A Quantum Safe Authentication Protocol for Remote Keyless Entry Systems in Cars

Rohini Poolat Parameswarath
Department of ECE
National University of Singapore
Singapore
rohini.p@nus.edu.sg

Nalam Venkata Abhishek
Infocomm Technology Cluster
Singapore Institute of Technology
Singapore
venkata.abhishek@singaporetech.edu.sg

Biplab Sikdar
Department of ECE
National University of Singapore
Singapore
bsikdar@nus.edu.sg

***Abstract*—The keyless entry systems in cars enable users to lock or unlock cars remotely. One of the popular types of keyless entry systems used in cars is the Remote Keyless Entry (RKE) system. With the advent of quantum computers, quantum computing-enabled cyber-attacks are an imminent threat. The security offered by current cryptographic techniques is inadequate to protect systems such as RKE from such future quantum attacks. In this paper, we propose a quantum-safe authentication protocol leveraging Quantum Key Distribution (QKD) that authenticates a legitimate key fob before unlocking the car. We present a formal security proof and an informal analysis to show that the protocol is secure against several attacks. To the best of our knowledge, this is the first protocol that protects RKE systems from future quantum computing-enabled cyber-attacks, in addition to the existing replay and RollJam attacks.**

***Index Terms*—Authentication protocol, quantum gates, Quantum Key Distribution (QKD), remote keyless entry systems, security.**

I. Introduction

Keyless entry systems are integral components of modern cars. The Remote Keyless Entry (RKE) systems enable the user to unlock or lock the car door with the click of a button on the key fob. This paper focuses on the security of RKE systems. In RKE systems, the key fob transmits Radio Frequency (RF) signals when the key fob button is pressed by the user. The first generation of RKE systems used static codes where the same code is sent to the receiver whenever the user presses a button on the key fob. Later on, RKE systems built on rolling codes were made available in cars where the code increments with the key fob button press. Being an easy target for attackers, several attacks have been reported against keyless entry systems [1]–[4]. Keyless entry systems that use the same code for all unlock signals are susceptible to replay attacks as the signals can be captured and replayed later on by an adversary. Even the rolling code-based RKE systems are susceptible to certain types of replay attacks known as RollJam attacks [5].

Several solutions based on classical cryptography have been proposed in the literature to protect keyless entry systems from various attacks [6]–[9]. However, most algorithms are based on traditional symmetric and asymmetric cryptographic techniques. The security of systems that employ asymmetric cryptographic techniques is contributed by the difficulty of solving the underlying mathematical problems, like the discrete logarithm problem or the integer factorization problem. However, with the introduction of algorithms such as Shor's algorithm [10], a quantum cryptanalysis algorithm that can solve the integer factorization problem and the discrete logarithm problem efficiently, the security of systems based on asymmetric cryptographic techniques is at stake. Grover's search [11] is an exhaustive key search algorithm that can be employed to make the search for the key used in symmetric encryption techniques faster [12]. Grover's search can be used for a brute force attack on an N-bit symmetric cryptographic key scheme to find the key in $2^{\frac{N}{2}}$ iterations. By employing Grover's search, the security level of the popular symmetric cryptographic key scheme, Advanced Encryption Standard (AES), reduces by half [13]. Note that symmetric cryptographic schemes with larger key sizes can mitigate the impact of Grover's search. However, asymmetric cryptographic algorithms, that are not quantum-safe, are commonly employed to establish the key for symmetric encryption in systems that use symmetric encryption [14]. Side-channel attacks also have been attempted on symmetric encryption schemes [15]–[18].

Therefore, algorithms resistant to quantum computer-enabled attacks are required for securing RKE systems. Quantum Key Distribution (QKD) is a technique that can help to make systems quantum-resistant. This approach requires the presence of a wireless optical channel which can be easily achieved in the current scenario. The fact that the parties participating in the QKD process may quickly identify an eavesdropper is the major advantage that motivates the use of QKD in this scenario. This advantage can be attributed to the properties of the quantum systems [19].

A. Related Work

We present the related literature in this section.

RKE: Various vulnerabilities that exist in keyless entry systems and the attacks against them have been demonstrated in literature [2]–[4]. The authors of [20] performed attacks on RKE systems in different car models. To protect RKE systems from replay attacks, authentication protocols based on timestamps [6] and a symmetric encryption algorithm [8] have been proposed in the literature. An authentication protocol

979-8-3503-2928-5/23/$31.00 ©2023 IEEE

based on timestamps and XOR encoding was proposed in [7]. A scheme built on an asymmetric cryptographic technique to authenticate a legitimate key fob was proposed in [9]. A mutual authentication scheme for RKE systems was proposed in [21]. However, the protocol in [21] requires a key fob to be equipped with additional hardware (a Physical Unclonable Function (PUF)). Also, the protocols proposed in [6]–[9] and [21] do not protect RKE systems from quantum-enabled attacks.

QKD in hardware-limited systems: The use of QKD for hardware-limited systems has been explored in the literature. In [22], the authors proposed a lightweight transmission mechanism for secure data exchange in IoT networks. The proposed algorithm defends the network from eavesdroppers. The authors also showed that by using QKD-based algorithms, the latency and power efficiency can be improved. The authors of [23] have also demonstrated that the battery lifetime of IoT devices can be improved by deploying QKD-based algorithms for secure data exchanges. The authors of [24] proposed a novel technique for simulating QKD between IoT devices and a server. They claim that the proposed technique can be applied with fiber or with free space optics. In [25], the authors proposed a QKD system using the decoy-state method. According to the authors, the proposed system is immune to various attacks with reasonable performance.

B. Motivation and Our Contributions

It is essential to secure RKE systems from various attacks. Several solutions built on symmetric or asymmetric cryptographic techniques have been proposed in the literature to secure RKE systems from various attacks. However, none of these solutions address quantum computing-enabled attacks and only focus on attacks by classical computers. The protocols built on asymmetric cryptographic techniques can be compromised by using Shor's algorithm [10] and quantum computers. The protocols based on symmetric cryptographic techniques are vulnerable to Grover's search [11], Shor's algorithm if they employ asymmetric cryptographic techniques to derive the symmetric key, and side-channel attacks [15]–[18].

The contributions of this paper can be summarised as follows:

- A quantum-safe authentication protocol for RKE systems based on QKD: We propose an authentication protocol based on a key derived through QKD. Quantum mechanical principles serve as the foundation for the proposed protocol's security.
- Efficient design of the protocol: In the proposed protocol, the participants derive the bases for quantum measurement from the established quantum key while transmitting the message. This approach eliminates the need for public announcement of bases. It is more efficient than using random bases and their announcement as the sender and receiver do not have to discard photons due to basis mismatch. All photons transmitted are useful in this approach.
- Protection against conventional and quantum computing-enabled attacks: The proposed protocol offers protection from conventional replay, RollJam, and impersonation attacks as well as future quantum computing-enabled attacks.
- Security analysis: We provide a formal security proof and an informal security analysis to show the proposed protocol's robustness.

II. System Model and Adversary Model

A. System Model

The system consists of a key fob and a receiver at the car. The user activates the lock or unlock operations by pressing the corresponding key fob buttons. Then, RF signals indicating the operation to be carried out are transmitted to the car.

B. Adversary Model

We assume that the adversary has the capability to perform attacks with conventional and quantum computers. By using conventional computers, the attacker may eavesdrop on, capture, jam, or replay the signals between the key fob and the car. The adversary may also eavesdrop on and capture the messages exchanged over a quantum channel. The adversary may have the capability to perform physical attacks on the key fob to get the stored secrets, if any. Also, the adversary can execute effective computational attacks using quantum computers. With these capabilities, the adversary can carry out the following attacks:

- **Replay Attack:** RKE systems that always use the same code are highly vulnerable to replay attacks as the adversary may capture the signals and replay them later to get access.
- **RollJam Attack:** In the rolling code-based RKE systems, the code increments with every unlock operation. Though they are immune to replay attacks, they can be the targets of RollJam attacks. In the RollJam attack, when the key fob sends an unlock signal, the attacker captures and jams it. Then, the user attempts to unlock the car again. The second signal is also captured and jammed by the attacker. Together with this step, the attacker sends the first stored unlock signal to the car so that the car gets unlocked. The user does not notice that he/she has been the victim of an attack since the car gets unlocked on the second attempt. Now the attacker has captured a valid signal to unlock the car that can be used later.
- **Quantum-enabled attacks on RKE systems:** RKE systems that employ symmetric key encryption are vulnerable to Grover's search and side-channel attacks. Also, it has been shown that the security of the systems based on asymmetric cryptographic techniques can be broken using quantum algorithms such as Shor's algorithm [10].

We can model the capabilities of an attacker A to eavesdrop, capture, jam, or send a message m over the quantum or classical channels, or perform physical attacks on the key fob using the following queries:

- ***Monitor()*** models the query when A attempts to monitor the exchanged messages between the key fob and the car over the quantum or the classical channel.
- ***Capture(m)*** models the query when A attempts to capture message m sent between the key fob and the car over the quantum or the classical channel.
- ***Send(m)*** models the query when A attempts to send message m to the receiver. The message m can be sent over the quantum or the classical channel.
- ***Drop(m)*** models the query when A attempts to jam m from the key fob to the receiver to prevent m from reaching the car receiver.
- ***Retrieve()*** models the query when A performs physical attacks on key fobs to retrieve any secrets stored in the key fob memory.

An attacker may call these queries a polynomial number of times.

III. Authentication Protocol

We employ QKD to arrive at a key between the key fob and the car receiver. Then, based on the derived key, messages are sent in a secure manner from the key fob to the car receiver.

A. Preliminaries

In this subsection, we briefly present the basics of quantum key distribution and quantum gates.

Quantum Key Distribution: Quantum key distribution leverages the properties of quantum mechanics to derive a symmetric key in such a manner that any eavesdropping by an adversary will be known to the sender and the receiver [26]. A QKD link consists of two channels: a uni-directional quantum channel that transmits photons and a bi-directional classical channel. Any medium which allows light to go through acts as a 'quantum channel'. The quantum channel can be line-of-sight free space or optical fiber. QKD provides unconditional security with an authenticated classical channel. Without authentication in the classical channel, there is a risk of man-in-the-middle attack. The usual method to authenticate a classical channel is pre-sharing symmetric keys between the two involved entities [27].

Bennett and Brassard defined the first QKD protocol in 1984 called the BB84 protocol [26]. In this protocol, the sender generates a stream of classical bits. These bits are encoded into a sequence of polarized photons. The resultant sequence is sent over the quantum channel to the receiver as qubits. When the receiver receives this sequence, it measures the received photons' polarization in a random sequence of basis. Then, the receiver informs the sender about the basis that was used for each photon. This step is carried out over the classical channel. The sender informs the receiver which bases used for measurement were correct. This step is also carried out over the classical channel. Then, both parties keep only the data from the correct measurements and test the correlation. If there is no eavesdropping on the channel by an adversary, the correlation will be high and a symmetric key is established between the two parties. If the correlation is less than a threshold value, the process will be repeated to derive a key.

Quantum Gates: A quantum gate is a quantum circuit that operates on qubits and enables quantum state transformations [28]. Since quantum state transformations are reversible, quantum gates also are reversible [28]. A quantum gate can be represented by a unitary matrix, e.g., a quantum gate that operates on l qubits can be represented by a $2^l \times 2^l$ unitary matrix. We use the identity gate I and the X gate in the design of the protocol. X gate is the quantum counterpart of the NOT gate used in classical computing. The I and X gates on a single qubit are given below:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

B. Proposed Protocol

Assumptions: We assume that the car receiver and the key fob are installed with QKD devices. We also assume that a pre-shared symmetric key exists between the key fob and the car receiver prior to the key fob's first use. For example, the car manufacturer can pre-load a symmetric key in the key fob and the car receiver. This is to authenticate the classical channel in the QKD link for the first instance of the use of the key fob. After that, with every authentication event, the classical channel will be authenticated with a different key. There exists a counter value at the key fob. For the first instance of the use of the key fob, this value is set to zero.

Mutual Authentication Between the Key fob and the Receiver:

The authentication phase is illustrated in Figure 1. Whenever the key fob button is pressed, the following actions are performed:

Step 1: As mentioned in the assumptions, a pre-shared symmetric key S_k exists between the key fob and the car receiver before the first instance of the use of the key fob. S_k is used to authenticate the classical channel in the QKD link. Then, as described in Section III-A, a key P_k of length n is established between the key fob and the car receiver through the QKD process. Let $S = P_k$.

Step 2: The counter value is incremented by 1. Then, the key fob appends the command to be performed (e.g., 'unlock') to its identifier (ID) and the counter value to generate a message Y of n bits, i.e., $Y = \{ID \parallel counter \parallel cmd\}$. Let y_i represent the i^{th} bit of Y.

Step 3: The key fob generates a vector Y^q of n qubits from Y. The basis to convert a classical bit y_i to a qubit y_i^q is selected based on the following rule:

$$Basis = \begin{cases} Rectilinear, & \text{If } S_i = 0, \\ Diagonal, & \text{Otherwise.} \end{cases} \tag{1}$$

Hence, if $y_i = 0$, based on whether $S_i = 0$ or $S_i = 1$, $y_i^q = |0\rangle$ or $y_i^q = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Similarly, if $y_i = 1$, based on whether $S_i = 0$ or $S_i = 1$, $y_i^q = |1\rangle$ or $y_i^q = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. This can be written as:

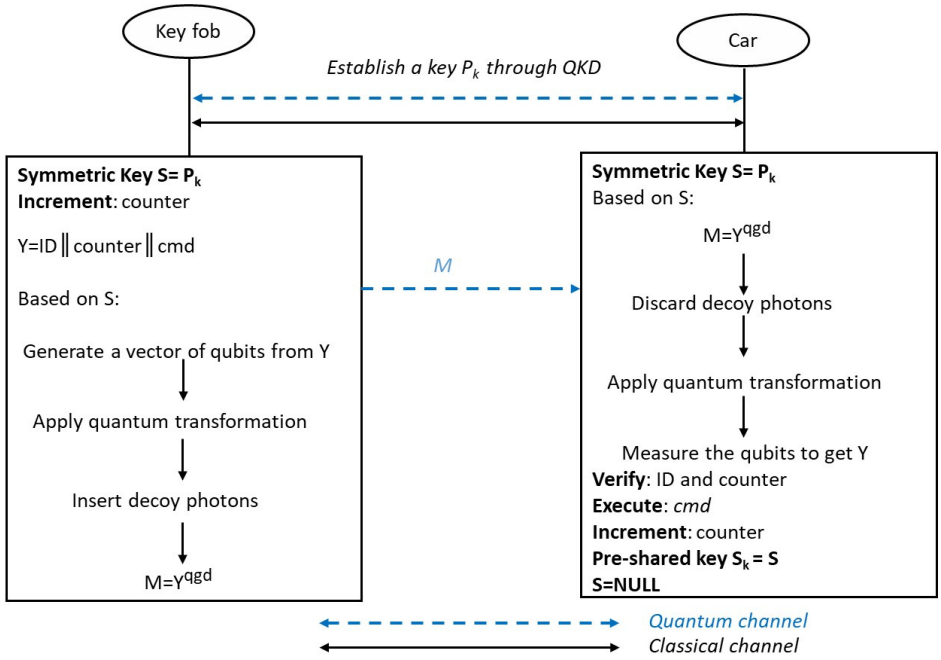

Fig. 1: The key fob authentication phase.

$$y_i^q = \begin{cases} |0\rangle, & \text{If } y_i = 0 \text{ and } S_i = 0, \\ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), & \text{If } y_i = 0 \text{ and } S_i = 1, \\ |1\rangle, & \text{If } y_i = 1 \text{ and } S_i = 0, \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), & \text{If } y_i = 1 \text{ and } S_i = 1. \end{cases} \quad (2)$$

Step 4: The I and X quantum gates are applied to the qubits of Y^q to produce quantum state transformations. Let the resultant message be Y^{qg}. The gate to be applied to a qubit y_i^q is determined using the following rule:

$$Gate = \begin{cases} X, & \text{If } S_i = 0, \\ I, & \text{Otherwise.} \end{cases} \quad (3)$$

After applying the quantum gates, the i^{th} bit of Y^{qg} can be written as:

$$y_i^{qg} = \begin{cases} |1\rangle, & \text{If } y_i = 0 \text{ and } S_i = 0, \\ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), & \text{If } y_i = 0 \text{ and } S_i = 1, \\ |0\rangle, & \text{If } y_i = 1 \text{ and } S_i = 0, \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), & \text{If } y_i = 1 \text{ and } S_i = 1. \end{cases} \quad (4)$$

Step 5: Next, the sender generates n decoy photons $\{q_0, q_1, \cdots, q_{n-1}\}$ from the states $|0\rangle, |1\rangle, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ and inserts them into Y^{qg} to construct Y^{qgd}. The positions where the decoy photons are inserted is based on the following rule:

$$\text{Position} = \begin{cases} \text{Every even position}, & \text{If } S_0 = 0, \\ \text{Every odd position}, & \text{Otherwise.} \end{cases} \quad (5)$$

The resultant message Y^{qgd} can be written as:

$$Y^{qgd} = \begin{cases} (y_0^{qg}, q_0, y_1^{qg}, q_1, \cdots, q_{n-1}), & \text{If } S_0 = 0, \\ (q_0, y_0^{qg}, q_1, y_1^{qg}, \cdots, y_{n-1}^{qg}), & \text{Otherwise.} \end{cases} \quad (6)$$

Step 6: The key fob sends $M = Y^{qgd}$ to the receiver over a quantum channel. Upon receiving Y^{qgd}, the receiver first finds the positions of decoy photons based on Equation (5). Then, the receiver discards the decoy photons from Y^{qgd} to generate Y^{qg}. Subsequently, the receiver applies the I or X quantum gates to the qubits of Y^{qg} based on Equation (3) to generate Y^q. Note that the quantum gates are reversible. After that, the receiver measures each qubit y_i^q of Y^q using a rectilinear or diagonal basis based on Equation (1) and generates Y.

The receiver extracts the ID of the key fob as well as the counter value from Y and verifies them. If an adversary attempts to eavesdrop on the message sent by the key fob, errors will be introduced and the verification will fail at the receiver. If the ID and counter value verifications by the receiver are successful, the operation corresponding to the command mentioned in Step 2 is executed at the car and the counter value is incremented. After the successful execution of the operation, the key S of the current session will be used to authenticate the classical channel in the next authentication event while deriving the next symmetric key. It will not be used to decode the next unlock message from the key fob, i.e., $S_k = P_k$ and $S = NULL$. This is to prevent replay attacks.

In Step 3 of the proposed protocol, the key fob and the receiver derive the bases for quantum measurement from the quantum key established in Step 1. These bases are used while preparing the message to transmit. This approach eliminates

the requirement for public announcement of bases. It is more efficient than using random bases and their announcement as the sender and receiver do not have to discard photons due to basis mismatch.

IV. Security Analysis

We first present the security analysis of the proposed protocol to show that it is secure against classical and quantum attacks. After that, we compare the proposed protocol with other existing protocols based on the achieved security properties.

A. Formal Security Proof for the Proposed Authentication Protocol

Lemma 1: An attacker cannot clone quantum states.

Proof. According to the no-cloning theorem [29], the adversary cannot make copies of a quantum state. Hence, we can write that the advantage of the adversary in trying to clone the quantum state is 0:

$$Adv_{A,Cloning} = 0. \tag{7}$$

■

Lemma 2. An attacker A cannot obtain any secrets from the key fob.

Proof. No secrets are stored in the key fob memory. The symmetric key is established during each authentication session. Hence, even with the *Retrieve()* query and physical attack, A cannot obtain the key from the key fob. ■

Theorem 1: The derived symmetric key is secure.

Proof. The security of the derived symmetric key can be assessed by modelling a security game. If an attacker A can get the symmetric key for a session correctly, A wins the game. The game where A attempts to get the symmetric key is given below:

1) The key fob sends a sequence of photons to the car receiver over the quantum link.
2) The key fob shares some information with the car receiver over the classical channel about the photons sent and derives a symmetric key P_k of length n.
3) A derives the symmetric key as P_k^*.
4) A wins the game if it can derive the accurate symmetric key, i.e., if $P_k = P_k^*$.

The adversary's advantage in this security game is the probability of deriving the symmetric key correctly. It can be written as $Adv_{key} = Pr[P_k = P_k^*]$. As mentioned in Lemma 1, the adversary cannot make copies of a quantum state to measure it. From Lemma 2, even with the *Retrieve()* query, A cannot retrieve the key from the key fob. Due to the principles of quantum mechanics, the adversary cannot capture and measure the photons to derive the symmetric key without being noticed by the sender and the receiver. Hence, the only option for A to obtain the symmetric key P_k is to make a random guess. Since there are n bits in P_k, the probability of guessing P_k correctly is $\frac{1}{2^n}$ which is negligible. As a result, $Adv_{key} = Pr[P_k = P_k^*] = \frac{1}{2^n}$. ■

Theorem 2: The vehicle cannot be unlocked by replaying the previous messages.

Proof. An attacker A may try to replay a previous message from the key fob. We can model this replay attempt by the following security game:

1) A key P_k is derived through the QKD technique.
2) The key fob generates a message M of qubits based on the symmetric key $S = P_k$ and sends it over the quantum channel to unlock the car.
3) A captures the message M by executing the $Capture(M)$ query over the quantum channel. A stores M.
4) The car unlocks. The symmetric key for the session S is set to $NULL$ at the car receiver.
5) A replays M and sends it to the car receiver by executing the $Send(M)$ query over the quantum channel. A wins the game if the car unlocks.

After the successful unlock operation, the key S is set to $NULL$ at the car receiver in Step 4. It is not valid for the next sessions. As a result, when A replays M, it cannot be decoded by the car receiver. Hence, the probability of executing the operation at the car as a result of replaying M can be written as $Adv_{replay} = 0$. ■

Theorem 3: The vehicle cannot be unlocked through RollJam attacks.

Proof. An attacker A's attempt to execute the RollJam attack can be modelled by the following security game:

1) A key P_k^1 is established between the sender and the receiver through the QKD technique.
2) The key fob generates a message M_1 based on the symmetric key $S = P_k^1$ and sends it to the receiver over the quantum channel to unlock the car.
3) A captures the message M_1 by calling the *Capture(M_1)* query over the quantum channel. A stores M_1.
4) A calls the *Drop(M_1)* query over the quantum channel to jam M_1.
5) Since the first unlock attempt failed, the user presses the unlock button once more.
6) A new key P_k^2 is established. The key fob generates a message M_2 based on the symmetric key $S = P_k^2$ and sends it over the quantum channel to unlock the car.
7) A captures the message M_2 by calling the *Capture(M_2)* query. A stores M_2.
8) A jams the message by running the *Drop(M_2)* query. At the same time, A sends the message M_1 to the car by calling the *Send(M_1)* query.
9) If A can unlock the car, A can replay the message M_2 by using the *Send(M_2)* query later to unlock the car. If A is able to unlock the car, A wins the game.

In Step 6, a new key P_k^2 is established and S is set to P_k^2, i.e., $S = P_k^2$. As a result, when A replays M_1 (generated based on the symmetric key $S = P_k^1$) in Step 8, it cannot be decoded by the car receiver. Hence, the car does not unlock again and the user will notice the presence of the attacker. Thus, with the proposed protocol in place, the adversary cannot execute the

TABLE I: Comparison of the proposed protocol with other protocols: security properties

Features	Greene et al. [6]	Greene et al. [7]	Glocker et al. [8]	Parameswarath et al. [9]	Proposed Protocol
Resilience Against Quantum Attacks	No	No	No	No	Yes
Key fob Authentication	Yes	Yes	Yes	Yes	Yes
Protection From Replay Attacks	Yes	Yes	Yes	Yes	Yes
Protection From RollJam Attacks	Yes	Yes	No	Yes	Yes
Is Clock Synchronization Necessary?	Yes	Yes	No	Yes	No
Security Proof	No	No	No	No	Yes

RollJam attack. A's advantage in this game can be modelled as $Adv_{RollJam} = 0$. ■

Theorem 4: The proposed protocol provides authentication of a legitimate key fob.

Proof. An attacker A's attempt to get authenticated as a key fob can be modelled as a security game. The steps are given below:

1) A calls *Send(M)* to send a message M to the car as a key fob.
2) If the car unlocks after successful authentication, the attacker wins the security game.

A must send a valid message M to the car receiver to get authenticated. If A wants to generate a valid message, A needs to know the symmetric key. Due to the principles of quantum mechanics, A's attempt to capture and measure the photons in an attempt to derive the symmetric key will be detected by the sender and the receiver. From Theorem 1, if there are n bits in the symmetric key, the probability of predicting the symmetric key is $\frac{1}{2^n}$ which is negligible. Hence, the probability of A generating a valid message M is negligible and can be ignored. From Theorems 2 and 3, the attacker cannot retransmit previous messages through the replay or the RollJam attacks. As a result, A's advantage in successful authentication, Adv_{Auth}, is negligible. Hence, authentication will be successful only if the message originated from a legitimate key fob. Thus, the proposed authentication protocol provides authentication of a legitimate key fob. ■

B. Informal Security Analysis

Protection against attacks by Shor's algorithm and quantum computer: In the proposed protocol, the key is derived through QKD making use of the principles of quantum mechanics. Unlike the conventional asymmetric cryptographic techniques used to derive a symmetric key, QKD is not based on the assumption of the complexity of the underlying mathematical concepts and the adversary's inability to solve them efficiently. Hence, the proposed protocol is immune to attacks by Shor's algorithm and quantum computers.

Protection Against Impersonation Attacks: To impersonate a key fob, the adversary needs to send a valid message based on a shared key. The key is derived between the key fob and the car receiver by sending photons. Eavesdropping on the photons shared between the key fob and car receiver to derive the key will expose the attacker, as per the principles of quantum mechanics. Hence, the attacker cannot eavesdrop on the key. Thus, the symmetric key is not available to the attacker. As a result, the protocol provides protection against impersonation attacks.

C. Comparison of Security Properties

Next, we compare the proposed protocol with other protocols based on the security properties it offers. Table I summarises the comparison of the security features. The main distinguishing feature of the proposed protocol is the protection it provides against quantum attacks. Though [6]–[9] address some of the key security challenges faced by RKE systems, they have not addressed the threat from quantum attacks. The key fob and the receiver must have synchronized clocks for the protocols proposed in [6], [7], and [9] to work as expected. The proposed protocol does not have the requirement for clock synchronization. To summarise, the proposed protocol provides protection against attacks by classical computers as well as quantum-enabled attacks.

V. Simulation Experiments

We have simulated the QKD process by using the quantum simulator QuVis [30]. We measured the parameters in two scenarios: no eavesdropping and eavesdropping. Random bases were selected to send polarized photons in both scenarios. The eavesdropper also used random bases. In each scenario, 500 photons were sent from the source to the destination in batches of 100. The total number of photons sent (N_t), the number of final key bits (N_k), the number of errors (N_e), and the error probability ($P_n = N_e/N_k$) were recorded during the simulation. The results for no eavesdropping and eavesdropping scenarios are summarised in Table II.

TABLE II: Error probabilities

No eavesdropping

N_t	N_k	N_e	P_n
100	45	0	0
200	103	0	0
300	158	0	0
400	206	0	0
500	252	0	0

With eavesdropping

N_t	N_k	N_e	P_n
100	49	9	0.184
200	104	25	0.24
300	160	44	0.275
400	224	66	0.295
500	277	77	0.278

The simulation results indicate that eavesdropping increases the error probability at the receiver that can be detected by the sender and receiver.

VI. Conclusion

Given the rise in the development of quantum computers, the need to replace traditional cryptography systems with quantum-safe systems is essential. One such scenario that would benefit from adopting QKD is the RKE system. In

this paper, we proposed a QKD-based protocol for secure key exchange in RKE systems. We also presented a security analysis of the proposed protocol. Through the security proofs, we have demonstrated that the proposed protocol is secure against threats by an adversary with classical and quantum computing capabilities.

VII. Acknowledgement

This research is supported by the National Research Foundation, Singapore and A*STAR under its Quantum Engineering Programme (National Quantum-Safe Network, NRF2021-QEP2-04-P01).

References

[1] K. Joo, W. Choi, and D. H. Lee, "Hold the door! fingerprinting your car key to prevent keyless entry car theft," in *27th Annual Network and Distributed System Security Symposium, NDSS 2020, San Diego, California, USA, February 23-26, 2020*. The Internet Society, 2020.

[2] A. I. Alrabady and S. M. Mahmud, "Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs," *IEEE transactions on vehicular technology*, vol. 54, no. 1, pp. 41–50, 2005.

[3] F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlides, "Lock it and still lose it - on the (in) security of automotive remote keyless entry systems," in *Proceedings of the 25th USENIX Security Symposium*, 2016, pp. 929 – 944.

[4] R. Benadjila, M. Renard, J. Lopes-Esteves, and C. Kasmi, "One car, two frames: attacks on hitag-2 remote keyless entry systems revisited," in *11th {USENIX} Workshop on Offensive Technologies ({WOOT} 17)*, 2017.

[5] Defcon 23 rolljam attack. [Online]. Available: https://samy.pl/defcon2015/

[6] K. Greene, D. Rodgers, H. Dykhuizen, K. McNeil, Q. Niyaz, and K. A. Shamaileh, "Timestamp-based defense mechanism against replay attack in remote keyless entry systems," in *2020 IEEE International Conference on Consumer Electronics (ICCE)*, 2020, pp. 1–4.

[7] K. Greene, D. Rodgers, H. Dykhuizen, Q. Niyaz, K. Al Shamaileh, and V. Devabhaktuni, "A defense mechanism against replay attack in remote keyless entry systems using timestamping and xor logic," *IEEE Consumer Electronics Magazine*, vol. 10, no. 1, pp. 101–108, 2020.

[8] T. Glocker, T. Mantere, and M. Elmusrati, "A protocol for a secure remote keyless entry system applicable in vehicles using symmetric-key cryptography," in *2017 8th International Conference on Information and Communication Systems (ICICS)*. IEEE, 2017, pp. 310–315.

[9] R. P. Parameswarath and B. Sikdar, "An authentication mechanism for remote keyless entry systems in cars to prevent replay and rolljam attacks," in *2022 IEEE Intelligent Vehicles Symposium (IV)*, 2022, pp. 1725–1730.

[10] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134.

[11] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996, pp. 212–219.

[12] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, "Applying grover's algorithm to aes: quantum resource estimates," in *Post-Quantum Cryptography*. Springer, 2016, pp. 29–43.

[13] R. Asif, "Post-quantum cryptosystems for internet-of-things: a survey on lattice-based algorithms," *IoT*, vol. 2, no. 1, pp. 71–91, 2021.

[14] X. Bogomolec, J. G. Underhill, and S. A. Kovac, "Towards post-quantum secure symmetric cryptography: A mathematical perspective," *Cryptology ePrint Archive*, 2019.

[15] D. J. Bernstein, "Cache-timing attacks on aes," 2005. [Online]. Available: https://mimoza.marmara.edu.tr/~msakalli/cse466_09/cache%20timing-20050414.pdf

[16] A. Bogdanov, "Improved side-channel collision attacks on aes," in *International Workshop on Selected Areas in Cryptography*. Springer, 2007, pp. 84–95.

[17] R. Wang, H. Wang, and E. Dubrova, "Far field em side-channel attack on aes using deep learning," in *Proceedings of the 4th ACM Workshop on Attacks and Solutions in Hardware Security*, 2020, pp. 35–44.

[18] Y. Niu, J. Zhang, A. Wang, and C. Chen, "An efficient collision power attack on aes encryption in edge computing," *IEEE Access*, vol. 7, pp. 18 734–18 748, 2019.

[19] H. Zhang, Z. Ji, H. Wang, and W. Wu, "Survey on quantum information security," *China Communications*, vol. 16, no. 10, pp. 1–36, 2019.

[20] O. A. Ibrahim, A. M. Hussain, G. Oligeri, and R. Di Pietro, "Key is in the air: Hacking remote keyless entry systems," in *Security and Safety Interplay of Intelligent Software Systems*. Springer, 2018, pp. 125–132.

[21] R. P. Parameswarath and B. Sikdar, "A puf-based lightweight and secure mutual authentication mechanism for remote keyless entry systems," in *GLOBECOM 2022-2022 IEEE Global Communications Conference*. IEEE, 2022, pp. 1776–1781.

[22] G. Liu, J. Han, Y. Zhou, T. Liu, J. Chen *et al.*, "Qslt: A quantum-based lightweight transmission mechanism against eavesdropping for iot networks," *Wireless Communications and Mobile Computing*, vol. 2022, 2022.

[23] A. Mavromatis, F. Ntavou, E. H. Salas, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Experimental demonstration of quantum key distribution (qkd) for energy-efficient software-defined internet of things," in *2018 European Conference on Optical Communication (ECOC)*, 2018, pp. 1–3.

[24] H. A. Al-Mohammed and E. Yaacoub, "On the use of quantum communications for securing iot devices in the 6g era," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2021, pp. 1–6.

[25] H. Ma and B. Chen, "An authentication protocol based on quantum key distribution using decoy-state method for heterogeneous iot," *Wireless Personal Communications*, vol. 91, no. 3, pp. 1335–1344, 2016.

[26] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. A. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, pp. 3–28, 1992.

[27] L.-J. Wang, K.-Y. Zhang, J.-Y. Wang, J. Cheng, Y.-H. Yang, S.-B. Tang, D. Yan, Y.-L. Tang, Z. Liu, Y. Yu *et al.*, "Experimental authentication of quantum key distribution with post-quantum cryptography," *npj quantum information*, vol. 7, no. 1, pp. 1–7, 2021.

[28] E. Rieffel and W. Polak, "An introduction to quantum computing for non-physicists," *ACM Computing Surveys (CSUR)*, vol. 32, no. 3, pp. 300–335, 2000.

[29] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[30] "The Quantum Mechanics Visualisation Project," Online, https://www.st-andrews.ac.uk/physics/quvis/, [Accessed: Mar 2023].