Confidentiality Enhanced Life-Cycle Assessment

Sakine Yalman & Achim D. Brucker

UNIVERSITY OF EXETER

Outline

- Background and Motivation
  - Supply Chain – Life-Cycle Assessment
  - Security and Privacy Concerns
- Confidentiality Enhanced Life-Cycle Assessment
- Evaluation
- Future Works

Supply Chain Systems Life-Cycle Assessment

Security and Confidentiality Concerns

- Protection of trade secrets is problematic because of data sharing in supply chain, precisely in life-cycle assessment!
- These concerns prevent close collaborations within supply chains and limit the achieving better life cycle assessments of products.

IoT enters Life-Cycle Assessment

Today, LCA:

- Offline
- Historic values

With IoT, LCA:

- Actual sensor data
- Real-time

Security and Confidentiality Problems Persist!

LCA has some potential security risks. It can reveal:

- Confidential data about production processes,
- Business relationships between partners in a supply chain.

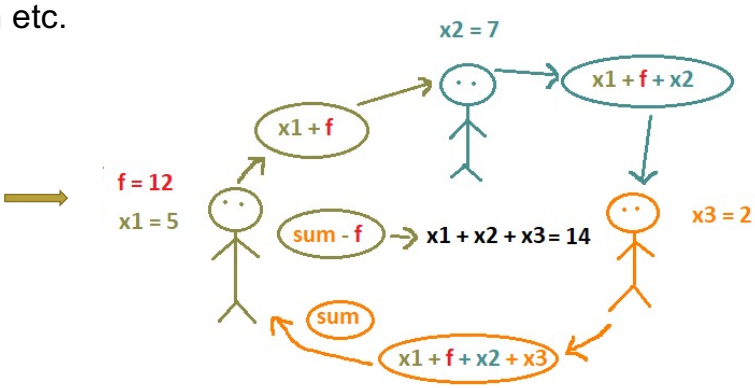
! Therefore, companies are not willing to share the data necessary for LCA based on sensor data.

Privacy-Enhancing Technologies

Privacy Preserving Techniques

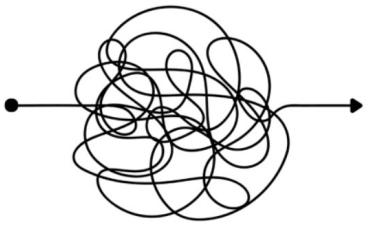
- Secure Multi-Party Computation
- Homomorphic encryption etc.

Example
Yao's Millionaires' Problem



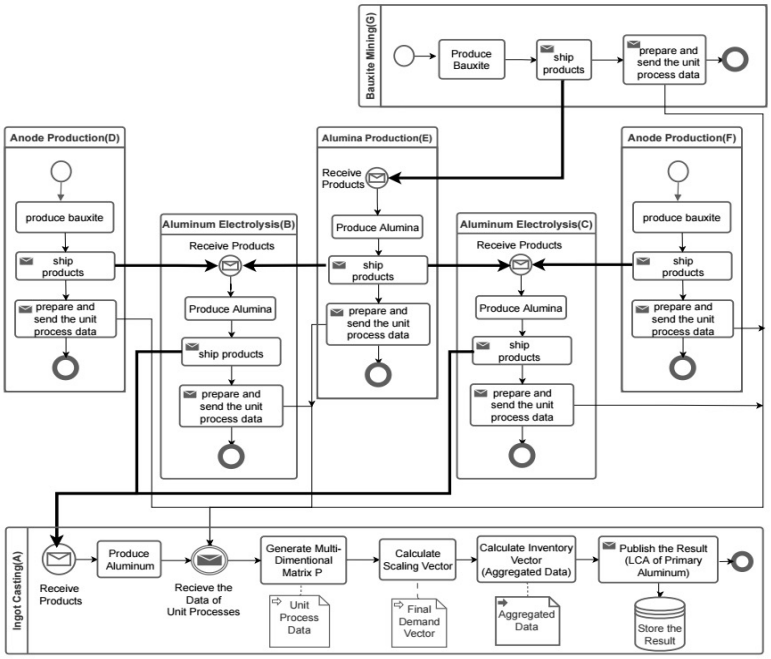
Privacy Preserving Techniques are **Not** well suitable for smart devices!

- Performance, storage and resources constrains.

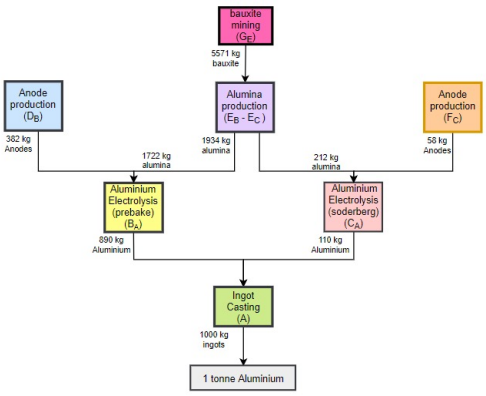


The BPMN diagram of LCA of Aluminum Production

International Aluminium Institute - 2010



Traditional Life-cycle assessment



International Aluminium Institute 2010

$$P = (P_0|P_1|P_2|\cdots|P_n)$$

$$P = \left(\frac{\mathcal{A}}{\mathcal{B}}\right)$$ → Economic flows; Environmental flows

Particulates, NO_2, SO_2 and Mercury

$$q = \left(\frac{f}{g}\right)$$ → Final demand vector

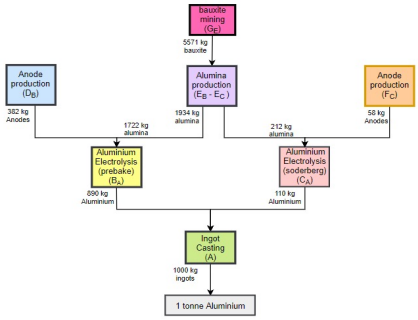
$$s = \mathcal{A}^{-1} \cdot f$$ → Scale vector

$$g = \mathcal{B} \cdot s = \begin{pmatrix} 0.04 & 194\times10^{-5} & 77\times10^{-4} & 21\times10^{-5} & 10\times10^{-5} & 56\times10^{-5} & 17\times10^{-5} \\ 0.07 & 26\times10^{-5} & 16\times10^{-5} & 56\times10^{-5} & 151\times10^{-5} & 68\times10^{-5} & 0.00 \\ 0.11 & 1528\times10^{-5} & 1179\times10^{-5} & 305\times10^{-5} & 975\times10^{-5} & 244\times10^{-5} & 0.00 \\ 0.00 & 0.00 & 0.00 & 0.00 & 0.00 & 24\times10^{-5} & 0.00 \end{pmatrix} \cdot \begin{pmatrix} 1.00 \\ 890.00 \\ 110.00 \\ 382.00 \\ 58.00 \\ 1934.00 \\ 5571.00 \end{pmatrix} = \begin{pmatrix} 4.73 \\ 1.94 \\ 21.45 \\ 0.46 \end{pmatrix}$$

Inventory vector

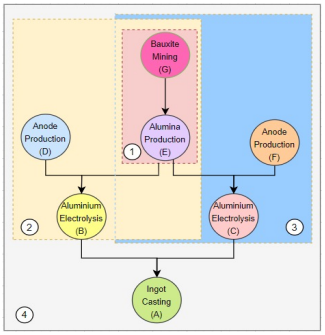
An Approach to Ensure Confidentiality in LCA

International Aluminium Institute 2010



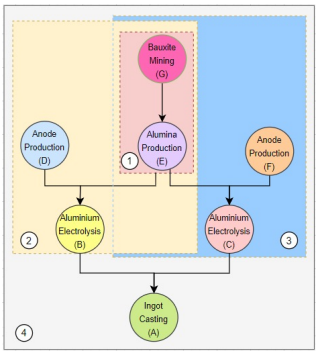
A big system with a lot of parties and complex computations

Recursive computation



One level aggregations
Small groups of parties and Lightweight computations

An Approach to Ensure confidentiality in LCA



RECURSIVE COMPUTATION

$$g_1 = \begin{pmatrix} 56\times10^{-5} \\ 68\times10^{-5} \\ 244\times10^{-5} \\ 24\times10^{-5} \end{pmatrix} \begin{pmatrix} 17\times10^{-5} \\ 0.00 \\ 0.00 \\ 0.00 \end{pmatrix} \cdot \begin{pmatrix} 1.00 \\ 2.881 \end{pmatrix} = \begin{pmatrix} 10,497\times10^{-7} \\ 68\times10^{-5} \\ 244\times10^{-5} \\ 24\times10^{-5} \end{pmatrix}$$

$$g_2 = \begin{pmatrix} 194\times10^{-5} \\ 26\times10^{-5} \\ 1,528\times10^{-5} \\ 0.00 \end{pmatrix} \begin{pmatrix} 21\times10^{-5} \\ 56\times10^{-5} \\ 305\times10^{-5} \\ 0.00 \end{pmatrix} \begin{pmatrix} 10,497\times10^{-7} \\ 68\times10^{-5} \\ 244\times10^{-5} \\ 24\times10^{-5} \end{pmatrix} \cdot \begin{pmatrix} 1.00 \\ 0.429 \\ 1.935 \end{pmatrix} = \begin{pmatrix} 406\times10^{-5} \\ 181\times10^{-5} \\ 2,131\times10^{-5} \\ 46\times10^{-5} \end{pmatrix}$$

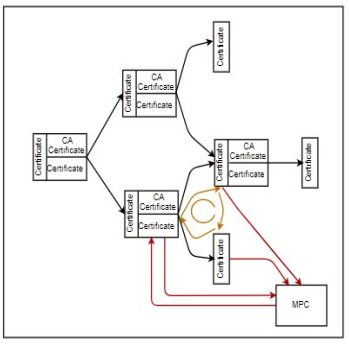
$$g_3 = \begin{pmatrix} 77\times10^{-4} \\ 16\times10^{-5} \\ 1,179\times10^{-5} \\ 0.00 \end{pmatrix} \begin{pmatrix} 10\times10^{-5} \\ 151\times10^{-5} \\ 975\times10^{-5} \\ 0.00 \end{pmatrix} \begin{pmatrix} 10,497\times10^{-7} \\ 68\times10^{-5} \\ 244\times10^{-5} \\ 24\times10^{-5} \end{pmatrix} \cdot \begin{pmatrix} 1.00 \\ 0.527 \\ 1924.00 \end{pmatrix} = \begin{pmatrix} 977\times10^{-5} \\ 226\times10^{-5} \\ 2,162\times10^{-5} \\ 46\times10^{-5} \end{pmatrix}$$

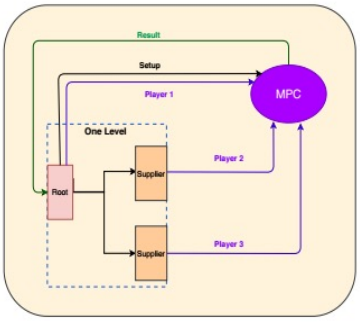
$$g_4 = \begin{pmatrix} 0.04 \\ 0.07 \\ 0.11 \\ 0.00 \end{pmatrix} \begin{pmatrix} 406\times10^{-5} \\ 181\times10^{-5} \\ 2,162\times10^{-5} \\ 46\times10^{-5} \end{pmatrix} \begin{pmatrix} 977\times10^{-5} \\ 226\times10^{-5} \\ 2,162\times10^{-5} \\ 46\times10^{-5} \end{pmatrix} \cdot \begin{pmatrix} 1.00 \\ 0.89 \\ 0.11 \end{pmatrix} = \begin{pmatrix} 475\times10^{-5} \\ 194\times10^{-5} \\ 2,145\times10^{-5} \\ 46\times10^{-5} \end{pmatrix}$$

$$1000\ kg\ \text{of}\ Primary\ Aluminium = \begin{pmatrix} 4.73 \\ 1.94 \\ 21.45 \\ 0.46 \end{pmatrix}$$

How are we ensuring confidentiality ?

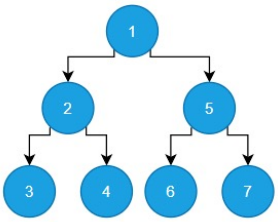
- **Sub-computations / aggregations** - prevents companies to learn the relationships between other companies in the supply chain.
- **Certificate Authorization** - protects from outside attacks.
- **Secure Multi-Party Computation (SMPC)** – prevent the disclosure of companies' confidential data.
- Why we **cannot** apply SMPC into traditional LCA **naively**:
  - Complexity of formula being computed,
  - The number of companies involved.

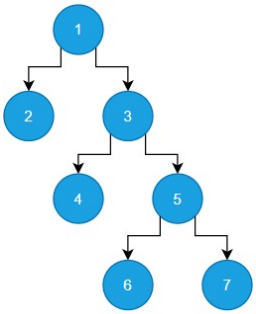


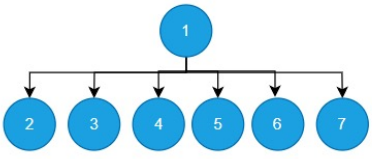


Not only Security/Privacy but also Performance!

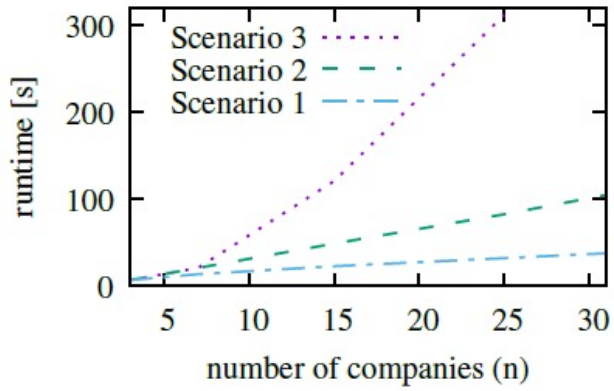
- To evaluate the performance of our LCA prototype, we use benchmarking.
- Generate and run 3 different test scenarios; a balanced binary tree, a linear list and a flat supply chain.







The Runtime Results of Test Scenarios



Future Work

In SMPC, the function being computed is already encrypted. However, participants in the supply chain can still enter wrong values.

- **Combine our approach with Secure Commitment Schemes** to be able to check participants enter the correct values.

SPMC guarantees that participants of a computation only learn their own inputs and the result of the computation and ignores the information that participants of a supply chain can infer from information learned within one or several LCAs.

- We plan to **develop a security and privacy analysis** that goes beyond the rather abstract security guarantees provided by SMPC.
- We plan to **extend our threat analysis** to include such inferred information, supporting companies in their decision to join (or not join) a supply chain.

Thank you.

CONTACT:

Sakine Yalman

sy359@exeter.ac.uk
https://emps.exeter.ac.uk/computer-science/staff/sy359
@sakine_yalman

Achim Brucker

a.brucker@exeter.ac.uk
https://emps.exeter.ac.uk/computer-science/staff/ab1185
@adbrucker

The Detailed Results

n	t_1[s]	$\frac{\delta_1}{t_1}$	t_2[s]	$\frac{\delta_2}{t_2}$	t_3[s]	$\frac{\delta_3}{t_3}$
3	7	0.06	7	0.07	7	0.06
7	14	0.03	21	0.04	21	0.02
15	23	0.03	49	0.02	121	0.04
25	-	-	83	0.01	312	0.03
31	38	0.02	105	0.01	-	-