Journal of Air Transport Management xxx (2016) 1–9

Contents lists available at ScienceDirect

Journal of Air Transport Management

journal homepage: www.elsevier.com/locate/jairtraman

Towards a secure trading of aviation CO_2 allowance

Massimiliano Zanin [a, b, *, 1], Tuba Toru Delibasi [c, g, 1], Julio César Triana [d], Vaishali Mirchandani [d], Emilio Álvarez Pereira [d], Alberto Enrich [d], David Perez [a], Cengiz Paşaoğlu [e, f], Melih Fidanoglu [g], Emre Koyuncu [g], Guney Guner [g], Ibrahim Ozkol [g], Gokhan Inalhan [g]

[a] Innaxis Research Institute, Madrid, Spain
[b] Universidade Nova de Lisboa, Lisboa, Portugal
[c] Bahcesehir University, Istanbul, Turkey
[d] Team&Cloud, Madrid, Spain
[e] General Directorate of State Airports Authority (DHMİ), Ankara, Turkey
[f] Gazi University, Ankara, Turkey
[g] Istanbul Technical University, Istanbul, Turkey

ARTICLE INFO

Article history:
Received 31 July 2015
Received in revised form
14 November 2015
Accepted 4 February 2016
Available online xxx

Keywords:
Secure Multi-party Computation
CO_2 allowance trading
Market auctions

ABSTRACT

The growth of world air traffic has been accompanied by a significant increase of its environmental impact, including CO_2 emissions, which has forced the European Union to include aviation in its Emission Trading Scheme (EU ETS). The EU ETS is a market-based mechanism that obliges airlines to buy or sell carbon permits, thus forcing them to share confidential information with their competitors in an auction-based market. Disclosure of confidential information will be one of the main barriers for the ETS adoption. In this contribution we describe the design and implementation of a Secure Multi-party Computation framework, capable of overcoming these barriers. The framework runs as an online, cloud-based computational service for performing CO_2 trading securely without the need of sharing business information. Benefits and limitations of the proposed approach are discussed, as well as the challenges to be overcome towards an operational implementation.

1. Introduction

Air transport, as all other socio-technical systems, is always in search of ways for improving its cost efficiency. Programs pursuing this aim have appeared throughout the world: SESAR in Europe, NextGen in USA, OneSky in Australia, SIRIUS in Brazil, or CARATS in Japan. Beyond these different names, they all share similar concepts, such as the idea that efficiency can be improved only by ensuring a continuous flow of information between the agents and stakeholders involved in the operation. Some examples include sharing future trajectory intentions by aircraft, negotiations for slot exchange by airlines, or the continuous monitoring of global mobility and CO_2 emissions. Such data flow is also necessary when increasing safety is the objective, *i.e.* in the analysis of past incidents and accidents, thus of historical operational data.

Achieving such seamless flow of information entails two important and contradictory challenges. First, most ATM data are considered confidential and sensitive and, hence, private - both for their commercial value, and for the political or social consequences some of the analyses may cause; any solution should thus guarantee an adequate level of confidentiality. Second, at the same time, data should be stored and processed in a safe and efficient way, which usually implies the use of a *cloud*-based infrastructure. This may generate security problems, as the exact location of data in the cloud is generally not known (Kaufman, 2009).

Present solutions, like SESAR's System Wide Information Management (SWIM) (Meserole and Moore, 2007), only partially tackle these two problems. Specifically, SWIM is based on a public-key infrastructure, allowing users to only access those sets of data included in their authorisation class. Data are released to the party requiring them, hence the security of the system is as good as the security of the worst procedure implemented by anyone party. As a result, the usefulness of the whole paradigm depends on trust: both

* Corresponding author. Innaxis Research Institute José Ortega y Gasset 20, planta 6. 28006 Madrid, Spain.
E-mail address: mzanin@innaxis.org (M. Zanin).
[1] These authors contributed equally to this work.

http://dx.doi.org/10.1016/j.jairtraman.2016.02.005
0969-6997/

between users, and between these and the system managers.

A completely different approach to this problem is provided by the use of *secure computation techniques*, allowing to deal with confidentiality issues without limiting the ability of performing relevant computation on private data. Generally speaking, *Secure Multi-party Computation* (SMC) is a set of techniques and algorithms that allows two or more untrusted parties to perform some kind of computation over a data set, while keeping their respective information private. Thus, once the computation is over, the only new information that each party should possess is the output of that computation, without any additional knowledge on the information provided by the other party. In other words, instead of providing any party with the full data set (and thus creating a security issue to be managed) or denying the access to it (effectively blocking any possibility of using the data), the data owners could allow third parties to run computations on encrypted information, without real access to the full dataset.

Secure computation has hitherto been used to solve several real-world problems, from secure sealed-bid auction (Damgard et al., 2007), elections with an electronic voting scheme (Vegge, 2009), benchmarking (Bogdanov et al., 2012), up to defense applications in military operations (Pathak and Joshi, 2009). On the other hand, it has never been applied to air transport, in spite of the large number of problems in which private data have to be interchanged.

Here we make a first step towards an operational use of SMC in air transport, by describing the design and implementation of a secure auction system for CO_2 emission rights. It allows the execution of auctions without the need of publicly sharing the bid price, which is a business sensitive information from the airline point of view. Fig. 1 illustrates such market-based mechanism, in which several airlines bid for buying the emission rights from a selling airline, *i.e.* one having a positive CO_2 allowance. Here the secure bidding mechanism is enabled by a set of SMC clients, running SMC algorithms that rank the individual bids in a collaborative way, while ensuring that the individual bids are not disclosed to any of the parties and that the individual bids cannot be tracked to each of the involved airlines. A *referee* initialises the bidding process and assures the systematic operation of the whole market-based auction, while not accessing any information about the individual bids. Finally, the winner of the auction (if any) is disclosed.

Beyond this introduction, the paper is organised as follows. Section 2 introduces the Secure Multi-party Computation concept, providing insight on its origin, applicable computation processes and the associated computational complexities. Section 3 reviews the problems of CO_2 allowance trading across airlines. Afterwards, Sections 4 and 5 respectively present the design and implementation of the secure auction system. Finally, Section 6 analyses the computational cost of performing an auction, and Section 7 draws some final conclusions.

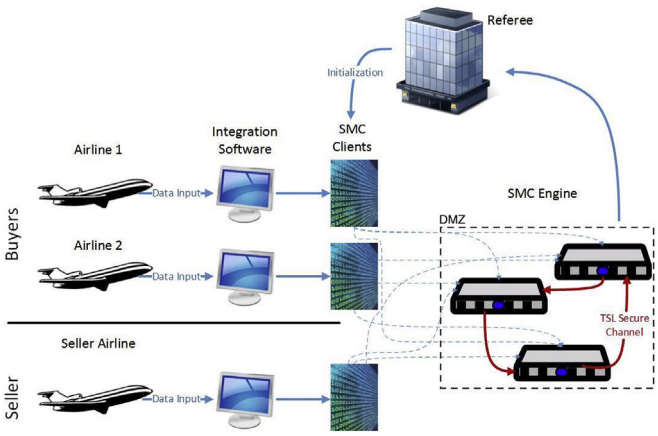

Fig. 1. Schematic representation of a SMC architecture for CO_2 allowance trading between airlines, i.e. a secondary market scenario. See Section 4 for further details.

2. What is Secure Multi-party computation?

The evolution of cryptographic needs, from simple data security to identity verification, reached its last step in recent years, as some applications required combining data security with the possibility of executing calculations upon them. One example of such problem is the so-called *Yao's Millionaires' problem* (Yao, 1982). Suppose two millionaires, Alice and Bob, who are interested in knowing which one of them is richer without revealing their actual wealth. More generally, this is tantamount to a problem of evaluating the inequality $a \geq b$ for two numbers a and b, without revealing their actual values.

Since this seminal work, different approaches, or *primitives*, have been used to implement SMC protocols. Independently on the problem to be solved, *e.g.* ranking, auction or set intersection problems, the protocol has to be constructed by means of a combination of these primitives, being therefore the building blocks of any SMC solution. The four combinations that have by and large been used in real-world applications are *Secret Sharing* (Shamir, 1979) (Blakley, 1979), *Oblivious Transfers* (Kilian, 1988), *Garbled Circuits* (Huang et al., 2011) and *Homomorphic Encryption* (Van Dijk et al., 2010).

In the two following subsections, we firstly describe the basics of *Secret Sharing*, the primitive used in the secure auction system here presented; secondly, we discuss the problem of the computational cost of SMC operations, due to its relevance in real-world applications.

2.1. Rank two numbers by means of secret sharing

As its name suggests, Secret Sharing is a set of techniques aimed at distributing a secret, *i.e.* private information that should be concealed, among a group of participants, each one of them receiving just one piece of the secret. The secret can then be reconstructed only when a sufficient number of participants work collaboratively, as individual shares are of no use on their own. For instance, suppose that one is to encode the secret, in this case a binary number s, among different parties. To all (except one) parties, the user holding the secret would send a random number p_i, while the last party would receive the result of $s \oplus p_1 \oplus p_2 \oplus \ldots \oplus p_{n-1}$, $\oplus$ being the bitwise exclusive OR (XOR) operation. In order to recover the secret, all parties should collaborate, and calculate the bitwise XOR of all parties numbers ps.[2] Suppose next that all parties want to perform a Boolean operation on private numbers they own, without revealing such numbers to the other participants. Following the previous example, each one of them can divide and share its number through a set of shares ps; afterwards, all parties execute the Boolean operation on the shares they have, and finally they collaboratively retrieve the final results.

While Secret Sharing was described by Shamir (Shamir, 1979) and Blakley (Blakley, 1979) before the work of Yao in 1979, its use

[2] To illustrate, if $s = 1010$, it can be decomposed into $p_1 = 0111$ and $p_2 = 1101$. The original number can be recovered only by calculating $s = 0111 \oplus 1101 = 1010$, which requires all parties (here, two) to contribute with their private shares. On the other hand, each individual share alone yields no information about s. Note that the XOR operation between two bits yields one only when the two input bits are different, *i.e.*, $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$ and $1 \oplus 1 = 0$.

Please cite this article in press as: Zanin, M., et al., Towards a secure trading of aviation CO_2 allowance, Journal of Air Transport Management (2016), http://dx.doi.org/10.1016/j.jairtraman.2016.02.005

for secure computation was not initially recognised.

In the previous simple example of secure computation, under normal circumstances a party is not able to recover the original number of another participant. There are nevertheless some important limitations. First, a group of participants can *collude*, *i.e.* agree to collaborate in order to retrieve the secrets of the other parties; and second, it only allows to perform Boolean operations on individual bits, an important constraint in real applications.

In the sake for completeness, we here present a brief overview of the algorithm for solving the auction problem in a secure way, through the use of the *secret sharing* paradigm, by evaluating an inequality (*i.e.* $a<b$) between two integer and positive numbers. Notice that once this operation is available, obtaining the highest bid is just a matter of evaluating the inequality for all pairs of bids. Due to its mathematical complexity, only the main steps are here reviewed: the interested reader may refer to Ref. (Nishide and Ohta, 2007). for further details and implementation considerations.

Consider two parties, P_1 and P_2, respectively holding a secret number a and b. Let p be an odd prime, l the bit length of p, and Z_p the associated prime field.[3] p should be chosen such that $a \in Z_p$ and $b \in Z_p$, *i.e.* that $a, b \in \{0, 1, \ldots, p-1\}$. For the sake of simplicity, we also suppose that both a and b can be expressed in a binary format; for instance, a is divided into the shares $\{[a_{l-1}]_p, \ldots, [a_0]_p\}$, such that $a = \sum_{i=o}^{l-1} 2^i a_i$ with $a_i \in \{0, 1\}$. Thus, this first step of the computation yields a set of shares $[a_i]_p$ and $[b_i]_p$, which should securely be interchanged between the parties.[4] At the end, each party should have a different piece of both a and b, but must not be able to reconstruct the whole number (except in the case of his own number). To illustrate, let us assume that a and b are decomposed into two shares each; the first party will then receive b_2, the second a_1; the first party will then be able to work with the second part of both numbers, *i.e.* a_2 and b_2, while conversely the second party will control the first part of both numbers (a_1 and b_1). As required, no party will receive the full set of shares of a number it does not own.

Given $[a_i]_p$ and $[b_i]_p$, the next step involves calculating $[a<b]_p$ without revealing a and b. For $0 \leq i \leq l-1$, the parties compute $[c_i]_p = [a_i \oplus b_i]_p = [a_i]_p + [b_i]_p - 2[a_i b_i]_p$ in parallel,[5] for then compute $[d_i]_p = \mathrm{V}_{j=i}^{l-1}[c_j]_p$ by using a Prefix-Or operation.[6] Next, they define $[e_i]_p = [d_i - d_{i+1}]_p$, where $[e_{l-1}]_p = [d_{l-1}]_p$. Finally, the parties compute $[a<b]_p = \sum_{i=0}^{l-1}([e_i]_p \times [b_i]_p)$.

Table 1 reports two simple examples of such computation, with all the required intermediate steps. In order to make the explanation simple, all shares $[a_i]_p$ and $[b_i]_p$ are represented together: in a real secure computation, they would be split among the parties, such that no one has full knowledge of the other numbers.

Table 1
Example of the secure evaluation of the $a<b$ binary inequality, for two sets of initial numbers. Here $p=5$ (and thus $Z_p \in \{0\ldots4\}$) and $l=3$.

a	[001]	[011]
b	[010]	[000]
$[c_i]_p = [a_i \oplus b_i]_p$	[011]	[011]
$[d_i]_p = \mathrm{V}_{j=i}^{l-1}[c_j]_p$	[011]	[011]
$[e_i]_p = [d_i - d_{i+1}]_p$	[010]	[010]
$[a<b]_p = \sum_{i=0}^{l-1}([e_i]_p \times [b_i]_p)$	$\sum[010] = 1$	$\sum[000] = 0$

[3] A *prime field* Z_p is the field composed by all integer numbers in the range $[0, p-1]$, p being a prime number. This is equivalent to saying that all operations must involve integer numbers smaller than p.

[4] In what follows, $[\cdot]$ denotes any variable that is shared among the parties.

[5] The operator $\oplus$ represent the standard bit-wise XOR operation.

[6] The *Prefix-Or* is an algorithm that allows calculating the Boolean OR operation over a set of distributed shares in a constant number of rounds. More information can be found in Ref (Chandra et al., 1983).

2.2. SMC computational cost

In spite of the interest raised in recent years by SMC, and of the large number of real-world applications in which this cryptographic technique has been successfully used, the implementation of SMC solutions is still limited by their computational cost.

The dominant factor defining the complexity of a SMC protocol is the number of cryptographic operations required. An increment in the complexity of the computation to be performed usually results in a more-than-linear increment in the computational cost. Even keeping the computation constant, the number of players is an important aspect to be considered. For instance, the computational cost of a protocol based on the secret sharing scheme of n players usually implies the creation of n^2 shares, representing an average cost by operation of $O(n^2)$ - see, for instance, the previous example of the calculation of a Boolean function. The situation is even more complicated when non-linear operations are included in the mix, like comparisons and multiplications, which greatly increase the computational complexity and the evaluation cost. Finally, even in simple scenarios, parties are required to exchange a large quantity of information, thus making the velocity of the interconnecting network a major bottleneck.

The topic of the computational cost of the SMC auction system will be fully discussed in Section 6; at this stage, nevertheless, the reader should be aware of the limitation imposed by the computational cost, which may make otherwise interesting solutions unfeasible in real-world implementations.

3. CO_2 trading in European aviation

The European Union (EU) took the lead of environmental policy fighting against climate change by implementing the world's largest emission trading scheme for certain greenhouse gases. In order to reduce pollution, and thus lower the effects of global warming, the EU has established a market-based instrument known as *emission trading* or *cap and trade*. It consists of a central entity that sets an upper limit to the amount of pollutants that can be emitted by a company or an activity sector; such amount is converted into *rights to emit*, which can be traded in a specific market. Any company that is emitting more pollutant than its limit should buy additional rights, in order to avoid sanctions; on the other hand, a green company would have a surplus of emission rights, which can be sold in the market. In theory, this mechanism allows an efficient emissions reduction through a market mechanism, as green companies are receiving indirect incentives. The EU Emission Trading Scheme (ETS) covers approximately 11.000 power stations and industrial plants in 31 countries (EU countries and the three European Economic Area-European Free Trade Association EEA-EFTA countries: Iceland, Liechtenstein and Norway), as well as aviation industry. In spite of the economic crisis and downs, world air traffic continues to grow - see Fig. 2. Along with the growth in air transport activity and hence, in fuel consumption, increased environmental impacts must also be taken into account. Although emissions from aviation account for a small part (around 3%) of the EU's total annual greenhouse gas emissions, aviation is one of the fastest-growing sources due to increasing air traffic over the years (Toru, 2011). Thus, the EU views international aviation as a substantial emitter of greenhouse gases considering that the sector is expected to grow significantly in the medium and long term (FAA, 2013).

ICAO agreed to develop a global market-based mechanism to

Please cite this article in press as: Zanin, M., et al., Towards a secure trading of aviation CO_2 allowance, Journal of Air Transport Management (2016), http://dx.doi.org/10.1016/j.jairtraman.2016.02.005

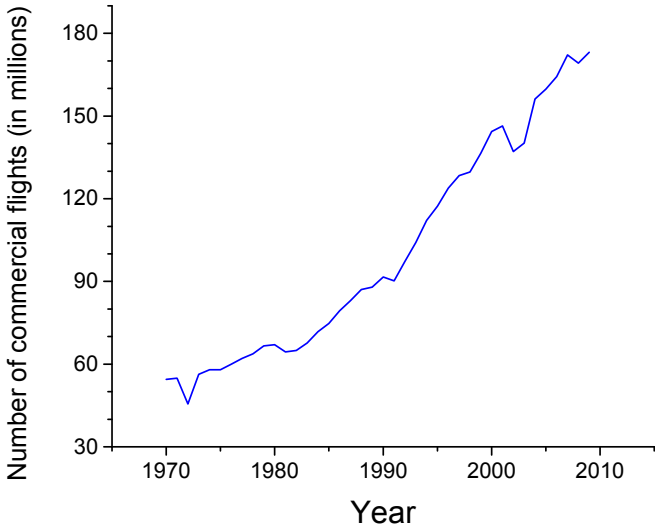

Fig. 2. Representation of the worldwide air traffic growth, expressed in terms of millions of commercial flights. Data source: The World Bank.

address international aviation emissions by 2016, and to apply it by 2020. During the period from 2013 to 2020, the EC has followed and will follow the "stop the clock" Decision,[7] including only the flights between airports located in the EEA into the Emission Trading Scheme (ETS) until the global measure enters into force (see (European Union, 2014)). The reviewed proposal covers the flights between airports in the EEA, which are obliged to hold carbon permits for the proportion of emissions that take place within EEA airspace. All flights between the EEA and least developed countries, low-income countries and lower-middle income countries, and which have a share of less than 1% of international aviation activity would be exempted from the EU ETS (see (European Commission, 2014)).

By 2014, emissions from the aviation sector is capped at 95-percent of the annual average from the years 2004–2006. From 2015 to 2016, such cap will be reduced in the proportion to the reduced scope in the EU. By 2020, the EU will apply the global market-based mechanism addressing international aviation emissions, which is agreed to be developed by ICAO by 2016. Until the global solution, the 85-percent of allocations are distributed for free for the period from 2013 to 2016 to airlines operating between airport in the EEA and the 15-percent is auctioned; as for the period from 2016 to 2020, solutions will be discussed by the EC in the next future. By 2020, it is planned to auction off all the allowances in global market according to the expected global solution.

Briefly, the ETS starts off the concept that polluters are allowed to pollute, provided that they buy sufficient permits to emit the volume of CO_2 that their operations generate. The essential elements of the EU ETS, which has been in operation since 2005, are that it sets a cap on the total number of permits available in the market, and that participants are allowed to trade these permits. As with any other traded commodity, the price for the permits is set by the market and depends on the balance of supply and demand. Under ETS, airlines receive tradable allowances covering a certain level of CO_2 emissions from their flights per year. The amount of emissions depends on the airline fuel efficiency, and so does the required number of emission permits (one allowance represents one ton of CO_2). Any airline emitting more than its allowed volume of CO_2 will either have to reduce emissions, or buy extra allowances. Airlines can buy allowances from the existing EU ETS and also have the possibility to buy them from the so-called Kyoto mechanisms, which involve emissions-reduction projects in developing and industrialised countries. Non-compliance with the requirements of ETS leads to a penalty per missing allowance, in addition to the requirement to buy missing allowances, and even possible ban on operations. Thus, airlines may then be forced to buy and sell CO_2 emission rights in the market. The less carbon intense airlines will be able to sell their excess allowances to airlines that are more carbon intense. The price for an allowance will be determined by auctioning, which is governed by the EU ETS Auctioning Regulation guaranteeing predictability, cost-efficiency, fair access to auctions and simultaneous access to relevant information for all operators. EU ETS implements a single-round, sealed bid, uniform price auction. (See, Commission Regulation (EU) No 1143/2013 (European Commission, 2014)).

Under the above auction design, bidders can place any number of bids during a single bidding window of the auction, each bid specifying the number of allowances the bidders would like to buy at a given price. The bidding window is open for at least 2 h. Directly following the closure of the bidding window, the auction platform determines and publishes the clearing price at which demand and offer for allowances converge. Successful EU ETS auction bidders are the ones who have placed bids for allowances at or above the clearing price. Under the EU ETS auction rules all successful bidders pay the same price, regardless of the price they specified in their bids.

Much concern has been raised by the ETS among the aviation industry, and much research has been devoted to the estimation of its economic impact ((Toru, 2011), (Albers et al., 2009), (Brueckner and Zhang, 2010), (Scheelhaase et al., 2010), (Vespermann and Wald, 2011)). One of the issues provided by airlines against the ETS has been the confidentiality of information, *i.e.* the fact that important business characteristics can be derived by studying the bidding process of buying and selling emission rights.

Specifically, through this system, upon setting the rules for the marketplace, airlines can engage in permit trading; yet, this may result in a more complicated structure than initially hypothesised because of the information revealed during the process. First, the ETS requires revealing critical information, as CO_2 emissions are proportional to fuel consumption and thus to aircraft take-off weights. Airlines have the right to buy and sell CO_2 allowances in other markets, *i.e.* in markets corresponding to other economic activities, thus creating a network of interconnected markets. Finally, if at some point only one airline is able to sell CO_2 allowance, it may try to force the system toward a higher price, thus burning the market by making use of a monopolistic situation.

In the next Sections, we describe how a secure computation system to perform CO_2 allowance trading can be designed and implemented, allowing the airlines to keep their target prices secret.

4. Secure aviation CO_2 allowance trading: system design

There are two types of market that can be considered in aviation CO_2 allowance trading: primary and secondary market. In a primary market, airlines can buy CO_2 emission rights directly from the regulator, or from other industries. In the secondary market, the airlines can trade CO_2 emission rights between themselves. In both cases, transactions are regulated by an auction mechanism, with several airlines bidding for buying allowances. As the allowances allocated to aircraft operators are valid only in aviation industry, airlines cannot sell CO_2 allowances to other industries (Faber and Brinke, 2011). However, in both transactions, publicly revealing

[7] Decision No. 377/2013/EU.

Please cite this article in press as: Zanin, M., et al., Towards a secure trading of aviation CO_2 allowance, Journal of Air Transport Management (2016), http://dx.doi.org/10.1016/j.jairtraman.2016.02.005

the bids may result in revealing future commercial strategies. Thus, a secure auction process may be required, to ensure participant data confidentiality. Also, it is important to note that the CO_2 allowance is location independent. In other words, if an airline buys or sells CO_2 allowance rights in the market, its total quota will drop at every location where the EU ETS is implemented. In a hypothetical case, an airline can acquire additional CO_2 allowance capacity and may decide against renewing its ageing fleet with higher emissions. In that sense, the emission allowance is not only a real financial commodity but also a tradable right applicable without any location limitations across the EU ETS geography. Note that such aspect is relevant for the development of a secure auction system: only a single market has to be considered, without the need of including spatial information in each bid.

Although there are two types of markets for auctioning process (primary and secondary), the underlying algorithms remain the same for both situations. In the case of the seller being an airline, one is facing a secondary market, as already depicted in Fig. 1; conversely, a primary market would have the industry (*i.e.* the primary source of the CO_2 allowances) as the seller. In both cases, there are three types of parties in an auctioning process: the buying airlines, the selling airline/industry, and the referee. The SMC auction process also includes an auction type (*i.e.* single or multi round), computation process of the winner, the integration process of the auction and also a quality assurance. These properties are described here below.

4.1. Auction type

In any trading process, two parties have to meet and put two prices in common, respectively the minimum price the seller would accept and the maximum price the buyer is willing to pay. However, the way the actual bargaining is executed differs according to the procedure of the auction process. It is common to see different outcomes depending on the scheme of the auction. Consider the two typical auction types below:

- Single Round Auction – In this scheme, if the seller price is lower than the highest bid, two types of scenarios occur. In the first scenario, there are no matching highest bids, thus only one buyer airline wins the auction. Alternatively, if two airlines match each other in the highest bid, there would be no winner, although it is unlikely. If CO_2 allowance cannot be sold, then, in the future, a completely independent auction process could be organised. Note that, in this case, the number of rounds is variable, and a new auction may be created according to the result of the previous one.
- Multi Round Auction – In this scheme, the number of auction rounds are determined before the auction starts. Even if there is a winning bid in the first round, the remaining planned auctions are executed, thus allowing participants to adjust their proposed prices. This further allows to implement elimination processes. For example, in the earlier rounds, bidders whose bids are less than the bid of the seller price are discarded, and another round is started whether there is a single winning bid or not. These elimination rounds and actual deciding rounds can be mixed to create a full auctioning scheme. Such schemes involves scenarios such as double auctions, in which market clearing price is computed based on sealed bids.

As an illustrative example, we consider the single round auction scheme for the SMC architecture. Nevertheless, the proposed architecture is capable of doing not only single but also multi round auctions including multiple sellers, multiple buyers and with multiple round of auctions.

4.2. Computation requirements

The computation process begins in the participants' premises. A SMC client will prepare the data each party introduced in its Integration Software Application and then it will be forwarded to the SMC Engines following Secret Sharing principle. Once the SMC Engine confirms that it received all of the data needed for computations, it will proceed to secure computing the bid rank, and by returning the auction result to all participants. Notice that this process is similar to a standard agent-based auction protocol; nevertheless, the main difference resides in the fact that the information processed by the engine is encrypted, and thus that no sensitive information can be recovered, not by the participants nor by an external attacker (see Section 2.1 for an example). If the seller price for CO_2 allowance is higher than the price proposed by all of the buyers, then no transaction will occur. In this situation, if there is a willingness to sell on the seller side, then a completely separate and independent auction can be organised. However, if there is one and only one winning bid, a winner will be declared.

4.3. The integration software

The integration software is in charge of creating, opening, managing and closing auctions. All participants should have individualised access to it. Also, an external referee will act as an auction manager. All the data will be stored locally and will be the input for the corresponding SMC-client once the auction is closed. When the SMC Engine returns the final result, the integration software will inform all participants and/or the referee.

4.4. The quality assurance process

According to the best practices of Quality Assurance, a Quality Assurance Test Plan should be implemented, including at least:

- Functional testing, *i.e.* verifying the process as a whole.
- System testing, *i.e.* validating the process as a whole.
- Performance testing.

Basically, the main aims of these tests are to check the efficient operation of SMC servers, SMC client communication interface, and the communications between the clients and the servers. The plan should include both a test prior to deployment and a periodical test plan.

4.5. Roles

In order to structure the algorithms, roles of each participant must be defined. There are three different types of levels. In business level, all roles have a high level vision over the project. In technical level, roles have technical knowledge and capabilities. In quality assurance level, roles will be used to check if the requirements are met. Below is a systematic way of description of each of these roles:

1) Business Level
   a) Participant
      - Airline Planner Buyer: buys CO_2 allowance rights in auctions from the primary and secondary market.
      - Airline Planner Seller: sells CO_2 allowance rights in auctions of the secondary market.
      - Industry Planner Seller: sells CO_2 allowance rights in auctions of the primary market.
   b) External Referee

Please cite this article in press as: Zanin, M., et al., Towards a secure trading of aviation CO_2 allowance, Journal of Air Transport Management (2016), http://dx.doi.org/10.1016/j.jairtraman.2016.02.005

- Supervises the bidding process by opening, managing, and closing secure auctions.
- May veto an operation if it is illegal or it threatens the openness of the market.
- Is not allowed to receive nor obtain any private information involved in the computation.

2) Technical Level
   a) Participants' Security Admin. Verifies data and system security and integrity.
   b) Participants' System Admin. Installs and maintains the needed hardware and software to assure a correct secure auction process in each of the participants' premises. Also sets up the equipment to comply with the basic security standards.
   c) Cloud System Admin. Installs and maintains the needed software to assure a correct secure auction process in the cloud, and sets up the equipment to comply with the basic security standards.
   d) Integration Admin. Installs, develops, manages and maintain the integration process application.
   e) SMC Client. Prepares and sends the encrypted data.
   f) SMC Server. Computes and sends the auction results.
3) Quality Assurance Level
   a) Quality Assurance Manager. Verifies and validates the entire process including implementation and maintenance, and monitors all processes and methods used to ensure quality.

5. Secure aviation CO_2 allowance trading: system implementation

Once the requirements and roles of the secure auction system have been defined in the previous Section, it is still necessary to tackle some implementation choices. Specifically, this Section is devoted to two of them: the selection of the SMC protocol and library to perform the secure computation; and the desired characteristics of the integration software, *i.e.* of the interface connecting the user with the secure computation (see Section 4.3). Finally, Section 5.3 presents the resulting Graphical User Interface of the system.

5.1. Choosing the SMC library

The choice of the SMC library to be implemented has been guided by four considerations. First of all, as the aim of this development is not only to advance the state of the art in secure computation, but also to demonstrate the usefulness of SMC in an aeronautical environment, only existing frameworks have been considered. This allows reducing the development complexity; more important, it also limits the sources of insecurities, as frameworks have been validated by cryptographic experts. Second, and following the previous consideration, the chosen framework should be based on an Open Source Licence, to ensure the long-term continuity of the project, and the possibility of a community-based validation. The computation system has also to be multi-party optimal, thus able to easily scale to a large number of participants. And finally, even if the CO_2 allowance trading is not a time-critical process, the SMC process has to be fast enough and scale well with an increasing number of participants.

Four SMC software library were analysed in the light of the previous requirements: Sharemind (Bogdanov et al., 2008), VIFF (VIFF Developement Team, 2009), FairPlay (Malkhi et al., 2004) and SEPIA (Many et al., 2012). SEPIA was the only one fulfilling all conditions, by being optimised for handling large amounts of data and being currently maintained by its developers - see Table 2 for details.

Finally, the requirements of fast computations and scalability suggested the use of a cloud environment, in which different auctions can be easily set up without being limited to any predefined computational infrastructure. In order to ensure security against third-party intrusions, communications should be performed over the Internet via secure protocols, being the Transport Layer Security (TLS) the most natural choice. Furthermore, the computation engine is required to be behind a *demilitarized zone* (DMZ), *i.e.* a small network inserted as a "neutral zone" between a private network and the outside public network, which prevents outside users from getting direct access to the private server. While all these measures enable a higher security of the system, they also imply an important communication cost; for instance, TLS encryption requires some costly negotiations between client and server, and the limited network bandwidth between the machines of a cloud infrastructures may further slow the computation. The balance between security and computation time in a cloud environment will be further discussed in Section 6.

5.2. Integration software requirements

As previously introduced in Section 4.3, the integration process is in charge of creating, opening, managing and closing auctions. It is in other words the link between the user (participant or referee) and the SMC engine. Some requirements for the implementation of an integration software are reported here below:

- It has been implemented in Java, to ensure cross-platform operability. This has been verified in different environments, including Windows, OS X and Linux machines.
- Communications between all machines are encrypted according to the TLS standard.
- Data input and output, *e.g.* price definition and results delivery, are performed through CSV files. This simplifies the interface with external programs, including automatic data processing software (for instance, any software the airline may have to keep track of its CO_2 allowance needs).
- Software elements (*i.e.* the integration system and the SMC engine) are launched by executing .BAT files, which start JAVA machines and initialise the corresponding program.

5.3. The final Graphical User Interface

As a final point, we here present the resulting Graphical User Interface (GUI) that has been developed for both participants and the referee. Specifically, Fig. 3 includes four panels, showing the most steps in the execution of an auction:

- (Top left) Registration of a new participant. This includes the usual information, like user name and password. This step should be performed by one (or more) responsible people of the airline, although just one of them can participate in an auction at the time.
- (Top right) Creation of a new auction. This operation can only be executed by the referee, after receiving a request from one of the sellers.
- (Bottom left) Main control screen, as seen by one of the participants (not the referee). A list of open auctions is displayed, and through the *Select* link, the participant can submit its bid price.
- (Bottom right) Main control screen, as seen by the referee. Both completed and on-going auctions are shown. In the former case, the system displays the result of the computation (*i.e.* the winner, if any, and the winning price); in the latter, the referee

Please cite this article in press as: Zanin, M., et al., Towards a secure trading of aviation CO_2 allowance, Journal of Air Transport Management (2016), http://dx.doi.org/10.1016/j.jairtraman.2016.02.005

Table 2
Comparative analysis of four SMC libraries.

Framework	SEPIA	VIFF	FairplayMP	Sharemind
Licence	Open Source (GNU)	Open Source (GNU)	Open Source (GPL)	Closed Source
Multithreaded	Yes	No	No	No
Last release	2012	2009	2008	2013
Language	Java	Python	Java	SecreC
Multiplications/sec.	145,000 (3 nodes)	326 (5 nodes)	1.6 (5 nodes)	160,000 (3 nodes)

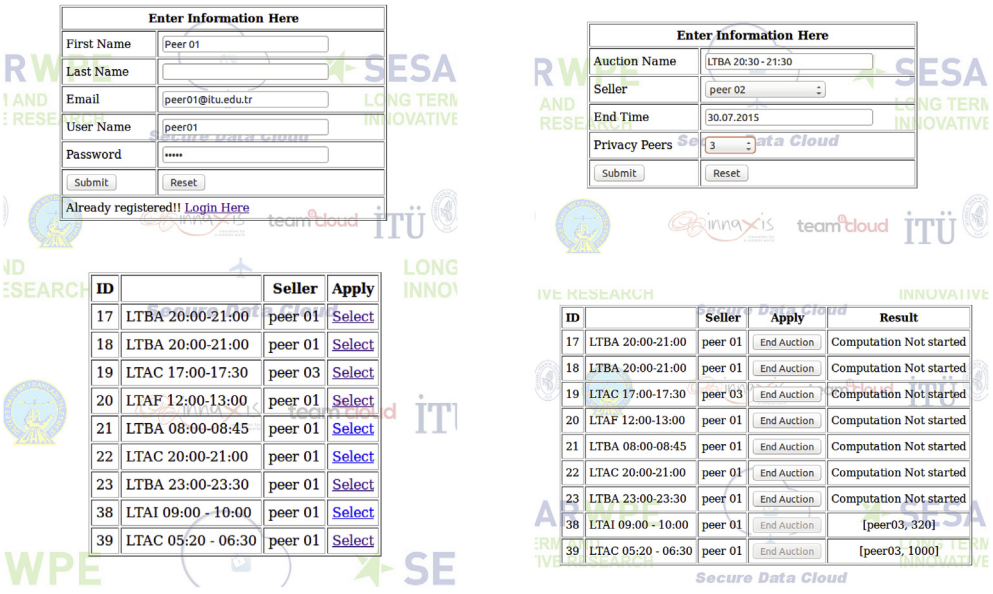

Fig. 3. Examples of the system's graphical interface – see Section 5.3 for details.

has the option of end the auction, and start the computation process.

The system has been developed as a web service, accessible through Java Server Pages (JSP). JSP is a platform independent technology that enables creating dynamic web pages through the Java programming language. Hence, it is possible to run the integration software on all the Java installed platforms. A Tomcat v7.0 server operates all activities of the users (*e.g.* login, registration, selection of trade) through the integration software. The login information of the participants and the data set associated with the trading process are stored in MySQL database. In order to reach this database through the Java platforms, the system utilises JDBC (Java Database Connectivity) interface.

6. Analysis of the computational cost

One of the main problems limiting the applicability of SMC to real-world problems is the large computational cost required to perform even simple analyses. As seen in Section 2.1, comparing two numbers requires multiple computational steps, for dividing the initial data in shares and manipulate them in separate servers. Beyond the pure mathematical manipulations, two more costs have to be included: the internal communication cost of transmitting shares in a secure way between servers, and the global communication overhead of setting up the system. The situation is further complicated by the non-linearity of the process: adding participants to the computation, or performing the computation in a large number of secure servers, increases the cost in a more-than-linear way (Damgard et al., 2007) (Bogetoft et al., 2009).

Fig. 4 reports the results of a set of velocity tests performed on the functional auction server, as a function of the number of clients (i.e. of participants, left panels) and SMC servers (right panels). The execution time of each analysis has been divided in three parts:

- *Computation cost* (blue bars of Fig. 4). Time required to create and manipulate the shares.
- *Communication cost* (green bars). Time spent by the SMC servers to transmit information among themselves, as required to perform the secure computation.
- Communication overhead (yellow bars). Any other time cost, including the initial setup of the system, authentication of the clients, network discovery, synchronisation between servers, *etc.*

Additionally, two scenarios have been considered. Top panels of Fig. 4 report the cost of performing the full computation process in a local system, *i.e.* in a single laptop, thus minimising the cost of the communication between the different elements. On the other hand, bottom panels correspond to a cloud deployment, in which each client and server is executed in an independent machine in the Amazon's Elastic Cloud Computing platform (Jackson et al., 2010). The fact of having SMC deployed in a cloud platform ensures higher security and computational power, but at the same time, a lack of control on the way the network is organised, and thus on the time spent in the communication steps.

Several conclusions can be drawn from Fig. 4. First of all, the largest share is always the communication overhead, usually followed by the inter-server communication. This highlights the importance of the quality and speed of the network used. The

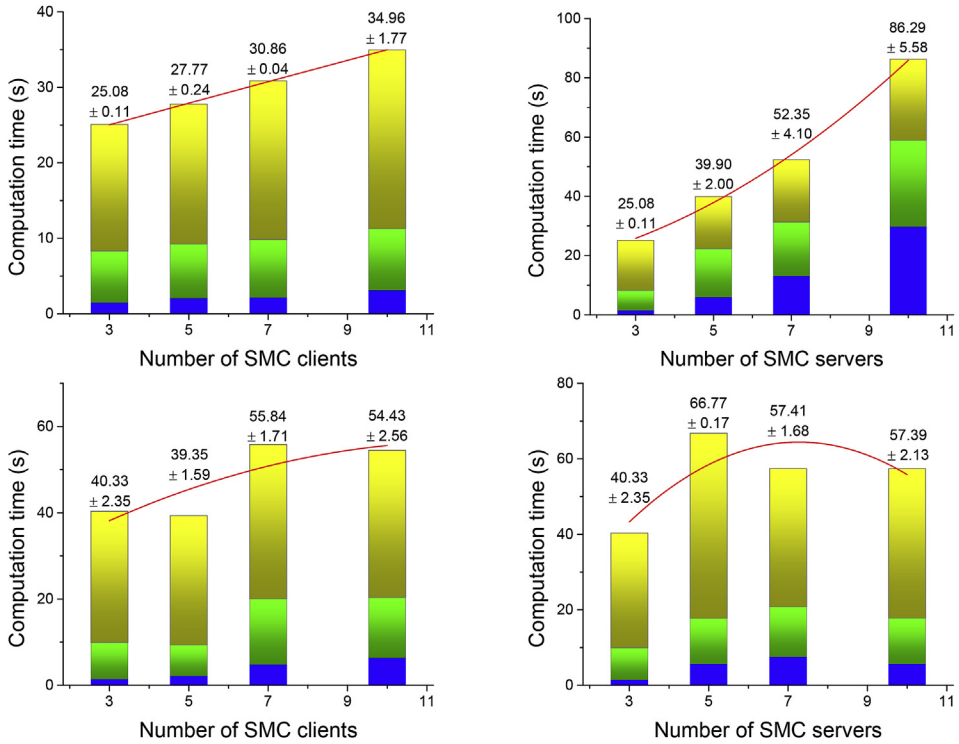

Fig. 4. Computational cost as a function of the number of SMC servers and clients. Top (bottom) panels depicts the cost of performing the computation in a local environment (in a cloud environment). Left panels corresponds to a fixed number of SMC servers (3 in each case), while right ones to a fixed number of participants (3 SMC clients). Blue, green and yellow bars respectively correspond to the secure computation time, the communication time between SMC servers, and communication overhead. Red lines represent the best quadratic fits on the total computation cost.

evolution of the total computation time in a local environment is almost linear with the number of clients n (quadratic fit of $t = 20.70 + 1.45n - 0.002n^2$, $R^2 = 0.998$), and quadratic with the number of servers s ($t = 15.33 + 1.96s + 0.51s^2$, $R^2 = 0.989$). On the other hand, results for the cloud environment are more complicated, as communication delays may appear for causes outside the control of the user. As a consequence, even computing with a small number of SMC servers may result in large overheads.

It is important to notice that these results correspond to a real implementation, which includes times (like the communication overheads) that are not part of the SMC engine itself, but are nevertheless part of the real system. An operational implementation of the proposed SMC auction system should thus use these results as a starting point for a cost-benefit analysis, aimed at balancing the added security of using a cloud infrastructure, with the decreased control over the execution time.

7. Conclusions

In this contribution, we have presented an overview of the cryptographic field known as *Secure Multi-Party Computation*, and discussed how it can be applied to the problem of creating secure CO_2 auctions in aviation. Towards this aim, a working prototype of a secure auction system has been designed and implemented, based on the SEPIA library (Many et al., 2012).

The secure bidding mechanism is enabled by a set of SMC clients, running SMC algorithms that rank the individual bids in a collaborative way, while ensuring that the individual bids are not disclosed to any of the parties and that the individual bids cannot be tracked to each of the involved airlines. This solves the problem of data confidentiality, recognised as one of the major problems in the ETS mechanism: by participating in the market, airlines are required to disclose confidential information, as CO_2 emissions are proportional to fuel consumption and thus to aircraft take-off weights.

Thanks to its characteristics, SMC is expected to yield benefits for stakeholders in a large number of problems, in which data confidentiality is of high importance: from other bidding processes, *e.g.* slot trading, up to the secure benchmarking of airline operational information.

Acknowledgement

This work is co-financed by EUROCONTROL acting on behalf of the SESAR Joint Undertaking (the SJU) and the EUROPEAN UNION as part of Work Package E in the SESAR Programme. Opinions expressed in this work reflect the authors views only and EUROCONTROL and/or the SJU shall not be considered liable for them or for any use that may be made of the information contained herein.

References

Albers, S., Buhne, J., Peters, H., 2009. Will the EU-ETS instigate airline network reconfigurations? J. Air Transp. Manag. 15, 1–6.

Blakley, G.R., 1979. Safeguarding cryptographic keys.. In: Managing Requirements Knowledge. International Workshop on, p. 313.

Bogdanov, D., Laur, S., Willemson, Jan, 2008. Sharemind: a framework for fast privacy-preserving computations. In: In Computer Security-esorics 2008. Springer Berlin Heidelberg, pp. 192–206.

Bogdanov, D., Talviste, R., Willemson, Jan, 2012. Deploying secure multi-party computation for financial data analysis. In: In Financial Cryptography and Data Security. Springer Berlin Heidelberg, pp. 57–64.

Bogetoft, P., Christensen, D.L., Damgård, I., Geisler, M., Jakobsen, T., et al., 2009. Secure multiparty computation goes live. In: Financial Cryptography and Data Security. Springer Berlin Heidelberg, pp. 325–343.

Brueckner, J.K., Zhang, A., 2010. Airline emission charges: Effects on airfares, service quality, and aircraft design. Transp. Res. Part B Methodol. 44 (8–9), 960–971. September-November 2010.

Chandra, A.K., Fortune, S., Lipton, R.J., 1983. Lower bounds for constant depth circuits for prefix problems. ICALP 109–117.
Damgard, I., Geisler, M., Krøigaard, M., 2007. Efficient and secure comparison for online auctions. Inf. Secur. Priv. 416–430.
European Commission, 2014. Aviation Emissions: Commission Proposes Applying EU ETS to European Regional Airspace from 1 January 2014-MEMO/13/906 16/10/2013.
European Union, 2014. Document L:2014:129:TOC. Official J. Eur. Union, L 129 (30). April 2014.
FAA, 2013. FAA Aerospace Forecast Fiscal Years 2013-2033.
Faber, J., Brinke, L., 2011. The inclusion of aviation in the EU emissions trading system, an economic and environmental Assessment. ICTDS Glob. Platf. Clim. Change, Trade Sustain. Energy 5. http://www.ictsd.org/downloads/2011/11/the-inclusion-of-aviation-in-the-eu-emissions-trading-system.pdf.
Huang, Y., Evans, D., Katz, J., Malka, L., 2011. Faster secure two-party computation using garbled circuits. USENIX Secur. Symposium 201 (1).
Jackson, K.R., Ramakrishnan, L., Muriki, K., Canon, S., Cholia, S., Shalf, J., Wasserman, H.J., Wright, N.J., 2010. Performance analysis of high performance computing applications on the amazon web services cloud. In: Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on.
Kaufman, L.M., 2009. Data security in the world of cloud computing. Secur. Priv. IEEE 7 (4), 61–64.
Kilian, J., 1988. Founding crytpography on oblivious transfer. Proceedings of the twentieth annual ACM symposium on Theory of computing. ACM.
Malkhi, D., Nisan, N., Pinkas, B., Sella, Y., 2004. Fairplay-Secure two-party computation system. USENIX Secur. Symposium 4.
Many, D., Burkhart, M., Dimitropoulos, X., 2012. Fast private set operations with sepia. Tech. Rep. 345.
Meserole, J.S., Moore, J.W., 2007. What is system wide information management (SWIM)? Aerosp. Electron. Syst. Mag. IEEE 22 (5), 13–19.
Nishide, T., Ohta, K., 2007. Multiparty computation for interval, equality, and comparison without bit-decomposition protocol. Public Key Cryptogr. 2007, 343–360.
Pathak, R., Joshi, S., 2009. Secure multi-party computation protocol for defense applications in military operations using Virtual Cryptography. Commun. Comput. Inf. Sci. 40 (8), 389–399.
Scheelhaase, J., Grimme, W., Schaefer, M., 2010. The inclusion of aviation into the EU emission trading scheme - impacts on competition between European and non-European network airlines. Transp. Res. (Part D) 15, 14–25.
Shamir, A., 1979. How to share a secret. Commun. ACM 22 (11), 612–613.
Toru, T., 2011. European air traffic facing raising fuel prices and carbon permits: an Empirical analysis. In: IIOC Boston Proceeding, Rising Stars Session.
Van Dijk, M., Gentry, C., Halevi, S., Vaikuntanathan, V., 2010. Fully Homomorphic Encryption over the Integers. In Advances in CryptologyEUROCRYPT 2010. Springer Berlin Heidelberg, pp. 24–43.
Vegge, H., 2009. Realizing Secure Multiparty Computations.
Vespermann, J., Wald, A., 2011. Much Ado about Nothing? – an analysis of economic impacts and ecologic effects of the EU-emission trading scheme in the aviation industry. Transp. Res. Part A Policy Pract. Elsevier, Elsevier 45 (10), 1066–1076.
VIFF Developement Team, 2009. Viff, the Virtual Ideal Functionality Framework.
Yao, A.C., 1982. Protocols for secure computations. In: Proceedings of the 23rd Annual Symposium on Foundations of Computer Science.

Please cite this article in press as: Zanin, M., et al., Towards a secure trading of aviation CO_2 allowance, Journal of Air Transport Management (2016), http://dx.doi.org/10.1016/j.jairtraman.2016.02.005