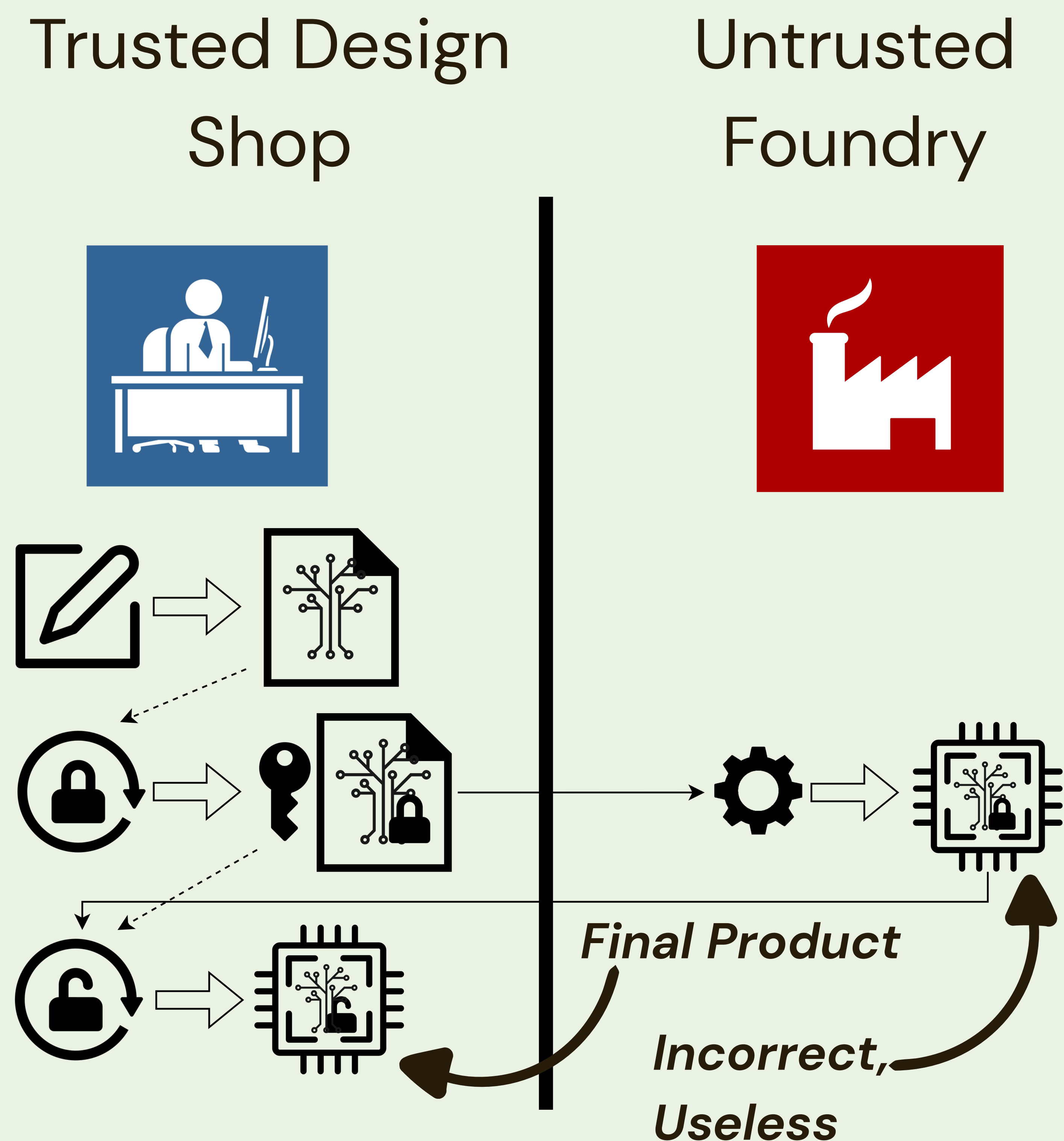
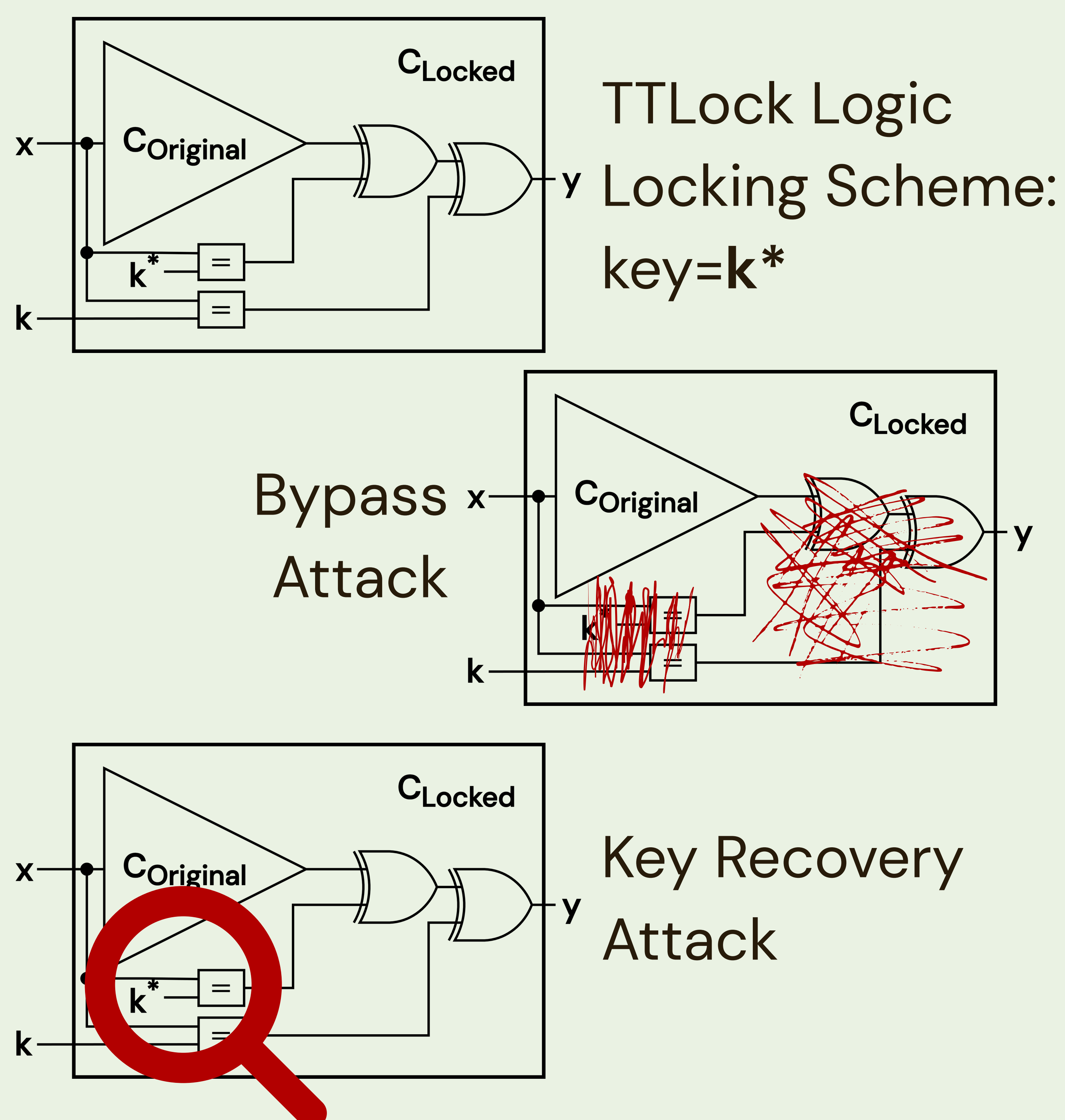


# Mixed Method Circuit Security

## Context: Logic Locking

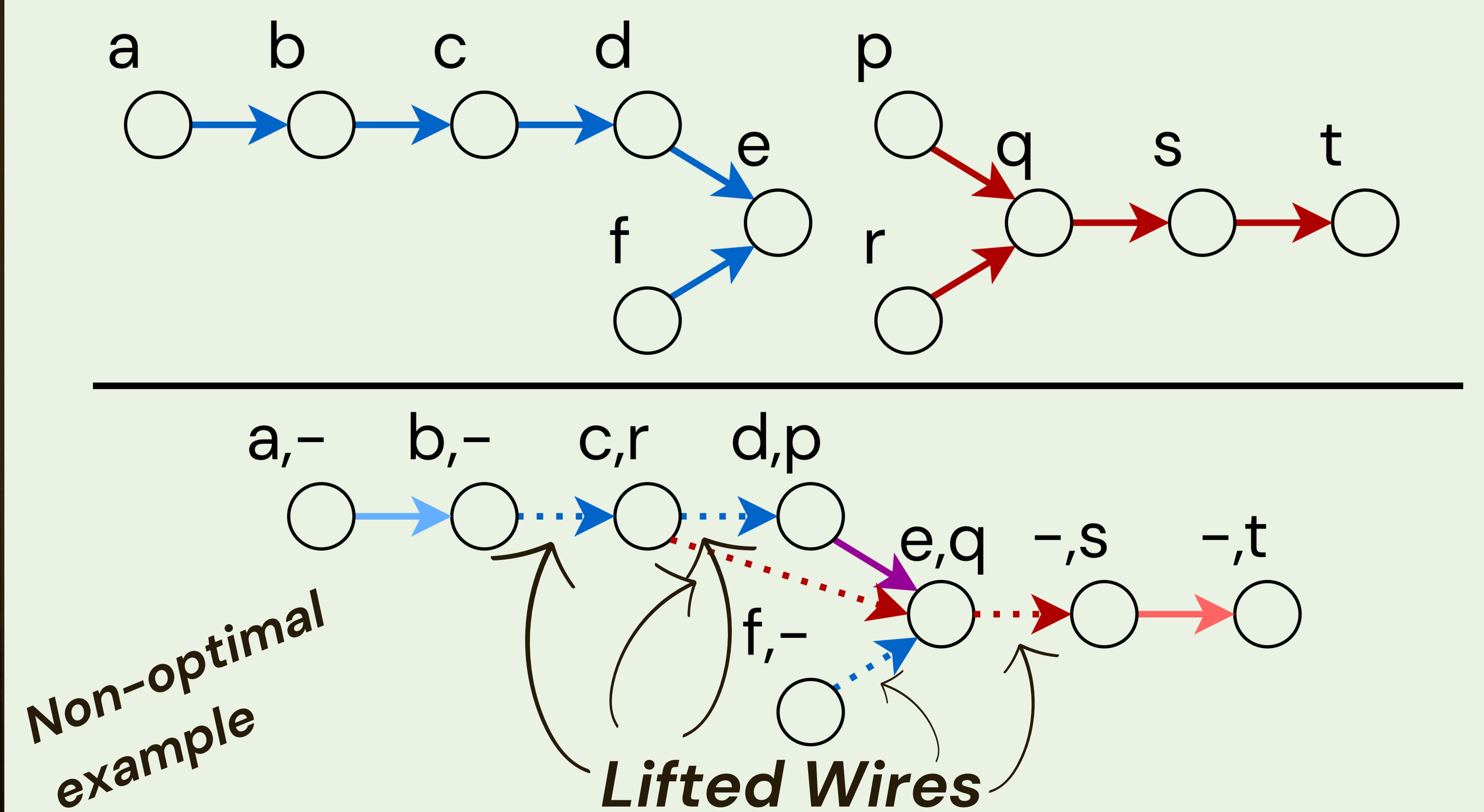


# Threats



## Addition: Wire Lifting

- **Obfuscate** circuit structure
- **Trade-off**: # lifted wires vs. security
- **Approach**: overlay similar subcircuits



# Hardness

Min. cost problem for defender  $\text{LW}(G, H, k)$

### Min. lifted wire overlay for fixed subcircuit

**Theorem**  $\text{Clique}(H, j) \leq \text{LW}(G, H, k)$


- Proof similar to  $\text{Clique}(H, j) \leq \text{SubIso}(G, H)$ 
  - Set  $G$  to clique of size  $j$ , ...
- Difference: cost of dark red edges (below)

$$\text{Clique}(\mathbf{H}, |\mathbf{V}[\mathbf{G}]|) \not\Leftarrow \text{LW}(\mathbf{G}, \mathbf{H}, 0) \quad \mathbf{Clique}(\mathbf{H}, |\mathbf{V}[\mathbf{G}]|) \Leftarrow \text{LW}(\mathbf{G}, \mathbf{H}', |\uparrow|)$$

**Must fix  $| \nearrow |$  to known quantity!**

**Define**  $j = |V[G]|; i = |V[H]|$   
 $\uparrow = k = j(i - j)$

## Then

$$\text{LW}(G, H', k)$$


Clique(H, j)

```

H' ← H
W ← LargeClique()
VW ← V[W]
∀ {u, v} ∈ V[H] × V[H] ∧ {u, v} ∉ EU[H]
do  w ← ∈ VW;
    VW ← VW \ {w};
    V[H'] ← E[H'] ∪ {w};
    E[H'] ← E[H'] ∪ {<u, w>, <v, w>}

```

