Enabling the Aviation CO_2 Allowance Trading Through Secure Market Mechanisms

Massimiliano Zanin[*][†][‡], David Perez[*]
[*]Innaxis Research Institute, Madrid, Spain
[†]Universidade Nova de Lisboa, Lisboa, Portugal
{mzanin, dp}@innaxis.com

Tuba Toru Delibasi[‡]
Bahcesehir University, Istanbul, Turkey
Istanbul Technical University, Istanbul, Turkey
tuba.toru@eas.bahcesehir.edu.tr

Gokhan Inalhan, Melih Fidanoglu,
Emre Koyuncu, Ibrahim Ozkol
Istanbul Technical University, Istanbul, Turkey
{inalhan, melih.fidanoglu,
emre.koyuncu, ozkol}@itu.edu.tr

Emilio Álvarez Pereira, Vaishali Mirchandani,
Alberto Enrich, Julio César Triana
Team&Cloud, Madrid, Spain
{ealvarez, vmirchandani,
aenrich, jtriana}@telenium.es

Cengiz Paşaoğlu
DHMI, Istanbul, Turkey
cengiz.pasaoglu@dhmi.gov.tr

***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 supply or demand carbon permits, thus forcing them to share confidential information with their competitors in an auction-based market. In this contribution, we propose the use of a Secure Multi-Party Computation framework, which allows airlines to buy and sell emission rights without disclosing confidential information. After introducing the basics of this family of cryptographic techniques, we describe a computational platform for performing secure CO_2 trading, and analyse the expected benefits for the involved stakeholders.**

***Keywords*— Secure Multi-Party Computation; CO_2 Allowance Trading; Market Auctions**

I. Introduction

In a similar way to all socio-technical systems, air transport is always in the 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, one priority is shared: 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 important challenges, which should be tackled by any enabling system. First, the agents of the system must be able to exchange information. As 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 - the system should guarantee an adequate level of confidentiality. Finally, data should be stored and processed in a safe and efficient way, which usually implies the use of a *cloud*-based infrastructure.

Present solutions, like SESAR's System Wide Information Management (SWIM) [1], are able to tackle these three points, but with important limitations. Specifically, SWIM is based on a public-key infrastructure, allowing users to only access those sets of data included in their authorization class. Although this may seem secure, data are actually released to the party requiring them, hence the security of the system is as good as the security of the worst procedure implemented by the entities. As a result, the usefulness of the whole paradigm depends on trust: both 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

[‡] These authors contributed equally to this work.

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 (in this case, 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.

Nowadays, there are several problems tackled using a secure computation approach, with applications spanning from secure sealed-bid auction [2], [3], [4], elections with an electronic voting scheme [5], and benchmarking [6], up to defense applications in military operations [7].

In this contribution we review some of the main concepts of SMC, and discuss how they can be applied to air transport problems. Specifically, we will discuss how an auction for CO_2 emission rights can be made secure by the use of SMC techniques, thus enabling the execution of auctions without the need of sharing business sensitive information between stakeholders. Figure 1 illustrates such a 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 system initializes the bidding process, and assures the systematic operation of the whole market based auction. The illustrated system is referred to as the *secondary market* auction process. This is in comparison to a later discussed *primary market* auction process, in which airlines buy CO_2 allowance from other industries or directly from the regulator.

In the next sections, we first introduce the secure multi-party computation concept, providing insight on its origin, applicable computation processes and the associated computational complexities. The *SecureDataCloud* WP-E project is then presented, which is focused on the application of SMC techniques to the multi-party negotiation problems seen in air transportation sector. Finally, we introduce the business case synopsis for the CO_2 trading across airlines, and demonstrate how the SMC techniques can be utilized to achieve both secondary and primary market allowance trading in a secure and reliable fashion.

II. 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*, firstly introduced by Andrew Yao, a prominent computer scientist and computational theorist [8]. The problem discusses 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 solving the inequality $a \geq b$ for two numbers a and b, without revealing their actual values.

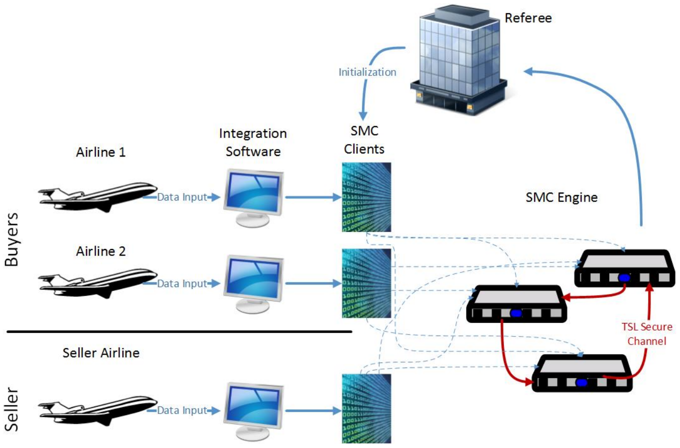

Fig. 1: Schematic representation of a SMC architecture for CO_2 allowance trading between airlines, *i.e.* a secondary market scenario. See Section V for further details.

Since the seminal work of Yao, 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. They are therefore the building blocks of any SMC solution. The four that have been mostly used in real-world applications are *Secret Sharing*, *Oblivious Transfers*, *Gambled Circuits* and *Homomorphic Encryption*.

For the sake of completeness, here we describe the basics of *Secret Sharing*: both for being one of the simplest primitives, and for exemplifying the types of computation that can be performed within SMC. 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 would send a random number p_i, while the last 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. Now, let us suppose that all parties want to perform a Boolean operation on private numbers they own. Following the previous example, each one of them can divide its number in a set of numbers ps; afterwards, all parties execute the Boolean operation on the share they have, and finally they collaboratively retrieve the final results. Notice that under no circumstance a party is able to recover the original number of another participant.

Let us present an additional example of how secret sharing can be used to perform a simple calculation. Consider three people, *e.g.* Alice, Bob and Charlie, each holding a secret number (say x_a, x_b and x_c). Due to confidentiality reasons, they cannot share these numbers with the other parties; nevertheless, they need to calculate their sum, that is $x = x_a + x_b + x_c$. The solution to this problem is the following. Firstly, Alice chooses a random number r and privately sends $r + x_a$ to Bob. Afterwards, Bob adds his secret number and privately sends $r + x_a + x_b$ to Charlie. Finally, Charlie does the same with his personal number and sends $r + x_a + x_b + x_c$ back to Alice. At the end of this process, Alice can recall the random number r, subtract it from the received value $r + x_a + x_b + x_c$, and announce the result. Notice how none of them learns the input of the other parties: for instance, Alice's random number r prevents Bob from knowing her private number.

While secret sharing was discovered by Shamir [9] and Blakley [10] before the work of Yao in 1979, its use for secure computation was not initially recognised.

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, which is usually proportional to the number of gates composing the target operation circuit. This means that an increment in the complexity of the computation to be performed results in a higher 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.

Even avoiding further mathematical and technical details, the reader should be aware of the limitation imposed by the computational cost of SMC protocols, which may make otherwise interesting solutions unfeasible in real-world implementations.

III. Introducing SecureDataCloud

While SMC techniques have been used in a large number of real-world problems, these still do not include the air transport sector. The aim of the recently launched WP-E project *SecureDataCloud* is just that: propose SMC as a new paradigm in air transport, to deal with confidentiality issues without limiting the ability of performing relevant computation of private data [11].

The main objective of the SecureDataCloud project is to raise awareness, within the Air Transport and ATM communities, about the potential benefits that can derive from the implementation of secure computation techniques in aviation. This global objective is pursued by a two-fold strategy. On the one side, the project will make available to the aviation community a set of documents presenting and explaining secure computation techniques, also including a software framework that will simplify the implementation of this concept in new and yet unforeseen problems. On the other side, SecureDataCloud will provide the analysis and documentation of a small number of Case Studies, *i.e.* specific problems that can be solved by means of this approach, demonstrating the feasibility and benefits of secure computation in real operational environments.

The expected results of this project will take the form of general guidelines for the application of secure computation techniques, which will materialize in the following three outputs:

- Guidelines for the implementation of secure computation techniques in different Business Cases, *i.e.* high-level descriptions of situations in which secure computation can provide an added value to ATM. This will include a review of requirements, benefits for the ATM stakeholders involved, and algorithms and protocols availability. Clearly, this will be a useful document for any stakeholder interested in solving a problem using this technology.
- Software Reference Framework. This software framework will include functions, algorithms and protocols that will constitute the starting ground for anyone beginning a new development.
- Complete simulation results for two Case Studies. They will include real experiments on the use of secure computation and precise figures for important metrics, like the computational cost or the data transmission bandwidth required to ensure proper functionality. Additionally, it will include measurements of the guaranteed security levels.

The use of this technology would enable the improvement of uncountable applications within Air Traffic Management, starting with actual research activities. Among others, these include safety, allowing analysts to mine some specific pattern inside historical data, without actually accessing the data sets and thus ensuring confidentiality; understanding global properties of air transport, as for instance the number of passengers in a given route, or actual fuel consumptions; or improving the cooperation between airlines, fostering mechanisms such as slot bidding. In the next section, we review a specific applicable business case in which CO_2 allowance trading can be achieved by SMC across industries and airlines while ensuring bidding privacy and compliance to emission standards as set by the European Union.

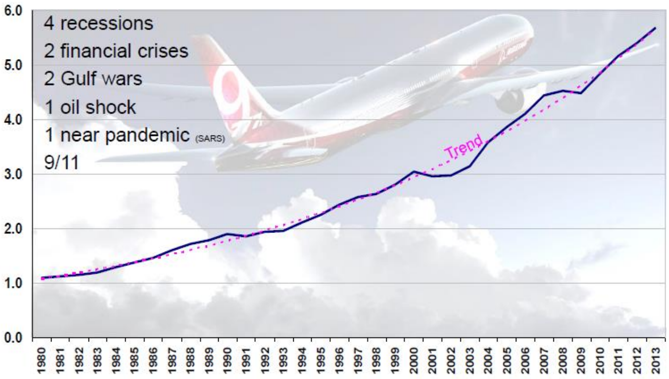

Fig. 2: Representation of the worldwide air traffic growth, expressed in terms of Passenger-Kilometers in trillions - ICAO scheduled traffic [15].

IV. 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 slower 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 system (ETS) covers approximately 11000 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 Figure 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 ([12], [13], [14]). 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 [15], [16].

ICAO agreed to develop a global market-based mechanism to 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[1], including only the flights between airports located in the EEA into the Emission Trading Scheme (ETS) until the global measure enters into force (see [17]). 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 [18]).

The European Commission initially planned to require all airlines flying to and from European Union airports to join the ETS, in which permits would be needed for the emissions in the European airspace from all flights, regardless their operator origin. However, airlines asked for a global solution, leading the EC to develop the "stop the clock". The decision had been reviewed and the EC accepted to wait for a global solution by the International Civil Aviation Organization (ICAO). By 2014, emissions from the aviation sector is capped at 95-percent of the annual average from the years 2004 to 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

[1] Decision No. 377/2013/EU

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 tonne 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 industrialized 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 [18]).

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 two hours. 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 many researches have been devoted to the estimation of its economic impact ([12], [13], [19], [20], [21], [22]). 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 hypothesized 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 section, we first tackle the problem by introducing a SMC paradigm for this specific business case. This paradigm allows airlines to trade emission rights without publicly revealing their target prices. While this has mainly been tackled as a secondary market problem involving agreements between airlines, this business case can also be expanded to primary market situations which can involve not only airlines but other industries involved in bidding process. As this business study is designed to mitigate confidentiality risks, we expect it to be relevant to airlines, in what refers to the lack of confidentiality of the ETS.

V. Application of SMC to Aviation CO_2 Allowance Trading

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. As the allowances allocated to aircraft operators is valid only in aviation industry, airlines cannot sell CO_2 allowance to other industries [23]. However, in both transactions, revealing the bids publicly 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 EU ETS scheme is implemented. In a hypothetical case, an airline can acquire additional CO_2 allowance capacity and may decide against renewing its aging 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 scheme geography.

Although there are two types of markets for auctioning process, the underlying algorithms remain the same for both situations. There are three types of parties in an auctioning process: the buying airlines, the selling airline/industry, and the referee. This is depicted both in the primary (Figure 3) and secondary (Figure 1) auction process. 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.

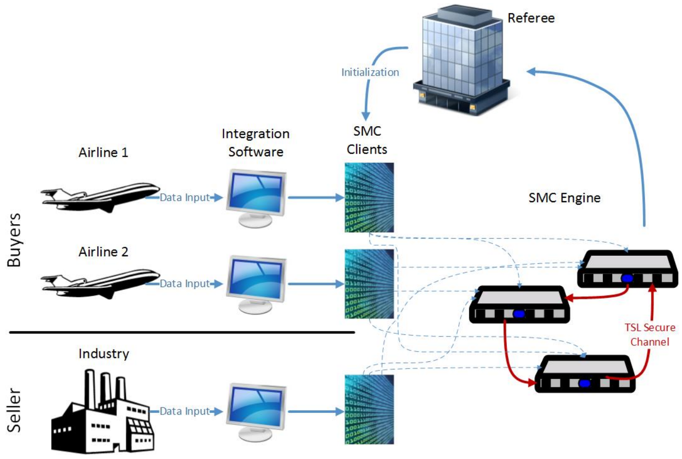

Fig. 3: Schematic representation of a SMC architecture for CO_2 allowance trading in a primary market.

A. 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. In the second scenario, 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 organized.
- Multi Round Auction – In this scheme, the number of auction rounds are determined before the auction starts. If there is no winning bid in a round, another round will be commenced. Also, elimination scenarios can be put into the auction scheme. 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.

B. The Computation Process

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 VI 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 organized. However, if there is one and only one winning bid, a winner will be declared.

C. The Integration Process

The integration process is in charge of creating, opening, managing and closing auctions. All participants should have individualized 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.

D. 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.

E. 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) Market Regulation Entity:
        - Wants a secure CO_2 allowance bidding process.
    b) 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.
    c) External Referee
        - 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.
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.
        - 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.
        - 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.
        - Monitors all processes and methods used to ensure quality.

VI. The secure computation

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. Specifically, we describe a simplified procedure which allows evaluating an inequality (*i.e.* $a < b$) between two integer and positive numbers - 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 described here: the interested reader may refer to [24] for further details and implementation considerations.

Let us start by considering 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. p should be chosen such that $a \in Z_p$ and $b \in Z_p$, *i.e.* that $a \in \{0, 1, \ldots, p-1\}$. In the sake of simplicity, we also suppose that both a and b can be easily expressed in a binary format. Thus a and b can be shared in a bit-based form; 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 $a \in \{0, 1\}$. 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[2].

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[3], for then compute $[d_i]_p = \vee_{j=i}^{l-1} [c_j]_p$ by using a Prefix-Or operation[4]. 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 I 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 should be split among the parties, such that no one has full knowledge of the other numbers.

VII. 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. 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, recognized 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

[2] In what follows, we denote by $[\cdot]$ any variable that is shared among the parties.

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

[4] 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 [25].

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

TABLE I: Example of the secure evaluation of the $a < b$ binary inequality, for two sets of initial numbers. Here $p = 5$ (and thus $Z_p \in \{0 \dots 4\}$) and $l = 3$.

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.

Acknowledgment

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 re- flect 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

[1] J. S. Meserole and J. W. Moore, *What is System Wide Information Management (SWIM)?*. Aerospace and Electronic Systems Magazine, IEEE, 22(5), pp. 13–19, 2007.

[2] C. Cachin, *Efficient private bidding and auctions with an oblivious third party.* In Proceedings of the 6th ACM conference on Computer and communications security, pp. 120–127, 1999.

[3] I. Dåmgard, M. Geisler and M. Krøigaard, *Efficient and secure comparison for on-line auctions.* In Information Security and Privacy, pp. 416-430, 2007.

[4] O. Catrina and F. Kerschbaum, *Fostering the uptake of secure multiparty computation in e-commerce.* In Third International Conference on Availability, Reliability and Security, pp. 693–700, 2008.

[5] H. Vegge, *Realizing Secure Multiparty Computations.* 2009.

[6] D. Bogdanov, R. Talviste and Jan Willemson, *Deploying secure multiparty computation for financial data analysis.* In Financial Cryptography and Data Security, Springer Berlin Heidelberg, pp. 57–64, 2012.

[7] R. Pathak and S. Joshi, *Secure Multi-party Computation Protocol for Defense Applications in Military Operations Using Virtual Cryptography.* Communications in Computer and Information Science 40 (8), pp. 389–399, 2009.

[8] A. C. Yao, *Protocols for Secure Computations.* In Proceedings of the 23rd Annual Symposium on Foundations of Computer Science, 1982.

[9] A. Shamir, *How to share a secret.* Communications of the ACM, 22(11), pp. 612–613, 1979.

[10] G. R. Blakley, *Safeguarding cryptographic keys.* In Managing Requirements Knowledge, International Workshop on, pp. 313, 1979.

[11] M. Zanin, D. Pérez, G. Inalhan, C. Paşaoğlu and E. Álvarez Pereira, *SecureDataCloud: Introducing Secure Computation in ATM.* SESAR Innovation Days, Stockholm, 2013.

[12] Scheelhaase, J., and Grimme, W., *Emissions trading for international aviation- an estimation of the economic impact on selected European airlines*, Journal of Air Transport Management, 13, pg. 253-263, 2010.

[13] Toru, T., *European Air Traffic Facing Raising Fuel Prices and Carbon Permits: An Empirical Analysis*, IIOC Boston Proceeding, Rising Stars Session, 2011.

[14] European Commission, *Commission Regulation (EU) on ETS*, No 1143/2013, 2013.

[15] Boeing, *Boeing Current Market Outlook 2014*, 2014.

[16] FAA, *FAA Aerospace Forecast Fiscal Years 2013-2033*, 2013.

[17] European Union, *Document L:2014:129:TOC*, Official Journal of the European Union, L 129, 30 April 2014, 2014.

[18] European Commission, *Aviation emissions: Commission proposes applying EU ETS to European regional airspace from 1 January 2014- MEMO/13/906 16/10/2013*, 2014.

[19] Albers, S., Buhne, J., and Peters, H., *Will the EU-ETS instigate airline network reconfigurations?*. Journal of Air Transport Management, vol. 15, 1-6, 2009.

[20] Brueckner,J.K. and Zhang, A., *Airline emission charges: Effects on airfares, service quality, and aircraft design*, Transportation Research Part B: Methodological, Volume 44, Issues 8-9, September-November 2010, pg. 960-971, 2010.

[21] Scheelhaase, J., Grimme, W., Schaefer, M., *The inclusion of aviation into the EU emission trading scheme - impacts on competition between European and non-European network airlines*, Transportation Research (Part D), Vol. 15, pp. 14-25, 2010.

[22] Vespermann, J., and Wald, A., *Much Ado about Nothing? - An analysis of economic impacts and ecologic effects of the EU-emission trading scheme in the aviation industry*, Transportation Research Part A: Policy and Practice, Elsevier, Elsevier, vol. 45(10), pages 1066-1076, 2011.

[23] Faber J, Brinke L., *The Inclusion of Aviation in the EU Emissions Trading System, An Economic and Environmental Assessment*, ICTDS Global Platform on Climate Change, Trade and Sustainable Energy, 2011.

[24] T. Nishide and K. Ohta, *Multiparty computation for interval, equality, and comparison without bit-decomposition protocol.* In Public Key CryptographyPKC 2007, pp. 343–360, 2007.

[25] A. K. Chandra, S. Fortune and R. J. Lipton, *Lower bounds for constant depth circuits for prefix problems.* ICALP, pp.109–117, 1983.