Quantum secret sharing and random hopping: Using single states instead of entanglement

V. Karimipour and M. Asoudeh
Department of Physics, Sharif University of Technology, Teheran, Iran
and Department of Physics, Azad University, Northern Branch, Tehran, Iran

(Received 11 June 2015; published 2 September 2015)

Quantum secret sharing (QSS) protocols between N players, for sharing classical secrets, either use multipartite entangled states or use sequential manipulation of single d-level states only when d is prime (A. Tavakoli *et al.*, arXiv:1501.05582). We propose a sequential scheme which is valid for any value of d. In contrast to A. Tavakoli *et al.* whose efficiency (number of valid rounds) is $\frac{1}{d}$, the efficiency of our scheme is $\frac{1}{2}$ for any d. This, together with the fact that in the limit $d \longrightarrow \infty$ the scheme can be implemented by continuous variable optical states, brings the scheme into the domain of present day technology.

DOI: 10.1103/PhysRevA.92.030301 PACS number(s): 03.67.Hk, 03.67.Dd

Introduction. Quantum key distribution (QKD) [1,2] is among the best experimentally developed areas [3] in the field of quantum information science. With the rapid growth in demand for secure communication in our world, it is imaginable that in the near future it will soon be an integrated part of modern communication systems. At the very basis of this development lies the fact that QKD either uses bipartite entanglement [2] or sequential preparation and measurements of states by two parties, both of which are within reach of present technologies. In view of the need for more and more collaborative activities, quantum secret sharing (QSS) is at least at the same level of demand as QKD. QSS is the act of splitting a message so that only by collaboration of all the receivers, can it be retrieved. The question now is, is it possible to put QSS between an arbitrary number of parties, on the same level of experimental feasibility as QKD? Until a few years ago, the answer seemed to be no, because the known QSS schemes relied on multipartite entangled states which are much more difficult to prepare and more fragile than bipartite ones. Recent developments seem to point to a positive answer to this question.

The idea of using entanglement for sharing a secret key between three persons was first briefly pointed out in [4] and then developed in [5], where it was shown that local measurements of a Greenberger-Horne-Zeilinger state [6], enable three or four parties to share a random sequence of bits as a secret key. Generalization to many parties using multipartite entangled two-level states were developed in [7,8], and with separable two-level states in [9]. Generalization of QKD and QSS schemes to d-level states, again relying on multipartite entanglement, were studied in [10] and [11], respectively. Finally generalization of these entanglement-based schemes to continuous variable states [14] was reported in many works [12,13,15–20], where in some of them, such as [12,13], the polarization degrees of freedom of photons were used, and in the others, coherent or Gaussian states of light were used.

Along with all this theoretical and experimental success, and in view of the difficulty in creating and maintaining multiparty entangled states, a basic question has always been whether it is possible to do QSS between n parties by using a lesser amount of entanglement. This question received a partial positive answer, where it was shown that multipartite entanglement of qubits can be replaced by two-body entanglement [21] or by product states [22,23], the latter works being a combination of two or more QKD protocols of BB84 types [1] and all of them using qubit states. A sequential scheme with a proof of principle for its experimental realization was then reported in [24] where its security problem was discussed in [25,26].

It was then quite natural to ask if this sequential scheme can be generalized for d-level states, to which a positive answer was found for d being an odd prime in [27]. The efficiency (the average percentage of valid rounds) of this scheme which uses a system of $d+1$ Gaussian MUB's, is $\frac{1}{d}$, which becomes negligible for large d and vanishes for continuous variables. The aim of this Rapid Communication is to propose an entanglement-free QSS protocol which is valid for any d, uses the simple generalized Pauli and Hadamard gates, and leads to familiar operations in the continuous variable limit and, moreover, whose efficiency is $\frac{1}{2}$ for all d. We hope that removing the previous restrictions will bring the QSS scheme closer to experimental realization with current technology.

In order to proceed, a quick review of the method of [27] is in order, which is based on using mutually unbiased bases (MUBs) in Hilbert spaces of prime dimensions. There are $N+1$ players which are denoted by $R_0, R_1, R_2, \dots, R_N$. The first player, R_0, prepares a reference state and acts on it by an operator which depends on two random integers $0 \leqslant a_0,\ b_0 \leqslant d-1$ and passes the state to the next player who acts similarly on the state. In the end, the state which reaches the last player, Bob, depends on two parameters, $A := \sum_{i=0}^{N} a_i$ and $B := \sum_{i=0}^{N} b_i$. This player always measures the received state in a fixed basis, and only when $B = 0$ which happens one out of d runs, is there a perfect correlation between his measured result m and the random numbers a_i in the form

$$\sum_{i=0}^{N} a_i = m. \tag{1}$$

In other rounds no correlation exists and the round is discarded. If the protocol is run for $\approx Ld$ rounds and a number of L rounds are successful, then a sequence of perfectly correlated random strings are shared between all the players. If we denote by K_i the long sequence of dits $(a_{i,1}, a_{i,2}, a_{i,3} \cdots a_{i,L})$ for the ith player, and by $\mathcal{K} = (-m_1, -m_2, \dots, -m_L)$ the long sequence of negative-measured values by R_N, then according to (1) we have

$$\mathcal{K} \oplus K_0 \oplus K_1 \oplus K_2 \oplus \cdots \oplus K_N = 0, \tag{2}$$

where by $\oplus$ we mean a dit-wise sum modulo d between all the strings.

While this is an important step, the restriction to prime dimensions and the specific form of the operators used by the players make it difficult to go to the limit of continuous variables, a limit which has been most promising in actual implementation of many protocols by optical means [14].

In this Rapid Communication we report an entanglement-free QSS scheme between $N+1$ players who use a d-level state, where d is arbitrary. With d being arbitrary, one can now hope that experimental implementation will be much more feasible.

QSS scheme using a single qudit state for general d. The key insight is to look at the protocol of [27] as a random walk in a lattice of states, comprised of the bases of MUBs. With this random walk picture at hand, we can alleviate the restriction to prime numbers by devising a new lattice and new hopping operators. We take a $4 \times d$ lattice folded into a torus, where d is arbitrary. Let d be any positive integer and consider the computational orthonormal basis states for C^d, the complex d-dimensional Hilbert space as

$$\mathcal{B} = \{|k\rangle, 0 \leqslant k \leqslant d-1\}. \tag{3}$$

Let $\omega = e^{2\pi i/d}$ be the dth root of unity and F be the Fourier transform operator defined as

$$F := \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} \omega^{ij} |i\rangle\langle j|. \tag{4}$$

The operator F has the following interesting properties, which result from the identity $\sum_{i=0}^{d-1} \omega^r = d\delta_{r,0}$:

$$F^2 = \sum_{k=0}^{d-1} |-k\rangle\langle k|, \quad F^4 = I. \tag{5}$$

Furthermore, when acting on the state $|k\rangle$, F creates another state $|a_k\rangle$,

$$|\xi_k\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{jk} |k\rangle, \tag{6}$$

which constitutes another basis $\hat{\mathcal{B}}$,

$$\hat{\mathcal{B}} = \{|\xi_k\rangle, 0 \leqslant k \leqslant d-1\}, \tag{7}$$

mutually unbiased basis with respect to $\mathcal{B}$. Consider now the generalized Pauli operators $X := \sum_{k=0}^{d-1} |k+1\rangle\langle k|$ and $Z := \sum_{k=0}^{d-1} \omega^k |k\rangle\langle k|$. These two operators act as shift operators on the bases $\mathcal{B}$ and $\hat{\mathcal{B}}$, respectively:

$$X|k\rangle = |k+1\rangle, \quad Z|\xi_k\rangle = |\xi_{k+1}\rangle. \tag{8}$$

Conversely when acting on the bases $\hat{\mathcal{B}}$ and $\mathcal{B}$, the operators X and Z act as phase operators:

$$X|\xi_k\rangle = \omega^{-k}|\xi_k\rangle, \quad Z|k\rangle = \omega^k|k\rangle. \tag{9}$$

We also note that

$$F|k\rangle = |\xi_k\rangle, \quad F|\xi_k\rangle = |-k\rangle. \tag{10}$$

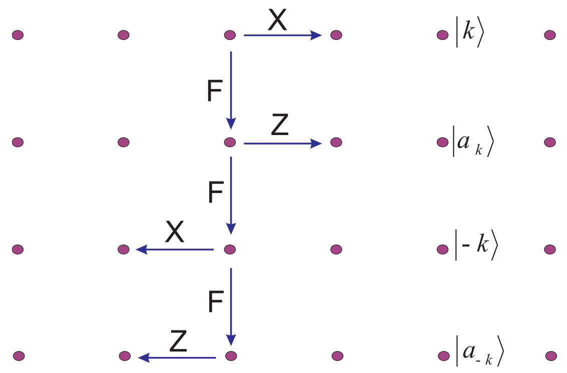

FIG. 1. (Color online) The action of each player causes the point representing the state to do a random hopping in this lattice of states. It is important to note that the Z operators in the first and the third rows and the X operators in the second and fourth rows do nothing (they just add overall phases). These phases can safely be ignored.

In view of these relations it is convenient to draw the four rows of states of $\mathcal{B}$ and $\hat{\mathcal{B}}$ in the order shown in Fig. 1.

Running the protocol. The steps of the protocol are as follows:

(1) R_0 starts from the state $|0\rangle$ and acts on it by the operators $X^{a_0} Z^{b_0} F^{c_0}$ (where $0 \leqslant a_0, b_0 \leqslant d-1$ are random integers and $c_0 = 0,1$). She then sends this state to the first player, R_1, who acts on the received state by $X^{a_1} Z^{b_1} F^{c_1}$ and then sends the state to the second player, R_2, who does the same thing. The process repeats until the state reaches the last player, R_N. He also acts on the state by $X^{a_N} Z^{b_N} F^{c_N}$ and measures it in the computational or $\mathcal{B}$ basis. The final state before this measurement is given by

$$|\Psi\rangle = \prod_{i=0}^{N} (X^{a_i} Z^{b_i} F^{c_i})|0\rangle. \tag{11}$$

(2) After measurement of R_N, all the players $R_0, R_1, R_2, \ldots, R_N$ are asked by Alice (the one who controls the protocol whom we call Alice; she can be any of the players) to publicly announce their integers c_i which are 0 or 1. Also they can be asked by Alice to make this announcement in random order. It is crucial that the integers a_i and b_i are kept secret from the players and are not announced at any stage. If

$$\sum_{i=0}^{N} c_i = 0 \bmod 2, \tag{12}$$

the round is treated as valid, since this means that the point has landed on the correct basis $\mathcal{B}$ for the measurement of R_N, otherwise it is discarded.

(3) In valid rounds, we are certain that the point representing the state lies on the computational basis B and when R_N measures this state he obtains a definite and deterministic value denoted by m_N. In invalid rounds, due to the MUB property of the two bases B and $\tilde{B}$, a completely random result is obtained and no perfect correlation exists between the result of R_N measurements and the random bits applied by others.

But what is the exact form of the correlation? It is not as simple as Eq. (1), but it is as perfect as it is. Looking at the lattice in Fig. 1, it is crucial to note that in the first and third rows, the Z operator does nothing (it just adds an overall phase

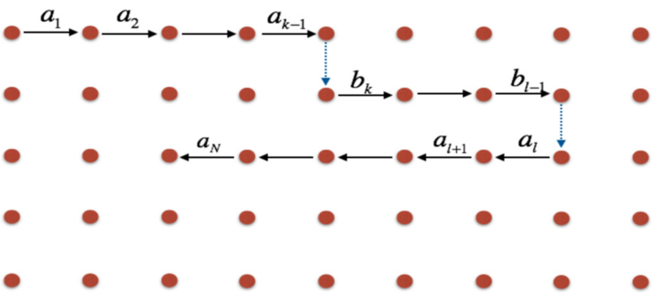

FIG. 2. (Color online) A simple example of a random path in the lattice of states, when only two players apply F operators. In order not to clutter the figure, we have shown all the steps to be of unit size (between neighboring sites). The steps can be of any size between non-neighboring sites. The first and the last rows are the same.

to the state). The same is true for the X operator in the second and fourth rows. This means that the effect of these operators on these respective rows can safely be ignored. So suppose that the operator F is applied only twice, by the players R_k and R_l. Figure 2 shows the path of the random walk. Modulo an overall phase, the final state is given by

$$|\Psi\rangle=\left|\sum_{i=0}^{k-1} a_i+\sum_{i=k}^{l-1} b_i-\sum_{i=l}^{N} a_i\right\rangle := |A_{0,k-1}+B_{k,l-1}-A_{l,N}\rangle, \tag{13}$$

where

$$A_{r,s} := \sum_{i=r}^{s-1} a_i, \quad B_{r,s} := \sum_{i=r}^{s-1} b_i. \tag{14}$$

Or suppose that the operator F is applied four times, by the players R_k, R_l, R_m, and R_n. Figure 3 shows the path of the random walk and the final state is given by

$$|\Psi\rangle = |A_{0,k-1}+B_{k,l-1}-A_{l,m-1}-B_{m,n-1}+A_{n,N}\rangle. \tag{15}$$

The pattern is now clear. Although it is straightforward, we do not attempt to clutter the text with writing general formulas for the final state corresponding to a given random path. The point to emphasize is that once the numbers c_i are publicly announced, all the parties R_0 to R_N know the positions of the F operators—the vertical steps. Note that the vertical steps are of unit size. In those valid rounds, the value measured by R_N has perfect correlation with those used by all the other parties. Let us elaborate this by an example. Suppose there are six players R_0 to R_5 and two F operators are used in round 1 and round 2, but in two different places. For example, in round 1 the F operators are in positions 2 and 5, and in round 2 the F operators are in positions 1 and 4. Then according to (13) if we denote the values that R_5 measures in these two rounds respectively by m and m', we will have

$$\begin{aligned} a_0+a_1+b_2+b_3+b_4-a_5 &= m_5,\\ a_0'+b_1'+b_2'+b_3'-a_4'-a_5' &= m_5'. \end{aligned} \tag{16}$$

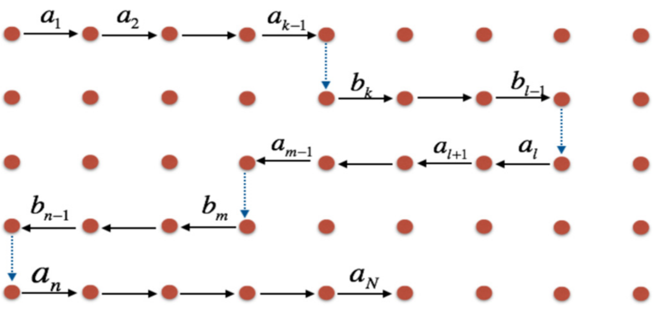

FIG. 3. (Color online) A simple example of a random path in the lattice of states, when only four players apply F operators.

Since the positions of the F operators (the vertical steps) are known by the public announcement of all the c_i's, they know how to arrange their keys $K_0,K_1,\ldots,K_5$ from the above d-level integers. For example, the first numbers of these keys are $K_0=(a_0,a_0',\ldots)$, $K_1=(a_1,b_1',\ldots)$, $K_2=(b_2,b_2',\ldots)$, $K_3=(b_3,b_3',\ldots)$, $K_4=(b_4,-a_4',\ldots)$, $K_5=(-a_5,-a_5',\ldots)$, and $\mathcal{M}_5=(-m_5,-m_5',\ldots)$. Then we have

$$K_0\oplus K_1\oplus K_2\oplus K_3\oplus K_4\oplus K_5\oplus \mathcal{M}_5=0. \tag{17}$$

In this way a secret key is created between all the parties which can be used for sharing messages via public classical channels.

Using the shared key. Let us denote the random string $K_N+\mathcal{M}_N$ of the last player by $\mathcal{K}_N$. Therefore the shared random key which has been established satisfies $K_0+K_1+\cdots+K_{N-1}+\mathcal{K}_N=0$.

Like any other QSS scheme, any player R_i can play the role of Alice who wants to send a secret message to another player R_j (playing the role of Bob) who will retrieve the message by the collaboration of other parties. Alice can send a message $\mathcal{M}$ in the form $\mathcal{M}\oplus K_i$ to Bob. Ali,e who now controls the protocol (like any other QSS scheme), asks the other parties to send their random keys to Bob who retrieves the message by performing the relation $(\mathcal{M}\oplus K_i)\oplus\sum_{j\neq i}K_j$, which in view of the previous relation gives the message $\mathcal{M}$.

Security against attacks. We can now consider how the protocol is secure against attacks. A round of the protocol corresponds to a random path on the lattice of states as shown in Fig. 3. If any of the players wants to measure his received qudit and keeps a copy of it, he should know the basis, but this is not possible for him, because the integers c_i or equivalently the F moves, are announced only after all measurements are done. Since the two bases $\mathcal{B}$ and $\hat{\mathcal{B}}$ are MUBs with respect to each other, blind measurement in a basis causes an error rate of $\frac{d-1}{d}$ in the final measured qudit by Bob. This type of intervention or cheating is easily detectable by publicly comparing a subsequence of the shared key. These considerations also apply if a group of players enter a plot to intercept the key, since they can be collectively considered as a single party to which the basis used by the previous parties is not known.

Another conceivable attack is that a group of players, each entangle their respective received qudits from previous players to some ancilla and store part of the information in these ancillas. They can then collaborate with each other and share this collected information to retrieve the key. A standard way for entangling a received state $|\psi\rangle$ to an ancilla is to start the ancilla in the state $|+\rangle := \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle$ and act on the joint state $|+\rangle\otimes|\psi\rangle$ by a generalized controlled-NOT (CNOT) operator, $\text{CNOT}|i,j\rangle := |i,i+j\rangle$. If the received state is a computational state $|q\rangle$, then this action results in $\text{CNOT}|+\rangle\otimes|q\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle\otimes|i+q\rangle$, which is a maximally entangled state. In this way the ancilla will be in a completely mixed state and stores no information of the qudit q. However, if the received qudit is of the form $|\xi_q\rangle$, that is, a Fourier basis state, then the ancilla can indeed store some information of q. In this case we find that CNOT$|+\rangle \otimes |\xi_q\rangle = |\xi_{-q}\rangle \otimes |\xi_q\rangle$. In this way, information about q is stored in the ancilla without leaving any trace in the state $|\xi_q\rangle$ which is being communicated between the players. Each player can then measure his ancilla in the Fourier basis $\hat{B}$ and retrieve q. However, since a received state can be in one of the states $|q\rangle$ or $|\xi_q\rangle$ with equal probability, each player has a 50% chance of successfully storing information in his ancilla, leaving no trace in the transmitted state $|\xi_q\rangle$, and 50% chance of completely decohering the state $|q\rangle$. In this second case he commits an error rate of $\frac{d-1}{d}$ on each state. Again by publicly announcing a subsequence of the key, the players can discern the existence of a plot within the group.

Conclusion. We have proposed a scheme for multiparty secret sharing which uses a single d-level state for arbitrary d, and alleviates the need for entanglement. The basic idea is the analogy with a random walk performed by a particle through a lattice of states. This walk is the result of random sequential unitary operations on a single particle by the players one after the other. In view of the fact that the players do not have information about each others unitary operations, the path of the particle resembles a random walk which lands on a particular row (a particular basis) only when certain conditions are met. This condition is revealed only after public announcement of some parameters of the operations after all the measurements have been done. In the limit of $d \longrightarrow \infty$, the local actions of the players will become $X(s)Z(t)F^c$ where s and t are continuous variables and $c = 0,1$. Here $X(s) = e^{is\hat{p}}$ and $Z(t) = e^{it\hat{x}}$ with $\hat{x}$ and $\hat{p}$ the position and momentum operators ($[\hat{x},\hat{p}] = i\hbar$) (corresponding to the quadratures of a mode of electromagnetic field) and F the Fourier transform between the position and momentum bases. Quantum optical realizations of these relations then puts this protocol quite within the reach of present day technology.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), Vol. 175, p. 8.

[2] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[4] M. Zukowski, A. Zeilinger, M. A. Horne, and H. Weinfurter, Acta Phys. Pol. A **93**, 187 (1998).

[5] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[6] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic, Dordrecht, 1989); D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).

[7] A. Sen(De), U. Sen, and M. Zukowski, Phys. Rev. A **68**, 032309 (2003).

[8] Li Xiao, Gui Lu Long, Fu-Guo Deng, and Jian-Wei Pan, Phys. Rev. A **69**, 052307 (2004).

[9] Zhan-jun Zhang, Yong Li, and Zhong-xiao Man, Phys. Rev. A **71**, 044301 (2005).

[10] Nicolas J. Cerf, Mohamed Bourennane, Anders Karlsson, and Nicolas Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

[11] I.-Ching Yu, F.-L. Lin, and C.-Y. Huang, Phys. Rev. A **78**, 012344 (2008).

[12] Y.-A. Chen *et al.*, Phys. Rev. Lett. **95**, 200502 (2005).

[13] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, Phys. Rev. Lett. **98**, 020503 (2007).

[14] Samuel L. Braunstein and Peter van Loock, Rev. Mod. Phys. **77**, 513 (2005).

[15] Tomáš Tyc and Barry C. Sanders, Phys. Rev. A **65**, 042310 (2002).

[16] Andrew M. Lance, Thomas Symul, Warwick P. Bowen, Tomáš Tyc, Barry C. Sanders, and Ping Koy Lam, New J. Phys. **5**, 4 (2003).

[17] Andrew M. Lance, Thomas Symul, Warwick P. Bowen, Barry C. Sanders, and Ping Koy Lam, Phys. Rev. Lett. **92**, 177903 (2004)

[18] Frédèric Grosshans, Gilles Van Assche, Jerîome Wenger, Rosa Brouri, Nicolas J. Cerf, and Philippe Grangiera, Nature (London) **421**, 238 (2003).

[19] Frèdèric Grosshans and Philippe Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[20] Stefano Pirandola, Stefano Mancini, Seth Lloyd, and Samuel L. Braunstein, Nat. Phys. **4**, 726 (2008).

[21] Anders Karlsson, Masato Koashi, and Nobuyuki Imoto, Phys. Rev. A **59**, 162 (1999).

[22] Guo-Ping Guo and Guang-Can Guo, Phys. Lett. A **310**, 4 (2003).

[23] Feng-Li Yan and Ting Gao, Phys. Rev. A **72**, 012304 (2005).

[24] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Phys. Rev. Lett. **95**, 230505 (2005).

[25] S.-J. Qin, F. Gao, Q.-Y. Wen, and F.-C. Zhu, Phys. Rev. A **76**, 062324 (2007).

[26] G.-P. He, Phys. Rev. Lett. **98**, 028901 (2007); for the reply see C. Schmid, P. Trojek, P. M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, *ibid.* **98**, 028902 (2007).

[27] A. Tavakoli, I. Herbauts, M. Zukowski, and M. Bourennane, arXiv:1501.05582.