Quantum Private Membership Aggregation

Alptug Aytekin Mohamed Nomeir Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
aaytekin@umd.edu *mnomeir@umd.edu* *ulukus@umd.edu*

***Abstract*—We consider the problem of private set membership aggregation of N parties by using an entangled quantum state. In this setting, the N parties, which share an entangled state, aim to *privately* know the number of times each element (message) is repeated among the N parties, with respect to a universal set $\mathcal{K}$. This problem has applications in private comparison, ranking, voting, etc. We propose an encoding algorithm that maps the classical information into distinguishable quantum states, along with a decoding algorithm that exploits the distinguishability of the mapped states. The proposed scheme can also be used to calculate the N party private summation modulo P.**

I. Introduction

Seemingly superior computational powers of quantum computers pose a threat to classical security and privacy algorithms as shown in [1]. One way to combat this prevailing threat is to design quantum algorithms. Ever since the first quantum key distribution protocol of [2], quantum cryptography, a field which uses quantum mechanics to carry out classical cryptographic tasks, has become a very active research area. A few of the many important sub-fields of quantum cryptography are quantum key distribution, quantum secret sharing, and quantum multiparty computation.

As a specific problem in quantum multiparty computation, we consider the problem of quantum private membership aggregation (QPMA). In this problem, there are N parties, each of which having a subset of elements from a universal set. These parties wish to learn the frequency of the occurrence of each element in the universal set while hiding their own subsets from other parties as much as possible, i.e., even after having learned the frequency of all elements in the universal set, any guess about the subset possessed by any party should be equivalent to blind estimation. Further, the parties want to accomplish this in the presence of an eavesdropper which is wiretapping all the communication links. This problem has applications in many settings, such as confidence voting, ranking, and so on, which should ideally be carried out in anonymity for better results. To achieve their goals, parties select one of their own as the leader party which then computes the desired result by using a quantum algorithm. Fig. 1 shows the system model for this problem, with elements from the English alphabet and Party 0 acting as the leader party.

Classically, various versions of this problem have been studied: [3] introduced the private set intersection (PSI) problem, in which the parties want to learn the elements that exist in all parties, without leaking any further information about their own sets. [4] found the information-theoretic capacity of 2-party PSI; and [5] generalized the scheme to N-party PSI. [6] studied a similar problem, in which the parties want to learn whether a certain element occurs at least K times in the parties or not, called the K-PSI problem. [7] then extended the K-PSI problem based on the existing private information retrieval (PIR) schemes [8], [9] to carry out the aggregation privately. We note that a key difference between [7] and the current paper is that, in [7], the user wants to learn the frequency of a certain element without leaking the identity of the chosen element, whereas here, the goal is to find the frequency of all elements, that is, there is no privacy requirement on the element whose frequency is being checked. Further, in the current paper, each party possesses only one database as opposed to [7] where each party possesses multiple replicated databases.

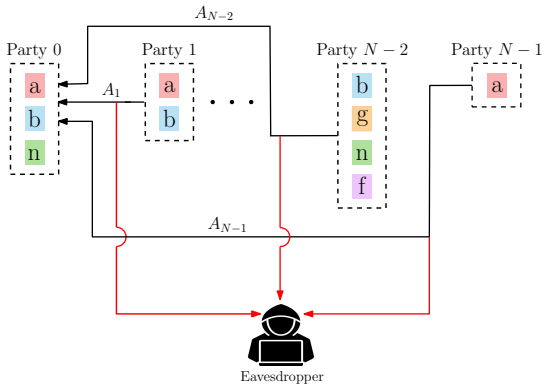

Fig. 1. N parties wish to aggregate membership of each element from a universal alphabet in their individual sets privately among themselves, and securely against an external eavesdropper, using an entangled quantum state.

Even though private quantum summation and aggregation schemes are common in the literature, to our knowledge, ours is the first paper to use an aggregation scheme on set membership function with N parties.[1] Further, it is the first in the way information is encoded and decoded. In [11]–[17], sequential-operating algorithms are used in which party i encodes its information on a set of quantum states, and sends the states to party $i+1$, until a leader party or a trusted third party which has initiated the scheme, compares the initial and the final sets to find the result. Of these, [13] is similar to our paper in using Sylvester clock matrix to encode the information. There are parallel-operating algorithms such as [18]–[23] that make use of quantum states to create a set of shared common randomness that adds up to 0, which masks

[1]We remark that even though [10] does not explicitly state their problem as a PMA problem, it computes the intersection and the union of two sets, which is exactly equivalent to PMA in the two-party case (i.e, $N=2$ case).

their announcement of membership function to the leader party, and then the leader party carries out the summation. What differentiates our scheme from these schemes in the literature is the fact it is a parallel-operating coding scheme that encodes the aggregation results to distinguishable quantum states and decodes thereafter, as opposed to creating "modulo-zero-sum randomness" as [18] calls it.

II. Preliminaries and Notation

Let $[n] \coloneqq \{0, \dots, n-1\}$. To indicate the powerset of a set $\mathcal{X}$, $2^{\mathcal{X}}$ is used. $\mathbf{1}[A]$ is used to denote the indicator function of the event A. e_i^D is used to denote the D-dimensional vector whose elements are all 0 except a 1 at the ith index. Whenever the dimensionality of this vector is clear from the context, the superscript is dropped for brevity. I_k denotes the identity matrix of size $k \times k$. $(A)_{ij}$ denotes the (i,j)th element of a matrix A. All logarithms are taken with respect to base 2.

Definition 1 (Partial trace operation) *Let $\{A_i\}_i \in \mathcal{V}_A$ and $\{B_i\}_i \in \mathcal{V}_B$. For the composite matrix $\sum_i A_i \otimes B_i \in \mathcal{V}_A \otimes \mathcal{V}_B$, partial trace operation with respect to a given subsystem is,*

$$tr_A\left(\sum_i A_i \otimes B_i\right) \coloneqq \sum_i tr(A_i) B_i, \tag{1}$$

$$tr_B\left(\sum_i A_i blue \otimes B_i\right) \coloneqq \sum_i tr A_i tr(B_i). \tag{2}$$

The following definitions follow from [24].

Definition 2 (Density matrices) *Density matrix of the quantum system A which is in the state $|\psi_j\rangle$ with probability p_j,*

$$\rho_A \coloneqq \sum_j p_j |\psi_j\rangle \langle\psi_j|, \tag{3}$$

where $p_j \geq 0$, $\sum_j p_j = 1$.

We note here that when $p_j = 1$ for some j, the density matrix reduces to $\rho = |\psi_j\rangle \langle\psi_j|$. This is known as a pure state. For brevity, in those cases, instead of ρ, $|\psi_j\rangle$ will be used to indicate it.

Definition 3 (Von Neumann entropy) *For a density matrix ρ describing the system A, Von Neumann entropy is,*

$$S(\rho) = S(A) \coloneqq -tr(\rho \log \rho) = H(\Lambda), \tag{4}$$

where $tr(\cdot)$ is the trace operator, Λ is the set of the eigenvalues of ρ, and $H(\cdot)$ is the Shannon entropy.

Definition 4 (Quantum conditional entropy) *The conditional entropy of a quantum system A with respect to a quantum system B is,*

$$S(A|B) \coloneqq S(A,B) - S(B). \tag{5}$$

Definition 5 (Quantum mutual information) *The quantum mutual information between two quantum systems A, B is,*

$$S(A;B) \coloneqq S(A) + S(B) - S(A,B) \tag{6}$$

$$= S(A) - S(A|B). \tag{7}$$

Definition 6 (Quantum operation) *A quantum operation ε is a linear, completely-positive map of density matrices.*

Finally, we use the following simple lemmas that are stated without proofs.

Lemma 1 *Let A and B share a quantum system ρ. If $\rho = \rho_A \otimes \rho_B$, where $\rho_i = tr_j(\rho)$, then, $S(A;B) = 0$.*

Lemma 2 *Let $\varepsilon(\rho) \coloneqq U\rho U^\dagger$, where U is a unitary matrix. Then, ε is a linear completely positive trace-preserving, CPTP, map.*

Let $\mathcal{H}$ be a d-dimensional Hilbert space. Let $\{|i\rangle\}_0^{d-1}$ be a basis for it. Let $\omega_d \coloneqq e^{\sqrt{-1}\frac{2\pi}{d}}$. Then, let $\mathsf{Z}_d \coloneqq \sum_{k=0}^{d-1} \omega_d^k |k\rangle \langle k|$. This is known as the Sylvester clock matrix [25]. Similarly, when the dimensionality is to be understood from the context, the subscript will be dropped on Z_d and ω_d.

A projective-valued measurement (PVM) consists of the set $\{P_i\}_i$ such that $P_i^2 = P_i$ and $\sum_i P_i = I_d$ where d is the dimension of the underlying Hilbert space $\mathcal{H}$. For a density matrix ρ, the result of the PVM $\{P_i\}_i$ is i with probability $tr(P_i\rho)$. For a pure state $\rho = |\xi\rangle \langle\xi|$, this is simply $\langle\xi| P_i |\xi\rangle$.

Lemma 3 *An orthonormal basis for the Hilbert space $\mathcal{H}$ constitutes a PVM.*

Similarly, a partial PVM is a PVM for a subsystem of $\mathcal{H}$, denoted by $\mathcal{H}_a$ with dimension d_a. That is, the partial PVM $\{P_{a,i}\}_i$ should satisfy $P_{a,i}^2 = P_{a,i}$ and $\sum_i P_{a,i} = I_{d_a}$.

III. Problem Formulation

In this problem, there is a universal set $\mathcal{K}$ with $|\mathcal{K}| = K$. There are N parties, each with a set $\mathcal{N}_i \subseteq \mathcal{K}$ for $0 \leq i \leq N-1$. We note that the probability distribution for realizations of $\mathcal{N}_i$ is not important for the achievable scheme.

Let $\mathbb{F}$ be a field. There exists a bijective map f from $\mathcal{K}$ to $[K]$. Define $g : 2^{[K]} \to \mathbb{F}^K : \mathcal{A} \mapsto \sum_{i=0}^{K-1} e_i \mathbf{1}[i \in \mathcal{A}]$. Notice that g is an injection. Thus, the composite map $g \circ f$ is an injection as well so that it is possible to find $\mathcal{N}_i$ from $(g \circ f)(\mathcal{N}_i)$. $(g \circ f)(\mathcal{N}_i)$ is commonly called the incidence vector of the subset $\mathcal{N}_i$ of $\mathcal{K}$. Let $E_{[N]}$ denote the N-tuple of incidence vectors of all parties.[2] The image of $g \circ f$ under a singleton is called the "set membership output." Each party stores its incidence vector $E_i \coloneqq (g \circ f)(\mathcal{N}_i)$ in one server.

Without loss of generality, any party can be chosen as the leading party. Let the leader be the Lth party, $0 \leq L \leq N-1$.

In this work, to have privacy/security against an eavesdropper, we allow that party i and the leader party share common randomness U_i prior to the initialization of the scheme. Since the common randomness is shared and the leader party does not previously know the incidence vector E_i, we have

$$I(E_i; U_i) = 0, \qquad i \in [N]. \tag{8}$$

[2]Here, N-tuple is used instead of the set to account for the possible repetitions.

Before the scheme starts, all parties share a quantum system ρ_0 in the composite Hilbert space $\otimes_{k=0}^{N-1}\mathcal{H}_k$. Here, $\mathcal{H}_k$ is the Hilbert space for the quantum system of the kth party. When the scheme starts, the ith party encodes its information using the mapping Enc_i and then shares its part of the quantum system with the leader party. The quantum system transmitted is called the answer of the ith party, denoted with A_i.

The answer of the ith party depends only on its randomness and its incidence vector, that is,

$$S(A_i|E_i, U_i) = 0. \tag{9}$$

After each party has sent their answers, the leader party will have $\rho_f = (Enc_1 \otimes \ldots \otimes Enc_N)(\rho_0)$. This quantum system will be denoted by $A_{[N]}$.

The leader party should be able to decode the frequency of occurrence of each element in $\mathcal{K}$ by combining the answers,

$$[\text{correctness}] \quad S\left(\sum_{i=1}^{N} E_i \Big| A_{[N]}\right) = 0. \tag{10}$$

This decoding is done by applying a Dec_L map to ρ_f.

All parties are considered to be semi-honest (i.e., honest but curious); all parties act according to the described scheme, yet they are curious to learn as much as possible from what they get. Privacy of the parties except the leader party require,

$$[\text{privacy}] \quad S(E_{[N]}; A_{[N]}, U_{[N]}) = I\left(E_{[N]}; \sum_{i=1}^{N} E_i\right), \tag{11}$$

so that the leader party should not be able to learn anything more specific about the incidence vectors than what it could infer after learning $\sum_{i=1}^{N} E_i$.

Moreover, if the quantum channel between party i and the leader party has been wiretapped by a passive eavesdropper, no information about the incidence vectors should leak, i.e.,

$$[\text{security}] \quad S(E_i; A_i) = 0, 0 \leq i \leq N-1, i \neq L. \tag{12}$$

The download cost of the system is defined with respect to the leader party. From the leader's perspective, it will download $\log\left(\otimes_{k\in[N]\setminus\{L\}} \dim(\mathcal{H}_k)\right)$ qudits.

IV. Main Results

Theorem 1 *Let the optimal download cost of the quantum private membership aggregation (QPMA) problem be D^*. Then,*

$$D^* \leq (N-1)K \log P^*, \tag{13}$$

where N is the number of parties and P^* is the smallest prime number that is larger than N.

Remark 1 *It might seem that the dependence of the download cost in Theorem 1 on K is bad, but it should be noted that, at the end of the scheme, the frequency of occurrence of all elements in the set $\mathcal{K}$ is found. Thus, on average, per element in the set, the download cost is $(N-1)\log P^*$.*

V. Proposed Scheme

We first give the general scheme in Subsection V-A, and then present a representative example in Subsection V-B.

A. General Scheme

Let P be the smallest prime number that is at least equal to N. Let $\mathbb{F}_P := \mathbb{Z}/P\mathbb{Z} = \mathbb{Z}_P$ be the underlying field for the operations on classical information.

Let $\mathcal{H}$ be a P-dimensional Hilbert space with the $\{|i\rangle\}_0^{P-1}$ basis (a.k.a. computational or Z basis). Let $|\psi\rangle = \frac{1}{\sqrt{P}}\sum_{k=0}^{P-1} \underbrace{|k\ldots k\rangle}_{N \text{ times}}$, and $|\phi_m\rangle = \frac{1}{\sqrt{P}}\sum_{k=0}^{P-1} \omega_P^{mk} \underbrace{|k\ldots k\rangle}_{N \text{ times}}$, where mk is the multiplication in $\mathbb{F}_P$, $m \in \mathbb{F}_p$. Also notice that $|\psi\rangle = |\phi_0\rangle$.

Let $|\psi\rangle^{\otimes K} = \underbrace{|\psi\rangle \otimes \ldots \otimes |\psi\rangle}_{K \text{ times}}$. The lth party has the qudits at $(l+mN)$th locations where $m \in [K]$. That is, to aggregate the occurrence of $x \in \mathcal{K}$, the parties share an entangled state $|\psi\rangle$ with the lth party having the lth qudit, for all $x \in \mathcal{K}$.

The lth party shares U_i which is uniformly distributed in $\mathbb{F}_P^K$ with the leader. The encoding of the incidence vector to qudits is done by applying the Sylvester clock matrix Z_P, also known as phase operation. The final state after encoding is,

$$|\psi_e\rangle = \otimes_{l=0}^{K-1}(\otimes_{k=0}^{N-1}(\mathsf{Z}^{(U_k+E_k)_l}))\,|\psi\rangle^{\otimes K} \tag{14}$$

$$= (\otimes_{k=0}^{N-1}\mathsf{Z}^{(U_k+E_k)_0})\,|\psi\rangle \otimes \ldots \otimes (\otimes_{k=0}^{N-1}\mathsf{Z}^{(U_k+E_k)_{K-1}})\,|\psi\rangle \tag{15}$$

Remark 2 *In the encoding stage, since the leader party does not send anything to itself, there is no need to be concerned with the eavesdropper. Thus, the leader party does not apply any shared randomness in its encoding. Moreover, since technically the leader party already knows its set membership results, it does not have to do any encoding at all.*

After this encoding is done, the parties send their quantum systems to the leader party. Then, the leader uses the shared randomness information and does the following,

$$|\psi_f\rangle = \otimes_{l=0}^{K-1}(\otimes_{k=0}^{N-1}(\mathsf{Z}^{-(U_k)_l}))\,|\psi_e\rangle \tag{16}$$

$$= (\otimes_{k=0}^{N-1}\mathsf{Z}^{(E_k)_0})\,|\psi\rangle \otimes \ldots \otimes (\otimes_{k=0}^{N-1}\mathsf{Z}^{(E_k)_{K-1}})\,|\psi\rangle \tag{17}$$

Looking at (17), the final state $|\psi_f\rangle$ is effectively separated into K parts each with N qudits. These parts can then be dealt with individually as they form a tensor product state. The motivation of how the individuals parts do not contain any information about each other can be seen from Lemma 1. To decode the information, the leader applies a partial PVM to N qudits to utilize the K-separation of $|\psi_f\rangle$ mentioned above. The requirement for the PVM set is that it should include $|\phi_m\rangle\langle\phi_m|$ for $m \in [N]$. The output of partial PVM at the lth location of K-separation then gives the membership aggregation result of the element in $\mathcal{K}$ corresponding to l. If the measurement gives $|\phi_m\rangle$, then the aggregation result is m, whereas if any other output is read, it indicates at least one party is Byzantine. As shown in the scheme, the download cost from each party is $K \log P$. Thus, the leader downloads

from $(N-1)$ parties, so that the download cost of the scheme is $(N-1)K\log P$ as stated in Theorem 1.

Remark 3 *The $\log P$ in the download cost appears since a logarithm with base 2 is being used. The leader party in fact downloads $(N-1)K$ qudits. Thus, one might have actually suggested using $(N-1)K$ as the download cost. However, by using the logarithm with a fixed base, we see that the low download cost will also have to induce a lower field size on $\mathbb{F}_P$, which is a merit since realizing qudits in increasing field sizes can be tricky.*

B. Representative Example

Let there be $N=3$ parties, with the universal alphabet $\mathcal{K}=\{a,b,c,d\}$. Let the 0th, 1st and 2nd parties have the sets $\mathcal{N}_0=\{a,c\}$, $\mathcal{N}_1=\{a,b,c\}$ and $\mathcal{N}_2=\{c\}$, respectively. Then, the incidence vectors are $E_0=(1,0,1,0)$, $E_1=(1,1,1,0)$, and $E_2=(0,0,1,0)$.

Then, choose $P=3=N$. Thus, a 3-dimensional Hilbert space $\mathcal{H}$ with basis $\{|0\rangle,|1\rangle,|2\rangle\}$. Thus, $\omega_3=e^{\sqrt{-1}\frac{2\pi}{3}}$ and the clock operation is $\mathsf{Z}=|0\rangle\langle 0|+\omega|0\rangle\langle 0|+\omega^2|0\rangle\langle 0|$. Then, each $|\phi_m\rangle$, $m\in[3]$, can be written as

$$|\phi_0\rangle=\frac{1}{\sqrt{3}}\left(|000\rangle+|111\rangle+|222\rangle\right), \tag{18}$$

$$|\phi_1\rangle=\frac{1}{\sqrt{3}}\left(|000\rangle+\omega|111\rangle+\omega^2|222\rangle\right), \tag{19}$$

$$|\phi_2\rangle=\frac{1}{\sqrt{3}}\left(|000\rangle+\omega^2|111\rangle+\omega^4|222\rangle\right). \tag{20}$$

The shared quantum state of the parties is then given by $|\phi_0\rangle\otimes|\phi_0\rangle\otimes|\phi_0\rangle\otimes|\phi_0\rangle$, i.e., a $|\phi_0\rangle$ state for each element of $\mathcal{K}$. As stated, any arbitrary party can be chosen as the leader, thus without loss of generality, let $L=1$. For security against the eavesdropper, parties 0 and 2 will each share a random vector with the leader party. Thus, party 0 will share $U_0=(U_{00},U_{01},U_{02},U_{03})\in\mathbb{F}_3^4$ and party 2 will share $U_2=(U_{20},U_{21},U_{22},U_{23})\in\mathbb{F}_3^4$ with the leader, prior to the initialization of encoding and after the selection of the leader.

Then, encoding will start. Per Remark 2, leader does not have to do any encoding operation as it already knows its own incidence vector, but for the sake of the argument, let us consider that it does and as mentioned in Remark 2, will not use shared randomness in the encoding stage.

For $a\in\mathcal{K}$, the encoding is given by the operation $\mathsf{Z}^{U_{00}+1}\otimes\mathsf{Z}\otimes\mathsf{Z}^{U_{20}}$. Applying this operation to $|\phi_0\rangle$ gives the result

$$\begin{aligned}&\left(\mathsf{Z}^{U_{00}+1}\otimes\mathsf{Z}\otimes\mathsf{Z}^{U_{20}}\right)|\phi_0\rangle\\&=\frac{1}{\sqrt{3}}(|000\rangle+\omega^{2+U_{00}+U_{20}}|111\rangle+\omega^{4+2U_{00}+2U_{20}}|222\rangle),\\&=|\phi_{2+U_{00}+U_{20}}\rangle.\end{aligned} \tag{21}$$

Similar analysis can be carried out for other elements in $\mathcal{K}$. After the encoding stage is done by each party, the final encoded shared quantum state is given by,

$$\begin{aligned}|\psi_e\rangle=&|\phi_{2+U_{00}+U_{20}}\rangle\otimes|\phi_{1+U_{01}+U_{21}}\rangle\otimes\\&|\phi_{3+U_{02}+U_{22}}\rangle\otimes|\phi_{U_{03}+U_{23}}\rangle.\end{aligned} \tag{22}$$

Afterwards, parties 0 and 2 send their shares of qudits to party 1 for decoding. Using the shared randomness, the leader applies (16) and obtains,

$$|\psi_f\rangle=|\phi_2\rangle\otimes|\phi_1\rangle\otimes|\phi_0\rangle\otimes|\phi_0\rangle, \tag{23}$$

since $3=0$ in $\mathbb{F}_3$. Then, the leader party applies a partial PVM which includes $|\phi_0\rangle,|\phi_1\rangle,|\phi_2\rangle$ states to each 3 qudit parts of the tensor product in (23). The measurement results will give 2 for a, 1 for b, 0 for c, and 0 for d. However, since the leader already knows it has $c\in E_1$, it can then infer that c is in fact present in every party's subset.

VI. Proofs

Lemma 4 *The proposed scheme is secure against an eavesdropper.*

Proof: Note that the kth party does the Z operation on one of its shared lth qudit $(U_k+E_k)_l$ times. Using one-time pad theorem [26], we see that $(E_k)_l$ is secure against a party that does not know $(U_k)_l$. Since this is correct $\forall l\in[K]$, $\forall k\in[N]$, the scheme is secure against an eavesdropper. ■

Lemma 5 *It is possible to construct a partial PVM using $|\phi_m\rangle=\frac{1}{\sqrt{P}}\sum_{k=0}^{P-1}\omega_P^{mk}\underbrace{|k\dots k\rangle}_{N\text{ times}}$ states.*

Proof: First, note that,

$$\langle\phi_m|\phi_n\rangle=\frac{1}{N}\sum_{k=0}^{P-1}\sum_{l=0}^{P-1}\omega_P^{-mk}\omega_P^{nl}\langle k\dots k|l\dots l\rangle \tag{24}$$

$$=\frac{1}{N}\sum_{k=0}^{P-1}\sum_{l=0}^{P-1}\omega_P^{nl-mk}\delta_{k,l} \tag{25}$$

$$=\frac{1}{N}\sum_{k=0}^{P-1}\omega_P^{(n-m)k} \tag{26}$$

$$=\delta_{n,m} \tag{27}$$

Notice that $\underbrace{|k\dots k\rangle}_{N\text{ times}}$ is P^N dimensional vector. Hence, it commits a basis of P^N vectors. Since $N\geq 1,\ P\geq N$, we have $P^N\geq N-1$. Thus, using $|\phi_m\rangle$ with $m\in[N]$, the leader party can always construct an orthonormal basis including these states, possibly using a procedure such as Gram-Schmidt.

Then, using that orthonormal basis and invoking Lemma 3, the leader can construct a PVM $\{P_i\}_i$ for a P^N dimensional Hilbert space. Then, this PVM can be used to construct the partial PVM $\{P_i\otimes\underbrace{I_P\otimes\dots\otimes I_P}_{N-1\text{ times}}\}_i$.

This process can then be used similarly to construct a partial PVM for the other N-qudit parts of the K-separation mentioned in Section V. ■

Remark 4 *From* (27) *and the superposition coefficients of $|\phi_m\rangle$ states in computational basis, it can be observed that*

$|\phi_m\rangle$ states are N-qudit Fourier states for the P-dimensional subspace of $\mathcal{H}^{\otimes N}$.

Lemma 6 *The proposed scheme satisfies the privacy criterion.*

Proof: Note that,

$$\omega_P^k \underbrace{|k\dots k\rangle}_{N \text{ times}} = (\mathsf{Z} \otimes \underbrace{I_P \otimes \dots I_P}_{N-1 \text{ times}}) \underbrace{|k\dots k\rangle}_{N \text{ times}} \tag{28}$$

$$= (I_P \otimes \mathsf{Z} \otimes \underbrace{I_P \otimes \dots I_P}_{N-2 \text{ times}}) \underbrace{|k\dots k\rangle}_{N \text{ times}} \tag{29}$$

$$= (\underbrace{I_P \otimes \dots \otimes I_P}_{l \text{ times}} \otimes \mathsf{Z} \otimes \underbrace{I_P \otimes \dots I_P}_{N-l-1 \text{ times}}) \underbrace{|k\dots k\rangle}_{N \text{ times}} \tag{30}$$

Thus, any linear combination of $\underbrace{|k\dots k\rangle}_{N \text{ times}}$ states will be blind to which party applied the Z operation.

Then, using the fact that $(A\otimes B) = (A\otimes I)(I\otimes B)$, we see that privacy is guaranteed no matter how many parties apply the Z operation.

From (30), we note that the posterior estimation of the leader party after the scheme about $(E_k)_l$ is,

$$P((E_k)_l = 1 | A_{[N]} = |\phi_m\rangle)$$

$$= \frac{P((E_k)_l = 1, A_{[N]} = |\phi_m\rangle)}{P(A_{[N]} = |\phi_m\rangle)} \tag{31}$$

$$= \frac{P((E_k)_l = 1, \sum_{i=0}^{N-1}(E_i)_l = m)}{P(\sum_{i=0}^{N-1}(E_i)_l = m)} \tag{32}$$

$$= P((E_k)_l = 1 | \sum_{i=0}^{N-1}(E_i)_l = m)), \tag{33}$$

as $|\phi_m\rangle$ can happen with any m parties having 1 at the lth index of their incidence vector. Thus, from the answers, the leader cannot learn anything more than what could be learnt from $\sum_{i=0}^{N-1} E_i$. Hence, the privacy constraint is satisfied. ■

Lemma 7 *The proposed scheme satisfies the correctness criterion.*

Proof: From (30) and the fact that $(A\otimes B) = (A\otimes I)(I\otimes B)$, if m parties apply the Z operation to their qudits,

$$(I_P \otimes \dots \otimes^{i(0)} \mathsf{Z} \otimes \dots \otimes^{i(m-1)} \mathsf{Z} \otimes I_P) \underbrace{|k\dots k\rangle}_{N \text{ times}}$$

$$= (\underbrace{I_p \dots \otimes I_P}_{k \text{ times}} \otimes \mathsf{Z}^m \otimes \underbrace{I_p \dots \otimes I_P}_{N-k-1 \text{ times}}) \underbrace{|k\dots k\rangle}_{N \text{ times}}, \tag{34}$$

where the left superscript indicates which party does the Z operation and $i : [m] \to [N]$ is an injection; see Remark 7. Then, we have,

$$(\mathsf{Z}^m \otimes \underbrace{I_P \otimes \dots \otimes I_P}_{N-1 \text{ times}}) |\psi\rangle = \frac{1}{\sqrt{P}} (\mathsf{Z}^m \otimes \underbrace{I_P \otimes \dots \otimes I_P}_{N-1 \text{ times}})$$

$$\times \sum_{n=0}^{P-1} \underbrace{|n\dots n\rangle}_{N \text{ times}} \tag{35}$$

$$= \frac{1}{\sqrt{P}} \sum_{n=0}^{P-1} \omega_P^{mn} \underbrace{|n\dots n\rangle}_{N \text{ times}} \tag{36}$$

$$= |\phi_m\rangle . \tag{37}$$

Thus, using the partial PVMs constructed in Lemma 5, the leader party can carry out partial measurements. If the result is one of the $|\phi_m\rangle$ states for $m \in [N]$, it means that m parties applied the Z operation, thus the membership aggregation result is m. However, as mentioned in Lemma 5, since there are at least N elements in that PVM, if anything other than a $|\phi_m\rangle$ has been measured, it indicates the existence of a Byzantine element in the system. ■

Remark 5 *We note here that although the scheme sometimes detects the Byzantine elements, it may fail to detect them as well. Moreover, even in the cases it detects them, it cannot correct them. Thus, the scheme is not Byzantine-proof.*

Remark 6 *If N is a prime number itself, then $P = N$ is a valid choice for the underlying field. However, note that, in that case, N parties applying the Z operation is equivalent to no parties applying it. Yet, the leader is able to differentiate between those cases based on its set membership result.*

Remark 7 *Equation* (34) *can actually be generalized. Let $f : [N] \to \mathbb{F}_p$ such that $\sum_{k\in[N]} f(k) = m$. Then,*

$$(\mathsf{Z}^{f(0)} \otimes \dots \otimes \mathsf{Z}^{f(N-1)}) \underbrace{|k\dots k\rangle}_{N \text{ times}}$$

$$= (\underbrace{I_p \dots \otimes I_P}_{k \text{ times}} \otimes \mathsf{Z}^m \otimes \underbrace{I_p \dots \otimes I_P}_{N-k-1 \text{ times}}) \underbrace{|k\dots k\rangle}_{N \text{ times}}, \tag{38}$$

Corollary 1 *Looking at Lemma 5 and Remark 7, if the partial PVMs include $|\phi_m\rangle$ for $m \in [P]$, the proposed scheme carries out quantum private summation modulo P.*

VII. Conclusions

We developed a private membership aggregation scheme using quantum states. The scheme provides privacy to the legitimate parties that participate in the scheme, and security against external eavesdroppers. Essentially, the proposed scheme is a quantum private summation modulo P scheme. The proposed scheme makes use of the phase operation to encode the information into specific N-qudit Fourier transform states, which then makes use of the fact that the Fourier transform is a unitary operation to construct an orthonormal measurement basis. However, one caveat of using such bases is the fact that the Fourier transform is only a unitary operation on a field, as it involves addition and multiplication. Thus far, the results in the literature lack other parallel-operating private quantum summation algorithms that carry out the private summation on ring or even group structures rather than relying on fields, which can be the point of a future study.

REFERENCES

[1] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *IEEE FOCS*, November 1994.

[2] C. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *IEEE ICCSSP*, 1984.

[3] B. Pinkas, T. Schneider, and M. Zohner. Faster private set intersection based on OT extension. In *USENIX Security Symposium*, August 2014.

[4] Z. Wang, K. Banawan, and S. Ulukus. Private set intersection: A multi-message symmetric private information retrieval perspective. *IEEE Transactions on Information Theory*, 68(3):2001–2019, March 2022.

[5] Z. Wang, K. Banawan, and S. Ulukus. Multi-party private set intersection: An information-theoretic approach. *IEEE Journal on Selected Areas in Information Theory*, 2(1):366–379, March 2021.

[6] A. Elkordy, Y. Ezzeldin., and S. Avestimehr. Federated K-private set intersection. In *ACM CIKM*, October 2022.

[7] M. Nomeir, S. Vithana, and S. Ulukus. Private membership aggregation. In *IEEE MILCOM*, December 2023.

[8] H. Sun and S. A. Jafar. The capacity of private information retrieval. *IEEE Transactions on Information Theory*, 63(7):4075–4088, July 2017.

[9] S. Ulukus, S. Avestimehr, M. Gastpar, S. A. Jafar, R. Tandon, and C. Tian. Private retrieval, computing, and learning: Recent progress and future challenges. *IEEE Journal on Selected Areas in Communications*, 40(3):729–748, March 2022.

[10] Y. Chen, H. Situ, Q. Huang, and C. Zhang. A novel quantum private set intersection scheme with a semi-honest third party. *Quantum Information Processing*, 22(12):429, December 2023.

[11] D. Ming-Yi. Multi-party quantum summation within a d-level quantum system. *International Journal of Theoretical Physics*, 59(5):1638–1643, March 2020.

[12] W. Liu, Y. Wang, and W. Fan. An novel protocol for the quantum secure multi-party summation based on two-particle Bell states. *International Journal of Theoretical Physics*, 56(9):2783–2791, September 2017.

[13] T. Ye and J. Hu. Quantum secure multiparty summation based on the phase shifting operation of d-level quantum system and its application. *International Journal of Theoretical Physics*, 60(3):819–827, March 2021.

[14] C. Zhang, Z. Sun, Y. Huang, and D. Long. High-capacity quantum summation with single photons in both polarization and spatial-mode degrees of freedom. *International Journal of Theoretical Physics*, 53(3):933–941, March 2014.

[15] S. Lv, X. Jiao, and P. Zhou. Multiparty quantum computation for summation and multiplication with mutually unbiased bases. *International Journal of Theoretical Physics*, 58(9), September 2019.

[16] R. Shi, Y. Mu, H. Zhong, J. Cui, and S. Zhang. Secure multiparty quantum computation for summation and multiplication. *Scientific Reports*, 6(1):19655, 2016.

[17] Z. Ji, H. Zhang, H. Wang, F. Wu, J. Jia, and W. Wu. Quantum protocols for secure multi-party summation. *Quantum Information Processing*, 18(168):1–19, June 2019.

[18] M. Hayashi and T. Koshiba. Verifiable quantum secure modulo summation. 2019. Available online at arXiv:1910.05976.

[19] K. Sutradhar. Secure multiparty quantum aggregating protocol. *Quantum Information and Computation*, 23(3-4):245–256, 2023.

[20] C. Zhang, H. Situ, Q. Huang, and P. Yang. Multi-party quantum summation without a trusted third party based on single particles. *International Journal of Quantum Information*, 15(2):1750010, January 2017.

[21] H. Yang and T. Ye. Secure multi-party quantum summation based on quantum Fourier transform. *Quantum Information Processing*, 17(6):129, June 2018.

[22] X. Chen, G. Xu, Y. Yang, and Q. Wen. An efficient protocol for the secure multi-party quantum summation. *International Journal of Theoretical Physics*, 49(11):2793–2804, November 2010.

[23] K. Sutradhar and H. Om. A generalized quantum protocol for secure multiparty summation. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 67(12):2978–2982, April 2020.

[24] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[25] J. Sylvester. Thoughts on inverse orthogonal matrices, simultaneous sign-successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 34(232):461–475, December 1867.

[26] C. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, October 1949.