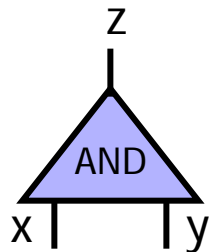
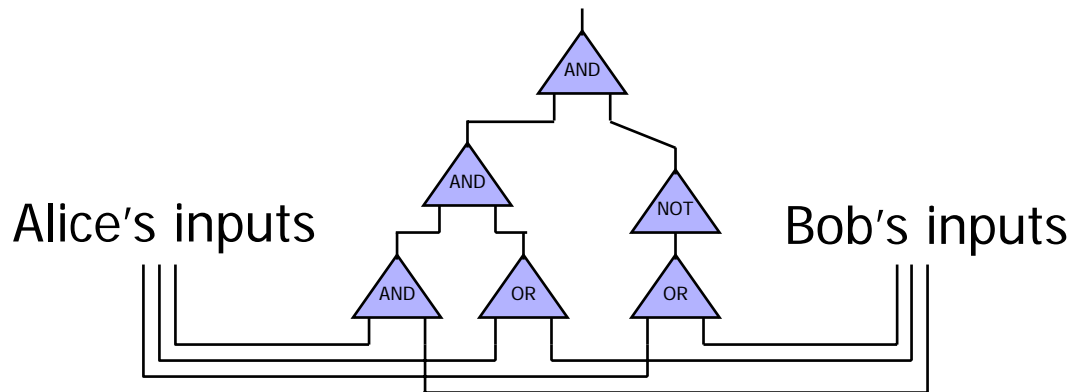


Yao's Protocol

Vitaly Shmatikov

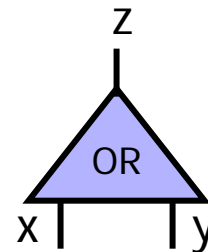
Yao's Protocol

- ◆ Compute **any** function securely
 - ... in the semi-honest model
- ◆ First, convert the function into a **boolean circuit**



Truth table:

x	y	z
0	0	0
0	1	0
1	0	0
1	1	1

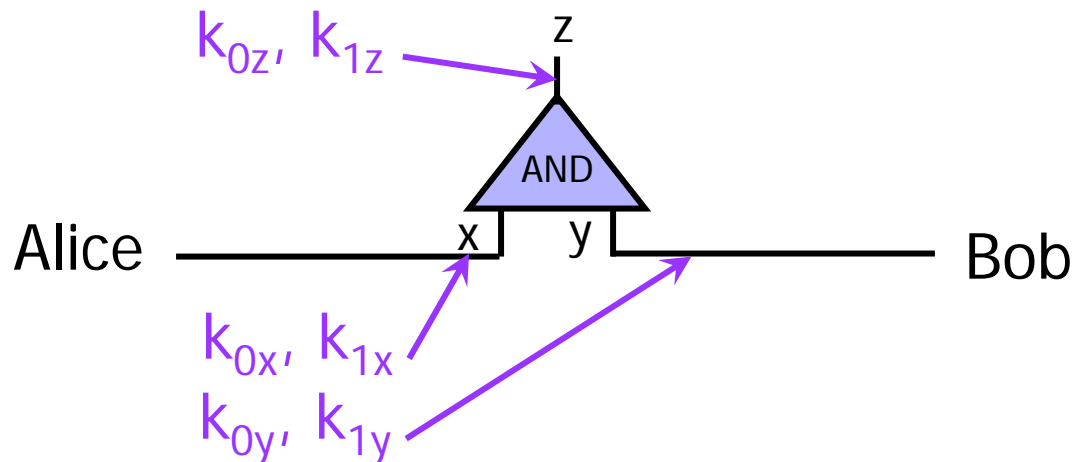


Truth table:

x	y	z
0	0	0
0	1	1
1	0	1
1	1	1

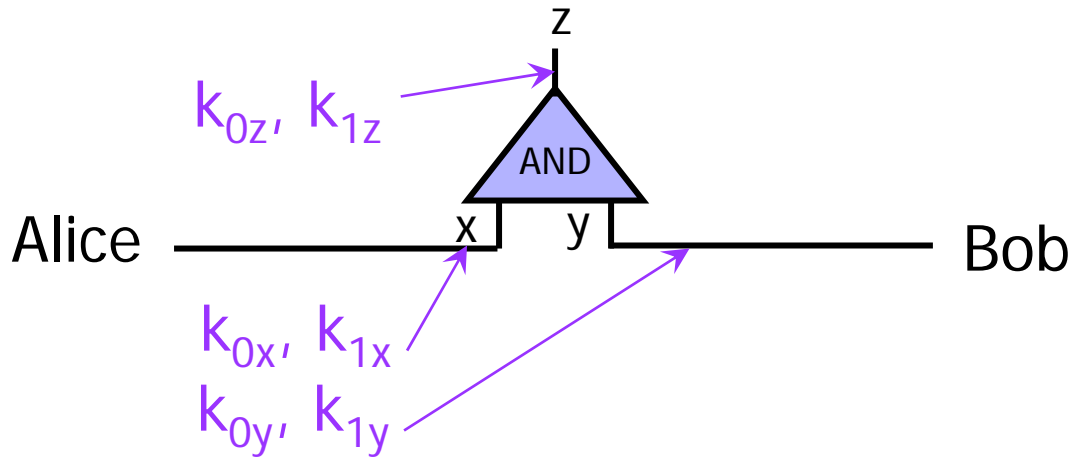
1: Pick Random Keys For Each Wire

- ◆ Next, evaluate one gate securely
 - Later, generalize to the entire circuit
- ◆ Alice picks two **random keys** for each wire
 - One key corresponds to "0", the other to "1"
 - 6 keys in total for a gate with 2 input wires



2: Encrypt Truth Table

- ◆ Alice encrypts each row of the truth table by encrypting the output-wire key with the corresponding pair of input-wire keys



Original truth table:

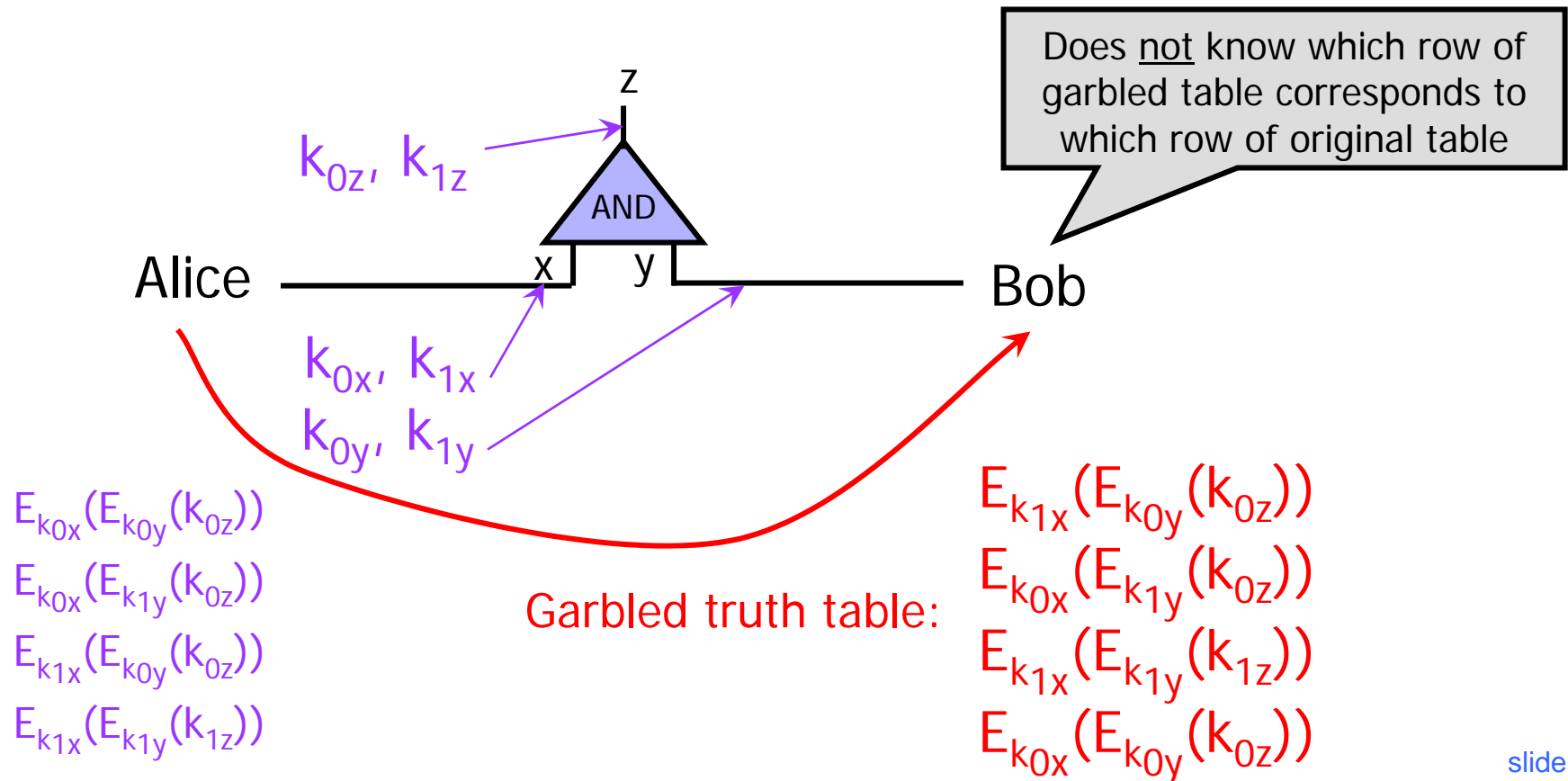
x	y	z
0	0	0
0	1	0
1	0	0
1	1	1

Encrypted truth table:

$$\begin{aligned}
 & E_{k_{0x}}(E_{k_{0y}}(k_{0z})) \\
 & E_{k_{0x}}(E_{k_{1y}}(k_{0z})) \\
 & E_{k_{1x}}(E_{k_{0y}}(k_{0z})) \\
 & E_{k_{1x}}(E_{k_{1y}}(k_{1z}))
 \end{aligned}$$

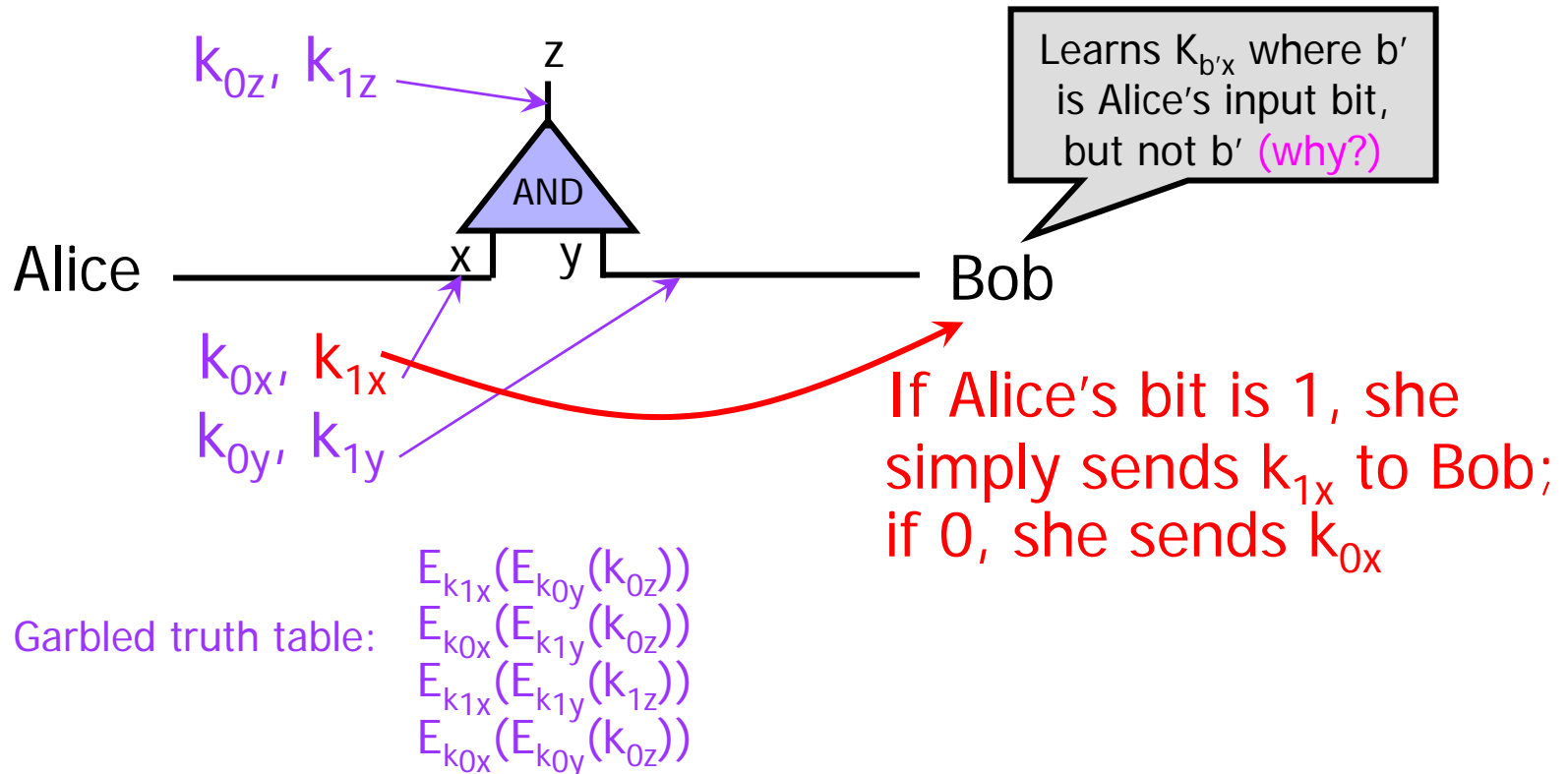
3: Send Garbled Truth Table

- ◆ Alice randomly permutes ("garbles") encrypted truth table and sends it to Bob



4: Send Keys For Alice's Inputs

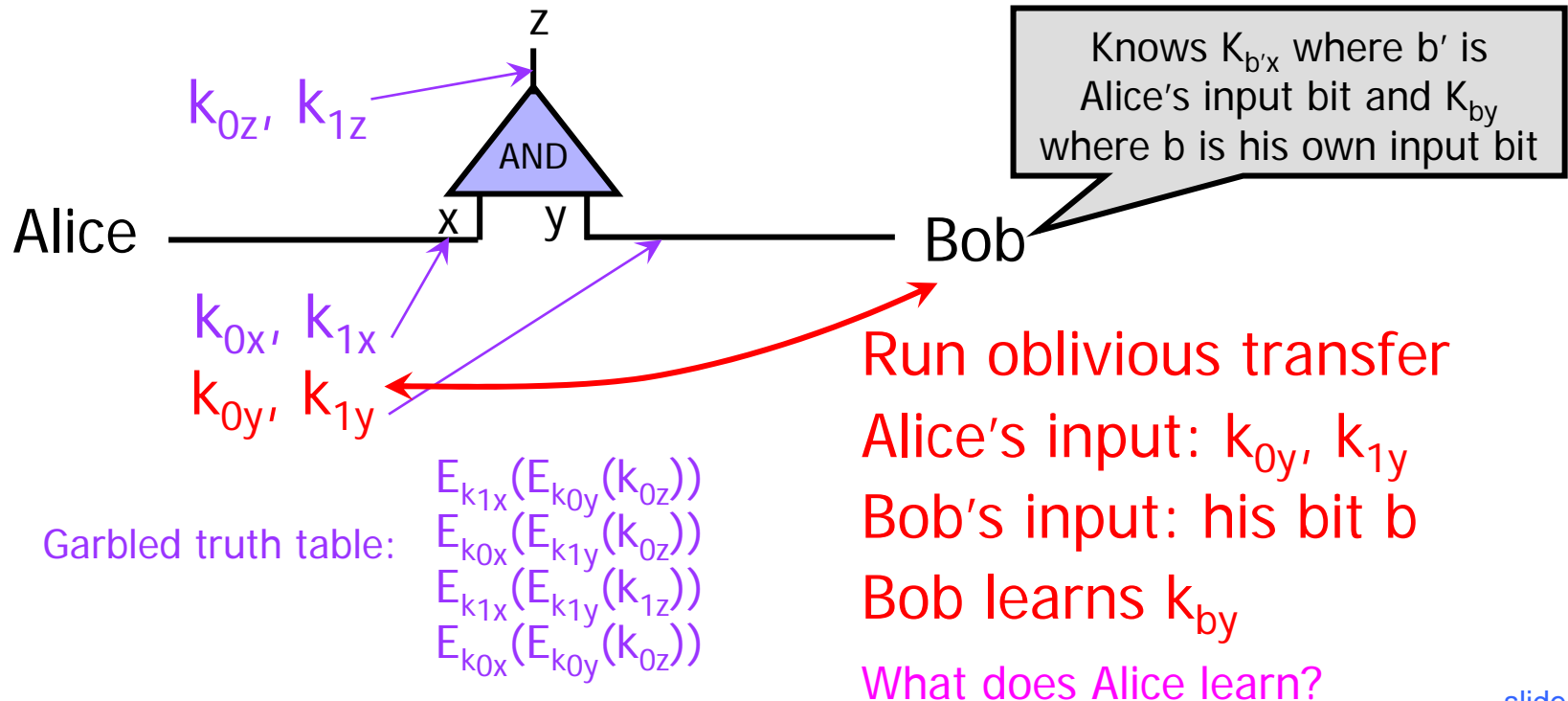
- ◆ Alice sends the key corresponding to her input bit
 - Keys are random, so Bob does not learn what this bit is



5: Use OT on Keys for Bob's Input

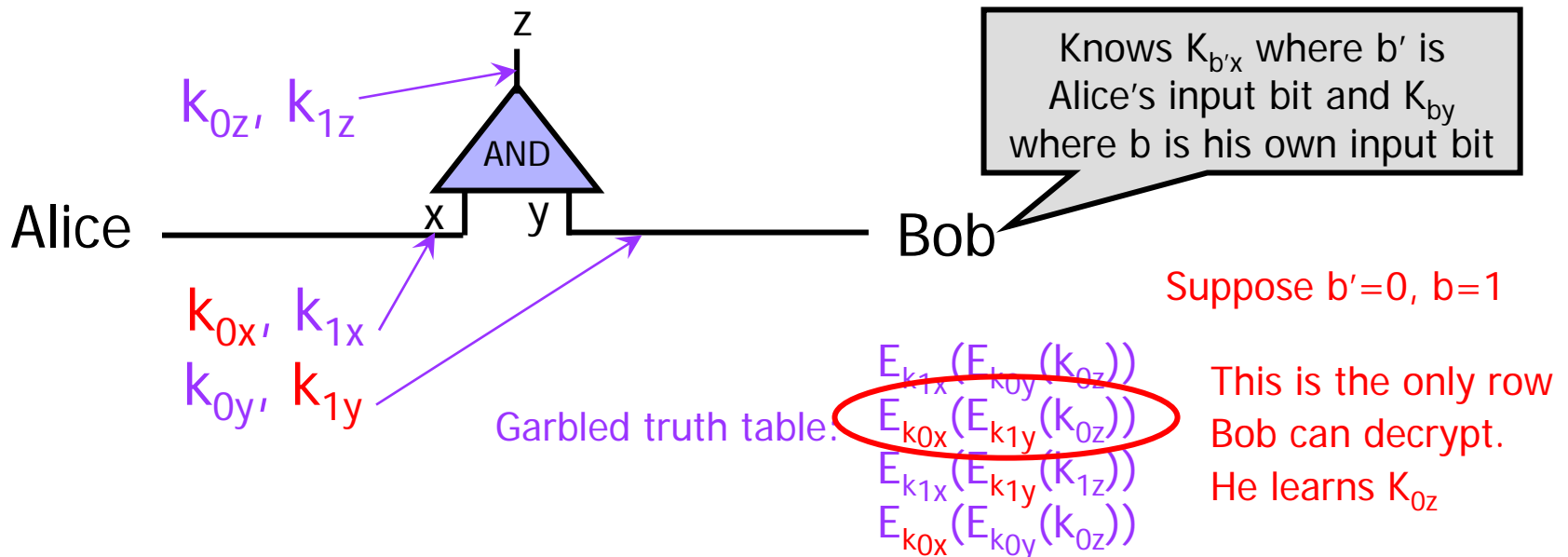
◆ Alice and Bob run oblivious transfer protocol

- Alice's input is the two keys corresponding to Bob's wire
- Bob's input into OT is simply his 1-bit input on that wire



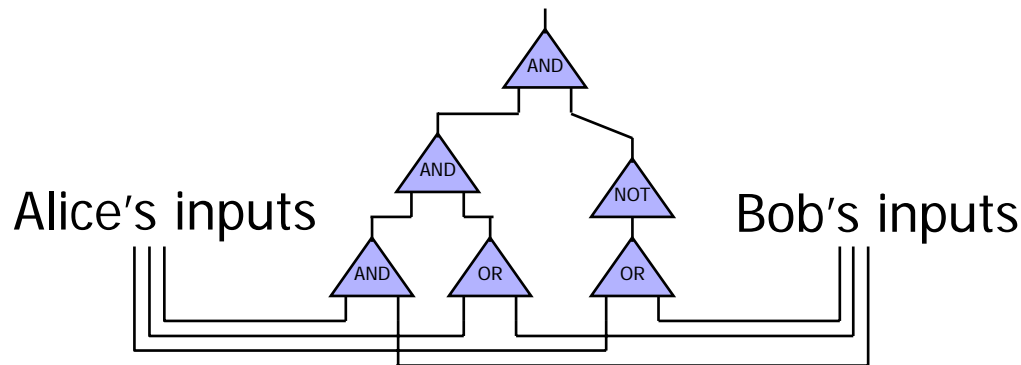
6: Evaluate Garbled Gate

- ◆ Using the two keys that he learned, Bob decrypts exactly one of the output-wire keys
 - Bob does not learn if this key corresponds to 0 or 1
 - Why is this important?



7: Evaluate Entire Circuit

- ◆ In this way, Bob evaluates entire garbled circuit
 - For each wire in the circuit, Bob learns only one key
 - It corresponds to 0 or 1 (Bob does not know which)
 - Therefore, Bob does not learn intermediate values (why?)



- ◆ Bob tells Alice the key for the final output wire and she tells him if it corresponds to 0 or 1
 - Bob does not tell her intermediate wire keys (why?)

Brief Discussion of Yao's Protocol

- ◆ Function must be converted into a circuit
 - For many functions, circuit will be huge
- ◆ If m gates in the circuit and n inputs, then need $4m$ encryptions and n oblivious transfers
 - Oblivious transfers for all inputs can be done in parallel
- ◆ Yao's construction gives a constant-round protocol for secure computation of any function in the semi-honest model
 - Number of rounds does not depend on the number of inputs or the size of the circuit!