Quantum Secure Threshold Private Set Intersection Protocol for IoT-Enabled Privacy Preserving Ride-Sharing Application

Tapaswini Mohanty, Vikas Srivastava, Sumit Kumar Debnath, Ashok Kumar Das, *Senior Member, IEEE*, Biplab Sikdar, *Senior Member, IEEE*

***Abstract*—The Internet of Things (IoT)-enabled ride sharing is one of the most transforming and innovative technologies in the transportation industry. It has myriads of advantages, but with increasing demands there are security concerns as well. Traditionally, cryptographic methods are used to address the security and privacy concerns in a ride sharing system. Unfortunately, due to the emergence of quantum algorithms, these cryptographic protocols may not remain secure. Hence, there is a necessity for privacy-preserving ride sharing protocols which can resist various attacks against quantum computers. In the domain of privacy preserving ride sharing, a threshold private set intersection (TPSI) can be adopted as a viable solution because it enables the users to determine the intersection of private data sets if the set intersection cardinality is greater than or equal to a threshold value. Although TPSI can help to alleviate privacy concerns, none of the existing TPSI is quantum secure. Furthermore, the existing TPSI faces the issue of long-term security. In contrast to classical and post quantum cryptography, quantum cryptography (QC) provides a more robust solution, where QC is based on the postulates of quantum physics (e.g., Heisenberg uncertainty principle, no cloning theorem, etc.) and it can handle the prevailing issues of quantum threat and long-term security. Herein, we propose the *first* QC based TPSI protocol which has a direct application in privacy preserving ride sharing. Due to the use of QC, our IoT-enabled ride sharing scheme remains quantum secure and achieves long-term security as well.**

***Index Terms*—Internet of Things (IoT), ride-sharing, quantum communication, private set intersection, long-term security.**

I. Introduction

The Internet of Things (IoT) is a cutting-edge technology that will connect numerous physical things that communicate without the need for human contact. In technical terms, IoT is a network of connected computing devices, mechanical and digital machinery, items, animals, or people that may exchange data across a network without needing human-to-human or human-to-computer communication. Thus, it is expected that IoT will be a crucial part of our daily lives in the coming years. IoT offers a wide range of applications in every aspect of our lives.

The IoT's conveniences come with new security dangers and privacy concerns that need to be appropriately handled. The key challenges in an IoT environment are concerns such as privacy, authorization, verification, access control, system setup, information storage, and administration. IoT being so pervasive in day-to-day human life makes it a great risk to users' privacy. Ignoring these privacy and security concerns would negatively impact many elements of our life, including our houses and the vehicles we use to get to work, and our bodies. IoT privacy protection is essential because an outsider may learn a lot about a person's life by listening in on the sensed data that their wearable technology and smart home gadgets relay. Even if IoT devices just report metadata, it is possible to gather a significant quantity of data about a user's daily life by combining the metadata from several compromised things that surround him/her over time. As a result, security and privacy concerns must be resolved in order to provide users confidence in their privacy and control over their personal information before the IoT is widely used.

In the transportation industry, IoT-enabled ride sharing plays an important role due to its wide advantages like reduced travel expenditure, reduced congestion, etc. It further helps in reducing the pollution. Despite its advantages, several road-blocks have restricted its widespread adoption. For instance, the current technique used in ride sharing is centralized [1] and the service provider companies have access to passengers data. Thus, if ride sharing is put in practice without proper assessment, it may turn out to be a tool for damaging and compromising the passenger's privacy. As a consequence, privacy preserving ride sharing [2] becomes essential where two users only want to share a ride if large parts of their trajectories on a map intersect. In this case, the users may be interested in the concrete intersection of their routes, but only if the overlap is large. Over the years, several proposals have been given for privacy preserving ride sharing in [3]–[7]. Among these, threshold private set intersection (TPSI) seems to be the most suitable candidate to address the problem. TPSI is a two party cryptographic protocol that allows the entities to obtain the intersection of their private sets only when the cardinality of

This work was supported in part by the National Research Foundation, Singapore; in part by A*STAR under its Quantum Engineering Programme (National Quantum-Safe Network) under Grant NRF2021-QEP2-04-P01; in part by the Ripple Centre of Excellence Scheme, Centre of Excellence (CoE) in Blockchain, IIIT Hyderabad, India; and in part by the International Mathematical Union (IMU) and the Graduate Assistantships in Developing Countries (GRAID) Program. (*Corresponding author: Ashok Kumar Das.*)

Tapaswini Mohanty, Vikas Srivastava, and Sumit Kumar Debnath are with the Department of Mathematics, National Institute of Technology, Jamshedpur 831 014, India (e-mail: mtapaswini37@gmail.com; vikas.math123@gmail.com; sdebnath.math@nitjsr.ac.in).

Ashok Kumar Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology at Hyderabad, Hyderabad 500 032, India (e-mail: ashok.das@iiit.ac.in).

Biplab Sikdar is with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117576 (e-mail: bsikdar@nus.edu.sg)

the intersection is greater than or equal to a threshold value. In TPSI, nothing beyond the intersection is revealed to the recipients. In the current state of the art, many designs of TPSI [8]–[15] have been proposed. Security of nearly all of them rely on the number theoretical hardness assumptions. With the advent of quantum algorithms, like Shor's algorithm [16], these hard problems are no longer secure in the quantum domain. Also, the existing TPSI protocols don't address the problem of long-term security. This makes the requirement of quantum computer immune TPSI protocols which can attain long-term security. Quantum cryptography (QC) seems to be the ideal choice to address these issues because unlike classical cryptography (which is based on hardness of number theoretic problems), quantum cryptography is immune from quantum computing attacks (e.g. Shor's algorithm). In addition, it provides long terms security. Therefore, QC is an ideal alternative to provide security and privacy in an IoT setting. The security of QC depends upon the principles of quantum mechanics. QC is primarily based on the Heisenberg Uncertainty principle and the principle of photon polarization. The security of QC-based cryptographic primitives is based on the inviolability of the aforementioned principles. In our proposed design, we make use of the part of QC which uses these two principles to build secure cryptographic primitives.

A. *Motivation*

The following are the main motivations behind the proposal of the scheme in this paper:

- Private set intersection (PSI) is one of most important primitives for secure computation. As already discussed, current protocols for PSI are based on number-theoretic hardness assumptions, and hence they would not be secure in the future due to attacks through quantum algorithms [16]. Motivated by this, researchers have designed several protocols for PSI in the quantum domain [17]–[28]. However, in certain scenarios, the standard PSI functionality is not enough. In particular, it may happen that the clients may only be agreeing to reveal the intersection only if there is a large intersection. This functionality may be achieved through TPSI. *However, there is no construction of secure TPSI protocol in the quantum domain.*
- The security of nearly all of the existing state-of-the-art TPSI relies on the number-theoretical hardness assumptions. The emergence of quantum computing makes these protocols obsolete and insecure. There is a lack of TPSI protocols which can resist these attacks by quantum computers. Hence, it is high time to design a quantum resistant protocol to achieve the threshold private set intersection functionality.
- IoT-enabled ride sharing is one of the fastest growing industries. Use of IoT in the ride-sharing sector can bring disruptive changes. External data regarding the traffic situation, traffic lights, etc., can be used to address issues like congestion and jams in the cities. Data collected through IoT sensors can also help in providing a better user experience as these information can be factored while assigning cars, estimating time and expenditure of travel etc. *However, there is no IoT-enabled ride sharing scheme that can resist quantum attacks.*
- With Shor's algorithm, number theoretic cryptographic schemes can be easily broken. Almost all of the currently used state of the art schemes [29]–[35] used to provide security and privacy in an IoT setting [36] are based on number theoretic problems. Hence, security of all such IoT systems is under a great threat [37]. As of the year 2022, organizations have built quantum computers with up to 50 qubits [38]. Big companies are investing a lot on quantum hardware [39]. In addition, there has been development of software development kit (SDK) which can be used by anyone to work with quantum computers. There are also cloud services that can be used for running a code on a real quantum computer. Even one quantum computer is enough to mount a full scale quantum attack on an IoT system. To address the threat possessed by the quantum computing attacks (like Shor's Algorithm or Grover's Algorithm), cryptographic research community has started working in a new direction of research known as Post quantum cryptography (PQC). The security of PQC depends on mathematical problems which are hard to solve even for a quantum computer. Over the last five years, a lot of work has been done in the context of PQC-based cryptographic primitives for an IoT system [37], [40]–[42]. Although, PQC is an exciting alternative, it suffers from the fact that it does not provide long term security. QC provides an alternative direction of research to provide strong security guarantees, i.e., QC-based primitives provides long term security as well as security against quantum attacks. This motivates us to design QC-based protocols for IoT systems.

B. *Research Contributions*

In this paper, we focus on the design and analysis of TPSI in the context of QC. We call our proposed design as QuTPSI. Design of the proposed scheme is motivated by the works of [18], [43]. The quantum key distribution (QKD) in [44], and I, S and T quantum gates are used as the fundamental building blocks of our design. Security of QuTPSI is based on the basic principles of quantum mechanics. As a consequence, it is secure against quantum attacks and provides long-term security, unlike the existing works [8], [11], [45], [46]. Our design achieves the stipulated security requirements of a TPSI, namely, the trusted party can not obtain any information about the private sets of the users, no user gets any information about the private set of other apart from the intersection, and also an outsider is unable to obtain information about the private sets of users. Both computation and communication cost of QuTPSI is $\mathcal{O}(q+(r+r^*)q)$ where q, r and r^* denote the size of the private vectors, number of initial photons, and number of auxiliary photons, respectively. Our proposed QuTPSI is practical and reliable with present quantum hardware technologies, since simple single-particle projective measurements and single photons are used in the design. We also investigate the probable application of our presented design QuTPSI in the context of IoT-enabled ride sharing.

C. Paper Outline

The remainder of this paper is structured as follows. The related works in the domain of TPSI are discussed at length in Section II. We discuss the mathematical preliminaries in Section III. We describe the construction of our proposed quantum secure TPSI in Section IV. The correctness and security analysis are given in Section V and Section VI, respectively. We compare our design with other existing TPSI in Section VII. Next, we explain how our proposed design can be used as a building block in an IoT-enabled ride-sharing stetting in Section VIII. Finally, the paper is concluded in Section IX.

II. Related Work: Classical TPSI Protocols

The work of Kissner *et al.* [11] dealt with the problem of designing an effective protocol for TPSI and over-threshold PSI. The schemes presented in [11] employed cryptographic methods like homomorphic encryption, equivocal commitment and mix-net and shuffling protocol, and were proven to be secure in honest-but-curious and malicious setting.

In 2018, Zhao *et al.* [14] designed an application oriented TPSI in the server-client model. From the efficiency point of view, the constructions presented by [14] provided linear complexity in the size of the set. Their work greatly improved the classical approach based on Garbled circuit. By utilizing the additively homomorphic encryption, Ghosh *et al.* [8] presented the first construction and study of TPSI with sub-linear complexity (in the size of the set). This was one of the first works that theoretically characterized this class of TPSI. In addition, they provided a lower bound on the complexity of sub-linear TPSI. This was the first work which initiated the study of sublinear TPSI and provided a first characterization of its communication complexity.

The authors in [8] pointed out a not yet known connections between TPSI, set reconciliation protocol, sparse polynomial interpolation. In 2020, Badrinarayanan *et al.* [10] extended the work of [8] and presented two functionalities for multi-party TPSI using the cryptographic primitives like homomorphic encryption. The authors in [10] solved one of the open problems mentioned in the work provided in [8]. Two over threshold multi-party private set intersection were constructed by Mahdavi *et al.* [9] by utilizing cryptographic building blocks like Shamir secret sharing scheme and oblivious pseudo-random functions. They designed a constant round protocol with communication complexity of $O(nmtk)$.

Recently, Bay *et al.* [12] proposed two PSI protocols using bloom filter and threshold homomorphic public-key encryption schemes. Their design scaled quadratically in the number of parties involved with no requirement of a trusted-dealer. The protocols presented in [12] are secure in the semi-honest model. Table I provides a summary of various techniques, advantages and limitations of existing TPSI in two party and multi-party setting.

III. Mathematical Preliminaries

In this section, we discuss about the I, S and T gates [47]. Quantum gate is a unitary operator described by a unitary matrix. More specifically, a quantum gate operating on n qubits can be represented by a unitary matrix of size $2^n \times 2^n$. For a single qubit, we require a matrix of order $2^1 = 2$. In other words, a quantum gate acting on a single qubit (also known as single qubit gate) will be a 2×2 unitary matrix. $I, S,$ and T are three single qubit gates represented as

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix}, \text{ and } T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix},$$

respectively.

Input/output truth table for S and T gate are given in Table II and Table III. Note that S and T gates perform a rotation by an angle of $\pi/2$ radian and $\pi/4$ radian, respectively, around Z-axis.

From the above definition of S and T gates, we can observe that ST and TS both correspond to a rotation by an angle of $3\pi/4$ radian around Z-axis with matrix representation

$$TS = ST = \begin{pmatrix} 1 & 0 \\ 0 & e^{i3\pi/4} \end{pmatrix}.$$

Input/output truth tables for $ST = TS$ gate are given in Table IV.

IV. Proposed Quantum Threshold Private Set Intersection (QuTPSI)

In this section, we first provide a high-level overview of the proposed QuTPSI. Next, we provide the detailed description of QuTPSI.

A. High-Level Overview of QuTPSI

The QuTPSI is run between Charlie with private set $C = \{c_1, \ldots, c_l\} \subseteq \mathbb{Z}_q$ and Donald with private set $D = \{d_1, \ldots, d_m\} \subseteq \mathbb{Z}_q$. A trusted third party (TP) is also involved in this protocol for determining the set intersection cardinality by interacting with Charlie and Donald. If the cardinality is greater than or equal to a prefixed threshold value $t (\in \mathbb{N})$, then the TP sends necessary information to Charlie and Donald for calculating the intersection. The protocol for QuTPSI is summarized in Figs. 3, 1, and 2.

B. Detailed Description of QuTPSI

In the following, Charlie and Donald privately evaluate the desired intersection. We now explain our proposed QuTPSI in detail. The steps involved in QuTPSI are as follows:

1) Charlie and Donald execute a QKD [44] protocol in order to share a nonzero binary secret key sk of length greater than or equal to $\lceil \log_2(q) \rceil$ bits. Let sk correspond to $k \in \mathbb{Z}_q$. In the following, Charlie calculates $C^* = \{kc_1 \mod q, \cdots, kc_l \mod q\}$, and Donald calculates $D^* = \{kd_1 \mod q, \cdots, kd_m \mod q\}$ by using the secret integer k.

TABLE I
TECHNIQUES, ADVANTAGES AND LIMITATIONS OF EXISTING TPSI IN TWO PARTY AND MULTI-PARTY SETTING

Scheme	Cryptographic Techniques	Advantages	Drawbacks/Limitations
Kissner *et al.* [11]	* Hash Functions * Mix-Net and Shuffling Protocol * Equivocal Commitment * Additively Homomorphic Encryption	* TPSI for $n \geq 2$ honest-but-curious parties * Secure against $n-1$ dishonest colluding parties * Over threshold PSI in the malicious setting	* Does not offer long term security * Insecure against quantum attacks
Zhao *et al.* [14]	* Additive Homomorphic Encryption * Oblivious Polynomial Evaluations * Bloom Filters	* Application oriented * Server client model	* Vulnerable against quantum attacks * Does not offer long term security * Does not consider malicious adversary model
Ghosh *et al.* [8]	* Oblivious Linear Function Evaluation * Additive Homomorphic Encryption	* Started the study of sublinear TSPI * Pointed out a not yet known connections between TPSI, set reconciliation protocol, sparse polynomial interpolation	* Does not offer long term security * Insecure against quantum attacks
Badrinarayai *et al.* [10]	* Threshold Fully Homomorphic Encryption * Threshold additive homomorphic encryption with distributed setup	* Sublinear (in the set sizes) communication lower and upper bounds for TPSI * Achieve semi-honest security where up to $(n-1)$ parties could be corrupted * Protocols in star network topology	* Does not offer long term security * Insecure against quantum attacks
Mahdavi *et al.* [9].	* Shamir's Secret Sharing * Oblivious Pseudo-Random Functions * Paillier Cryptosystem	* Constant round protocol * A practical implementation and evaluation of TPSI protocol	* Does not offer long term security * Insecure against quantum attacks
Bay *et al.* [12]	* Bloom Filters and Inverted Bloom Filters * Additivelly Homomorphic Threshold PKE	* First TPSI protocol to be implemented and open-sourced * No trusted dealer required	* Does not offer long term security * Insecure against quantum attacks

TABLE II
INPUT/OUTPUT TRUTH TABLES FOR S GATE

Input	Output
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$e^{\frac{i\pi}{2}}\|1\rangle$

TABLE III
INPUT/OUTPUT TRUTH TABLES FOR T GATE

Input	Output
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$e^{\frac{i\pi}{4}}\|1\rangle$

TABLE IV
INPUT/OUTPUT TRUTH TABLES FOR ST GATE

Input	Output
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$e^{\frac{i3\pi}{4}}\|1\rangle$

2) Utilizing the sets C^* and D^*, Charlie and Donald generate respective private vectors $(x_0, x_1, \ldots, x_{q-1})$ and $(y_0, y_1, \ldots, y_{q-1})$ over $\mathbb{Z}_q$ in the following manner,

$$x_i = 0 \text{ if } i \notin C^*,\ x_i = 1 \text{ if } i \in C^*$$
$$y_i = 0 \text{ if } i \notin D^*,\ y_i = 1 \text{ if } i \in D^*.$$

3) Charlie and Donald share a q-bit private-key K by employing a QKD protocol [44]. The i-th bit of K is considered as $K(i)$.
4) TP randomly chooses q groups of photons, where each group contains r photons (also called initial photons) having the same state from $\{|0'\rangle, |1'\rangle, |+'\rangle, |-'\rangle\}$ with $|0'\rangle = cos\theta|0\rangle + sin\theta|1\rangle$, $|1'\rangle = sin\theta|0\rangle - cos\theta|1\rangle$, $|+'\rangle = \frac{1}{\sqrt{2}}(|0'\rangle + |1'\rangle)$, and $|-'\rangle = \frac{1}{\sqrt{2}}(|0'\rangle - |1'\rangle)$ for $\theta \in (0, \frac{\pi}{10})$. Let the set of these q groups of photons be $A = \{a_1^1, \cdots, a_r^1; a_1^2, \cdots, a_r^2; \cdots; a_1^q, \cdots, a_r^q\}$. TP makes two such copies of A, applies $R_{3\pi/4} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i3\pi}{4}} \end{pmatrix}$ on one such copy and writes down the resulting set as $A_{\frac{3\pi}{4}}$. Note that TP keeps $A_{\frac{3\pi}{4}}$ with it for future and proceeds with A in the next step.
5) In each group of A, TP randomly inserts $r^* \leq r$ randomly chosen single photons (also called auxiliary photons) from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. The resulting set is considered as A^* which may have the form $\{a_1^1,\ a_1^{*1}\ \cdots,\ a_{r^*}^{*1},\ \cdots,\ a_r^1;\ a_1^2,\ \cdots,\ a_1^{*2},\ \cdots,\ a_{r^*}^{*2},\ \cdots a_r^2; \cdots;\ a_1^q,\ \cdots,\ a_{r^*}^{*2}\ \cdots,\ a_{r^*}^{*2},\ \cdots,\ a_r^q\}$. In addition, TP randomly inserts randomly selected l_1 decoy photons from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ in A^* to get A^{**}. TP also notes the position and initial state of each photon and sends A^{**} to Charlie through a quantum channel.
6) On receiving A^{**}, Charlie first queries for l_1 decoy photon positions and corresponding measurement bases, and then announces the measurement results of each of those decoy photons in the correct bases. In the following, TP checks the eavesdropping by comparing these measurement results with the initial states of these l_1 decoy photons. If the error rate is less than or equal to the threshold value which is predetermined by them, they proceed to the next step; otherwise, they abort the process.
7) Charlie gets A^* after discarding the l_1 decoy photons from A^{**}. Now Charlie operates the quantum operators I or S or T to each photon of all the groups of A^* in

the following manner: operates I to each of the photons of the i^{th} group if $x_{i-1} = 0$, operates S to each of the photons of the i^{th} group if $x_{i-1} = 1$ and $K(i) = 0$, and operates T to each of the photons of the i-th group if $x_{i-1} = 1$ and $K(i) = 1$. Let the resulting set be denoted by A_C^*. To avoid eavesdropping, Charlie adds l_2 randomly chosen decoys from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ into A_C^* to get A_C^{**}. Charlie notes the positions and the initial states of these decoy photons and sends the resulting set A_C^{**} to Donald.

8) On receiving A_C^{**}, Donald interacts with Charlie in the similar manner as discussed in Step 6 to detect eavesdropping. If there is no such eavesdropping, Donald discards all the l_2 decoy photons to get A_C^*. In the following, Donald operates the quantum operators I or S or T to each photon of each group of A_C^* in the following manner: operates I to each of the photons of the i-th group if $y_{i-1} = 0$, operates T to each of the photons of the i-th group if $y_{i-1} = 1$ and $K(i) = 0$, and operates S to each of the photons of the i-th group if $y_{i-1} = 1$, $K(i) = 1$. Suppose the resulting set is A_{CD}^*. In order to prevent eavesdropping, Donald adds l_3 decoy photons into A_{CD}^* to get A_{CD}^{**}. These decoy photons are randomly chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Donald notes the positions and initial states of these decoy photons and sends the resulting set A_{CD}^{**} to TP.

9) On receiving A_{CD}^{**}, TP interacts with Donald using similar technique as discussed in Step 6 to check whether there is eavesdropping. If not, then TP discards all l_3 decoy photons to get A_{CD}^*, and performs the following steps:
   (i) Discards all the auxiliary photons added during Step 5 from each group and gets A_{CD} (say).
   (ii) Sets a count variable p as 0.
   (iii) Measures all the photons of the set A_{CD}.
   (iv) For $1 \leq i \leq r$, if the measurement result of the i-th group of A_{CD} is same as the i-th group of the set $A_{\frac{3\pi}{4}}$, then increases p by 1 i.e. $p = p + 1$.
   (v) Writes L as the set of indices for which group the measurement result of A_{CD} matches with $A_{\frac{3\pi}{4}}$
   (vi) If p is less than t, then aborts the process and outputs 0; otherwise sends L to Charlie and Donald.

10) Let C_{int} and D_{int} be two empty sets. For each $i \in L$, Charlie computes $c_s = k^{-1}(i-1) \mod q$ and appends c_s to C_{int}, while Donald computes $d_t = k^{-1}(i-1) \mod q$ and appends d_t to D_{int}. Finally, the resulting sets C_{int} and D_{int} are respectively the desired intersection for Charlie and Donald. In fact $D_{int} = C_{int}$.

The communication flows of our proposed design are finally provided in Figs. 3, 1, and 2. For a better understanding of our design, a toy example is give in Section A.

V. Correctness of QuTPSI

In the section, we prove the correctness of our proposed design. We first show that TP is able to correctly calculate the intersection cardinality. Without loss of generality, let the initial state of all the elements of the i-th group of A prepared by TP in Step 4 be $|0'\rangle$. Recall that, TP also applies $\begin{pmatrix}1 & 0\\ 0 & e^{\frac{i3\pi}{4}}\end{pmatrix}$ on one of the copies of A to get $A_{\frac{3\pi}{4}}$. It implies that the state $|0'\rangle$ in $A_{\frac{3\pi}{4}}$ is rotated by an angle of $\frac{3\pi}{4}$ radian.

Consider the case when $K(i) = 0$. A similar analysis can be done for the other case $K(i) = 1$.

- **Case I** ($K(i) = 0$)**:** The following possibilities may arise.
  (i) $x_{i-1} = 0$ and $y_{i-1} = 0$. Then Charlie applies quantum gate I on $|0'\rangle$, and subsequently Donald applies quantum gate I on $I|0'\rangle$. Therefore, in the resulting i-th group, the states $|0'\rangle$s are rotated by an angle of zero radian. Thus, the measurement result does not match with the i-th group of $A_{\frac{3\pi}{4}}$, and hence, it has no contribution to the intersection cardinality.
  (ii) $x_{i-1} = 0$ and $y_{i-1} = 1$. In this case, Charlie and Donald operate I on $|0'\rangle$, and T on $I|0'\rangle$, respectively. Thereby, in the resulting i-th group, the states $|0'\rangle$s are rotated by an angle of $\frac{\pi}{4}$ radians which mismatches with the i-th group of $A_{\frac{3\pi}{4}}$. Therefore, it contributes nothing towards the intersection cardinality.
  (iii) $x_{i-1} = 1$ and $y_{i-1} = 0$. Then, Charlie applies S on $|0'\rangle$, and later Donald operates quantum gate I on $S|0'\rangle$. As a consequence, in the resulting i-th group, the states $|0'\rangle$s are rotated by an angle of $\frac{\pi}{2}$ radian. This result does not match with the i-th group of $A_{\frac{3\pi}{4}}$. Thereby, it does not contribute anything towards the intersection cardinality.
  (iv) $x_{i-1} = 1$ and $y_{i-1} = 1$. In this case, Charlie operates S on $|0'\rangle$, and subsequently Donald applies quantum gate T on $S|0'\rangle$. Therefore, in the resulting i-th group, the states $|0'\rangle$s are rotated by an angle of $\frac{3\pi}{4}$ radians. So the resulting state will match with the i-th group of $A_{\frac{3\pi}{4}}$. Note that, in this case TP increases p by 1 as mentioned in Step 9 of the protocol. Hence, it contributes towards intersection cardinality.
- **Case II** ($K(i) = 1$)**:** A similar analysis can be done for this case with the following four possibilities.
  (i) $x_{i-1} = 0$ and $y_{i-1} = 0$. Then the resulting i-th group will not match with the i-th group of $A_{\frac{3\pi}{4}}$ as the resulting i-th group is obtained by an angle zero radian rotation. Consequently, this case contributes nothing towards the intersection cardinality.
  (ii) $x_{i-1} = 0$ and $y_{i-1} = 1$. Here the resulting i-th group is obtained by $\frac{\pi}{2}$ radians rotation, where rotation of 0 radian is due to Charlie and $\frac{\pi}{2}$ radians rotation is due to Donald. As a result, it does not match with the i-th group of $A_{\frac{3\pi}{4}}$. Thus, this case does not contribute to the intersection cardinality.
  (iii) $x_{i-1} = 1$ and $y_{i-1} = 0$. In this case, due to Charlie's rotation about an angle of $\frac{\pi}{4}$ radians and Donald's rotation about an angle of 0 radian, the resulting i-th group will not match with the i-th group of $A_{\frac{3\pi}{4}}$ and hence, it will not provide any contribution to the intersection cardinality.

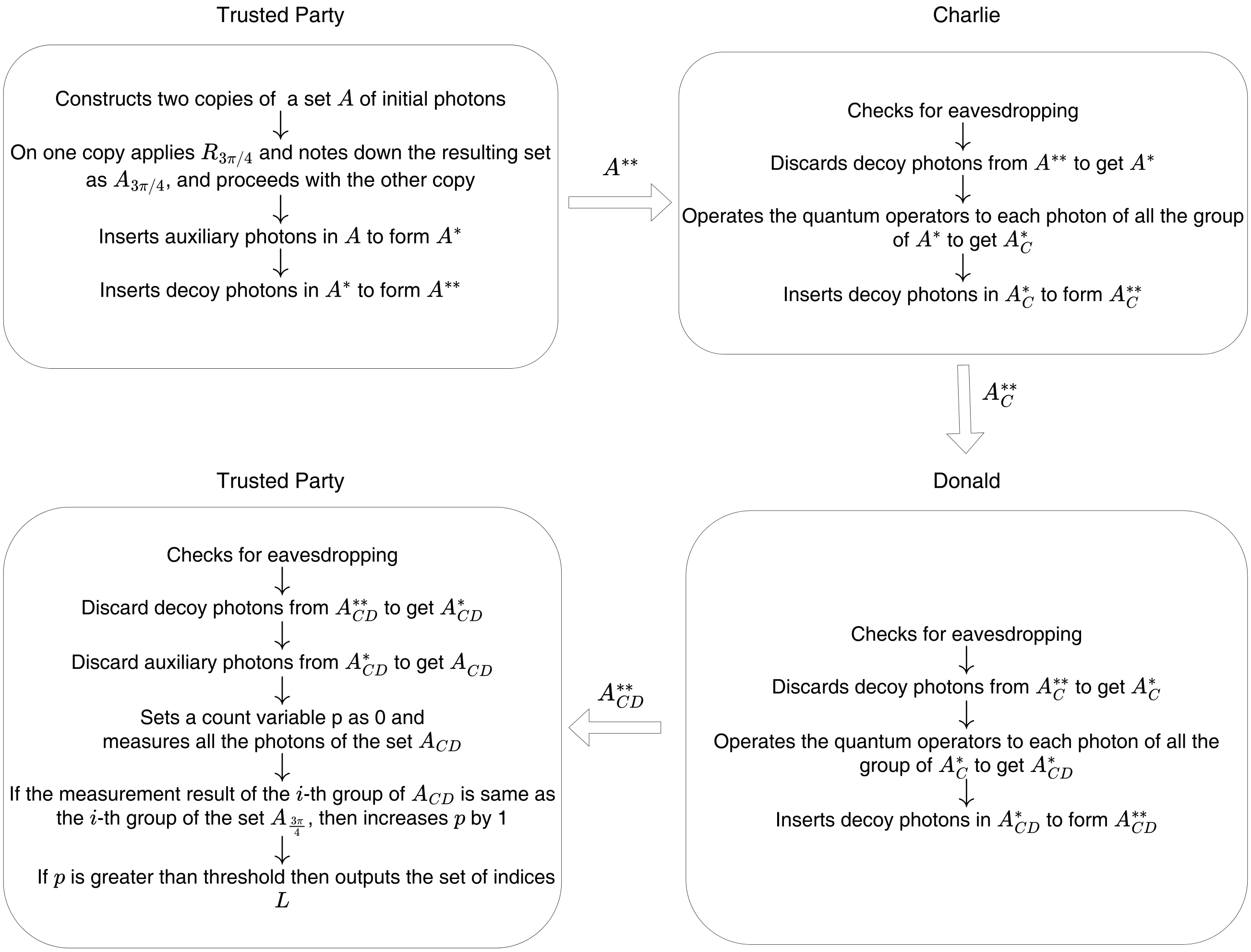
Trusted Party
Constructs two copies of a set A of initial photons
On one copy applies $R_{3\pi/4}$ and notes down the resulting set as $A_{3\pi/4}$, and proceeds with the other copy
Inserts auxiliary photons in A to form A^*
Inserts decoy photons in A^* to form A^{**}
A^{**}
Charlie
Checks for eavesdropping
Discards decoy photons from A^{**} to get A^*
Operates the quantum operators to each photon of all the group of A^* to get A^*_C
Inserts decoy photons in A^*_C to form A^{**}_C
A^{**}_C
Donald
Checks for eavesdropping
Discards decoy photons from A^{**}_C to get A^*_C
Operates the quantum operators to each photon of all the group of A^*_C to get A^*_{CD}
Inserts decoy photons in A^*_{CD} to form A^{**}_{CD}
A^{**}_{CD}
Trusted Party
Checks for eavesdropping
Discard decoy photons from A^{**}_{CD} to get A^*_{CD}
Discard auxiliary photons from A^*_{CD} to get A_{CD}
Sets a count variable p as 0 and measures all the photons of the set A_{CD}
If the measurement result of the i-th group of A_{CD} is same as the i-th group of the set $A_{\frac{3\pi}{4}}$, then increases p by 1
If p is greater than threshold then outputs the set of indices L

Fig. 1. Communication flow of our proposed design (Step 4 to Step 9)

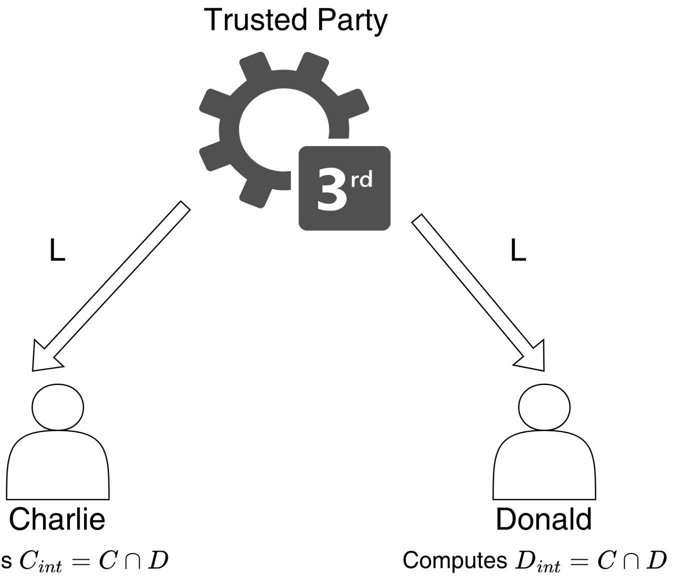

Fig. 2. Communication flow of our proposed design (Step 10)

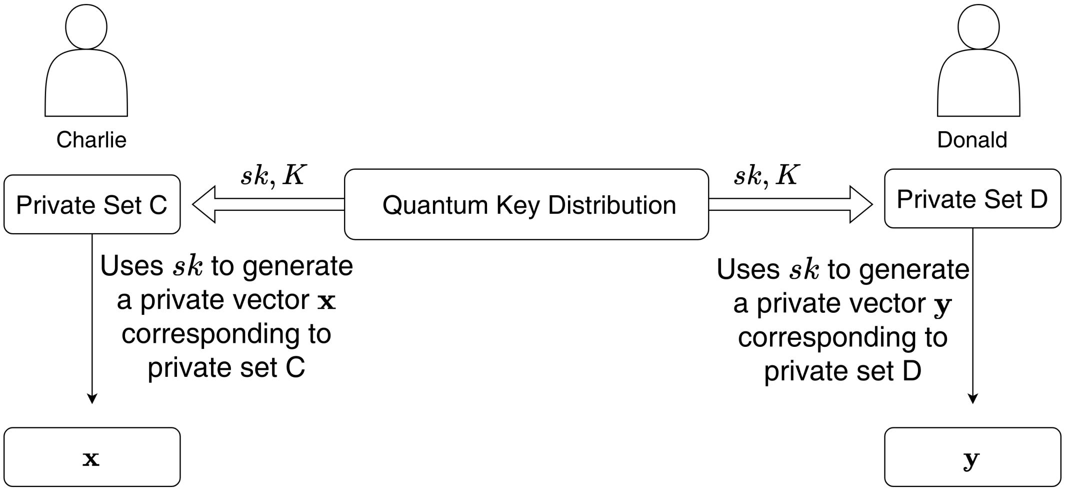
Charlie
Donald
Private Set C
sk, K
Quantum Key Distribution
sk, K
Private Set D
Uses sk to generate a private vector $\mathbf{x}$ corresponding to private set C
Uses sk to generate a private vector $\mathbf{y}$ corresponding to private set D
$\mathbf{x}$
$\mathbf{y}$

Fig. 3. Communication flow of our proposed design (Step 1 to Step 3)

(iv) $x_{i-1} = 1$ and $y_{i-1} = 1$. In this case, Charlie and Donald gives $\frac{\pi}{4}$ radians and $\frac{\pi}{2}$ radians rotations, respectively. As a consequence, the resulting i-th group is obtained by $\frac{3\pi}{4}$ radian rotation which is same as the i-th group of $A_{\frac{3\pi}{4}}$. This case contributes to the intersection cardinality since TP increases p by 1 only when the i-th resulting group matches with the i-th group of $A_{\frac{3\pi}{4}}$.

From the above analysis, we observe that the initial state is rotated by an angle of $\frac{3\pi}{4}$ radian if and only if $x_{i-1} = 1$ and $y_{i-1} = 1$ for both cases $K(i) = 0$ and $K(i) = 1$. We now show that counting such pairs $(x_{i-1} = 1, y_{i-1} = 1)$ gives us the actual intersection cardinality, i.e., $|C \cap D| = |C^* \cap D^*| = \sum_{i=0}^{q-1} x_i y_i$. By the construction of (x_{i-1}, y_{i-1}), $i-1 \in C^* \cap D^*$ if $x_{i-1} = 1$ and $y_{i-1} = 1$. This yields $|C^* \cap D^*| = \sum_{i=0}^{q-1} x_i y_i$. Note that the elements of C^* and D^* are obtained from C and D, respectively, by modular multiplication with the integer k. For an $i \in C^* \cap D^*$ there exist $s \in \{1, \cdots, l\}$ and $t \in \{1, \cdots, m\}$ such that $(kc_s \mod q) = i$ and $(kd_t \mod q) = i$, i.e., $c_s = k^{-1}(i) \mod q$ and $d_t = k^{-1}(i) \mod q$ which implies $c_s = d_t \in C \cap D$. On the other hand, for all element $e \in C \cap D$, $ke(\mod q) \in C^* \cap D^*$. Thus, we can conclude that $|C \cap D| = |C^* \cap D^*|$ which is equal to $\sum_{i=0}^{q-1} x_i y_i$.

We now show that Charlie and Donald are able to calculate the intersection correctly. If $i \in L$ then $|0'\rangle$ is rotated by $\frac{3\pi}{4}$ radians. It means that $x_{i-1} = 1$ and $y_{i-1} = 1$, which in turn implies that $i-1 \in C^* \cap D^*$. Hence, there exist $s \in \{1, \cdots, l\}$ and $t \in \{1, \cdots, m\}$ such that $(kc_s \mod q) = i - 1$ and $(kd_t \mod q) = i - 1$, i.e., $c_s = k^{-1}(i-1) \mod q$ and $d_t = k^{-1}(i-1) \mod q$. Thus, $c_s = d_t \in C \cap D$. In other words, corresponding to each $i \in L$ or $i-1 \in C^* \cap D^*$, Charlie and Donald are able to compute the corresponding $e \in C \cap D$ such that $e = k^{-1}(i) \mod q$. Again, $|C \cap D| = |C^* \cap D^*|$. Hence, the participants can correctly calculate the intersection $C \cap D$ by computing $k^{-1}(i-1) \mod q$ for each $i \in L$.

VI. Security Analysis

In this section, we prove that QuTPSI protocol meets the following security requirements:

(i) TP can not obtain any information about the private sets of Charlie and Donald.
(ii) Donald gets no information about the private set of Charlie apart from $C \cap D$.
(iii) Charlie does not get any information about Donald's private set, beyond $C \cap D$.
(iv) An outsider is unable to obtain information about the private sets of Charlie and Donald.

Theorem 1. *TP can not obtain any information about the private sets of Charlie and Donald.*

Proof. A dishonest TP may prepare entangled photons instead of single photons to obtain information about the private sets of Charlie and Donald. Suppose TP initially prepares the entangled photon $\frac{1}{\sqrt{3}}|01\rangle + \frac{\sqrt{2}}{\sqrt{3}}|10\rangle$, keeps the first photon and sends the second photon to Charlie. Then, the reduced density matrix corresponding to the first photon is

$$\frac{1}{3}|0\rangle\langle 0| + \frac{2}{3}|1\rangle\langle 1|.$$

As the reduced density matrix is independent of the unitary operator applied to the photon, so TP can not gain any information about the private set of Charlie.

There is another possibility of how TP can act. If TP eavesdrops to get information about the private sets of Charlie, then he may apply the unambiguous state discrimination (USD) to successfully guess the initial states of the selected photons which is different from the decoy photons. The success probability to know the initial states is $\mathsf{Prob}^{USD} = 1 - F(\rho_0, \rho_1)$, where $F(\rho_0, \rho_1)$ is the fidelity between the two quantum states which TP seeks to discriminate. Let $|0'\rangle$ be the initial state prepared by TP. Then, $S(|0'\rangle) = \cos(\theta)|0\rangle + e^{\frac{i\pi}{2}} \sin(\theta)|1\rangle$

(i.e., $x_{i-1} = 1$), and thus, the successful probability of USD is

$$\begin{aligned}\mathsf{Prob}^{USD} &= 1 - F(\rho_0, \rho_1)\\ &= 1 - (\cos^2(2\theta) + \frac{1}{4}\sin^4(2\theta)).\end{aligned}$$

If $\theta = \frac{\pi}{20}$,

$$\begin{aligned}\mathsf{Prob}^{USD} &= 1 - (\cos^2(2\theta) + \frac{1}{4}\sin^4(2\theta))\\ &= 1 - \left(\cos^2\left(\frac{2\pi}{20}\right) + \frac{1}{4}\sin^4\left(\frac{2\pi}{20}\right)\right)\\ &= 1 - 0.906\\ &\approx 0.094.\end{aligned}$$

Therefore, the success probability of TP in deducing $x_{i-1} = 0$ or $x_{i-1} = 1$ is 0.094. Also, TP does not know the secret key k, and hence, TP can not obtain any information about the private set of Charlie. □

Theorem 2. *Donald gets no information about the private set of Charlie.*

Proof. In order to obtain any information about the private set of Charlie, Donald measures the photons of the set A^*_C. If $x_{i-1} = 0$ then Charlie did nothing and therefore the i-th group is the same as what TP prepared initially. As Donald does not know the actual measurement bases, he can guess $x_{i-1} = 0$ with probability $\frac{1}{2}$. If $x_{i-1} = 1$, then Charlie applies S or T according to $K(i)$. Also, in this case, Donald guesses $x_{i-1} = 1$ with probability $\frac{1}{2}$ as he does not know the actual measurement bases. As a result, Donald is unable to extract any information about the private set of Charlie. □

Theorem 3. *Charlie does not get any information about Donald's private set, beyond $C \cap D$.*

Proof. If Charlie wants to get any information about the private set of Donald, he needs to intercept the quantum communication channel between Donald and TP. Note that, Charlie does not know the actual positions of the initial photons and auxiliary photons. In addition, all these photons are non-orthogonal, therefore, these are indistinguishable. Hence, Charlie does not get any information about Donald's private set, beyond $C \cap D$. □

Theorem 4. *An outsider is unable to obtain any information about the private sets of Charlie and Donald.*

Proof. If an outsider wants any information about the private sets of Charlie and Donald then he may perform entangle measurement attack on a decoy photon state, say $|\psi\rangle_d \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. On receiving the decoy state $|\psi\rangle_d$, he prepares an ancillary state $|0\rangle_a$ and operates an oracle operator $\mathcal{O}_\delta : |\delta_1\rangle|\delta_2\rangle \mapsto |\delta_1\rangle|\delta_2 \oplus \delta(\delta_1)\rangle$.

- **Case I:** If $|\psi\rangle_d$ is $|0\rangle$ or $|1\rangle$, then

$$\mathcal{O}_\delta|\psi\rangle_d|0\rangle_a = \begin{cases} |0\rangle|0 \oplus \delta(0)\rangle_a & \\ = |0\rangle|\delta(0)\rangle_a, & \text{if } |\psi\rangle_d = |0\rangle \\ |1\rangle|0 \oplus \delta(1)\rangle_a & \\ = |1\rangle|\delta(1)\rangle_a, & \text{if} |\psi\rangle_d = |1\rangle. \end{cases}$$

- **Case II:** If $|\psi\rangle_d \in \{|+\rangle, |-\rangle\}$, then

$$\begin{aligned}\mathcal{O}_\delta|\psi\rangle_d|0\rangle_a &= \frac{\mathcal{O}_\delta|0\rangle|0\rangle_a \pm \mathcal{O}_\delta|1\rangle|0\rangle_a}{\sqrt{2}}\\ &= \frac{|0\rangle|0 \oplus \delta(0)\rangle_a \pm |1\rangle|0 \oplus \delta(1)\rangle_a}{\sqrt{2}}\\ &= \frac{|0\rangle|\delta(0)\rangle_a \pm |1\rangle|\delta(1)\rangle_a}{\sqrt{2}}\\ &= \frac{1}{\sqrt{2}}[\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|\delta(0)\rangle_a \pm |\delta(1)\rangle_a}{\sqrt{2}}\\ &+ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \frac{|\delta(0)\rangle_a \mp |\delta(1)\rangle_a}{\sqrt{2}}].\end{aligned}$$

By the above analysis, we see that if $|\psi\rangle_d \in \{|0\rangle, |1\rangle\}$, the outsider can guess correctly but if $|\psi\rangle_d \in \{|+\rangle, |-\rangle\}$ then the success probability is $\frac{1}{2}$. In addition, all these photons are non orthogonal so these states are indistinguishable. Therefore, the outsider fails to obtain any information about the private sets of Charlie or Donald. Also, an outsider does not know the secret key k, and hence, the outsider can not obtain any information about the entities private sets. □

VII. Performance Analysis

The communication cost and computation cost of the proposed scheme are discussed below. Next, we compare the performance of the proposed scheme with the existing competing schemes of Hallgren *et al.* [48], Ghosh and Nilges [49], Ghosh and Simkin [8], Badrinarayanan *et al.* [10] and Zhang *et al.* [50].

A. Communication Cost

In the proposed scheme, $\lceil \log_2(q) \rceil + q$ qubits are required to be transferred during the key sharing. $3(r + r^*)q + l_1 + l_2 + l_3$ qubits are needed to be shared for the computation of cardinality of private sets. Let $|L|$ be the cardinality of L in bits. The set of indices L can be sent as a bitstring of length q by putting 1 at the places for which the indices are contained in L and 0 at the remaining places. Thus, $2q$ additional bits are needed to be transferred for the computation of intersection.

B. Computation Cost

In the proposed scheme, $\lceil \log_2(q) \rceil + q + l_1 + l_2 + l_3$ projective measurements are required. $2rq + r^*q + l_1 + l_2 + l_3$ single photons are needed to be prepared. $2rq + 2(r + r^*)q$ quantum unitary operations have to be performed. In addition, we also require $l + m + 2p$ modular multiplications.

Our scheme is very efficient as it does not employ any complicated oracle operators. In addition, it utilizes single photons and simple single-particle projective measurements. Thereby, it has the potential of being implemented with the current quantum hardware technologies [51], [52].

C. Comparative Study

Since our proposed design is the first quantum cryptography based TPSI, we compare our scheme with other existing state

TABLE V
COMPARISON TABLE OF OUR PROPOSED PROTOCOL WITH EXISTING TPSI PROTOCOLS

Protocol	Computation cost	Communication cost	Quantum cryptography based	Long-term security
Hallgren *et al.* [48]	$\mathcal{O}(n^2)$	$\mathcal{O}(\lambda n)$	No	No
Ghosh and Nilges [49]	$\mathcal{O}(n \log^2 n)$	$\mathcal{O}(n\lambda)$	No	No
Ghosh and Simkin [8]	$\mathcal{O}((n-t)^4)$	$\mathcal{O}(t)$	No	No
Badrinarayanan *et al.* [10]	$\mathcal{O}((n-t)^4)$	$\mathcal{O}(Nt)$	No	No
Zhang *et al.* [50]	$\mathcal{O}(n \log n)$	$\mathcal{O}(\lambda M)$	No	No
Proposed (QuTPSI)	$\mathcal{O}(q + (r + r^*)q)$	$\mathcal{O}(q + (r + r^*)q)$	Yes	Yes

n: size of the private sets, λ: security parameter, δ: the number of hash functions, t: the threshold value, M: the length of Bloom filter and N: the number of parties, q: size of the private vectors of the users, r: number of initial photons, r^*: number of auxiliary photons.

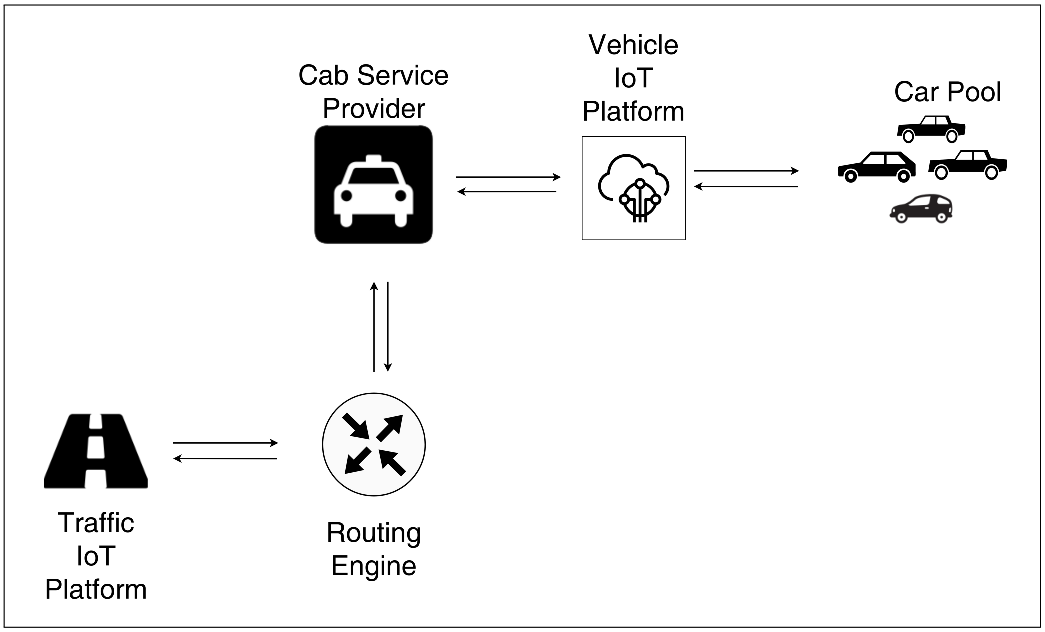

Fig. 4. Communication flow of Phase IV

of the art TPSI protocols. A comparative study on communication and computational costs, and functionality features among the proposed scheme and the existing competing schemes of Hallgren *et al.* [48], Ghosh and Nilges [49], Ghosh and Simkin [8], Badrinarayanan *et al.* [10] and Zhang *et al.* [50], has been provided in Table V. Our proposed design is in quantum domain, and hence, its computational and communication overhead involves qubits and other quantum resources. The existing competing schemes [8], [10], [48]–[50] are having classical computational and communication cost. Therefore, no direct comparison can be made based on computational and communication cost point of view. But, our proposed design is superior to these schemes due to its advanced security features. The design of [8], [10], [48]–[50] are based on classical hardness assumptions. Hence, in near future these scheme will become obsolete and insecure. Even one quantum computer is enough to mount an attack over these schemes. These schemes also fails to provide long term security. In contrast, our proposed design is long term secure. In addition, it provides security against quantum adversary as well as classical adversary. Security is one of the most important component of an IoT system, and our proposed design assures strong security guarantees with minimal quantum resources. The results are summarized in Table V.

VIII. APPLICATION TO IOT-ENABLED PRIVACY PRESERVING RIDE SHARING

In this section, we explain how our proposed quantum secure TPSI scheme (QuTPSI) can be utilized as a building block in an IoT-enabled ride sharing setting.

We first give a high level overview of the system design. Our model allows two people, say Charlie and Donald, to share the ride if the intersection of their routes is greater than or equal to a certain predefined threshold value. The complete system model can be categorized into four phases. In Phase I, Charlie and Donald interact with each other. Here, they execute a quantum key distribution (QKD) among themselves to hide their private trajectories. The next two phases (i.e., Phase II and Phase III) involve a trusted third party (TP), which assists Charlie and Donald in calculating the intersection of their private routes. At the end of Phase III, Charlie and Donald know what their shared path is. In Phase IV, the clients who wish to share the ride, contact a car leasing service provider Cab for the further process.

A. Various Phases

The details of the phases are provided in the following subsections. A supporting example for Phase I, Phase II and Phase III is provided in Section A.

1) Phase I: Let Charlie and Donald be the two clients who wish to share their journey. Suppose traj_C and traj_D denote respectively the private trajectories of Charlie and Donald. Now, they execute a quantum key distribution (QKD) protocol to share a non-zero binary secret key, say sk. In the following, they use sk to modify traj_C and traj_D into $\mathsf{traj}^*_\mathsf{C}$ and $\mathsf{traj}^*_\mathsf{D}$, respectively. Using the aforementioned modifications, Charlie and Donald then generate respective private vectors corresponding to their trajectories, namely $\mathbf{x}$ and $\mathbf{y}$. In the end, Charlie and Donald share a q-bit private-key K by again employing some QKD protocol. They store this key K for the future purposes. An illustrative diagram for this purpose is already given in Fig. 3.

2) Phase II: This phase involves the trusted TP. TP randomly chooses a set A consisting of q groups of photons, where each group contains r photons. It makes two such copies of A, then applies $R_{3\pi/4}$ on one such copy, and writes down the resulting set as $A_{3\pi/4}$. It keeps $A_{3\pi/4}$ and proceeds with A in the next step. In each group of A, TP randomly inserts randomly chosen single photons, also known as auxiliary photons. The resulting set is denoted by A^*. In addition, TP also randomly inserts randomly selected decoy photons in A^* to get A^{**}. After noting down the position and initial states of each photon, TP sends A^{**} to Charlie through a quantum channel.

Charlie on his end, discards the decoy photons from A^{**}. Now, Charlie uses the key K shared in Phase I and operates the quantum operators I or S or T to each photon of all the groups of A^* as per the rules specified in Step 7 of the proposed scheme (see Section IV-B). To avoid eavesdropping, Charlie also adds some randomly chosen decoy photons to form a set A^{**}_C, and sends the final set to Donald. On receiving A^{**}_C from Charlies, Donald proceeds in the similar fashion as Charlie. In particular, he discards all the decoy photons, and then uses the pre-shared key K to operate the quantum operators I or S or T to each photon of each group according to rules specified in Step 8. In order to prevent eavesdropping, Donald adds decoy photons to form the set A^{**}_{CD}. Donald sends the resulting set A^{**}_{CD} to TP. In the end, TP follows Step 9 to calculate L, and sends it to Charlie and Donald. L has sufficient information which can be used by Charlie and Donald to calculate the intersection. Fig. 1 gives an illustrative summary of this phase.

3) Phase III: For each $i \in L$, Charlie computes $c_s = k^{-1}(i-1) \mod q$, while Donald computes $d_t = k^{-1}(i-1) \mod q$. This collection of c_s and d_s actually gives them the shared trajectories. In other words, $\{c_s\} = \mathsf{traj}_\mathsf{C} \cap \mathsf{traj}_\mathsf{D} = \{d_t\}$ (refer to Section V).

4) Phase IV: Charlie and Donald know what paths they are going to share. They contact a car-leasing service provider (we call it as Cab) for the ride-sharing service. A message broker is used to send their requests to the Cab. Cars associated with the Cab exchange data with it through a customized vehicle IoT platform. These cars have IoT sensors fitted in that collect data related to location of the car, pick-ups, and drop-offs, and send it to the vehicle IoT platform. While on the other side, Cab sends the information about client-assignments and route-instructions to the connected cars via the same vehicle IoT platform. Through the data sent by a traffic routing engine, Cab calculates the travel times for the shared trajectories. The data received through routing engine can also be utilized to provide a better service to the users. This routing engine gets information about changes in traffic situation through a dedicated traffic-IoT platform. Fig. 4 shows an illustrative diagram for this phase.

B. Discussions

We have seen how our scheme (QuTPSI) can be utilized in ride-sharing setting. We now discuss some of the security risks and how our scheme alleviates the security concerns. Charlie and Donald might try to know the private trajectories of each other and hamper the security and privacy of the system. Our design ensures that the passengers learn not more than the intersection of their private trajectories (refer to Theorem 2 and Theorem 3). The third party involved in Phase II and Phase III can not obtain any information about the private routes of passengers (refer to Theorem 1). Our design also ensures that no outsider can learn the passengers private information (refer to Theorem 4). Our scheme relies on quantum cryptography. As a consequence, it provides security against the attacks by quantum computer and achieves long term security. Thus, QuTPSI can be utilized as a building block to design a quantum secure IoT-enabled ride sharing scheme.

IX. Conclusion

In this article, to the best of our knowledge, we propose the *first* quantum cryptography based threshold private set intersection protocol QuTPSI. The security of QuTPSI is based on the quantum physical laws. Hence, it provides security against attacks through quantum algorithms. In addition, it also provides long-term security, unlike the the classical TPSI protocols. Moreover, we investigated the possible application of our presented design QuTPSI in the domain of ride sharing to develop a quantum computer resistant long-term secure privacy preserving ride sharing application.

Appendix A
Toy Example

In this section, we give an illustrative example for our proposed design.

A. Phase I

Let traj_C, and traj_D be the private trajectories of Charlie and Donald represented by the set $C = \{1, 2, 4\}$ and $D = \{0, 1, 2, 3\}$ respectively. The individual elements of these sets belongs to $\mathbb{Z}_5$. Charlie and Donald share a secret integer $k = 2$ through QKD. We set the threshold value to be $t = 2$. Now using $k = 2$, they transform the set corresponding to their private trajectories into $\mathsf{traj}^*_\mathsf{C} = \{2 \cdot 1 \mod 5, 2 \cdot 2 \mod 5, 2 \cdot 4 \mod 5\} = \{2, 4, 3\}$ and $\mathsf{traj}^*_\mathsf{D} = \{2 \cdot 0 \mod 5, 2 \cdot 1 \mod 5, 2 \cdot 2 \mod 5, 2 \cdot 3 \mod 5\} = \{0, 2, 4, 1\}$ Utilizing the sets $\mathsf{traj}^*_\mathsf{C}$

TABLE VI
CHOICE OF OPERATOR FOR CHARLIE IN TOY EXAMPLE GIVEN IN SECTION A

x	0	0	1	1	1
K	0	1	0	1	1
Operator	I	I	S	T	T

TABLE VII
CHOICE OF OPERATOR FOR DONALD IN TOY EXAMPLE GIVEN IN SECTION A

y	1	1	1	0	1
K	0	1	0	1	1
Operator	T	S	T	I	S

and $\mathsf{traj}^*_{\mathsf{D}}$, Charlie and Donald generate their respective private vectors $x = 00111$ and $y = 11101$ by going through rules described in Step 2. In the next step, by employing a QKD protocol they share a 5-bit secret key $K = K_1K_2K_3K_4K_5 = 01011$.

B. Phase II

TP prepares 5 group of photons with $r = 3$, and $r^* = 2$. TP prepares two copies of the set $A = \{|0'\rangle, |0'\rangle, |0'\rangle; |+'\rangle, |+'\rangle, |+'\rangle; |0'\rangle, |0'\rangle, |0'\rangle; |1'\rangle, |1'\rangle, |1'\rangle; |-'\rangle, |-'\rangle, |-'\rangle\}$. In the following, TP applies $\begin{pmatrix}1 & 0\\ 0 & e^{\frac{i3\pi}{4}}\end{pmatrix}$ on one of the copies and get the set $A_{\frac{3\pi}{4}}$. In each group of A, TP randomly inserts $r^* \leq r$ randomly chosen single photons (also called auxiliary photons). Let the position of the auxiliary photons in each group be the following: Group$_1 = 4^{th}$ and 5^{th} position, Group$_2 = 4^{th}$ and 5^{th} position, Group$_3 = 1^{st}$ and 2^{nd} position, Group$_4 = 1^{st}$ and 5^{th} position, and Group$_5 = 3^{rd}$ and 5^{th}position. Let the resulting set be $A^* = \{|0'\rangle, |0'\rangle, |0'\rangle, |1'\rangle, |0'\rangle; |+'\rangle, |+'\rangle, |+'\rangle, |1'\rangle, |-'\rangle; |1'\rangle, |0'\rangle, |0'\rangle, |0'\rangle, |0'\rangle; |1'\rangle, |1'\rangle, |1'\rangle, |1'\rangle, |1'\rangle; |-'\rangle, |-'\rangle, |1'\rangle, |-'\rangle, |+'\rangle\}$. In the next step, TP adds some decoy photons in A^* to get A^{**} and sends A^{**} to Charlie. Charlie discards decoy photons from A^{**} to get A^*. Now Charlie operates the quantum operators I or S or T to each photon of all the group of A^* according to rules described in Step 7. For our case, Table VI summarizes which operator to use. Let the resulting set be denoted by $A^*_C = \{|0'\rangle, |0'\rangle, |0'\rangle, |1'\rangle, |0'\rangle; |+'\rangle, |+'\rangle, |+'\rangle, |1'\rangle, |-'\rangle; S|1'\rangle, S|0'\rangle, S|0'\rangle, S|0'\rangle, S|0'\rangle; T|1'\rangle, T|1'\rangle, T|1'\rangle, T|1'\rangle, T|1'\rangle; T|-'\rangle, T|-'\rangle, T|1'\rangle, T|-'\rangle, T|+'\rangle\}$. Charlie further adds decoy photons to A^*_C to get A^{**}_C and sends it to Donald. Donald removes decoy photons from A^{**}_C to get A^*_C. In the following, Donald operates the quantum operators I or S or T to each photon of each group of A^*_C by following the rules described in Step 8. Table VII describes the choice of operator for our case. Let the resulting set be $A^*_{CD} = \{T|0'\rangle, T|0'\rangle, T|0'\rangle, T|1'\rangle, T|0'\rangle; S|+'\rangle, S|+'\rangle, S|+'\rangle, S|1'\rangle, S|-'\rangle; TS|1'\rangle, TS|0'\rangle, TS|0'\rangle, TS|0'\rangle, TS|0'\rangle; T|1'\rangle, T|1'\rangle, T|1'\rangle, T|1'\rangle, T|1'\rangle; ST|-'\rangle, ST|-'\rangle, ST|1'\rangle, ST|-'\rangle, ST|+'\rangle\}$ In the following, Donald add decoy photons to A^*_{CD} to get A^{**}_{CD} and sends the resulting set to TP. TP removes decoy photons from A^{**}_{CD} to get A^*_{CD}. It discards auxiliary photons (underlined states) from $A^*_{CD} = \{T|0'\rangle, T|0'\rangle, T|0'\rangle, \underline{T|1'\rangle}, \underline{T|0'\rangle}; S|+'\rangle, S|+'\rangle, S|+'\rangle, \underline{S|1'\rangle}, \underline{S|-'\rangle}; \underline{TS|1'\rangle}, \underline{TS|0'\rangle}, TS|0'\rangle, TS|0'\rangle, TS|0'\rangle; \underline{T|1'\rangle}, T|1'\rangle, T|1'\rangle, T|1'\rangle, \underline{T|1'\rangle}; ST|-'\rangle, ST|-'\rangle, ST|1'\rangle, ST|-'\rangle, ST|+'\rangle\}$ to get $A_{CD} = \{T|0'\rangle, T|0'\rangle, T|0'\rangle; S|+'\rangle, S|+'\rangle, S|+'\rangle; TS|0'\rangle, TS|0'\rangle, TS|0'\rangle; T|1'\rangle, T|1'\rangle, T|1'\rangle; ST|-'\rangle, ST|-'\rangle, ST|-'\rangle\}$. In the following, TP measures all photons of all groups and compare it with $A_{\frac{3\pi}{4}}$. Since $TS = ST = \begin{pmatrix}1 & 0\\ 0 & e^{\frac{i3\pi}{4}}\end{pmatrix}$, therefore, 3^{rd} and 5^{th} group of A_{CD} are identical with the 3^{rd} and 5^{th} group of $A_{\frac{3\pi}{4}}$. As two position are matching, count variable p is equal to 2. Note that if ith group matches, then $i-1 \in L$, therefore $L = \{2, 4\}$. As $p \geq t$, TP sends L to both Charlie and Donald.

C. Phase III

Charlie computes $k^{-1} = 2^{-1} \mod 5 = 3$ and as $L = \{2, 4\}$ the desired intersection $C \cap D = \{2.3 \mod 5, 4.3 \mod 5\} = \{1, 2\}$. In a similar way Donald computes the intersection as $C \cap D = \{1, 2\}$.

REFERENCES

[1] M. Furuhata, M. Dessouky, O. Fernando, M.-E. Brunet, X. Wang, and S. Koenig, "Ridesharing: The state-of-the-art and future directions," *Transportation Research Part B: Methodological*, vol. 57, pp. 28–46, 2013.

[2] A. B. Sherif, K. Rabieh, M. M. Mahmoud, and X. Liang, "Privacy-preserving ride sharing scheme for autonomous vehicles in big data era," *IEEE Internet of Things Journal*, vol. 4, no. 2, pp. 611–618, 2016.

[3] X. Wang, Z. Ning, M. Zhou, X. Hu, L. Wang, Y. Zhang, F. R. Yu, and B. Hu, "Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1314–1345, 2018.

[4] Y. He, J. Ni, X. Wang, B. Niu, F. Li, and X. Shen, "Privacy-preserving partner selection for ride-sharing services," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 5994–6005, 2018.

[5] Y. Luo, X. Jia, S. Fu, and M. Xu, "pride: Privacy-preserving ride matching over road networks for online ride-hailing service," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1791–1802, 2018.

[6] X. Shen, L. Wang, Q. Pei, Y. Liu, and M. Li, "Location privacy-preserving in online taxi-hailing services," *Peer-to-Peer Networking and Applications*, vol. 14, no. 1, pp. 69–81, 2021.

[7] H. Xie, Y. Guo, and X. Jia, "A privacy-preserving online ride-hailing system without involving a third trusted server," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3068–3081, 2021.

[8] S. Ghosh and M. Simkin, "The communication complexity of threshold private set intersection," in *Annual International Cryptology Conference*. Springer, 2019, pp. 3–29.

[9] R. A. Mahdavi, T. Humphries, B. Kacsmar, S. Krastnikov, N. Lukas, J. A. Premkumar, M. Shafieinejad, S. Oya, F. Kerschbaum, and E.-O. Blass, "Practical over-threshold multi-party private set intersection," in *Annual Computer Security Applications Conference*, 2020, pp. 772–783.

[10] S. Badrinarayanan, P. Miao, S. Raghuraman, and P. Rindal, "Multi-party threshold private set intersection with sublinear communication," in *IACR International Conference on Public-Key Cryptography*. Springer, 2021, pp. 349–379.

[11] L. Kissner and D. Song, "Private and threshold set-intersection," CARNEGIE-MELLON UNIV PITTSBURGH PA DEPT OF COMPUTER SCIENCE, Tech. Rep., 2004.

[12] A. Bay, Z. Erkin, J.-H. Hoepman, S. Samardjiska, and J. Vos, "Practical multi-party private set intersection protocols," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1–15, 2021.

[13] A. Jeppsson, "Implementing two threshold private set intersection protocols based on homomorphic encryption," 2021.

[14] Y. Zhao and S. S. M. Chow, "Can you find the one for me? privacy-preserving matchmaking via threshold psi," Cryptology ePrint Archive, Report 2018/184, 2018, https://ia.cr/2018/184.

[15] Y. He, J. Ni, X. Wang, B. Niu, F. Li, and X. Shen, "Privacy-preserving partner selection for ride-sharing services," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 5994–6005, 2018.

[16] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[17] R.-h. Shi, Y. Mu, H. Zhong, and S. Zhang, "Quantum oblivious set-member decision protocol," *Physical Review A*, vol. 92, no. 2, p. 022309, 2015.

[18] R.-H. Shi and M. Zhang, "A feasible quantum protocol for private set intersection cardinality," *IEEE Access*, vol. 7, pp. 72 105–72 112, 2019.

[19] R.-h. Shi, Y. Mu, H. Zhong, J. Cui, and S. Zhang, "An efficient quantum scheme for private set intersection," *Quantum Information Processing*, vol. 15, no. 1, pp. 363–371, 2016.

[20] R.-H. Shi, "Quantum multiparty privacy set intersection cardinality," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 4, pp. 1203–1207, 2020.

[21] R.-H. Shi and Y.-F. Li, "Quantum private set intersection cardinality protocol with application to privacy-preserving condition query," *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2022.

[22] W. Liu and H.-W. Yin, "A novel quantum protocol for private set intersection," *International Journal of Theoretical Physics*, vol. 60, no. 6, pp. 2074–2083, 2021.

[23] W.-J. Liu, W.-B. Li, and H.-B. Wang, "An improved quantum private set intersection protocol based on hadamard gates," *International Journal of Theoretical Physics*, vol. 61, no. 3, pp. 1–11, 2022.

[24] B. Liu, M. Zhang, and R. Shi, "Quantum secure multi-party private set intersection cardinality," *International Journal of Theoretical Physics*, vol. 59, no. 7, pp. 1992–2007, 2020.

[25] S. K. Debnath, K. Dey, N. Kundu, and T. Choudhury, "Feasible private set intersection in quantum domain," *Quantum Information Processing*, vol. 20, no. 1, pp. 1–11, 2021.

[26] A. A. Jolfaei, H. Mala, and M. Zarezadeh, "Eo-psi-ca: Efficient outsourced private set intersection cardinality," *Journal of Information Security and Applications*, vol. 65, p. 102996, 2022.

[27] X. Cheng, R. Guo, and Y. Chen, "Cryptanalysis and improvement of a quantum private set intersection protocol," *Quantum Information Processing*, vol. 16, no. 2, pp. 1–8, 2017.

[28] A. Maitra, "Quantum secure two-party computation for set intersection with rational players," *Quantum Information Processing*, vol. 17, no. 8, pp. 1–21, 2018.

[29] Y. Zhang, R. H. Deng, D. Zheng, J. Li, P. Wu, and J. Cao, "Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial iot," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 9, pp. 5099–5108, 2019.

[30] J. Sun, Y. Su, J. Qin, J. Hu, and J. Ma, "Outsourced decentralized multi-authority attribute based signature and its application in iot," *IEEE Transactions on Cloud Computing*, vol. 9, no. 3, pp. 1195–1209, 2019.

[31] K. Sowjanya, M. Dasgupta, and S. Ray, "A lightweight key management scheme for key-escrow-free ecc-based cp-abe for iot healthcare systems," *Journal of Systems Architecture*, vol. 117, p. 102108, 2021.

[32] J. Zhang, W. Bai, and Y. Wang, "Non-interactive id-based proxy re-signature scheme for iot based on mobile edge computing," *IEEE Access*, vol. 7, pp. 37 865–37 875, 2019.

[33] R. Cheng, K. Wu, Y. Su, W. Li, W. Cui, and J. Tong, "An efficient ecc-based cp-abe scheme for power iot," *Processes*, vol. 9, no. 7, p. 1176, 2021.

[34] Y. Yu, L. Guo, S. Liu, J. Zheng, and H. Wang, "Privacy protection scheme based on cp-abe in crowdsourcing-iot for smart ocean," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10 061–10 071, 2020.

[35] S. Das and S. Namasudra, "Multi-authority cp-abe-based access control model for iot-enabled healthcare infrastructure," *IEEE Transactions on Industrial Informatics*, 2022.

[36] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182–8201, 2019.

[37] T. M. Fernandez-Carames, "From pre-quantum to post-quantum iot security: A survey on quantum-resistant cryptosystems for the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457–6480, 2019.

[38] P. Murali, D. M. Debroy, K. R. Brown, and M. Martonosi, "Toward systematic architectural design of near-term trapped ion quantum computers," *Communications of the ACM*, vol. 65, no. 3, pp. 101–109, 2022.

[39] V. Hassija, V. Chamola, V. Saxena, V. Chanana, P. Parashari, S. Mumtaz, and M. Guizani, "Present landscape of quantum computing," *IET Quantum Communication*, vol. 1, no. 2, pp. 42–48, 2020.

[40] S. Ebrahimi, S. Bayat-Sarmadi, and H. Mosanaei-Boorani, "Post-quantum cryptoprocessors optimized for edge and resource-constrained devices in iot," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5500–5507, 2019.

[41] D. Xu, X. Wang, Y. Hao, Z. Zhang, Q. Hao, H. Jia, H. Dong, and L. Zhang, "Ring-explwe: A high-performance and lightweight post-quantum encryption scheme for resource-constrained iot devices," *IEEE Internet of Things Journal*, vol. 9, no. 23, pp. 24 122–24 134, 2022.

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

[43] C. Zhang, Y. Long, Z. Sun, Q. Li, and Q. Huang, "Three-party quantum private computation of cardinalities of set intersection and union based on ghz states," *Scientific Reports*, vol. 10, no. 1, pp. 1–10, 2020.

[44] V. Scarani, A. Ac'in, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Phys. Rev. Lett.*, vol. 92, p. 057901, Feb 2004.

[45] E. Zhang, J. Chang, and Y. Li, "Efficient threshold private set intersection," *IEEE Access*, vol. 9, pp. 6560–6570, 2021.

[46] S. Zhao, M. Ma, X. Song, H. Jiang, Y. Yan, and Q. Xu, "Lightweight threshold private set intersection via oblivious transfer," in *International Conference on Wireless Algorithms, Systems, and Applications*. Springer, 2021, pp. 108–116.

[47] P. K. Roy, "Quantum logic gates."

[48] P. Hallgren, C. Orlandi, and A. Sabelfeld, "PrivatePool: Privacy-Preserving Ridesharing," in *IEEE 30th Computer Security Foundations Symposium (CSF)*, 2017, pp. 276–291.

[49] S. Ghosh and T. Nilges, "An algebraic approach to maliciously secure private set intersection," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2019, pp. 154–185.

[50] E. Zhang, J. Chang, and Y. Li, "Efficient threshold private set intersection," *IEEE Access*, vol. 9, pp. 6560–6570, 2021.

[51] Y. Cao, Y.-H. Li, K.-X. Yang, Y.-F. Jiang, S.-L. Li, X.-L. Hu, M. Abulizi, C.-L. Li, W. Zhang, Q.-C. Sun, and et al., "Long-distance free-space measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 125, no. 26, Dec 2020.

[52] A. L. Migdall, E. Meyer-Scott, C. Silberhorn *et al.*, "Single-photon sources: Approaching the ideal through multiplexing," 2020.

Tapaswini Mohanty is currently working as "a Ph.D. student at the Department of Mathematics, National Institute of Technology, Jamshedpur, India. She completed her Master's degree from the Institute of Science, Banaras Hindu University, India, in 2019. Her research interests include Quantum Cryptography, and Private Set Operations."

Vikas Srivastava is working as "a research scholar in the Department of Mathematics, National Institute of Technology, Jamshedpur, India. He has completed his BS-MS dual degree in Mathematics from Indian Institute of Science Education and Research (IISER), Mohali, India in 2017. His research interests include cryptography, network security and blockchain technology."

Sumit Kumar Debnath received "an M.Sc. degree in Mathematics from IIT Kharagpur in 2012, and also a Ph.D. degree in Cryptology and Network Security from the Department of Mathematics, IIT Kharagpur in 2017. He is currently an Assistant Professor at the Department of Mathematics, National Institute of Technology, Jamshedpur, India. He is a life member of the Cryptology Research Society of India (CRSI). His research interests include multivariate cryptography, lattice-based cryptography, network security and blockchain. He has published more than 27 papers in international journals and conferences in his research areas."

Ashok Kumar Das (Senior Member, IEEE) received "a Ph.D. degree in computer science and engineering, an M.Tech. degree in computer science and data processing, and an M.Sc. degree in mathematics from IIT Kharagpur, India. He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, IIIT, Hyderabad, India. He also worked as a visiting faculty with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA 23435, USA. His current research interests include cryptography, system and network security including security in smart grid, Internet of Things (IoT), Internet of Drones (IoD), Internet of Vehicles (IoV), Cyber-Physical Systems (CPS) and cloud computing, intrusion detection, blockchain and AI/ML security. He has authored over 330 papers in international journals and conferences in the above areas, including over 280 reputed journal papers. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He has been listed in the Web of Science (Clarivate$^{\text{TM}}$) Highly Cited Researcher 2022 in recognition of his exceptional research performance. He is serving or has served on the editorial board of IEEE Systems Journal, Journal of Network and Computer Applications (Elsevier), Computer Communications (Elsevier), Journal of Cloud Computing (Springer), Cyber Security and Applications, IET Communications, KSII Transactions on Internet and Information Systems, and International Journal of Internet Technology and Secured Transactions (Inderscience), and has served as a Program Committee Member in many international conferences. He also served as one of the Technical Program Committee Chairs of the first International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, June 2019, and second International Congress on Blockchain and Applications (BLOCKCHAIN'20), L'Aquila, Italy, October 2020. His Google scholar citations include over 15,000 citations with h-index: 73 and i10-index: 207."

Biplab Sikdar (Senior Member, IEEE) received "the B.Tech. degree in electronics and communication engineering from North Eastern Hill University, Shillong, India, in 1996, the M.Tech. degree in electrical engineering from the Indian Institute of Technology, Kanpur, India, in 1998, and the Ph.D. degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. He is an Associate Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore, where he serves as the Vice Dean with the Faculty of Engineering. He was an Assistant Professor from 2001 to 2007 and an Associate Professor from 2007 to 2013 with the Department of Electrical, Computer, and Systems Engineering, Rensselaer Polytechnic Institute from 2001 to 2013. His research interests include IoT and cyber–physical system security, network security, and network performance evaluation. Dr. Sikdar was served as an Associate Editor for the IEEE Transactions on Communications from 2007 to 2012 and an Associate Editor for the IEEE Transactions on Mobile Computing from 2014 to 2017. He is a member of Eta Kappa Nu and Tau Beta Pi."