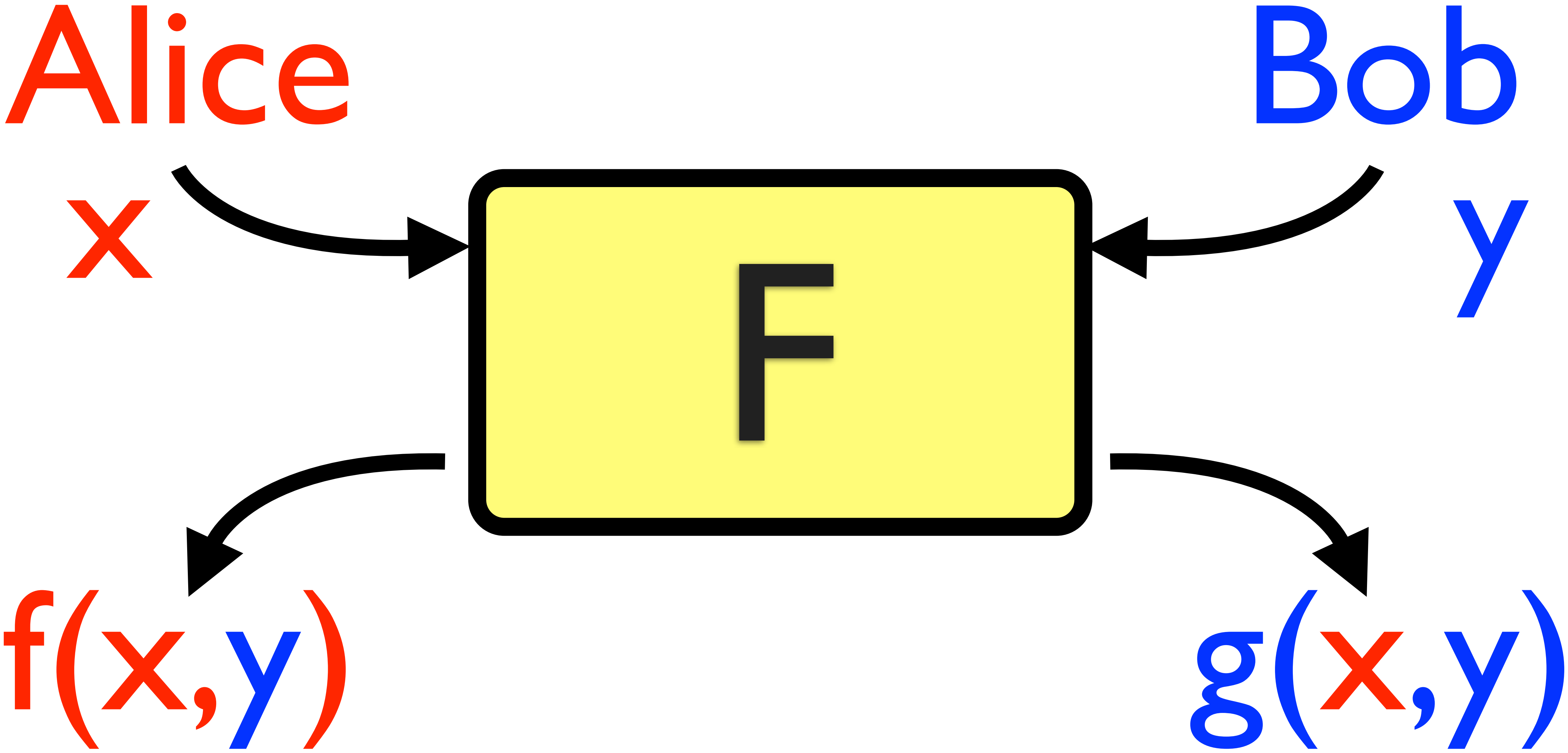
Billion-Gate

Secure Computation with Malicious Adversaries

Ben Kreuter, abhi shelat, and Chih-hao Shen

University of Virginia

Secure 2PC [Yao82]



Alice

x

Bob

y

F

$f(x,y)$

$g(x,y)$

Threat Models

Semi-Honest [Yao82]

Malicious [GMW86]

Our Contributions

- **Very Large Circuits**
- Fastest Semi-Honest System: **~400k gates/sec**
- **KSS Thesis**: Malicious security incurs (**1+ε**) time overhead over Semi-Honest security
- Fastest Malicious System

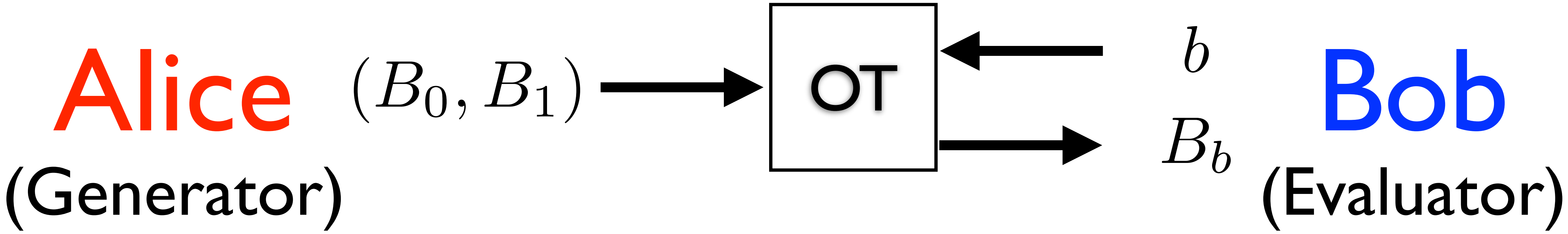
KSS Thesis

In a model with O(k) cores and O(k) bandwidth, the "TIME OVERHEAD" of malicious security over semi-honest security is

$$(1+\varepsilon)$$

k: secure parameter

Yao’s Garbled Circuit



Alice

(Generator)

(B_0, B_1)

OT

b

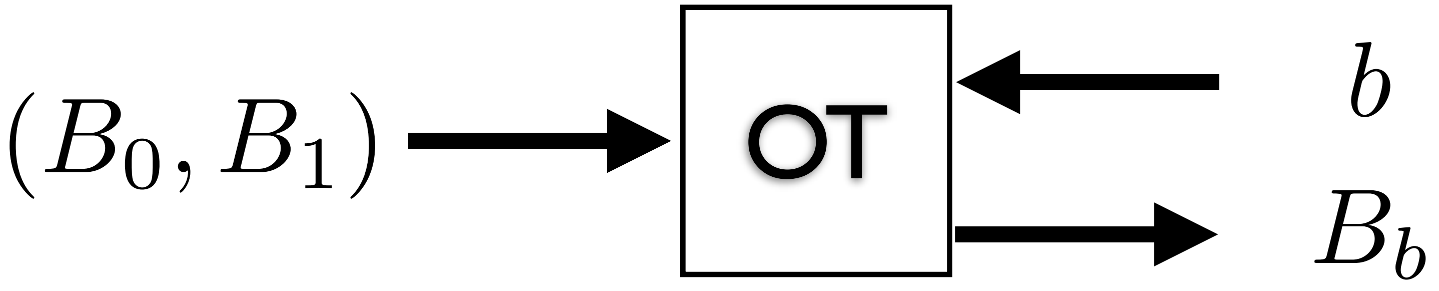
B_b

Bob

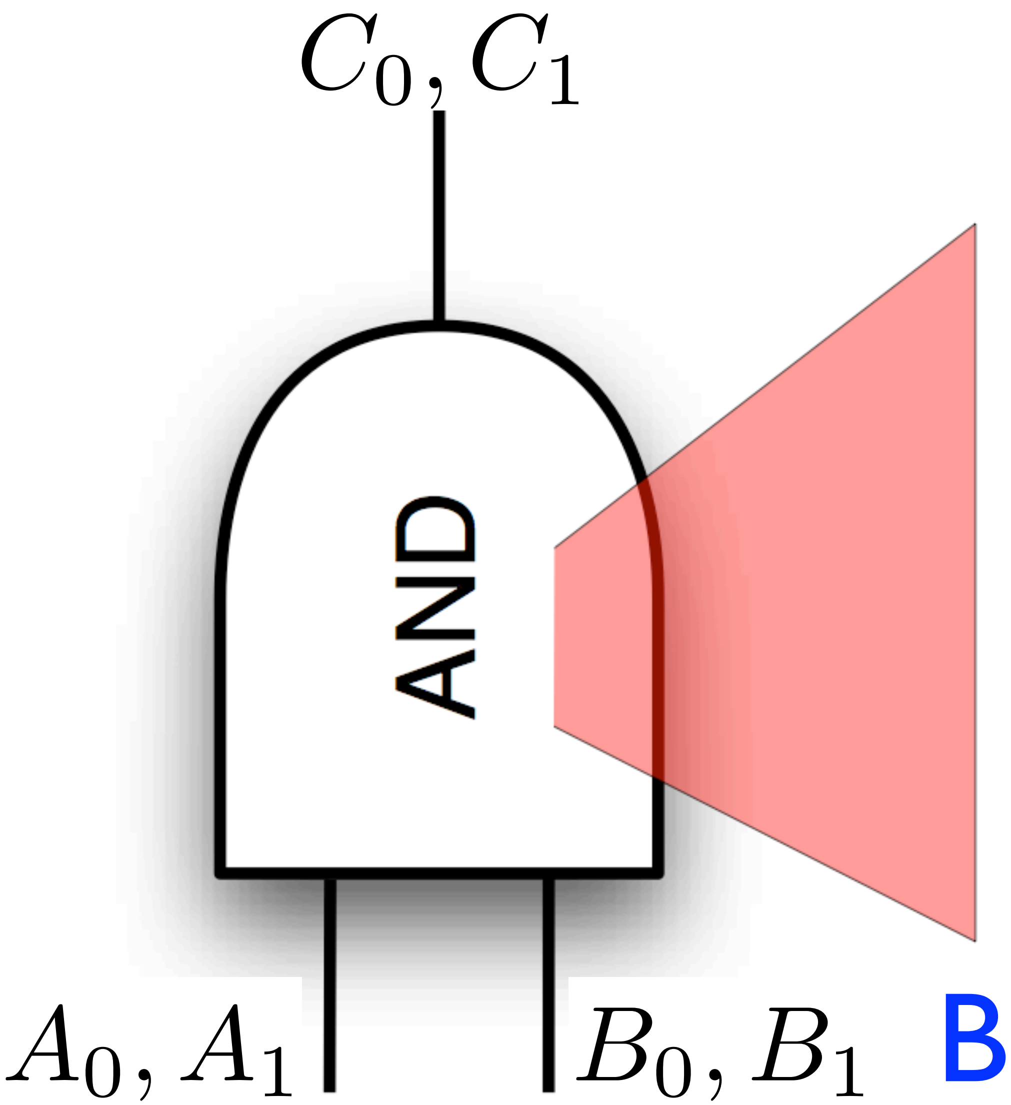
(Evaluator)

Yao's Garbled Circuit

Alice
(Generator)



Bob
(Evaluator)



Alice

Bob

$\mathtt{Enc}_{A_0}(\mathtt{Enc}_{B_1}(C_0))$

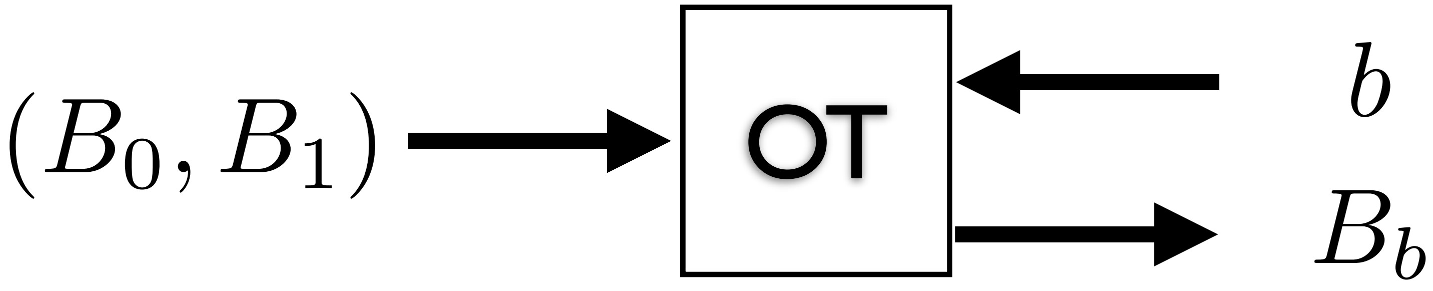
$\mathtt{Enc}_{A_1}(\mathtt{Enc}_{B_1}(C_1))$

$\mathtt{Enc}_{A_0}(\mathtt{Enc}_{B_0}(C_0))$

$\mathtt{Enc}_{A_1}(\mathtt{Enc}_{B_0}(C_0))$

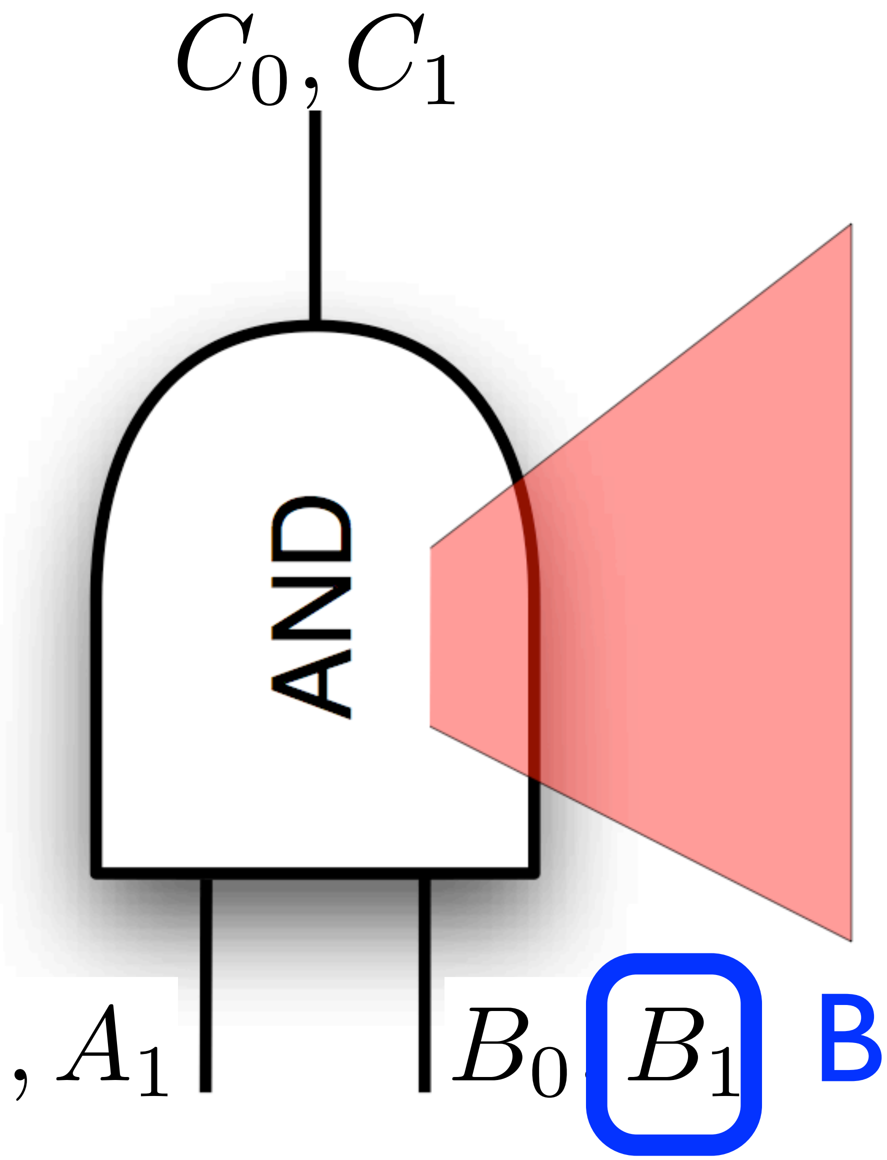
Yao's Garbled Circuit

Alice
(Generator)



Bob
(Evaluator)

Example:



$\mathtt{Enc}_{A_0}(\mathtt{Enc}_{B_1}(C_0))$

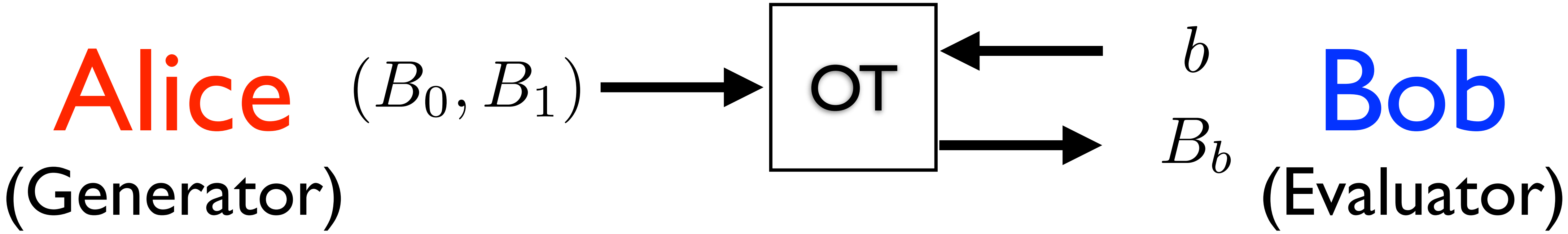
$\mathtt{Enc}_{A_1}(\mathtt{Enc}_{B_1}(C_1))$

$\mathtt{Enc}_{A_0}(\mathtt{Enc}_{B_0}(C_0))$

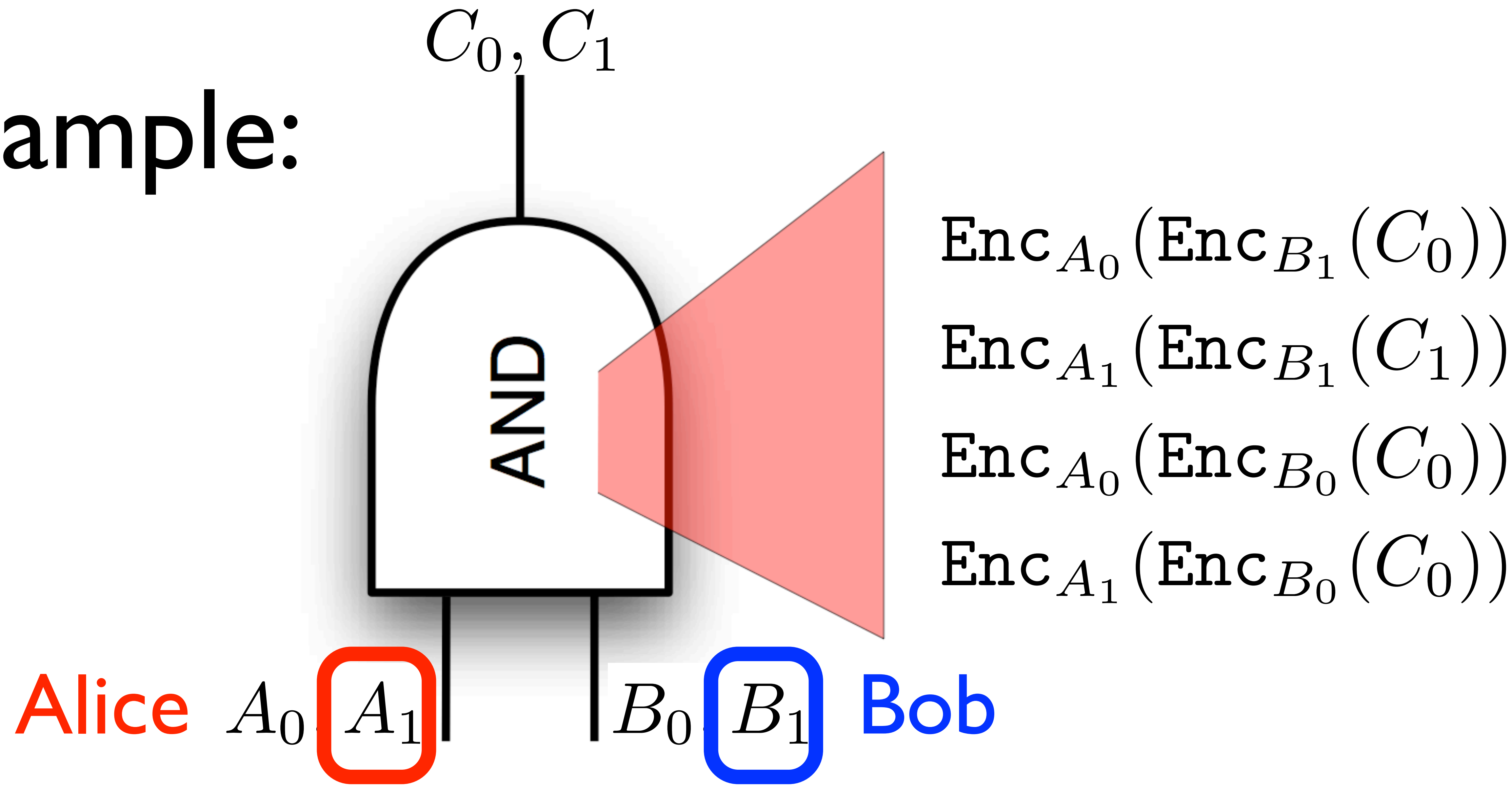
$\mathtt{Enc}_{A_1}(\mathtt{Enc}_{B_0}(C_0))$

Alice A_0, A_1 B_0 $\boxed{B_1}$ Bob

Yao's Garbled Circuit



Example:



$$\texttt{Enc}_{A_0}(\texttt{Enc}_{B_1}(C_0))$$

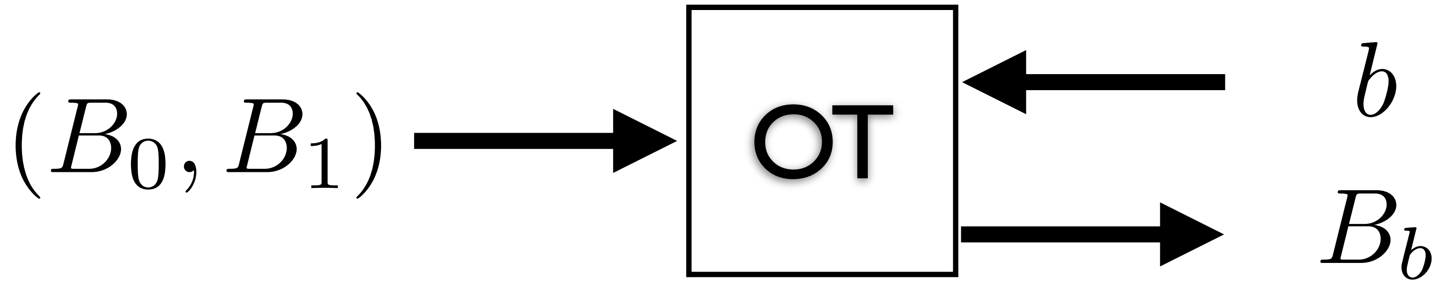
$$\texttt{Enc}_{A_1}(\texttt{Enc}_{B_1}(C_1))$$

$$\texttt{Enc}_{A_0}(\texttt{Enc}_{B_0}(C_0))$$

$$\texttt{Enc}_{A_1}(\texttt{Enc}_{B_0}(C_0))$$

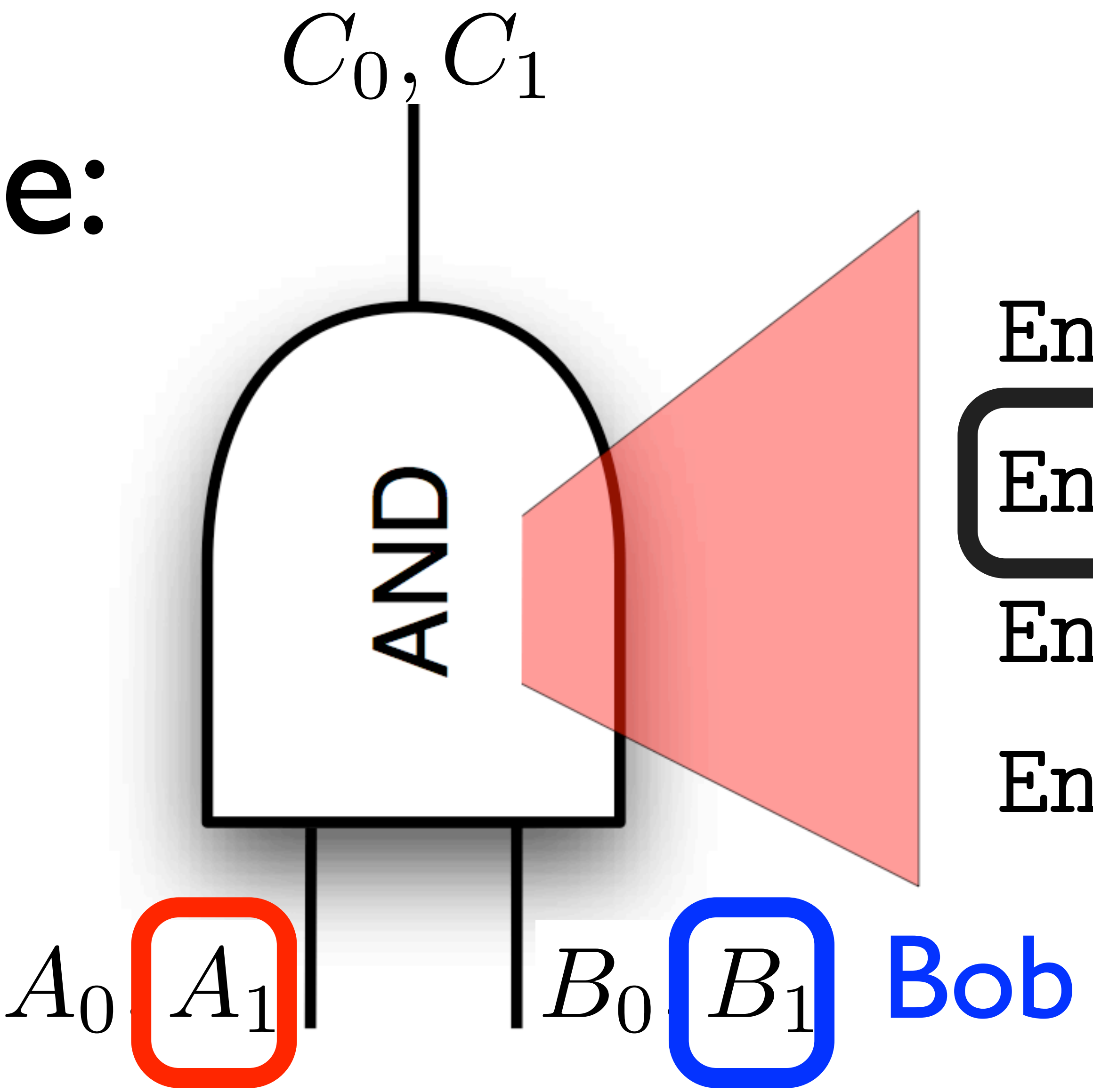
Yao’s Garbled Circuit

Alice
(Generator)



Bob
(Evaluator)

Example:



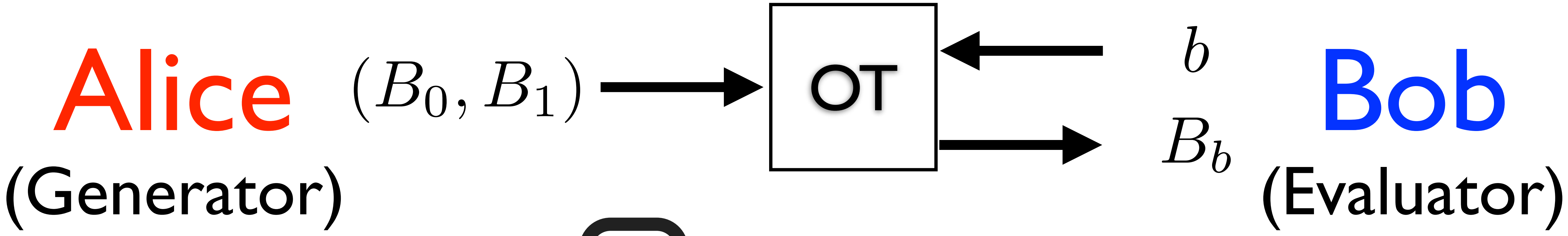
$$\mathtt{Enc}_{A_0}(\mathtt{Enc}_{B_1}(C_0))$$

$$\boxed{\mathtt{Enc}_{A_1}(\mathtt{Enc}_{B_1}(C_1))}$$

$$\mathtt{Enc}_{A_0}(\mathtt{Enc}_{B_0}(C_0))$$

$$\mathtt{Enc}_{A_1}(\mathtt{Enc}_{B_0}(C_0))$$

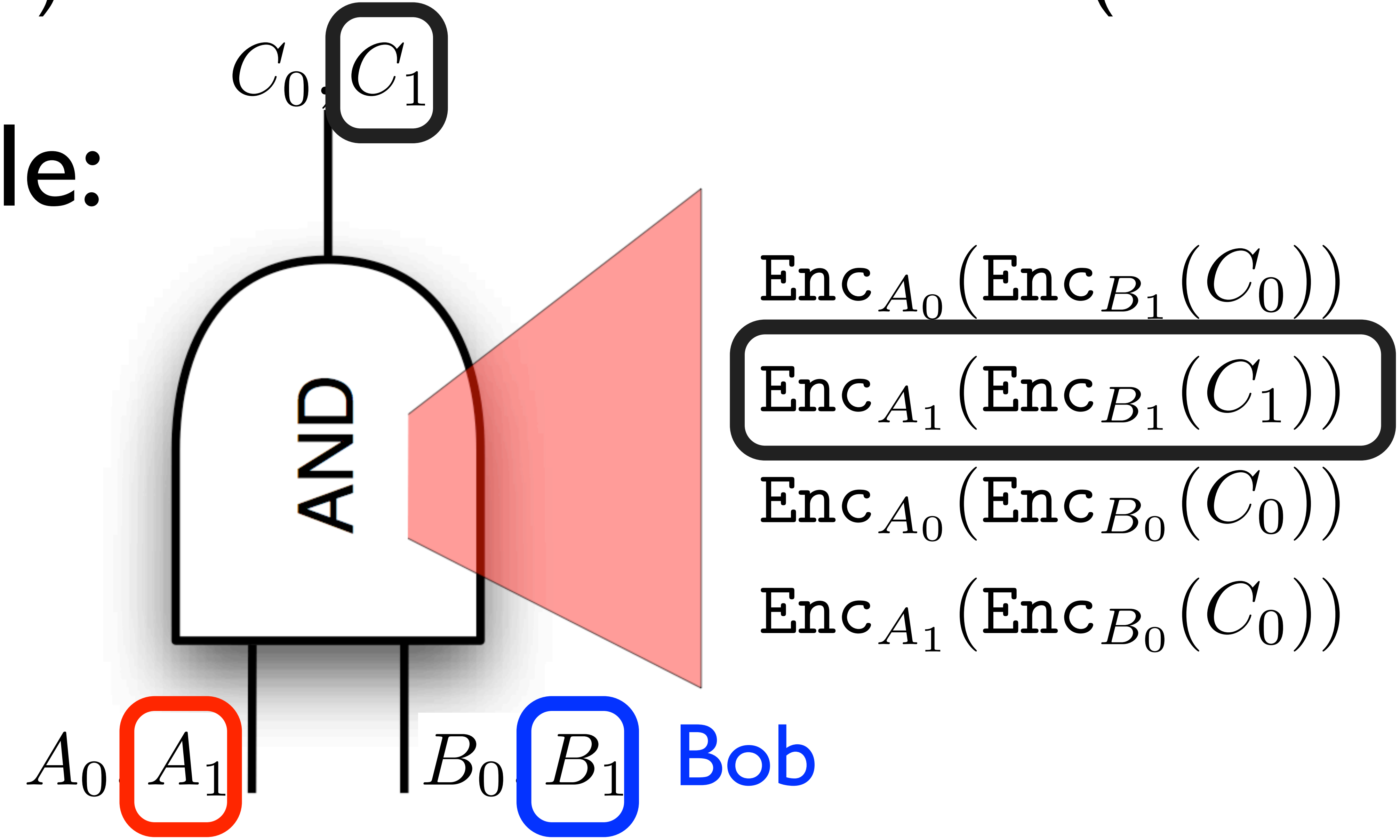
Yao's Garbled Circuit



Alice (B_0, B_1) → OT ← b Bob

(Generator) B_b (Evaluator)

Example:



$C_0, \boxed{C_1}$

$\mathtt{Enc}_{A_0}(\mathtt{Enc}_{B_1}(C_0))$

$\boxed{\mathtt{Enc}_{A_1}(\mathtt{Enc}_{B_1}(C_1))}$

$\mathtt{Enc}_{A_0}(\mathtt{Enc}_{B_0}(C_0))$

$\mathtt{Enc}_{A_1}(\mathtt{Enc}_{B_0}(C_0))$

Alice $A_0, \boxed{A_1}$ $B_0, \boxed{B_1}$ Bob

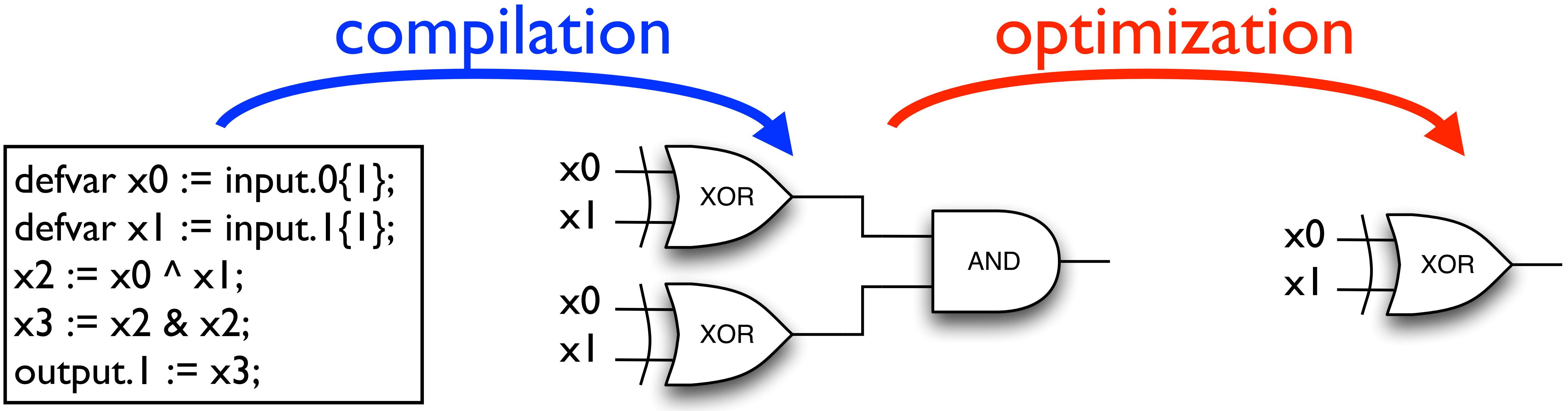
Challenges in Malicious Security

Large Circuits

Fast Protocols

Progress on S2PC over
Big Circuits

[MNPS04]	4k gates	Fairplay compiler [MNPS04]
[LP07, PSSW09]	34k gates	
[SS11]	34k gates	
[NNOB11]	560m gates (34k X 16384)	
[HEKM11]	1.2b gates	Circuit Library [HEKM11]
[This Work]	**5.9b gates**	**Our Compiler**



```
defvar x0 := input.0{1};
defvar x1 := input.1{1};
x2 := x0 ^ x1;
x3 := x2 & x2;
output.1 := x3;
```

Our Compiler

- High-level Programming Language
- Multi-pass
- Local/Global Optimizations
- XOR-favoring

Large Circuits

	size (gates)	Compile Time	
AES-128	5.0×10^4	$\sim 10^{-1}$	(<1 sec)
Dot_4^{64}	4.6×10^5	$\sim 10^0$	(6 secs)
RSA-32	1.8×10^6	$\sim 10^1$	(21 secs)
EDT-255	1.6×10^7	$\sim 10^2$	(3 mins)
RSA-256	9.3×10^8	$\sim 10^4$	(4 hrs)
EDT-4095	5.9×10^9	$\sim 10^5$	(3 days)

Compile AES: This work (<1 sec) vs Fairplay (12 mins)

Large Circuits

Hardware:
Amazon EC2
68.4 GB RAM
8 cores

	size (gates)	
AES-128	5.0×10^4	**Fairplay**
Dot_4^{64}	4.6×10^5	
RSA-32	1.8×10^6	
EDT-255	1.6×10^7	
RSA-256	9.3×10^8	
EDT-4095	5.9×10^9	**This work**

100,000x Bigger

Progress on Fast Protocols

[MNPS04]	600 gates/sec, 2^{-80} security semi-honest
[LP07, PSSW09]	40 gates/sec, 2^{-40} security malicious
[SS11]	120 gates/sec, 2^{-40} security malicious
[NNOB11]	12k gates/sec, 2^{-80} security malicious
[HEKM11]	96k non-XOR gates/sec, 2^{-80} security semi-honest
[This Work]	**432k gates/sec** **(154k non-XOR)**, 2^{-80} security **malicious**

Aug, 2012

Techniques in Our Protocol

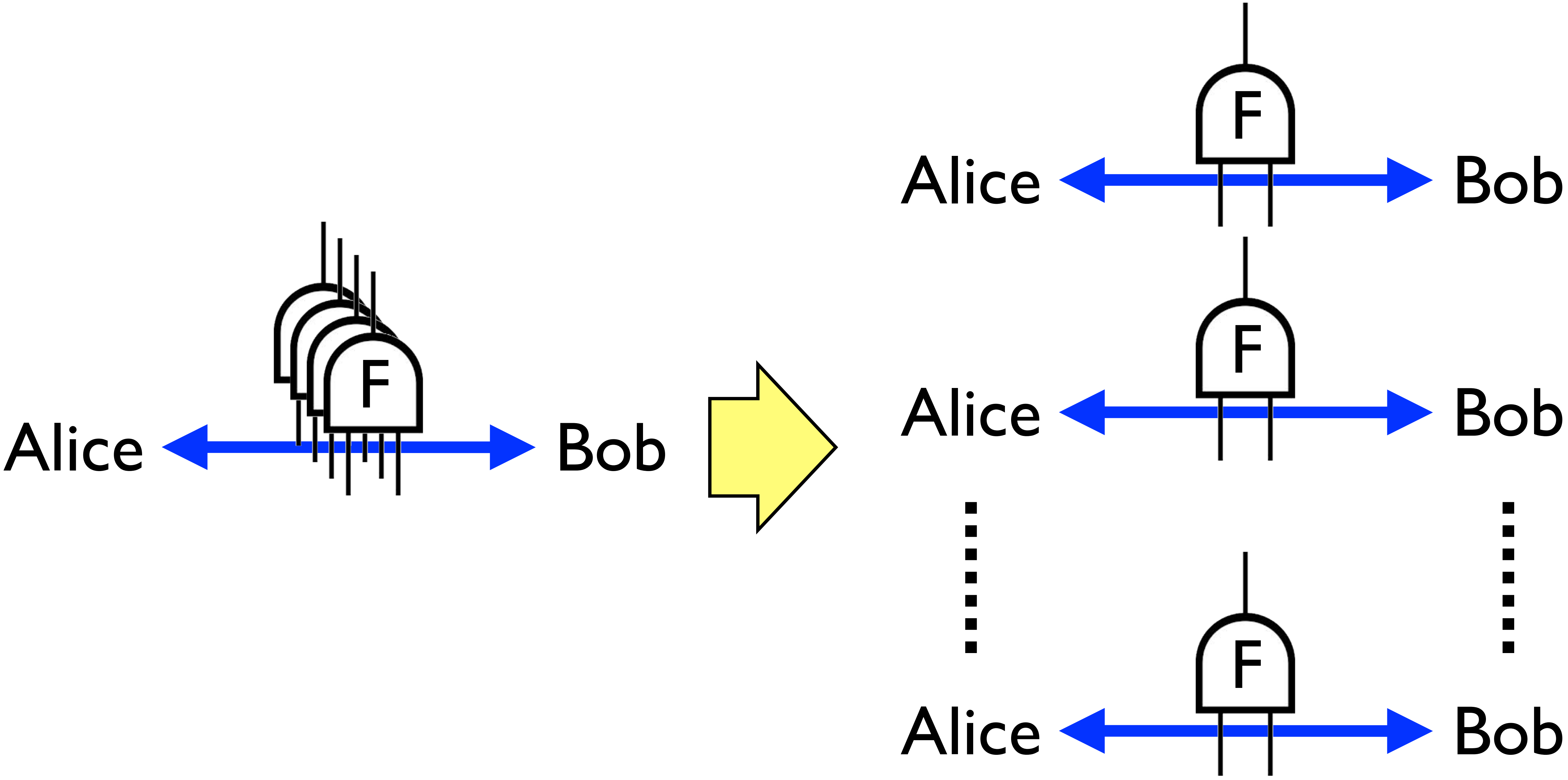
Security (Malicious Model)

Cut-and-Choose	LP07
Input Consistency	SS11
Selective Failure	LP07
Output Authentication	Ki08

Performance

Free XOR	KS08
Garbled Row Reduction	PSSW09
Random Seed Checking	GMS08

Parallelization



Alice F Bob

Alice F Bob

Alice F Bob

Alice F Bob

KSS Thesis

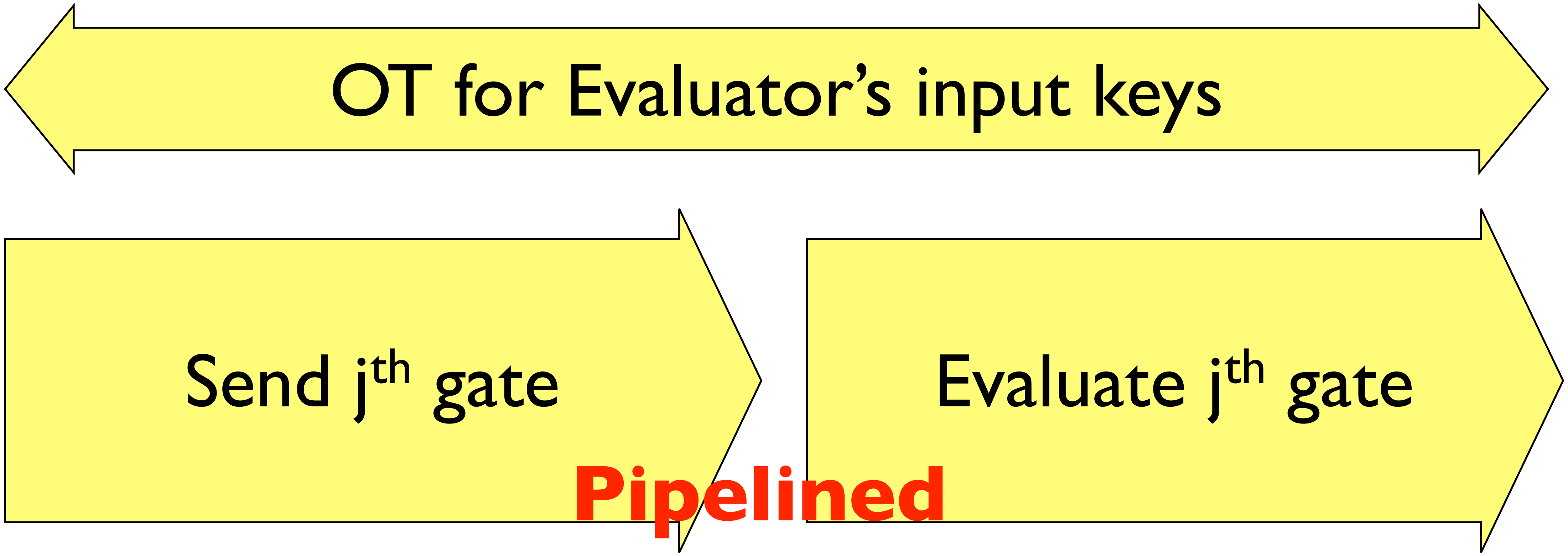
	Baseline Yao (semi-honest)	Time-Priority (malicious)
Time:	I+C	I+C+ε
Comm:	Y	256Y (for 2^{-80} security)

I: initial setup C: circuit garbling

In a model with O(k) cores and O(k) bandwidth, the "TIME OVERHEAD" between semi-honest security and malicious security is (1+ε)

k: secure parameter

Baseline Yao



OT for Evaluator's input keys

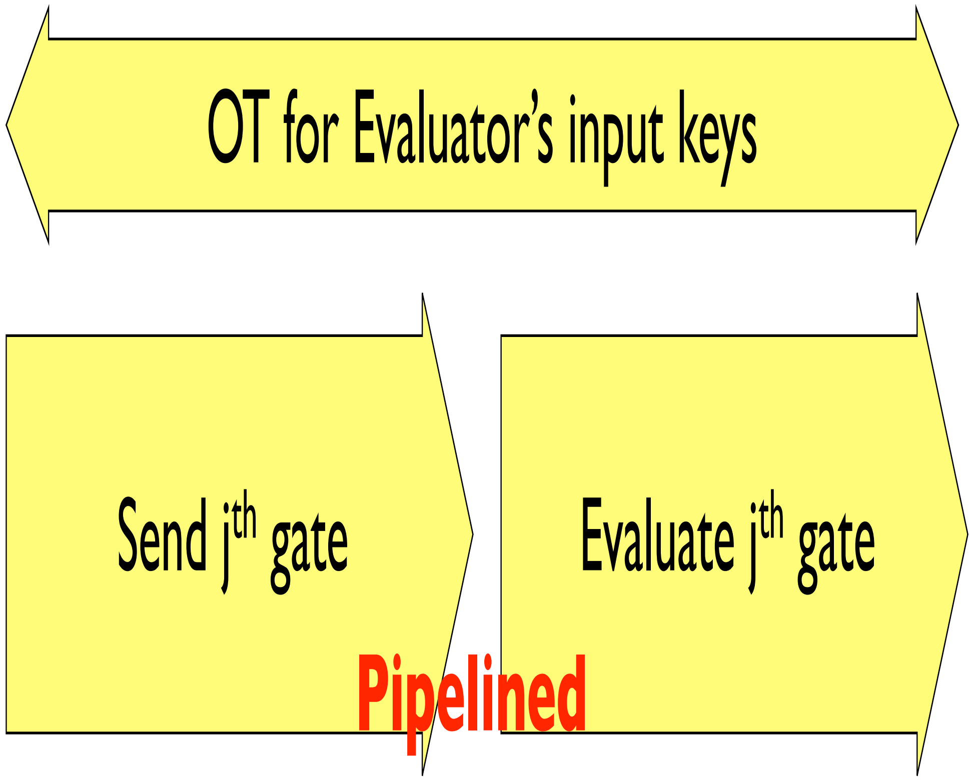
Send jth gate

Evaluate jth gate

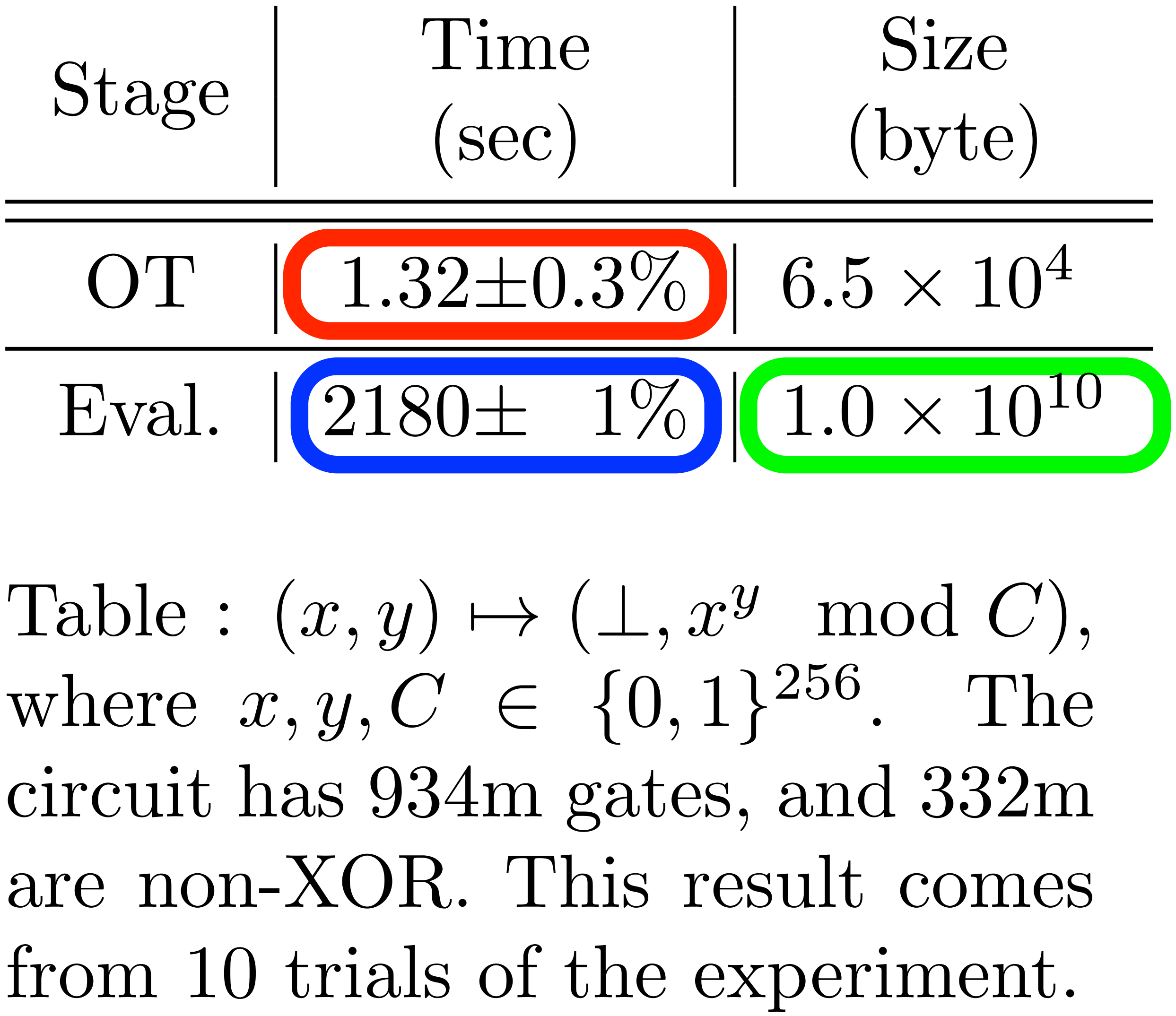
Pipelined

[HEKM11]

Baseline Yao



I



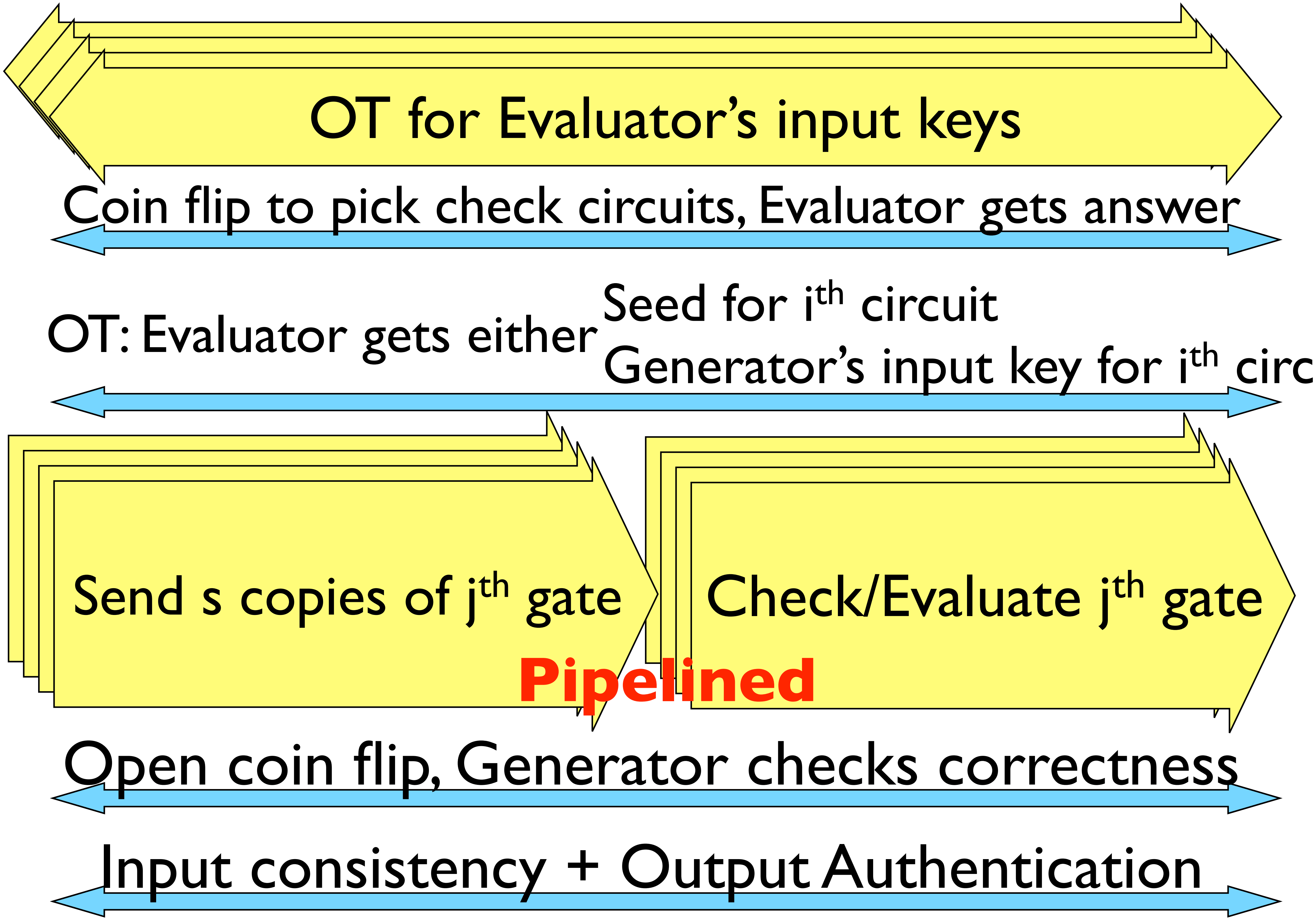
Stage	Time (sec)	Size (byte)
OT	1.32±0.3%	6.5×10^4
Eval.	2180± 1%	1.0×10^{10}

C

Table : $(x, y) \mapsto (\perp, x^y \mod C)$, where $x, y, C \in \{0,1\}^{256}$. The circuit has 934m gates, and 332m are non-XOR. This result comes from 10 trials of the experiment.

428k gates/sec

Time-Priority



OT for Evaluator's input keys

Coin flip to pick check circuits, Evaluator gets answer

OT: Evaluator gets either Seed for i^{th} circuit
Generator's input key for i^{th} circuit

Send s copies of j^{th} gate

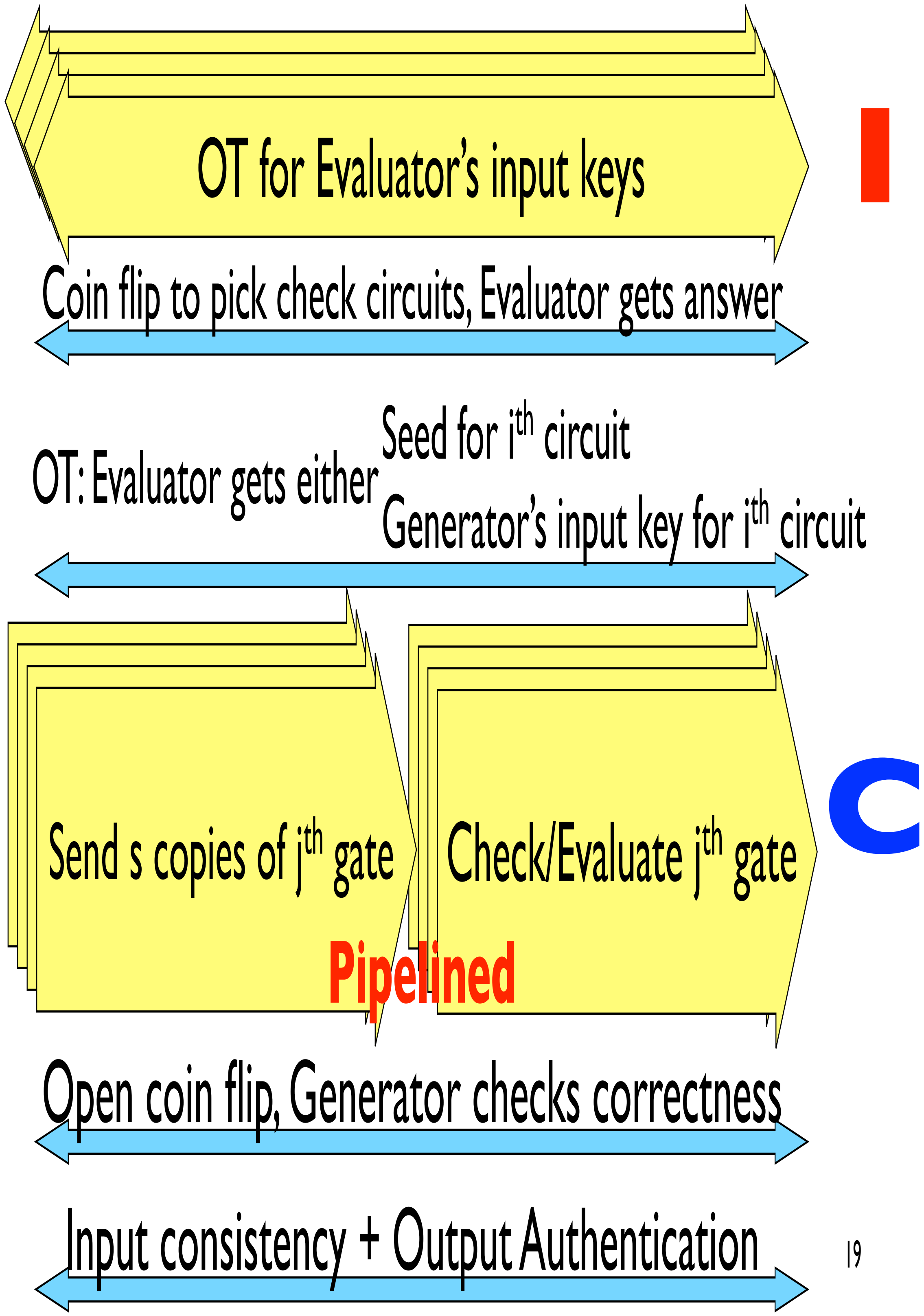
Check/Evaluate j^{th} gate

Pipelined

Open coin flip, Generator checks correctness

Input consistency + Output Authentication

Time-Priority



OT for Evaluator's input keys

Coin flip to pick check circuits, Evaluator gets answer

OT: Evaluator gets either Seed for i^{th} circuit

Generator's input key for i^{th} circuit

Send s copies of j^{th} gate

Check/Evaluate j^{th} gate

Pipelined

Open coin flip, Generator checks correctness

Input consistency + Output Authentication

I

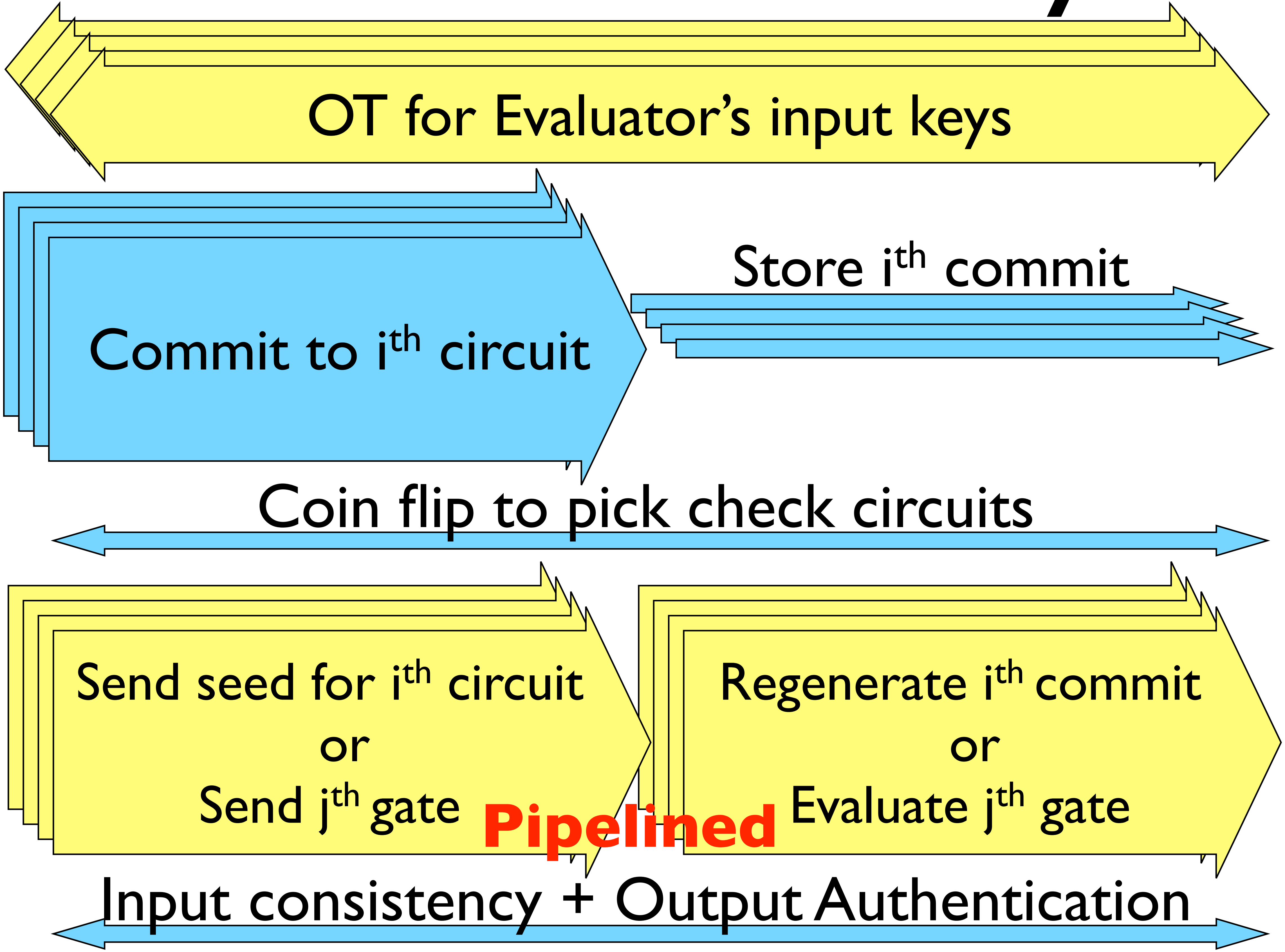
Stage	Time (sec)	Size (byte)
OT	1.4± 9%	1.1×10^7
Cut-&-Chk.	0.001±0.7%	6.2×10^1
2nd OT	0.1±0.8%	4.1×10^6
Eval.	2160±0.4%	2.6×10^{12}
Input Chk.	0.003± 15%	5.3×10^5

C

Table : $(x, y) \mapsto (\perp, x^y \mod C)$, where $x, y, C \in \{0,1\}^{256}$. The circuit has 934m gates, and 332m are non-XOR. Each party has 256 nodes. 256 copies of the circuit are used. This result comes from 10 trials of the experiment.

~1x ~256x

Comm-Priority



OT for Evaluator’s input keys

Commit to i^{th} circuit

Store i^{th} commit

Coin flip to pick check circuits

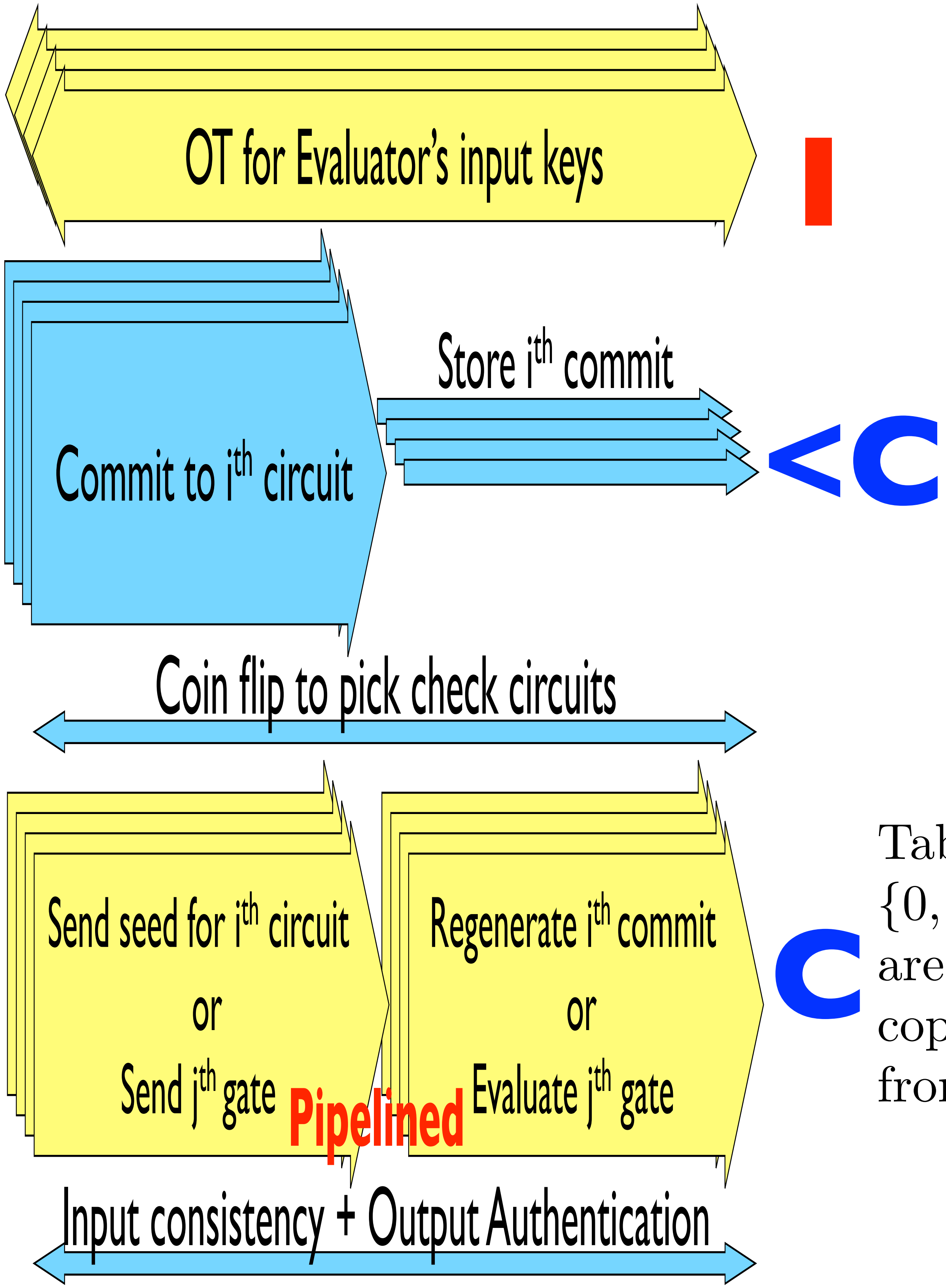
Send seed for i^{th} circuit
or
Send j^{th} gate

Pipelined

Regenerate i^{th} commit
or
Evaluate j^{th} gate

Input consistency + Output Authentication

Comm-Priority



OT for Evaluator's input keys

I

Commit to ith circuit

Store ith commit

<C

Coin flip to pick check circuits

Send seed for ith circuit

or

Send jth gate

Pipelined

Regenerate ith commit

or

Evaluate jth gate

C

Input consistency + Output Authentication

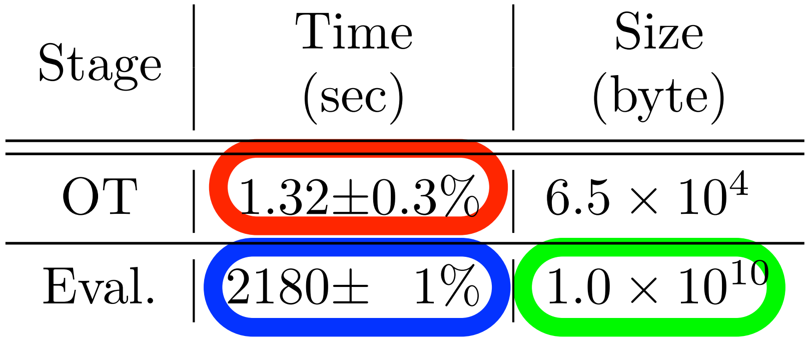
Stage	Time (sec)	Size (byte)
OT	1.4± 5%	1.1×10^7
Commit	1231±0.2%	2.6×10^3
Cut-&-Chk.	0.004± 22%	6.2×10^1
Eval.	2270± 1%	1.0×10^{12}
Input Chk.	0.07±0.3%	5.3×10^5

Table : $(x, y) \mapsto (\bot, x^y \mod C)$, where $x, y, C \in \{0,1\}^{256}$. The circuit has 934m gates, and 332m are non-XOR. Each party has 256 nodes. 256 copies of the circuit are used. This result comes from 10 trials of the experiment.

~1.6x ~102x

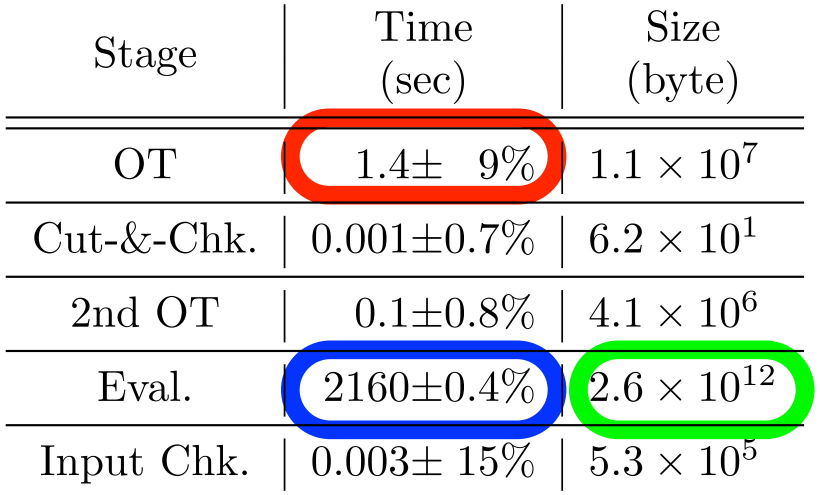
KSS Thesis

Baseline Yao (semi-honest)



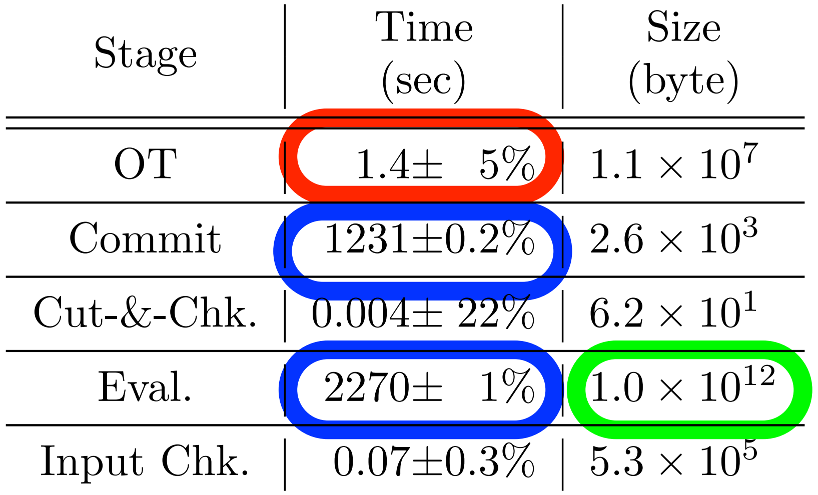
Stage	Time (sec)	Size (byte)
OT	1.32±0.3%	6.5×10^4
Eval.	2180± 1%	1.0×10^{10}

Time-Priority (malicious)



Stage	Time (sec)	Size (byte)
OT	1.4± 9%	1.1×10^7
Cut-&-Chk.	0.001±0.7%	6.2×10^1
2nd OT	0.1±0.8%	4.1×10^6
Eval.	2160±0.4%	2.6×10^{12}
Input Chk.	0.003± 15%	5.3×10^5

Comm-Priority (malicious)

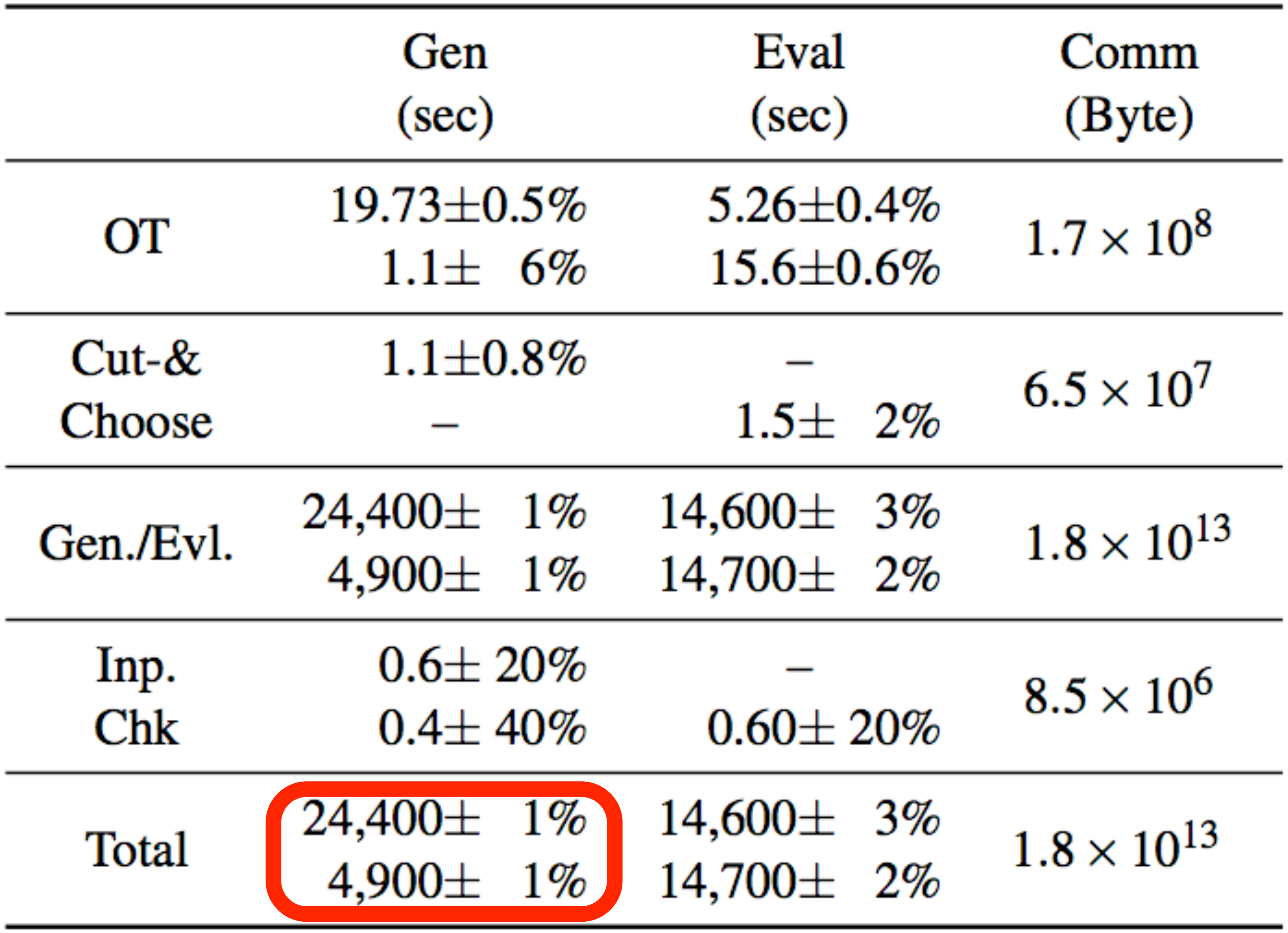


Stage	Time (sec)	Size (byte)
OT	1.4± 5%	1.1×10^7
Commit	1231±0.2%	2.6×10^3
Cut-&-Chk.	0.004± 22%	6.2×10^1
Eval.	2270± 1%	1.0×10^{12}
Input Chk.	0.07±0.3%	5.3×10^5

Cores:	1	256	256
Time:	1+C	1+C+ε	1+<2C+ε
Comm:	Y	256Y	102Y

In a model with O(k) cores and O(k) bandwidth, the "TIME OVERHEAD" between semi-honest security and malicious security is (1+ε)

4095x4095 Edit Distance



	Gen (sec)	Eval (sec)	Comm (Byte)
OT	19.73±0.5% 1.1± 6%	5.26±0.4% 15.6±0.6%	1.7×10^8
Cut-& Choose	1.1±0.8% –	– 1.5± 2%	6.5×10^7
Gen./Evl.	24,400± 1% 4,900± 1%	14,600± 3% 14,700± 2%	1.8×10^{13}
Inp. Chk	0.6± 20% 0.4± 40%	– 0.60± 20%	8.5×10^6
Total	24,400± 1% 4,900± 1%	14,600± 3% 14,700± 2%	1.8×10^{13}

size: **5.9b** (2.4b non-xor)

rate: **201k** per sec (82k non-xor)

256 cores. 6 trials. time-priority approach.

RSA256 (latest)

Comm-Priority

Stage	Time (sec)	Size (byte)
OT	1.4	1.1×10^7
Commit	1231	2.6×10^3
Cut-&-Chk.	0.004	6.2×10^1
Eval.	2270	1.0×10^{12}
Input Chk.	0.07	8.0×10^5
Total	3510	1.0×10^{12}

size: 934m/332m (non-XOR)

rate: **266k/95k** (non-XOR) / sec.

256 cores. 10 trials.

Time-Priority

Stage	Time (sec)	Size (byte)
OT	1.41	1.1×10^7
Cut-&-Chk.	0.001	6.2×10^1
2nd OT	0.1	4.1×10^6
Eval.	2160	2.6×10^{12}
Input Chk.	0.003	5.3×10^5
Total	2161	2.6×10^{12}

size: 934m/332m (non-XOR)

rate: **432k/154k** (non-XOR) / sec.

256 cores. 10 trials.

Future Work

- Just-in-time compiler
- GPU+FPGA

Questions?