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

Circom

$$\begin{array}{c}
6 - + & 4b \\
6 - \times & 4xb
\end{array}$$

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

$$\begin{array}{c}
x - \cancel{x} \cdot \cancel{y} \cdot \cancel{y} + x \cdot \cancel{y} \cdot y + 17
\end{array}$$

$$\begin{array}{c}
x - \cancel{x} \cdot \cancel{y} \cdot \cancel{y} \cdot \cancel{y} + 17
\end{array}$$

$$\begin{array}{c}
x - \cancel{x} \cdot \cancel{y} \cdot \cancel{y} \cdot \cancel{y} + 17
\end{array}$$

$$\begin{array}{c}
x - \cancel{x} \cdot \cancel{y} \cdot \cancel{y} \cdot \cancel{y} + 17
\end{array}$$

why?

- (1) Witnesses increase

  honesty and security in

  proof construction and

  circuit execution
- ② General circuit and verification setup reduce cost for privacy.
- 3 Signal: inputs, witnesses, outputs

$$\begin{cases} x \cdot x = m_1 & 0 = M_2 + M_4 + 17 \\ M_1 \cdot y = M_2 & Rank 1 Constraint System \\ y \cdot y = M_3 & RICS \end{cases}$$

$$\begin{cases} x \cdot x = m_1 & 0 = M_2 + M_4 + 17 \\ Rank 1 & Constraint System \\ RICS & RICS \end{cases}$$

