Secure Multi-Party Computation

Secure two-party computation

f

x

$f(x, y)$

y

$f(x, y)$

x and y remain secret

Secret sharing

Alice

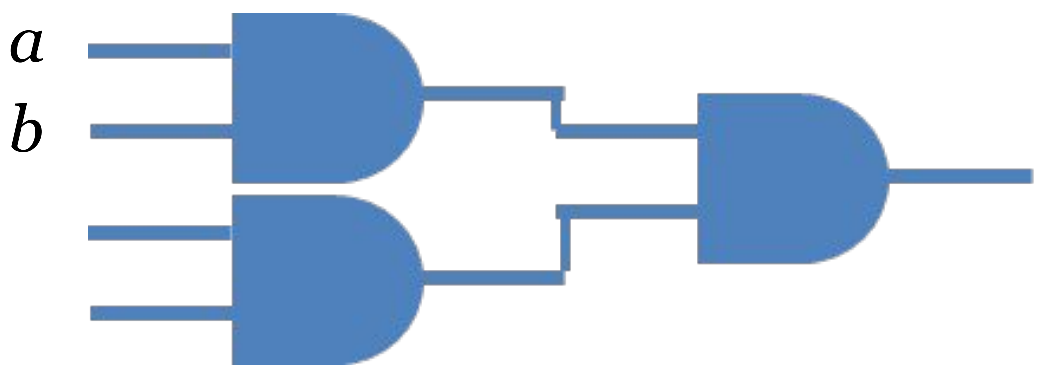
$$a = a_0 \oplus a_1$$

a_0 $\qquad$ a_1

Bob

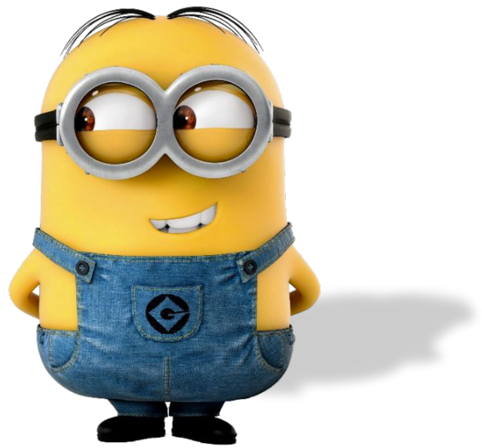
GMW protocol

Input:



Alice

Bob



$a \quad a_0 = a \oplus a_1$

a_1 →

$b_1 = b \oplus b_0 \quad b$

← b_0

GMW protocol

XOR gates

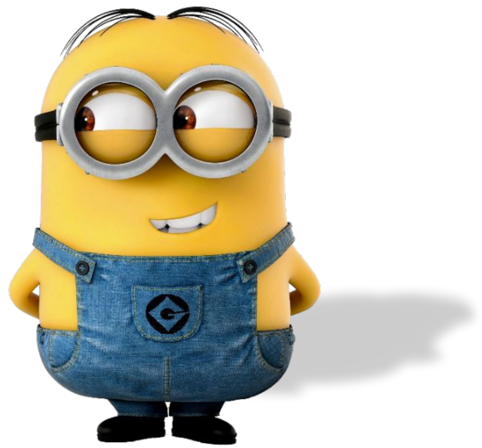
Alice

a_0

b_0

$c_0 = (a_0 \oplus b_0)$

Bob



a_1

b_1

$c_1 = (a_1 \oplus b_1)$

$$
\begin{aligned}
c &= a \oplus b \\
&= (a_0 \oplus a_1) \oplus (b_0 \oplus b_1) \\
&= (a_0 \oplus b_0) \oplus (a_1 \oplus b_1)
\end{aligned}
$$

GMW protocol

AND gates

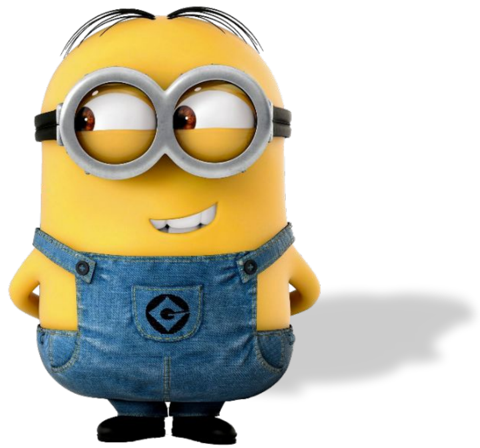
Alice

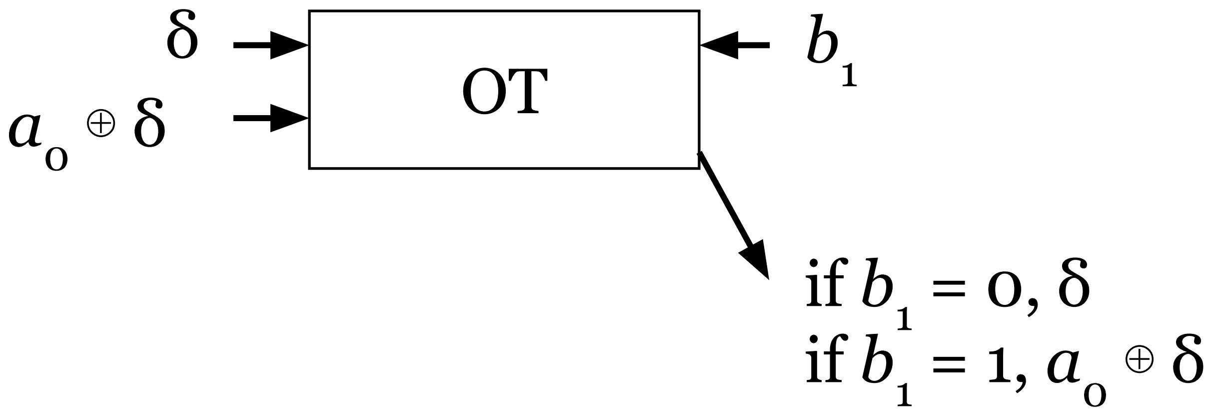
a_0

δ

b_1

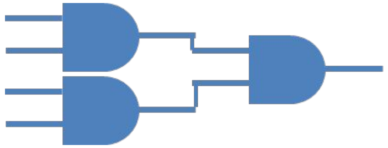
Bob





Yao's garbled circuit

f



x

Alice

Garbled Table
Enc $_{A_0,B_0}$ (C_0)
Enc $_{A_0,B_1}$ (C_0)
Enc $_{A_1,B_0}$ (C_0)
Enc $_{A_1,B_1}$ (C_1)

Garbled Table
Enc $_{D_0,E_0}$ (F_0)
Enc $_{D_0,E_1}$ (F_0)
Enc $_{D_1,E_0}$ (F_0)
Enc $_{D_1,E_1}$ (F_1)

Garbled Table
Enc $_{D_0,E_0}$ (F_0)
Enc $_{D_0,E_1}$ (F_0)
Enc $_{D_1,E_0}$ (F_0)
Enc $_{D_1,E_1}$ (F_1)

y

Bob

Keys for x: e.g., A_0 , B_1

Keys for y: oblivious transfer

D_0

D_1

OT

$y_0 = 1$

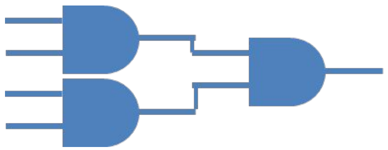
D_1 , E_0

$f(x,y) = 0$

G_0

Yao's garbled circuit

f



x

Alice

Garbled Table	Garbled Table	Garbled Table
Enc $_{A_0,B_0}(C_0)$	Enc $_{D_0,E_0}(F_0)$	Enc $_{D_0,E_0}(F_0)$
Enc $_{A_0,B_1}(C_0)$	Enc $_{D_0,E_1}(F_0)$	Enc $_{D_0,E_1}(F_0)$
Enc $_{A_1,B_0}(C_0)$	Enc $_{D_1,E_0}(F_0)$	Enc $_{D_1,E_0}(F_0)$
Enc $_{A_1,B_1}(C_1)$	Enc $_{D_1,E_1}(F_1)$	Enc $_{D_1,E_1}(F_1)$

Keys for x: e.g., A_0 , B_1

Keys for y: oblivious transfer

$D_0 \rightarrow$ OT $\leftarrow y_o = 1$

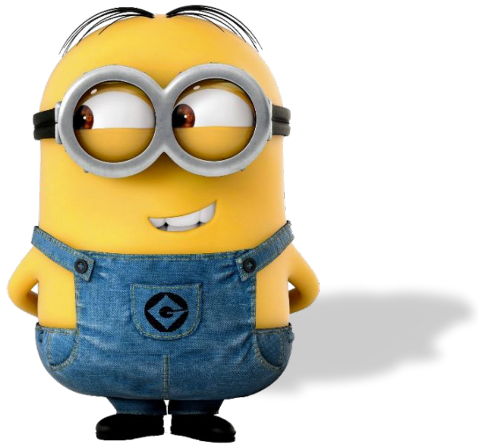
$D_1 \rightarrow$

D_1 , E_0

G_0, G_1

y

Bob



$f(x,y) = 0$

Semi-honest vs. malicious

Semi-honest adversary: follow the protocol, try to infer information from the transcript

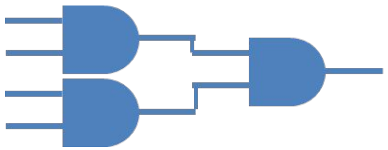
Malicious: deviate from the protocol arbitrarily

What can go wrong with malicious adversaries?

x

Alice

f



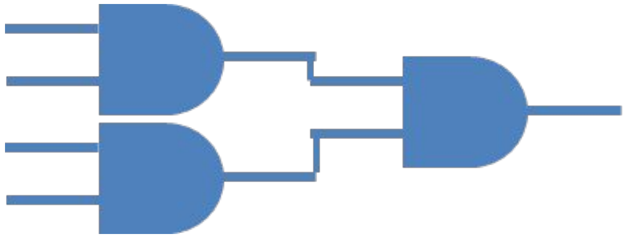
Garbled Table	Garbled Table	Garbled Table
$Enc_{A_0,B_0}(C_0)$	$Enc_{D_0,E_0}(F_0)$	$Enc_{D_0,E_0}(F_0)$
$Enc_{A_0,B_1}(C_0)$	$Enc_{D_0,E_1}(F_0)$	$Enc_{D_0,E_1}(F_0)$
$Enc_{A_1,B_0}(C_0)$	$Enc_{D_1,E_0}(F_0)$	$Enc_{D_1,E_0}(F_0)$
$Enc_{A_1,B_1}(C_1)$	$Enc_{D_1,E_1}(F_1)$	$Enc_{D_1,E_1}(F_1)$

y

Bob

Attacks by malicious adversaries

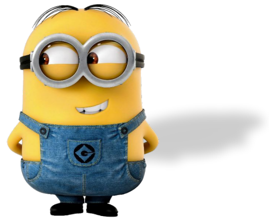
1. Wrong function
2. Selective failure



Alice

Garbled Table
Enc $A_0,B_0\,(C_0)$
Enc $A_0,B_1\,(C_0)$
~~Enc $A_1,B_0\,(C_0)$~~
Enc $A_1,B_1\,(C_1)$

Bob



Attacks by malicious adversaries

1. Wrong function
2. Selective failure
3. Bit flipping

Solution for malicious security

- Open the garbled circuit?

Cut and choose

- Alice sends 2 copies of garbled circuit to Bob
- Bob randomly selects 1 and asks Alice to open it
- Bob uses the other for MPC
- Pr[garbled circuit used by Bob is wrong] = ?

Repetition

- Repeat cut-and-choose by k times
- Learn the output if all are the same*
- Pr[all garbled circuits used by Bob are wrong] = $\frac{1}{2^k}$

Additional problems

- Majority instead of all

- Input consistency: commitments
  - $c \leftarrow \text{commit}(m, r)$
  - $\{0,1\} \leftarrow \text{open}(c, m, r)$

  Binding and hiding

Advanced techniques for malicious security

- Bucketing

- Authenticated garbling

Honest majority vs. dishonest majority

Honest majority: < n/2 malicious parties

- Can be information-theoretic secure
- More efficient*

Dishonest majority: >= n/2 malicious parties

- Computational assumptions
- Cryptographic operations

Special cases

2 PC

- Simple and challenging

3 PC with 1 malicious

- Usually the most efficient

4 PC with 1 malicious

Static vs. adaptive

- Static: adversary fixes the parties to corrupt at the beginning of the protocol
- Adaptive: adversary can adaptively choose parties to corrupt. Erasure doesn’t trivially solve the problem

Fairness and output delivery

- Fair: either all parties receive the correct output, or no party does
  - Motivation: auction

Fairness and output delivery

- Cannot be achieved with dishonest majority
  - Limits on the Security of Coin Flips When Half the Processors are Faulty, Richard Cleve 86

- Computational setting:
  - Honest majority $< n/2$ malicious parties

- Information theoretic setting:
  - $< n/3$ malicious parties
  - $< n/2$ malicious parties and broadcast channel