Secure Computations

Valeria Nikolaenko
Security Lunch
Examples:
- Billionaires problem
- Voting/Elections
- Sealed-bid auctions
  - Sugar beet auctions (Denmark)
  - Auction for the Norwegian Postal and Telecommunications authority
  - Solution for trading "energy saving projects"
- Face recognition
- Dynamic password authentication

Companies:
- Cybernetica [http://sharemind.cyber.ee/](http://sharemind.cyber.ee/)
- Particia [http://www.partisia.dk](http://www.partisia.dk)
- ... etc
Dynamic password verification

• User has Security Token with key $K$ hardwired

• Security Token computes and displays $psw = AES_{K}(\text{time stamp})$

• User sends $psw$

• Server computes $AES_{K}(\text{time stamp})$ and compares

Since PSSW'09 became common to benchmark MPC against single block AES
Progress over time

Single block of AES

<table>
<thead>
<tr>
<th>Year</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td>7 sec</td>
</tr>
<tr>
<td>2013</td>
<td>0.012 sec</td>
</tr>
</tbody>
</table>

10³ improvement

FHE: 36 hours

FHE: HUGE computation, little communication
MPC: little computation, LARGE communication
History

MPC parameters:
1. Total number of parties & number of malicious parties
2. Run-time: offline phase, online phase, amortized cost
3. Total amount of communication & number of rounds
4. Assumptions

FOCS’86 Yao-protocol
• Computationally secure against any number of malicious parties
• # rounds = constant

STOC’87 GMW-protocol
• Computationally secure against any number of malicious parties
• # rounds = depth

STOC’88 BGW-protocol
• Unconditionally secure with honest majority
• # rounds = depth
## State of the art

<table>
<thead>
<tr>
<th></th>
<th>Throughput (ops per sec)</th>
<th>32-bit Integer Mult</th>
<th>2500</th>
<th>Intel 4004 did 46000 per sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comparison</td>
<td>800000</td>
<td>≈ 386 performance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32-bit Integer Mult</td>
<td>2500</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Addition</td>
<td>50</td>
<td>ENIAC did 384 FLOPS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Floating point Mult</td>
<td>100</td>
<td>ENIAC did 384 FLOPS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Nigel Smart Google Tech Talk on SPDZ system
Frameworks

- **FastGC**
  - Framework
  - University of Virginia & University of Mariland (USA)
  - Semi-honest Yao
  - [http://mightbeevil.org/](http://mightbeevil.org/)

- **Tasty**
  - Compiler
  - Ruhr-University Bochum (Germany)
  - Semi-honest Yao + HE
  - [https://code.google.com/p/tastyproject/](https://code.google.com/p/tastyproject/)

- **SAPI**
  - Framework, tools for MPC
  - Bar-Ilan University (Israel)
  - [http://crypto.biu.ac.il/about-sapi.php](http://crypto.biu.ac.il/about-sapi.php)

- **SEPIA**
  - Network monitoring system
  - ETH Zurich (Switzerland)
  - Semi-honest secret sharing
  - [http://sepia.ee.ethz.ch/](http://sepia.ee.ethz.ch/)

- **KSS12**
  - Compiler
  - University of Virginia (USA)
  - Malicious Yao

- **Sharemind**
  - Compiler, SDK
  - Cybernetica (Estonia)
  - Combination of techniques, semi-honest
  - [http://sharemind.cyber.ee/](http://sharemind.cyber.ee/)

- **VIFF**
  - Framework
  - University of Aarhus (Denmark)
  - Semi-honest secret sharing
  - [http://viff.dk/](http://viff.dk/)

- **SEPIA**
  - Network monitoring system
  - ETH Zurich (Switzerland)
  - Semi-honest secret sharing
  - [http://sepia.ee.ethz.ch/](http://sepia.ee.ethz.ch/)

- **CBMC-GC**
  - ANSI-C compiler
  - Vienna University of Technology (Austria)
  - Semi-honest Yao
  - [http://forsyte.at/software/cbmc-gc/](http://forsyte.at/software/cbmc-gc/)

- **PICCO**
  - C compiler
  - University of Notre Dame (USA)
  - Semi-honest secret sharing
  - [https://code.google.com/p/pico-compiler/](https://code.google.com/p/pico-compiler/)

- **SPDZ**
  - Commercial software, compiler for Python-like code
  - University of Bristol (UK)
  - Malicious secret sharing + HE
  - ...
Computational model

Why circuit?
- Work flow is data-independent

Are there other models?
- Yes
- Example: multiparty-quick-sort
  - Shuffle inputs
  - For each swap in quick sort, do:
    - securely compute and reveal comparisons
    - swap, repeat

\[
\begin{align*}
f(b, x_1, x_2) &= \text{RAM} \\
&= \begin{cases} 
  x_1 + x_2 & \text{if } (b == 0) \\
  x_1 \cdot x_2 & \text{else}
\end{cases} \\
&= b \cdot x_1 \cdot x_2 + (1 - b) \cdot (x_1 + x_2)
\end{align*}
\]
1. Sorting Networks  (late 60’s)

\[(a_1, a_2, \ldots, a_M) \rightarrow (a_1' \leq a_2' \leq \ldots \leq a_M')\]

\[a_1 \rightarrow a_1' = \min(a_1, a_2)\]
\[a_2 \rightarrow a_2' = \max(a_1, a_2)\]

Compare-and-Swap circuit

Usual sort \(O(n \log n)\)
AKS sorting network \(O(n \log n)\)
Batcher, or Bitonic \(O(n \log^2 n)\)
1. Sorting Networks (late 60’s)
2. Private sets intersection
   Weighted sets intersection
   Geometric algorithms: convex hull on the union of the points
3. Data structures: queues, stacks, associative maps, priority queues
4. Complex numerical tasks:
Privacy preserving Data-Mining

Users

Data model

f(data, data, data, ⬤) = DM(Dec(data, ⬤), ..., Dec(data, ⬤))

2 parties MPC

Trusted Party
Matrix Factorization

\[ r_{ij} \approx \langle u_i, v_j \rangle \]

\[
(U, V) = \arg \min_{U,V} \frac{1}{M} \sum_{(i,j) \in R} (r_{ij} - \langle u_i, v_j \rangle)^2
\]

\( u_i \) – profile of user \( i \), \( v_j \) – profile of item \( j \)
Designing Circuit

\[(i, j, r_{ij})_{ij \in R}\]

Gradient Update Layer:

\[\begin{align*}
F & \text{or } i = 1 \ldots n, \quad j = 1 \ldots m, \quad t = 0, \ldots, K \\
\mathbf{u}_i^t &= \mathbf{u}_i^{t-1} + \gamma \cdot \sum_{(i, j) \in R} \mathbf{u}_i \left( r_{ij} - \langle \mathbf{u}_i, \mathbf{v}_j \rangle \right) \\
\mathbf{v}_j^t &= \mathbf{v}_j^{t-1} + \gamma \cdot \sum_{(i, j) \in R} \mathbf{v}_j \left( r_{ij} - \langle \mathbf{u}_i, \mathbf{v}_j \rangle \right)
\end{align*}\]

Naively: quadratic time
Our approach: linear up to \(\log^2\) factor
Key idea: use sorting networks
Performance

• Our system:
  • 15,000 ratings – 1.5 days on 1.9GHz 16 cores, 128GB RAM commodity servers
  • Running time: $O(M \log^2 M)$, where $M$ – number of ratings
  • Highly parallelizable
  • Practical for moderate size databases

• In real world:
  • MF is run once a week
  • IMDB database: ~ 10 million ratings
QUESTIONS
FOUND IN GOOGLE AUTOCOMPLETE

WHY ARE THERE PSYCHICS?
WHY ARE HATS SO EXPENSIVE?
WHY IS THERE COFFEE IN MY SHAMPOO?
WHY DO YOUR BOOBS HURT?
WHY ARE AMERICANS AFRAID OF DRAGONS?
WHY ARE THERE SLAVES IN THE BIBLE?
WHY DO TWINS HAVE DIFFERENT FINGERTIPS?
WHY IS HTTPS CROSSED OUT IN RED?
WHY IS THERE A LINE THROUGH HTTPS ON FACEBOOK?
WHY IS HTTPS IMPORTANT?
WHY AREN'T MY ARMS GROWING?
WHY ARE THERE 8 SUMS OF DAYS?
WHY IS THERE POLIOMYELITIS?
WHY ARE THERE SO MANY CROWS IN ROCHESTER, MN?
WHY AREN'T ECONOMISTS RICH?
WHY ARE MUSSELS CALLED CLAMS?
WHY ARE MY EARS RINGING?
WHY ARE THERE SO MANY AVENGERS?
WHY ARE THE AVENGERS FIGHTING THE X-MEN?
WHY IS WOLVERINE NOT IN THE AVENGERS?
WHY AREN'T THERE DINOSAURS?
WHY ARE THERE CELEBRITIES?
WHY DO SNAKES EXIST?
WHY DO OYSTERS HAVE PEARLS?
WHY ARE DUCKS CALLED DUCKS?
WHY DO THEY CALL IT THE CLAP?
WHY ARE KYLE AND CARTMAN FRIENDS?
WHY IS THERE AN ARROW ON AANG'S HEAD?
WHY ARE TEXT MESSAGES BLUE?
WHY ARE THERE MUSTACHES ON CLOTHES?
WHY ARE THERE MUSTACHES ON CARS?
WHY ARE THERE SO MANY BIRDS IN OHIO?
WHY IS THERE SO MUCH RAIN IN OHIO?
WHY IS OHIO WEATHER SO WEIRD?
WHY ARE THERE MALE AND FEMALE BIKES?
WHY ARE THERE BRIDESMAIDS?
WHY DO DYING PEOPLE DANCE UPSTAIRS?
WHY ARE OLD KUNG FUS DIFFERENT?
WHY ARE THERE TINY SPIDERS IN MY HOUSE?
WHY DO SPIDERS COME INSIDE?
WHY ARE THERE HANGING SPIDERS IN MY HOUSE?
WHY ARE THERE TONS OF SPIDERS IN MY HOUSE?
WHY ARE THERE SPIDERS IN MY ROOM?
WHY ARE THERE SO MANY SPIDERS IN MY ROOM?
WHY DO SPIDER BITES ITCH?
WHY IS MT. VESUVIUS THERE?
WHY DO THEY SAY T MINUS?
WHY ARE THERE AN OWL IN MY BACKYARD?
WHY IS THERE AN OWL OUTSIDE MY WINDOW?
WHY IS THERE AN OWL ON THE DOLLAR BILL?
WHY DO OWLS ATTACK PEOPLE?
WHY ARE AK 47S SO EXPENSIVE?
WHY ARE THERE HELICOPTERS CIRCLING MY HOUSE?
WHY ARE THERE GODS?
WHY ARE CIGARETTES LEGAL?
WHY ARE THERE DUCKS IN MY POOL?
WHY IS JESUS WHITE?
WHY IS THERE LIQUID IN MY EAR?
WHY DO Q TIPS FEEL GOOD?