} + a_2 x_{i_{t-1}}^2 + \cdots + a_{t-1} x_{i_{t-1}}^{t-1} &= y_{i_{t-1}} - s \end{aligned}$$

# Proof of the Theorem - ctd.

Define

$$B = \begin{bmatrix} x_{i_1} & x_{i_1}^2 & \cdots & x_{i_1}^{t-1} \\ x_{i_2} & x_{i_2}^2 & \cdots & x_{i_2}^{t-1} \\ \vdots & \vdots & \vdots & \vdots \\ x_{i_{t-1}} & x_{i_{t-1}}^2 & \cdots & x_{i_{t-1}}^{t-1} \end{bmatrix}.$$

Then the system of $t-1$ equations in the previous slide can be expressed as

$$B \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_{t-1} \end{bmatrix} = \begin{bmatrix} y_{i_1} - s \\ y_{i_2} - s \\ \vdots \\ y_{i_{t-1}} - s \end{bmatrix}.$$

# Proof of the Theorem - ctd.

Clearly,

$$\begin{aligned}
\det(B) &= x_{i_1} \cdots x_{i_{t-1}} \det \begin{bmatrix} 1 & x_{i_1}^1 & \cdots & x_{i_1}^{t-2} \\ 1 & x_{i_2}^1 & \cdots & x_{i_2}^{t-2} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & x_{i_{t-1}}^1 & \cdots & x_{i_{t-1}}^{t-2} \end{bmatrix} \\
&= x_{i_1} \cdots x_{i_{t-1}} \prod_{1 \le j < k \le t-1} (x_{i_k} - x_{i_j}) \\
&\neq 0.
\end{aligned}$$

This means that $B$ is invertible.

# Proof of the Theorem - ctd.

Note that

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_{t-1} \end{bmatrix} = B^{-1} \begin{bmatrix} y_{i_1} - s \\ y_{i_2} - s \\ \vdots \\ y_{i_{t-1}} - s \end{bmatrix}.$$

For any value of $s$ in $\mathbf{Z}_p$, this set of equations has a unique solution $(a_1, \cdots, a_{t-1})$. Hence these $t-1$ shares $(x_{i_1}, y_{i_1}), \ldots, (x_{i_{t-1}}, y_{i_{t-1}})$ give no information on $s$.

# An Example of the Shamir $(t, n)$-Threshold Scheme

**System parameters:** $(p, t, n) = (17, 3, 5)$.

**Secret space:** $\mathbf{Z}_{17}$.

**Designing a secret $s$:** A dealer chose $s = 13$.

**Participants:** $P_1, P_2, P_3, P_4, P_5$.

# An Example of the Shamir $(t, n)$-Threshold Scheme

**Computing and distributing the shares:** The dealer first chose 5 distinct nonzero elements of $\mathbf{Z}_p$, $x_i = i$, $1 \leq i \leq 5$.

The dealer then chose 2 elements of $\mathbf{Z}_p$, $a_1 = 10$ and $a_2 = 2$. The dealer formed

$$a(x) = s + a_1 x + a_2 x^2 = 13 + 10x + 2x^2.$$

Then the shares are $(i, y_i)$, where

$$\begin{aligned} y_1 &= a(1) = 8, \quad & y_2 &= a(2) = 7, \\ y_3 &= a(3) = 10, \quad & y_4 &= a(4) = 0, \\ y_5 &= a(5) = 11. \end{aligned}$$

The dealer then gave $(i, y_i)$ to $P_i$ as his/her share.

# An Example of the Shamir $(t, n)$-Threshold Scheme

**Recovering the secret:** Suppose that $P_1$, $P_3$ and $P_5$ want to recover the secret $s$ with their shares. They solve the following equations

$$\begin{aligned} a(1) &= s + a_1 + a_2 = 8 = y_1, \\ a(3) &= s + 3a_1 + 9a_2 = 10 = y_3, \\ a(5) &= s + 5a_1 + 8a_2 = 11 = y_5. \end{aligned}$$

The unique solution is $(s, a_1, a_2) = (13, 10, 2)$. So $s = 13$.

# A Modified Version of the Shamir Scheme

# The Modified Shamir Scheme

**Computing and distributing the shares in the modified scheme:**
The dealer first chooses $n$ pairwise distinct nonzero elements of $\mathbf{Z}_p$, denoted by $x_i$, $1 \leq i \leq n$.

The dealer then chooses (independently at random) $t-1$ elements of $\mathbf{Z}_p$, $a_1, a_2, \cdots, a_{t-1}$. For each $1 \leq i \leq n$, the dealer computes $y_i = a'(x_i)$, where

$$a'(x) = a_{t-1} + a_1 x + a_2 x^2 + \cdots + a_{t-2} x^{t-2} + s x^{t-1}.$$

The dealer then gives $(x_i, y_i)$ to participant $P_i$ as his/her share of $s$.

**Remark:** Only the dealer knows $s$ and $a_1, \cdots, a_{t-1}$.

**Question:** Is this modified version a $(t, n)$-threshold scheme?

# Some References and Other Information

# References and other Information

**History:** The idea of secret sharing goes back to ancient times. The threshold schemes were studied independently by Blakely and Shamir in 1979.

**Comments:** Secret sharing is mathematically well defined, and some of their properties can be rigorously proved. Many secret sharing schemes have been proposed. Interested readers may consult the following references.

A. Beimel, Secret-sharing schemes: a survey, In: IWCC 2011: Coding and Cryptology pp. 11–46.

`https://link.springer.com/chapter/10.1007/978-3-642-20901-7_2`

D. G. Stinson, Cryptography: Theory and Practice, CRC Press, 1995.

# Online Demo of Shamir's Secret Sharing Scheme

In the following URLs, you find two demos of the Shamir secret sharing scheme:

`https://simon-frey.com/s4/`

`https://iancoleman.io/shamir/`

**Remark:** A software implementation of the Shamir secret sharing scheme is a good final year project!