Secure alignment of coordinate systems using quantum correlation

F. Rezazadeh,[1] A. Mani,[2,*] and V. Karimipour[1]
[1]*Department of Physics, Sharif University of Technology, P.O. Box 11155-9161, Tehran, Iran*
[2]*Department of Science Engineering, University of Tehran, Tehran, Iran*
(Received 5 April 2017; published 11 August 2017)

We show that two parties far apart can use shared entangled states and classical communication to align their coordinate systems with a very high fidelity. Moreover, compared with previous methods proposed for such a task, i.e., sending parallel or antiparallel pairs or groups of spin states, our method has the extra advantages of using single-qubit measurements and also being secure, so that third parties do not extract any information about the aligned coordinate system established between the two parties. The latter property is important in many other quantum information protocols in which measurements inevitably play a significant role.

DOI: 10.1103/PhysRevA.96.022310

I. INTRODUCTION

Almost any protocol in quantum communication between two or more parties requires measurements in bases which are agreed upon by the parties involved [1–4]. This in turn requires that they establish aligned reference frames between them with arbitrary precision. It has been realized that spatial direction is a type of information named "unspeakable quantum information" [5] which cannot be transmitted by sending classical bits unless the sender (Alice) and the receiver (Bob) have a common coordinate system. Instead, physical objects, e.g., photons, must be sent [6] to convey this information.

The problem of setting a reference frame between two separate parties can be reduced to the problem of sharing three mutually orthogonal directions. Some methods of direction sharing are based on transmission of spin states (qubits), followed by single or multiqubit measurements which are performed by the receiver [7–10]. For example, Gisin and Popescu investigate the case when many pairs of parallel or anti-parallel spins are transmitted from Alice to Bob and show that a higher fidelity is achieved when the two spins are antiparallel to each other [7]. In [7], the strategy of Bob for guessing the direction of spins sent to him is based on using a specific measurement of two-qubit entangled states. The inequivalence with the case of two parallel spins is justified by noting that there is no universal NOT machine which can turn any unknown pair of antiparallel spins into a pair of parallel spins. It is shown in [8] that in such a case, the average optimal fidelity of direction sharing is equal to $\frac{N+1}{N+2}$. This line of thought has been further pursued in [11], where it has been shown that for conveying the direction $\mathbf{n}$, Alice can encode it into a specific eigenstate of the operator $\mathbf{S}\cdot\mathbf{n}$ where $\mathbf{S}$ is the total spin operator and send it to Bob who will discern $\mathbf{n}$ with a collective measurement.

In another interesting approach, Alice and Bob find the unitary operation that rotates the (rigid) frame of Bob to align it with the (rigid) frame of Alice [12,13]. Thus in one go, the two frames are aligned. The method is based on sharing a $2N$-qubit highly entangled state upon which collective measurements are done by Bob after Alice has sent her N-qubit share to him. Clearly this method, while being optimal in a theoretical sense, is experimentally demanding.

In all these works and many other similar works [14–17] the question of secrecy of the directions has not been considered and for that reason the question of a possible role that shared entangled states can play for such a goal has not been discussed. In view of the role that any quantum communication protocol is based on measurements in aligned coordinate systems, it is natural to demand that such alignment be made in a secure and secret way so that only the legitimate parties know the directions and nobody else. To the best of our knowledge, there are only few works about the problem of security of reference frames, a notable example being [18] where Alice and Bob share a classical string of bits to achieve security.

In this paper we introduce a method for direction sharing which uses only bipartite entangled states and single-qubit measurements instead of multipartite entangled states and collective measurements. Moreover, no qubits are sent from one party to the other, and there is no need for sharing strings of classical bits to ascertain security. In our protocol N singlet states are shared between Alice and Bob and they do single-qubit measurements in their specific but private directions. Finally, they publicly announce the results of their measurements. From the correlations in these public data they can discern information about the relative angle between their directions of measurement and eventually align their coordinate systems in a precise way. Besides the secrecy in the common coordinate systems, our protocol has the advantage of using only single-qubit measurements, compared to multiqubit measurements proposed in other methods [18–22].

We should also mention Ref. [23], where similar ideas to those of the present paper are suggested and mutual information is used to align the two directions. There are, however, important differences between [23] and the present work. When the number of singlets is infinite, Bahder essentially tries to do an extensive (essentially continuous) search in order to find the direction which maximizes the mutual information. This certainly gives the aligned direction but is clearly infeasible for the experiment. In the same limit, we do the alignment by determining the angles of one axis of Alice by measuring the correlations with those of Bob who measures his qubits in three different directions. So we do not need an exhaustive search over the sphere. When the number of pairs is finite, Bahder only goes as far as to estimate the angle between two directions using a Bayesian approach similar to that of us. However, knowing only this angle, it is not evident around which axis the vectors should be rotated to be aligned.

*mani.azam@ut.ac.ir

 ©2017 American Physical Society

Moreover, the important point is that finite-N fluctuations of correlations need to be carefully taken into account to extract useful geometrical information from these correlations. This problem will be dealt with in this paper.

In a sense our work is the converse of what is done in quantum key distribution (QKD) [3,4], where Alice and Bob publicly announce their measurement bases but keep for themselves the results of measurements. Here they publicly announce their measurement results (the sequence of 0's and 1's or +'s and -'s), and from these public results they align their axes. In the same way as QKD is secure, this protocol is also secure in the sense that eavesdroppers cannot gain information about the aligned directions.

A special case of our method is when Alice and Bob already agree on a fixed direction, say the z direction, and they only want to align their x and y axes perpendicular to this axis. In this case, which we call the two-dimensional case, the protocol is simpler and can be done in just one step by estimating the angle between two directions and a complete alignment is achieved with a very high fidelity. In the general case where there is no *a priori* agreed direction or plane, two or three steps are needed, and again our method will lead to a very good estimate of the relative directions and hence alignment of coordinate systems. In both two- and three-dimensional cases, we first consider the ideal case where an infinite number of singlet states has been shared between Alice and Bob and then consider the realistic case where a finite number of N states has been shared, in which case we obtain the fidelity of the protocol as a function of the number of shared singlets N. We will see that with few shared singlets, very high fidelities can be obtained.

The paper is organized as follows: In Sec. II we show how correlations of measurements of singlet states by two parties can lead to an estimation of the angle between directions of measurements. This is explained in two subsections, first for the ideal case where the number of singlets N is infinite and then for the finite N case, where we use a Bayesian approach to calculate the probabilities [24]. In Sec. III, we consider the geometrical problem of estimating a vector or direction by such measurements, and we compare our fidelities with those of others. The paper ends with a Conclusion section containing a discussion about the security of the protocol.

II. USING ENTANGLED STATES TO ESTIMATE THE ANGLE BETWEEN TWO DIRECTIONS

Consider two parties, Alice and Bob, far apart from each other and sharing a number of singlet states

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \tag{1}$$

where $|0\rangle$ and $|1\rangle$ are the eigenvectors of $\vec{\sigma}\cdot\vec{z}$, and $\vec{\sigma}$ is the vector of Pauli matrices:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2}$$

To set up a shared direction in space, Alice and Bob use the correlations in their measurements to find how they should correct or rotate their axes of measurement. Alice and Bob measure their spins in two arbitrary directions known only to each of them separately. For example, Bob measures his spin in his supposedly **z** direction, and Alice measures her spins in a direction which in the coordinate system of Bob is denoted by **m** having an angle θ with **z**. The aim of the experiment is to make the best estimate for this angle from the measurement of correlations. To this end, one of the parties, say Alice, publicly announces her results in the form of a sequence $(a_1,a_2,\dots a_k,\dots)$, where $a_i = \pm 1$. Bob compares this sequence with his own results $[(b_1,b_2,\dots b_k,\dots), b_i = \pm 1]$ and calculates the correlations between these two sequences, which for N shared singlet pairs, is given by

$$q_N = \frac{1}{N}\sum_{i=1}^{N} a_i\overline{b_i}. \tag{3}$$

This correlation function can be rewritten as

$$\begin{aligned} q_N &= \frac{N_{+-} + N_{-+} - N_{++} - N_{--}}{N} \\ &= \frac{N_d - N_s}{N} = \frac{2N_d - N}{N}, \end{aligned} \tag{4}$$

where N_{ab} denotes the number of the times that Alice obtains a value of a and Bob obtains a value of b, and N_d and N_s are the number of times that Alice and Bob obtain different and the same results, respectively. It is evident that $-1 \leqslant Q \leqslant 1$. If **m** and **z** are either parallel or antiparallel, then the results will be fully correlated or fully anticorrelated and $|Q| = 1$. For perpendicular directions, Bob obtains a value very close to 0. From this correlation Bob can eventually determine the axis **m** of Alice in a three-step process. We will complete the idea in this section by first considering the ideal case in which an infinite number of singlet pairs are shared among Alice and Bob and then considering the case of an finite number of shared singlet pairs.

A. The case when an infinite number of pairs are shared

In this case we will have

$$Q_\infty = P_{+-} + P_{-+} - P_{++} - P_{--}, \tag{5}$$

where P_{ab} now denotes the probability of Alice obtaining a value of a and Bob obtaining a value of b. These probabilities are equal to

$$P_{+-} = |\langle m_+, z_-|\psi\rangle|^2, \tag{6}$$

with similar expressions for the other three terms. A simple calculation shows that

$$P_{+-} = P_{-+} = \frac{1}{2}\cos^2\frac{\theta}{2}, \quad P_{++} = P_{--} = \frac{1}{2}\sin^2\frac{\theta}{2}, \tag{7}$$

and from (5) we find

$$Q_\infty = \cos\theta. \tag{8}$$

If infinite singlet pairs were shared between Alice and Bob, then the value of Q_∞ does not show any fluctuation and Bob could find the exact value of the angle θ from (8). Therefore while Alice is measuring along the **m** direction, Bob can make measurements along his x, y, and z directions to determine the

Euler angles of $\mathbf{m}$ and hence completely determine the vector $\mathbf{m}$ in the form

$$\mathbf{m} = q_x\,\mathbf{x} + q_y\,\mathbf{y} + q_z\,\mathbf{z}. \tag{9}$$

If he has some prior knowledge about the vector $\mathbf{m}$ being either in the upper or lower hemisphere, then he can determine the vector $\mathbf{m}$ by only two sets of measurements in the form

$$\mathbf{m} = q_x\,\mathbf{x} + q_y\,\mathbf{y} \pm \sqrt{1 - q_x^2 - q_y^2}\,\mathbf{z}, \tag{10}$$

where the sign is determined by the aforementioned prior knowledge. In the realistic case where the number of singlets is finite, then the above two methods, which we label as methods A and B, respectively, differ in their fidelity versus resource (i.e., number of singlets) used. We will make a detailed comparison of the two methods in the sequel.

B. The case where a finite number of pairs are shared

In the realistic case where we have only a finite number N of singlets, the correlations will fluctuate around their mean values and we can estimate only the vector $\mathbf{m}$. As the number of pairs increases the fluctuations decay and the fidelity of our estimation also increase. To estimate the angle between two directions used by Alice and Bob from correlations of their quantum measurements, we use the standard estimation procedure based on Bayesian inference [24]. However, as in the ideal case, the rest of problem has a geometrical character and there are various methods for estimation of the final vector $\mathbf{m}$, and the final fidelity depends on our method of estimation. In any method used for estimation, the fidelity of the estimation between the original vector of Alice ($\mathbf{m}$) and the estimated vector $\mathbf{m}_e$ is given by

$$F(\mathbf{m}_e,\mathbf{m}) = \frac{(1 + \mathbf{m}\cdot\mathbf{m}_e)}{2}. \tag{11}$$

The average fidelity of this procedure is then given by

$$\overline{F_N} := \int d\mathbf{m} \int d\mathbf{m}_e\, P_N(\mathbf{m}_e|\mathbf{m}) \frac{(1 + \mathbf{m}\cdot\mathbf{m}_e)}{2}, \tag{12}$$

where $P_N(\mathbf{m}_e|\mathbf{m})$ is the conditional probability that the vector of Alice is $\mathbf{m}$ and it is estimated to be $\mathbf{m}_e$. Here $d\mathbf{m} = \frac{1}{4\pi} d\cos\theta\, d\phi$ with a similar expression for $d\mathbf{m}_e$.

We first consider estimation of the angle between one vector and $\mathbf{z}$ direction, say θ from measurement of correlations. Alice and Bob share N singlets where Bob is measuring his qubits in his $\mathbf{z}$ direction and Alice is measuring her qubits in a direction which appears as $\mathbf{m}$ in the coordinate system of Bob. The correlation in this case is a random variable Q_N which takes values q_N. In view of the relation (4) and (7), we have the conditional probability for the correlation to be q_N:

$$P(q_N|\mathbf{z},\mathbf{m}) = \binom{N}{N_d} \left(\cos^2\frac{\theta}{2}\right)^{N_d} \left(\sin^2\frac{\theta}{2}\right)^{N-N_d}. \tag{13}$$

Note that this probability depends only on the angle θ, so it can equally be written as $P(q_N|\theta)$. Moreover, it is easily seen from this binomial distribution that

$$\langle q_N\rangle = \cos\theta, \quad \langle q_N^2\rangle = \cos^2\theta + \frac{1}{N}\sin^2\theta, \tag{14}$$

facts which will be used later on.

Remarks on notation.

(i) Since we take the measurement axis of Bob to be fixed along the $\mathbf{z}$ direction, we sometimes omit $\mathbf{z}$ from the conditional probabilities when there is no risk of confusion.

(ii) As it is evident from (4), the correlation q_N has a one-to-one correspondence with N_d, e.g., the number of times where Alice and Bob obtain opposite results in their measurements. In the following summations we use these two instead of each other, i.e., summing over q from -1 to 1 is equivalent to summing over N_d from 0 to N.

The conditional probability that Alice has measured her spins along $\mathbf{m}$ given a specific value of correlation q_N is given by

$$P(\mathbf{m}|q_N) = \frac{P(q_N|\mathbf{m})P(\mathbf{m})}{P(q_N)} = \frac{P(q_N|\mathbf{m})P(\mathbf{m})}{\int d\mathbf{m}\; P(q_N|\mathbf{m})P(\mathbf{m})}, \tag{15}$$

where $P(\mathbf{m})$ is the probability that Alice has measured her spins in the direction $\mathbf{m}$ and in the absence of any preference, this probability is taken to be uniform. From (13) we obtain

$$\begin{aligned}\int d\mathbf{m} P(q_N|\mathbf{m}) &= \frac{1}{4\pi}\int d\phi d\cos\theta \binom{N}{N_d}\left(\cos^2\frac{\theta}{2}\right)^{N_d}\left(\sin^2\frac{\theta}{2}\right)^{N-N_d} \\ &= \frac{1}{N+1},\end{aligned} \tag{16}$$

where we have used the formula for the β function

$$\begin{aligned}B(x+1,y+1) &= \frac{x!y!}{(x+y+1)!} \\ &= \int d\theta \left(\cos\frac{\theta}{2}\right)^{2x+1}\left(\sin\frac{\theta}{2}\right)^{2y+1}.\end{aligned} \tag{17}$$

This leads to

$$P(\mathbf{m}|q_N) = \frac{(N+1)!}{N_d!(N-N_d)!}\left(\cos^2\frac{\theta}{2}\right)^{N_d}\left(\sin^2\frac{\theta}{2}\right)^{N-N_d}. \tag{18}$$

We now follow the standard estimation strategy and find the best estimate for $\mathbf{m}$ as

$$\mathbf{m}_e := \int \mathbf{m} P(\mathbf{m}|q_N) d\mathbf{m}, \tag{19}$$

or equivalently, by using $\mathbf{z}\cdot\mathbf{m} = \cos\theta$ and $\mathbf{z}\cdot\mathbf{m}_e = \cos\theta_e$,

$$\cos\theta_e := \int \cos\theta\, P(\mathbf{m}|q_N) d\mathbf{m}. \tag{20}$$

Using (18), a straightforward calculation now gives

$$\cos\theta_e = \frac{N}{N+2} q_N, \tag{21}$$

which goes to Eq. (8) for infinite N. This gives the estimated angle θ_e between $\mathbf{z}$ and $\mathbf{m}$.

III. ALIGNMENT OF COORDINATE SYSTEMS

The complete alignment of two coordinate systems is equivalent to the determination of the complete orientation

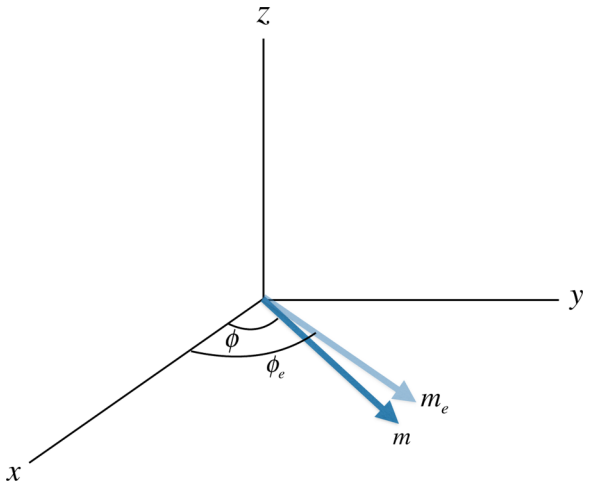

FIG. 1. Two-dimensional coordinate sharing scheme shown in the coordinate system of Bob: Alice and Bob agree on the **z** direction and they want to share the direction **m** which has been located in the x-y plane. Bob estimates the desired direction $\mathbf{m}_e$ due to the value of the correlation function.

of two orthogonal vectors of Alice in Bob coordinate system. Therefore this problem reduces to the determination of one single vector of Alice in Bob coordinate system. This part is purely geometrical, to which we now turn. To this end, we first study the case of two dimensions where Alice and Bob agree on a third direction (or a plane) and then go on to the full dimensional problem.

A. Two-dimensional coordinate systems

Here we assume that Alice and Bob agree on a third direction, say **z**, and their problem is to align two x-y coordinate systems in plane perpendicular to this direction, see Fig. 1.

The fidelity in this case is given by $F(\mathbf{m}_e,\mathbf{m}) = \frac{1+\cos(\phi-\phi_e)}{2}$, where ϕ and ϕ_e are respectively the actual and estimated angles of Alice vector with Bob x axis. Using (12) we find the average fidelity to be

$$\overline{F}_N = \frac{1}{\pi}\int_0^{\pi} d\phi \sum_{N_d=0}^{N} \binom{N}{N_d} \left(\cos^2\frac{\phi}{2}\right)^{N_d} \times \left(\sin^2\frac{\phi}{2}\right)^{N-N_d} \frac{1+\cos(\phi-\phi_e)}{2}, \tag{22}$$

and straightforward calculations by using the β function (17) give us

$$\overline{F}_N = \frac{1}{2} + \frac{N}{4(N+2)} + \frac{1}{\pi(N+1)} \times \sum_{N_d=0}^{N} \sqrt{1-\left(\frac{2N_d-N}{N+2}\right)^2}. \tag{23}$$

For large N, this leads to

$$\lim_{N\to\infty} \overline{F}_N = \frac{3}{4} + \frac{1}{\pi}\int_{q=-1}^{1} \sqrt{\left(\frac{1-q}{2}\right)\left(\frac{1+q}{2}\right)}dq = 1. \tag{24}$$

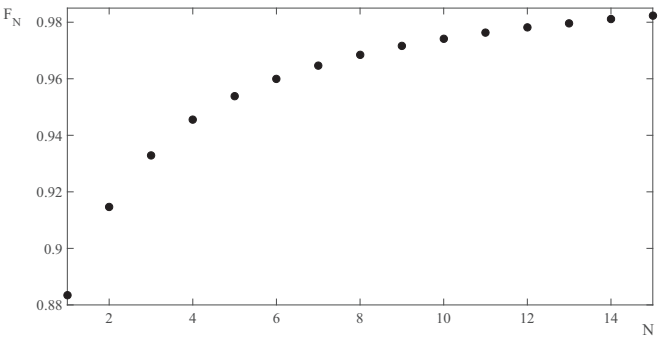

FIG. 2. The average fidelity for different values of N when the direction **m** which is estimated by Bob is located in a specific plane that he is aware of.

Figure 2 shows the behavior of fidelity for different values of shared singlet pairs N. As it can be seen in this figure, Alice and Bob can achieve the average fidelity around 0.9 by using only three singlet pairs.

B. Three-dimensional coordinate systems

We now come to the problem of aligning a full three-dimensional coordinate system. This reduces to the problem of sharing three aligned directions. Similar to the procedure expressed in the ideal case of Sec. II A, Alice and Bob may use $3N$ shared singlet pairs in method A, Eq. (9), or use $2N$ singlet pairs as in method B, Eq. (10). We explain in detail both methods and compare them with each other and also with the method of Massar and Popescu [8].

1. Method A: Using 3N singlets

Let $3N$ singlet pairs be shared between Alice and Bob and they want to share the original vector **m**, which in the coordinate system of Bob has the form

$$\mathbf{m} = \cos\alpha\ \mathbf{x} + \cos\beta\ \mathbf{y} + \cos\gamma\ \mathbf{z}, \tag{25}$$

as it is shown in Fig. 3. While Alice measures all her qubits along the **m** direction, Bob measures his qubits in the directions

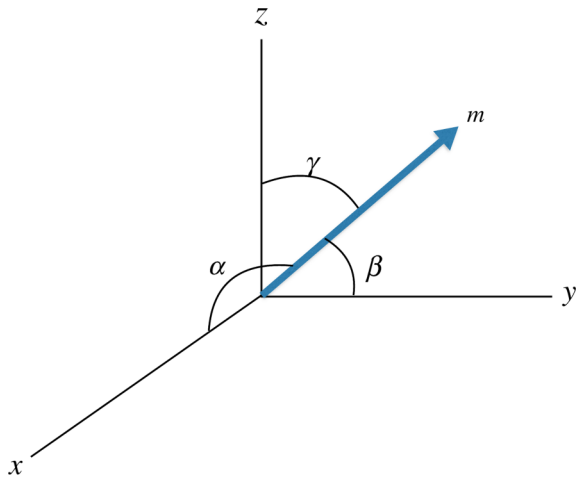

FIG. 3. Alice and Bob want to share the direction **m**, which in the coordinate system of Bob makes the angles α, β, and γ with x, y, and z axes, respectively.

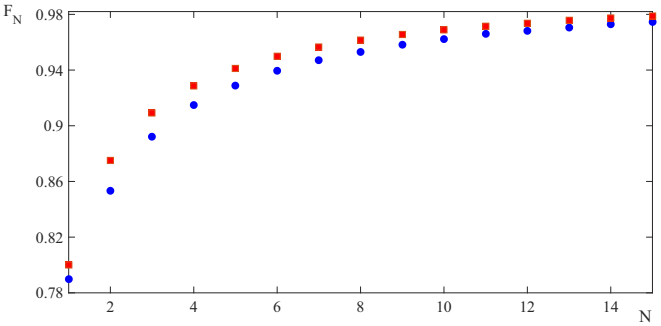

FIG. 4. The blue circles show the behavior of the average fidelity for different values of N when $3N$ singlet pairs are shared between Alice and Bob and they use method A of Sec. III B to share a direction. The upper red squares show the optimal fidelity $\frac{3N+1}{3N+2}$ which is achievable only by collective measurements [8]. We use $3N$ in the formula of optimal fidelity in order to have a comprehensive comparison.

$\mathbf{x}$, $\mathbf{y}$, and $\mathbf{z}$ (N qubits in each direction) and finds the respective correlations $q_{x,N}$, $q_{y,N}$, and $q_{z,N}$. Then by using Eqs. (9) and (21), he estimates $\mathbf{m}$ to be

$$\mathbf{m}_e = \frac{1}{\sqrt{q_x^2+q_y^2+q_z^2}}(q_x\mathbf{x}+q_y\mathbf{y}+q_z\mathbf{z}). \tag{26}$$

Note that in the above equation and hereafter we have dropped the subscript N from q for brevity, that is, q_x stands for $q_{x,N}$. Note that due to fluctuations, q_i's are no longer equal to the cosine of the angles of $\mathbf{m}$ with the three axes, and hence the sum of their squares do not add to unity. Therefore normalization of the final vector is part of the estimation procedure in Eq. (26).

The probability of obtaining these correlations depends on the angles α, β, and γ as given by (13) [see the paragraph after (13)]. Therefore we have

$$P(\mathbf{m}_e|\mathbf{m}) = P(q_x,q_y,q_z|\mathbf{m}) = P(q_x|\alpha)P(q_y|\beta)P(q_z|\gamma), \tag{27}$$

where $P(q_{x,N}|\alpha)$ is given by (13), with θ replaced by α and similar formulas for the other two probabilities hold. The fidelity between the vector and its estimate is given by $F(\mathbf{m}_e,\mathbf{m}) = \frac{1}{2}(1+\mathbf{m}_e\cdot\mathbf{m})$, and the average fidelity is then given by

$$F_N^A = \sum_{q_x,q_y,q_z=-1}^{1}\int d\mathbf{m}P(\mathbf{m}_e|\mathbf{m})F(\mathbf{m}_e,\mathbf{m}). \tag{28}$$

Here the sum over q_i from -1 to 1 can be replaced with the sum over $N_{i,d}$ from 0 to N [see the second remark after Eq. (13)], and the probability is given by (27). The right-hand side of (28) can be computed numerically, and the behavior of the average fidelity for different values of N can be seen in Fig. 4. One can see that our protocol achieves high fidelities for small values of N, even though we have used just one-qubit measurements. The optimal fidelity of direction sharing is calculated in [8] when Alice sends the state $|m\rangle^{\otimes N}$ to Bob, and they show that the optimal measurement procedure necessarily involves a positive operator-valued measure on the whole system and cannot be achieved by performing measurements on the components of the system; however, we reach the optimal fidelity by only a very small gap. Figure 4 compares the average direction sharing fidelities of our protocol with that of the optimal method [8] for different values of N. For example when $N=2$, Alice and Bob use six singlet pairs and one-qubit measurements to share the direction $\mathbf{m}$ with average fidelity 0.85, while the optimal fidelity $\frac{6+1}{6+2}=0.875$ can be achieved exclusively by global measurements. Hence if the laboratory restrictions force us to have simple measurements, our method will be a very good procedure for direction sharing.

2. *Method B: Using 2N singlets*

Let $2N$ singlet pairs be shared between Alice and Bob. By the same procedure as in the ideal case of an infinite number of pairs (Sec. II A), while Alice is measuring along the $\mathbf{m}$ direction, Bob measures his first N qubits along the x axis and the other qubits along the y axis, and from the respective correlations q_x and q_y and by using Eq. (21) he can estimate the vector $\mathbf{m}_e$ to be

$$\mathbf{m}_e = \frac{Nq_x}{N+2}\mathbf{x}+\frac{Nq_y}{N+2}\mathbf{y} + \sqrt{1-\left(\frac{Nq_x}{N+2}\right)^2-\left(\frac{Nq_y}{N+2}\right)^2}\ \mathbf{z}, \tag{29}$$

where we have used the partial information that the vector $\mathbf{m}$ lies in the northern hemisphere and hence have chosen the plus sign for m_z.

Note that due to fluctuations of the values q_x and q_y for finite N, it may happen that $(\frac{Nq_x}{N+2})^2+(\frac{Nq_y}{N+2})^2>1$, in which case $\mathbf{m}_e$ cannot be defined. Such cases are inadmissible. Bob has to abandon his inadmissible cases and repeat the protocol to obtain acceptable values for q_x and q_y. The question is then what is the probability that Bob obtains inadmissible correlations, that is, the probability of obtaining $(\frac{Nq_x}{N+2})^2+(\frac{Nq_y}{N+2})^2>1$. To put a bound on this probability, we use the Chebyshev formula according to which for a positive random variable X we have

$$\Pr(X\geqslant a)\leqslant\frac{\langle X\rangle}{a}. \tag{30}$$

In view of (14), this gives after some simple algebra

$$\Pr(inadmissible)\equiv\Pr\left(q_x^2+q_y^2\geqslant\left(\frac{N+2}{N}\right)^2\right) \leqslant\left(1-\cos^2\gamma+\frac{1}{N}(1+\cos^2\gamma)\right), \tag{31}$$

where γ is the angle between $\mathbf{m}$ and the z axis. Obviously the probability depends on the angle γ. Averaging over all angles γ in the northern hemisphere, this will give a bound

$$\langle\Pr(inadmissible)\rangle\leqslant\left(\frac{N}{N+2}\right)^2\left(\frac{2}{3}+\frac{4}{3N}\right), \tag{32}$$

which shows that for large N at least one-third of pairs lead to admissible correlations. In fact, it is much better than this, and numerical calculations show that the admissible probability is about 0.9 for $N=15$. Since not all steps of the protocol of method B are admissible, in order to have

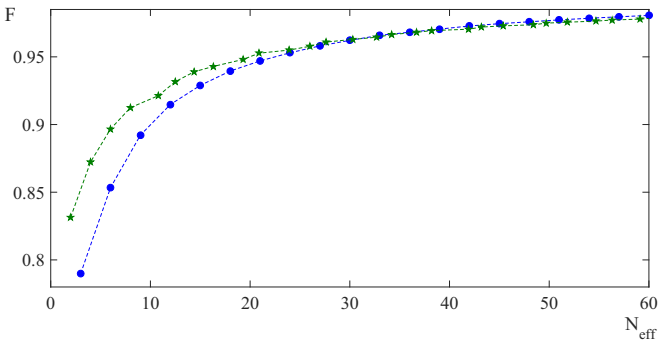

FIG. 5. Average fidelity of estimation for two different methods as a function of the effective number of singlet pairs used in each run of the protocols. Blue circles correspond to the fidelities of method A, and green stars correspond to the fidelities of method B. For more explanation see the paragraph after Eq. (32).

a comprehensive comparison between methods A and B, we define the effective number of pairs used in each protocol to be $N_{\text{eff}} = \frac{N_{\text{used}}}{\Pr(admissble)}$ for each method. N_{used} is the number of pairs used in each run of the protocols. In method A, $N_{\text{used}} = 3N$ and $\Pr(admissible) = 1$, while for method B $N_{\text{used}} = 2N$ and the admissible probability has been calculated numerically. Figure 5 shows the fidelities of both methods as a function of the effective number of pairs used. Note that although in method B Alice and Bob use $2N$ pairs, they rely on *a priori* information about their axes (for example, being in the upper or lower hemisphere), and for small values of N this prior information helps them to achieve higher fidelities compared with method A (see Fig. 5). As N increases both methods reach the same fidelity, which means that Alice and Bob compensate the lack of prior information in this case by consuming extra shared singlets. For sufficiently large values of N, the fidelity of method A exceeds that of method B, as expected.

IV. CONCLUSION

In this article we have introduced a method for secure alignment of coordinate systems between two distant parties in a way which prevents third parties from getting information about the aligned coordinate systems. This is certainly significant for the two parties who want to use measurements along different bases for performing quantum information tasks. The method is essentially based on obtaining information about directions from the correlations in the measurement results on singlet states shared between the two parties. The presented method achieves a very high average fidelity even though we have just one-qubit measurements. In a sense this is the converse of what is done in quantum key distribution, where instead of publicly announcing the measurement bases, Alice and Bob publicly announce the measurement results, which enables them to align their coordinate systems. Of course they both have to trust the dealer who has sent them truly singlet pairs.

The protocol is secure in the following sense: Clearly the access of Eve to the classical strings $(a_1,a_2,\ldots,a_N)$ OR $(b_1,b_2,\ldots,b_N)$ publicly announced by Alice OR Bob does not convey to her any information about the actual measurement directions of them. However, the whole protocol can be sabotaged by Eve in the following ways. She can entangle herself with the entangled pairs shared by Alice and Bob, i.e., sharing a GHZ state with them, in which case the correlations between Alice and Bob will be diminished considerably and will not lead to aligned reference frames. This kind of sabotage can be detected later by running a test quantum information protocol by Alice and Bob.

The other way that Eve can interfere is in the initial process of distributing singlets between the two parties. For each singlet which is to be distributed and shared by Alice and Bob, Eve can intercept the qubit of, say, Alice, and instead produce a new singlet, one qubit of which is kept by herself and the other one sent to Alice. In this way she can share a singlet with Alice and another singlet with Bob. If in our protocol both Alice and Bob were to announce their classical strings of bits, then this would enable Eve to align two reference frames, one with Alice and the other with Bob, preventing Alice and Bob from sharing an aligned reference frame. By further intercepting the classical communications between Alice and Bob, Eve could interfere with any quantum information protocol being run between Alice and Bob. However, in our protocol only one of the parties announces his or her classical bits (results of measurements) while the other party keeps her or his results for comparison and determines the correlations. Therefore in this kind of attack, Eve can only align her reference frame with one of the parties. Further interception of classical messages between Alice and Bob does not help her anymore in hiding her presence, which can be detected by them once they perform a test quantum information protocol.

ACKNOWLEDGMENTS

We would like to thank members of the QI group at Sharif University of Technology for their various useful comments on this work. A.M. would like to acknowledge the financial support of University of Tehran for this research under Grant No. 30375/01/01.

[1] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[2] A. Barenco and A. K. Ekert, J. Mod. Opt. **42**, 1253 (1995).
[3] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE Press, 1984), pp. 175–179.
[4] C. H. Bennett and G. Brassard, IBM Technical Disclosure Bulletin **28**, 3153 (1985).
[5] A. Peres and P. F. Scudo, arXiv:quant-ph/0201017.
[6] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Rev. Mod. Phys. **79**, 555 (2007).
[7] N. Gisin and S. Popescu, Phys. Rev. Lett. **83**, 432 (1999).
[8] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).
[9] E. Bagan, M. Baig, A. Brey, R. Munoz-Tapia, and R. Tarrach, Phys. Rev. Lett. **85**, 5230 (2000).

[10] A. Peres and P. F. Scudo, Phys. Rev. Lett. **86**, 4160 (2001).
[11] E. Bagan, M. Baig, A. Brey, R. Munoz-Tapia, and R. Tarrach, Phys. Rev. A **63**, 052309 (2001).
[12] A. Acin, E. Jane, and G. Vidal, Phys. Rev. A **64**, 050302 (2001).
[13] E. Bagan, M. Baig, and R. Munoz-Tapia, Phy. Rev. A **69**, 050303 (2004).
[14] R. Derka, V. Buzek, and A. K. Ekert, Phys. Rev. Lett. **80**, 1571 (1998).
[15] J. I. Latorre, P. Pascual, and R. Tarrach, Phys. Rev. Lett. **81**, 1351 (1998).
[16] D. Bruss, A. Ekert, and C. Macchiavello, Phys. Rev. Lett. **81**, 2598 (1998).
[17] S. Massar, Phys. Rev. A **62**, 040101(R) (2000).
[18] G. Chiribella, L. Maccone, and P. Perinotti, Phys. Rev. Lett. **98**, 120501 (2007).
[19] A. Peres and P. F. Scudo, Phys. Rev. Lett. **87**, 167901 (2001).
[20] N. H. Lindner, A. Peres, and D. R. Terno, Phys. Rev. A **68**, 042308 (2003).
[21] G. Chiribella, G. M. D'Ariano, P. Perinotti, and M. F. Sacchi, Phys. Rev. Lett. **93**, 180503 (2004).
[22] P. Kolenderski and R. Demkowicz-Dobrzanski, Phys. Rev. A **78**, 052333 (2008).
[23] T. B. Bahder, Quantum Inf. Process. **15**, 1069 (2016).
[24] B. van Fraassen, *Laws and Symmetry* (Oxford University Press, Oxford, UK, 1989).