Transputation: Transport framework for secure computation

Markus Brandt, Claudio Orlandi, Kris Shrishak, Haya Shulman
Secure Computation

Alice and Bob
.. have **private inputs**
.. want to **jointly compute a function**
.. reveal the **output** and **nothing more**
Secure 2PC setting in this talk

- Yao’s garbled circuits: Constant round
- Passive security
- Concrete efficiency
1 Bandwidth – bottleneck?

- Computation time has significantly reduced due to
  - Circuit optimizations
  - Hardware support for cryptography
- 2PC based on garbled circuits have reached the theoretical lower bound [ZRE15]
- Bandwidth is believed to be the main bottleneck
- Bandwidth is underutilized.
- TCP sockets are used in all
  - secure computation implementations
  - network settings
2 Why not use other transport protocols?

- Hard to integrate transport protocols to the application
- One-size does not fit all
- Depends on
  - Circuit size
  - Size of inputs
  - Network conditions
3 The problem with evaluations

- Do not reflect real world complexities
- Performance measured in ideal settings
- Extra work to setup realistic evaluation testbed
Transputation Framework
Transputation Framework

- Automates the usage and integration of transport layer protocols into secure computation implementations.

- Modular design
  - Separates program logic from network code
  - Allows extension with other secure computation protocols
  - Easy to extend with new transport protocols
2PC Layer

- PRF assumption [GLNP15]
  - 4-2 Garbled-row-reduction + XOR-1

- Circular related key assumption [ZRE15]
  - Free-XOR + Half-gates

- Ideal cipher assumption [BHKR13]
  - Fixed-Key AES + Free-XOR + Half-gates

<table>
<thead>
<tr>
<th>Assumption</th>
<th>AES</th>
<th>SHA256</th>
<th>MinCut</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRF</td>
<td>0.59</td>
<td>3.41</td>
<td>69.04</td>
</tr>
<tr>
<td>Circular</td>
<td>0.21</td>
<td>2.77</td>
<td>30.52</td>
</tr>
<tr>
<td>Ideal cipher</td>
<td>0.21</td>
<td>2.77</td>
<td>30.52</td>
</tr>
</tbody>
</table>

Garbled circuit size in MB
Transport Layer: Basics

- End-to-end communication between the applications on different hosts
- Sender: Segments data received from the application
- Receiver: Reassembles segments into messages
Transport Layer

Principles
- Reliability
- Flow control
- Congestion control
- Fairness

Protocol selection
- Latency
- Bandwidth
- Packet Loss
Transport Layer Protocols

- **TCP**
  - Reliable but poor bandwidth utilization
  - Reacts on packet-level events (ACK)
  - Transmission rate controlled with additive increase multiplicative decrease (AIMD) algorithm

- **UDP**
  - Unreliable
Transport Layer Protocols

UDT

- UDP-based data transfer protocol
- Reliability added at the application layer
- Timer-based congestion control
- Loss indicated with Negative ACK (NACK)
- Uses Decreasing AIMD algorithm.
Evaluation Testbed

- Distributed evaluation setup tailored for 2PC
- Supports various transport protocols
- Allows 2PC developers to perform real life evaluations
Evaluations:
Latency

AES

MinCut

SHA256
Evaluations:
Packet loss

SHA256

MinCut
Evaluations:
Bandwidth

AES

MinCut

SHA256
## Evaluation results

<table>
<thead>
<tr>
<th>Circuit</th>
<th>Setting</th>
<th>Ideal cipher</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>TCP</td>
<td>UDT</td>
<td>TCP</td>
<td>UDT</td>
<td>TCP</td>
<td>UDT</td>
<td>TCP</td>
<td>UDT</td>
<td></td>
</tr>
<tr>
<td>AES</td>
<td>LAN</td>
<td>2.4</td>
<td>187.1</td>
<td>2.9</td>
<td>191.3</td>
<td>7</td>
<td>202.7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EU-US</td>
<td>127.4</td>
<td>403.9</td>
<td>126.3</td>
<td>408.3</td>
<td>130.4</td>
<td>444.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EU-AUS</td>
<td>312.44</td>
<td>566.84</td>
<td>310.88</td>
<td>580.2</td>
<td>377.92</td>
<td>592.5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA256</td>
<td>LAN</td>
<td>13.5</td>
<td>191.9</td>
<td>19.9</td>
<td>226.7</td>
<td>30.5</td>
<td>233.45</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EU-US</td>
<td>146.23</td>
<td>332.24</td>
<td>151.99</td>
<td>318.26</td>
<td>266.46</td>
<td>411.96</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EU-AUS</td>
<td>362.53</td>
<td>568.22</td>
<td>394.13</td>
<td>587.03</td>
<td>650.44</td>
<td>612.43</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MinCut</td>
<td>LAN</td>
<td>255.19</td>
<td>598.2</td>
<td>267.2</td>
<td>740.2</td>
<td>700.8</td>
<td>1255.9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EU-US</td>
<td>2616.59</td>
<td>896.74</td>
<td>2783.6</td>
<td>957.6</td>
<td>4911.89</td>
<td>1802.25</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EU-AUS</td>
<td>8204.61</td>
<td>1068.07</td>
<td>8693.57</td>
<td>1163.14</td>
<td>13805.2</td>
<td>2001.27</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Garbled circuit size
Comparison for different assumptions
Future Work

- Active security
- MPC
- Custom transport protocol for specific applications
Thank you
References

Efficient Garbling from a Fixed-Key Blockcipher, S&P 2013

Fast garbling of circuits under standard assumptions, CCS 2015

[ZRE15] Samee Zahur, Mike Rosulek, and David Evans.
Two halves make a whole - reducing data transfer in garbled circuits using half gates, EUROCRYPT 2015