Enabling the Aviation CO₂ Allowance Trading Through Secure Market Mechanisms

Massimiliano Zanin
mz@innaxis.org
Problem:

Computing without trust

- Airlines benchmarking
- Airport slot trading
- CO₂ allowance trading
- Data mining on safety data
- Safety benchmarking
- ...

Secure CO₂ allowance trading :: Introduction
Secure CO\textsubscript{2} allowance trading :: Introduction

Problem:

SWIM, the solution?

SWIM, information transfer enabler

Based on a public-key infrastructure

privacy as good as the privacy of the worst procedure implemented by the entities

Back to the starting point!
Problem:

CO₂ allowance trading

Increasing air traffic = increasing CO₂ emissions

Emission trading or cap and trade
Problem: Emission trading or cap and trade

Upper limit to the amount of pollutants that can be emitted Rights to emit, to be traded in a specific market.

More emissions: buy additional rights
Less emissions: rights can be sold in the market

Efficient emissions reduction through a market mechanism, as green companies are receiving indirect incentives.
Problem:

*Emission trading* or *cap and trade*

$\text{CO}_2$ emissions $\propto$ fuel consumption $\propto$ take-off weight

Fairness of the trading system
Secure Multi-party Computation (SMC)

Subfield of cryptography.

Methods for parties to jointly compute a function over their inputs, while keeping these inputs private.

Andrew C. Yao, 1982: the millionaire problem

Andrew Chi-Chih Yao
Objectives:

Introduce SMC into Air Transport
Software Reference Framework
Simulation and analysis of two Case Studies
# Secure \( CO_2 \) allowance trading

## Introduction

**\( CO_2 \) allowance trading**

<table>
<thead>
<tr>
<th>Primary market</th>
<th>Secondary market</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Seller:</strong></td>
<td><strong>Industry</strong></td>
</tr>
<tr>
<td><strong>Buyers:</strong></td>
<td><strong>One or more airlines</strong></td>
</tr>
<tr>
<td><strong>Seller’s input data:</strong></td>
<td><strong>Minimum price</strong></td>
</tr>
<tr>
<td><strong>Buyers’ input data:</strong></td>
<td><strong>Bid</strong></td>
</tr>
<tr>
<td><strong>Result:</strong></td>
<td><strong>Max bid, ( iif ) bid &gt; minimum price</strong></td>
</tr>
</tbody>
</table>
Secure CO₂ allowance trading :: Introduction
Secure CO₂ allowance trading :: An example

Secure auction

Secure ranking

Secure evaluation of $a > b$
Secure CO\textsubscript{2} allowance trading :: An example

Secure evaluation of $a > b$

\begin{align*}
00000047859283759201 \\
00000057483928374627
\end{align*}

1. Find the first non-equal digit
2. Compare them for $a > b$
<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
<th>$P_1$</th>
<th>$P_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secret number:</td>
<td>Secret number:</td>
<td>Secret number:</td>
<td>Secret number:</td>
</tr>
<tr>
<td>[0 0 1]</td>
<td>[0 1 0]</td>
<td>$a$</td>
<td>$b$</td>
</tr>
</tbody>
</table>
## Secure CO₂ allowance trading :: An example

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
<th>$P_1$</th>
<th>$P_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secret number:</td>
<td>Secret number:</td>
<td>Secret number:</td>
<td>Secret number:</td>
</tr>
<tr>
<td>[0 0 1]</td>
<td>[0 1 0]</td>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>Shares:</td>
<td>Shares:</td>
<td>Shares:</td>
<td>Shares:</td>
</tr>
<tr>
<td>[0] [0] [1]</td>
<td>[0] [1] [0]</td>
<td>{[a_3], [a_2], [a_1]}</td>
<td>{[b_3], [b_2], [b_1]}</td>
</tr>
</tbody>
</table>
Secure CO₂ allowance trading :: An example

Alice

Secret number: [0 0 1]

Shares: [0] [0] [1]

Sharing the shares:
[0] [0] [1]
[0] [1] [0]
[0] [0] [1]

Bob

Secret number: [0 1 0]

Shares: [0] [1] [0]

Sharing the shares:
[0] [1] [0]
[0] [0] [1]

P₁

Secret number: a

Shares: \{[a₃], [a₂], [a₁]\}

Sharing the shares:

P₂

Secret number: b

Shares: \{[b₃], [b₂], [b₁]\}
### Secure CO₂ allowance trading: An example

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
<th>$P_1$</th>
<th>$P_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$[0 \ 0 \ 1]$</td>
<td>$[0 \ 1 \ 0]$</td>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>$[0 \ [0] \ [1]]$</td>
<td>$[0 \ [1] \ [0]]$</td>
<td>${[a_3], [a_2], [a_1]}$</td>
<td>${[b_3], [b_2], [b_1]}$</td>
</tr>
<tr>
<td>$[0 \ [1] \ [0]]$</td>
<td>$[0 \ [0] \ [1]]$</td>
<td>$c_i = [a_i \oplus b_i]$</td>
<td></td>
</tr>
</tbody>
</table>

**XOR of every bit:**

$[1 \ [1]]$  $[0]$
### Secure CO₂ allowance trading: An example

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
<th>$P_1$</th>
<th>$P_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Alice values" /></td>
<td><img src="image2" alt="Bob values" /></td>
<td><img src="image3" alt="Alice values" /></td>
<td><img src="image4" alt="Bob values" /></td>
</tr>
</tbody>
</table>

#### XOR of every bit:

| $[1\ 1]$ | $[0]$ |

#### Prefix-OR:

| $[1\ 1]$ | $[0]$ |

#### Calculations:

- $c_i = [a_i \oplus b_i]$
- $d_i = \bigvee_{j \text{ from } 3 \text{ to } i} c_j$
Secure CO₂ allowance trading :: An example

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
<th>$P_1$</th>
<th>$P_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0 0 1]</td>
<td>[0 1 0]</td>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>[0] [0] [1]</td>
<td>[0] [1] [0]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[0] [1] [0]</td>
<td>[0] [0] [1]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

XOR of every bit:

- Alice: [1] [1] [0]
- Bob: [0] [1] [0]

Prefix-OR:

- Alice: [1] [1] [0]
- Bob: [0] [1] [0]

Evolution of $d$:

- Alice: [1] [0] [0]
- Bob: [0] [1] [0]

$c_i = [a_i \oplus b_i]$

$d_i = \bigvee_{j \text{ from } 3 \text{ to } i} c_j$

$e_i = [d_i - d_{i+1}]$
### Secure CO₂ allowance trading :: An example

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
<th>$P_1$</th>
<th>$P_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$[0\ 0\ 1]$</td>
<td>$[0\ 1\ 0]$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$[0\ 0\ 1]$</td>
<td>$[0\ 1\ 0]$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$[0\ 0\ 1]$</td>
<td>$[0\ 1\ 0]$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$[1\ 1\ 1]$</td>
<td>$[0\ 0\ 1]$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$[1\ 1\ 1]$</td>
<td>$[0\ 0\ 1]$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$[1\ 1\ 1]$</td>
<td>$[0\ 0\ 1]$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- $c_i = [a_i \oplus b_i]$
- $d_i = V_{(j\ from\ 3\ to\ i)}\ c_j$
- $[e_i] = [d_i - d_{i+1}]$

### Example

- $a < b$: 
  
  $[0\ 1\ 0] = 1$

- $a < b$: 
  
  $\text{Sum (} [e_i] \times [b_i] \text{)}$
### Secure CO₂ allowance trading: An example

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0 0 1]</td>
<td>[0 1 0]</td>
</tr>
<tr>
<td>[0] [0] [1]</td>
<td>[0] [1] [0]</td>
</tr>
<tr>
<td>[0] [1] [0]</td>
<td>[0] [0] [1]</td>
</tr>
<tr>
<td>[1] [1]</td>
<td>[0] [1]</td>
</tr>
<tr>
<td>[1] [1]</td>
<td>[0] [0]</td>
</tr>
<tr>
<td>[1] [0]</td>
<td>[0]</td>
</tr>
</tbody>
</table>

- **Detect bits that are different in both shares**
  - $c_i = [a_i \oplus b_i]$
- $d_i = V_{(j \text{ from } 3 \text{ to } i)} c_j$
- $[e_i] = [d_i - d_{i+1}]$

**a < b:**
- $[0 1 0] = 1$
- $\sum ([e_i] \times [b_i])$
### Secure CO₂ allowance trading :: An example

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
<th>$P_1$</th>
<th>$P_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0 0 1]</td>
<td>[0 1 0]</td>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>[0] [0] [1]</td>
<td>[0] [1] [0]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[0] [1] [0]</td>
<td>[0] [0] [1]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[1] [1]</td>
<td>[0]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[1] [1]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[1] [0]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Detect the first bit that is different in both shares</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[
c_i = [ a_i \oplus b_i ]
\]

\[
d_i = V_{(j \text{ from 3 to } i)} \ c_j
\]

\[
[ e_i ] = [ d_i - d_{i+1} ]
\]

**a < b:**

\[
[0 1 0] = 1
\]

**Sum:**

\[
\sum ([ e_i ] \times [ b_i ])
\]
Secure CO₂ allowance trading :: An example

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
<th>$P_1$</th>
<th>$P_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0 0 1]</td>
<td>[0 1 0]</td>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>[0] [0] [1]</td>
<td>[0] [1] [0]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[0] [1] [0]</td>
<td>[0] [0] [1]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[1] [1]</td>
<td>[0]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[1] [1]</td>
<td>[0]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[1] [0]</td>
<td>[0]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

$a < b$: Check if $b$ has a 1 in that position

Sum ($[e_i] \times [b_i]$)

$c_i = [a_i \oplus b_i]$

$d_i = V_{(j \text{ from } 3 \text{ to } i)} c_j$

$[e_i] = [d_i - d_{i+1}]$
No drawbacks?

Of course they are…

High computational cost

Lots of shares should be exchanged between the parties
Cost of encrypting and decrypting information
Visit our demonstrator!

Secure CO₂ allowance trading :: Conclusions

---

**Analyzing delay reports**

*An example of Secure Multi-party Computation in ATM*

By the SecureDataCloud team: [www.innaxis.org/securedatacloud](http://www.innaxis.org/securedatacloud)

**The scenario:**
Creation of delay reports using cleaned information coming from different stakeholders, securely merged in order to achieve additional knowledge about causes of delays and their evolution through time. Several stakeholders collaborate by introducing delay information inside the system: pilot, airline representatives, ATC officers, EUROCONTROL’s Network Manager Unit, airport representatives, and handling organisations. Different types of analyses will be performed, including average delays extraction, averages by causes, and airlines ranking.

**The secure computation:**

---

**Secure Slot Trading**

*An example of Secure Multi-party Computation in ATM*

By the SecureDataCloud team: [www.innaxis.org/securedatacloud](http://www.innaxis.org/securedatacloud)

**The scenario:**
We consider an airline planning to operate a new route between two airports. Therefore, at a strategic level, the airline firstly tries to buy slots from both airports, i.e., in the primary market. Afterwards, if this first step was not successful, it may try to buy a suitable slot in the secondary market, i.e., from other airlines. These two different operations are depicted in the picture: in the upper left part, the airline enters an auction in the primary market; conversely, in the lower left part, it tries to buy the asset from other airlines.

**The secure computation:**