Secure Computation on Mobile Devices

CS 1120
December 2, 2011

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

Sharing contact list with a stranger is unacceptable

Someone nearby also knows Alice and 8 other contacts of yours!
Trust someone else?

Bob

Facebook

Alice
The Dilemma

Can we interact with others and control our data?
Secure Two-Party Computation

Alice
Private Data: $a$

Bob
Private Data: $b$

Garbled Circuit Protocol

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

Andrew Yao, 1982/1986
# Yao’s Garbled Circuits

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a)</td>
<td>(b)</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

\[ \text{AND} \]
Computing with Meaningless Values?

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>$a_0$</td>
<td>$b_0$</td>
</tr>
<tr>
<td>$a_0$</td>
<td>$b_1$</td>
</tr>
<tr>
<td>$a_1$</td>
<td>$b_0$</td>
</tr>
<tr>
<td>$a_1$</td>
<td>$b_1$</td>
</tr>
</tbody>
</table>

$a_i, b_i, x_i$ are random values, chosen by the circuit generator but meaningless to the circuit evaluator.
Computing with Garbled Tables

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>$a_0$</td>
<td>$b_0$</td>
</tr>
<tr>
<td>$a_0$</td>
<td>$b_1$</td>
</tr>
<tr>
<td>$a_1$</td>
<td>$b_0$</td>
</tr>
<tr>
<td>$a_1$</td>
<td>$b_1$</td>
</tr>
</tbody>
</table>

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

Bob can only decrypt one of these!

Garbled And Gate

- $\text{Enc}_{a_0,b_0}(x_0)$
- $\text{Enc}_{a_0,b_1}(x_0)$
- $\text{Enc}_{a_1,b_0}(x_0)$
- $\text{Enc}_{a_1,b_1}(x_1)$
Chaining Garbled Circuits

We can do any computation privately this way!
# Yao’s Garbled Circuits

The table below shows the truth table for the AND function.

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

The diagram below illustrates the AND gate with inputs $a$ and $b$ and output $x$. 

![AND gate diagram](image-url)
Computing with Meaningless Values?

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>$a_0$</td>
<td>$b_0$</td>
</tr>
<tr>
<td>$a_0$</td>
<td>$b_1$</td>
</tr>
<tr>
<td>$a_1$</td>
<td>$b_0$</td>
</tr>
<tr>
<td>$a_1$</td>
<td>$b_1$</td>
</tr>
</tbody>
</table>

$a_i$, $b_i$, $x_i$ are random values, chosen by the circuit generator but meaningless to the circuit evaluator.
We use 80-Bit Random Numbers

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?

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a)</td>
<td>(b)</td>
</tr>
<tr>
<td>(a_0)</td>
<td>(b_0)</td>
</tr>
<tr>
<td>(a_0)</td>
<td>(b_1)</td>
</tr>
<tr>
<td>(a_1)</td>
<td>(b_0)</td>
</tr>
<tr>
<td>(a_1)</td>
<td>(b_1)</td>
</tr>
</tbody>
</table>
Computing with Meaningless Values?

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>193</td>
<td>$b_0$</td>
</tr>
<tr>
<td>193</td>
<td>$b_1$</td>
</tr>
<tr>
<td>$a_1$</td>
<td>$b_0$</td>
</tr>
<tr>
<td>$a_1$</td>
<td>$b_1$</td>
</tr>
</tbody>
</table>

Really 80-Bit Numbers
## Computing with Meaningless Values?

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a)</td>
<td>(b)</td>
</tr>
<tr>
<td>193</td>
<td>(b_0)</td>
</tr>
<tr>
<td>193</td>
<td>(b_1)</td>
</tr>
<tr>
<td>465</td>
<td>(b_0)</td>
</tr>
<tr>
<td>465</td>
<td>(b_1)</td>
</tr>
</tbody>
</table>

Really 80-Bit Numbers
Computing with Meaningless Values?

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>193</td>
<td>657</td>
</tr>
<tr>
<td>193</td>
<td>$b_1$</td>
</tr>
<tr>
<td>465</td>
<td>657</td>
</tr>
<tr>
<td>465</td>
<td>$b_1$</td>
</tr>
</tbody>
</table>

Really 80-Bit Numbers
Computing with Meaningless Values?

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>193</td>
<td>657</td>
</tr>
<tr>
<td>193</td>
<td>255</td>
</tr>
<tr>
<td>465</td>
<td>657</td>
</tr>
<tr>
<td>465</td>
<td>255</td>
</tr>
</tbody>
</table>

Really 80-Bit Numbers
## Computing with Meaningless Values?

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>193</td>
<td>657</td>
</tr>
<tr>
<td>193</td>
<td>255</td>
</tr>
<tr>
<td>465</td>
<td>657</td>
</tr>
<tr>
<td>465</td>
<td>255</td>
</tr>
</tbody>
</table>

Really 80-Bit Numbers
## Computing with Meaningless Values?

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>193</td>
<td>657</td>
</tr>
<tr>
<td>193</td>
<td>255</td>
</tr>
<tr>
<td>465</td>
<td>657</td>
</tr>
<tr>
<td>465</td>
<td>255</td>
</tr>
</tbody>
</table>

Really 80-Bit Numbers
## Computing with Garbled Tables

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>193</td>
<td>657</td>
</tr>
<tr>
<td>193</td>
<td>255</td>
</tr>
<tr>
<td>465</td>
<td>657</td>
</tr>
<tr>
<td>465</td>
<td>255</td>
</tr>
</tbody>
</table>

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

**Really 80-Bit Numbers**
### Garbled And Gate

<table>
<thead>
<tr>
<th>Encryption</th>
<th>Plaintext</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Enc_{193;255}(844)$</td>
<td></td>
</tr>
<tr>
<td>$Enc_{465;657}(123)$</td>
<td></td>
</tr>
<tr>
<td>$Enc_{465;657}(844)$</td>
<td></td>
</tr>
<tr>
<td>$Enc_{193;657}(844)$</td>
<td></td>
</tr>
</tbody>
</table>

| $a_0$ | 193 |
Oblivious Transfer

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>$b_0$</td>
<td>657</td>
</tr>
<tr>
<td>$b_1$</td>
<td>255</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Garbled And Gate</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Enc_{193;255}(844)$</td>
</tr>
<tr>
<td>$Enc_{465;657}(123)$</td>
</tr>
<tr>
<td>$Enc_{465;657}(844)$</td>
</tr>
<tr>
<td>$Enc_{193;657}(844)$</td>
</tr>
</tbody>
</table>
Potential Applications

Common Contacts

Favorite Movies

Voting, Auctions & more!

Hyper-Targeted Advertising

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.