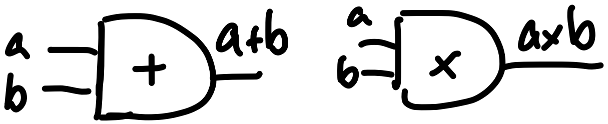
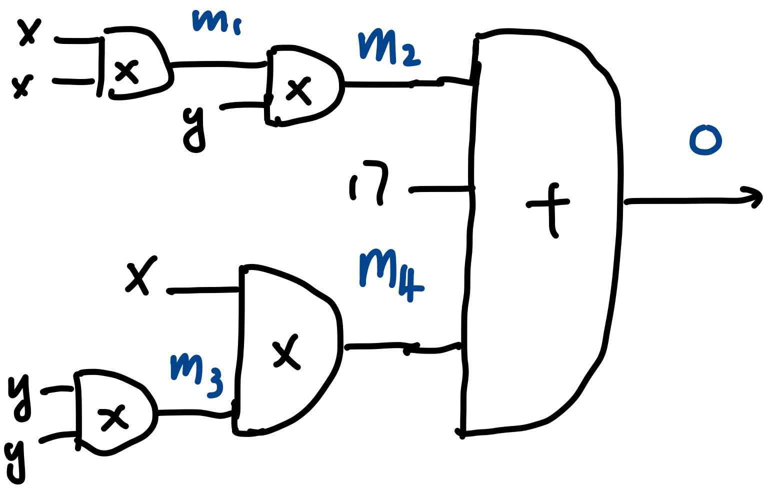
$f(x,y) = x^2y + xy^2 + 17$, $f(x,y) \to z$, prove you know x, y s.t. $f(x,y) = z$, without showing x, y.

Circom



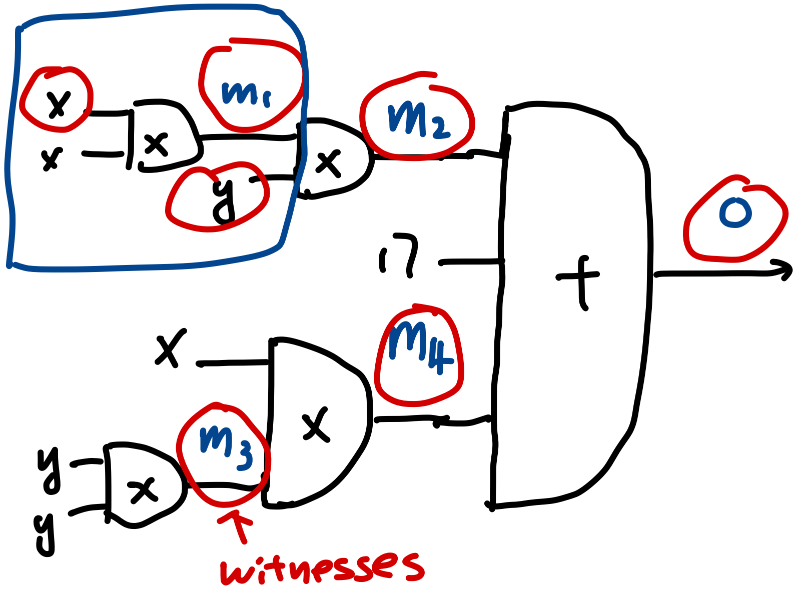
$$f(x,y) = \boxed{\boxed{x \cdot x}\, y} + x \cdot \boxed{y \cdot y} + 17$$



why?

① Witnesses increase honesty and security in proof construction and circuit execution

② General circuit and verification setup reduce cost for privacy.



$$\boxed{f(x,y) = x^2y + xy^2+17}$$

③ Signal: inputs, witnesses, outputs

$$\begin{cases} x \cdot x = m_1 \\ m_1 \cdot y = m_2 \\ y \cdot y = m_3 \\ x \cdot m_3 = m_4 \end{cases} \qquad O = m_2 + m_4 + 17$$

Rank 1 Constraint System

RICS