

# GEMS OF TCS

## SECRET SHARING

---

Sasha Golovnev

November 16, 2022

# 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 Tobago, 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  $s_1, \dots, s_n$

## $n$ -OUT-OF- $n$ SECRET SHARING

- For secret message  $m$ , generate  $n$  shares  $s_1, \dots, s_n$
- Each of  $n$  players gets their share

## $n$ -OUT-OF- $n$ SECRET SHARING

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

## $k$ -OUT-OF- $n$ SECRET SHARING

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

## $k$ -OUT-OF- $n$ SECRET SHARING

- For secret message  $m$ , generate  $n$  shares  $s_1, \dots, s_n$
- Each of  $n$  players gets their share

## $k$ -OUT-OF- $n$ SECRET SHARING

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