GEMS OF TCS

SECRET SHARING

Sasha Golovnev
November 16, 2022
EXAMPLES

• Documents for a secret project
Examples

• Documents for a secret project
• Missile launch codes
EXAMPLES

- Documents for a secret project
- Missile launch codes
- Software release
EXAMPLES

- Documents for a secret project
- Missile launch codes
- Software release
- Blockchains
EXAMPLES

• Documents for a secret project
• Missile launch codes
• Software release
• Blockchains
• Internet Corporation for Assigned Names and Numbers (ICANN): Burkina Faso, Canada, Czech Republic, Trinidad and Tobego, China, USA, UK
2-out-of-2 Secret Sharing

- For secret message $m$, generate shares $s_A$ for Alice and $s_B$ for Bob
2-out-of-2 Secret Sharing

- For secret message $m$, generate shares $s_A$ for Alice and $s_B$ for Bob
- $s_A$ has no information about $m$
2-out-of-2 Secret Sharing

- For secret message $m$, generate shares $s_A$ for Alice and $s_B$ for Bob
- $s_A$ has no information about $m$
- $s_B$ has no information about $m$
2-out-of-2 Secret Sharing

• For secret message \( m \), generate shares \( s_A \) for Alice and \( s_B \) for Bob

• \( s_A \) has no information about \( m \)

• \( s_B \) has no information about \( m \)

• \( s_A \) and \( s_B \) are sufficient to recover \( m \)
\textbf{$n$-OUT-OF-$n$ SECRET SHARING}

- For secret message $m$, generate $n$ shares $S_1, \ldots, S_n$
$n$-out-of-$n$ Secret Sharing

- For secret message $m$, generate $n$ shares $S_1, \ldots, S_n$
- Each of $n$ players gets their share
$n$-out-of-$n$ Secret Sharing

- For secret message $m$, generate $n$ shares $S_1, \ldots, S_n$
- Each of $n$ players gets their share
- Every set of $n - 1$ shares has no information about $m$
**n-out-of-n Secret Sharing**

- For secret message $m$, generate $n$ shares $s_1, \ldots, s_n$
- Each of $n$ players gets their share
- Every set of $n - 1$ shares has no information about $m$
- Can recover $m$ from $s_1, \ldots, s_n$
For secret message $m$, generate $n$ shares $s_1, \ldots, s_n$
For secret message $m$, generate $n$ shares $S_1, \ldots, S_n$.

Each of $n$ players gets their share.
$k$-out-of-$n$ Secret Sharing

- For secret message $m$, generate $n$ shares $s_1, \ldots, s_n$
- Each of $n$ players gets their share
- Every set of $k - 1$ shares has no information about $m$
For secret message $m$, generate $n$ shares $S_1, \ldots, S_n$

Each of $n$ players gets their share

Every set of $k - 1$ shares has no information about $m$

Can recover $m$ from any set of $k$ shares
GENERAL SECRET SHARING