Practical Secure Function Evaluation

Diplomarbeit of Thomas Schneider, Supervision: Prof. V. Strehl and V. Kolesnikov, PhD
{thomas.schneider@informatik.stud, strehl@informatik.uni-erlangen.de, kolesnikov@research.bell-labs.com}

Contents and Contributions of this Thesis:

Summary and comparison of known SFE protocols with different representations of the boolean function f as boolean circuit or ordered binary decision diagram (OBDD).

Extension of OBDD-based SFE protocol [KJGB06] (secure in semi-honest model) to malicious model and OBDD-based PF-SFE protocol with small overhead.

PF-SFE can be reduced to SFE of a Universal Circuit (UC) that can be programmed to compute any function f of size k gates. Our practical UC construction* [KS08] is up to 50% smaller than the best UC of Valiant [Val76] when used in today’s PF-SFE.

Our improved SFE protocol* allows free evaluation of XOR gates:
- Based on SFE protocols Fairplay [MNPS04] & GESS [Kol05].
- Improves many important functions (e.g. addition, equality test) to 50%.
- UC-based PF-SFE protocols can be improved to even 25%.

Implementation of FairplayPF, an extension of the well-known Fairplay SFE system for practical PF-SFE. http://thomas.schneider.de/FairplayPF

Bibliography


Secure Function Evaluation (SFE) allows two parties Alice and Bob to securely evaluate a function f(u,v) on their private inputs u and v:
- each party learns the result z = f(x,y)
- each party learns nothing about the other party’s secret y resp. x

Secure Function Evaluation of Private Functions (PF-SFE) - same as SFE with additionally f being private:
- f is known by Bob only
- Alice learns nothing about f (besides size, #inputs and #outputs)

Practical Examples:
- Millionaires Problem (Maximum)
- Auctions
- Voting
- Keyed Database Search
- ...

Evaluation Speed

<table>
<thead>
<tr>
<th>Function Represent.</th>
<th>SFE Protocol</th>
<th>Proof of Security</th>
<th>Evaluation Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Semi-honest</td>
<td>Malicious</td>
</tr>
<tr>
<td>Circuit</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Yao [Yao86]         | Fairplay [MNPS04] | X| X | X | slow (Encry.).
| GESS [Kol05]        | improved SFE | X | X | X | medium (H) |
| OBDD                | OBDD SFE [KJGB06] | X | X | X | slow (Encry. fast) |
|                    | improved OBDD SFE | X | X | X | fast (E) |

Implementation of FairplayPF, an extension of the well-known Fairplay SFE system for practical PF-SFE. http://thomas.schneider.de/FairplayPF

Bibliography


