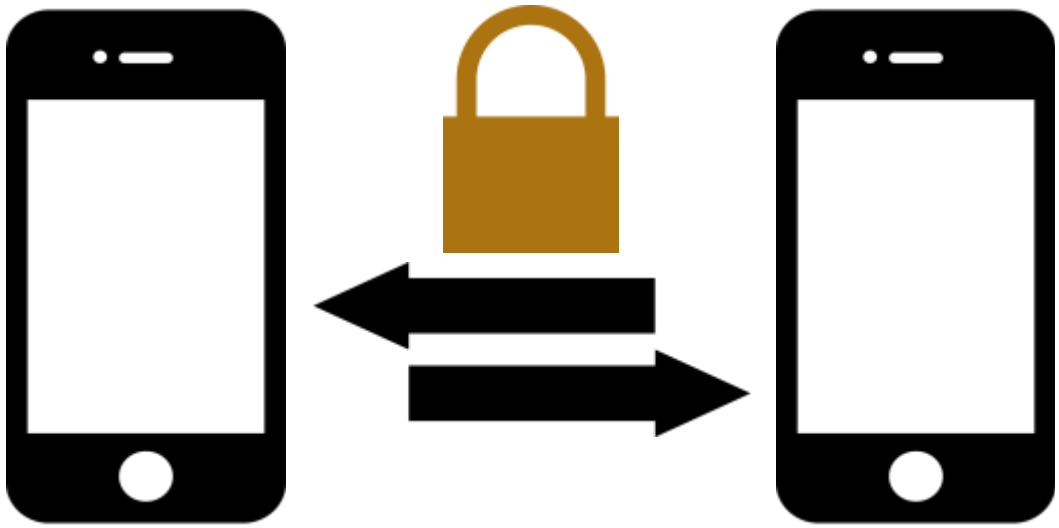
Secure Computation on Mobile Devices

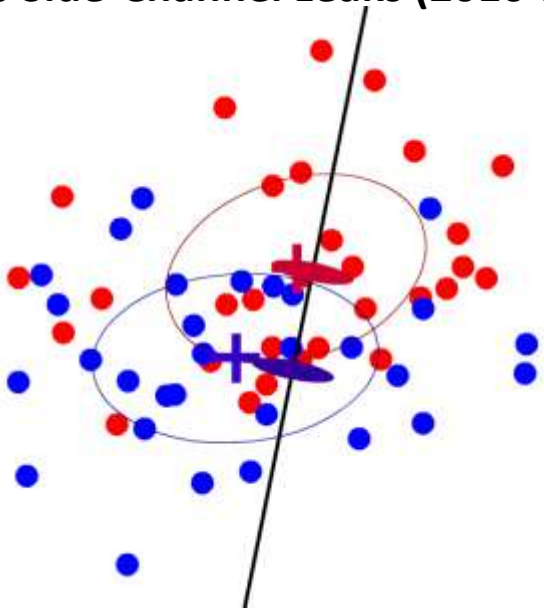


CS 1120
December 2, 2011

Peter Chapman
http://www.cs.virginia.edu/~pmc8p

Microsoft Research (Summer 2011)

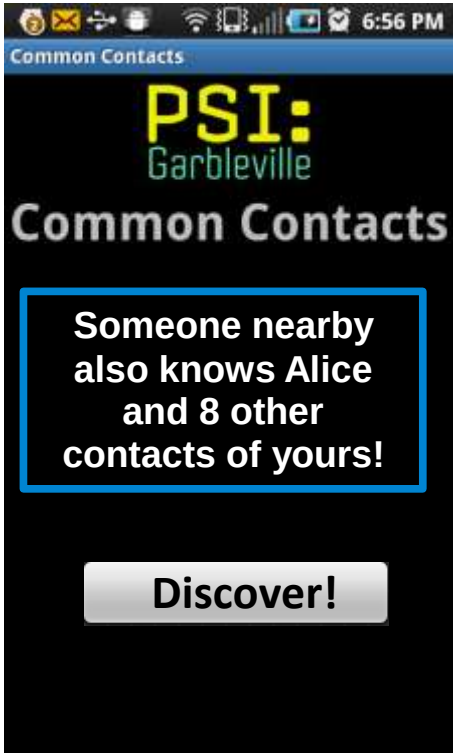
Web Side-Channel Leaks (2010-2011)



Secure Computation on Mobile Devices (2011-Present)

Mutual Contact Discovery

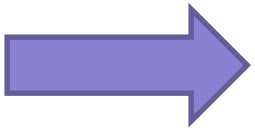
Bob

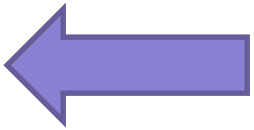


Alice

Sharing contact list with a stranger is unacceptable

Trust someone else?





Bob

Alice

The Dilemma

Can we interact with others *and* control our data?

Secure Two-Party Computation

Alice

Private Data: *a*

Garbled Circuit Protocol

Outputs $x = f(a, b)$ without revealing a to Bob or b to Alice.

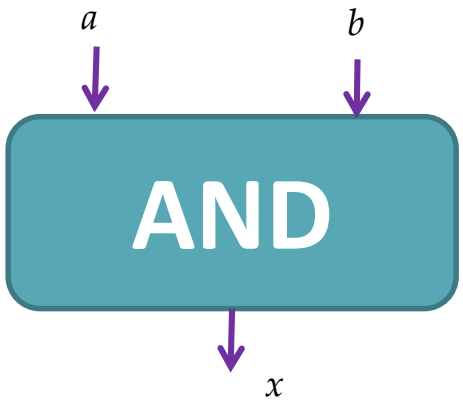
Bob

Private Data: *b*

Andrew Yao, 1982/1986

Yao's Garbled Circuits

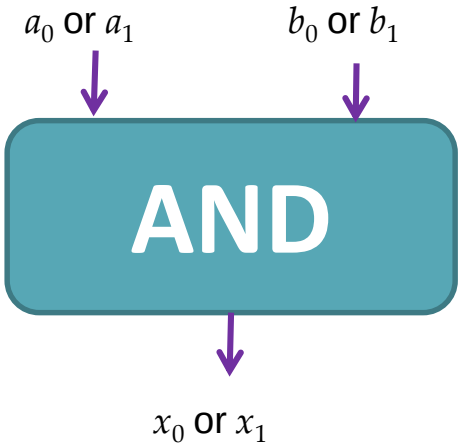
Inputs		Output
a	b	x
0	0	0
0	1	0
1	0	0
1	1	1



Computing with Meaningless Values?

Inputs		Output
a	b	x
a_0	b_0	x_0
a_0	b_1	x_0
a_1	b_0	x_0
a_1	b_1	x_1

a_i, b_i, x_i are **random** values, chosen by the **circuit generator** but **meaningless** to the **circuit evaluator**.

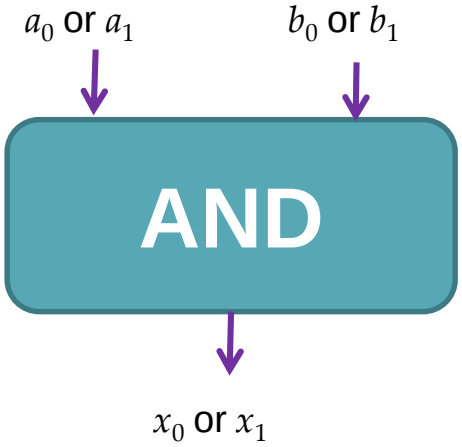


Computing with Garbled Tables

Inputs		Output
a	b	x
a_0	b_0	$Enc_{a0,b0}(x_0)$
a_0	b_1	$Enc_{a0,b1}(x_0)$
a_1	b_0	$Enc_{a1,b0}(x_0)$
a_1	b_1	$Enc_{a1,b1}(x_1)$

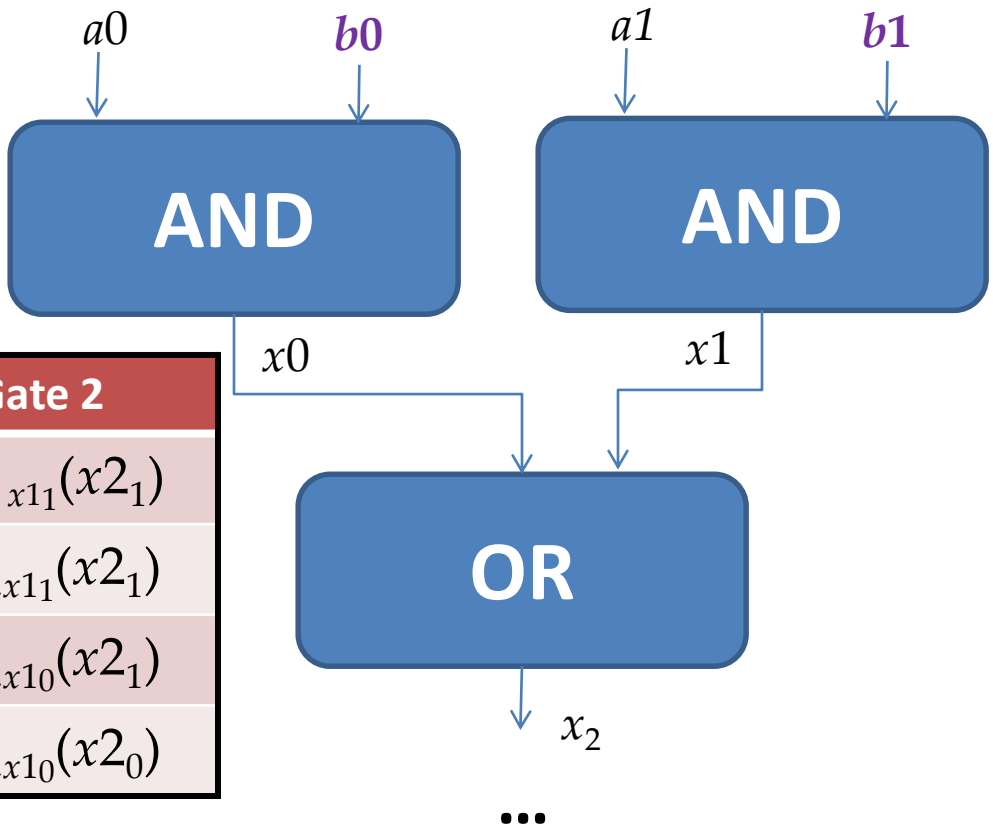
Bob can only decrypt **one** of these!

a_i, b_i, x_i are **random** values, chosen by the **circuit generator** but **meaningless** to the **circuit evaluator**.



Garbled And Gate
$Enc_{a0,\ b1}(x_0)$
$Enc_{a1,b1}(x_1)$
$Enc_{a1,b0}(x_0)$
$Enc_{a0,b0}(x_0)$

Chaining Garbled Circuits



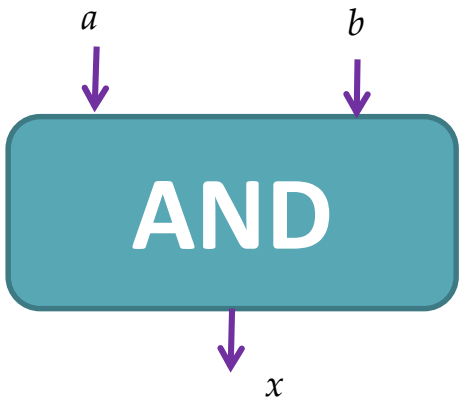
And Gate 1
$Enc_{a1_0,\, b1_1}(x1_0)$
$Enc_{a1_1,b1_1}(x1_1)$
$Enc_{a1_1,b1_0}(x1_0)$
$Enc_{a1_0,b1_0}(x1_0)$

Or Gate 2
$Enc_{x0_0,\, x1_1}(x2_1)$
$Enc_{x0_1,x1_1}(x2_1)$
$Enc_{x0_1,x1_0}(x2_1)$
$Enc_{x0_0,x1_0}(x2_0)$

We can do ***any*** computation privately this way!

Yao's Garbled Circuits

Inputs		Output
a	b	x
0	0	0
0	1	0
1	0	0
1	1	1



Computing with Meaningless Values?

Inputs		Output
a	b	x
a_0	b_0	x_0
a_0	b_1	x_0
a_1	b_0	x_0
a_1	b_1	x_1

a_i, b_i, x_i are **random** values, chosen by the **circuit generator** but **meaningless** to the **circuit evaluator**.

We use 80-Bit Random Numbers

```
11111111111111111111111111111111111111111010001000000010001000011011000001000
```

1,208,925,819,614,527,173,703,176

1 septillion, 208 sextillion, 925 quintillion, 819 quadrillion, 614 trillion, 527 billion, 173 million, 703 thousand, and 176

Computing with Meaningless Values?

Inputs		Output
a	b	x
a_0	b_0	x_0
a_0	b_1	x_0
a_1	b_0	x_0
a_1	b_1	x_1

Computing with Meaningless Values?

Really 80-Bit Numbers

Inputs		Output
a	b	x
193	b_0	x_0
193	b_1	x_0
a_1	b_0	x_0
a_1	b_1	x_1

Computing with Meaningless Values?

Really 80-Bit Numbers

Inputs		Output
a	b	x
193	b_0	x_0
193	b_1	x_0
465	b_0	x_0
465	b_1	x_1

Computing with Meaningless Values?

Really 80-Bit Numbers

Inputs		Output
a	b	x
193	657	x_0
193	b_1	x_0
465	657	x_0
465	b_1	x_1

Computing with Meaningless Values?

Really 80-Bit Numbers

Inputs		Output
a	b	x
193	657	x_0
193	255	x_0
465	657	x_0
465	255	x_1

Computing with Meaningless Values?

Really 80-Bit Numbers

Inputs		Output
a	b	x
193	657	844
193	255	844
465	657	844
465	255	x_1

Computing with Meaningless Values?

Really 80-Bit Numbers

Inputs		Output
a	*b*	*x*
193	*657*	*844*
193	*255*	*844*
465	*657*	*844*
465	*255*	*123*

Computing with Garbled Tables

Really 80-Bit Numbers

Inputs		Output
a	b	x
193	657	$Enc_{193;657}(844)$
193	255	$Enc_{193;255}(844)$
465	657	$Enc_{465;657}(844)$
465	255	$Enc_{465;255}(123)$

Bob can only decrypt **one** of these!

Garbled And Gate
$Enc_{193;255}(844)$
$Enc_{465;657}(123)$
$Enc_{465;657}(844)$
$Enc_{193;657}(844)$

Alice

Bob

Garbled And Gate
$Enc_{193;255}(844)$
$Enc_{465;657}(123)$
$Enc_{465;657}(844)$
$Enc_{193;657}(844)$

a_0	*193*

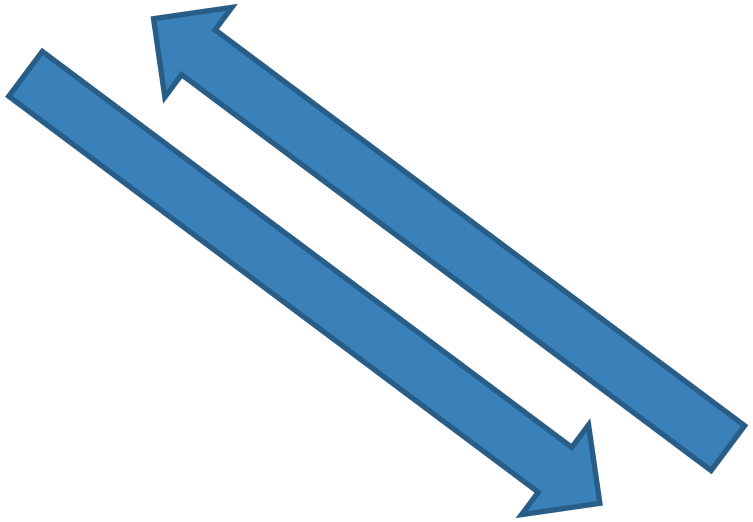
Oblivious Transfer

Alice **Bob**

b_0	*657*
b_1	*255*

193

0

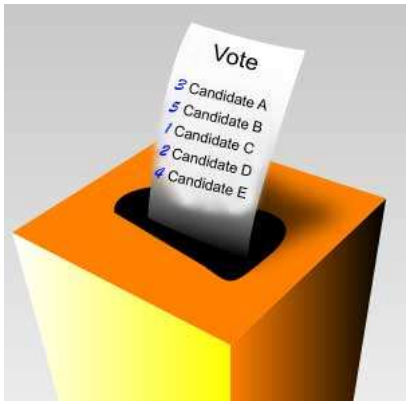


844

Garbled And Gate
$Enc_{193;255}(844)$
$Enc_{465;657}(123)$
$Enc_{465;657}(844)$
$Enc_{193;657}(844)$

Potential Applications

Common Contacts



Favorite Movies

Hyper-Targeted Advertising

Voting, Auctions & more!

Collaborative Scheduling

http://MightBeEvil.com/mobile/

Research Advice

Don’t be afraid.

Attributions

“iPhone” symbol from thenounproject.com collection.

"Lock" symbol from thenounproject.com collection.