Received: 2 November 2022 | Revised: 1 March 2023 | Accepted: 13 March 2023

DOI: 10.1049/qtc2.12059

ORIGINAL RESEARCH

Quantum privacy-preserving service for secure lane change in vehicular networks

Zeinab Rahmani[1,2,3] | Luis S. Barbosa[3,4,5] | Armando N. Pinto[1,2]

[1]Departamento de Eletrónica, Telecomunicações e Informática, Universidade de Aveiro, Aveiro, Portugal

[2]Instituto de Telecomunicações, Aveiro, Portugal

[3]International Iberian Nanotechnology Laboratory, Braga, Portugal

[4]Department of Computer Science, University of Minho, Braga, Portugal

[5]Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência, Porto, Portugal

Correspondence

Zeinab Rahmani.
Email: zeinab.rahmani@ua.pt

Funding information

Quest Project, Grant/Award Number: UIDB/50008/2020; Faculdade de Ciências e Tecnologia, Grant/Award Number: SFRH/BD/151111/2021

Abstract

Secure Multiparty Computation (SMC) enables multiple parties to cooperate securely without compromising their privacy. SMC has the potential to offer solutions for privacy obstacles in vehicular networks. However, classical SMC implementations suffer from efficiency and security challenges. To address this problem, two quantum communication technologies, Quantum Key Distribution (QKD) and Quantum Oblivious Key Distribution were utilised. These technologies supply symmetric and oblivious keys respectively, allowing fast and secure inter-vehicular communications. These quantum technologies are integrated with the Faster Malicious Arithmetic Secure Computation with Oblivious Transfer (MASCOT) protocol to form a Quantum Secure Multiparty Computation (QSMC) platform. A lane change service is implemented in which vehicles broadcast private information about their intention to exit the highway. The proposed QSMC approach provides unconditional security even against quantum computer attacks. Moreover, the communication cost of the quantum approach for the lane change use case has decreased by 97% when compared to the classical implementation. However, the computation cost has increased by 42%. For open space scenarios, the reduction in communication cost is especially important, because it conserves bandwidth in the free-space radio channel, outweighing the increase in computation cost.

KEYWORDS

quantum communication, quantum computing, quantum cryptography, quantum optics

1 | INTRODUCTION

Vehicular networks have great potential to improve road safety and passengers' convenience. Overtime, many applications, such as parking and toll payments [1], traffic management, car sharing [2] and collision warning [3] have been proposed. Despite all the advantages they provide, vehicular networks face privacy and security challenges [4]. On one hand, they inherit properties of wireless communication that causes the data to be easily eavesdropped; on the other hand, vehicles are located in open spaces, leading to potential privacy leakage that poses a threat to the lives and properties of the drivers.

Secure Multiparty Computation (SMC) is one of the promising methods to solve the privacy and security challenges in vehicular networks as it enables Vehicle-to-Everything (V2X) communications such that multiple vehicles can cooperate freely while no information about their private inputs is revealed to other parties [5]. In the 1980s, Andrew Yao presented the SMC concept, in which two untrusted parties compute a garbled circuit while retaining the privacy of their inputs [6]. Later, protocols for secure computation with more than two parties, such as the BMR protocol [7] which is an adaptation of the garbled circuit protocol for the multiparty situation, and the BGW protocol [8] which relies on secret sharing but focuses on arithmetic circuits, were developed. Afterward, protocols based on preprocessing models in which expensive computations are delegated to the offline phase were designed to accelerate the computation process [9–11]. Shortly after, the Faster Malicious Arithmetic Secure Computation with Oblivious Transfer (MASCOT) protocol [12] that realizes secure computation of arithmetic circuits over finite fields with dishonest majority, was presented in a preprocessing model. Despite the progress made in this area, classical SMC protocols suffer from two main challenges: security and efficiency.

Classical SMC implementations are based on public-key cryptography requiring large computation and communication costs, making it difficult to meet the security and efficiency requirements of vehicular network applications [13]. Additionally, classical SMC implementations that are based on prime number factorization or discrete logarithms are not secure in the presence of quantum computers due to Shor's algorithm [14]. Although post-quantum public-key protocols are being developed to address these challenges, it remains to be proven that they can offer a solution that complies with the security and efficiency requirements [15]. To overcome classical SMC constraints, quantum-based approaches were proposed. In 1984, Bennet and Brassad proposed a Quantum Key Distribution (QKD) protocol, known as BB84, in which symmetric keys are generated and distributed between two parties [16]. A significant property of the QKD is that an eavesdropper attempting to measure a quantum state introduces detectable perturbations [16]. Many researchers have been exploring the potential of quantum key distribution to provide secure communication [17–23]. In [17], evolution of quantum key distribution networks and their potential applications are investigated. In [18], a short survey of the current state of quantum key distribution technology and its potential applications in communication networks are provided. It discusses the challenges associated with industrialising the technology and outlines the research trends. In [19], different types of QKD protocols are discussed in various networking scenarios, and opportunities associated with their usage in networking are highlighted. In mobile network applications such as vehicular networks, satellite-based QKD could be deployed to transfer keys among vehicles [24–28]. In [24], authors discussed the progress in the field of satellite QKD, which is a secure communication technology to transmit encryption keys. Furthermore, the advantages of using satellites for QKD, such as their ability to provide global coverage, are explored. In [25], a new satellite-based QKD system that can provide secure communication over long distances is proposed. In [26], a protocol for satellite-to-ground QKD using a quantum repeater is presented. Their protocol is based on a quantum teleportation technique, which allows for the transfer of quantum information between two remote locations. Later in [29], the Quantum Oblivious Key Distribution (QOKD) protocol that generates and distributes quantum oblivious keys was introduced. Using quantum oblivious keys, [30] proposed the Optimise Quantum Oblivious Transfer (O-QOT) protocol that generates quantum-based Oblivious Transfers (OT). In [31], authors provided an overview of quantum oblivious transfer by investigating several quantum security models to emphasize the advantages of quantum OT over classical implementations.

In this paper, we propose a quantum secure SMC solution based on QKD, QOKD, and the MASCOT protocols for lane change in vehicular networks. The proposed solution is secure even against quantum computer attacks. In terms of efficiency, the needed communication resources are reduced by 97% while the computational resources are increased by 42%. The strong reduction in communication cost is of major relevance in vehicular networks, as the available spectrum to support the radio channel is a finite resource.

In the reminder of the paper, Section 2 presents a lane change service that assists vehicles to exit the highway safely. In Section 3, we develop a QSMC framework that uses QKD and QOKD quantum technologies alongside the MASCOT protocol to implement the lane change service. Section 4 describes the classical S-OT and OT Extension protocols. In Section 5, we provide security and complexity analysis of the classical and quantum protocols. Finally, Section 6 concludes the paper.

2 | THE LANE CHANGE SERVICE

Changing a lane when exiting the highway is one of the main causes of heavy traffic and sometimes even large chain crashes [4]. This section describes the implementation of a lane change service that assists vehicles to switch lanes and exit the highway safely. We consider n numbers of vehicles $\{v_1, v_2, \dots, v_p, \dots, v_q, \dots, v_n\}$ with locations $\{x_1, x_2, \dots, x_n\}$ and velocities $\{s_1, s_2, \dots, s_n\}$ in an m-lane highway and assume a subset of vehicles $\{v_p, \dots, v_q\}$ intend to exist on the highway. Therefore, they call for the lane change service to help them through the exit process. In the first step, the service asks for the private information of all the vehicles close to the exit point (e.g. vehicles that are within a radius of 5 km of the exit location). The private inputs for the proposed service are location, velocity, lane number, and exit intention of all the vehicles in the network. These inputs are then used to compute the proper times for vehicles that intend to exit the highway, considering the density of neighbouring vehicles. The exit intention is a Boolean flag b such that 0 represents no exit intention and 1 represents the intention to exit. Therefore, when a vehicle v_i intends to exit the highway, it changes its Boolean flag b_i to 1 and subsequently the protocol is activated. Next, the service asks for the following private inputs from each vehicle v_i:

- The vehicle's private location x_i
- The vehicle's private velocity s_i
- The vehicle's private lane number l_i
- The vehicle's private exit intention b_i

Given the exit location x_e as a constant parameter and the private location of the ith vehicle (x_i), the service computes the distance of each vehicle to the exit ($\Delta x_i = |x_e - x_i|$). As we are considering the highway as a straight path, the distance calculation can be done in one dimension. Note that this is not an unrealistic assumption as we only consider vehicles close to the exit point. Using the distance Δx_i and considering the formula $\Delta x = st$, the service computes the time that each vehicle takes to reach the exit point x_e. Considering the time difference between vehicles, the service evaluates the density of the neighbouring vehicles and computes the proper times for the desired vehicles to exit the highway. Through this service, each vehicle is supposed to gradually reduce its lane number step by step to decrease its distance from the exit point. Therefore, the service first checks the lane number l_i of the vehicles intending to exit. If l_i is equal to the exit lane, only one step calculation of $t_i = \Delta x_i / s_i$ is enough to compute the proper time. Otherwise, vehicles have to reduce their lane number to reach the exit lane, and for each lane change, a pair (t_c, l_c) is provided by the service. To compute the pair, the service only considers vehicles in the adjacent lane (l_c). Then, it computes the time difference Δt between the desired vehicle and the next approaching vehicle in the adjacent lane. The computation is continued until Δt reaches a value that is long enough for a vehicle to change its lane (e.g. 30 s). Using the same strategy, vehicles change their lanes until they reach the exit lane. Note that, in case the highway was crowded and there was no proper time for a vehicle to change the lane, a message would be sent to the approaching vehicles asking them to adjust their speed and provide empty space for the desired vehicle. In addition to these details, the service also provides the number of exiting vehicles as well as their approximate departure time, to the whole network. These outputs increase safety throughout the network, as vehicles are aware of all the ongoing events around them. The proposed service provides the following outputs:

- Each exiting vehicle receives its unique pair (t_c, l_c), for each lane change.
- The total number of exiting vehicles n_v, as well as their approximate exit time is provided to the whole network, to increase safety.

Note that the outputs could be announced either publicly or could be sent only to specific vehicles, in order to be kept private. In the lane change service some outputs are public while the others are sent only to specific vehicles in an encrypted way.

Figure 1 illustrates with a simplified example, the proposed service. Suppose that seven vehicles are driving on a highway with three lanes. One of the vehicles, v_1, in lane three (l_3) intends to exit the road, while the others continue on their paths. The service computes the time difference between v_1 and v_4 that is the nearest approaching vehicle in l_2, and obtains $\Delta t_1 = 10$ s. Since Δt_1 is too short, the computation is repeated for v_4 and v_5, and the result is $\Delta t_2 = 35$ s, which is considered long enough for v_1 to switch to the adjacent lane l_2. At this stage, a message with the content *'Please reduce your speed to ...and switch to l_2 after 10 s'* is sent to v_1. The same strategy is applied until v_1 switches to l_1 and exits the highway. Additionally, the other vehicles receive a message with the content *'A vehicle is exiting the highway at ...'*. It is interesting to note that, through the whole computation process, the vehicles' private information (location, velocity, lane number, exit intention) is not revealed to the other vehicles.

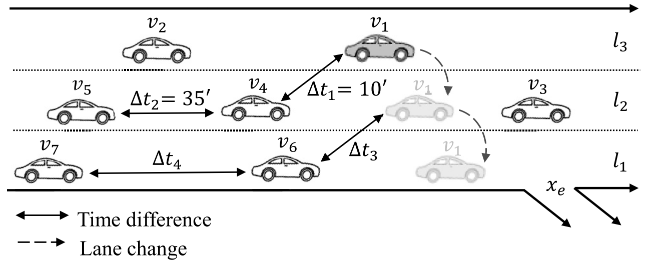

FIGURE 1 An example of the lane change service in a 3-lane highway with seven vehicles of which the vehicle v_1 intends to exit the highway. v. stands for vehicle, Δt. is the time difference between vehicles, l is the lane number in the highway, and x_e is the exit location. The values for Δt are chosen hypothetically for better illustration.

3 | QUANTUM IMPLEMENTATION

We propose a QSMC platform based on the OT-based MASCOT protocol to implement the lane change service securely and efficiently. Alongside MASCOT, we use the QKD and QOKD quantum protocols. The required technologies are described below. In [32], a study has been accomplished in which a QSMC approach is proposed to compute the phylogenetic tree from private genome sequences using quantum technologies. Their results show that quantum technologies can enable the private computation of phylogenetic trees with a low computational overhead.

In Table 1, we provide the list of acronyms used in this work, for more clarity.

3.1 | MASCOT multiparty protocol

Several protocols were developed to implement SMC [33–36]. To accomplish the lane change service in vehicular networks, we employ the MASCOT multiparty protocol that uses arithmetic circuits with active security [12]. MASCOT is an OT-based protocol. Consider Alice and Bob as two communicating parties. A 1-out-of-2 OT protocol takes m_0 and m_1 as Alice's inputs and $b \in \{0, 1\}$ as Bob's input. Then it outputs m_b to Bob

TABLE 1 List of acronyms used in this work.

Acronym	
AES	Advanced Encryption Standard
CV	Continuous Variable
DV	Discrete Variable
MASCOT	Faster Malicious Arithmetic Secure Computation with Oblivious Transfer
O-QOT	Optimised Quantum Oblivious Transfer
OT	Oblivious Transfer
QOKD	Quantum Oblivious Key Distribution
QSMC	Quantum Secure Multiparty Computation
SMC	Secure Multiparty Computation
S-OT	Simple Oblivious Transfer

and nothing to Alice. Through this protocol, Bob only obtains information about one message (m_b) and he learns nothing about the other message, and Alice learns nothing about Bob's choice (b). The advantage of the OT primitive is that it can be implemented using quantum technologies and independently of public-key cryptography, making it secure and efficient. MASCOT combines the online phase of the SPDZ protocol with an OT-based offline phase. The OT generation in MASCOT is done through the classical Simple OT (S-OT) protocol [37]. Along with the S-OT, MASCOT uses an OT Extension protocol to extend the number of generated base OTs [38]. This extension is necessary in SMC applications that require a very large number of OT per second.

3.2 | QKD and QOKD quantum technologies

In this section we provide a short overview on quantum technologies that are used in this work: QKD and QOKD. It is worth noting that although QKD and QOKD can be implemented using similar setups, they fulfil different purposes. Through QKD, we are able to apply encryption on the transformed messages, while QOKD is considered as a source of OT generation.

3.2.1 | Quantum key distribution

In order to secure communication among vehicles, we need to perform encryption on the transferred data. To this end we use the Advanced Encryption Standard (AES) [39] through the OpenSSL library. AES requires symmetric keys for encryption and decryption of the parties' private data. We use the QKD protocol [16], as a source to generate quantum-based symmetric keys. As a feature of QKD, a third party trying to eavesdrop on the symmetric keys introduces detectable perturbations. In practice, QKD can be implemented using two different approaches: Discrete-Variable Quantum Key Distribution (DV-QKD) and Continuous-Variable Quantum Key Distribution (CV-QKD). Due to our need for short-range communication in a lane change service, CV-QKD is a more suitable option as it provides a higher secure key rate over shorter distances. In vehicular network applications, vehicles transfer data through wireless communications because a physical connection cannot be established among them. Terahertz QKD has recently been demonstrated to be a viable solution for wireless mobile applications [40–43]. Satellite-based QKD is also a promising approach to transfer secure keys among vehicles in mobile networks [24–26]. However, a primary approach could be the use of QKD through optical fibres. The advantages of implementing QKD through optical fibre over wireless communications include improved reliability, lower cost, greater bandwidth, and higher security. As an example of a real-life situation, we can pre-share the keys using QKD, when the vehicles are being electrically charged. Notice that by pre-sharing the keys using QKD, we can avoid the use of classical public cryptography, therefore we achieve a quantum computer resistant solution.

3.2.2 | Quantum oblivious key distribution

The QOKD is a quantum-based protocol that enables two parties to produce quantum oblivious keys only known to them [29]. Oblivious keys are sequences of asymmetric keys in which one of the parties (Alice) knows all the keys while the other (Bob) has access to only half of the keys such that Alice gets no information about which keys are known to Bob. A significant property of QOKD is the ability of trusted parties to trace the presence of a third party trying to gain knowledge of the keys. In [30], a protocol known as O-QOT was proposed to generate oblivious transfer using QOKD. The O-QOT is implemented as follows:

As described in Protocol 1, the O-QOT receives two strings, m_0 and m_1, from Alice and c from Bob, then provides m_c to Bob. Therefore, Bob does not have access to other messages, and Bob's choice remains hidden from Alice. The O-QOT protocol contains two phases: the precomputation phase (oblivious key phase) that takes advantage of quantum technologies; and the transfer phase that performs secure computation. The oblivious key phase outputs k to Alice and $\tilde{k}$ to Bob as their oblivious keys. Note that only half of the bits of $\tilde{k}$ are identical to k; the other half is randomly generated. Along with $\tilde{k}$, Bob receives the bit stream x through which he can determine which bits are perfectly correlated with Alice's bits and which are not. The correlated bits are shown with 0, and the uncorrelated bits are represented with 1. Using the bit stream x, Bob can extract two strings, I_0 and I_1, where I_0 corresponds to the indices of oblivious keys that are known to Bob, while I_1 corresponds to the indices of oblivious keys that are unknown to Bob. Afterwards, he sends I_c to Alice according to his choice c. Next, Alice computes $e_i = m_i \oplus k|_{I_{c\oplus i}}$ for $i \in \{0, 1\}$ and transfers them to Bob. Finally, Bob obtains his output $m_c = e_c \oplus \left(k|_{I_0}\right)$. The notation $k|_{I_{c\oplus i}}$ refers to indices of the oblivious key k that corresponds to $I_{c\oplus i}$, and $\oplus$ denotes the bitwise XOR.

As all heavy computations are shifted to the oblivious key phase, and this phase is implemented before and independently of the second phase, the complexity cost of OT generation through this protocol is significantly reduced.

Protocol 1 O-QOT

```
Inputs: Strings $m_0$ and $m_1$ for Alice, and the bit $c$ for Bob.
Outputs: None for Alice and $m_c$ for Bob.

Oblivious key phase:
  1. Alice asks for a QOKD service. The QOKD service transfers $k$ to Alice and $(\tilde{k}, x)$ to Bob as their oblivious keys.
```

```
Oblivious transfer phase:
  1. Bob determines $I_0 = \{i | x_i = 0\}$ and $I_1 = \{i | x_i = 1\}$, and transfers to Alice only $I_c$
(instead of the ordered pair ($I_c$, $I_{c\oplus 1}$) which is used in QOT protocol).
  2. Alice sets $e_0$, $e_1$ such that $e_i = m_i \oplus k|_{I_{c\oplus i}}$
and sends them to Bob.
  3. Bob outputs $m_c = e_c \oplus \left(k|_{I_0}\right)$.
```

3.3 | Circuit generation

There are different ways of representing a computation, of which Boolean and arithmetic circuits are the most common. Boolean circuits use bit inputs and Boolean operations such as XOR and AND. In contrast, arithmetic circuits use elements of some field F as their inputs, and the gates of the circuit correspond to arithmetic operations such as additions and multiplications. Deciding whether to use a Boolean or arithmetic circuit depends on the type of computation performed. For arithmetic operations, it makes more sense to use an arithmetic circuit, while for non-arithmetic operations, such as integer comparison, Boolean circuits may reach higher efficiency. The computation in MASCOT is represented as an arithmetic circuit. As the lane change use case mainly requires arithmetic operations, such as multiplication and addition, the use of protocols with arithmetic circuits is more efficient. To generate a circuit that corresponds to the lane change service, we convert the proposed service described in section 2 to a mathematical function f. To accomplish this, the calculation is performed by function $f(x_1, v_1, l_1, b_1; \ldots; x_n, v_n, l_n, b_n)$ in which all parties provide their private data as inputs. Circuit generation is done through the MP-SPDZ repository [34] which is a versatile framework to benchmark various multiparty computation protocols such as MASCOT.

3.4 | QSMC platform

In Figure 2, a pictorial representation of the QSMC platform for the lane change use case is provided. To form the quantum SMC platform, we start by generating quantum oblivious keys through QOKD. Afterwards, using the keys, we generate oblivious transfer through the O-QOT protocol. As the OT generation in the MASCOT implementation is done through the *BaseOT::exec_base* method in the MP-SPDZ repository [34], we ask this method to make a call to the O-QOT protocol instead of the classical protocols (S-OT and OT Extension). Moreover, we utilise the QKD protocol to generate symmetric keys that are then used for AES encryption. Afterwards, we define the desired use case that is then converted to an arithmetic circuit. The circuit is integrated into MASCOT through the MP-SPDZ repository. The implementation steps are ordered as follows:

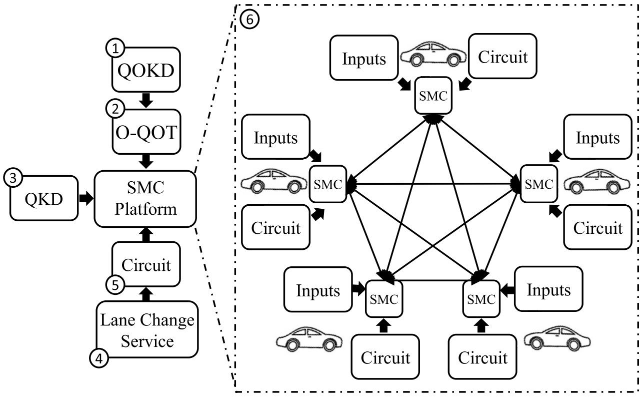

FIGURE 2 The QSMC functionality in vehicular networks for the lane change service. We start by generating quantum oblivious keys, quantum OTs, and quantum symmetric keys through Quantum Oblivious Key Distribution (QOKD), O-QOT, and Quantum Key Distribution (QKD) protocols, respectively. Afterwards, we define the lane change use case as a function f and then, we convert f to a circuit C by using high-level Python code compatible with the SMC platform. Finally, we perform secure computation among vehicles using their private inputs. Numbers 1 to 6 are associated with the implementation steps of the QSMC platform explained in the text.

1. Generation of quantum oblivious keys through QOKD.
2. Generation of quantum OTs through O-QOT protocol.
3. Generation of quantum symmetric keys through the QKD protocol to perform encryption and decryption using AES.
4. Definition of the lane change service as a function f, as described above.
5. Conversion of function f to an arithmetic circuit using the MP-SPDZ repository.
6. Performing secure computation among different parties by feeding the vehicle's private inputs into the QSMC platform and outputting the results.

The hierarchy of implementation steps is labelled with its corresponding number in Figure 2.

4 | CLASSICAL OBLIVIOUS TRANSFERS

Classical SMC protocols face security and efficiency challenges. However, they are the only available baseline to be compared with the quantum approach proposed here. In this section, we describe the S-OT and OT Extension protocols. Afterwards, we provide a comparison analysis of the quantum and classical protocols in the next section.

The OT functionality used in MASCOT is based on [37], a classical protocol derived from the Diffie-Hellman (DH) key exchange in which players exchange secret keys in a secure way over a public communication channel. The protocol is known as Simple OT (S-OT), and is implemented as follows: given a group $\mathbb{G}$ and a generator g, the sender (Alice) picks a random value a, calculates $A = g^a$ and sends it to the receiver (Bob). The generator g is a member of $\mathbb{G}$ such that $\forall i \in \mathbb{G}, \exists r : g^r = i$. Symmetrically, Bob samples a random value b and calculates B according to his arbitrary choice c. If

$c = 0$, the receiver obtains $B = g^b$, and if $c = 1$, he obtains $B = Ag^b$ and sends it to Alice. Both players obtain $g^{ab} = A^b = B^a$ and derive their corresponding secret keys. Alice computes $k_0 = H(B^a)$ and $k_1 = H((B/A)^a)$ (H for hash) to obtain her keys. Symmetrically, Bob computes $k_R = H(A^b)$ according to his bit choice c. Having these keys, we can start to implement the oblivious transfer functionality, as shown in Protocol 2. Next, Alice encrypts her input messages m_0 and m_1, and obtains $e_0 = E_{k_0}(m_0)$ and $e_1 = E_{k_1}(m_1)$ (E for encryption), which are then sent to Bob. Bob computes $m_c = D_{k_R}(e_b)$ (D for decryption) according to his bit choice by decrypting e_b and obtains the output message. Note that Bob can only decrypt one of the messages as he only has access to one of the keys.

Protocol 2 S-OT

```
Inputs: Strings $m_0$ and $m_1$ for Alice, and the bit $c$ for Bob.
Outputs: None for Alice and $m_c$ for Bob.

Key exchange phase
  1. Alice calls a DH key exchange service, which sends $k_0 = H(B^a)$ and $k_1 = H((B/A)^a)$ to Alice, and $k_R = H(A^b)$ to Bob.

Oblivious transfer phase:
  1. Alice computes $e_0 = E_{k_0}(m_0)$ and $e_1 = E_{k_1}(m_1)$ by encrypting her input massages and sends them to Bob.
  2. Bob decrypts one of the messages using his key and obtains the output message $m_c = D_{k_R}(e_b)$.
```

4.1 | The classical OT extension

We require a large number of OTs per second to perform practical computations through SMC protocols. MASCOT uses the S-OT protocol to generate few number of base OTs (128 base OTs) which are then extended via the OT Extension protocol, using symmetric cryptography [38]. The number of extended OTs depends on the number of multiplication triples that are necessary to compute the multiplication gates of the circuit. MASCOT requires 1408 OT Extension for each multiplication triple, considering a 128 bit filed with the constant parameter $\tau = 3$ and the statistic and computational security parameters $\kappa = \lambda = 128$ (see section 7.1 of [12]). In [38], the communication and computation complexity of the OT Extension protocol used in MASCOT are computed. The results show that in terms of computation resources, the OT Extension is very efficient.

5 | RESULTS AND DISCUSSION

The security and efficiency of SMC protocols heavily rely on the security and efficiency of the generated OTs. In the QSMC platform proposed in this paper, we generate OTs using quantum technologies. Therefore, we provide a comparison analysis for n executions of OTs between the classical OT protocols used in MASCOT and the O-QOT protocol used in the proposed QSMC platform.

5.1 | Security analysis

5.1.1 | Security model

The lane change service has been implemented through an SMC scenario with active security in the malicious adversarial model. In this model, dishonest parties may haphazardly drift from the protocol execution and try to cheat. Protocols that achieve security in the malicious adversary scenario have the highest security level, which means that the only thing that an adversary can do is to cause the honest parties to abort, but can never preclude the privacy of others.

5.1.2 | Security level

The security of the classical S-OT protocol relies on the assumption that parties are not able to compute the discrete logarithm of a random value due to the limited computational power. However, in 1995, Peter Shor published a quantum algorithm that can perform the computation of the discrete logarithm in polynomial time. The algorithm can also solve the prime number factorization problem. This poses a threat to asymmetric cryptographic methods that are based on prime number factorization or discrete logarithms, including elliptic curve cryptography, RSA, and DH key exchange. While security of the classical S-OT relies on the computational assumptions of parties, the quantum O-QOT is unconditionally secure even against quantum computers. This is because the key generation in O-QOT is done using quantum technologies that can be implemented independently of the public-key infrastructure, making it secure against quantum computer attacks. Quantum technologies rely on the no-cloning theorem, which makes it impossible to duplicate a quantum state without introducing detectable perturbations. Note that the OT Extension is considered secure as it is based on symmetric cryptography.

5.2 | Efficiency analysis

To evaluate our system, we compare the complexities of the quantum and classical protocols. In Tables 2 and 3, the computation and communication complexity of the O-QOT, S-OT, and OT Extension are represented. The values inside parenthesis refer to the cost of OT Extension. By communication complexity we mean the number of bits that are transferred among parties. The computational complexity is the amount of resources required to run the circuit, which particularly focuses on time and memory requirements.

We first consider the operations in the classical S-OT protocol (i.e. random number generation, modular

TABLE 2 Comparison of the communication complexities between quantum and classical approaches. S-OT stands for Simple Oblivious Transfer, O-QOT represents Optimised Quantum OT, RNG is random number generation, and n is the number of OTs.

	Quantum O-QOT	Classic S-OT and OT extension
Bit sent	$3n$	$2n + (128n + 10000)$

TABLE 3 Computation complexity of the O-QOT and S-OT protocols. S-OT stands for Simple Oblivious Transfer, O-QOT represents Optimised Quantum OT, and RNG is random number generation, and n is the number of OTs. The dash symbol '-' means the specified operation is not used in the protocol.

Operation	Quantum O-QOT	Classic S-OT and OT extension
Bitwise comparison	$3n$	-
Bitwise truncation	$7n$	-
Bitwise XOR	$5n$	$3n$
RNG	$3n$	$2n$
Hash	-	$3n + (2n + 336)$
Modular exponentiation	-	$5n$
Quantum state preparation	n	-
Quantum state measurement	n	-

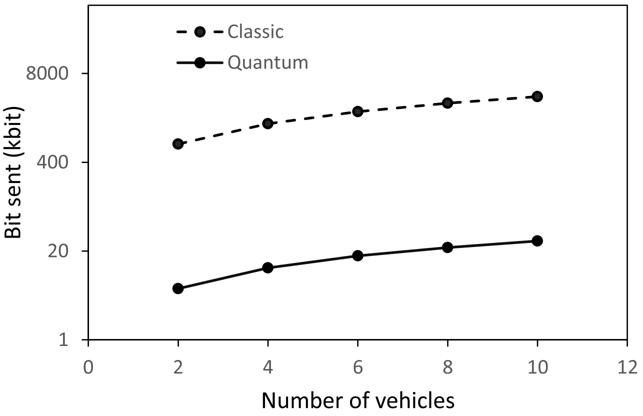

FIGURE 3 The communication cost of the classic and quantum models for various numbers of vehicles. We calculated the communication cost by taking into account the number of bits sent among parties, which is shown in Table 2. We calculated the number of OTs (n), considering the number of vehicles. Afterwards, we substituted n in Table 2 with the obtained value. As the costs for classic and quantum approaches are vastly different, the results are plotted on a logarithmic scale. Further details can be found in the text.

exponentiation, hash evaluation, and encryption operations). We consider the cost of each operation as follows:

1. Sampling a random number (RNG)
2. Computing A or B (modular exponentiation)
3. Computing $g^{ab} = A^b = B^a$ (modular exponentiation)
4. Computing each key using the hash function (hashing)
5. Encryption or decryption of each message (XOR)

In total, the S-OT protocol requires two random numbers, five modular exponentiation, three hashing, and three XOR (two for applying the encryption on Alice's messages, and one for decryption of a message by Bob). Also, the communication cost of the S-OT is $2n$ bits for n executions of OT. In addition to the S-OT protocol, MASCOT uses an OT Extension protocol that costs $2n + 336$ hashing for computations, and $128n + 10$ $kbit$ for communication purposes [38]. Similar to the classical protocols, we computed the complexity of the O-QOT protocol.

Table 2 represents the communication complexity of quantum and classical protocols. As it can be seen, the cost of O-QOT protocol is $3n$ which is always less than classical cost $2n + (128n + 10{,}000)$, regardless of the value of n (number of OTs).

Table 3 shows the computational complexity of quantum and classical protocols. To fairly compare the costs of the quantum and classic cases, we first need to consider the cost of each operation separately. For example, modular exponentiation is much more expensive than linear operations, such as bitwise XOR. One way to compare these operations is by calculating the execution time of them. Note that since the offline phase of protocols can be done in advance and independently of the user's private inputs, we only measure the execution times for operations in the online phase. Through the online phase, the S-OT requires $3n$ bitwise XOR, while the O-QOT needs $2n$ bitwise comparisons, $5n$ bitwise XORs, and $3n$ bitwise truncations. Moreover, the S-OT transfers $2n$ bits, while the O-QOT transfers $3n$ bits for communication during the online phase. We computed the execution time using the high_resolution_clock of the <chorno> library in C++. We carried out the implementations on Ubuntu (64-bit) 20.04 on ASUS Zenbook 14 UX425E laptop with 4 cores and an 11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz processor, and 16 GB of RAM.

We obtained the number of generated OTs (n) for the proposed lane change service as follows. For each vehicle, we require one multiplication gate to compute the relation $\Delta x = st$. According to the MASCOT protocol, each multiplication gate requires 2 multiplication triples, and each triple requires 128 base OT as well as 1408 OT Extension. The number of multiplication gates in the lane change service depends on the number of vehicles. Considering the number of vehicles, we calculated the amount of the transferred bits among vehicles and the run time for the quantum and classical protocols. The results are illustrated in Figures 3 and 4.

In Figure 3, the amount of the transferred bits for different number of vehicles $n_p = 2, 4, \ldots, 10$ is shown. For example, when two vehicles are in the highway, the communication costs are 5.6 and 742.2 $kbit$ for the quantum and classic protocols, respectively. As expected, by increasing the number of vehicles from 2 to 10, the total cost increases to 28 and 3670.8 $kbit$. In average, the communication cost of the O-QOT is significantly reduced by 97% for the lane change service. To obtain this value, we first compared the communication cost of the quantum and classic for n_p number of vehicles separately and

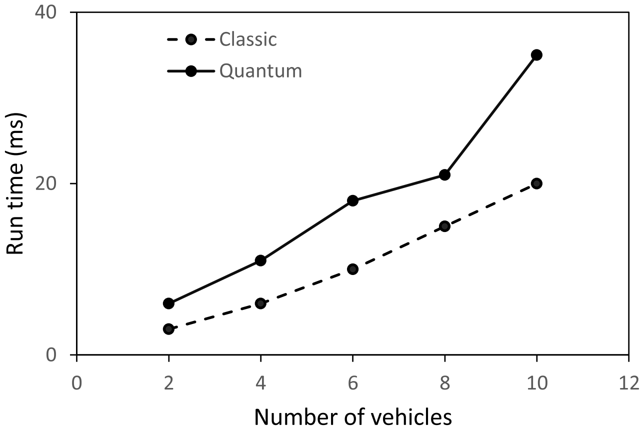

FIGURE 4 The run times of the classic and quantum models for various numbers of vehicles. To perform this computation, we considered the execution times for operators presented in Table 3. To this end, we used *high_resolution_clock* from <*chorono*> library in C++.

took the average. Despite the reduction in communication resources, the execution time of the O-QOT is higher than classical protocols by 42%, as shown in Figure 4. However, the strong reduction in communication cost is more relevant for vehicular network applications, as the available spectrum to support the radio channel is a finite resource. The value for computation cost is also obtained by taking the mean of five values for n_p number of vehicles. In [32], authors suggested an SMC system that utilises quantum cryptographic protocols to calculate a phylogenetic tree from a collection of confidential genome sequences. Similar to our work, [32] offers improved security against quantum computer attacks. Furthermore, they assessed the total running time of both quantum and classical systems, and their results showed that the quantum approach had a longer execution time, which is in line with our findings.

6 | CONCLUSION

Vehicular network applications suffer from security challenges. We use SMC technology in which several players can simultaneously compute a function while keeping their input private and secure. However, classical SMC implementations are prone to security and efficiency issues. Therefore, we proposed a quantum-based SMC framework that uses two quantum technologies (QKD and QOKD). This was applied to a lane change service in vehicular networks that guides vehicles to switch lanes and exit the road safely. We compared the security and complexity of the classical approach with the quantum one. The classical S-OT protocol is not secure against quantum computer attacks as it is based on public-key cryptography, while the O-QOT protocol is unconditionally secure even when quantum computers are available. Moreover, the communication complexity of the O-QOT protocol is less than that of the classical OT. The execution time for the quantum approach is higher than the one considered in the classical one. However, for vehicular network applications, the reduction in communication cost tends to be more relevant as bandwidth in the free-space radio channel is a limited resource.

AUTHOR CONTRIBUTIONS

Zeinab Rahmani: Conceptualization; Investigation; Methodology; Software; Writing (original draft); Validation. **Luis S. Barbosa**: Supervision; Funding acquisition; Project administration; Writing (review and editing). **Armando N. Pinto**: Supervision; Conceptualization; Funding acquisition; Project administration; Resources; Writing (review and editing).

ACKNOWLEDGEMENTS

This work is funded by Fundação para a Ciência e a Tecnologia (FCT)/MCTES through national funds and when applicable co-funded EU funds under the project UIDB/50008/2020 (action QUESTS). The work of Zeinab Rahmani was supported by the FCT through Fundo Social Europeu and through national funds, by the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Programme (COMPETE 2020) of the Portugal 2020 framework under the INL Quantum Portugal Initiative PhD Grant Ref. SFRH/BD/151111/2021.

Open access funding provided by IReL.

CONFLICT OF INTEREST STATEMENT

All the authors have approved the manuscript and agreed with its submission to the *IET Quantum Communication* journal. There are no conflicts of interest to disclose. We also declare that this manuscript is original, has not been published before, and is not under consideration by any media, including journals and conferences.

DATA AVAILABILITY STATEMENT

Data available on request from the authors.

ORCID

Zeinab Rahmani https://orcid.org/0000-0001-6357-4923

REFERENCES

1. Popa, R.A., Balakrishnan, H., Blumberg, A.J.: VPRIV: protecting privacy in location-based vehicular services. In: Proceedings of the 18th Conference on USENIX Security Symposium, Ser. SSYM'09, pp. 335–350. USENIX Association (2009)
2. Symeonidis, I., et al.: SEPCAR: a secure and privacy-enhancing protocol for car access provision. In: Foley, S.N., Gollmann, D., Snekkenes, E. (eds.) Computer Security – ESORICS 2017, pp. 475–493. Springer International Publishing (2017)
3. Rahmani, Z., Barbosa, L., Pinto, A.N.: Collision warning in vehicular networks based on quantum secure multiparty computation. In: II Workshop de Comunicação e Computação Quântica WQuantum, pp. 1–6 (2022)
4. Lee, M., Atkison, T.: Vanet applications: past, present, and future. Vehicular Commun. 28, 100310 (2021). [Online]. https://doi.org/10.1016/j.vehcom.2020.100310 https://www.sciencedirect.com/science/article/pii/S2214209620300814
5. Song, C., Zhang, M., Peng, W.: Research on secure and privacy-preserving scheme based on secure multi-party computation for vanet. J. Inf. Hiding Multimedia Signal Process. 9, 99–107 (2018)

6. Yao, A.C.: Protocols for secure computations. In: 23rd Annual Symposium on Foundations of Computer Science (Sfcs 1982), pp. 160–164. IEEE (1982)
7. Beaver, D., Micali, S., Rogaway, P.: The round complexity of secure protocols. In: Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing, Ser. STOC '90, pp. 503–513. Association for Computing Machinery (1990). [Online]. https://doi.org/10.1145/100216.100287
8. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness Theorems for Non-cryptographic Fault-Tolerant Distributed Computation, pp. 351–371. Association for Computing Machinery (2019). [Online]. https://doi.org/10.1145/3335741.3335756
9. Bendlin, R., et al.: Semi-homomorphic encryption and multiparty computation. In: Advances in Cryptology – EUROCRYPT 2011, Ser. Lecture Notes in Computer Science, K.G. Paterson, Ed., vol. 6632 Springer Berlin Heidelberg, pp. 169–188 (2011)
10. Damgård, I., et al.: Multiparty computation from somewhat homomorphic encryption. In: Advances in Cryptology – CRYPTO 2012, Ser. Lecture Notes in Computer Science, R. Safavi-Naini and R. Canetti, Eds., vol. 7417. Springer Berlin Heidelberg, pp. 643–662 (2012)
11. Damgård, I., et al.: Practical covertly secure mpc for dishonest majority – or: breaking the spdz limits. In: Computer Security – ESORICS 2013, Ser. Lecture Notes in Computer Science, J. Crampton, S. Jajodia, and K. Mayes, Eds., vol. 8134. Springer Berlin Heidelberg pp. 1–18 (2013)
12. Keller, M., Orsini, E., Scholl, P.: Mascot: Faster malicious arithmetic secure computation with oblivious transfer. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Ser. CCS '16, pp. 830–842. Association for Computing Machinery (2016). [Online]. https://doi.org/10.1145/2976749.2978357
13. Fasbender, A., Kesdogan, D., Kubitz, O.: Variable and scalable security: protection of location information in mobile ip. In: Proceedings of Vehicular Technology Conference – VTC, vol. 2, pp. 963–967. IEEE (1996)
14. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev. 41(2), 303–332 (1999). [Online]. https://doi.org/10.1137/S0036144598347011
15. Bernstein, D.J., Lange, T.: Post-quantum cryptography. Nature 549(7671), 188–194 (2017). [Online]. https://doi.org/10.1038/nature23461
16. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. Theor. Comput. Sci. 560, 7–11 (2014). [Online]. https://doi.org/10.1016/j.tcs.2014.05.025 https://www.sciencedirect.com/science/article/pii/S0304397514004241
17. Cao, Y., et al.: The evolution of quantum key distribution networks: on the road to the qinternet. IEEE Commun. Surv. Tutorials 24(2), 839–894 (2022). https://doi.org/10.1109/comst.2022.3144219
18. Liu, R., et al.: Towards the industrialisation of quantum key distribution in communication networks: a short survey. IET Quan. Commun. 3(3), 151–163 (2022). [Online] https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/qtc2.12044
19. Mehic, M., et al.: Quantum key distribution: a networking perspective. ACM Comput. Surv. 53(5), 1–41 (2020). [Online]. https://doi.org/10.1145/3402192
20. Sidhu, J.S., et al.: Advances in space quantum communications. IET Quan. Commun. 2(4), 182–217 (2021). [Online] https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/qtc2.12015
21. Bloom, Y., et al.: Quantum cryptography—a simplified undergraduate experiment and simulation. Physics 4(1), 104–123 (2022). [Online]. https://doi.org/10.3390/physics4010009 https://www.mdpi.com/2624-8174/4/1/9
22. Scarani, V., et al.: The security of practical quantum key distribution. Rev. Mod. Phys. 81(3), 1301–1350 (2009). [Online] https://link.aps.org/doi/10.1103/RevModPhys.81.1301
23. Sharma, P., et al.: Quantum key distribution secured optical networks: a survey. IEEE Open J. Commun. Soc. 2, 2049–2083 (2021). https://doi.org/10.1109/ojcoms.2021.3106659
24. Bedington, R., Mantilla, J., Ling, A.: Progress in satellite quantum key distribution. NPJ Quan. Inf. 3(1), 30 (2017). https://doi.org/10.1038/s41534-017-0031-5
25. Khan, I., et al.: Satellite-based qkd. Opt Photon. News 29(2), 26–33 (2018). https://doi.org/10.1364/opn.29.2.000026
26. Liao, S.-K., et al.: Satellite-to-ground quantum key distribution. Nature 549(7670), 43–47 (2017). https://doi.org/10.1038/nature23655
27. Mukhopadhyay, A., et al.: Study of different performance measures and their relations in satellite-based and terrestrial quantum communication. IET Quan. Commun. 2(4), 230–245 (2021). [Online] https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/qtc2.12016
28. Endo, H., Sasaki, M.: Secret key agreement for satellite laser communications [international communications satellite systems conference]. In: IET Conference Proceedings, 53 (2019). [Online] https://digital-library.theiet.org/content/conferences/10.1049/cp.2019.1258
29. Lemus, M., et al.: Generation and distribution of quantum oblivious keys for secure multiparty computation. Appl. Sci. 10(12), 4080 (2020). [Online]. https://doi.org/10.3390/app10124080 https://www.mdpi.com/2076-3417/10/12/4080
30. Santos, M.B., Pinto, A.N., Mateus, P.: Quantum and classical oblivious transfer: a comparative analysis. IET Quan. Commun. 2(2), 42–53 (2021). [Online] https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/qtc2.12010
31. Santos, M.B., Mateus, P., Pinto, A.N.: Quantum oblivious transfer: a short review. Entropy 24(7), 945 (2022). [Online]. https://doi.org/10.3390/e24070945 https://www.mdpi.com/1099-4300/24/7/945
32. Santos, M.B., et al.: Private computation of phylogenetic trees based on quantum technologies. IEEE Access 10, 38065–38088 (2022). https://doi.org/10.1109/access.2022.3158416
33. Bar Ilan University Cryptography Research Group: LIBSCAPI – the Secure Computation API. [Online] https://github.com/cryptobiu/libscapi
34. Keller, M.: MP-SPDZ: A Versatile Framework for Multi-Party Computation, Ser. CCS '20, pp. 1575–1590. Association for Computing Machinery (2020). [Online]. https://doi.org/10.1145/3372297.3417872
35. Demmler, D., Schneider, T., Zohner, M.: Aby – a Framework for Efficient Mixed-Protocol Secure Two-Party Computation (2015)
36. Chen, Y., et al.: Rosetta: A Privacy-Preserving Framework Based on TensorFlow (2020). https://github.com/LatticeX-Foundation/Rosetta
37. Chou, T., Orlandi, C.: The simplest protocol for oblivious transfer. In: Progress in Cryptology – LATINCRYPT 2015, Ser. Lecture Notes in Computer Science, K. Lauter and F. Rodríguez-Henríquez, Eds., vol. 9230. Springer International Publishing, pp. 40–58 (2015)
38. Keller, M., Orsini, E., Scholl, P.: Actively secure ot extension with optimal overhead. In: Advances in Cryptology – CRYPTO 2015, Ser. Lecture Notes in Computer Science, vol. 9215, pp. 724–741. Springer (2015). date of Acceptance: 08/05/2015
39. Daemen, J., Rijmen, V.: Aes Proposal. Rijndael (1999)
40. Ottaviani, C., et al.: Terahertz quantum cryptography. IEEE J. Sel. Area. Commun. 38(3), 483–495 (2020). https://doi.org/10.1109/jsac.2020.2968973
41. Kundu, N.K., et al.: Mimo terahertz quantum key distribution. IEEE Commun. Lett. 25(10), 3345–3349 (2021). https://doi.org/10.1109/lcomm.2021.3102703
42. Kundu, N.K., et al.: Channel estimation and secret key rate analysis of mimo terahertz quantum key distribution. IEEE Trans. Commun. 70(5), 3350–3363 (2022). https://doi.org/10.1109/tcomm.2022.3161008
43. Liu, C., et al.: Multicarrier multiplexing continuous-variable quantum key distribution at terahertz bands under indoor environment and in inter-satellite links communication. IEEE Photon. J. 13(4), 1–13 (2021). https://doi.org/10.1109/jphot.2021.3098717

How to cite this article: Rahmani, Z., Barbosa, L.S., Pinto, A.N.: Quantum privacy-preserving service for secure lane change in vehicular networks. IET Quant. Comm. 4(3), 103–111 (2023). https://doi.org/10.1049/qtc2.12059