

Example

- Back to our 2-bit machine
 - Let xor0, xor1 apply to both bits
 - Both bits output after each command
- Initial state: (0, 1)
- Inputs: $1_H 0_L 1_L 0_H 1_L 0_L$
- Outputs: 10 10 01 01 10 10
- Lara (at *Low*) sees: 001100
 - Does not know initial state, so does not know first input; but can deduce fourth input is 0
- Not deducibly secure