$\mathcal{G}_3$ Secret sharing

- Secret sharing is a method for distributing a secret by breaking it into shares.

$m_1 \leftarrow \$ \{0,1\}^n$

$m_2 \leftarrow \$ \{0,1\}^n$

$m_3 \leftarrow m \oplus m_1 \oplus m_2$

Without knowledge of all secrets, all possible values of m are equally probable. However, when all secrets are combined, we can compute $m = m_1 \oplus m_2 \oplus m_3$ and recover the message.

$m \in \{0,1\}^n$

6 secrets — 3 participants $(P_1, \ldots, P_3)$

- Nenhum par de participantes pode recuperar mensagem m
- Todos os 3 participantes juntos conseguem recuperar m.

$\mathcal{G}P1$)

1) $P_1 \cup P_2$ (m_1, m_2, m_3, m_4) → não recupera m

$P_1 \cup P_3$ (m_1, m_2, m_5, m_6) → " " "

$P_2 \cup P_3$ (m_3, m_4, m_5, m_6) → " " "

$P_1 \cup P_2 \cup P_3$ $(m_1, m_2, m_3, m_4, m_5, m_6)$ → recupera m

2) $P_2 \cup P_3$ (m_3, m_4, m_5, m_6) → não recupera m

$P_1 \cup P_3$ $(m_1, m_2, m_3, m_4, m_5, m_6)$ → recupera m

Não pode, pois tem 1 par que recupera a mensagem

3) $P_1 \cup P_3 (m_1, m_2, m_3, m_5, m_6)$ → não recupera

$P_2 \cup P_3 (m_3, m_4, m_5, m_6)$ → não recupera

$P_1 \cup P_2 \cup P_3$ → recupera m

4) $P_1 \cup P_3 (m_1, m_2, m_4, m_5)$ → não recupera

$P_2 \cup P_3 (m_1, m_3, m_4, m_5)$ → " "

$P_1 \cup P_2 \cup P_3 (m_1, m_2, m_3, m_4, m_5)$ → não recupera

R: A 1 e a 3.

P2)

$m_1, m_2, m_3 \leftarrow \$ \{0,1\}^n$

$m_4 = m \oplus m_1$

$m_5 = m \oplus m_2$

$m_6 = m \oplus m_3$

Distribuição:

$P_1 (m_1, m_5, m_6)$

$P_2 (m_2, m_4, m_6)$

$P_3 (m_3, m_4, m_5)$

Nenhum participante sozinho recupera m, mas qualque pa
recupera m, exemplo:

$P_1 \cup P_2 (m_1, m_5, m_6, m_2, m_4, m_6)$

- Tem m_1 e $m_4 = m \oplus m_1$

Logo: $m = m_1 \oplus m_4$.

P3) $x = 001$ $y = 010$

$x_0 = 101$ $x_1 = 110$

$x_2 = x \oplus x_0 \oplus x_1 = 001 \oplus 101 \oplus 110 = 010$

$x_0 \oplus x_1 \oplus x_2 = 101 \oplus 110 \oplus 010 = 001$ ✓

$y_0 = 011$ $y_1 = 100$

$y_2 = y \oplus y_0 \oplus y_1 = 010 \oplus 011 \oplus 100 = 101$

$y_0 \oplus y_1 \oplus y_2 = 011 \oplus 100 \oplus 101 = 010$ ✓

xOR entre duas

$z_0 = x_0 \oplus y_0 = 101 \oplus 011 = 110$

$z_1 = x_1 \oplus y_1 = 110 \oplus 100 = 010$

$z_2 = x_2 \oplus y_2 = 010 \oplus 101 = 111$

$z_0 \oplus z_1 \oplus z_2 = 110 \oplus 010 \oplus 111 = 011$

Análise da relação

$x = 001$

$y = 010$

$x \oplus y = 011 = z$

Ou seja, a relação $\underbrace{(x_0 \oplus y_0)}_{z_0} \oplus \underbrace{(x_1 \oplus y_1)}_{z_1} \oplus \underbrace{(x_2 \oplus y_2)}_{z_2} = x \oplus y$