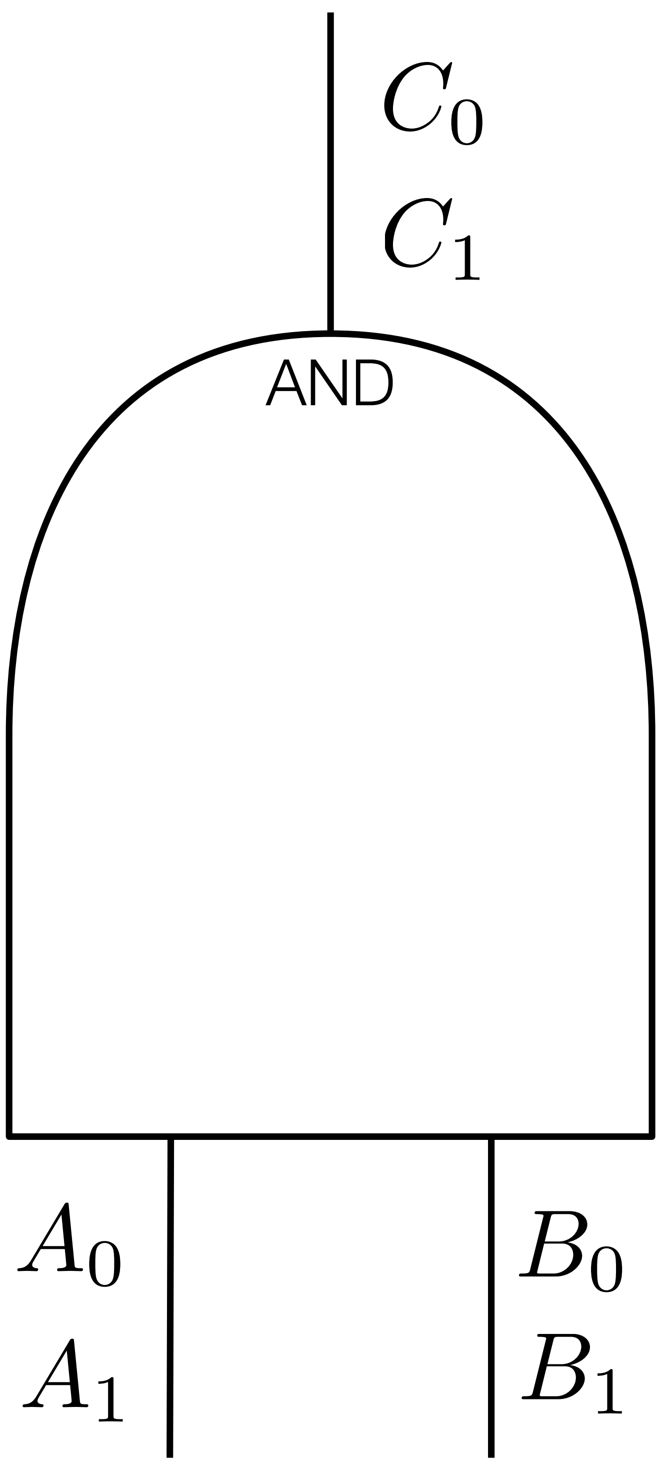
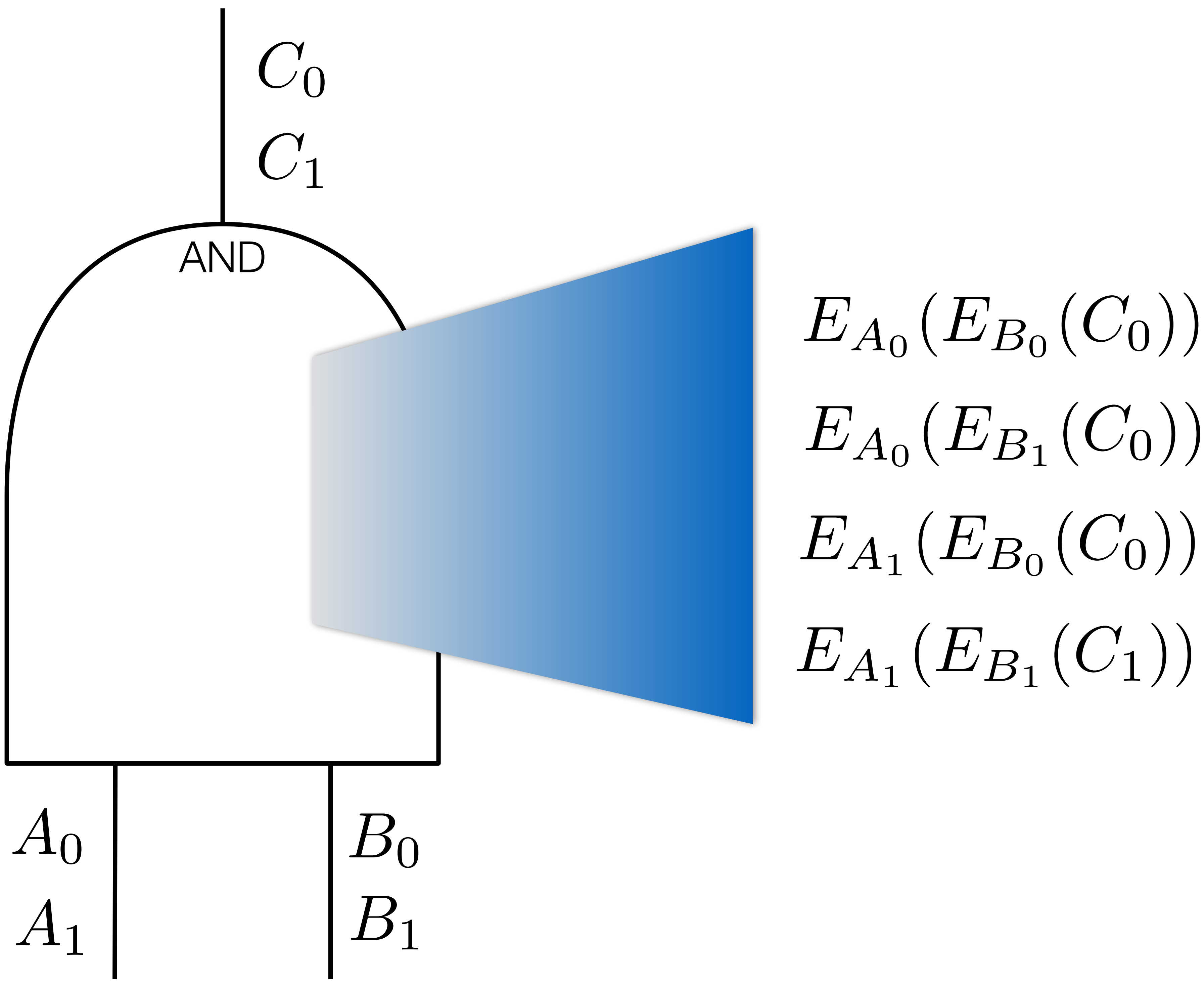
Garbling

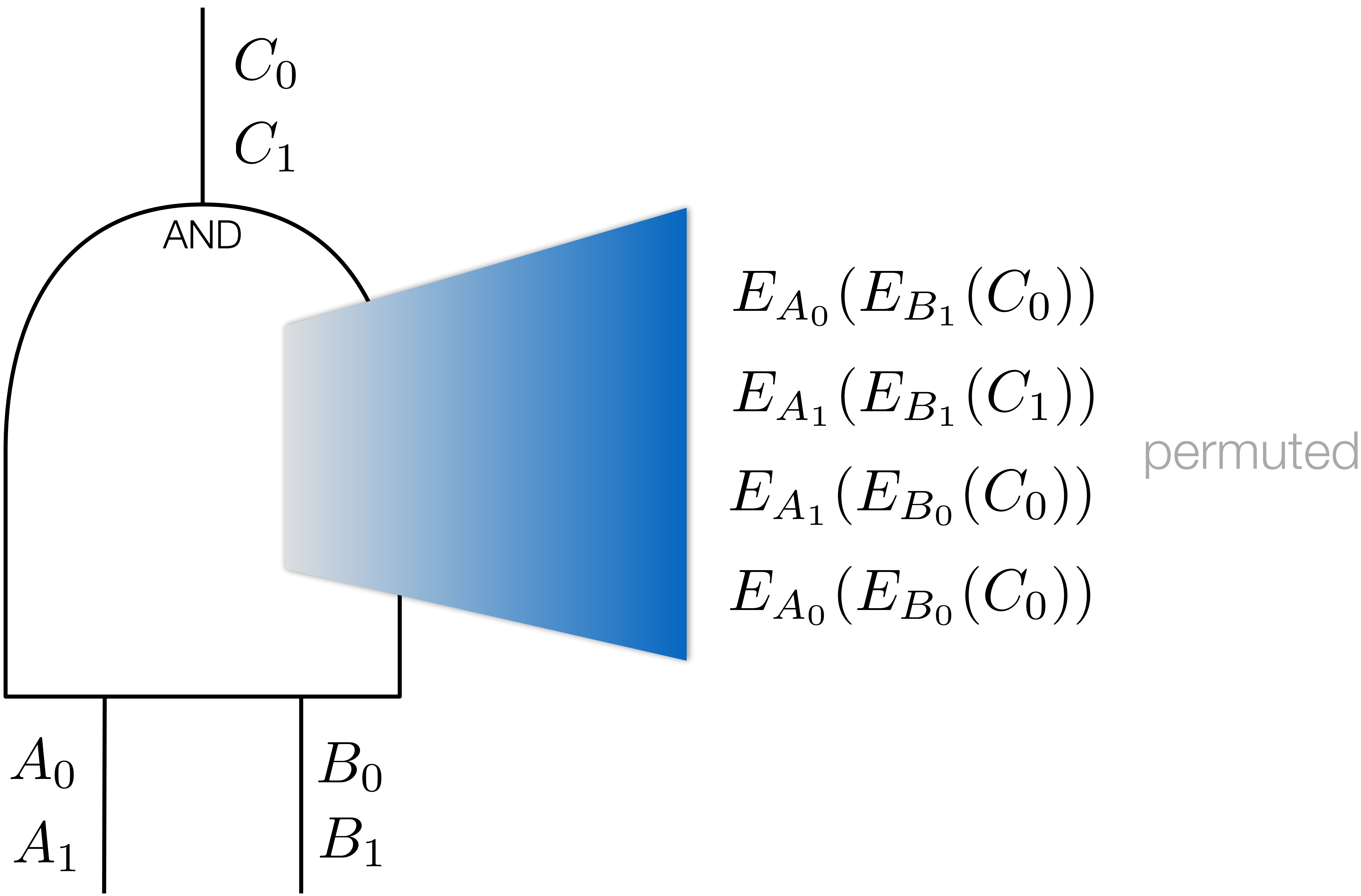
Yao Garbled Circuit



Classic Garbling

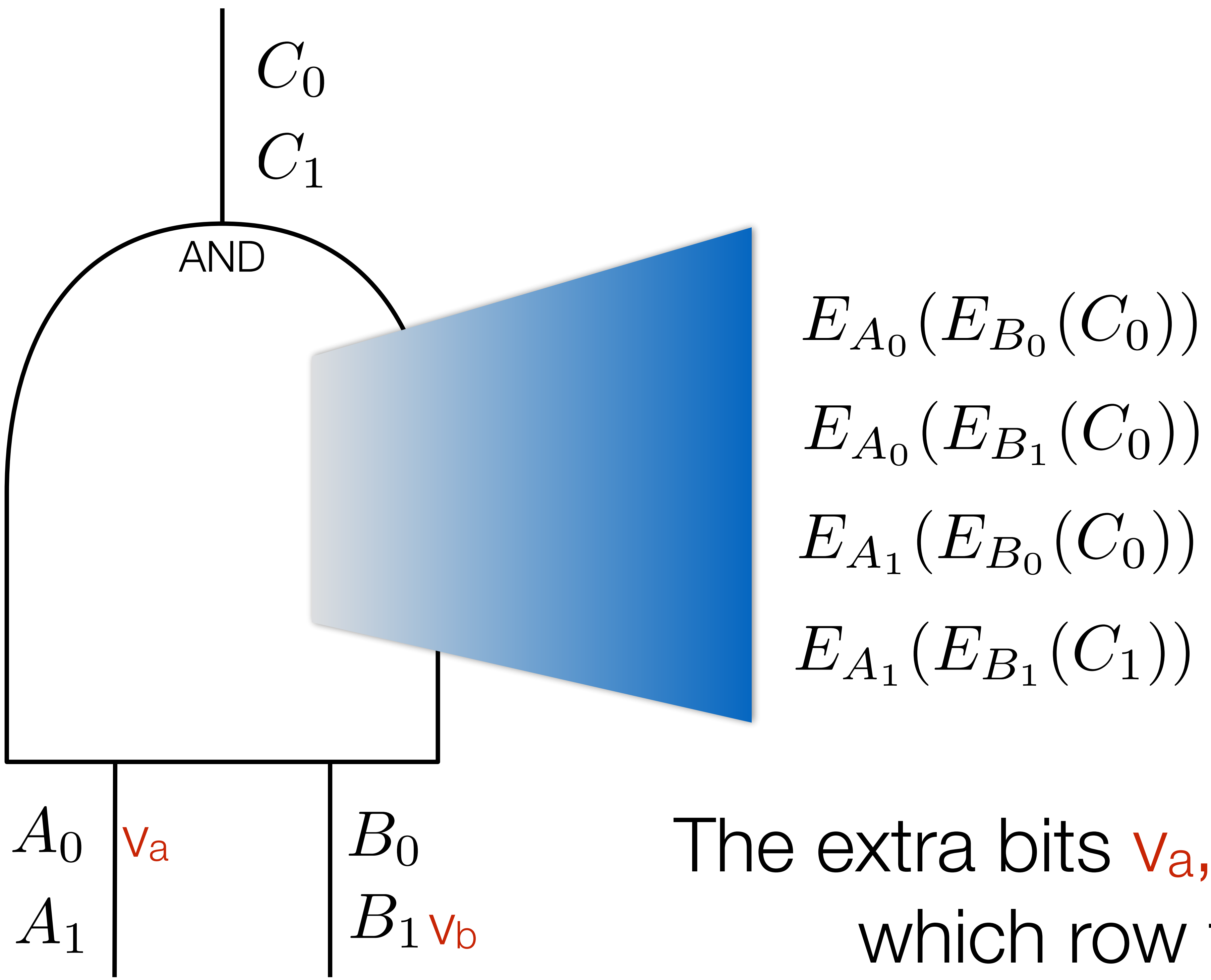


Classic Garbling



Permute bits

[Beaver-Micali-Rogaway]



The extra bits v_a,v_b designate which row to use.

Security property

Garbling of function: Gb(f), En(X)

Encoding of input: X

Output: y=f(x)

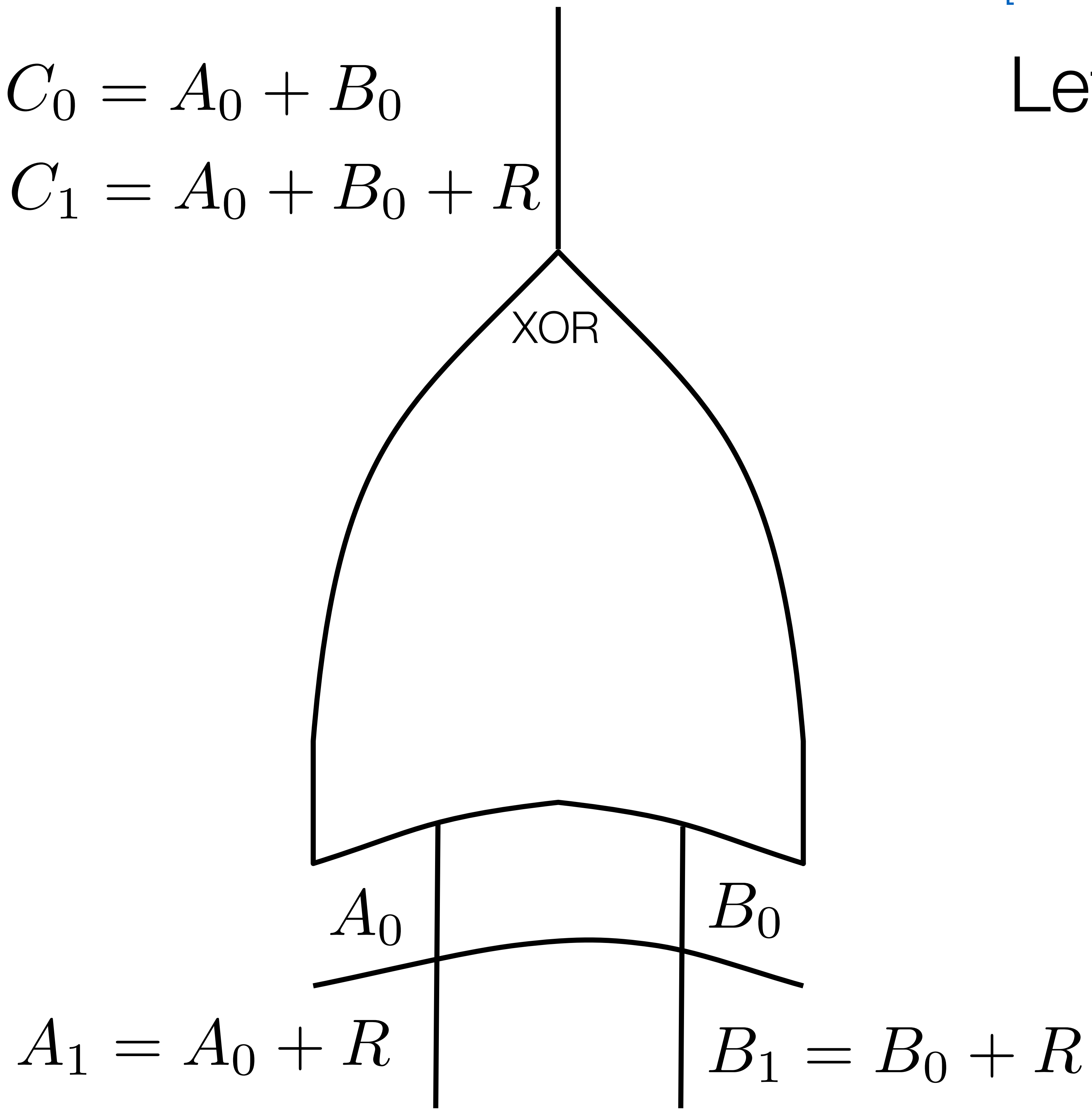
should be indistinguishable from

Sim(f,y)

Free XOR garbling

[Kolesnikov-Schneider]

Let R be a random string s.t. R mod 2 =1

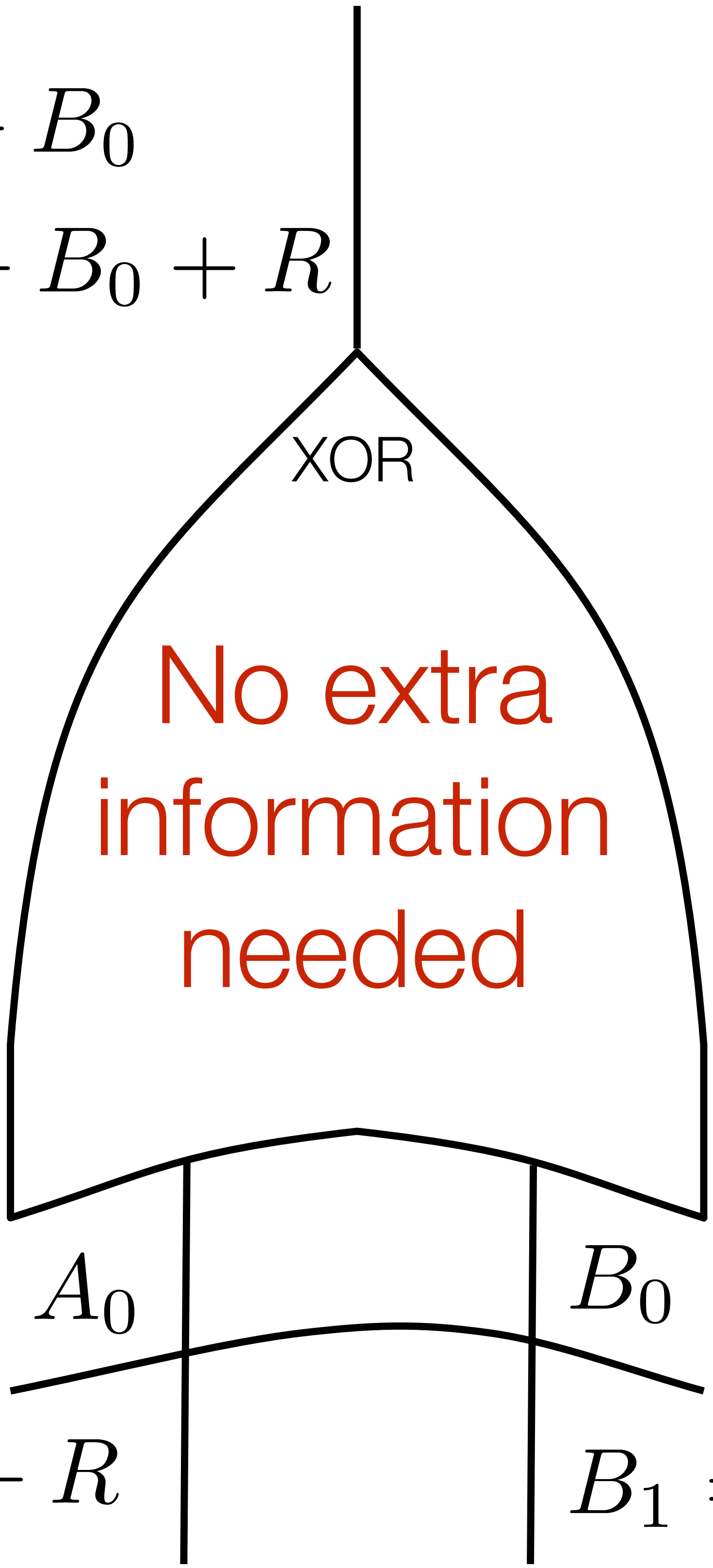


Free XOR garbling

[Kolesnikov-Schneider]

$C_0 = A_0 + B_0$

$C_1 = A_0 + B_0 + R$



$A_1 = A_0 + R$

$B_1 = B_0 + R$

Let R be a random string s.t. R mod 2 =1

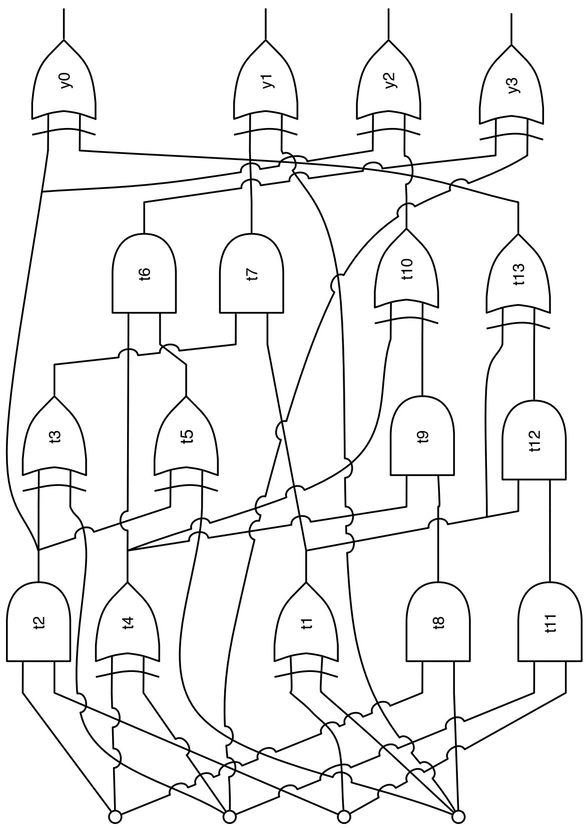
Evaluator simply XORs input wires to compute output wire. Secure with good Enc.

[Chou-Katz-Kumaresan-Zhou]

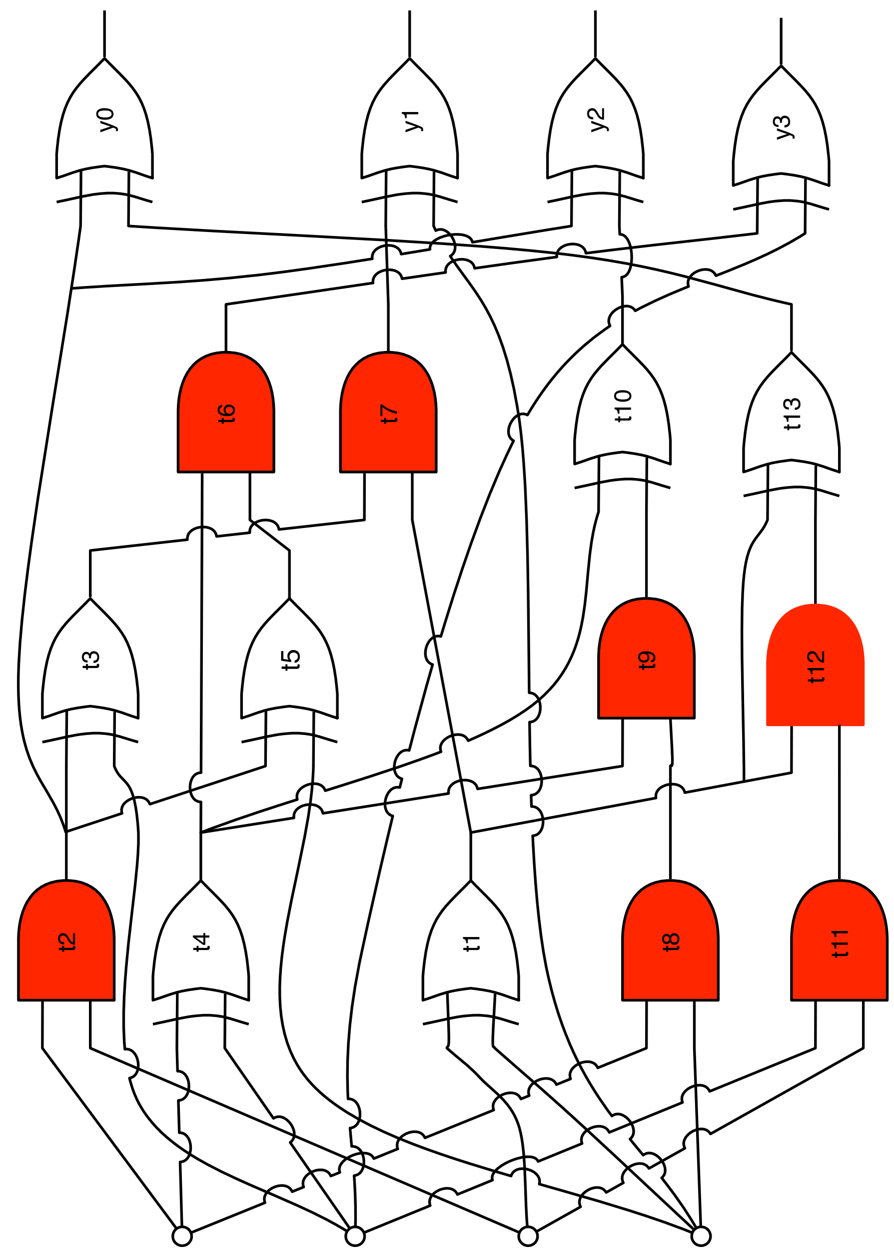
Why is gate-by-gate garbling the best (only) strategy?

Garbling gate by gate has disadvantages.

gate-by-gate introduces extra depth to the degarble circuit



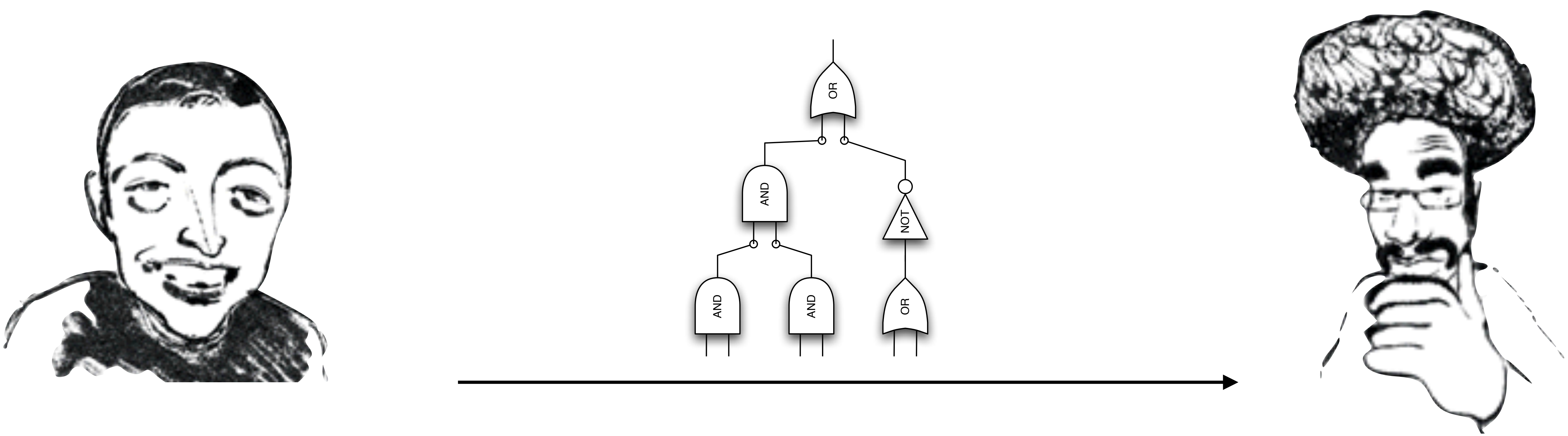
Plain



Each AND gate incurs extra depth of cryptographic H function

If the original circuit has depth d, then the garbled circuit may have depth d*depth(H)

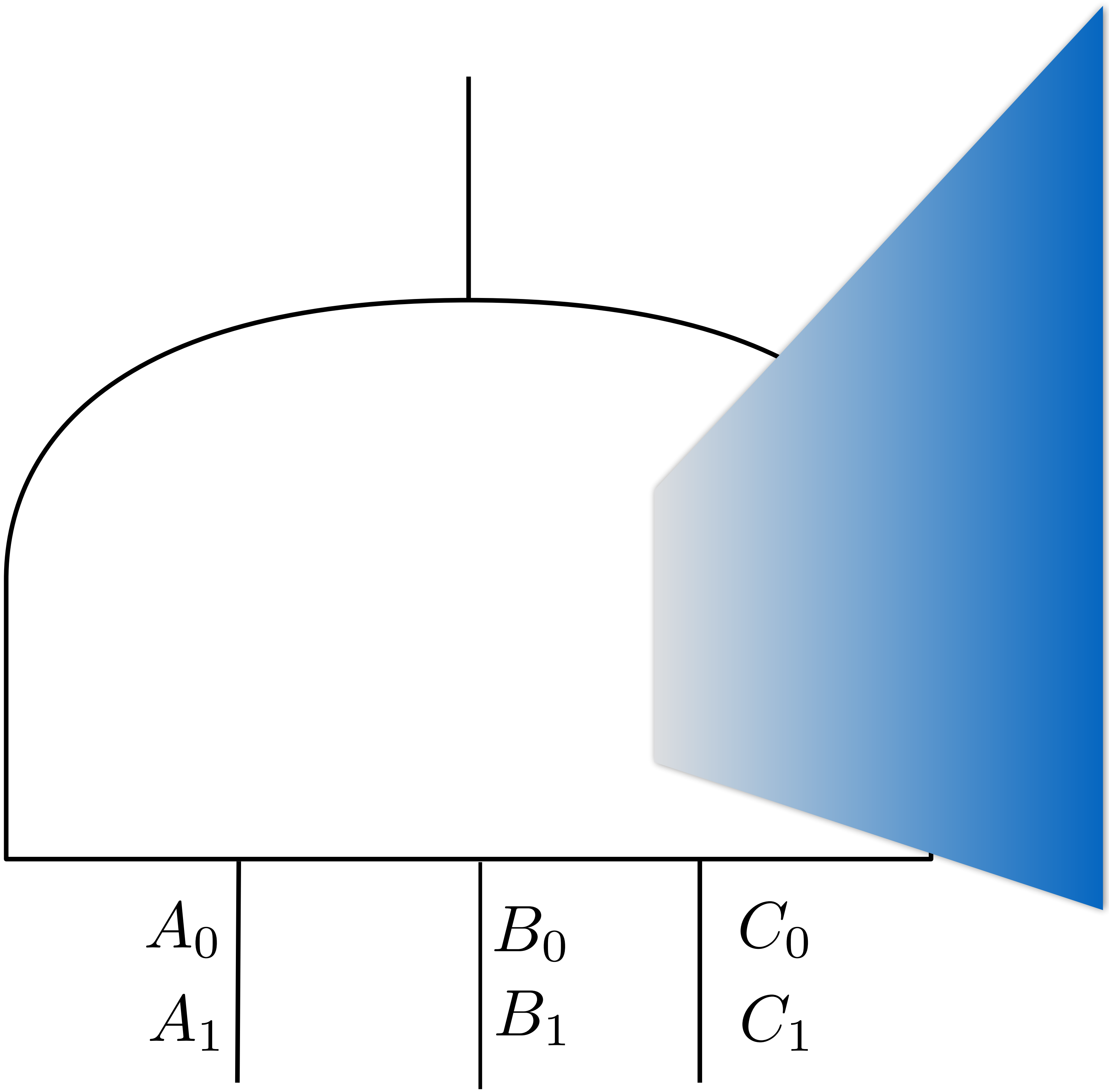
Q: Does gate-by-gate garbling minimize the size of the garbling?



Alternatives to gate-by-gate garbling?

[Applebaum-Ishai-Kushilevitz] ~~LWE~~

N-input gate = 2^n rows



$$E_{A_0}(E_{B_0}(E_{C_0}(D_0)))$$
$$E_{A_0}(E_{B_0}(E_{C_1}(D_0)))$$
$$E_{A_0}(E_{B_1}(E_{C_0}(D_0)))$$
$$E_{A_0}(E_{B_1}(E_{C_1}(D_0)))$$
$$E_{A_1}(E_{B_0}(E_{C_0}(D_0)))$$
$$E_{A_1}(E_{B_0}(E_{C_1}(D_0)))$$
$$E_{A_1}(E_{B_1}(E_{C_0}(D_0)))$$
$$E_{A_1}(E_{B_1}(E_{C_1}(D_1)))$$

[Boyar-Peralta]

$$c_\wedge(f_{2n}) \leq 2^{n+1} - n - 2$$

# of AND gates needed to compute a function of 2n vars

[Boyar-Peralta]

$$c_\wedge(f_{2n}) \leq 2^{n+1} - n - 2$$

This implies that the SIZE of a garbled circuit for f_{2n} using just AND gates is less than

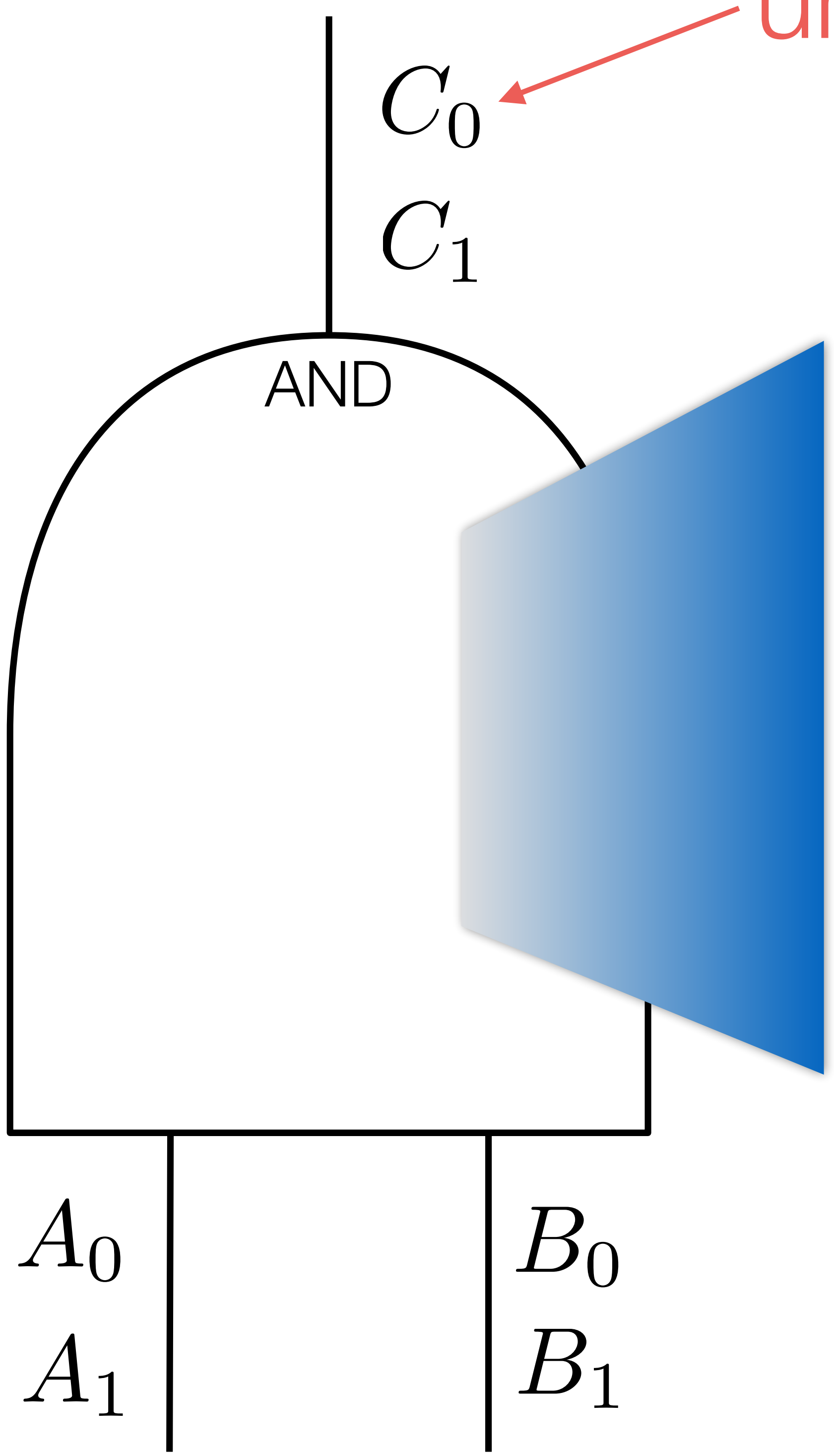
$$2^{n+3} - 4n - 8$$ ciphertexts

$$4 \cdot c_\wedge(f_{2n}) \leq 4(2^{n+1} - n - 2) < 2^{2n}$$

Garbled Row Reduction

[Naor-Pinkas-Sumner]

unconstrained variable



$$E_{A_0}(E_{B_0}(C_0))$$

$$E_{A_0}(E_{B_1}(C_0))$$

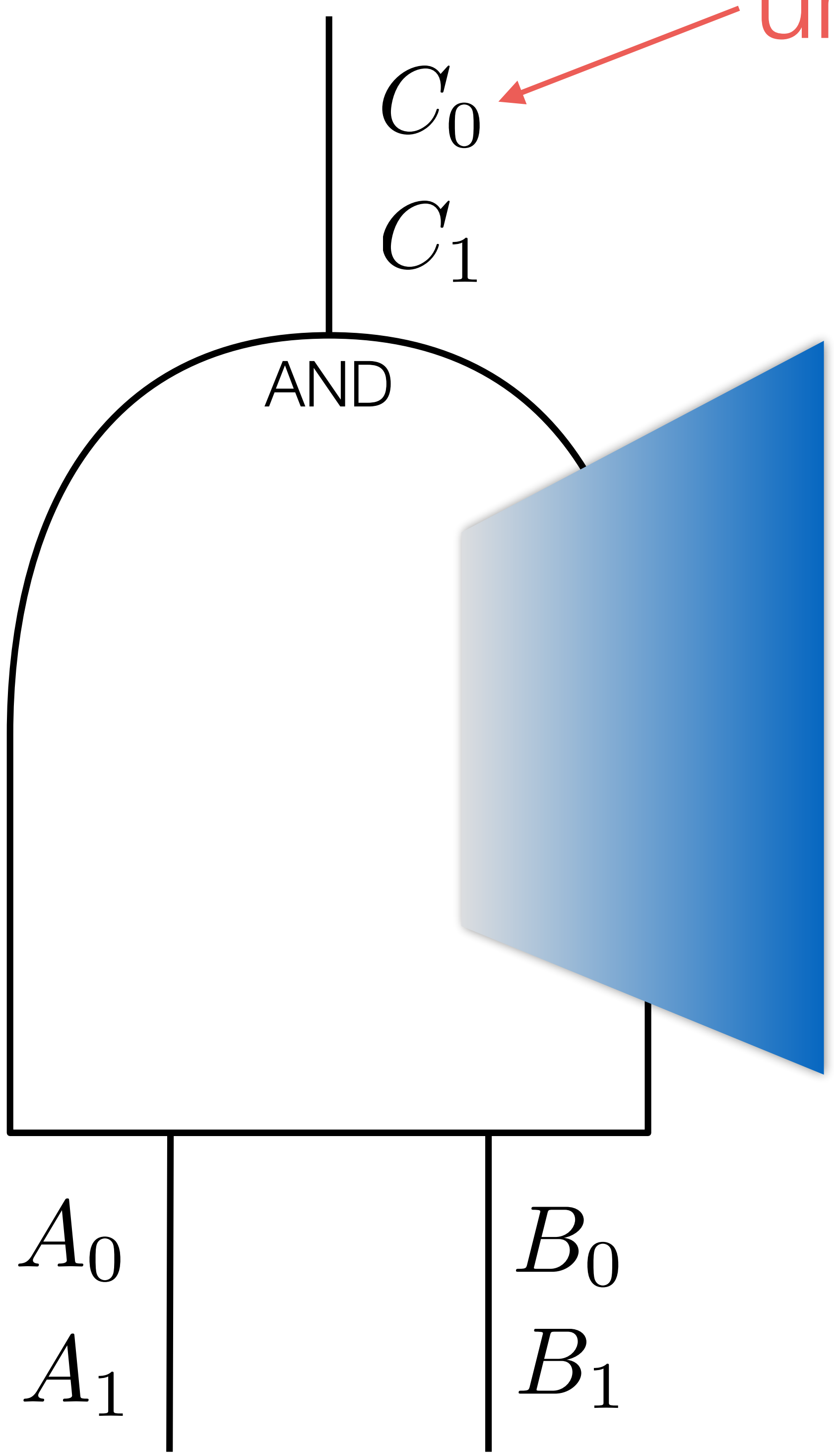
$$E_{A_1}(E_{B_0}(C_0))$$

$$E_{A_1}(E_{B_1}(C_1))$$

Garbled Row Reduction

[Naor-Pinkas-Sumne

unconstrained variable



$E_{A_0}(E_{B_0}(C_0))$ = 0

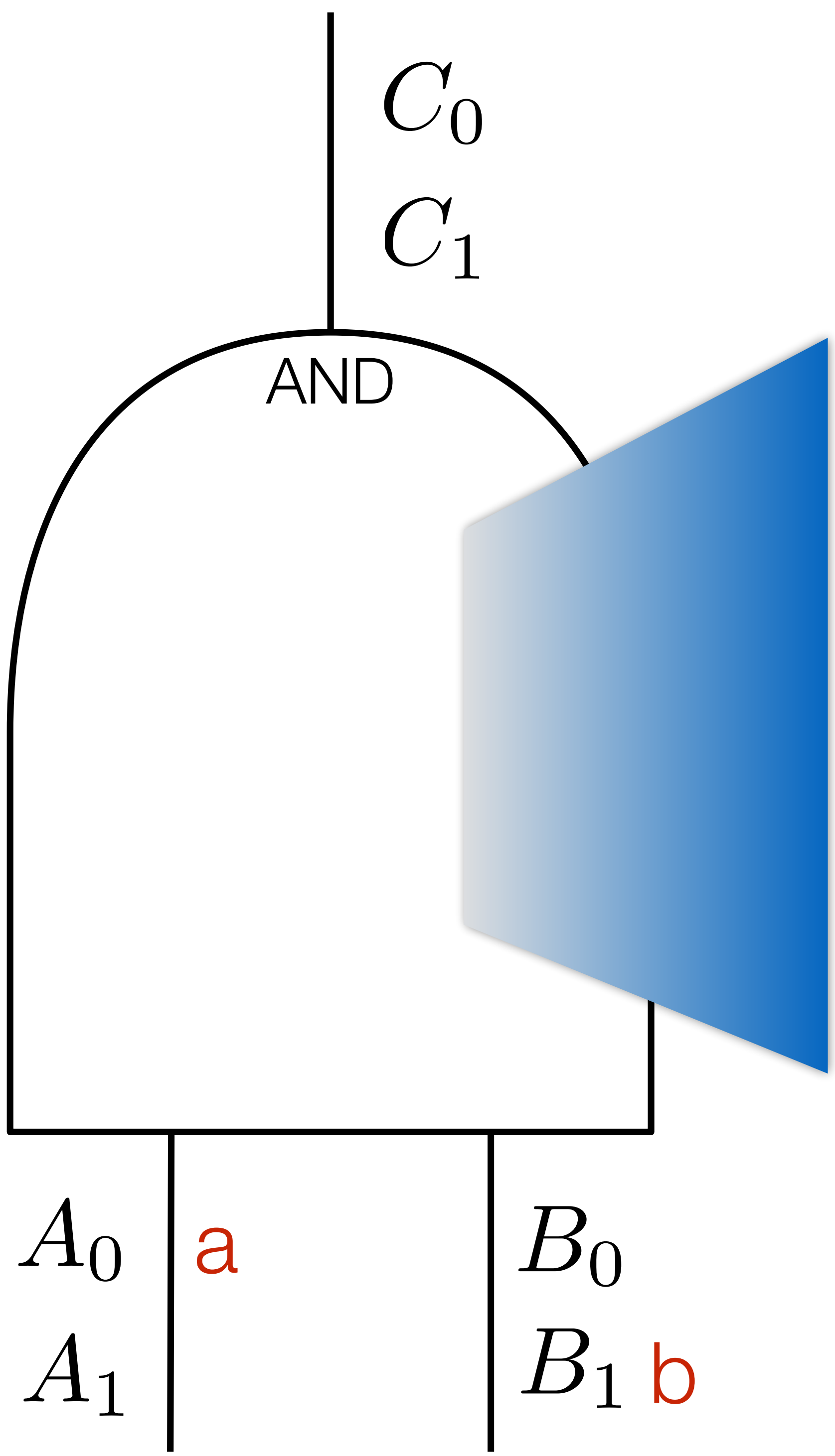
$E_{A_0}(E_{B_1}(C_0))$

$E_{A_1}(E_{B_0}(C_0))$

$E_{A_1}(E_{B_1}(C_1))$

implies that

$C_0 = D_{B_0}(D_{A_0}(0))$



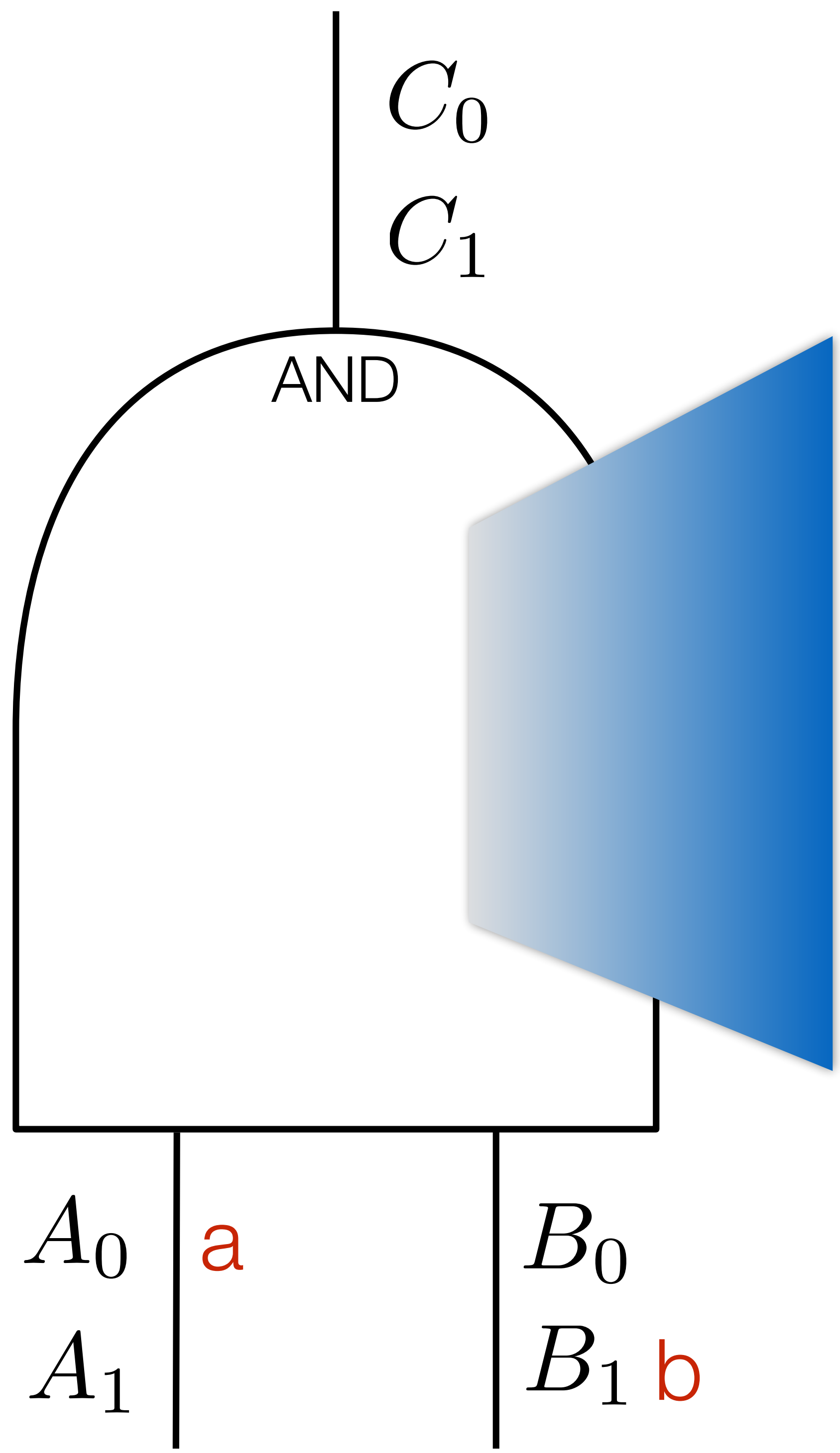
(0)

$E_{A_0}(E_{B_1}(C_0))$

$E_{A_1}(E_{B_0}(C_0))$

$E_{A_1}(E_{B_1}(C_1))$

3 rows,
not 4



(0)

$E_{A_0}(E_{B_1}(C_0))$

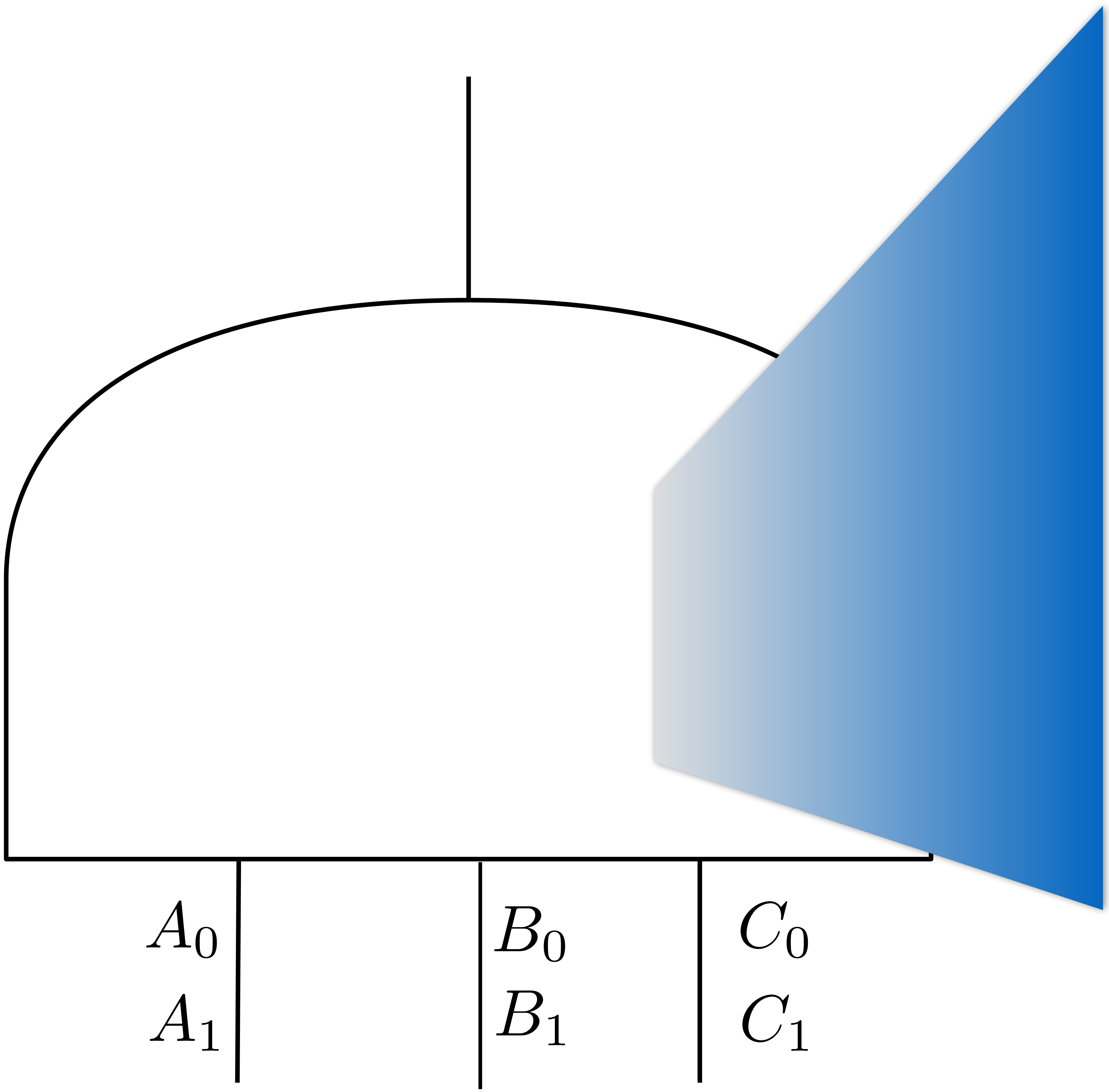
$E_{A_1}(E_{B_0}(C_0))$

$E_{A_1}(E_{B_1}(C_1))$

3 rows, not 4

works with Free-xor if $C_1 = C_0 + R$

N-input gate = 2^n-1 rows



(0)

$E_{A_0}(E_{B_0}(E_{C_1}(D_0)))$

$E_{A_0}(E_{B_1}(E_{C_0}(D_0)))$

$E_{A_0}(E_{B_1}(E_{C_1}(D_0)))$

$E_{A_1}(E_{B_0}(E_{C_0}(D_0)))$

$E_{A_1}(E_{B_0}(E_{C_1}(D_0)))$

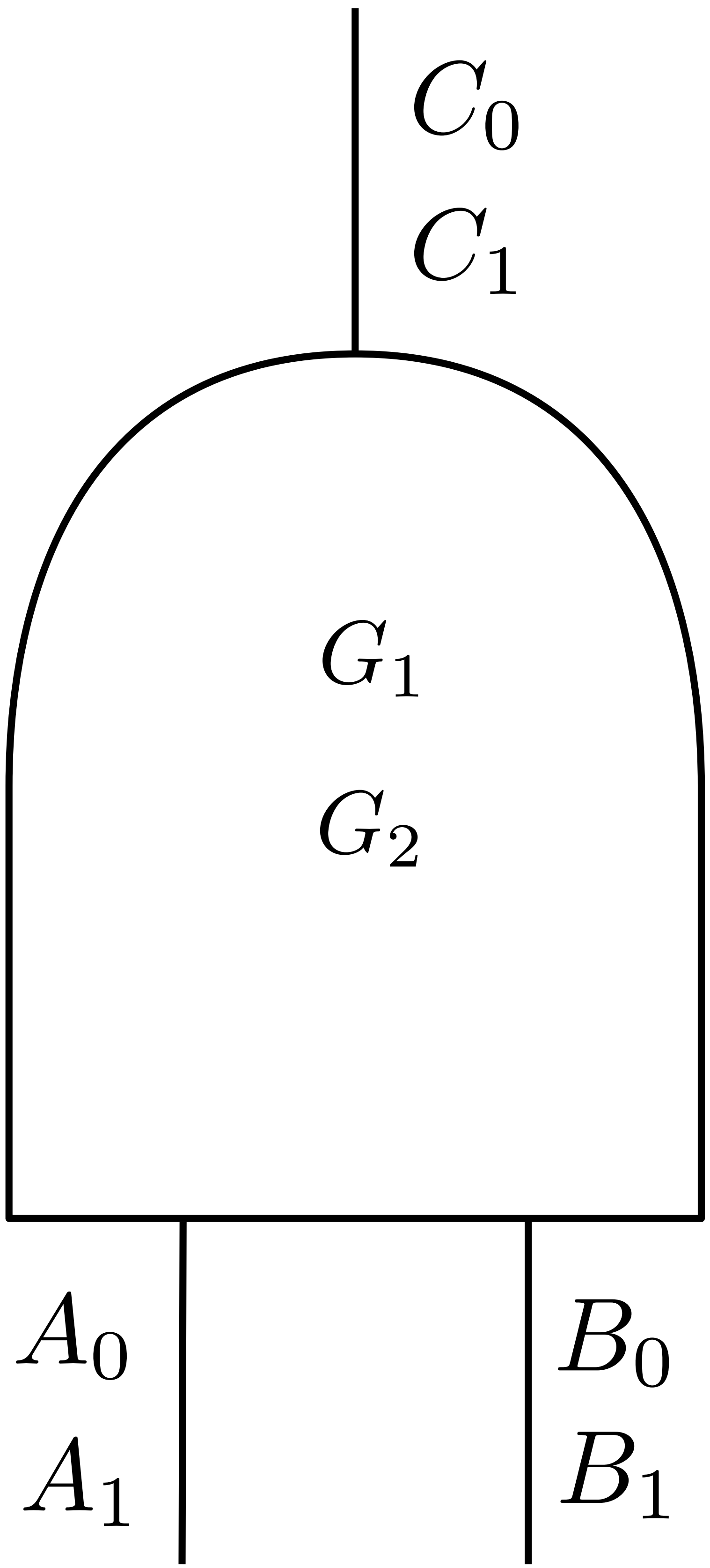
$E_{A_1}(E_{B_1}(E_{C_0}(D_0)))$

$E_{A_1}(E_{B_1}(E_{C_1}(D_1)))$

Still better to use AND$_2$ gates

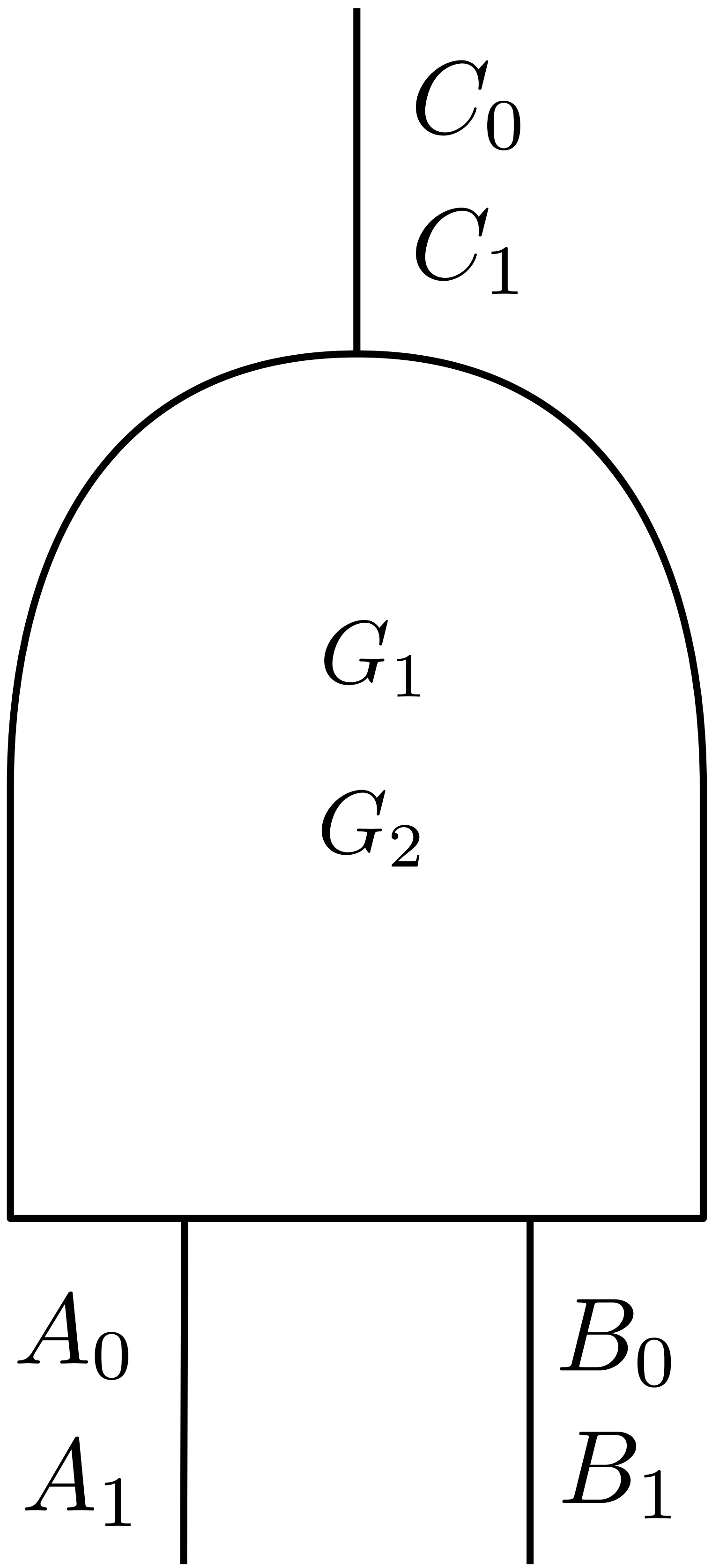
$$3 \cdot c_{\wedge}(f_{2n}) \leq 3(2^{n+1} - n - 2) < 2^{2n} - 1$$

2-row garbling [Naor-Pinkas-Sumner]



View the problem of garbling as one of secret sharing

2-row garbling [Naor-Pinkas-Sumner]



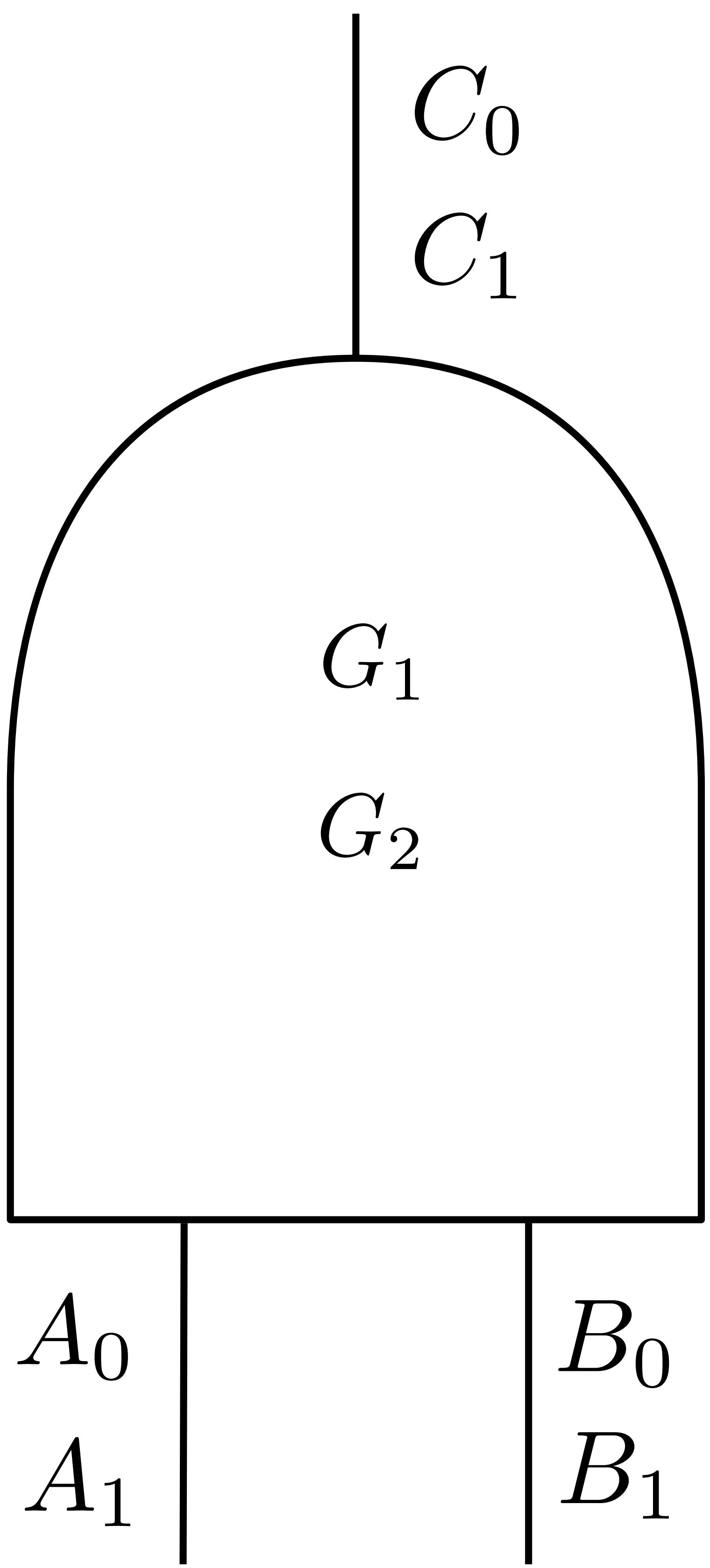
$H(A_1, B_1)$ G_1 G_2 C_0

$H(A_0, B_1)$

$H(A_0, B_0)$

$H(A_1, B_0)$

2-row garbling [Naor-Pinkas-Sumner]



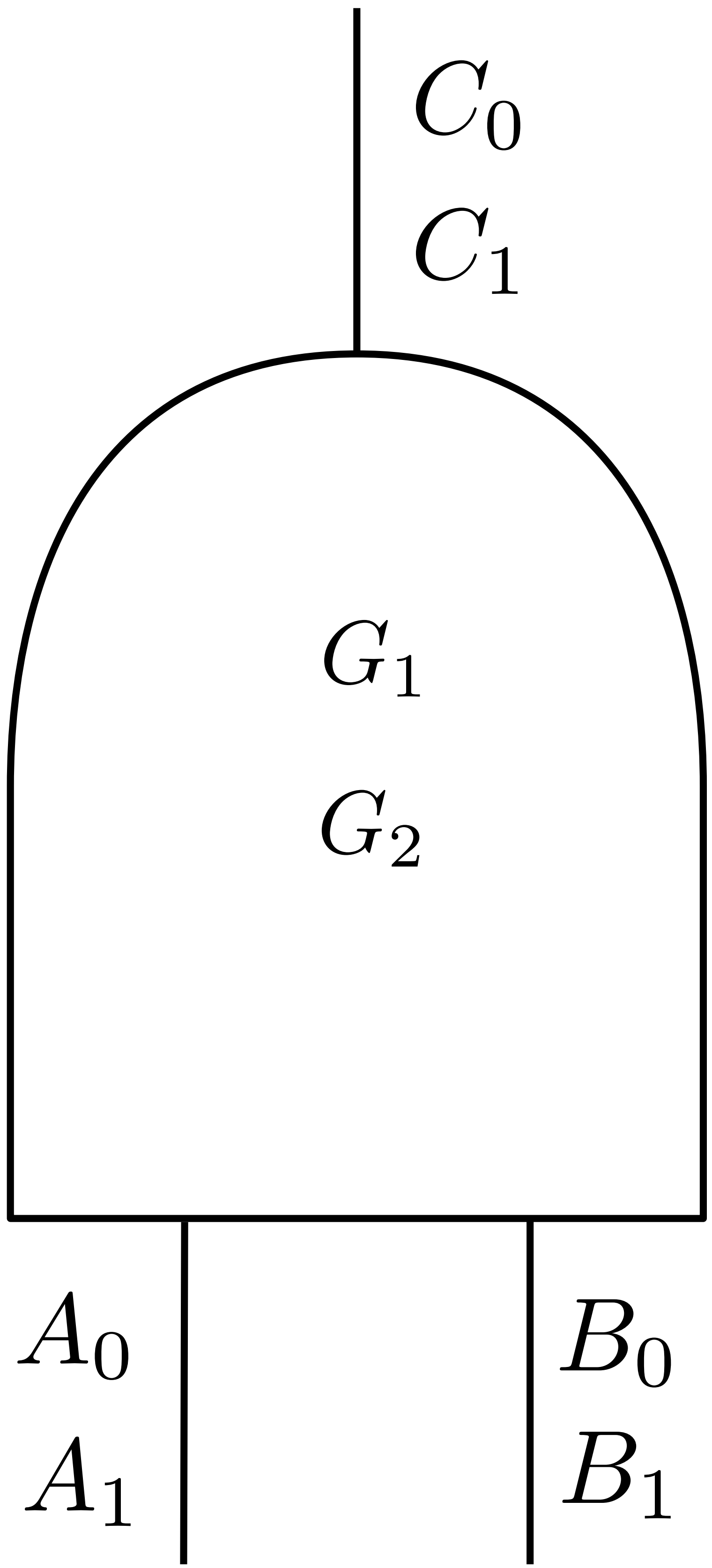
$H(A_1, B_1)$ G_1 G_2 C_0

$H(A_0, B_1)$

$H(A_0, B_0)$

$H(A_1, B_0)$

2-row garbling [Naor-Pinkas-Sumner]



$H(A_1, B_1)$ G_1 G_2 C_0

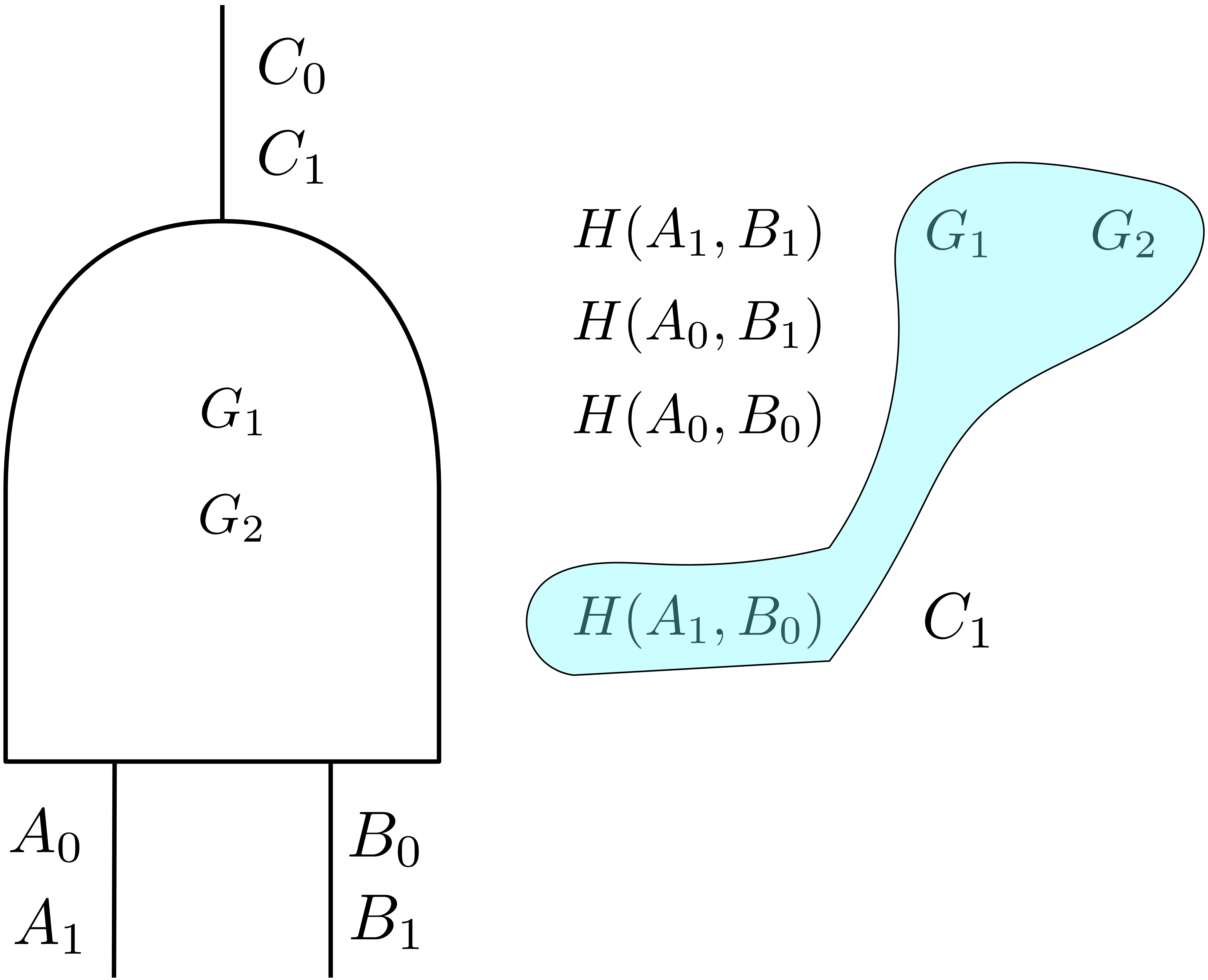
$H(A_0, B_1)$

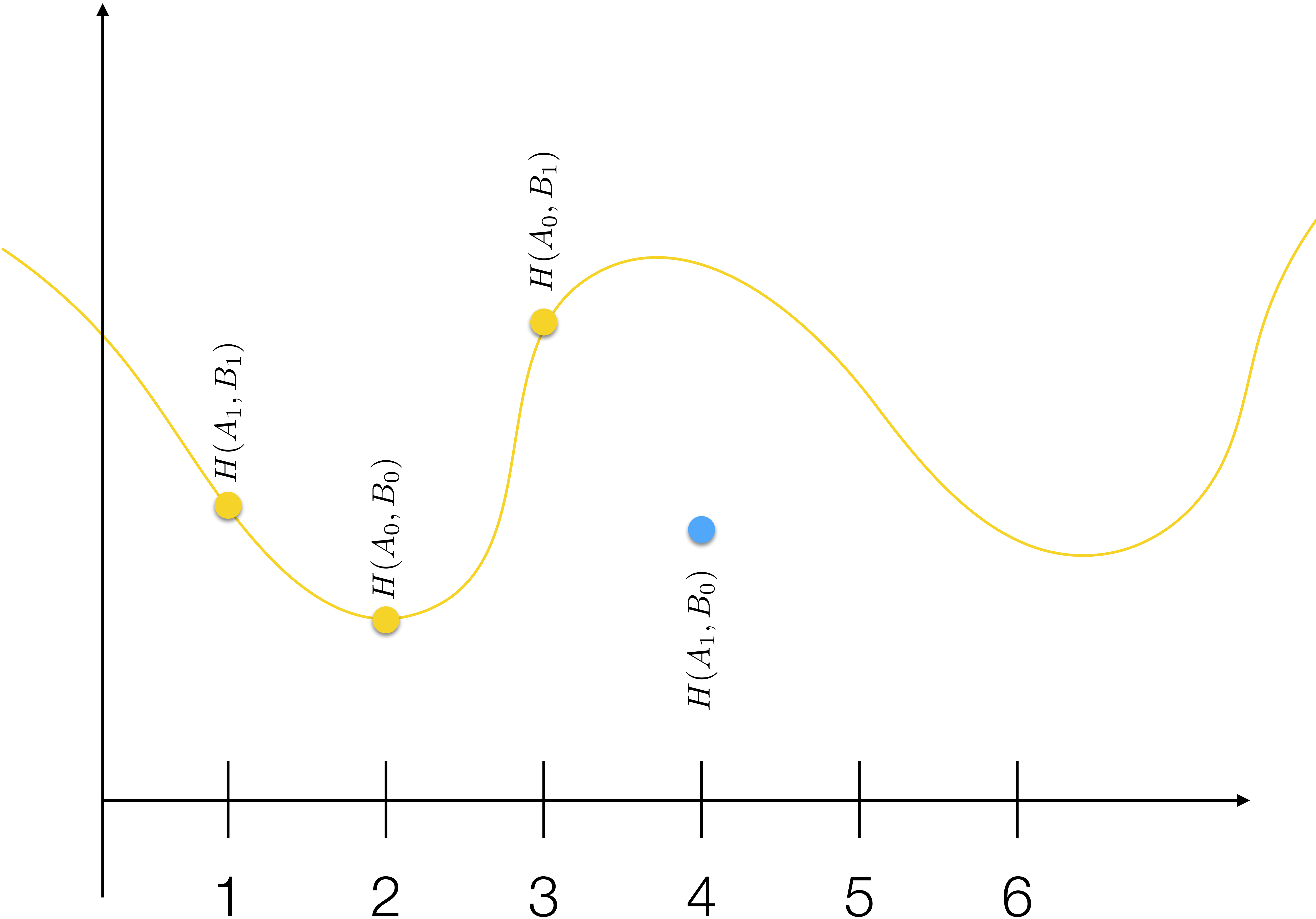
$H(A_0, B_0)$

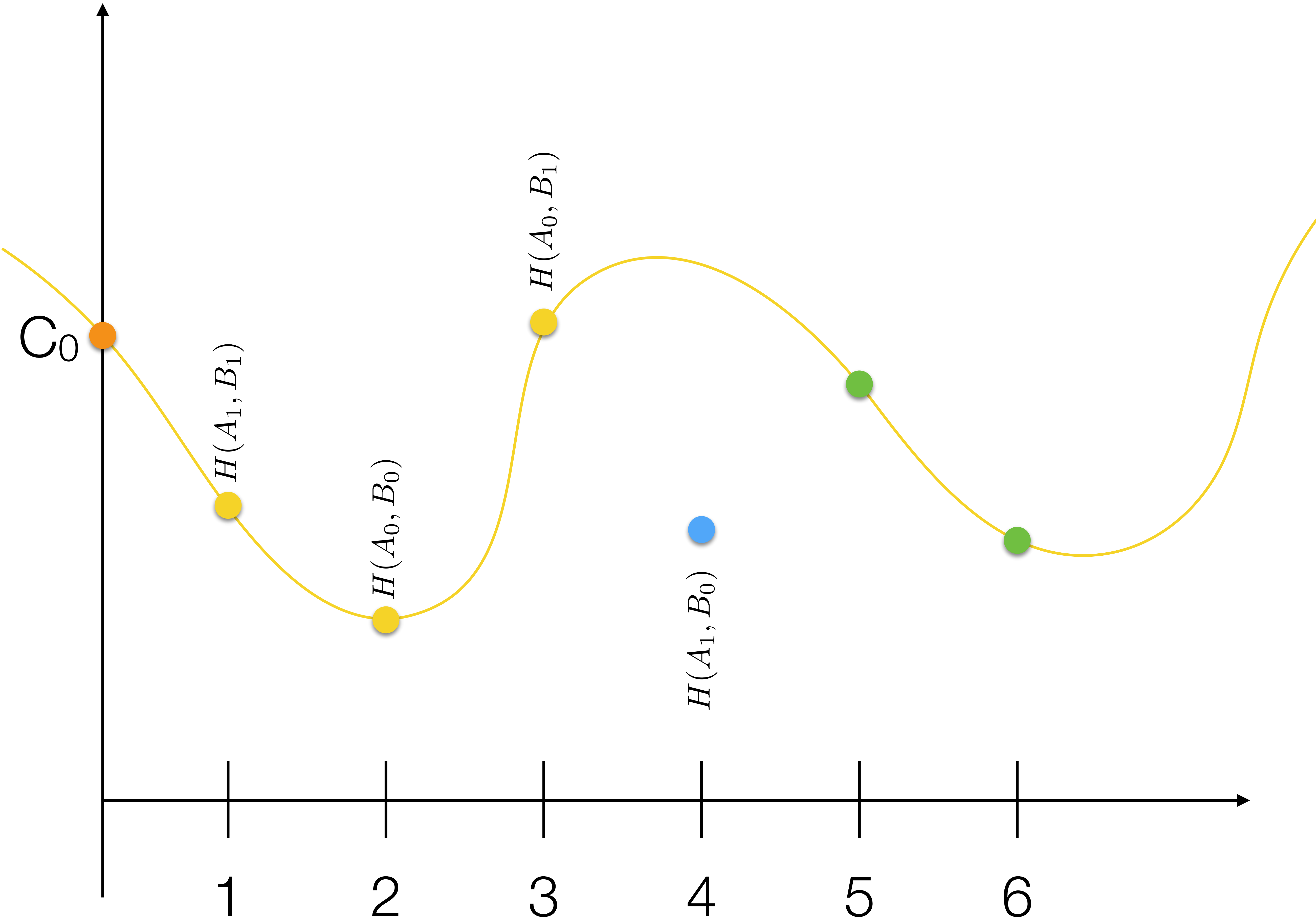
$H(A_1, B_0)$

2-row garbling

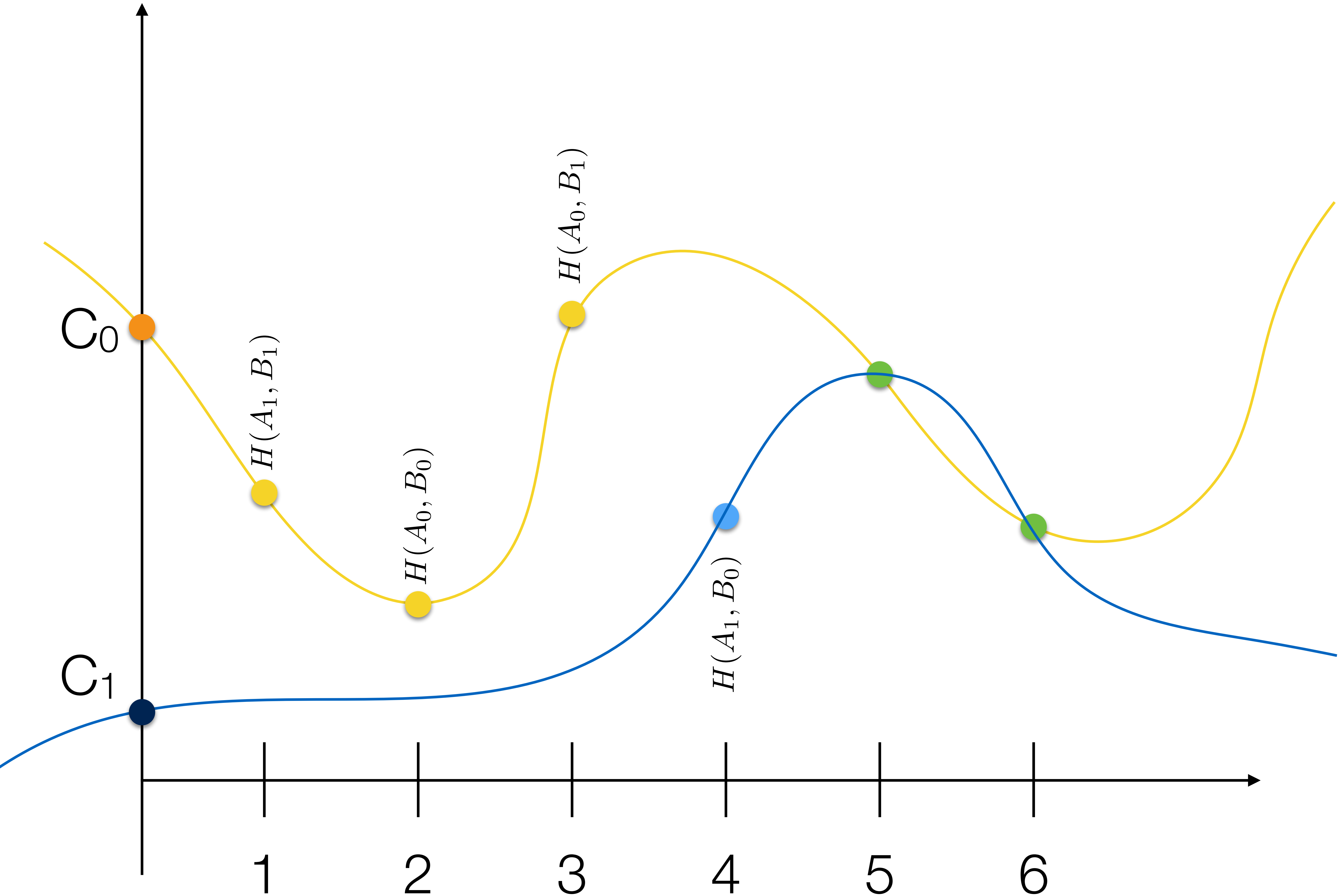
[Naor-Pinkas-Sumner]




$H(A_1, B_1)$
$H(A_0, B_0)$
$H(A_0, B_1)$
$H(A_1, B_0)$
1
2
3
4
5
6

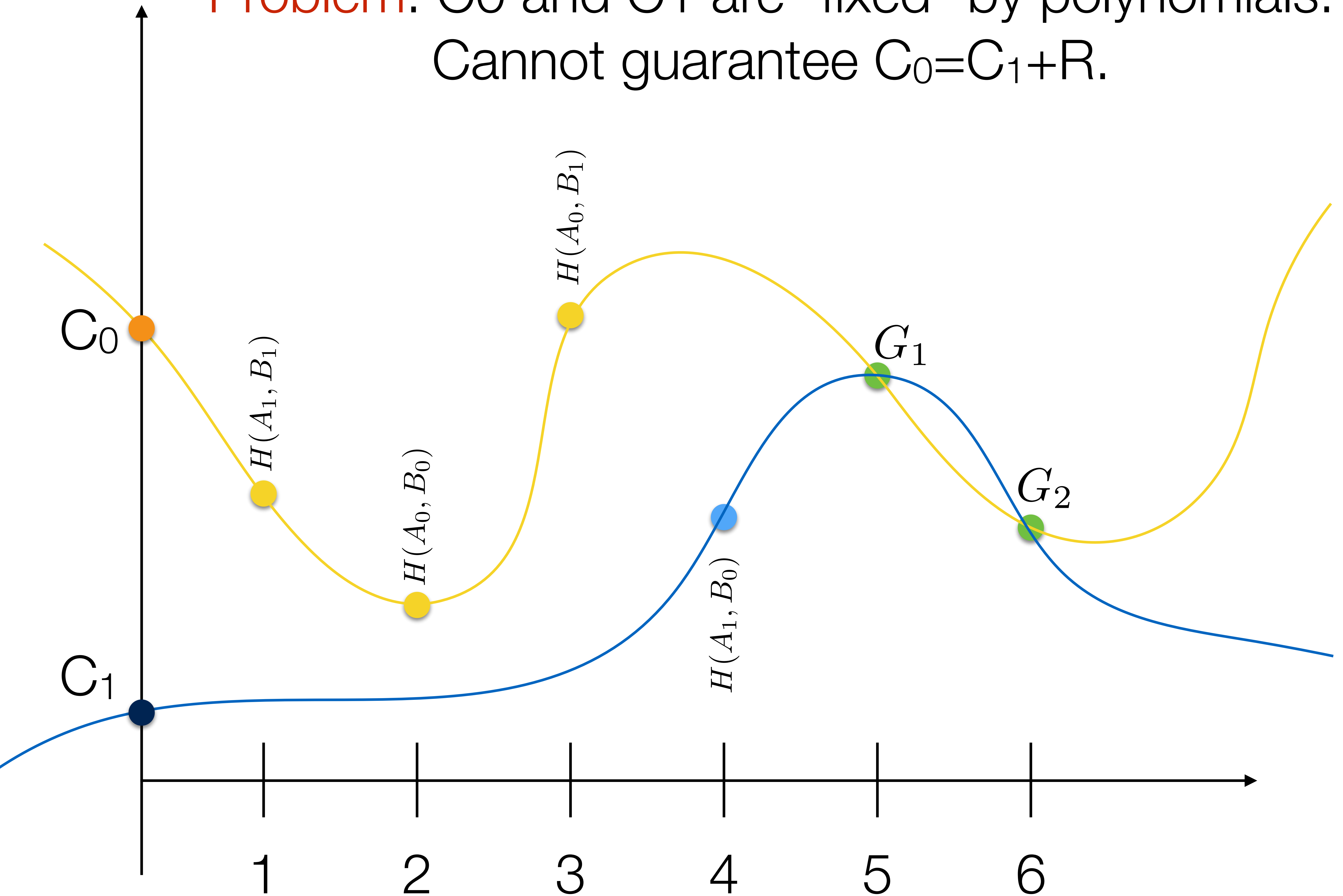


C_0
$H(A_1, B_1)$
$H(A_0, B_0)$
$H(A_0, B_1)$
$H(A_1, B_0)$
1
2
3
4
5
6



C0
C1
$H(A_1, B_1)$
$H(A_0, B_0)$
$H(A_0, B_1)$
$H(A_1, B_0)$
1
2
3
4
5
6

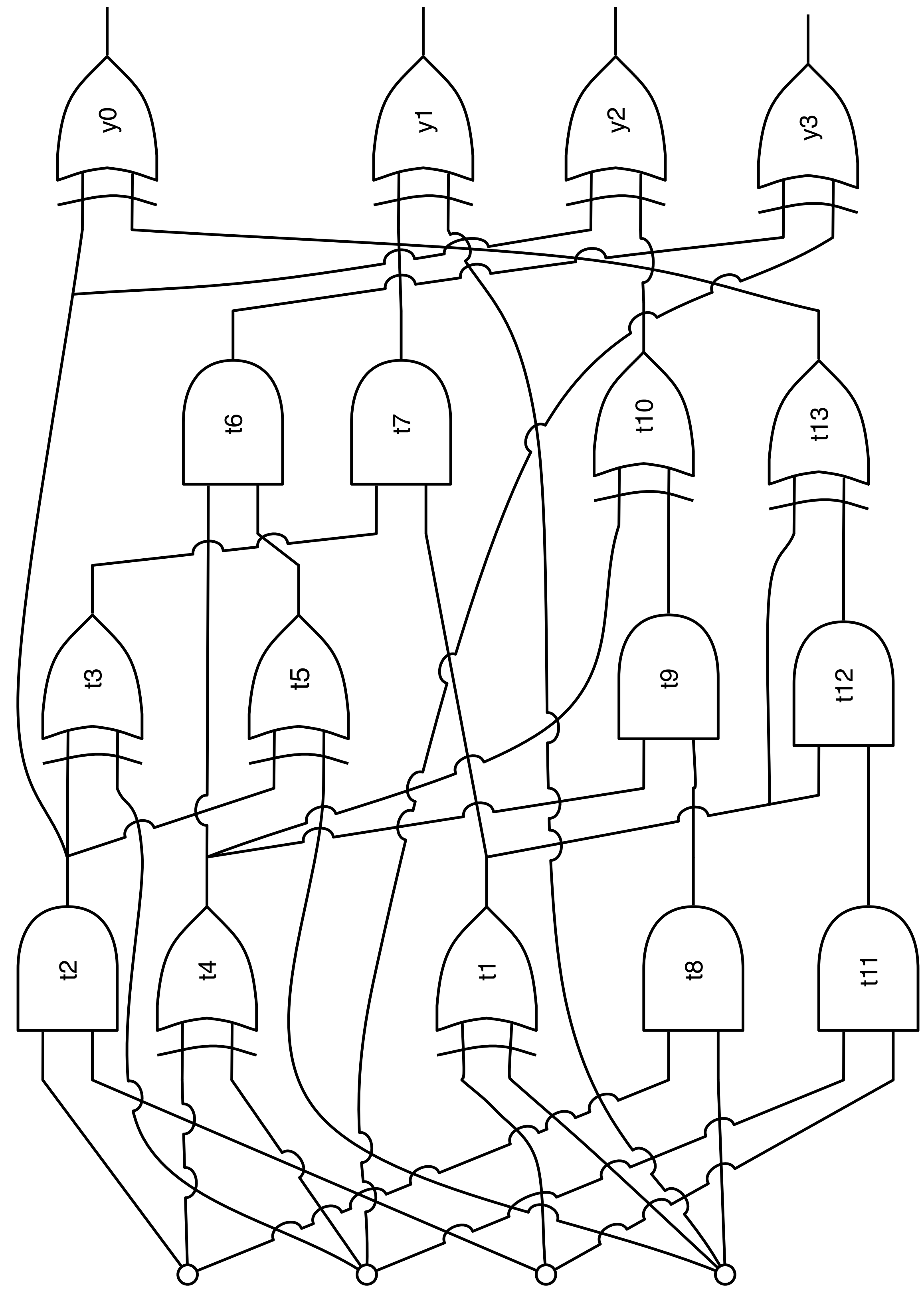
Problem: C0 and C1 are "fixed" by polynomials. Cannot guarantee $C_0 = C_1 + R$.

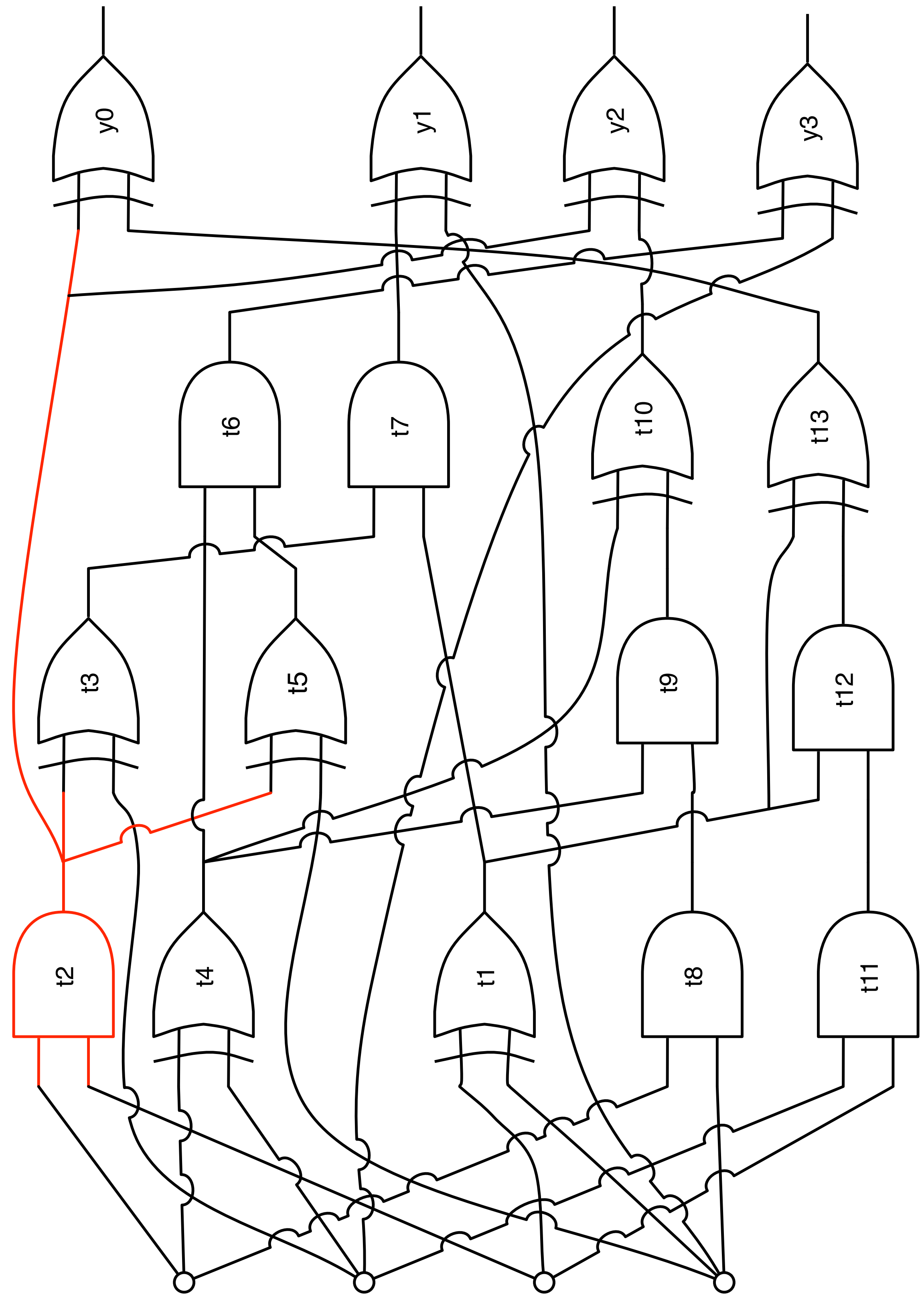


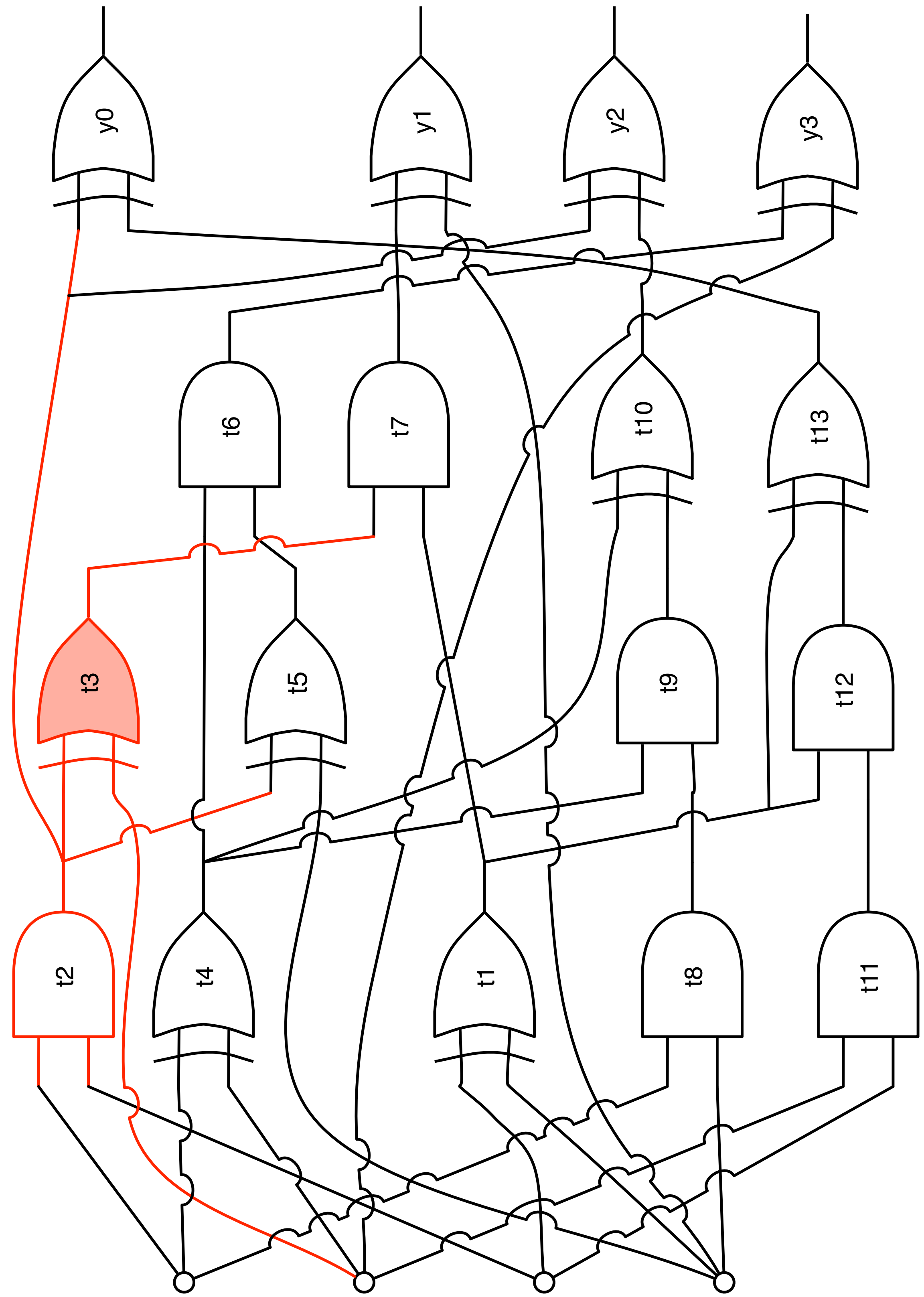
Still better to use AND_2 gates

Because XOR gates are not FREE!

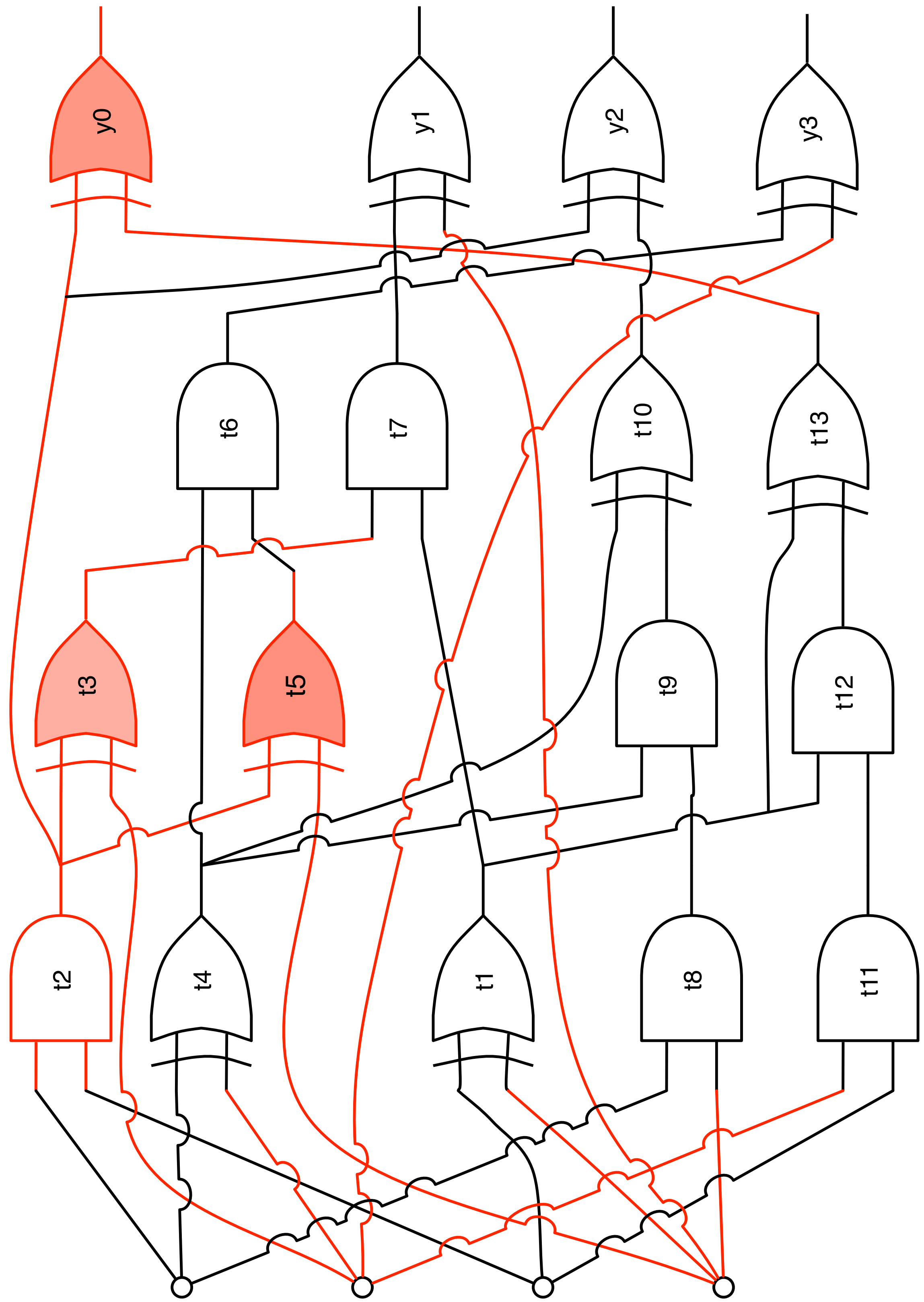
Flexor garbling [Mohassel-Rosulek]

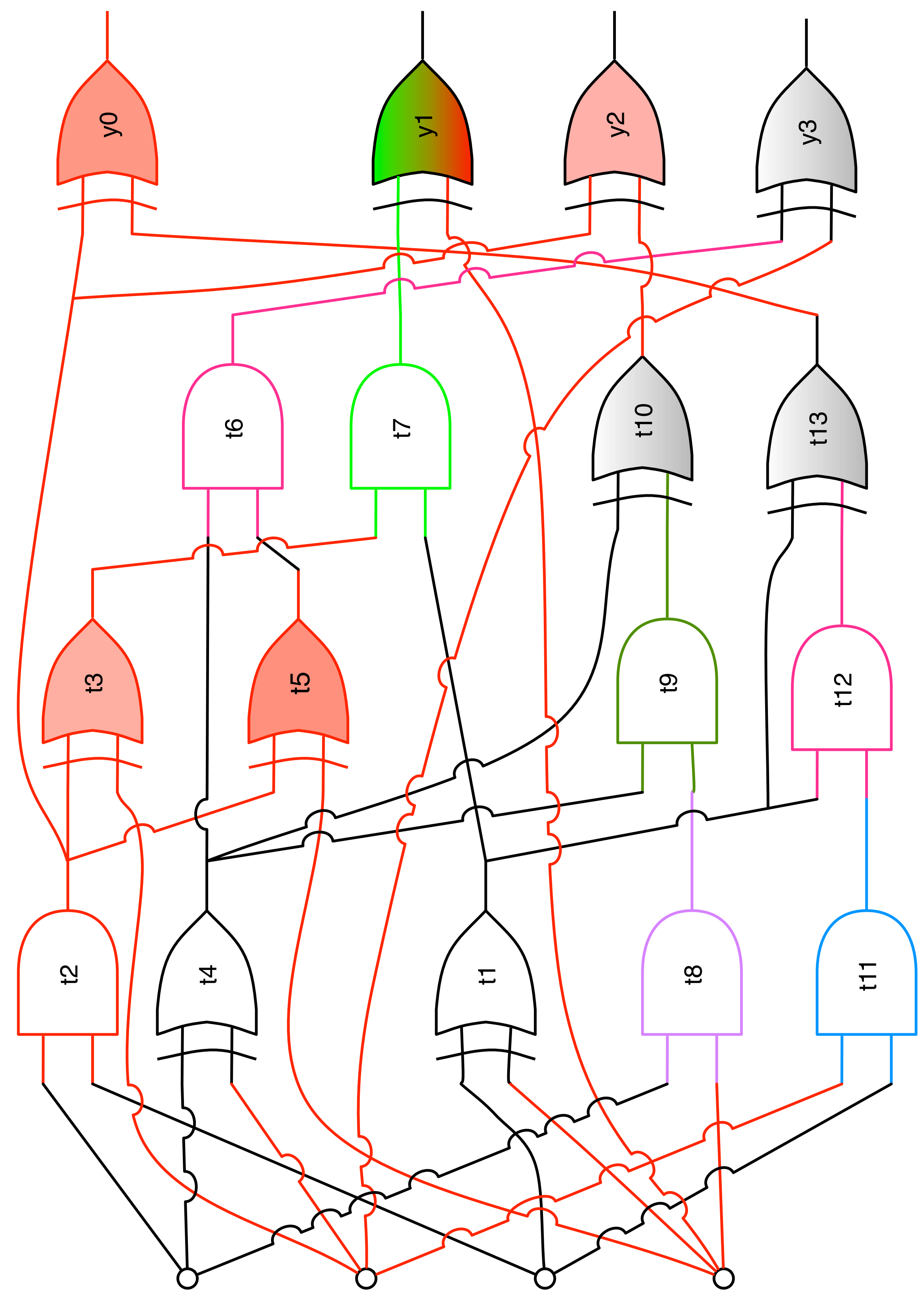



y0
y1
y2
y3
t6
t7
t10
t13
t3
t5
t9
t12
t2
t4
t1
t8
t11



y0
y1
y2
y3
t6
t7
t10
t13
t3
t5
t9
t12
t2
t4
t1
t8
t11

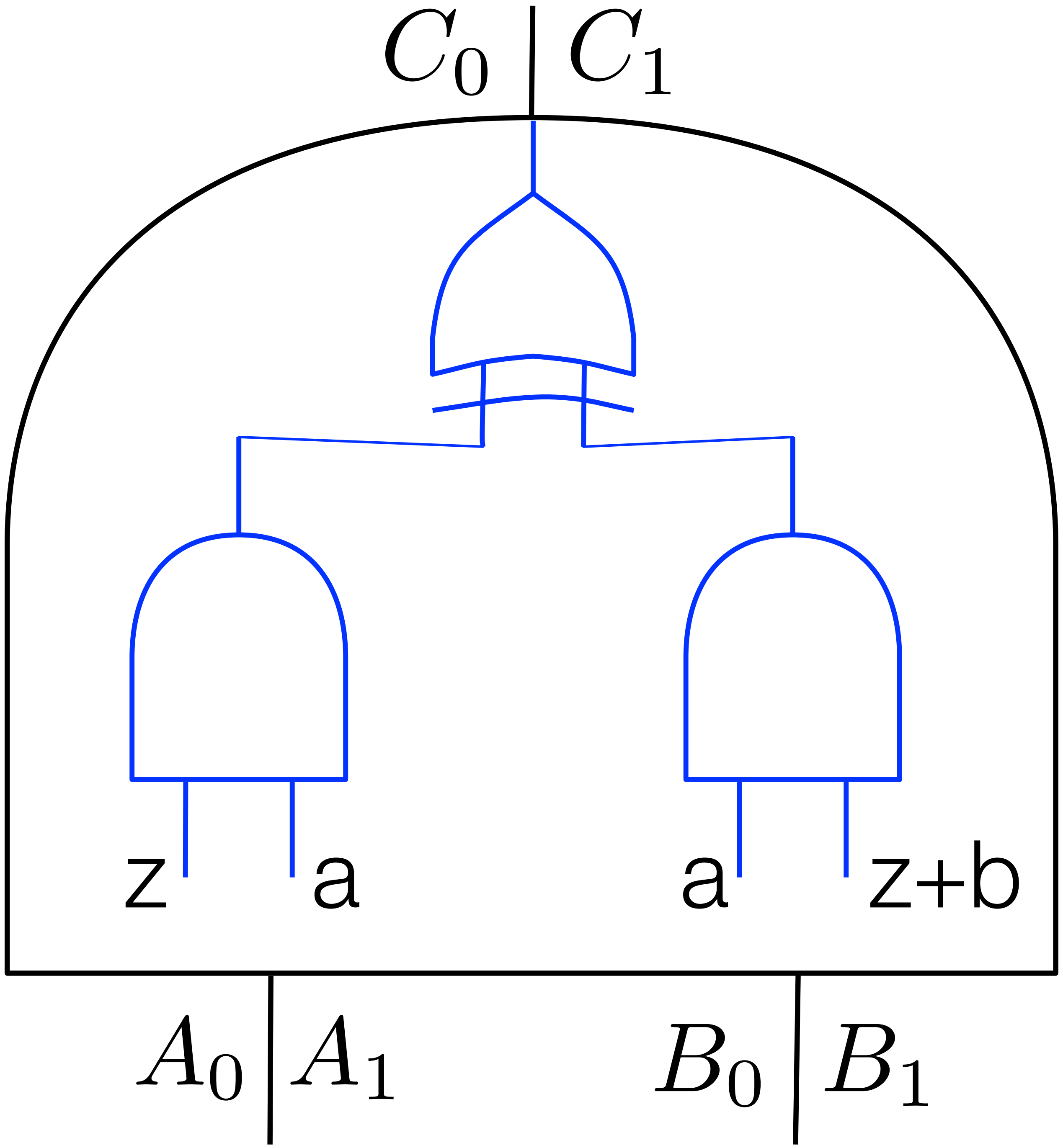

y0
y1
y2
y3
t6
t7
t10
t13
t3
t5
t9
t12
t2
t4
t1
t8
t11



Gates requires 0,1,2 ciphertexts

Half-gate Garbling

[Zahur-Evans-Rosulek]

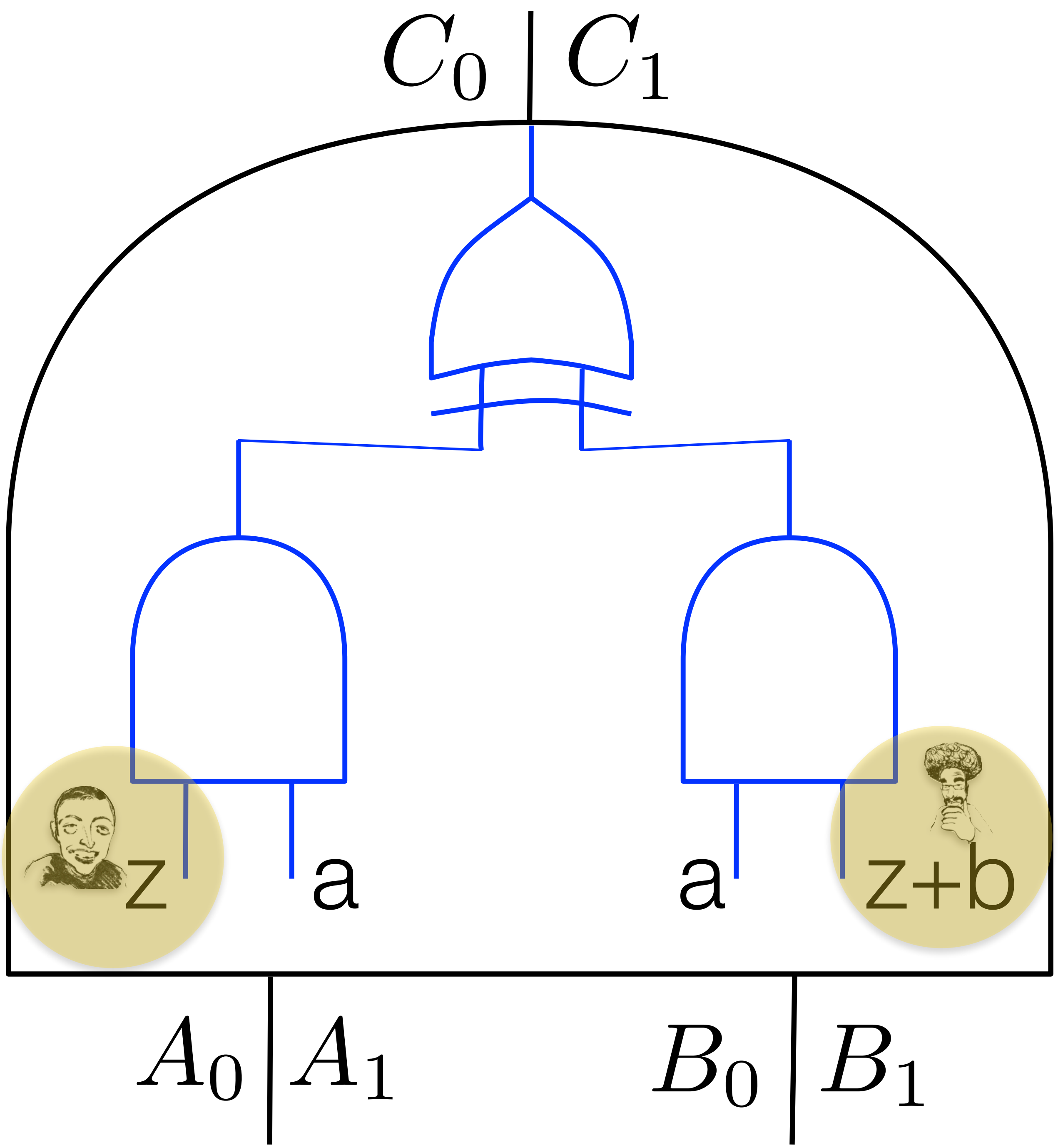


$$(a \wedge z) + (a \wedge (b + z) = a \wedge b$$

random bit

Half-gate Garbling

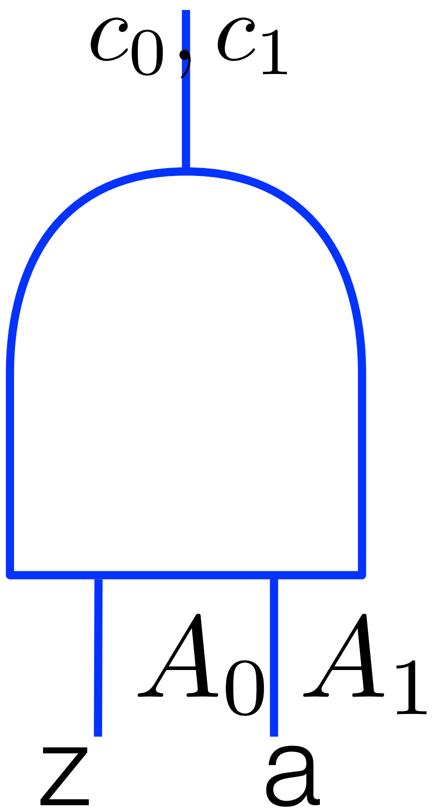
[Zahur-Evans-Rosulek]



$$(a \wedge z) + (a \wedge (b + z)) = a \wedge b$$

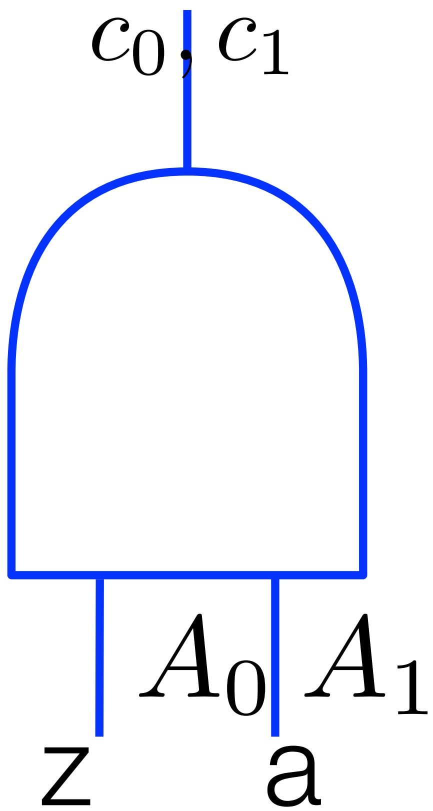
random bit

Generator knows z



z=0	z=1
$H(A_0) \oplus C_0$	$H(A_0) \oplus C_0$
$H(A_1) \oplus C_0$	$H(A_1) \oplus C_1$

Generator knows z

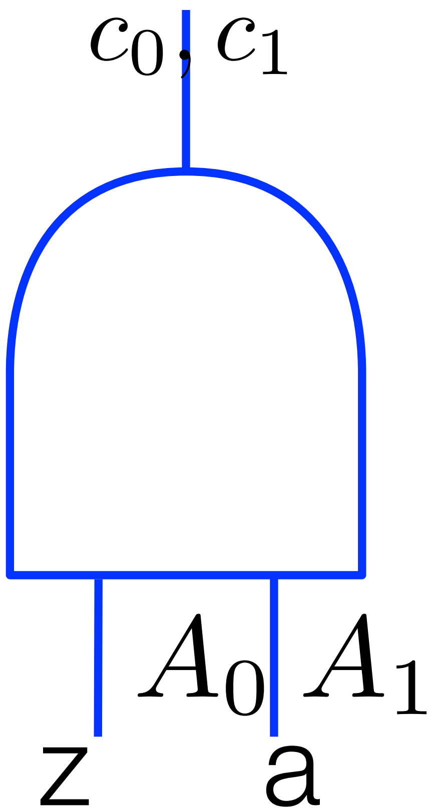


z=0	z=1
$\cancel{H(A_0) \oplus C_0}$	$H(A_0) \oplus C_0$
$H(A_1) \oplus C_0$	$H(A_1) \oplus C_1$

$C_0 = H(A_0)$

Step 1: Apply Garbled Row Reduction

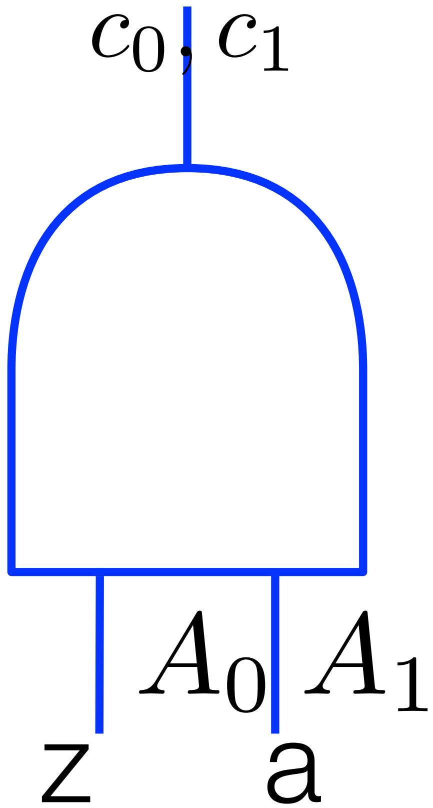
Generator knows z



z=0	z=1
0	0
$H(A_1) \oplus H(A_0)$	$H(A_1) \oplus C_1$
$C_0 = H(A_0)$	

Step 1: Apply Garbled Row Reduction

Generator knows z



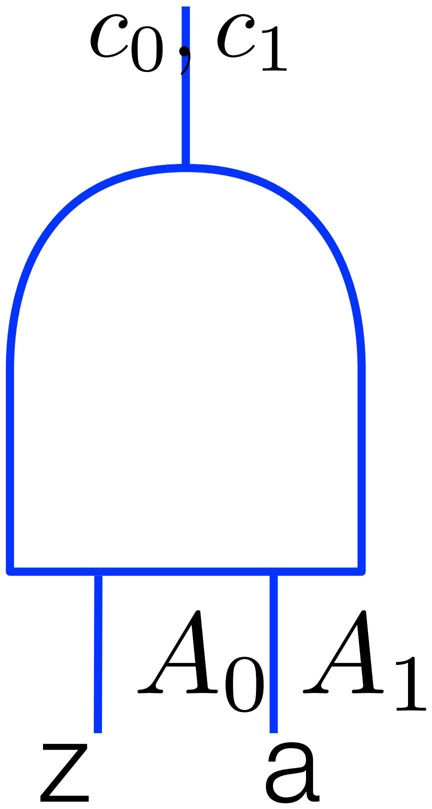
z=0	z=1
0	0
$H(A_1) \oplus H(A_0)$	$H(A_1) \oplus C_1$

$$C_0 = H(A_0)$$

$$C_1 = C_0 + R$$

Step 2: Free XOR

Generator knows z



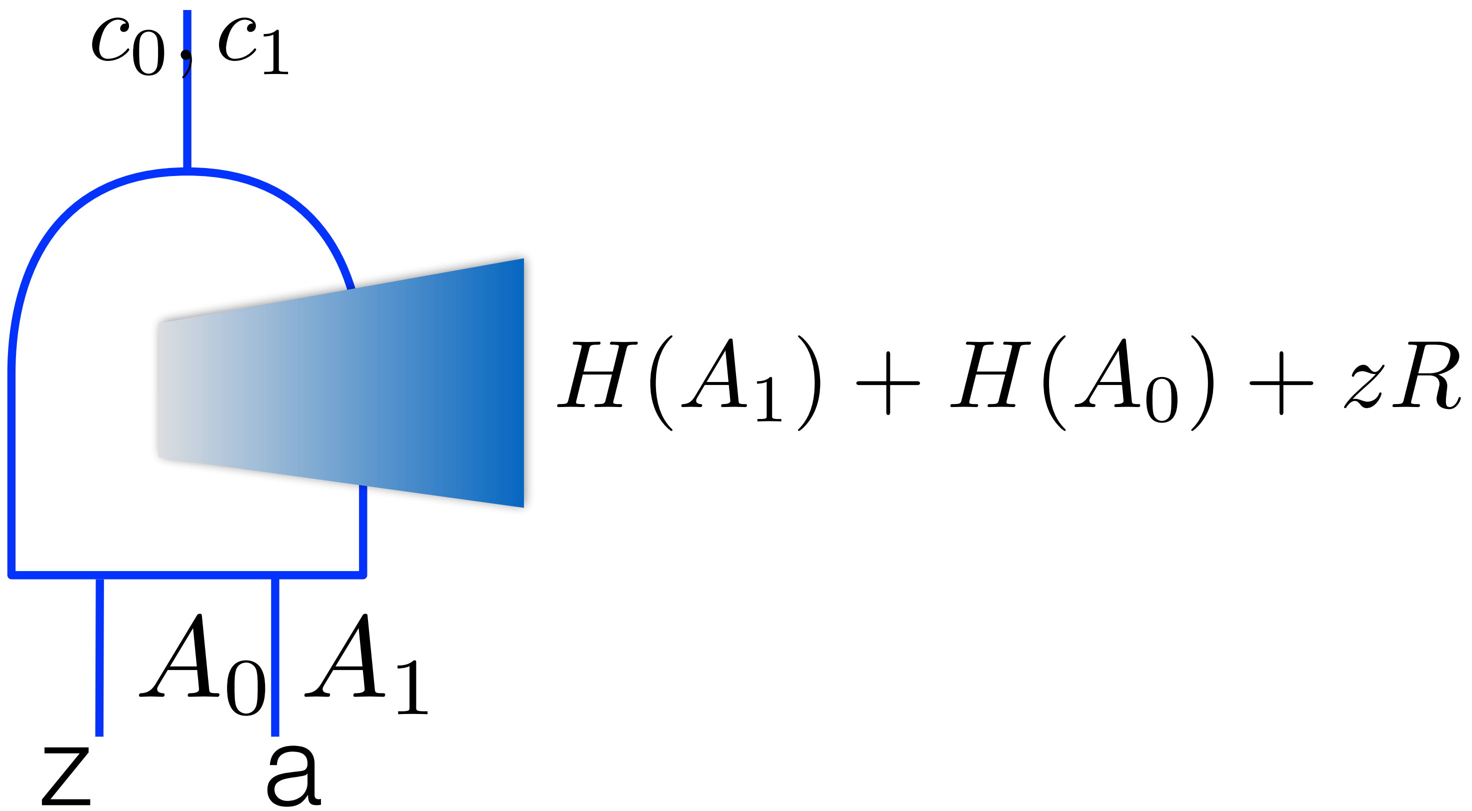
z=0	z=1
0	0
$H(A_1) \oplus H(A_0)$	$H(A_1) + H(A_0) + R$

$$C_0 = H(A_0)$$

$$C_1 = C_0 + R$$

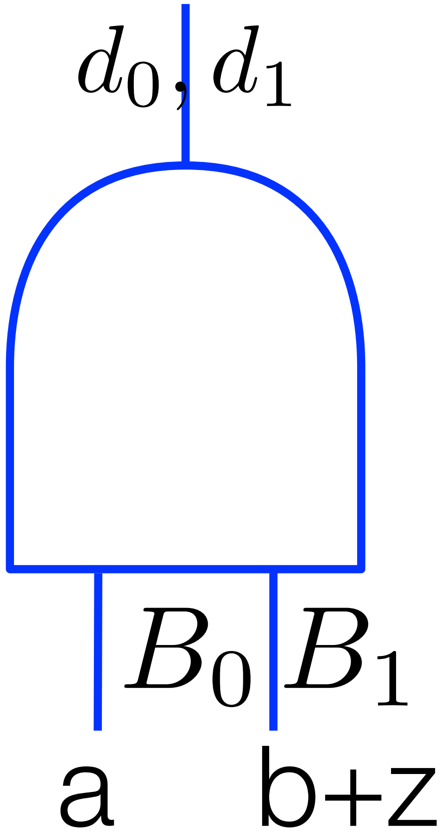
Step 2: Free XOR

Generator knows z

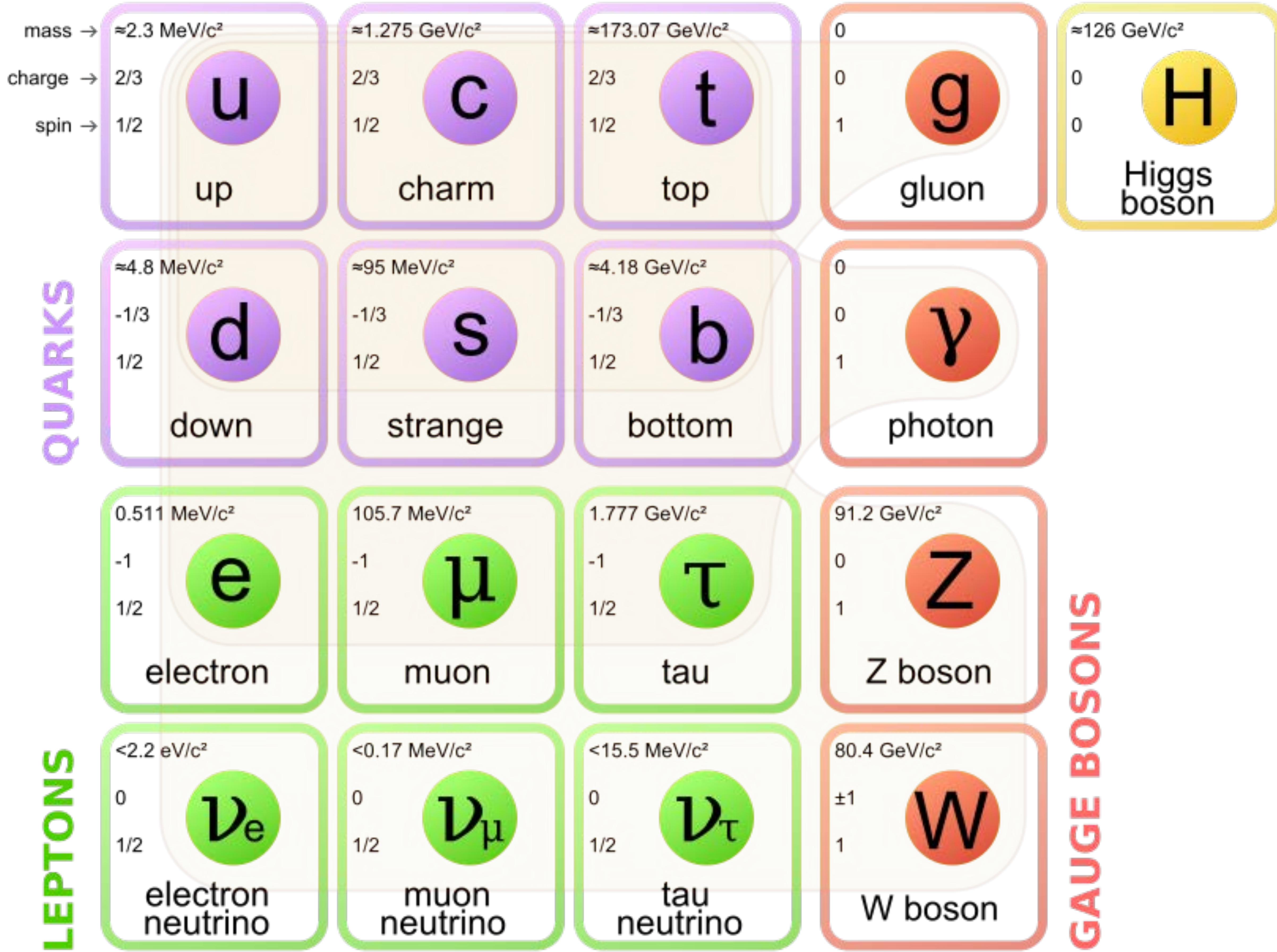


Step 2: Free XOR

Evaluator knows b+z



b+z=0	b+z=1
$H(A_0)+D_0$	$H(A_0)+D_0$
$H(A_1)+D_0$	$H(A_1)+D_1$



mass →
charge →
spin →
≈2.3 MeV/c²
2/3
1/2
u
up
≈1.275 GeV/c²
2/3
1/2
c
charm
≈173.07 GeV/c²
2/3
1/2
t
top
0
0
1
g
gluon
≈126 GeV/c²
0
0
H
Higgs boson
≈4.8 MeV/c²
-1/3
1/2
d
down
≈95 MeV/c²
-1/3
1/2
s
strange
≈4.18 GeV/c²
-1/3
1/2
b
bottom
0
0
1
γ
photon
QUARKS
0.511 MeV/c²
-1
1/2
e
electron
105.7 MeV/c²
-1
1/2
μ
muon
1.777 GeV/c²
-1
1/2
τ
tau
91.2 GeV/c²
0
1
Z
Z boson
<2.2 eV/c²
0
1/2
νe
electron neutrino
<0.17 MeV/c²
0
1/2
νμ
muon neutrino
<15.5 MeV/c²
0
1/2
ντ
tau neutrino
80.4 GeV/c²
±1
1
W
W boson
LEPTONS
GAUGE BOSONS

Work in progress

Malkin-Pastro-shelat

$$
\begin{array}{c}
\text{Input A} \\ \\ \text{Input B} \\ \\ \\ \\
\end{array}
\begin{bmatrix}
1 & 0 & a & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1-a & 0 & a & 0 \\
\hline
0 & 1 & b & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1-b & 0 & b \\
\hline
0 & 0 & p_b & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 1
\end{bmatrix}
\begin{bmatrix}
A \\ B \\ R \\ H(A) \\ H(B) \\ H(A+R) \\ H(B+R)
\end{bmatrix}
$$

Garbled gate

$$\left[\begin{array}{ccccccc} 1 & 0 & a & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1-a & 0 & a & 0 \\ \hline 0 & 1 & b & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1-b & 0 & b \\ \hline 0 & 0 & p_b & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right] \left[\begin{array}{c} A \\ B \\ R \\ H(A) \\ H(B) \\ H(A+R) \\ H(B+R) \end{array}\right]$$

Input A

Input B $=$

$$\left[\begin{array}{c} A + aR \\ aH(A) + (1+a)H(A+R) \\ \hline B + bR \\ bH(B) + (1+a)H(B+R) \\ \hline H(A) + H(A+R) + p_b R \\ A + H(B) + H(B+R) \end{array}\right]$$

Garbled gate

$$
\left[\begin{array}{ccccccc}
1 & 0 & a & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1-a & 0 & a & 0 \\
\hline
0 & 1 & b & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1-b & 0 & b \\
\hline
0 & 0 & p_b & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 \\
\end{array}\right]
\left[\begin{array}{c}
A \\
B \\
R \\
H(A) \\
H(B) \\
H(A+R) \\
H(B+R)
\end{array}\right]
$$

$$
= \left[\begin{array}{c}
A + aR \\
aH(A) + (1+a)H(A+R) \\
\hline
B + bR \\
bH(B) + (1+a)H(B+R) \\
\hline
H(A) + H(A+R) + p_b R \\
A + H(B) + H(B+R)
\end{array}\right]
\left[\begin{array}{c}
v_b \\
1 \\
0 \\
1 \\
v_a \\
v_b
\end{array}\right]^T
$$

This is what the evaluator does to the gate.

$$
\left[\begin{array}{ccccccc}
1 & 0 & a & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1-a & 0 & a & 0 \\
\hline
0 & 1 & b & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1-b & 0 & b \\
\hline
0 & 0 & p_b & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 \\
 & & & & & &
\end{array}\right]
\left[\begin{array}{c}
A \\ B \\ R \\ H(A) \\ H(B) \\ H(A+R) \\ H(B+R)
\end{array}\right]
$$

$$
= \left[\begin{array}{c}
A + aR \\
aH(A) + (1+a)H(A+R) \\
\hline
B + bR \\
bH(B) + (1+a)H(B+R) \\
\hline
H(A) + H(A+R) + p_b R \\
A + H(B) + H(B+R)
\end{array}\right]
\left[\begin{array}{c}
v_b \\ 1 \\ 0 \\ 1 \\ v_a \\ v_b \\ \\
\end{array}\right]^T
=
\begin{array}{l}
(v_b + v_b)(A)+ \\
0 \cdot B+ \\
(v_b a + v_a p_b)R+ \\
(1 + a + v_a)H(A) \\
(1 - b + v_b)H(B)+ \\
(a + v_a)H(A+R)+ \\
(b + v_b)H(B+R)
\end{array}
$$

$$
\left[\begin{array}{ccccccc}
1 & 0 & a & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1-a & 0 & a & 0 \\
\hline
0 & 1 & b & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1-b & 0 & b \\
\hline
0 & 0 & p_b & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 1
\end{array}\right]
\left[\begin{array}{c}
A \\ B \\ R \\ H(A) \\ H(B) \\ H(A+R) \\ H(B+R)
\end{array}\right]
$$

$$
= \left[\begin{array}{c}
A + aR \\
aH(A) + (1+a)H(A+R) \\
\hline
B + bR \\
bH(B) + (1+a)H(B+R) \\
\hline
H(A) + H(A+R) + p_b R \\
A + H(B) + H(B+R)
\end{array}\right]
\left[\begin{array}{c}
v_b \\ 1 \\ 0 \\ 1 \\ v_a \\ v_b
\end{array}\right]^T
=
\left[\begin{array}{c}
0 \\ 0 \\ (ab + p_a p_b)R \\ (1+p_a)H(A) \\ (1+p_b)H(B) \\ p_a H(A+R) \\ p_b H(B+R)
\end{array}\right]
$$

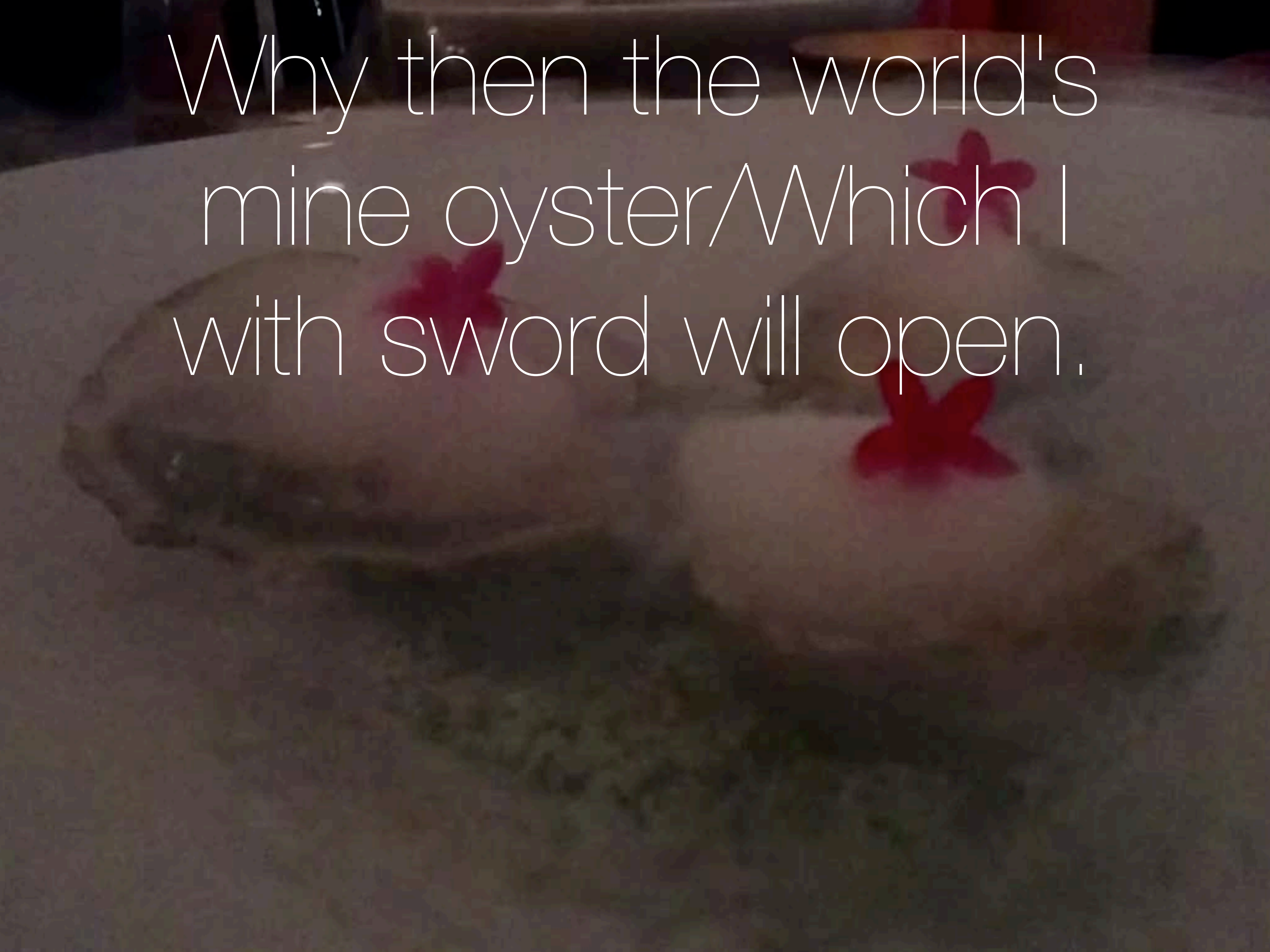
e.g. when $p_a = p_b = 0$, $C_0 = H(A) + H(B)$, $C_1 = C_0 + R$

Why would this scheme be secure?

$$
\left[\begin{array}{ccccccc}
1 & 0 & a & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1-a & 0 & a & 0 \\
\hline
0 & 1 & b & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1-b & 0 & b \\
\hline
0 & 0 & p_b & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 \\
 & & & & & &
\end{array}\right]
\left[\begin{array}{c}
A \\ B \\ R \\ H(A) \\ H(B) \\ H(A+R) \\ H(B+R)
\end{array}\right]
$$

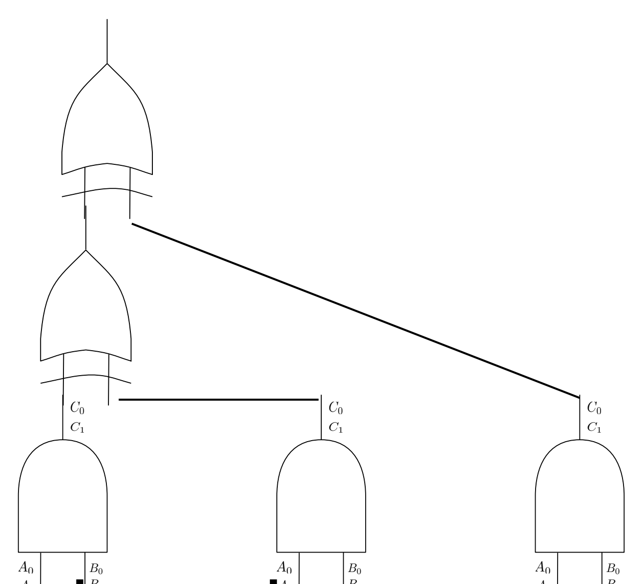
Step 1: Crypto argument about H.

Step 2: Rank argument about matrix.


Why then the world's mine oyster/Which I with sword will open.

Sum of quadratic terms

$$
\begin{bmatrix} v_b \\ 1 \\ v_c \\ 1 \\ v_a \\ 0 \\ v_a \\ v_b \\ v_c \end{bmatrix}
\left[\begin{array}{cccccccccc}
1 & 0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1+a & 0 & 0 & a & 0 & 0 \\
\hline
0 & 1 & 0 & b & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1+b & 0 & 0 & b & 0 \\
\hline
0 & 0 & 1 & c & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1+c & 0 & 0 & c \\
\hline
0 & 0 & 1 & p_b & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & p_c & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & p_a & 0 & 0 & 1 & 0 & 0 & 1
\end{array}\right]
\begin{bmatrix} A \\ B \\ C \\ R \\ H(A) \\ H(B) \\ H(C) \\ H(A+R) \\ H(B+R) \\ H(C+R) \end{bmatrix}
$$



ab + bc + ac

Generalized 1/2-gate garbling

Thm: Any quadratic polynomial in n-variables can be garbled using n ciphertexts.

(nk bits)

Sum of quadratic terms

$$
\begin{bmatrix} v_b \\ 1 \\ v_c \\ 1 \\ v_a \\ 0 \\ v_a \\ v_b \\ v_c \end{bmatrix}
\left[\begin{array}{cccccccccc}
1 & 0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1+a & 0 & 0 & a & 0 & 0 \\
\hline
0 & 1 & 0 & b & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1+b & 0 & 0 & b & 0 \\
\hline
0 & 0 & 1 & c & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1+c & 0 & 0 & c \\
\hline
0 & 0 & 1 & p_b & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & p_c & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & p_a & 0 & 0 & 1 & 0 & 0 & 1
\end{array}\right]
\begin{bmatrix} A \\ B \\ C \\ R \\ H(A) \\ H(B) \\ H(C) \\ H(A+R) \\ H(B+R) \\ H(C+R) \end{bmatrix}
$$

ab + bc + ac

Generalized 1/2-gate garbling

Thm: Any quadratic polynomial in n-variables can be garbled using n ciphertexts and non-adaptive H queries.

$$
\begin{bmatrix} v_b v_c \\ 1 \\ v_b \\ v_a v_c \\ 1 \\ v_c \\ v_a v_b \\ 1 \\ v_a \\ v_a \\ v_b \\ v_c \\ v_b v_c \\ v_a v_c \\ v_a v_b \\ \\ \end{bmatrix}
\left[\begin{array}{cccccccccccccccc}
1 & 0 & 0 & A & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \overline{A} & 0 & 0 & A & 0 & 0 & & & & & & \\
 & & & & & & & & & & \overline{A} & 0 & 0 & A & 0 & 0 \\
\hline
0 & 1 & 0 & B & 0 & 0 & 0 & 0 & 0 & 0 & & & & & & \\
0 & 0 & 0 & 0 & 0 & \overline{B} & 0 & 0 & B & 0 & & & & & & \\
 & & & & & & & & & & 0 & \overline{B} & 0 & 0 & B & 0 \\
\hline
0 & 0 & 1 & C & 0 & 0 & 0 & 0 & 0 & 0 & & & & & & \\
0 & 0 & 0 & 0 & 0 & 0 & \overline{C} & 0 & 0 & C & & & & & & \\
 & & & & & & & & & & 0 & 0 & \overline{C} & 0 & 0 & C \\
\hline
0 & 0 & 0 & p_b p_c & 1 & 0 & 0 & 1 & 0 & 0 & & & 1+p_c & & & p_c \\
0 & 0 & 0 & p_a p_c & 0 & 1 & 0 & 0 & 1 & 0 & 1+p_a & & p_a & & & \\
0 & 0 & 0 & p_a p_b & 0 & 0 & 1 & 0 & 0 & 1 & & 1+p_b & & & p_b & \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & 1 & & & 1 & \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & & 1 & & & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & & & 1 & & \\
\hline
A & B & C & R & h(A) & & & hA' & & & gA & & & g\overline{A} & &
\end{array}\right]
\begin{bmatrix} A \\ B \\ C \\ R \\ H(A) \\ H(B) \\ H(C) \\ H(A+R) \\ H(B+R) \\ H(C+R) \\ G(A) \\ G(B) \\ G(C) \\ G(A+R) \\ G(B+R) \\ G(C+R) \end{bmatrix}
$$

$$
\begin{aligned}
(p_b + b)(p_c + c)a &= abc + abp_c + acp_b + ap_b p_c \\
(p_a + a)(p_c + c)b &= abc + abp_c + bcp_a + bp_a p_c \\
(p_a + a)(p_b + b)c &= abc + acp_b + bcp_a + cp_b p_c \\
v_a p_b p_c &= ap_b p_c + p_a p_b p_c \\
v_b p_a p_c &= bp_a p_c + p_a p_b p_c \\
v_c p_a p_b &= cp_a p_b + p_a p_b p_c
\end{aligned}
$$

$$
\begin{bmatrix} v_b v_c \\ 1 \\ v_b \\ v_a v_c \\ 1 \\ v_c \\ v_a v_b \\ 1 \\ v_a \\ v_a \\ v_b \\ v_c \\ v_b v_c \\ v_a v_c \\ v_a v_b \\ \end{bmatrix}
\left[\begin{array}{cccccccccccccccc}
1 & 0 & 0 & A & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \overline{A} & 0 & 0 & A & 0 & 0 & & & & & & \\
 & & & & & & & & & & \overline{A} & 0 & 0 & A & 0 & 0 \\
\hline
0 & 1 & 0 & B & 0 & 0 & 0 & 0 & 0 & 0 & & & & & & \\
0 & 0 & 0 & 0 & 0 & \overline{B} & 0 & 0 & B & 0 & & & & & & \\
 & & & & & & & & & & 0 & \overline{B} & 0 & 0 & B & 0 \\
\hline
0 & 0 & 1 & C & 0 & 0 & 0 & 0 & 0 & 0 & & & & & & \\
0 & 0 & 0 & 0 & 0 & 0 & \overline{C} & 0 & 0 & C & & & & & & \\
 & & & & & & & & & & 0 & 0 & \overline{C} & 0 & 0 & C \\
\hline
0 & 0 & 0 & p_b p_c & 1 & 0 & 0 & 1 & 0 & 0 & & & 1+p_c & & & p_c \\
0 & 0 & 0 & p_a p_c & 0 & 1 & 0 & 0 & 1 & 0 & 1+p_a & & p_a & & & \\
0 & 0 & 0 & p_a p_b & 0 & 0 & 1 & 0 & 0 & 1 & & 1+p_b & & & p_b & \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & 1 & & & 1 & \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & & 1 & & & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & & & 1 & & \\
\hline
A & B & C & R & h(A) & & & hA' & & & gA & & & g\overline{A} & &
\end{array}\right]
\begin{bmatrix} A \\ B \\ C \\ R \\ H(A) \\ H(B) \\ H(C) \\ H(A+R) \\ H(B+R) \\ H(C+R) \\ G(A) \\ G(B) \\ G(C) \\ G(A+R) \\ G(B+R) \\ G(C+R) \end{bmatrix}
$$

$$(p_b+b)(p_c+c)a = abc + abp_c + acp_b + ap_bp_c$$
$$(p_a+a)(p_c+c)b = abc + abp_c + bcp_a + bp_ap_c$$
$$(p_a+a)(p_b+b)c = abc + acp_b + bcp_a + cp_bp_c$$
$$v_ap_bp_c = ap_bp_c + p_ap_bp_c$$
$$v_bp_ap_c = bp_ap_c + p_ap_bp_c$$
$$v_cp_ap_b = cp_ap_b + p_ap_bp_c$$

Generalized 1/2-gate garbling

Thm: Any degree-k polynomial in n-variables can be garbled using $\sum_{i=0}^{k-1} \binom{n}{i}$ ciphertexts

and non-adaptive H queries.

…versus 2^n previously

Wins on adaptivity

May win on size

$$
\begin{array}{cl}
\left(\begin{array}{ccccccccccccccccccccccccccccc}
1 & 0 & 0 & 0 & x_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & x_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & x_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & x_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & a_2a_3 + a_3a_4 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \neg a_2 & \neg a_2 & a_2 & a_2 & \neg a_3 & \neg a_3 & a_3 & a_4 & \neg a_1 & a_4 & \neg a_4 & a_4 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & a_1a_3 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & \neg a_1 & a_1 & \neg a_1 & a_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \neg a_3 & \neg a_3 & a_3 & a_3 \\
0 & 0 & 0 & 0 & a_1a_2 + a_1a_4 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \neg a_1 & a_1 & \neg a_1 & a_1 & 0 & 0 & 0 & 0 & \neg a_2 & a_2 & \neg a_2 & a_2 \\
0 & 0 & 0 & 0 & a_1a_3 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \neg a_1 & a_1 & \neg a_1 & a_1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \neg x_1 & x_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \neg x_2 & x_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \neg x_3 & x_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \neg x_4 & x_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \neg x_1 \neg x_2 & \neg x_1 x_2 & x_1 \neg x_2 & x_1 x_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \neg x_1 \neg x_3 & \neg x_1 x_3 & x_1 \neg x_3 & x_1 x_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \neg x_1 \neg x_4 & \neg x_1 x_4 & x_1 \neg x_4 & x_1 x_4 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \neg x_2 \neg x_3 & \neg x_2 x_3 & x_2 \neg x_3 & x_2 x_3 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right) \cdots
&
\begin{array}{l}
\leftarrow \text{Wire } 1 \\
\leftarrow \text{Wire } 2 \\
\leftarrow \text{Wire } 3 \\
\leftarrow \text{Wire } 4 \\
\leftarrow S = \{1\} \\
\leftarrow S = \{2\} \\
\leftarrow S = \{3\} \\
\leftarrow S = \{4\} \\
\leftarrow S = \{1, 2\} \\
\leftarrow S = \{1, 3\} \\
\leftarrow S = \{1, 4\} \\
\leftarrow S = \{2, 3\} \\
\leftarrow S = \{2, 4\} \\
\leftarrow S = \{3, 4\} \\
\\
\\
\\
\\
\\
\\
\\
\\
\\
\\
\end{array}
\end{array}
$$

1st block
2nd block

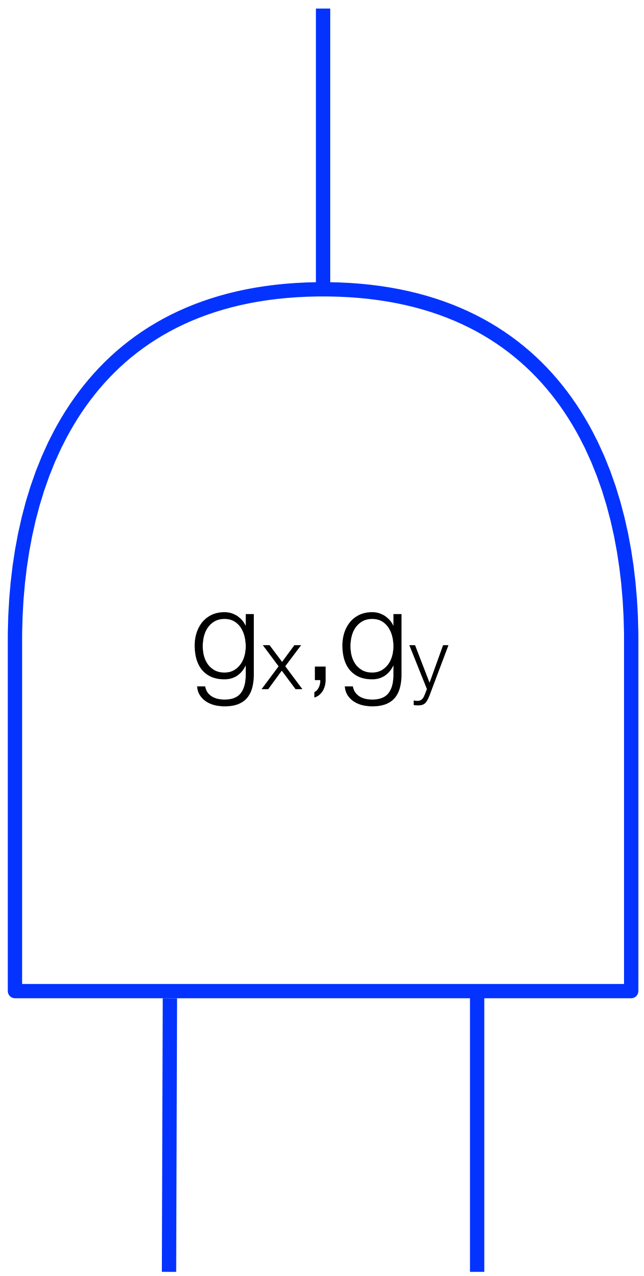
Fig. 2. Garbling matrix G_f for $f = x_1 \cdot x_2 \cdot x_3 + x_1 \cdot x_3 \cdot x_4$.

$$
\begin{pmatrix}
\alpha_2\alpha_3+\alpha_3\alpha_4 \\
\alpha_1\alpha_3 \\
\alpha_1\alpha_2+\alpha_1\alpha_4 \\
\alpha_1\alpha_3 \\
\alpha_1 \\
\alpha_2 \\
\alpha_3 \\
\alpha_4 \\
\alpha_1\alpha_2 \\
\alpha_1\alpha_3 \\
\alpha_1\alpha_4 \\
\alpha_2\alpha_3 \\
\alpha_2\alpha_4 \\
\alpha_3\alpha_4 \\
1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1
\end{pmatrix}^T
\left(\begin{array}{ccccccccccccccccccccccccccccc}
1 & 0 & 0 & 0 & x_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & x_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & x_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & x_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & a_2a_3+a_3a_4 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \neg a_2 & \neg a_2 & a_2 & a_2 & \neg a_3 & \neg a_3 & a_3 & a_4 & \neg a_1 & a_4 & \neg a_4 & a_4 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & a_1a_3 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & \neg a_1 & a_1 & \neg a_1 & a_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \neg a_3 & \neg a_3 & a_3 & a_3 \\
0 & 0 & 0 & 0 & a_1a_2+a_1a_4 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \neg a_1 & a_1 & \neg a_1 & a_1 & 0 & 0 & 0 & 0 & \neg a_2 & a_2 & \neg a_2 & a_2 \\
0 & 0 & 0 & 0 & a_1a_3 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \neg a_1 & a_1 & \neg a_1 & a_1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \neg x_1 & x_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \neg x_2 & x_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \neg x_3 & x_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \neg x_4 & x_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \neg x_1\neg x_2 & \neg x_1x_2 & x_1\neg x_2 & x_1x_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \neg x_1\neg x_3 & \neg x_1x_3 & x_1\neg x_3 & x_1x_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \neg x_1\neg x_4 & \neg x_1x_4 & x_1\neg x_4 & x_1x_4 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \neg x_2\neg x_3 & \neg x_2x_3 & x_2\neg x_3 & x_2x_3 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\cdots\right) =
$$

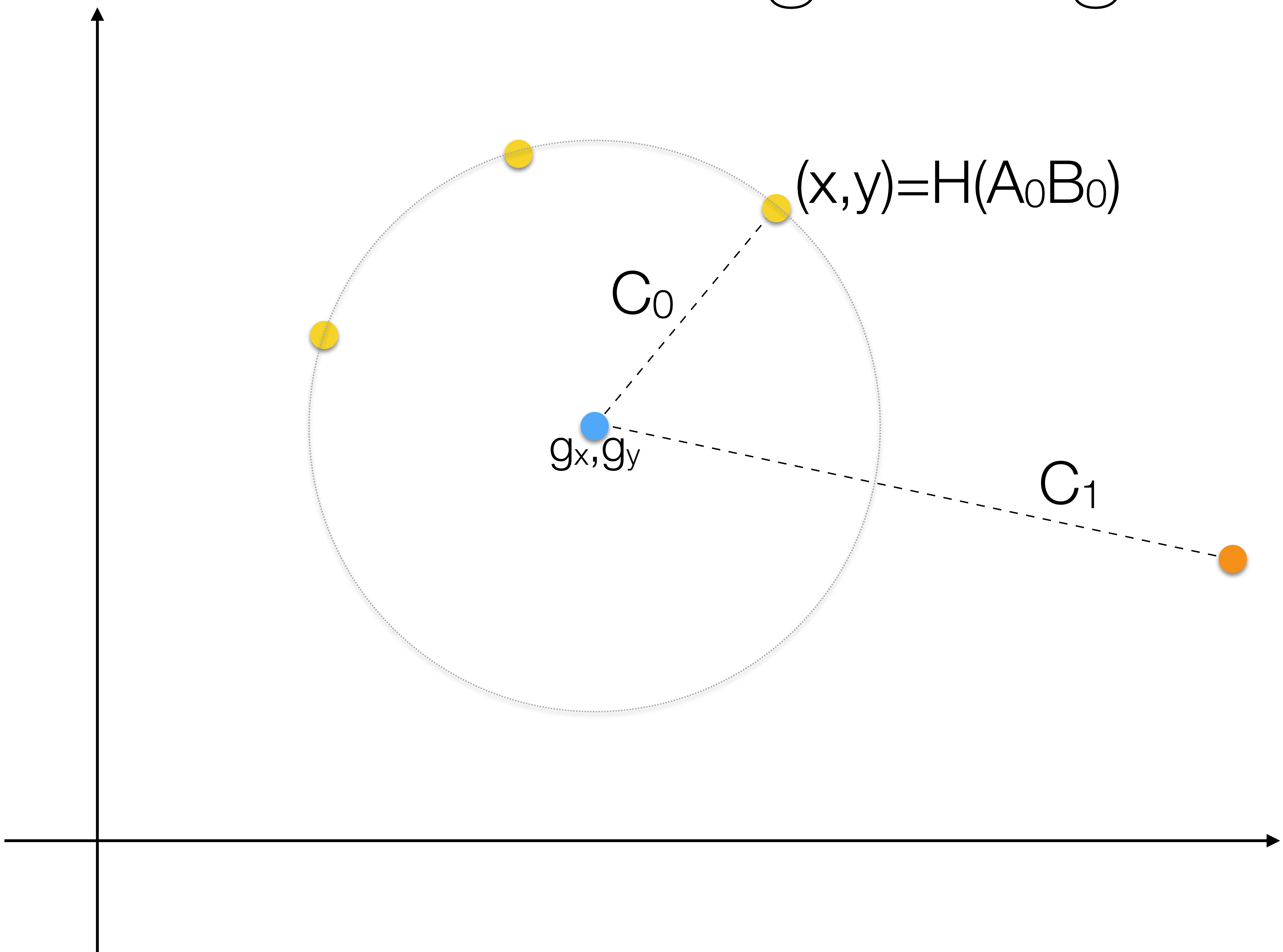
Reductionism fails

Every linear garbling scheme for AND requires 2*k bits. [Zahur-Evans-Rosulek]

Non-linear garbling



Non-linear garbling



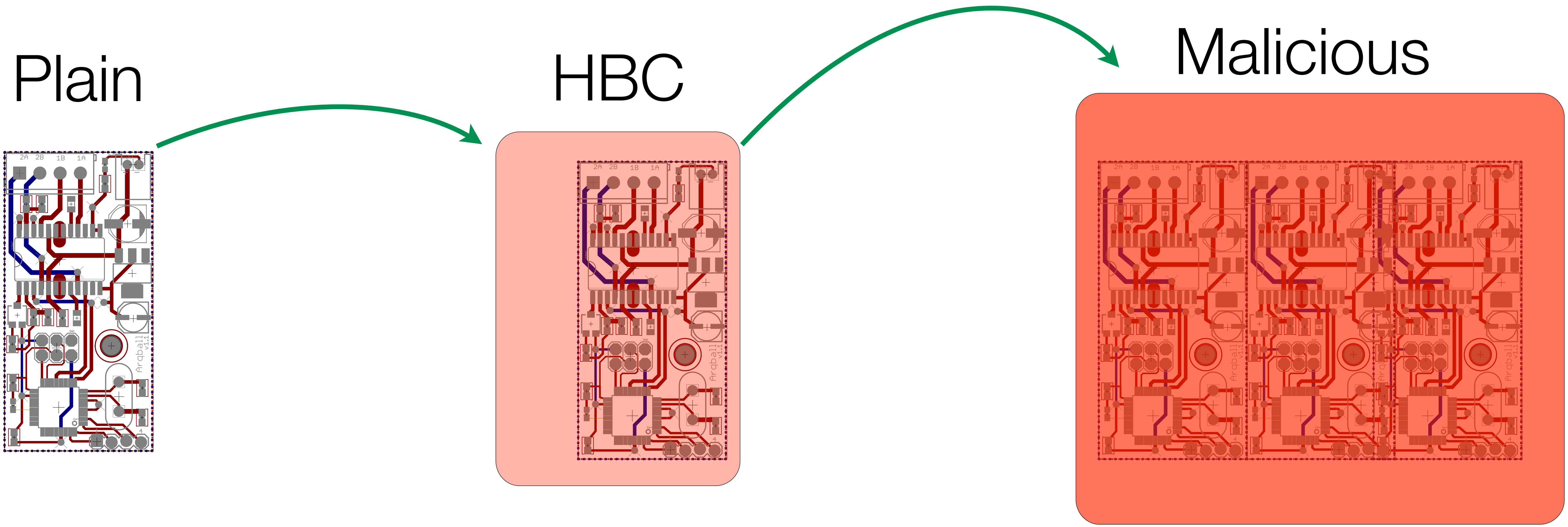
Q: Can non-linear garbling beat linear schemes?

Why study Garbled circuits?

Other protocols

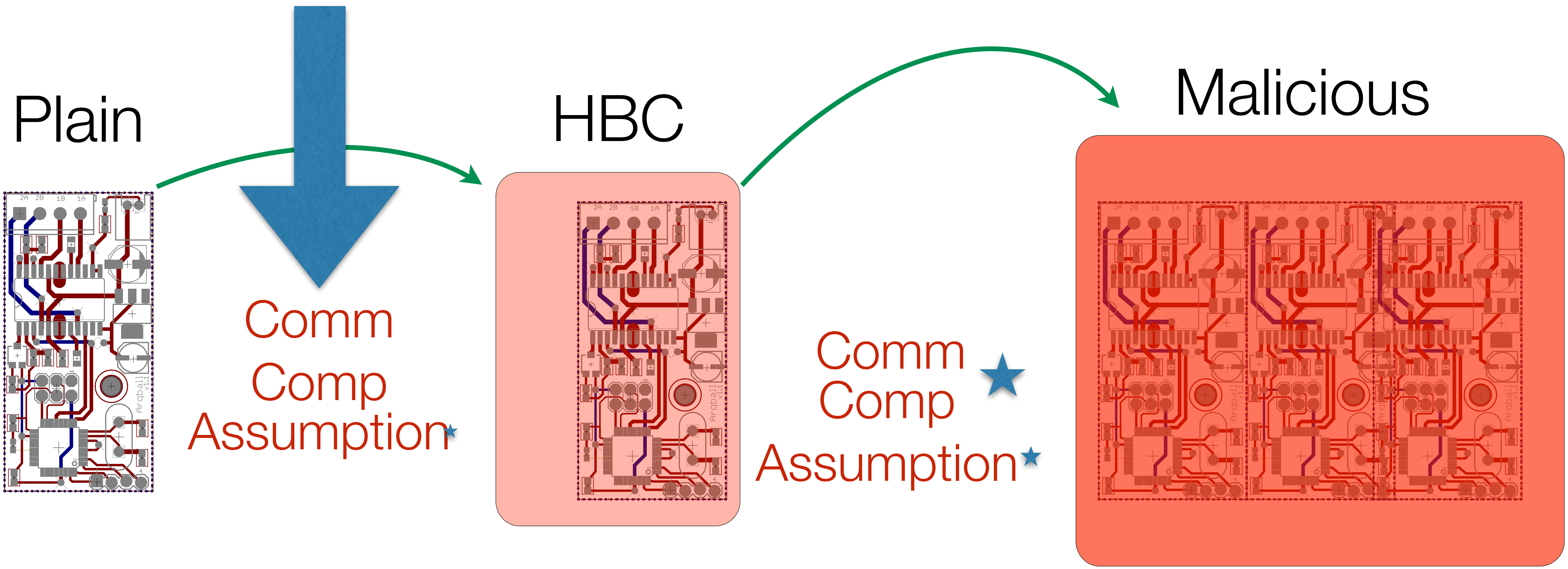
overhead

2-party Secure computation

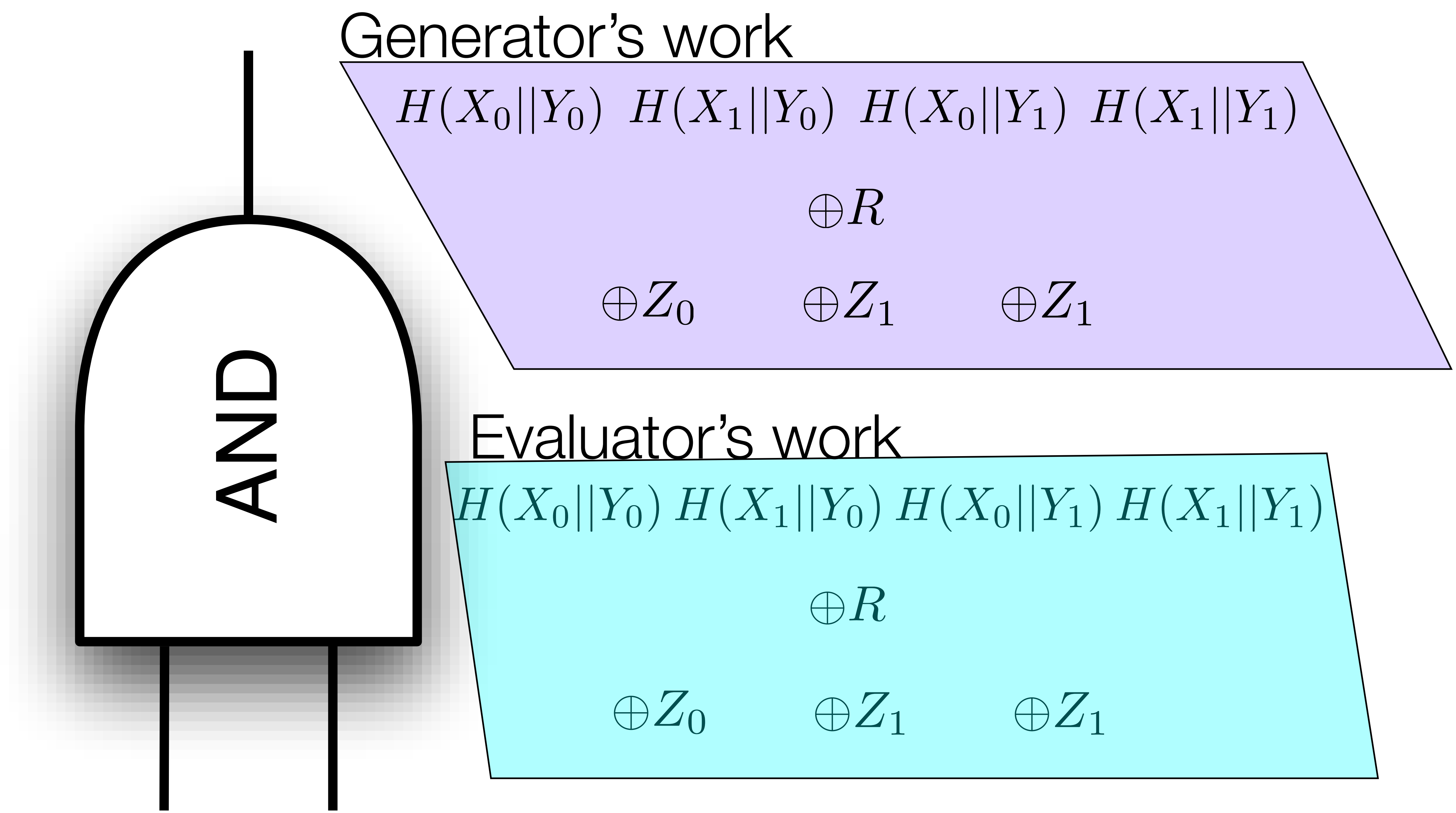


overhead

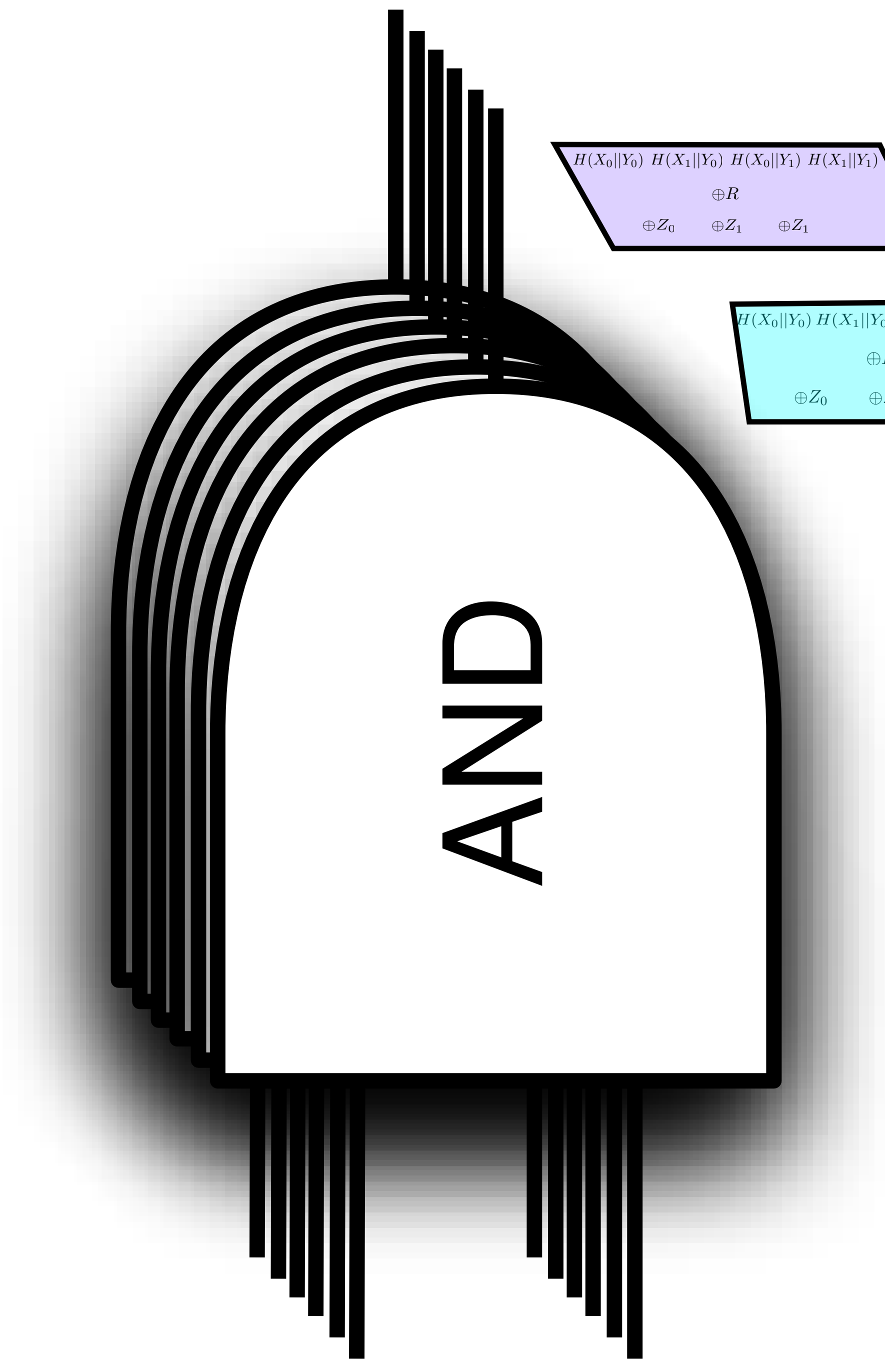
2-party Secure computation

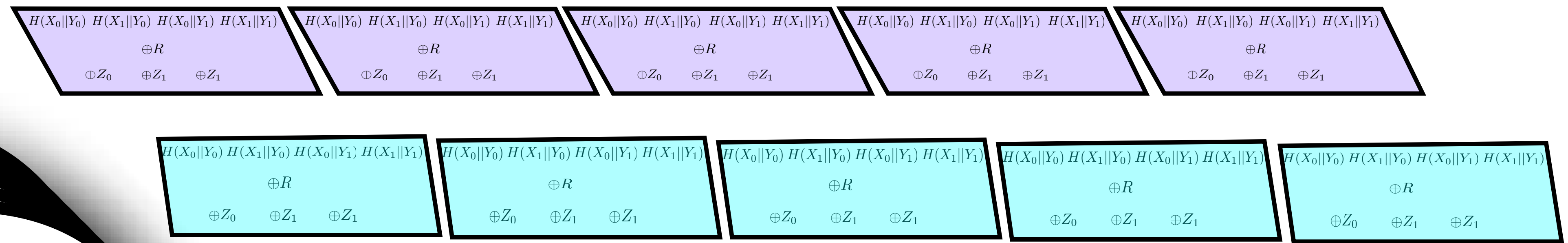


Parallelizability is KEY



AND
Generator's work
$H(X_0||Y_0)$ $H(X_1||Y_0)$ $H(X_0||Y_1)$ $H(X_1||Y_1)$
$\oplus R$
$\oplus Z_0$ $\oplus Z_1$ $\oplus Z_1$
Evaluator's work
$H(X_0||Y_0)$ $H(X_1||Y_0)$ $H(X_0||Y_1)$ $H(X_1||Y_1)$
$\oplus R$
$\oplus Z_0$ $\oplus Z_1$ $\oplus Z_1$





No additional per-gate depth for HBC v Malicious