Collision Warning in Vehicular Networks Based on Quantum Secure Multiparty Computation

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

[1]Department of Electronics, Telecommunications and Informatics – University of Aveiro Aveiro – Portugal

[2]Instituto de Telecomunicações (IT) – Aveiro – Portugal

[3]International Iberian Nanotechnology Laboratory (INL) – Braga – Portugal

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

[5]Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência (INESC TEC) Porto – Portugal

{zeinab.rahmani, anp}@ua.pt, lsb@di.uminho.pt

Abstract. *Quantum Secure Multiparty Computation (QSMC) is a technology that takes the advantage of quantum features allowing multiple parties to communicate in a secure and efficient manner while preserving their privacy. Using QSMC technology, we implement a collision warning use case in which vehicles can freely broadcast information while preserving the privacy of their confidential data. We integrate two quantum technologies namely Quantum Key Distribution (QKD) and Quantum Oblivious Key Distribution (QOKD) with the Malicious Arithmetic Secure Computation with Oblivious Transfer (MASCOT) protocol to implement a secure and efficient QSMC platform. This quantum approach significantly improves efficiency and security when we compare it with the classical implementation as both used quantum technologies (QKD and QOKD) are robust against quantum computer attacks.*

1. Introduction

Secure Multiparty Computation (SMC) could enable Vehicle-to-everything (V2X) communications such that multiple parties can cooperate while no information about their private inputs is revealed to the other parties. However, classical SMC usually is based on public key infrastructures that tend to be inefficient and insecure in the presence of quantum computers. We propose a Quantum Secure Multiparty Computation (QSMC) framework for collision warning in vehicular networks that can operate efficiently and securely even when a malicious party has access to a powerful quantum computer.

The concept of SMC was first introduced by Andrew Yao in the 1980s [Yao 1982]. In [Keller et al. 2016], the OT-based MASCOT multiparty protocol that realizes secure computation of arithmetic circuits over finite fields with a dishonest majority was presented in a preprocessing model. Despite the progress made in this area, SMC has seldom been used in practice as the proposed protocols were too slow for practical applications [Lemus et al. 2020]. To overcome classical SMC problems, researchers proposed quantum-based protocols to increase efficiency and security. In 1984, Bennet and Brassad proposed a Quantum Key Distribution (QKD) protocol, called the

BB84 in which symmetric keys are distributed between two parties and the information is encoded using polarized photons. A significant property of the QKD is that an eavesdropper trying to measure a quantum state must introduce detectable perturbations [Bennett and Brassard 2014]. Later in [Lemus et al. 2020], the Quantum Oblivious Key Distribution (QOKD) protocol was introduced to implement Quantum Oblivious Transfer (QOT) and consequently QSMC. One of the most significant usages of QSMC is in vehicular networks applications [Lee and Atkison 2021]. Although vehicular network services have already brought huge convenience to people's lives, they face urgent security challenges. SMC is one of the important methods to solve the privacy protection problems in vehicular networks as it guarantees the privacy of users' inputs and outputs. In [Song et al. 2018], an anonymous authentication scheme based on SMC is proposed in which the solution theory of linear equations systems and the oblivious transfer theory are employed. In [Popa et al. 2009], a system that can be used for toll collection, speed ticket generation, and insurance premium computation is developed. We develop a secure and efficient QSMC platform robust against quantum computer attacks, to implement a collision warning use case in vehicular networks. To this end, we integrate the proposed quantum technologies (QOK, QOKD, and QOT) with the MASCOT multiparty protocol.

This paper is organized as follows: In section 2, we provide an overview of the MASCOT protocol as well as the proposed quantum technologies. Afterward, we develop a collision warning use case in a vehicular network by integrating the QKD and QOKD with the MASCOT multiparty protocol in Section 3. In section 4, we present our quantitative results. Finally, we dedicate section 5 to the conclusion.

2. Framework Overview

Figure 1 shows an overview of the proposed collision warning use case. We leverage the MASCOT [Keller et al. 2016] protocol alongside quantum technologies to realize quantum-based multiparty communication in our network. In the following section, we first discuss that the original MASCOT protocol is not secure if the malicious party has access to powerful quantum computational resources. Therefore, we introduce the quantum technologies (QOK, QOKD, and consequently QOT) to be integrated with the MASCOT multiparty protocol, and finally use it in the proposed vehicular collision scenario.

2.1. MASCOT Multiparty Protocol

The MASCOT protocol [Keller et al. 2016] is implemented through MP-SPDZ framework [Keller 2020] which is a versatile framework to benchmark various multiparty computation protocols. In this work, we take advantage of the MASCOT protocol to perform secure computation for a collision warning use case in a vehicular network. The MASCOT protocol evaluates the desired function f that is represented as an arithmetic circuit with a malicious adversary. To perform the circuit computation, MASCOT uses an OT protocol based on [Chou and Orlandi 2015]. The security of MASCOT heavily relies on the security of the used the OT protocol. However, most classical OT implementations are inefficient, which precludes the practical use of OT-based applications. Therefore, the use of a secure and efficient QOT protocol is essential to meet the requirements of QSMC applications. To integrate quantum technologies with MASCOT protocol, we substitute the OT protocol used in MASCOT with QOKD, and consequently the QOT protocols proposed in [Lemus et al. 2020]. In the following, we explain these quantum-based technologies.

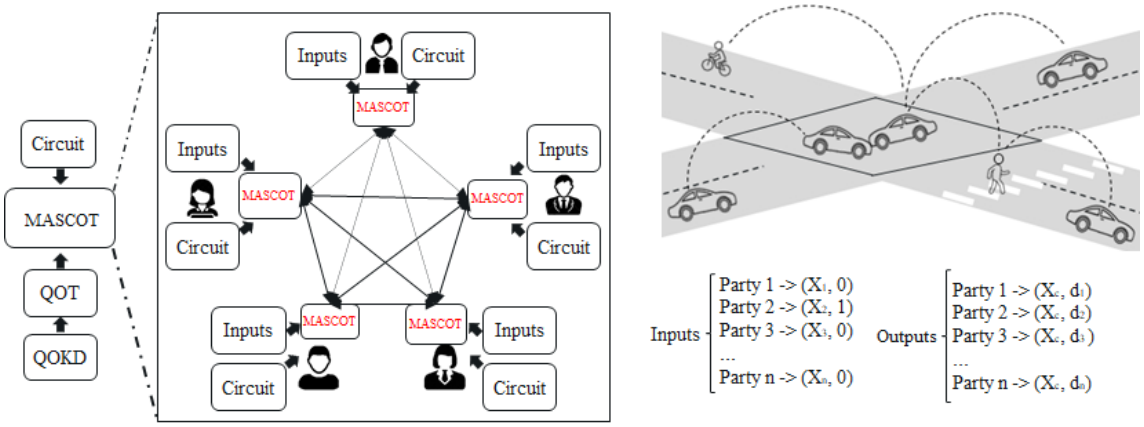

Figure 1. Overview of the proposed collision warning use case in a vehicular network equipped with a quantum technologies (QKD and QOKD). The right-hand side figure shows a collision event where each party sends its inputs namely the location (X_i), and the collision report (0 for no collision is seen, and 1 for collision is seen) to the MASCOT protocol. We obtain the circuit from a function ($|X_c - X_i|$) that computes the distance of each party to the collision location X_c. Finally, each party receives two outputs from the MASCOT protocol, indicating the collision location and distance from the collision location (i.e. (X_c, d_i)), while parties' input data remains private and secure. QOT and QOKD stand for the quantum technologies that insures the communications between the parties.

2.2. Quantum Key Distribution

To insure the communication between parties, we have to encrypt the data, which is commonly performed by the well-known cryptography tools (e.g. AES) that use symmetric keys, known by both parties. In [Bennett and Brassard 2014] proposed the quantum-based BB84 algorithm in which the symmetric keys are distributed between two parties. Quantum symmetric keys are identical sequences of bit streams distributed among parties in a way that both parties have access to the same keys. A significant property of this protocol is that a malicious entity can not measure a quantum state without introducing any perturbation to it. This property is known as no-cloning feature in quantum mechanics, which insures communication between parties.

2.3. Quantum Oblivious Key Distribution

In [Lemus et al. 2020] a QOKD protocol that generates and distributes oblivious keys is suggested. Oblivious Keys are a sequence of asymmetric keys, in which one of the parties (Alice) knows all the keys while the other (Bob) only knows half of the keys and Alice gets no information about which keys are known to Bob. Quantum oblivious keys allow the implementation of a fast and secure Quantum Oblivious Transfer (QOT) protocol in which a transmitter sends a small part of the information, but it remains oblivious to the receiver which piece has been transferred. We integrate QOT protocol with MASCOT multiparty protocol to compute the desired circuit gate by gate and perform secure communication among the parties.

3. Collision Warning Use Case

Road crashes represent a serious issue in vehicular networks and are one of the main causes of death. Using the developed QSMC platform, we implement a collision warning

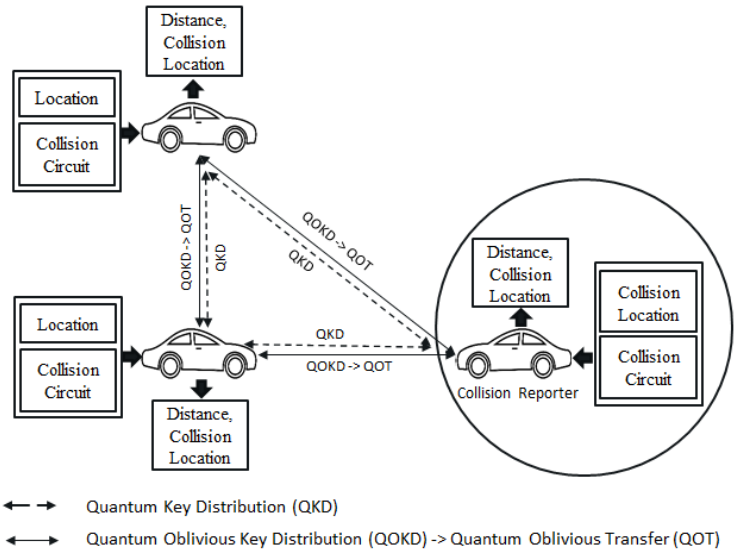

Figure 2. Network design of the QSMC framework for collision warning use case.

use case that enables multiple vehicles to cooperate freely while preserving the privacy of drivers' confidential data. When a collision is observed, a vehicle can freely broadcast information about this critical situation to other approaching vehicles. In the collision warning application each party has the two following inputs:

- Vehicle private location X_i
- A Boolean value b_i representing the observation of the collision (0 represent no accident observation and 1 represents the observation of the collision)

When a collision is observed a driver changes the Boolean value to 1 and subsequently the protocol is activated. The goal is to compute the distance of each vehicle from the collision location. To do so, We define a distance function $|X_c - X_i|$ in which X_c is the collision location and X_i is the location of the i-th vehicle. The designed function is then converted to an arithmetic circuit and is fed to the MASCOT protocol alongside the inputs of each vehicle. Afterward, each party receives the following outputs from the QSMC platform:

- Location of the accident X_c.
- The distance of each vehicle from the place of accident (d_i).

It is important to notice that the parties' private information (private location) is not revealed to the other parties. Figure 2 is a pictorial representation of the network design of the use case. Moreover, the implementation steps for collision warning use case is explained in protocol 1.

4. Results and Discussion

The minimum delay in processing the data in a network connection is known as low latency. A real-time system has a low latency close to zero milliseconds. However, reaching such systems in multiparty communication is not trivial as each block in the QSMC system imposes some delays to compute or transfer the data. As a rule of thumb, a latency lower than 100ms is known to be good while a latency lower than 50 ms is very good.

Protocol 1 Collision Warning

Parameters: Integers $l, r < l/2$, a holistic hash function family as $\mathbf{F}$ on $\{0,1\}^r$.

Inputs: Alice receives the string m_0 and $m_1 \in \{0,1\}^r$. Bob receives a bit b.

QOKD phase:

Call the QOKD service: QOKD uses oblivious key $(k,(k,x))$ with length l. QOKD sends k to Alice and sends k, x to Bob.

QOT phase:

1. Bob specifies two sequences $I_0 = \{i|x_i = 0\}$ and $I_1 = \{i|x_i = 1\}$. Bob sends the ordered pair $(I_b, I_{b\oplus 1})$ to Alice.
2. Alice samples two has functions $f_0, f_1 \in \mathbf{F}$ and then sends (s_0, s_1) to Bob. Here, $s_i = m_i \oplus f_i(k|I_{b\oplus i})$.
3. Bob calculates the outputs $m_b = s_b \oplus f_b(k|I_0)$.

MASCOT phase:

1. The generated QOTs are fed to the MASCOT protocol.
2. The collision circuit is generated for the desired function.

Collision warning phase:

The following inputs are used to calculate the circuit and final outputs are sent to each vehicle:

- Inputs: X_i the private location of vehicle; the bool b_i with value 0 for no collision observation, and 1 for collision occurrence
- Outputs: place of the collision X_c; distance from the place of collision d_i

We evaluate our system and analyze the execution time of the functions and executions the parties are performing in a simulation. The low latency is important in the proposed QSMC-based collision warning platform because the vehicles need to take immediate action when a collision is reported to avoid chain collisions and heavy traffic jams. Table 1 shows the performance of our platform when different numbers of parties are communicating at the same time. As it can be seen, when the number of parties increases from 3 to 10, the computational cost grows from 1 ± 0.04 ms to 5 ± 0.03 ms.

The level of security of the proposed platform is another aspect to consider. As mentioned before, no-cloning theorem indicates the impossibility of duplicating a quantum state. In fact, our QSMC platform generates the symmetric and asymmetric keys using the no-cloning feature which guarantee the security of our system.

5. Conclusion

In this paper, we propose a collision warning use case in vehicular networks that is based on quantum secure multiparty communication. We defined a computational function that measures the distance of the vehicles from the collision event. Then, we represent the function as an arithmetic circuit and feed it to a multiparty communication protocol (i.e. MASCOT). Further, to enhance the security of the MASCOT protocol, we use two quantum technologies (QKD and QOKD) instead of classical approaches. Our platform was proven to be secure and efficient with low latency for collision reports.

Table 1. Evaluation of latency, amount of sent data in megabytes, and number of rounds of the QSMC platform when the number of parties increases.

#Parties	Data sent (MB)	#Rounds	Computation time (ms)
3	0.05	32	1 ± 0.04
5	0.1	64	2 ± 0.02
10	0.2	144	5 ± 0.03

Acknowledgment

This work was supported in part by Fundação para a Ciência e a Tecnologia (FCT) 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, QUESTS project Ref. UIDB/50008/2020

References

Bennett, C. H. and Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

Chou, T. and Orlandi, C. (2015). The simplest protocol for oblivious transfer. In Lauter, K. and Rodríguez-Henríquez, F., editors, *Progress in Cryptology – LATINCRYPT 2015*, pages 40–58, Cham. Springer International Publishing.

Keller, M. (2020). Mp-spdz: A versatile framework for multi-party computation. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, page 1575–1590, New York, NY, USA. Association for Computing Machinery.

Keller, M., Orsini, E., and Scholl, P. (2016). Mascot: Faster malicious arithmetic secure computation with oblivious transfer. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, page 830–842, New York, NY, USA. Association for Computing Machinery.

Lee, M. and Atkison, T. (2021). Vanet applications: Past, present, and future. *Vehicular Communications*, 28:100310.

Lemus, M., Ramos, M. F., Yadav, P., Silva, N. A., Muga, N. J., Souto, A., Paunković, N., Mateus, P., and Pinto, A. N. (2020). Generation and distribution of quantum oblivious keys for secure multiparty computation. *Applied Sciences*, 10(12):4080.

Popa, R. A., Balakrishnan, H., and Blumberg, A. J. (2009). Vpriv: Protecting privacy in location-based vehicular services. In *Proceedings of the 18th Conference on USENIX Security Symposium*, SSYM'09, page 335–350, USA. USENIX Association.

Song, C., Zhang, M., and Peng, W.-P. (2018). Research on secure and privacy-preserving scheme based on secure multi-party computation for vanet. *J. Inf. Hiding Multim. Signal Process.*, 9(1):99–107.

Yao, A. C. (1982). Protocols for secure computations. In *23rd Annual Symposium on Foundations of Computer Science (SFCS 1982)*, pages 160–164.