Secure Two-Party Computation

Can Alice and Bob compute a function of their private data, without exposing anything about their data besides the result?

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>

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>0</td>
<td>0</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, b, x are random values, chosen by the circuit generator but meaningless to the circuit evaluator.

Secure Function Evaluation

Alice (circuit generator) Bob (circuit evaluator)

Picks $a \in \{0, 1\}^n$\(^a\)

Agree on $f(a, b) \rightarrow x$
Picks $b \in \{0, 1\}^l$

Bob’s Genome: ACTG... Markers (~1000): [0, 1, ..., 0]

Alice’s Genome: ACTG... Markers (~1000): [0, 0, ..., 1]

$x = f(g_A, g_B)$

Garbled Circuit Protocol

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

Andrew Yao, 1982/1986
Computing with Garbled Tables

Inputs | Output
---|---
a | x
\(a_0\) | \(b_0\) | \(Enc_{a_0,b_0}(x_0)\)
\(a_0\) | \(b_1\) | \(Enc_{a_0,b_1}(x_0)\)
\(a_1\) | \(b_0\) | \(Enc_{a_1,b_0}(x_1)\)
\(a_1\) | \(b_1\) | \(Enc_{a_1,b_1}(x_1)\)

Garbled And Gate
\(a_0 \land b_0 \rightarrow y_0\)
\(a_0 \land b_1 \rightarrow y_1\)
\(a_1 \land b_0 \rightarrow y_2\)
\(a_1 \land b_1 \rightarrow y_3\)

Bob can only decrypt
\(a_0, b_0, x\) are random values, chosen by the circuit generator but meaningless to the circuit evaluator.

Fairplay
Alice         Bob

Garbled Tables Generator

Private Set Intersection

Applications

- Private Personal Genomics
- Private AES Encryption
- Private Set Intersection

Privacy-Preserving Biometric Matching

Private Set Intersection

- Do Alice and Bob have any contacts in common?
- Two countries want to compare their miscreant lists
- Identify common medical records across hospitals
- Two companies want to do joint marketing to common customers
**Sort-Compare-Shuffle**

- **Sort**: Take advantage of total order of elements
- **Compare**: Compare adjacent elements
- **Shuffle**: Shuffle to hide positions

**Private Set Intersection Protocol**

Gates to generate and evaluate

- **Free**
- **Bitonic Sorting Circuit**: \( n \log(2n) \times 2\sigma \)
- **Waksman Permutation Network**: \( (3\sigma - 1)(n-1) + (2\sigma - 1) \)
- **\( n \log n - n + 1 \)**

**Private Set Intersection Results**

- **Seconds vs. Set Size (each set)**
- **32-bit values**

<table>
<thead>
<tr>
<th>Problem</th>
<th>Best Previous Result</th>
<th>Our Result</th>
<th>Speedup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hamming Distance (Face Recognition) – 900-bit vectors</td>
<td>213s [SCiFI, 2010]</td>
<td>0.051s</td>
<td>4176</td>
</tr>
<tr>
<td>Levenshtein Distance (genome, text comparison) – two 200-character inputs</td>
<td>534s [Jha+, 2008]</td>
<td>18.4s</td>
<td>29</td>
</tr>
<tr>
<td>Smith-Waterman (genome alignment) – two 60-nucleotide sequences</td>
<td>[Not Implementable]</td>
<td>447s</td>
<td>-</td>
</tr>
<tr>
<td>AES Encryption</td>
<td>3.3s [Henecka, 2010]</td>
<td>0.2s</td>
<td>16.5</td>
</tr>
<tr>
<td>Fingerprint Matching (1024-entry database, 640x8bit vectors)</td>
<td>~83s [Barni, 2010]</td>
<td>18s</td>
<td>4.6</td>
</tr>
</tbody>
</table>

**Some Other Results**

<table>
<thead>
<tr>
<th>Problem</th>
<th>Best Previous Result</th>
<th>Our Result</th>
<th>Speedup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scalable: 1 Billion gates evaluated at ~100,000 gates/second on laptop</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Collaborators**

- **Yan Huang** (UVa PhD Student)
- **Yikan Chen** (UVa PhD Student)
- **Samee Zahur** (UVa MS Student)
- **Peter Chapman** (UVa BACS Student)
- **Jonathan Katz** (University of Maryland)
- **Aaron Mackey** (UVa Public Health Genomics)

**David Evans**

- evans@cs.virginia.edu
- http://www.cs.virginia.edu/evans