Secret Sharing Schemes (SSS’s)

Definition
A SSS is a method of distributing shares to a number of participants, so that a subset of participants can determine the secret if and only if that subset is authorised to do so.
Definition

A **SSS** is a method of distributing shares to a number of participants, so that a subset of participants can determine the secret if and only if that subset is authorised to do so.
Authorised/Winning coalitions

The collection of authorised subsets is called access structure. From Game Theory perspective, an access structure is a simple game, and authorised subsets are winning coalitions.
The collection of authorised subsets is called *access structure*. 
The collection of authorised subsets is called *access structure*.

From Game Theory perspective, an access structure is a *simple game*, and authorised subsets are *winning coalitions*.
Authorised/Winning coalitions

- The collection of authorised subsets is called *access structure*.

- From Game Theory perspective, an access structure is a *simple game*, and authorised subsets are *winning coalitions*.
Secret $S = 10$

A $S$-SS (secret sharing scheme) is called perfect if unauthorised coalitions receive zero information about the secret.
Secret $S = 10$

Player A  
Player B
Secret $S = 10$

Player A
Share $S_1 = 6$

Player B
Share $S_2 = 4$

A SSS is called perfect if unauthorised coalitions receive zero information about the secret.
Secret $S = 10$

Player A
Share $S_1 = 6$

Player B
Share $S_2 = 4$

$S_1 + S_2 = 10$
Secret $S = 10$

Player A  
Share $S_1 = 6$

Player B  
Share $S_2 = 4$

$S_1 + S_2 = 10$

A SSS is called *perfect* if unauthorised coalitions receive zero information about the secret.
Secret $S < ab$

Player A          Player B
Secret $S < ab$

Player A

$S_1 = S \mod a$

Player B

$S_2 = S \mod b$
Secret $S < ab$

Player A

$S_1 = S \mod a$

Player B

$S_2 = S \mod b$

Solve using the Chinese Remainder Theorem
Secret $S < ab$

Player A
\[ S_1 = S \mod a \]

Player B
\[ S_2 = S \mod b \]

Solve using the Chinese Remainder Theorem

And this scheme is not perfect
**Length** of a share or secret is the number of bits used to write it.
**Length** of a share or secret is the number of bits used to write it.

**Definition**

A perfect SSS is called *ideal* if the length of the share is equal to the length of the secret.
**Length** of a share or secret is the number of bits used to write it.

**Definition**

A perfect SSS is called *ideal* if the length of the share is equal to the length of the secret.

Examples of ideal SSS are numerous, in particular, hierarchical SSS that will be considered later are ideal.
The Big Project

Problem

Characterise all ideal simple games.

This problem turned out to be extremely difficult, so the focus shifted to some subclasses of ideal simple games. The first subclass is called Weighted Simple Games (WSG), introduced by [von Neumann and Morgenstern, 1944].

Definition (Weighted simple games)

Let \( w_1, \ldots, w_n \) be a system of non-negative weights and \( q \geq 0 \).

We define \( \Gamma = \{ X \in 2^U | \sum_{i \in X} w_i \geq q \} \).
Problem

Characterise all ideal simple games.

Definition (Weighted simple games)

Let $w_1, \ldots, w_n$ be a system of non-negative weights and $q \geq 0$. We define

\[ \Gamma = \{ X \subseteq U | \sum_{i \in X} w_i \geq q \} \]
Problem

*Characterise all ideal simple games.*

This problem turned out to be extremely difficult, so the focus shifted to some subclasses of ideal simple games.
Characterise all ideal simple games.

- This problem turned out to be extremely difficult, so the focus shifted to some subclasses of ideal simple games.
- The first subclass is called Weighted Simple Games (WSG), introduced by [von Neumann and Morgenstern, 1944].

Definition (Weighted simple games)

Let $w_1, \ldots, w_n$ be a system of non-negative weights and $q \geq 0$. We define $\Gamma = \{ X \in 2^U | \sum_{i \in X} w_i \geq q \}$. 
The Big Project

Problem

Characterise all ideal simple games.

- This problem turned out to be extremely difficult, so the focus shifted to some subclasses of ideal simple games.
- The first subclass is called Weighted Simple Games (WSG), introduced by [von Neumann and Morgenstern, 1944].

Definition (Weighted simple games)

Let $w_1, \ldots, w_n$ be a system of non-negative weights and $q \geq 0$. We define

$$\Gamma = \{ X \in 2^U \mid \sum_{i \in X} w_i \geq q \}.$$
Example of weightedness

Example

An electronic fund transfer of a large sum of money can be authorised by either:

1. two general managers, or
2. three senior tellers, or
3. one general manager and two senior tellers.

If the two general managers have weights $w_{1a} = w_{1b} = 3$, and
If the three senior tellers have weights $w_{2a} = w_{2b} = w_{2c} = 2$, such that $q = 6$, then this is a weighted game.
Ideal WSG’s have been characterised.
Ideal WSG’s have been characterised.

A player whose removal from a winning coalition keeps the coalition winning is *Dummy*.
Characterisation of Ideal WSG’s

- Ideal WSG’s have been characterised.
- A player whose removal from a winning coalition keeps the coalition winning is *Dummy*.
- The characterisation is for simple games with no dummies.
Ideal WSG’s have been characterised.
A player whose removal from a winning coalition keeps the coalition winning is *Dummy*.

The characterisation is for simple games with no dummies.

**Theorem (Beimel, Tassa and Weinreb, 2008)**

A WSG $\Gamma$ is ideal iff one of the following three conditions holds:

- $\Gamma$ is a hierarchical simple game of at most two levels;
- $\Gamma$ is a tripartite simple game;
- $\Gamma$ is a composition of two ideal WSG’s.
The next step

Definition (Roughly Weighted (RWSG))

- If $X \in 2^U$ is such that $\sum_{i \in X} w_i > q$, then $X$ is authorized (belongs to $\Gamma$);
- If $Y \in 2^U$ is such that $\sum_{i \in Y} w_i < q$, then $Y$ is not authorized.
- If $Z \in 2^U$ is such that $\sum_{i \in Z} w_i = q$, then a tie-breaking rule will decide whether the set is authorized or not.

Problem: Characterise all ideal RWSGs.
The next step

Definition (Roughly Weighted (RWSG))

- If $X \in 2^U$ is such that $\sum_{i \in X} w_i > q$, then $X$ is authorized (belongs to $\Gamma$);
- If $Y \in 2^U$ is such that $\sum_{i \in Y} w_i < q$, then $Y$ is not authorized.

Problem
Characterise all ideal RWSGs.
### Definition (Roughly Weighted (RWSG))

- If \( X \in 2^U \) is such that \( \sum_{i \in X} w_i > q \), then \( X \) is authorized (belongs to \( \Gamma \));
- If \( Y \in 2^U \) is such that \( \sum_{i \in Y} w_i < q \), then \( Y \) is not authorized.
- If \( Z \in 2^U \) is such that \( \sum_{i \in Z} w_i = q \), then a tie-breaking rule will decide whether the set is authorized or not.
The next step

**Definition (Roughly Weighted (RWSG))**

- If $X \in 2^U$ is such that $\sum_{i \in X} w_i > q$, then $X$ is authorized (belongs to $\Gamma$);
- If $Y \in 2^U$ is such that $\sum_{i \in Y} w_i < q$, then $Y$ is not authorized.
- If $Z \in 2^U$ is such that $\sum_{i \in Z} w_i = q$, then a tie-breaking rule will decide whether the set is authorized or not.

Problem: Characterise all ideal RWSGs.
The next step

**Definition (Roughly Weighted (RWSG))**

- If $X \in 2^U$ is such that $\sum_{i \in X} w_i > q$, then $X$ is authorized (belongs to $\Gamma$);
- If $Y \in 2^U$ is such that $\sum_{i \in Y} w_i < q$, then $Y$ is not authorized.
- If $Z \in 2^U$ is such that $\sum_{i \in Z} w_i = q$, then a tie-breaking rule will decide whether the set is authorized or not.

**Problem**

*Characterise all ideal RWSGs.*
The natural class of Hierarchical simple games (HSG’s)

Figure: An m-level hierarchical simple game
In a DHSG, a coalition of participants is authorised if it contains at least $k_1$ members from level 1, or $k_2$ members from levels 1 and 2, or $k_3$ members from levels 1, 2 and 3 etc.
Definiton

In a DHSG, a coalition of participants is authorised if it contains at least $k_1$ members from level 1, or $k_2$ members from levels 1 and 2, or $k_3$ members from levels 1, 2 and 3 etc.

Example

An electronic fund transfer of a large sum of money can be authorised by either:

1. two general managers, or
2. three senior tellers, or
3. one general manager and two senior tellers.

So it is two levels:
The general managers $L_1$ with $k_1 = 2$, and
The senior tellers $L_2$ with $k_2 = 3$. 
Conjunctive Hierarchical simple game (CHSG)

**Definition**

In a CHSG, a coalition of participants is authorised if it contains at least \( k_1 \) members from level 1, *and* \( k_2 \) members from levels 1 and 2, *and* \( k_3 \) members from levels 1, 2 and 3 etc.
Conjunctive Hierarchical simple game (CHSG)

**Definition**

In a CHSG, a coalition of participants is authorised if it contains at least $k_1$ members from level 1, \textit{and} $k_2$ members from levels 1 and 2, \textit{and} $k_3$ members from levels 1, 2 and 3 etc.

**Example**

A passage of a resolution in the United Nations Security Council requires the vote of at least:

1. 9 members in total, \textit{and}
2. at least 5 permanent members.

So it is two levels:

The permanent members $L_1$ with $k_1 = 5$, \textit{and}

The non-permanent members $L_2$ with $k_2 = 9$. 
A coalition $X$ is said to be *blocking*, if $X^c$ is losing.
A coalition $X$ is said to be \textit{blocking}, if $X^c$ is losing.

\begin{definition}
The simple games $G$ and $G^d$ are duals of each other if the winning coalitions of $G^d$ are the blocking coalitions of $G$.
\end{definition}
A coalition $X$ is said to be \textit{blocking}, if $X^c$ is losing.

**Definition**

The simple games $G$ and $G^d$ are duals of each other if the winning coalitions of $G^d$ are the blocking coalitions of $G$.

**Theorem**

*DHSG’s and CHSG’s are duals of each other.*
A coalition $X$ is said to be *blocking*, if $X^c$ is losing.

**Definition**

The simple games $G$ and $G^d$ are duals of each other if the winning coalitions of $G^d$ are the blocking coalitions of $G$.

**Theorem**

*DHSG’s and CHSG’s are duals of each other.*

**Example**

The DHSG $k = (2, 4), \ n = (2, 4)$, is the dual game of the CHSG $k = (1, 3), \ n = (2, 4)$
A coalition $X$ is said to be blocking, if $X^c$ is losing.

**Definition**

The simple games $G$ and $G^d$ are duals of each other if the winning coalitions of $G^d$ are the blocking coalitions of $G$.

**Theorem**

DHSG’s and CHSG’s are duals of each other.

**Example**

The DHSG $k = (2, 4), n = (2, 4)$, is the dual game of the CHSG $k = (1, 3), n = (2, 4)$.

$\{1^2, 2\}$ is blocking in DHSG and is winning in CHSG,

$\{1, 2^2\}$ is blocking in DHSG and is winning in CHSG.
Weighted DHSG's

A trivial level is a level whose players either form authorised coalitions individually, or they are dummies.

Theorem (Beimel, Tassa and Weinreb, 2008)
A HSG is weighted iff it has up to four levels but only two non-trivial. The non-trivial levels $L_i, L_{i+1}$ must have either:

- $k_i + 1 = k_{i+1}$,
- $n_i + 1 = k_{i+1} - k_{i+1} - 1$.

An analogue of the above theorem for CHSG's is found by Duality.
A *trivial level* is a level whose players either form authorised coalitions individually, or they are dummies.
A *trivial level* is a level whose players either form authorised coalitions individually, or they are dummies.

**Theorem (Beimel, Tassa and Weinreb, 2008)**

*An HSG is weighted iff it has up to four levels but only two non-trivial. The non-trivial levels $L_i, L_{i+1}$ must have either:*

- $k_{i+1} = k_i + 1$, or
- $n_{i+1} = k_{i+1} - k_i + 1$. 
A trivial level is a level whose players either form authorised coalitions individually, or they are dummies.

**Theorem (Beimel, Tassa and Weinreb, 2008)**

A HSG is weighted iff it has up to four levels but only two non-trivial. The non-trivial levels $L_i, L_{i+1}$ must have either:

- $k_{i+1} = k_i + 1$, or
- $n_{i+1} = k_{i+1} - k_i + 1$.

- An analogue of the above theorem for CHSG’s is found by Duality.
Some definitions

In an access structure $\Gamma$, $i$ is said to be more senior than $j$, formally $i \succeq \Gamma j$, if $X \cup \{j\} \in \Gamma$ implies $X \cup \{i\} \in \Gamma$ for every set $X \subseteq U$ not containing $i$ and $j$. The game is called complete if $\succeq \Gamma$ is a total order.

A shift is a replacement of a player by a less senior one. A shift-maximal coalition is a losing coalition whose every superset is winning and cannot be obtained from any losing coalition by a shift.
Some definitions

In an access structure $\Gamma$, $i$ is said to be more senior than $j$, formally $i \succeq_\Gamma j$, if $X \cup \{j\} \in \Gamma$ implies $X \cup \{i\} \in \Gamma$ for every set $X \subseteq U$ not containing $i$ and $j$. The game is called \textit{complete} if $\succeq_\Gamma$ is a total order.
Some definitions

In an access structure $\Gamma$, $i$ is said to be more senior than $j$, formally $i \succeq_{\Gamma} j$, if $X \cup \{j\} \in \Gamma$ implies $X \cup \{i\} \in \Gamma$ for every set $X \subseteq U$ not containing $i$ and $j$. The game is called complete if $\succeq_{\Gamma}$ is a total order.

A shift is a replacement of a player by a less senior one.
Some definitions

- In an access structure $\Gamma$, $i$ is said to be more senior than $j$, formally $i \succeq_{\Gamma} j$, if $X \cup \{j\} \in \Gamma$ implies $X \cup \{i\} \in \Gamma$ for every set $X \subseteq U$ not containing $i$ and $j$. The game is called complete if $\succeq_{\Gamma}$ is a total order.

- A *shift* is a replacement of a player by a less senior one.

- A *shift-maximal* coalition is a losing coalition whose every superset is winning and cannot be obtained from any losing coalition by a shift.
The main tool in the characterisation:

**Theorem**

*The class of disjunctive hierarchical simple games are exactly the class of complete games with a unique shift-maximal losing coalition.*
Which HSGs are roughly weighted but not weighted?

The main tool in the characterisation:

**Theorem**

The class of disjunctive hierarchical simple games are exactly the class of complete games with a unique shift-maximal losing coalition.

- An analogue of the above theorem for CHSG’s is also found by Duality.
Theorem

A DHSG is roughly weighted if and only if it has up to three non-trivial levels, such that:

Example (i) $k_1 = 2$, $k_2 = 3$, $k_3 = 4$, with $n_1 = 2$, $n_2 = 2$, $n_3 = 3$ denoted $k = (2, 3, 4)$, $n = (2, 2, 3)$;

(ii) $k = (3, 4, 6)$, $n = (3, 3, 3)$. 

A characterisation for the Roughly weighted CHSG's is also found by Duality.
A DHSG is roughly weighted if and only if it has up to three non-trivial levels, such that:

- If it has two levels $L_i, L_{i+1}$, then $k_{i+1} = k_i + 2$.

Example:

(i) $k_1 = 2, k_2 = 3, k_3 = 4$, with $n_1 = 2, n_2 = 2, n_3 = 3$ denoted $k = (2, 3, 4)$, $n = (2, 2, 3)$.

(ii) $k = (3, 4, 6)$, $n = (3, 3, 3)$.

A characterisation for the roughly weighted CHSG's is also found by Duality.
Roughly Weighted DHSG that are non-weighted

Theorem

A DHSG is roughly weighted if and only if it has up to three non-trivial levels, such that:

- If it has two levels $L_i, L_{i+1}$, then $k_{i+1} = k_i + 2$;
- If it has three levels, then some restrictions apply to the number of players of each level;
A DHSG is roughly weighted if and only if it has up to three non-trivial levels, such that:

- If it has two levels $L_i, L_{i+1}$, then $k_{i+1} = k_i + 2$;
- If it has three levels, then some restrictions apply to the number of players of each level;

Example

(i) $k_1 = 2, k_2 = 3, k_3 = 4$, with $n_1 = 2, n_2 = 2, n_3 = 3$ denoted $k = (2, 3, 4), n = (2, 2, 3)$;
Theorem

A DHSG is roughly weighted if and only if it has up to three non-trivial levels, such that:

- If it has two levels $L_i, L_{i+1}$, then $k_{i+1} = k_i + 2$;
- If it has three levels, then some restrictions apply to the number of players of each level;

Example

(i) $k_1 = 2, k_2 = 3, k_3 = 4$, with $n_1 = 2, n_2 = 2, n_3 = 3$ denoted $k = (2, 3, 4), n = (2, 2, 3)$;
(ii) $k = (3, 4, 6), n = (3, 3, 3)$. 
A DHSG is roughly weighted if and only if it has up to three non-trivial levels, such that:

- If it has two levels $L_i, L_{i+1}$, then $k_{i+1} = k_i + 2$;
- If it has three levels, then some restrictions apply to the number of players of each level;

**Example**

(i) $k_1 = 2, k_2 = 3, k_3 = 4$, with $n_1 = 2, n_2 = 2, n_3 = 3$ denoted $k = (2, 3, 4), n = (2, 2, 3)$;
(ii) $k = (3, 4, 6), n = (3, 3, 3)$.

A characterisation for the Roughly weighted CHSG’s is also found by **Duality**.
THANK YOU!