Gems of TCS

Secret Sharing

Sasha Golovnev

November 22, 2021

Treasure Map

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

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 $s_1, \ldots, s_n$

k-out-of-n Secret Sharing

- For secret message m, generate n shares $s_1, \ldots, s_n$

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

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

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
- Can recover m from any set of k shares

General Secret Sharing