BLAZE: BLAZING FAST PRIVACY-PRESERVING
MACHINE LEARNING

ARPITA PATRA AND AJITH SURESH

Ajith Suresh
CrlS Lab, IISc
https://www.csa.iisc.ac.in/~cris
Outline

- Secure Multi-party Computation (MPC)
- MPC for small number of parties (3PC)
- Our Efficient BLAZE Protocol (Results)
- Privacy Preserving Machine Learning (PPML)
Secure Multi-party Computation (MPC) [Yao’82]

✓ A set of parties with private inputs wish to compute some joint function of their inputs.

✓ Goals of MPC:
  - **Correctness** – Parties should correctly evaluate the function output.
  - **Privacy** – Nothing more than the function output should be revealed
Secure Multi-party Computation (MPC) \cite{Yao82}

✓ A set of parties with private inputs wish to compute some joint function of their inputs.

✓ Goals of MPC:
  - **Correctness** – Parties should correctly evaluate the function output.
  - **Privacy** – Nothing more than the function output should be revealed
Secure Multi-party Computation (MPC) [{Yao’82}]

✓ A set of parties with private inputs wish to compute some joint function of their inputs.

✓ Goals of MPC:
  - **Correctness** – Parties should correctly evaluate the function output.
  - **Privacy** – Nothing more than the function output should be revealed
Secure Multi-party Computation (MPC) [Yao’82]

A set of parties with private inputs wish to compute some joint function of their inputs.

Goals of MPC:
- **Correctness** – Parties should correctly evaluate the function output.
- **Privacy** – Nothing more than the function output should be revealed
Secure Multi-party Computation (MPC) [Yao’82]

• Semi – honest:
  • Follows the protocol but tries to learn more

• Malicious:
  • Can arbitrarily deviate from the protocol
Secure Multi-party Computation (MPC) [Yao’82]

ADVERSARY

- Semi – honest:
  - Follows the protocol but tries to learn more

- Malicious:
  - Can arbitrarily deviate from the protocol

Malicious Corruption
MPC for small number of parties

- **Efficiency and Simplicity** [MRZ15, AFLNO16, FLNW17, CGMV17]
MPC for small number of parties

- **Efficiency** and **Simplicity** [MRZ15,AFLNO16,FLNW17,CGMV17]

- Our focus: MPC with 3 parties
MPC for small number of parties

- **Efficiency and Simplicity** ([MRZ15, AFLNO16, FLNW17, CGMV17])

- Our focus: MPC with 3 parties

- Corruption: honest majority
MPC for small number of parties

- **Efficiency and Simplicity** [MRZ15, AFLNO16, FLNW17, CGMV17]

- Our focus: MPC with 3 parties

- Corruption: honest majority
  - Majority of the parties are honest
  - 3PC - at most 1 corruption
MPC for small number of parties

- **Efficiency and Simplicity** [MRZ15, AFLNO16, FLNW17, CGMV17]
- Our focus: MPC with 3 parties
- Corruption: honest majority
- Outsourced Computation
MPC for small number of parties

- **Efficiency** and **Simplicity** [MRZ15,AFLNO16,FLNW17,CGMV17]
- Our focus: MPC with 3 parties
- Corruption: honest majority
- Outsourced Computation
- Pre-processing Model
MPC for small number of parties

- **Efficiency** and **Simplicity** [MRZ15, AFLNO16, FLNW17, CGMV17]

- Our focus: MPC with 3 parties

- Corruption: honest majority

- Outsourced Computation

- Pre-processing Model
  - Pre-processing phase
MPC for small number of parties

- **Efficiency and Simplicity** [MRZ15,AFLNO16,FLNW17,CGMV17]

- Our focus: MPC with 3 parties

- Corruption: honest majority

- Outsourced Computation

- Pre-processing Model
  - Pre-processing phase
    - Data-independent Computation
    - Relatively slow and expensive
MPC for small number of parties

- **Efficiency and Simplicity** \([\text{MRZ15, AFLNO16, FLNW17, CGMV17}]\)

- Our focus: MPC with 3 parties

- Corruption: honest majority

- Outsourced Computation

- Pre-processing Model
  - Pre-processing phase
  - Online Phase
MPC for small number of parties

- **Efficiency** and **Simplicity** \[MRZ15,AFLNO16,FLNW17,CGMV17\]

- Our focus: MPC with 3 parties

- Corruption: honest majority

- Outsourced Computation

- Pre-processing Model
  - Pre-processing phase
  - Online Phase

- Minimized communication
- Blazing fast
BLAZE PROTOCOL
BLAZE Protocol

$S_0$

$S_1$

$S_2$
BLAZE Protocol

$S_0$

$S_1$

$S_2$
BLAZE Protocol

\[ S_0 \]

\[ S_1 \]

\[ S_2 \]
BLAZE Protocol

$S_0$

$S_1$

$S_2$
BLAZE Protocol

$S_0$

$S_1$

$S_2$
BLAZE Protocol

$S_0$

$S_1$

$S_2$
BLAZE Protocol

Communication Cost per Multiplication Gate (malicious)

BLAZE: [https://eprint.iacr.org/2020/042](https://eprint.iacr.org/2020/042)

Mult: x \cdot y
### BLAZE Protocol

<table>
<thead>
<tr>
<th>Ref</th>
<th>Pre-processing (#elements)</th>
<th>Online (#elements)</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Araki et al’17</td>
<td>12</td>
<td>9</td>
<td>Abort</td>
</tr>
</tbody>
</table>

#### Communication Cost per Multiplication Gate (malicious)

*BLAZE*: [https://eprint.iacr.org/2020/042](https://eprint.iacr.org/2020/042)

*Multi*: \(x \cdot y\)
### BLAZE Protocol

<table>
<thead>
<tr>
<th>Ref</th>
<th>Pre-processing (#elements)</th>
<th>Online (#elements)</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Araki et al’17</td>
<td>12</td>
<td>9</td>
<td>Abort</td>
</tr>
<tr>
<td>ASTRA</td>
<td>21</td>
<td>4</td>
<td>Fair</td>
</tr>
</tbody>
</table>

**Communication Cost per Multiplication Gate (malicious)**

\[ \text{Mult: } x \cdot y \]

BLAZE: [https://eprint.iacr.org/2020/042](https://eprint.iacr.org/2020/042)
### BLAZE Protocol

<table>
<thead>
<tr>
<th>Ref</th>
<th>Pre-processing (#elements)</th>
<th>Online (#elements)</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Araki et al’17</td>
<td>12</td>
<td>9</td>
<td>Abort</td>
</tr>
<tr>
<td>ASTRA</td>
<td>21</td>
<td>4</td>
<td>Fair</td>
</tr>
<tr>
<td>Boneh et al’19</td>
<td>0</td>
<td>3</td>
<td>Abort</td>
</tr>
</tbody>
</table>

**Communication Cost per Multiplication Gate (malicious)**

Mult: $x \times y$

BLAZE: [https://eprint.iacr.org/2020/042](https://eprint.iacr.org/2020/042)
### BLAZE Protocol

<table>
<thead>
<tr>
<th>Ref</th>
<th>Pre-processing (#elements)</th>
<th>Online (#elements)</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Araki et al’17</td>
<td>12</td>
<td>9</td>
<td>Abort</td>
</tr>
<tr>
<td>ASTRA</td>
<td>21</td>
<td>4</td>
<td>Fair</td>
</tr>
<tr>
<td>Boneh et al’19</td>
<td>0</td>
<td>3</td>
<td>Abort</td>
</tr>
<tr>
<td><strong>BLAZE</strong></td>
<td><strong>3</strong></td>
<td><strong>3</strong></td>
<td><strong>Fair</strong></td>
</tr>
</tbody>
</table>

**Communication Cost per Multiplication Gate (malicious)**

BLAZE: [https://eprint.iacr.org/2020/042](https://eprint.iacr.org/2020/042)
Privacy Preserving Machine Learning (PPML)

Alice (Model Owner)

Model Parameters

ML Algorithm

Query

Result

Bob (Client)

Privacy ??
Privacy Preserving Machine Learning (PPML)

Alice
(Model Owner)

Bob
(Client)

ML Algorithm

Query

Result

Query

Model Parameters
Privacy Preserving Machine Learning (PPML)

Alice (Model Owner) → Model Parameters → ML Algorithm → Query → Result → Bob (Client)

Model Parameters
Solution ??

ML

MPC
MPC MEETS ML
Privacy Preserving Machine Learning (PPML)

Alice (Model Owner) → MPC → Bob (Client)

Model Parameters → Query → Result

Use MPC to achieve privacy
SECURE OUTSOURCED SETTING (SOC)

Alice (Model Owner)  →  MLaaS (3PC Servers)  →  Bob (Client)

Model Parameters  →  Query  →  Result
ML ALGORITHMS CONSIDERED

Linear Regression

Logistic Regression

Neural Networks

ML ALGORITHMS CONSIDERED

AJITH SURESH | CRYPTOGRAPHY AND INFORMATION SECURITY LAB, CSA, IISC

26-02-2020
Secure Dot Product

PPML using MPC: Hurdles to Clear
PPML using MPC: Hurdles to Clear

Secure Comparison

Secure Dot Product
PPML using MPC: Hurdles to Clear

- Secure Dot Product
- Embedding Floating point Numbers
- Secure Comparison
PPML using MPC: Hurdles to Clear

- Single bit to Arithmetic Value
- Secure Dot Product
- Embedding Floating point Numbers
- Secure Comparison
PPML using MPC: Hurdles to Clear

- Secure Dot Product
- Truncation
- Single bit to Arithmetic Value
- Secure Comparison
- Embedding Floating point Numbers
PPML using MPC: Hurdles to Clear

- Secure Dot Product
- Secure Comparison
- Embedding Floating point Numbers
- Single bit to Arithmetic Value
- Truncation
- Non-linear Activation Functions
PPML using MPC: Hurdles to Clear

- Secure Dot Product
- Secure Comparison
- Embedding Floating point Numbers
- Single bit to Arithmetic Value
- Truncation
- Non-linear Activation Functions

and many more...
## BLAZE Protocol

<table>
<thead>
<tr>
<th>Ref</th>
<th>Pre-processing (#elements)</th>
<th>Online (#elements)</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABY3</td>
<td>12d</td>
<td>9d</td>
<td>Abort</td>
</tr>
</tbody>
</table>

### Communication Cost per Dot Product

\[
X \bullet Y = \sum_{i=1}^{d} x_i \cdot y_i
\]

- \(d\) – #elements in each vector

---

BLAZE: [https://eprint.iacr.org/2020/042](https://eprint.iacr.org/2020/042)
## BLAZE Protocol

<table>
<thead>
<tr>
<th>Ref</th>
<th>Pre-processing (#elements)</th>
<th>Online (#elements)</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABY3</td>
<td>12d</td>
<td>9d</td>
<td>Abort</td>
</tr>
<tr>
<td>ASTRA</td>
<td>21d</td>
<td>2d+2</td>
<td>Fair</td>
</tr>
</tbody>
</table>

### Communication Cost per Dot Product

\[
X \diamond Y = \sum_{i=1}^{d} x_i \cdot y_i
\]

\(d\) – #elements in each vector

---

BLAZE: [https://eprint.iacr.org/2020/042](https://eprint.iacr.org/2020/042)
## BLAZE Protocol

<table>
<thead>
<tr>
<th>Ref</th>
<th>Pre-processing (#elements)</th>
<th>Online (#elements)</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABY3</td>
<td>12d</td>
<td>9d</td>
<td>Abort</td>
</tr>
<tr>
<td>ASTRA</td>
<td>21d</td>
<td>2d+2</td>
<td>Fair</td>
</tr>
<tr>
<td>Boneh et al’19*</td>
<td>0</td>
<td>3d</td>
<td>Abort</td>
</tr>
</tbody>
</table>

### Communication Cost per Dot Product

\[ X \mathbin{\square} Y = \sum_{i=1}^{d} x_i \cdot y_i \]

\( d \) – #elements in each vector
**BLAZE Protocol**

<table>
<thead>
<tr>
<th>Ref</th>
<th>Pre-processing (#elements)</th>
<th>Online (#elements)</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABY3</td>
<td>12d</td>
<td>9d</td>
<td>Abort</td>
</tr>
<tr>
<td>ASTRA</td>
<td>21d</td>
<td>2d+2</td>
<td>Fair</td>
</tr>
<tr>
<td>Boneh et al’19*</td>
<td>0</td>
<td>3d</td>
<td>Abort</td>
</tr>
<tr>
<td><strong>BLAZE</strong></td>
<td><strong>3d</strong></td>
<td><strong>3</strong></td>
<td><strong>Fair</strong></td>
</tr>
</tbody>
</table>

**Communication Cost per Dot Product**

\[ X \mathbin{\boxtimes} Y = \sum_{i=1}^{d} x_i \cdot y_i \]

\[ d = \text{#elements in each vector} \]

BLAZE: [https://eprint.iacr.org/2020/042](https://eprint.iacr.org/2020/042)
## Summary of Our Benchmarking Results

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Improvement in terms of Online Throughput over State-of-the-art protocols over WAN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Training</td>
</tr>
<tr>
<td>Linear Regression</td>
<td>333.22 x</td>
</tr>
<tr>
<td>Logistic Regression</td>
<td>53.19 x</td>
</tr>
<tr>
<td>Neural Networks</td>
<td>*</td>
</tr>
</tbody>
</table>

*Throughput for Training - #iterations processed by servers / minute

*Throughput for Prediction - #queries processed by servers / minute
### Summary of Our Benchmarking Results

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Ref.</th>
<th>Preprocessing</th>
<th>Online</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>TP</td>
<td>Gain</td>
</tr>
<tr>
<td>Linear Regression</td>
<td>ABY3</td>
<td>61.02</td>
<td>4.01×</td>
</tr>
<tr>
<td></td>
<td>BLAZE</td>
<td>244.74</td>
<td></td>
</tr>
<tr>
<td>Logistic Regression</td>
<td>ABY3</td>
<td>60.71</td>
<td>4.02×</td>
</tr>
<tr>
<td></td>
<td>BLAZE</td>
<td>243.81</td>
<td></td>
</tr>
</tbody>
</table>

**TABLE VI:** Throughput (TP) for ML Training for a batch size B-128 and feature size n-784

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Ref.</th>
<th>Preprocessing</th>
<th>Online</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>TP (×10³)</td>
<td>Gain</td>
</tr>
<tr>
<td>Linear Regression</td>
<td>ABY3</td>
<td>15.57</td>
<td>4.02×</td>
</tr>
<tr>
<td></td>
<td>BLAZE</td>
<td>62.61</td>
<td></td>
</tr>
<tr>
<td>Logistic Regression</td>
<td>ABY3</td>
<td>15.41</td>
<td>4.03×</td>
</tr>
<tr>
<td></td>
<td>BLAZE</td>
<td>62.13</td>
<td></td>
</tr>
<tr>
<td>Neural Networks</td>
<td>ABY3</td>
<td>0.10</td>
<td>4.01×</td>
</tr>
<tr>
<td></td>
<td>BLAZE</td>
<td>0.41</td>
<td></td>
</tr>
</tbody>
</table>

**TABLE VII:** Throughput (TP) for ML Inference for a feature size of n-784
THANK YOU!
References