CS 594 – Advanced Crypto (Spring 2026)

Alex Block

Lecture 6

February 4, 2026

Secret Sharing

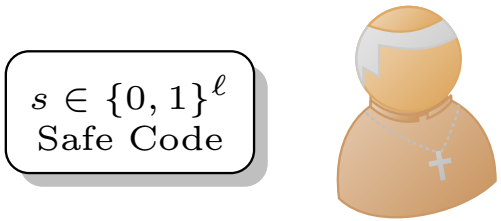
How Can You Securely Share a Secret?

How Can You Securely Share a Secret?

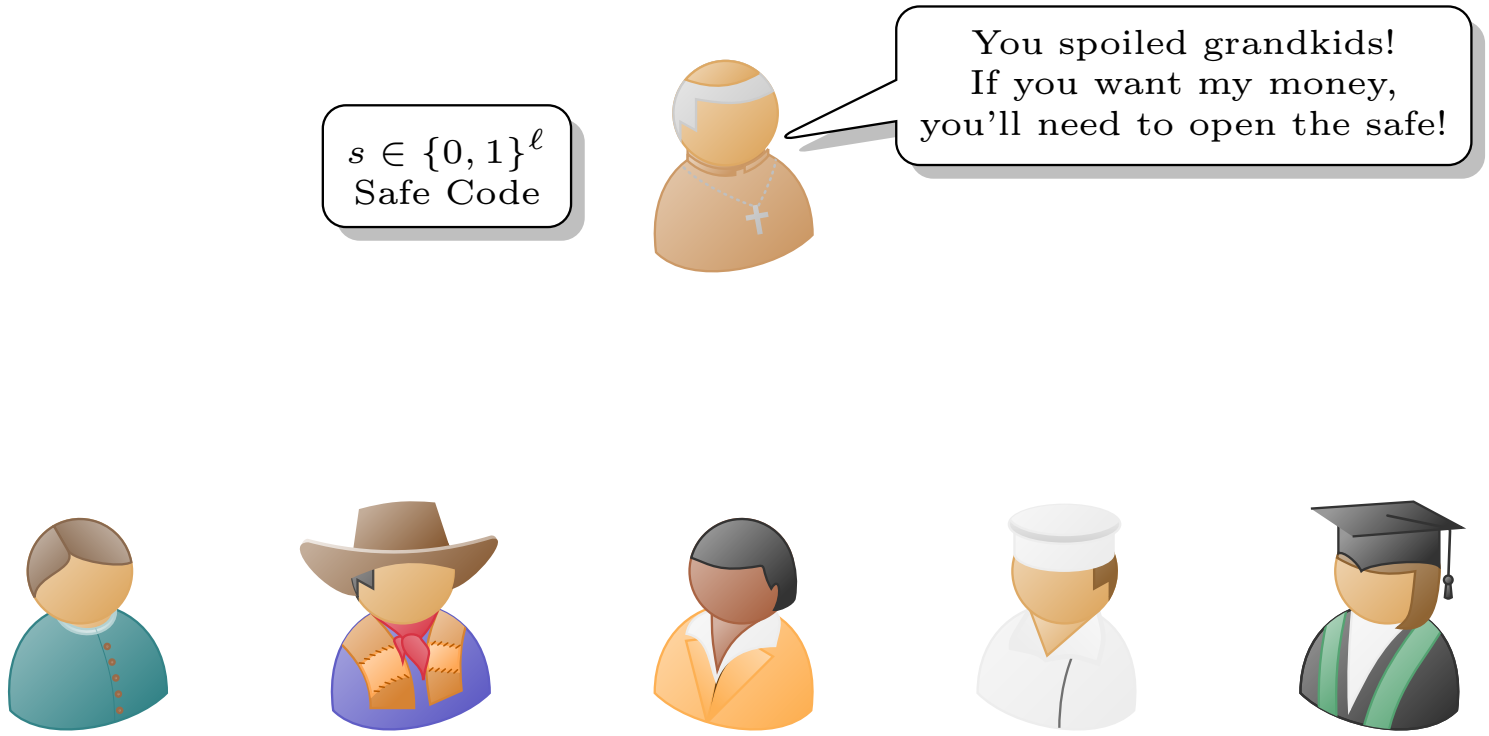
How Can You Securely Share a Secret?

$s \in \{0,1\}^\ell$
Safe Code

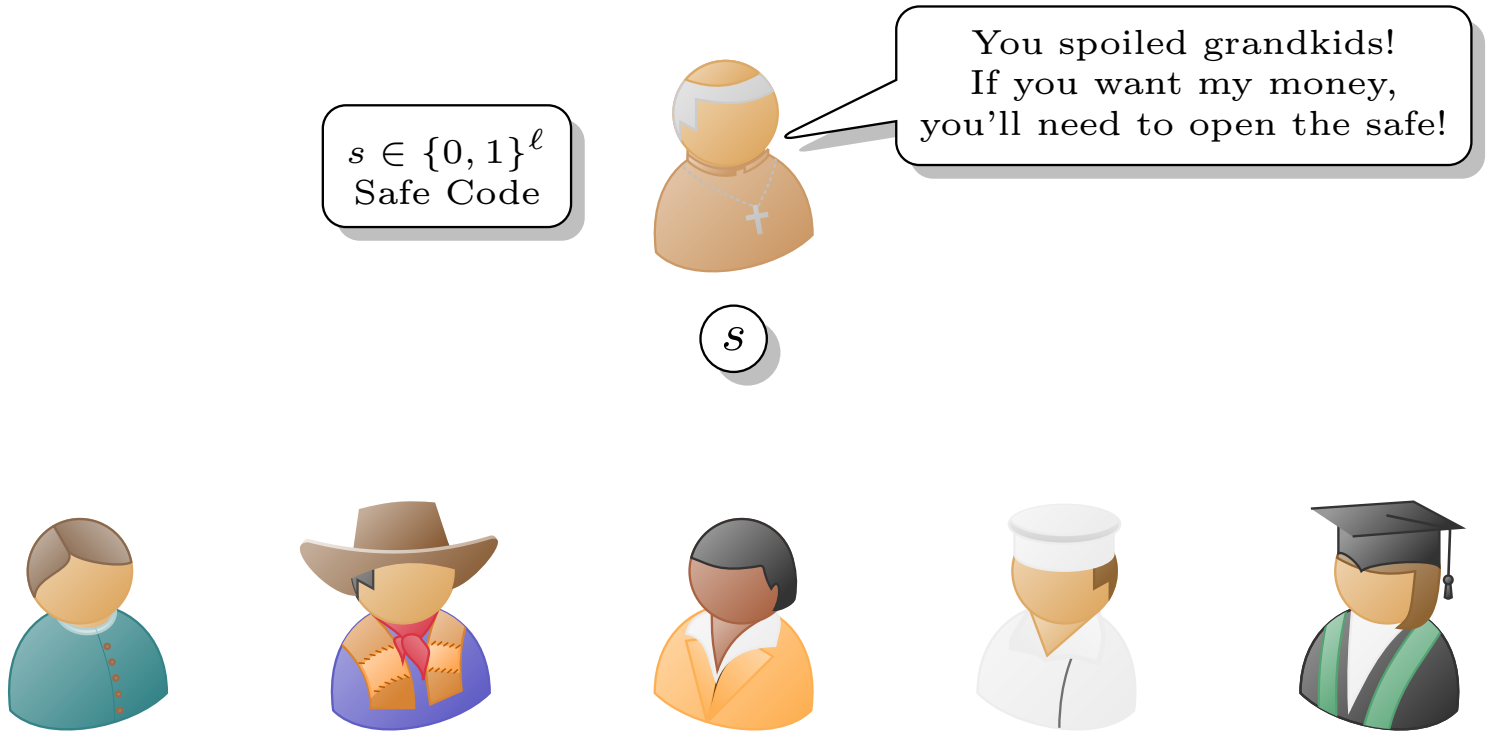
How Can You Securely Share a Secret?



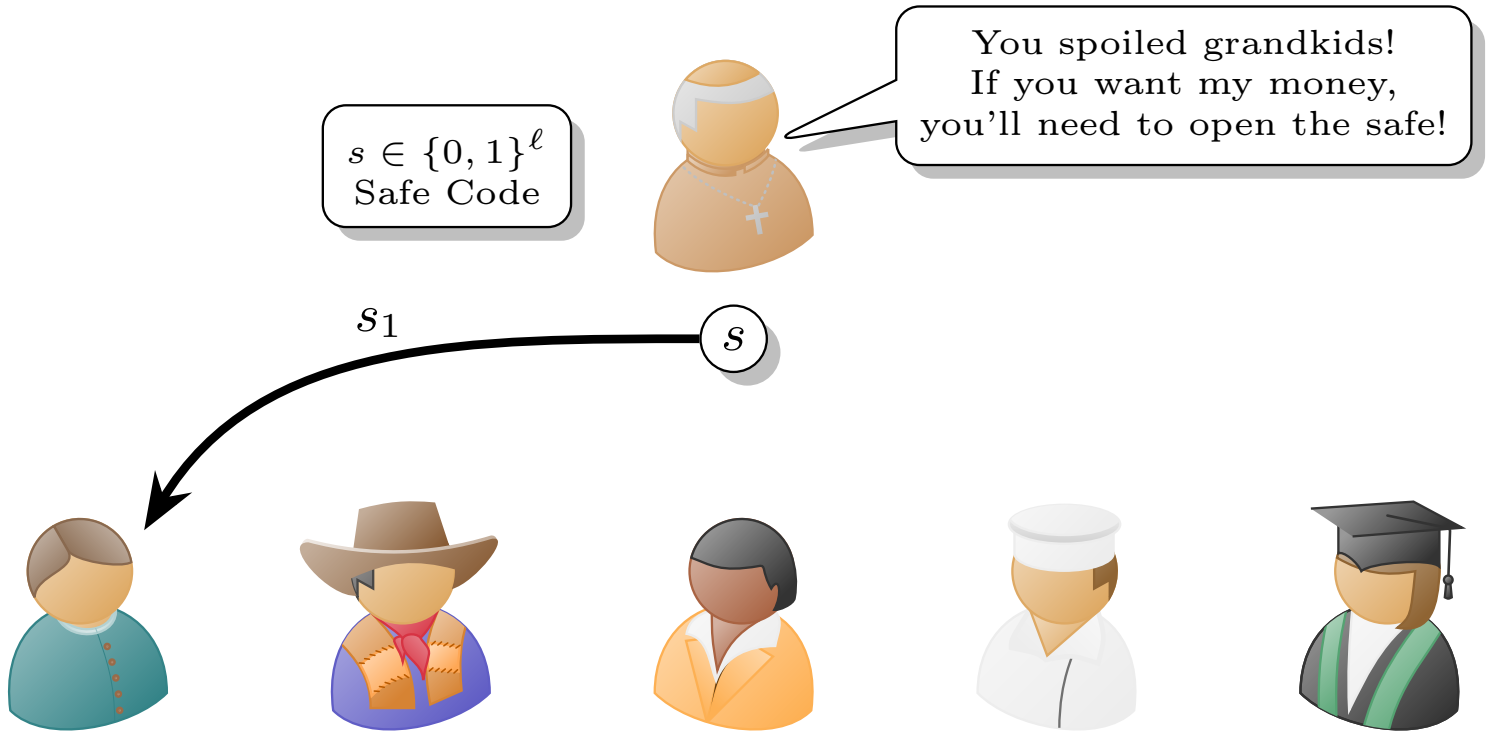
How Can You Securely Share a Secret?



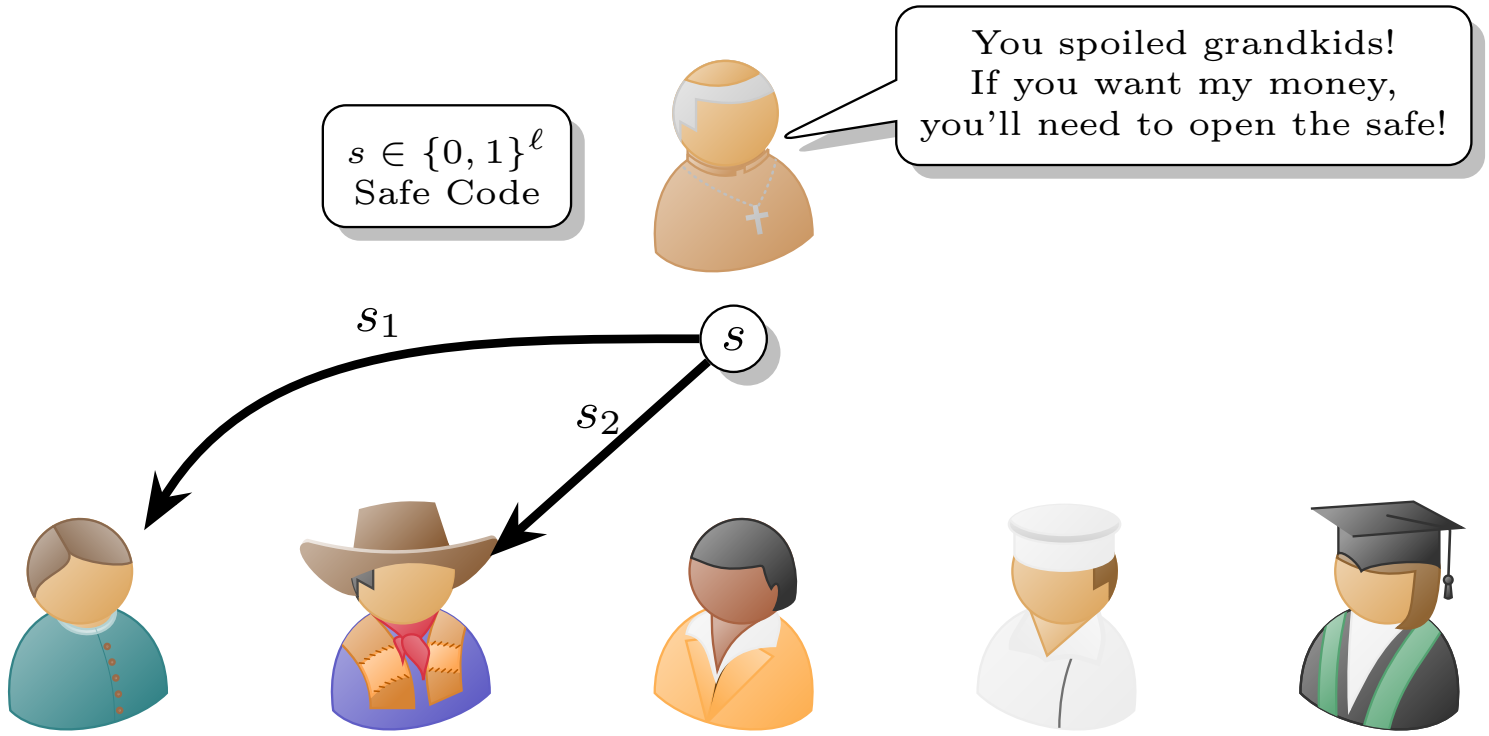
How Can You Securely Share a Secret?



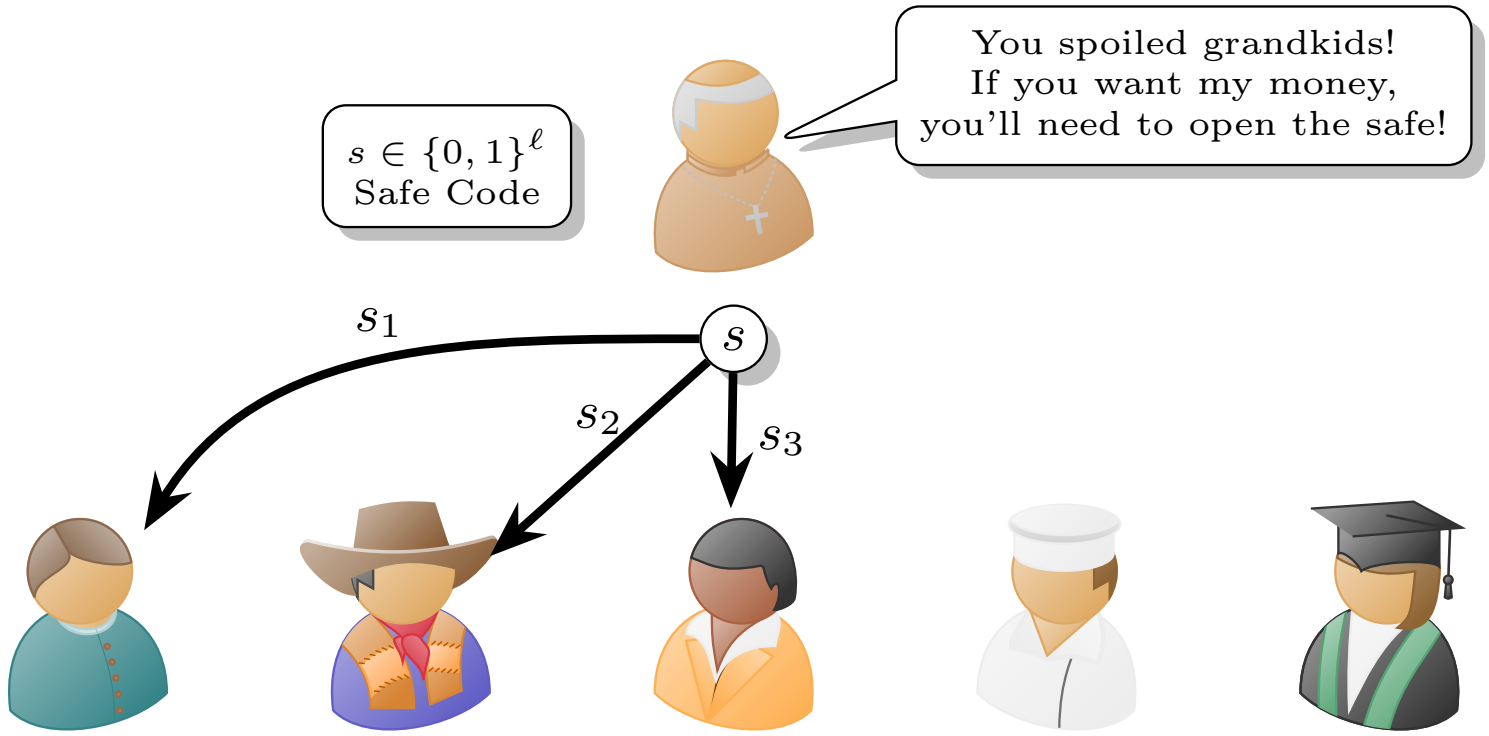
How Can You Securely Share a Secret?



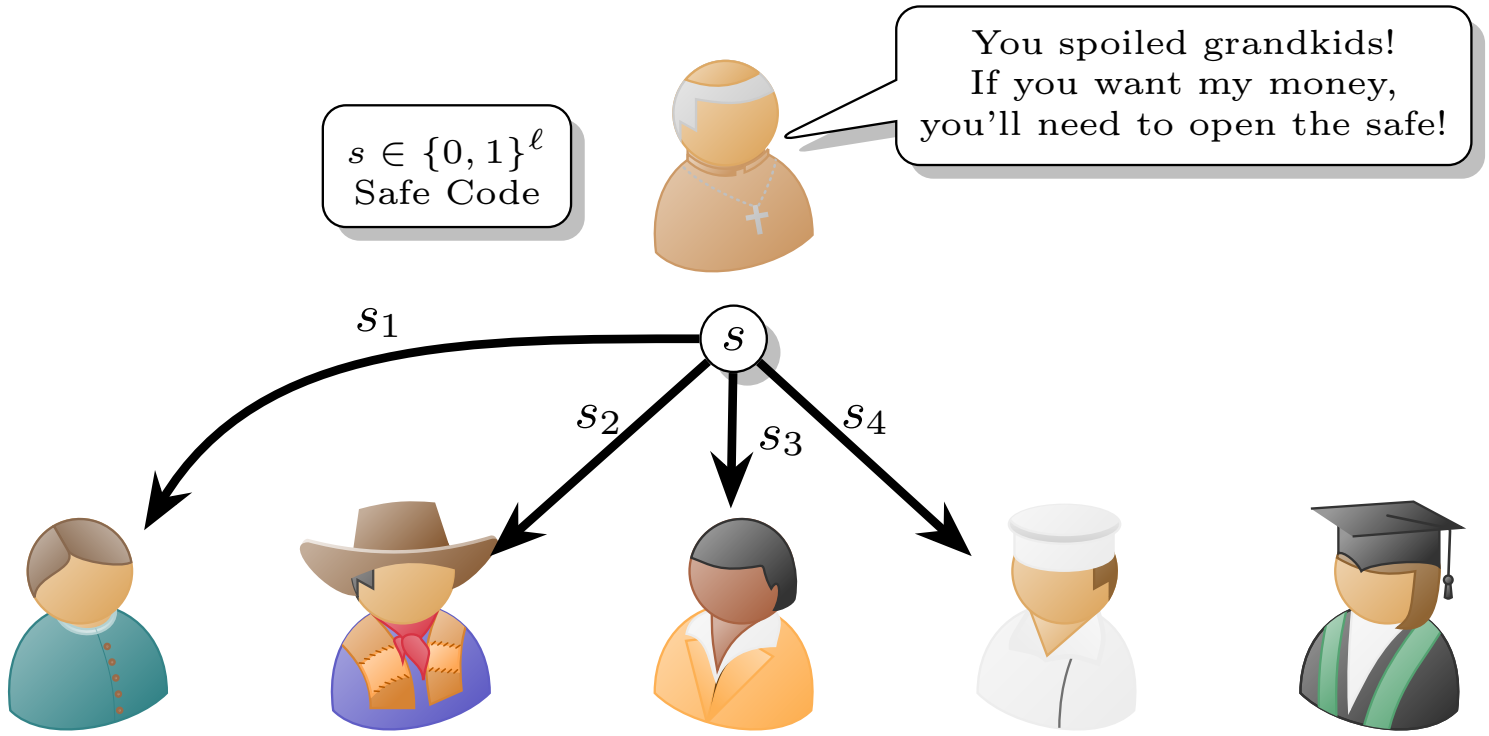
How Can You Securely Share a Secret?



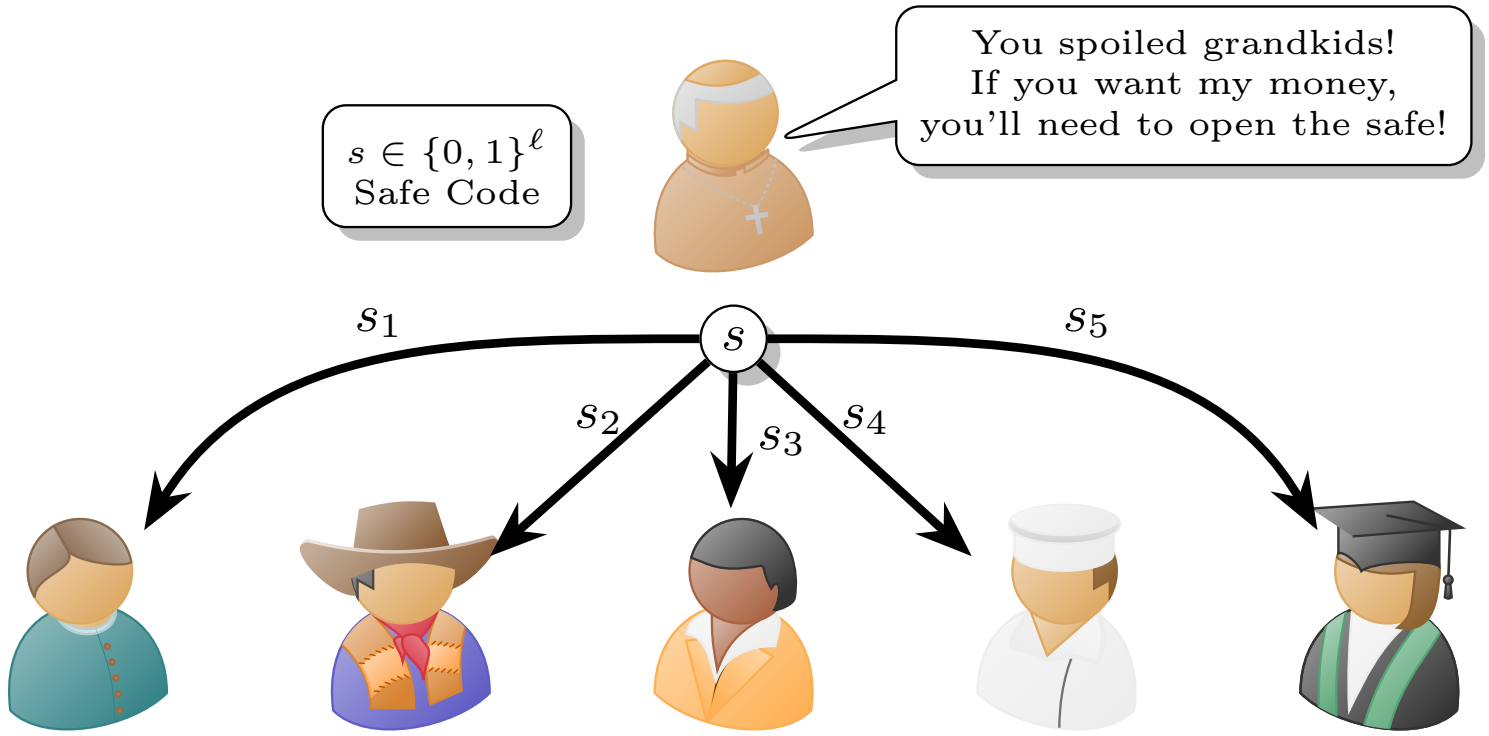
How Can You Securely Share a Secret?



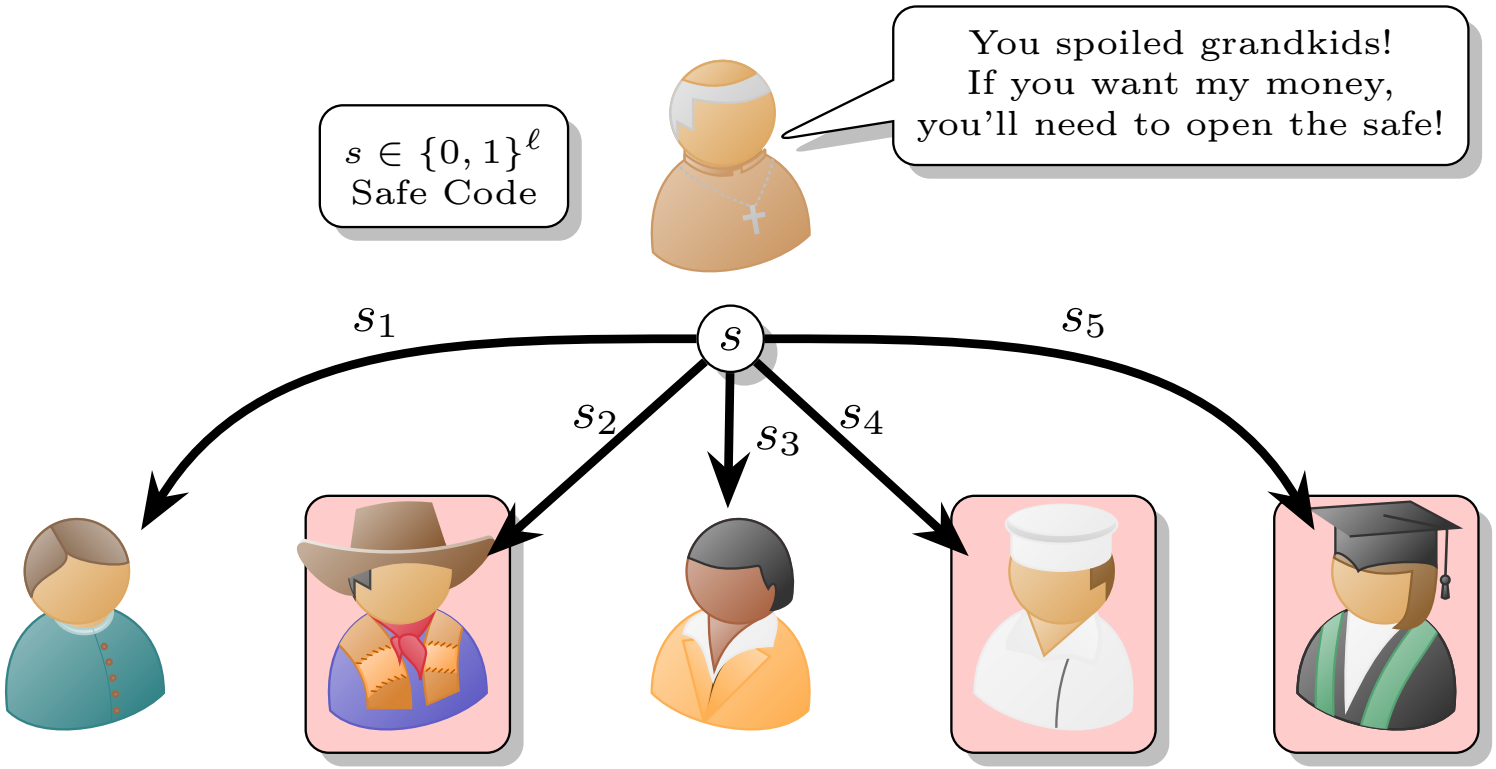
How Can You Securely Share a Secret?



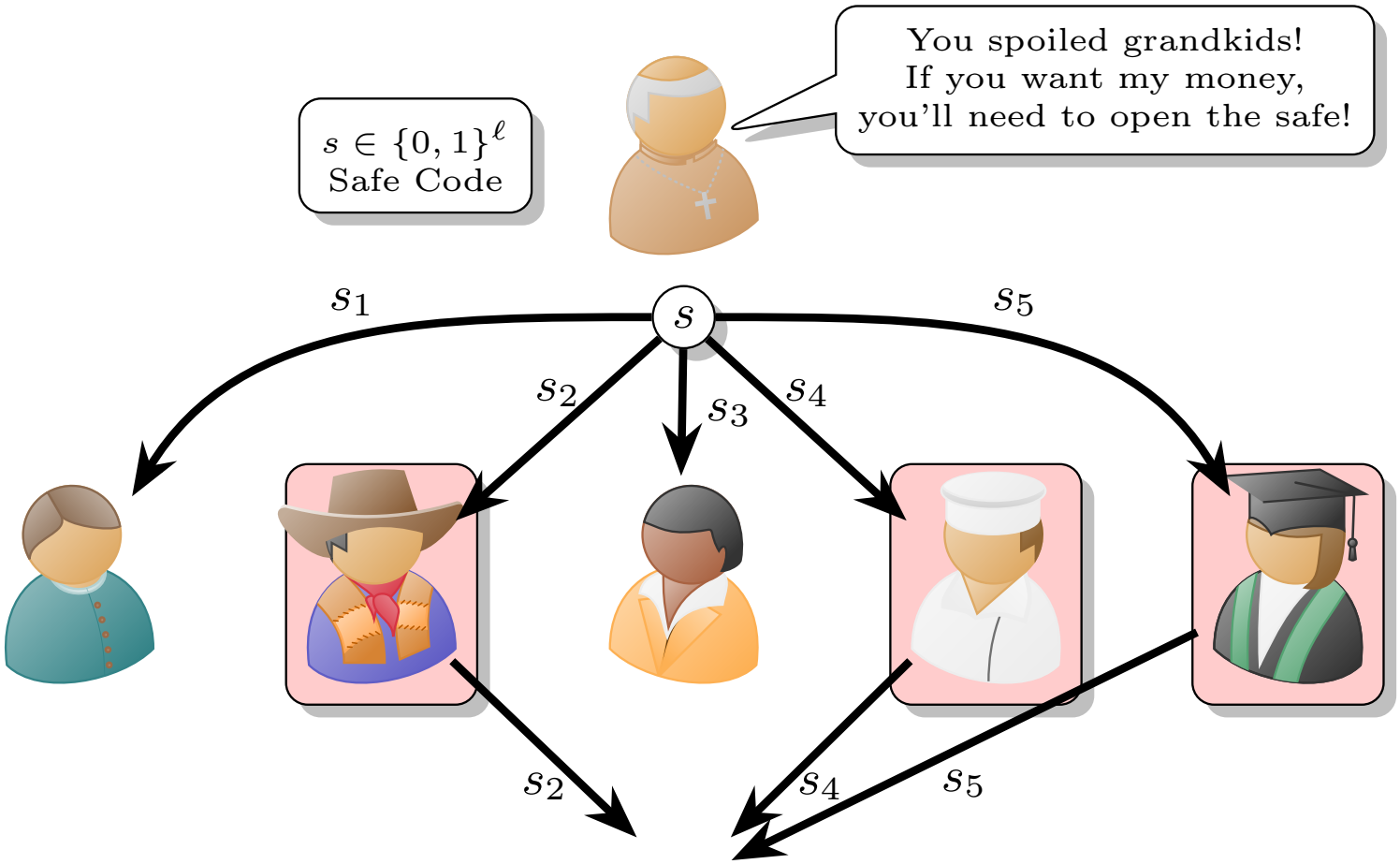
How Can You Securely Share a Secret?



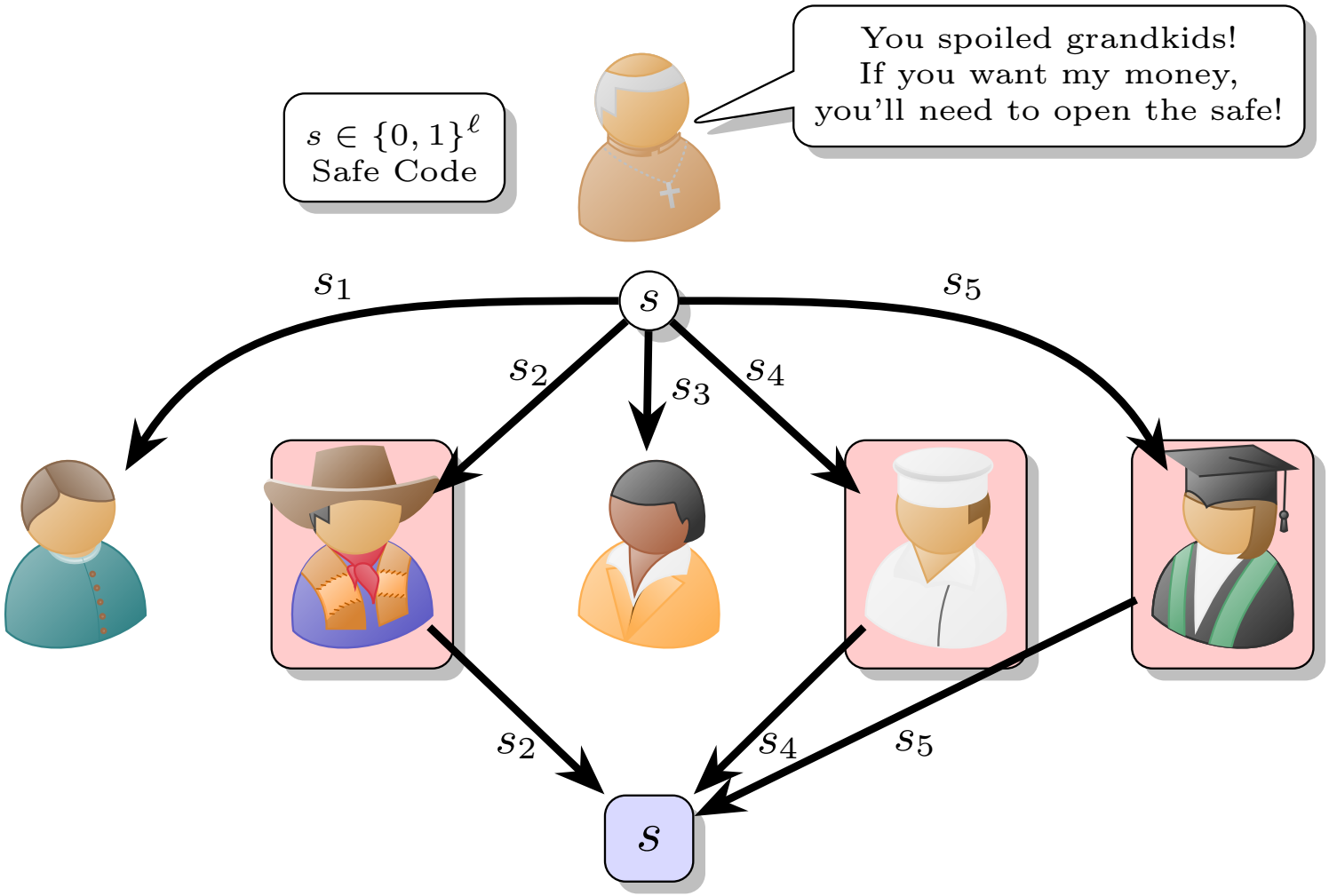
How Can You Securely Share a Secret?



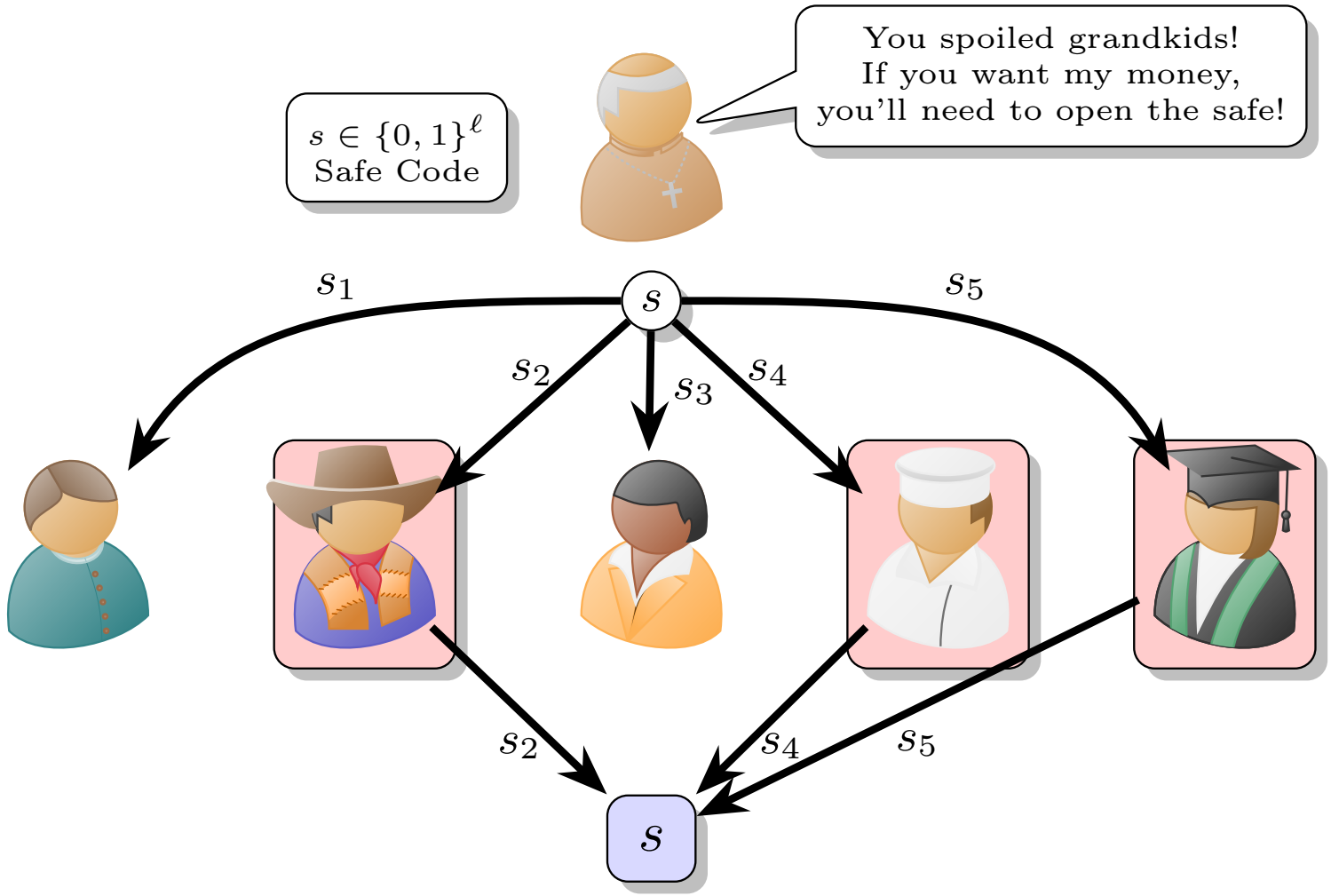
How Can You Securely Share a Secret?



How Can You Securely Share a Secret?



How Can You Securely Share a Secret?



$(3,5)$-threshold secret-sharing scheme

(Threshold) Secret Sharing

(Threshold) Secret Sharing

- Given a secret s, a *secret sharing scheme* is a way to encode s into several pieces called *shares* that you can share with multiple *parties*.

(Threshold) Secret Sharing

- Given a secret s, a *secret sharing scheme* is a way to encode s into several pieces called *shares* that you can share with multiple *parties*.

Definition 1 (t-out-of-n secret-sharing)

(Threshold) Secret Sharing

- Given a secret s, a *secret sharing scheme* is a way to encode s into several pieces called *shares* that you can share with multiple *parties*.

Definition 1 (t-out-of-n secret-sharing)

A (t, n)*(-threshold) secret-sharing scheme* consists of two alphabets: a set of *secrets* $\mathcal{M}$ and a set of *shares* $\mathcal{S}$;

(Threshold) Secret Sharing

- Given a secret s, a *secret sharing scheme* is a way to encode s into several pieces called *shares* that you can share with multiple *parties*.

Definition 1 (t-out-of-n secret-sharing)

A (t, n)*(-threshold) secret-sharing scheme* consists of two alphabets: a set of *secrets* $\mathcal{M}$ and a set of *shares* $\mathcal{S}$; and consists of the following algorithms:

(Threshold) Secret Sharing

- Given a secret s, a *secret sharing scheme* is a way to encode s into several pieces called *shares* that you can share with multiple *parties*.

Definition 1 (t-out-of-n secret-sharing)

A (t, n)*(-threshold) secret-sharing scheme* consists of two alphabets: a set of *secrets* $\mathcal{M}$ and a set of *shares* $\mathcal{S}$; and consists of the following algorithms:

- Share: $\mathcal{M} \to \mathcal{S}^n$ is a randomized algorithm that takes as input a secret $m \in \mathcal{M}$ and outputs a list of n *shares* $S \in \mathcal{S}^n$.

just a set

(i, s)

(Threshold) Secret Sharing

- Given a secret s, a *secret sharing scheme* is a way to encode s into several pieces called *shares* that you can share with multiple *parties*.

Definition 1 (t-out-of-n secret-sharing)

A (t, n)*(-threshold) secret-sharing scheme* consists of two alphabets: a set of *secrets* $\mathcal{M}$ and a set of *shares* $\mathcal{S}$; and consists of the following algorithms:

- $\mathsf{Share}\colon \mathcal{M} \to \mathcal{S}^n$ is a randomized algorithm that takes as input a secret $m \in \mathcal{M}$ and outputs a list of n *shares* $S \in \mathcal{S}^n$.
- $\mathsf{Reconstruct}\colon \mathcal{S}^{\leqslant n} \to \mathcal{M}$ is a deterministic algorithm which takes a (partial) list of shares $S \in \mathcal{S}$ as inputs and outputs a value $m \in \mathcal{M}$.

(Threshold) Secret Sharing

- Given a secret s, a *secret sharing scheme* is a way to encode s into several pieces called *shares* that you can share with multiple *parties*.

Definition 1 (t-out-of-n secret-sharing)

A (t, n)*(-threshold) secret-sharing scheme* consists of two alphabets: a set of *secrets* $\mathcal{M}$ and a set of *shares* $\mathcal{S}$; and consists of the following algorithms:

- $\mathsf{Share}\colon \mathcal{M} \to \mathcal{S}^n$ is a randomized algorithm that takes as input a secret $m \in \mathcal{M}$ and outputs a list of n *shares* $S \in \mathcal{S}^n$.
- $\mathsf{Reconstruct}\colon \mathcal{S}^{\leqslant n} \to \mathcal{M}$ is a deterministic algorithm which takes a (partial) list of shares $S \in \mathcal{S}$ as inputs and outputs a value $m \in \mathcal{M}$.

t is the *threshold* of the scheme and n is the *number of parties/shares*.

Secret Sharing: Correctness

Secret Sharing: Correctness

- A (t, n) secret-sharing scheme should allow:

Secret Sharing: Correctness

- A (t, n) secret-sharing scheme should allow:
  - Any group of $\geqslant t$ parties to recover the secret hidden in their shares; and

Secret Sharing: Correctness

- A (t, n) secret-sharing scheme should allow:
  - Any group of $\geqslant t$ parties to recover the secret hidden in their shares; and
  - Any group of $< t$ parties to learn *nothing* about the secret.

Secret Sharing: Correctness

- A (t, n) secret-sharing scheme should allow:
  - Any group of $\geqslant t$ parties to recover the secret hidden in their shares; and
  - Any group of $< t$ parties to learn *nothing* about the secret.

Definition 2 (Correctness of (t, n) secret-sharing)

Secret Sharing: Correctness

- A (t, n) secret-sharing scheme should allow:
  - Any group of $\geqslant t$ parties to recover the secret hidden in their shares; and
  - Any group of $< t$ parties to learn *nothing* about the secret.

Definition 2 (Correctness of (t, n) secret-sharing)

A (t, n) secret-sharing scheme $(\mathsf{Share}, \mathsf{Reconstruct})$ is *correct* if

Secret Sharing: Correctness

- A (t, n) secret-sharing scheme should allow:
  - Any group of $\geqslant t$ parties to recover the secret hidden in their shares; and
  - Any group of $< t$ parties to learn *nothing* about the secret.

Definition 2 (Correctness of (t, n) secret-sharing)

A (t, n) secret-sharing scheme $(\mathsf{Share}, \mathsf{Reconstruct})$ is *correct* if for all $m \in \mathcal{M}$ and for any $T \subset [n]$ such that $|T| \geqslant t$, we have

Secret Sharing: Correctness

- A (t, n) secret-sharing scheme should allow:
  - Any group of $\geqslant t$ parties to recover the secret hidden in their shares; and
  - Any group of $< t$ parties to learn *nothing* about the secret.

Definition 2 (Correctness of (t, n) secret-sharing)

A (t, n) secret-sharing scheme $(\mathsf{Share}, \mathsf{Reconstruct})$ is *correct* if for all $m \in \mathcal{M}$ and for any $T \subset [n]$ such that $|T| \geqslant t$, we have

$$\Pr\left[\mathsf{Reconstruct}\left((\mathsf{Share}(m)_i)_{i \in T}\right) = m\right] = 1$$

$(\mathsf{Share}(m) \to (s_1, \ldots, s_n))_{i \in [T]}$

$T = \{i_1, \ldots, i_{|T|}\} \mapsto (s_{i_1}, \ldots, s_{i_{|T|}})$

Secret Sharing: Security

Secret Sharing: Security

- How can we define what we mean by $< t$ parties learn *nothing*?

Secret Sharing: Security

- How can we define what we mean by $< t$ parties learn *nothing*?
  - Any subset of $< t$ shares should look *uniformly random*.

Secret Sharing: Security

- How can we define what we mean by $< t$ parties learn *nothing*?
  - Any subset of $< t$ shares should look *uniformly random*.

Definition 3 (Security of (t, n) secret-sharing)

Secret Sharing: Security

- How can we define what we mean by $< t$ parties learn *nothing*?
  - Any subset of $< t$ shares should look *uniformly random*.

Definition 3 (Security of (t, n) secret-sharing)

A (t, n) secret-sharing scheme $(\mathsf{Share}, \mathsf{Reconstruct})$ is *secure* if

Secret Sharing: Security

- How can we define what we mean by $< t$ parties learn *nothing*?
  - Any subset of $< t$ shares should look *uniformly random*.

Definition 3 (Security of (t, n) secret-sharing)

A (t, n) secret-sharing scheme $(\mathsf{Share}, \mathsf{Reconstruct})$ is *secure* if for all $m \in \mathcal{M}$ and

Secret Sharing: Security

- How can we define what we mean by $< t$ parties learn *nothing*?
  - Any subset of $< t$ shares should look *uniformly random*.

Definition 3 (Security of (t, n) secret-sharing)

A (t, n) secret-sharing scheme $(\mathsf{Share}, \mathsf{Reconstruct})$ is *secure* if for all $m \in \mathcal{M}$ and for any $T \subset [n]$ such that $|T| < t$, the following two distributions are *identical*

Secret Sharing: Security

- How can we define what we mean by $< t$ parties learn *nothing*?
  - Any subset of $< t$ shares should look *uniformly random*.

Definition 3 (Security of (t, n) secret-sharing)

A (t, n) secret-sharing scheme $(\mathsf{Share}, \mathsf{Reconstruct})$ is *secure* if for all $m \in \mathcal{M}$ and for any $T \subset [n]$ such that $|T| < t$, the following two distributions are *identical*

$\underline{D_0(m, T)}$
$(S_1, \ldots, S_n) \leftarrow \mathsf{Share}(m)$
return $(S_i)_{i \in T}$

D_0

Secret Sharing: Security

- How can we define what we mean by $< t$ parties learn *nothing*?
  - Any subset of $< t$ shares should look *uniformly random*.

Definition 3 (Security of (t, n) secret-sharing)

A (t, n) secret-sharing scheme $(\mathsf{Share}, \mathsf{Reconstruct})$ is *secure* if for all $m \in \mathcal{M}$ and for any $T \subset [n]$ such that $|T| < t$, the following two distributions are *identical*

$\underline{D_0(m, T)}$
$(S_1, \ldots, S_n) \leftarrow \mathsf{Share}(m)$
return $(S_i)_{i \in T}$

D_0

$\underline{D_1(m, T)}$
$(S_1, \ldots, S_n) \xleftarrow{\$} \mathcal{S}^n$
return $(S_i)_{i \in T}$

D_1

Secret Sharing: Security

- How can we define what we mean by $< t$ parties learn *nothing*?
  - Any subset of $< t$ shares should look *uniformly random*.

Definition 3 (Security of (t, n) secret-sharing)

A (t, n) secret-sharing scheme $(\mathsf{Share}, \mathsf{Reconstruct})$ is *secure* if for all $m \in \mathcal{M}$ and for any $T \subset [n]$ such that $|T| < t$, the following two distributions are *identical*

$$\underline{D_0(m, T)}$$
$$(S_1, \ldots, S_n) \leftarrow \mathsf{Share}(m)$$
$$\text{return } (S_i)_{i \in T}$$

D_0

$\equiv$

$$\underline{D_1(m, T)}$$
$$(S_1, \ldots, S_n) \xleftarrow{\$} \mathcal{S}^n$$
$$\text{return } (S_i)_{i \in T}$$

D_1

Insecure Naïve Secret Sharing

Insecure Naïve Secret Sharing

- Let $\mathcal{M} = \{0,1\}^{nk}$ for some $n, k \in \mathbb{Z}^+$.

↳ share with n people

- What is $\mathcal{S}$? $\mathcal{S} = \{0,1\}^n$

$m \in \mathcal{M}$:

$m = m_1 \| m_2 \| \cdots \| m_n$

$m_1 \in \{0,1\}^k$ (n,n) secret sharing

Insecure Naïve Secret Sharing

- Let $\mathcal{M} = \{0,1\}^{nk}$ for some $n, k \in \mathbb{Z}^+$.
- Naïve (n, n) secret sharing: split the secret into chunks!

should add randomness

2-out-of-2 Secret Sharing

2-out-of-2 Secret Sharing

- Let's design a simple $(2, 2)$ secret sharing scheme.

2-out-of-2 Secret Sharing

- Let's design a simple $(2, 2)$ secret sharing scheme.
- Let $\mathcal{M} = \mathcal{S} = \{0, 1\}^{\ell}$.

2-out-of-2 Secret Sharing

- Let's design a simple $(2, 2)$ secret sharing scheme.

- Let $\mathcal{M} = \mathcal{S} = \{0, 1\}^{\ell}$.

2-out-of-2 Secret Sharing

- Let's design a simple $(2, 2)$ secret sharing scheme.

- Let $\mathcal{M} = \mathcal{S} = \{0,1\}^\ell$.

$\Sigma = (\mathsf{Share}, \mathsf{Reconstruct})$

Share($m \in \{0,1\}^\ell$):
$s_1 \xleftarrow{\$} \{0,1\}^\ell$
$s_2 := m \oplus s_1$
(s_1, s_2)
$\equiv$
uniform

Reconstruct(s_1, s_2)
return $s_1 \oplus s_2$

2-out-of-2 Secret Sharing

- Let's design a simple $(2, 2)$ secret sharing scheme.

- Let $\mathcal{M} = \mathcal{S} = \{0,1\}^\ell$.

$\Sigma = (\mathsf{Share}, \mathsf{Reconstruct})$

$\underline{\mathsf{Share}(m):}$

$S_1 \xleftarrow{\$} \{0,1\}^\ell$

$S_2 := S_1 \oplus m$

return (S_1, S_2)

2-out-of-2 Secret Sharing

- Let's design a simple $(2, 2)$ secret sharing scheme.

- Let $\mathcal{M} = \mathcal{S} = \{0,1\}^\ell$.

$\Sigma = (\mathsf{Share}, \mathsf{Reconstruct})$

$\underline{\mathsf{Share}(m):}$
$S_1 \xleftarrow{\$} \{0,1\}^\ell$
$S_2 := S_1 \oplus m$
return (S_1, S_2)

$\underline{\mathsf{Reconstruct}(S_1, S_2):}$
return $S_1 \oplus S_2$

$(2, 2)$ Secret Sharing Correctness

- Let's prove correctness of this scheme.

$(2,2)$ Secret Sharing Correctness

- Let's prove correctness of this scheme.

Definition 2 (Correctness of (t,n) secret-sharing)

A (t,n) secret-sharing scheme $(\mathsf{Share}, \mathsf{Reconstruct})$ is *correct* if for all $m \in \mathcal{M}$ and for any $T \subset [n]$ such that $|T| \geqslant t$, we have

$$\Pr\left[\mathsf{Reconstruct}\left((\mathsf{Share}(m)_i)_{i\in T}\right) = m\right] = 1$$

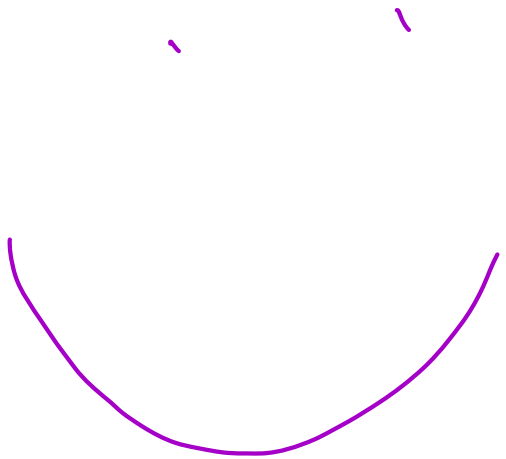
$(s_1, s_2) \leftarrow \mathsf{Share}(m)$

$s_2 = m \oplus s_1$

$s_1 \oplus s_2 = s_1 \oplus m \oplus s_1$

$= m \quad \forall s_1$

$(2, 2)$ Secret Sharing Correctness



$(2, 2)$ Secret Sharing Security

- Now, let's prove security of the scheme.

$(2, 2)$ Secret Sharing Security

- Now, let's prove security of the scheme.

Definition 3 (Security of (t, n) secret-sharing)

A (t, n) secret-sharing scheme $(\mathsf{Share}, \mathsf{Reconstruct})$ is *secure* if for all $m \in \mathcal{M}$ and for any $T \subset [n]$ such that $|T| < t$, the following two distributions are *identical*

$$\underline{D_0(m, T)}$$
$$(S_1, \ldots, S_n) \leftarrow \mathsf{Share}(m)$$
$$\text{return } (S_i)_{i \in T}$$

D_0

$$\equiv$$

$$\underline{D_1(m, T)}$$
$$(S_1, \ldots, S_n) \xleftarrow{\$} \mathcal{S}^n$$
$$\text{return } (S_i)_{i \in T}$$

D_1

(2, 2) Secret Sharing Security

$S_1 \equiv U_{\{0,1\}^l}$

By definition

$S_2 \equiv U_{\{0,1\}^l}$

$S_2 = m \oplus S_1$

$S_1 \xleftarrow{\$} \{0,1\}^l$

$(S_2)_1 = m_1 \oplus S_{1,1}$

$S_{1,1} \xleftarrow{\$} \{0,1\}$

$Pr[m_1 \oplus S_{1,1} = 0]$

$= Pr[S_{1,1} = m_1] = \frac{1}{2}$ ✓

n-out-of-n Secret Sharing

- Can you generalize the 2-out-of-2 secret-sharing we saw to n-out-of-n?

n-out-of-n Secret Sharing

- Can you generalize the 2-out-of-2 secret-sharing we saw to n-out-of-n?
- Keep $\mathcal{M} = \mathcal{S} = \{0,1\}^\ell$

n-out-of-n Secret Sharing

- Can you generalize the 2-out-of-2 secret-sharing we saw to n-out-of-n?
- Keep $\mathcal{M} = \mathcal{S} = \{0,1\}^\ell$

$\Sigma = (\mathsf{Share}, \mathsf{Reconstruct})$

Share(m):

Reconstruct($s_1, \ldots, s_n$)

return $\bigoplus_{i=1}^{n} s_i$

n-out-of-n Secret Sharing

- Can you generalize the 2-out-of-2 secret-sharing we saw to n-out-of-n?
- Keep $\mathcal{M} = \mathcal{S} = \{0,1\}^\ell$

$\Sigma = (\mathsf{Share}, \mathsf{Reconstruct})$

$\underline{\mathsf{Share}(m):}$
for $i = 1, \ldots, n-1$
$S_i \xleftarrow{\$} \{0,1\}^\ell$
$S_n = m \oplus \bigoplus_{i=1}^{n-1} S_i$
return $(S_1, \ldots, S_n)$

n-out-of-n Secret Sharing

- Can you generalize the 2-out-of-2 secret-sharing we saw to n-out-of-n?
- Keep $\mathcal{M} = \mathcal{S} = \{0,1\}^\ell$

$\Sigma = (\mathsf{Share}, \mathsf{Reconstruct})$

$\underline{\mathsf{Share}(m):}$
for $i = 1, \ldots, n-1$
  $S_i \xleftarrow{\$} \{0,1\}^\ell$
$S_n = m \oplus \bigoplus_{i=1}^{n-1} S_i$
return $(S_1, \ldots, S_n)$

$\underline{\mathsf{Reconstruct}(S_1, \ldots, S_n):}$
return $\bigoplus_{i=1}^{n} S_i$

(n, n) Secret Sharing Correctness

Definition 2 (Correctness of (t, n) secret-sharing)

A (t, n) secret-sharing scheme $(\mathsf{Share}, \mathsf{Reconstruct})$ is *correct* if for all $m \in \mathcal{M}$ and for any $T \subset [n]$ such that $|T| \geqslant t$, we have

$$\Pr\left[\mathsf{Reconstruct}\left((\mathsf{Share}(m)_i)_{i \in T}\right) = m\right] = 1$$

$s_i \xleftarrow{\$} \{0,1\}^\ell \quad \forall\, i \in [n-1]$

$s_n = m \oplus \bigoplus_{i=1}^{n-1} s_i$

Reconstruct$(s_1, \ldots, s_n)$:
return $\bigoplus_{i=1}^{n} s_i$

$$\bigoplus_{i=1}^{n} s_i = s_n \oplus \bigoplus_{i=1}^{n-1} s_i$$

$$= \left(m \oplus \bigoplus_{i=1}^{n-1} s_i\right) \oplus \bigoplus_{i=1}^{n-1} s_i = m \quad \checkmark$$

(n, n) Secret Sharing Security

Definition 3 (Security of (t, n) secret-sharing)

A (t, n) secret-sharing scheme $(\mathsf{Share}, \mathsf{Reconstruct})$ is *secure* if for all $m \in \mathcal{M}$ and for any $T \subset [n]$ such that $|T| < t$, the following two distributions are *identical*

$\underline{D_0(m, T)}$
$(S_1, \ldots, S_n) \leftarrow \mathsf{Share}(m)$
return $(S_i)_{i \in T}$

D_0

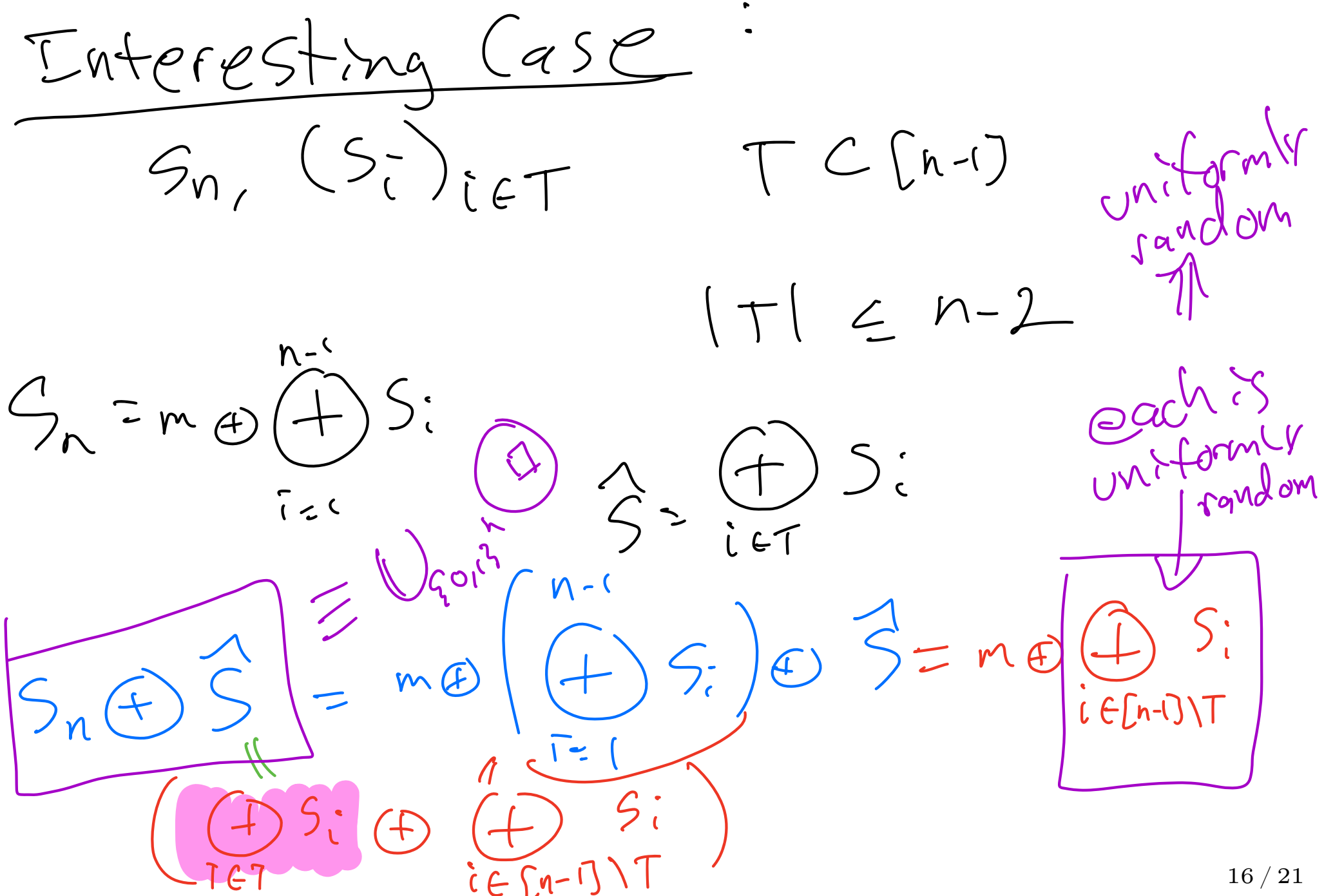
$\underline{D_1(m, T)}$
$(S_1, \ldots, S_n) \xleftarrow{\$} \mathcal{S}^n$
return $(S_i)_{i \in T}$

D_1

$S_1, \ldots, S_{n-1} \xleftarrow{\$} \{0,1\}^\lambda$

any subset of $[n-1]$ of size $\leq n-1$ is uniform by def.

(n,n) Secret Sharing Security



Additive Secret Sharing

- The (n, n) secret-sharing scheme we defined is an example of an *additive secret sharing scheme*

Additive Secret Sharing

- The (n, n) secret-sharing scheme we defined is an example of an *additive secret sharing scheme*

Definition 4 (Additive Secret Sharing)

Additive Secret Sharing

- The (n, n) secret-sharing scheme we defined is an example of an *additive secret sharing scheme*

Definition 4 (Additive Secret Sharing)

Let $\mathcal{M} = \mathcal{S} = \mathbb{G}$ be an additive group.

Additive Secret Sharing

- The (n, n) secret-sharing scheme we defined is an example of an *additive secret sharing scheme*

Definition 4 (Additive Secret Sharing)

Let $\mathcal{M} = \mathcal{S} = \mathbb{G}$ be an additive group. We say that a (n, n) secret-sharing scheme over $\mathbb{G}$ is *additive* if $(\mathsf{Share}, \mathsf{Reconstruct})$ are defined as follows.

Additive Secret Sharing

- The (n, n) secret-sharing scheme we defined is an example of an *additive secret sharing scheme*

Definition 4 (Additive Secret Sharing)

Let $\mathcal{M} = \mathcal{S} = \mathbb{G}$ be an additive group. We say that a (n, n) secret-sharing scheme over $\mathbb{G}$ is *additive* if $(\mathsf{Share}, \mathsf{Reconstruct})$ are defined as follows.

- $\mathsf{Share}(m)$: on input $m \in \mathbb{G}$, sample $S_1, \ldots, S_{n-1} \xleftarrow{\$} \mathbb{G}$, set $S_n = m - \sum_{i=1}^{n-1} S_i$, and output $(S_1, \ldots, S_n)$.

Additive Secret Sharing

- The (n, n) secret-sharing scheme we defined is an example of an *additive secret sharing scheme*

Definition 4 (Additive Secret Sharing)

Let $\mathcal{M} = \mathcal{S} = \mathbb{G}$ be an additive group. We say that a (n, n) secret-sharing scheme over $\mathbb{G}$ is *additive* if $(\mathsf{Share}, \mathsf{Reconstruct})$ are defined as follows.

- $\mathsf{Share}(m)$: on input $m \in \mathbb{G}$, sample $S_1, \ldots, S_{n-1} \xleftarrow{\$} \mathbb{G}$, set $S_n = m - \sum_{i=1}^{n-1} S_i$, and output $(S_1, \ldots, S_n)$.
- $\mathsf{Reconstruct}(S_1, \ldots, S_n)$: output $m = \sum_{i=1}^{n} S_i$.

Generalizing to t-out-of-n Secret Sharing

- Can you generalize the previous (n, n) secret sharing to a (t, n) secret sharing scheme?

Generalizing to t-out-of-n Secret Sharing

- Can you generalize the previous (n, n) secret sharing to a (t, n) secret sharing scheme?

- Hint: You'll have many different (t, t) additive secret sharings!

$(3, n) \longrightarrow \binom{n-1}{t-1}$ possible groups

part x

one can get x with

Generalizing to t-out-of-n Secret Sharing

- Can you generalize the previous (n, n) secret sharing to a (t, n) secret sharing scheme?
- Hint: You'll have many different (t, t) additive secret sharings!
- Idea: Use the previous scheme for (t, t) additive secret sharing, once for each possible subset $T \subset [n]$ of size $|T| = t$. $\binom{n}{t}$

Generalizing to t-out-of-n Secret Sharing

Generalizing to t-out-of-n Secret Sharing

$\Sigma = (\mathsf{Share}, \mathsf{Reconstruct})$

$\mathcal{M} = \mathcal{S} = \{0,1\}^{\ell}$

Generalizing to t-out-of-n Secret Sharing

$\Sigma = (\mathsf{Share}, \mathsf{Reconstruct})$

$\mathcal{M} = \mathcal{S} = \{0,1\}^\ell$

for all $T \subseteq [n]$

$\binom{n}{t}$

$\mathsf{Share}(m)$:

$\forall T \subset [n]$ s.t. $|T| = t$,

let $T = \{i_1, \ldots, i_t\}$

for $j = 1, \ldots, t-1$

$S_{T,i_j} \xleftarrow{\$} \{0,1\}^\ell$

$S_{T,i_t} = m \oplus \bigoplus_{j=1}^{t-1} S_{T,i_j}$

for $j = 1, \ldots, t$

$\mathbb{S}_{i_j} = \mathbb{S}_{i_j} \cup \{S_{T,i_j}\}$

return $(\mathbb{S}_1, \ldots, \mathbb{S}_n)$

Generalizing to t-out-of-n Secret Sharing

$\Sigma = (\mathsf{Share}, \mathsf{Reconstruct})$

$\mathcal{M} = \mathcal{S} = \{0,1\}^\ell$

$\underline{\mathsf{Share}(m):}$

$\forall T \subset [n]$ s.t. $|T| = t$,

let $T = \{i_1, \ldots, i_t\}$

  for $j = 1, \ldots, t-1$

    $S_{T,i_j} \xleftarrow{\$} \{0,1\}^\ell$

  $S_{T,i_t} = m \oplus \bigoplus_{j=1}^{t-1} S_{T,i_j}$

  for $j = 1, \ldots, t$

    $\mathbb{S}_{i_j} = \mathbb{S}_{i_j} \cup \{S_{T,i_j}\}$

 return $(\mathbb{S}_1, \ldots, \mathbb{S}_n)$

$\underline{\mathsf{Reconstruct}(\mathbb{S}_{i_1}, \ldots, \mathbb{S}_{i_t}):}$

Compute $T \subset [n]$ s.t.

$T = \{i_1, \ldots, i_t\}$

 return $\bigoplus_{j=1}^{t} S_{T,i_j}$

$//S_{T,i_j} \in \mathbb{S}_{i_j}$ *for all* j

Generalized (t, n) Additive Secret Sharing

- Scheme seems simple, but what are some issues with it?

Generalized (t, n) Additive Secret Sharing

- Scheme seems simple, but what are some issues with it?

- It is *not efficient*!

Generalized (t, n) Additive Secret Sharing

- Scheme seems simple, but what are some issues with it?
- It is *not efficient*!
- Every user i must store the set $\mathbb{S}_i$.

Generalized (t, n) Additive Secret Sharing

- Scheme seems simple, but what are some issues with it?
- It is *not efficient*!
- Every user i must store the set $\mathbb{S}_i$.
  - Each $\mathbb{S}_i$ contains a share $S_{T,i}$ *for every subset* $T \subseteq [n]$ such that $|T| = t$ and $i \in T$.

Generalized (t, n) Additive Secret Sharing

- Scheme seems simple, but what are some issues with it?
- It is *not efficient*!
- Every user i must store the set $\mathbb{S}_i$.
  - Each $\mathbb{S}_i$ contains a share $S_{T,i}$ *for every subset* $T \subseteq [n]$ such that $|T| = t$ and $i \in T$.
  - There are $\binom{n-1}{t-1}$ such subsets (of a total of $\binom{n}{t}$ subsets of size t).

Generalized (t, n) Additive Secret Sharing

- Scheme seems simple, but what are some issues with it?
- It is *not efficient*!
- Every user i must store the set $\mathbb{S}_i$.
  - Each $\mathbb{S}_i$ contains a share $S_{T,i}$ *for every subset* $T \in [n]$ such that $|T| = t$ and $i \in T$.
  - There are $\binom{n-1}{t-1}$ such subsets (of a total of $\binom{n}{t}$ subsets of size t).
  - This becomes *exponential* in ~~N~~ n when $t \approx$ ~~N~~ $n/2$!

$\left(\frac{n}{t}\right)^t \leq \binom{n}{t}$

$t = n/c$

$\Big(c\Big)^{n/c} = \Omega(2^n)$

Generalized (t, n) Additive Secret Sharing

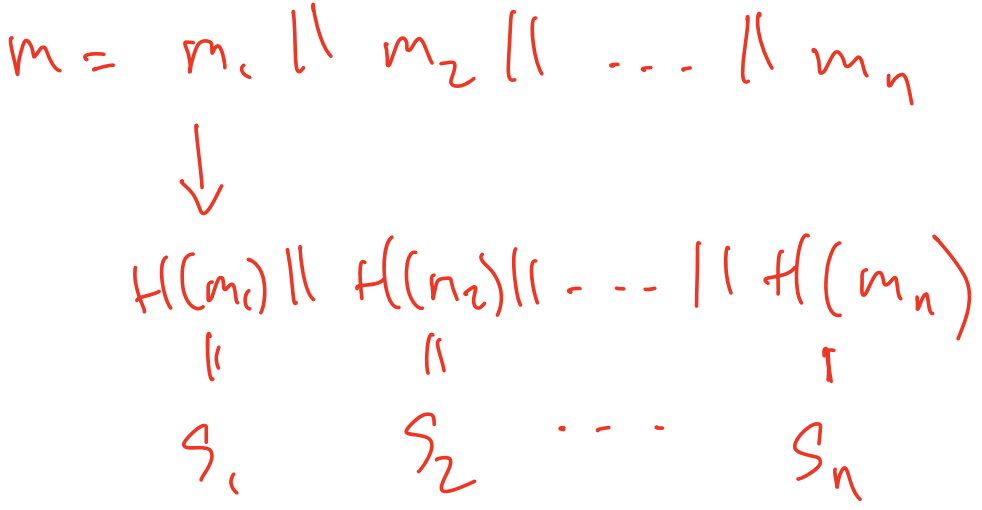
- Scheme seems simple, but what are some issues with it?
- It is *not efficient*!
- Every user i must store the set $\mathbb{S}_i$.
  - Each $\mathbb{S}_i$ contains a share $S_{T,i}$ *for every subset* $T \in [n]$ such that $|T| = t$ and $i \in T$.
  - There are $\binom{n-1}{t-1}$ such subsets (of a total of $\binom{n}{t}$ subsets of size t).
  - This becomes *exponential* in N when $t \approx N/2$!

- Error-correcting code
- Polynomials ↙ same thing

Can we make a more efficient (t, n) secret-sharing scheme?

Yes

Next Time: Shamir Secret Sharing and Linear Secret Sharing


m = m1 || m2 || ... || mn
H(m1) || H(m2) || ... || H(mn)
S1
S2
...
Sn