# Generalized flying-qudit scheme in arbitrary dimensions

Thomas Durt,[1,*] L. C. Kwek,[2,3] and Dagomir Kaszlikowski[3]
[1]*TENA-TONA Free University of Brussels, Pleinlaan 2, B-1050 Brussels, Belgium*
[2]*Department of Physics, Faculty of Science, National University of Singapore, Lower Kent Ridge, Singapore 119260, Republic of Singapore and National Institute of Education, Nanyang Technological University, 1 Nanyang Walk, Singapore 639798, Republic of Singapore*
[3]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Republic of Singapore*
(Received 28 December 2006; revised manuscript received 16 November 2007; published 22 April 2008)

We generalize in higher dimensions the so-called "flying-qubit scheme" that was described in the paper by Lim, Beige, and Kwek [Phys. Rev. Lett. **95**, 030505 (2005)]. In that paper, the authors proposed a scheme according to which distant atoms get entangled during a measurement, in the Bell basis, of photons (flying qubits) emitted by them. We show that although in principle a generalization of this scheme to arbitrary dimensions is possible, this theoretical proposal is not presently feasible in all dimensions because only qubit Bell states have been successively measured until now. Nevertheless we show that a many-qubits generalization of the flying-qubit scheme factorizes and reduces to the realization, in parallel, of many individual single-qubit schemes, for which it is known that they are realizable experimentally with the techniques that are available today. In other words, our approach shows that when $d$ is an even prime power ($d=2^m$), the flying-qudit scheme reduces to $m$ flying-qubit schemes. For $d=2^m$ and arbitrary $m$ the implementation of a generalized, maximally entangling, conditional qudit phase gate "with insurance" or "repeat-until-success" is thus shown to be feasible in practice by coupling $m$ (pairs of) two-level atoms to $m$ (pairs of) two-level (polarized) photons. Moreover, due to the parallelism of the task, the time necessary for completing successfully the task scales logarithmically in a function of $m$ while at the same time the dimension of the Hilbert space scales exponentially which presents promising perspectives regarding quantum informational realizations such as the quantum computer.

DOI: 10.1103/PhysRevA.77.042318 PACS number(s): 03.67.Lx, 02.70.−c, 03.65.Ud

## I. INTRODUCTION

Quantum computing based solely on linear optics scheme does not permit the realization of deterministic entangling gates. For probabilistic setups, the realization of entangling gates with success probabilities close to unity requires the presence of highly entangled ancilla states and quantum teleportation [1] as a universal quantum primitive [2]. In the proposal in Ref. [1] [Knill-Laflamme-Milburn (KLM)], the amount of required resources for the realization of quantum computing can be very large [3,4]. In the KLM proposal [1], the gates in a computational network succeed with a small probability of success. We therefore need to repeat the computation many times, either in terms of replication of devices or time, in order to achieve reasonable degree of success. In either case, the required resources (time and devices) scale exponentially with the number of gates. Since then, a lot of effort has been made to reduce the required resources for such realization [5], and in Ref. [6] an error correction scheme whose number of elementary logic operations scales as a polynomial function of the inverse of the gate error or failure rate was proposed. Experiments demonstrating the feasibility of proposed schemes have also been performed [7].

Recently, there has been proposals [8,9] based on hybrid systems. The linear optics scheme relies on flying qubits and their interactions with linear optics devices, such as beam splitters and mirrors. The advantage of the flying-qubit scheme is that it allows us to entangle distant atoms (stationary qubits) that never interacted directly by projecting photons emitted by them onto entangled states, which is an aspect of entanglement swapping. The proposal combines the robustness of atoms seen as quantum memories and the mobility of photons which are more likely to get entangled during a measurement process than the atoms. Versatility of the photons stems primarily from their mobility, while the inertia of atoms is perceived as an advantage for quantum storage besides being robust against decoherence. The hybrid schemes allow us to implement qubit atomic conditional phase gates (which are equal to Ising gates, up to local unitaries [8]) at relatively low cost. Despite of the fact that it is not possible to measure a pair of photons in a basis that consists of Bell states only (the best that we can do is to measure them in a basis that consists of two Bell states and two product states), the scheme presents a guarantee (insurance) in the sense that whenever the photons are projected onto a product state during the measurement, it is possible to reinitialize the system easily and to repeat the whole process so as to project the two photons finally onto a Bell state.

The paper is organized as follows. We describe the flying-qubit scheme in Sec. II. We show that the flying-qudit scheme can be realized in principle in arbitrary dimension in Sec. III. This generalization to arbitrary dimension requires the use of Gauss sums and the properties of the generalized Pauli group. The experimental implementation of this scheme is problematic because as far as we know, it is very difficult or impossible presently to measure qudit Bell states when $d$ is higher than 2. Nevertheless, a side result of our

*thomdurt@vub.ac.be

 

proof is that the implementation of the repeat-until-success linear optics distributed quantum computing scheme (or more precisely of a maximally entangling conditional 2-qudit phase gate) "factorizes" to the parallel implementation of maximally entangling conditional 2-qu$d$1it, 2-qu$d$2it, 2-qu$d$3it, etc., phase gates, where $d$ is factorized into a product of prime numbers $d1, d2, d3, \ldots$. In particular the realization of a maximally entangling conditional phase gate between two many-qubit systems factorizes to the parallel realization of many 2-qubit maximally entangling conditional phase gates. Therefore, we propose in Sec. IV a physically realizable implementation in the many-qubit case that reduces to parallel implementations of the original flying-qubit scheme for which, in principle, experimental realizability is feasible (Ref. [8]). We also show that, due to the parallelism of the task, the scalability in time of the whole process is very satisfactory. Indeed it scales logarithmically in function of the number of subsystems and not linearly as would be the case when the task is performed in series and not in parallel.

## II. ORIGINAL FLYING-QUBIT SCHEME

Let us first introduce the reference qubit bases or computational bases for atomic and photonic two-level systems $A$ and $B$. They consist of the orthogonal and normalized qubit states $|0\rangle^{A_{a(p)}}$ and $|1\rangle^{A_{a(p)}}$ and $|0\rangle^{B_{a(p)}}$ and $|1\rangle^{B_{a(p)}}$ [in what follows $A_a$ and $A_p$ ($B_a$ and $B_p$) refer to atoms in and photons from the distant regions $A$ ($B$)]. Let us now consider two other (photonic) qubit bases $A$ and $B$ described by [9]

$$|A_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{A_p} + |1\rangle^{A_p}),$$

$$|A_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{A_p} - |1\rangle^{A_p}),$$

$$|B_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{B_p} + |1\rangle^{B_p}),$$

$$|B_1\rangle = \frac{i}{\sqrt{2}}(|0\rangle^{B_p} - |1\rangle^{B_p}). \tag{1}$$

We note at this stage that Bell states of the form

$$|B_{ij}\rangle = \frac{1}{\sqrt{2}}\sum_{k=0}^{1} \gamma_2^{jk}|A_k\rangle|B_{k+i}\rangle \tag{2}$$

with $\gamma_2 = -1$ possess interesting properties: They are equally balanced relative to the computational basis $|\langle B_{ij}|m^A, n^B\rangle| = 1/2$, for all values of $i, j, m, n$ in $\{0,1\}$ and they are also maximally entangled relative to the subsystems $A$ and $B$ by construction.

The combination of these two properties makes the basis very appealing in relation to quantum computation. They lie at the heart of the so-called flying-qubit scheme that aims at realizing a maximally entangling unitary evolution on two distant atoms. In order to show this let us assume that two distant two-level atoms are prepared in the factorizable state $|\psi\rangle^{A_a}|\phi\rangle^{B_a} = (\alpha|0\rangle^{A_a} + \beta|1\rangle^{A_a})(\gamma|0\rangle^{B_a} + \delta|1\rangle^{B_a})$.

We now interact with the atoms in such a way that each of them emits a photon having its polarization entangled with the energy level of the atom (relevant references concerning experimental realizations of this transformation can be found in Refs. 12–15 of Ref. [8]),

$$|\psi\rangle^{A_a} \otimes |\phi\rangle^{B_a} \to (\alpha|0\rangle^{A_a}|0\rangle^{A_p} + \beta|1\rangle^{A_a}|1\rangle^{A_p}) \otimes (\gamma|0\rangle^{B_a}|0\rangle^{B_p} + \delta|1\rangle^{B_a}|1\rangle^{B_p}). \tag{3}$$

Let us then measure the polarization state of the two photons in a joint 2-qubit measurement that has at least an eigenstate that is maximally entangled and equally balanced relatively to the computational basis [such states are defined by Eqs. (1) and (2)]. Due to equal balance, this state can always be written in the form $\frac{1}{2}\Sigma_{k,l=0}^{1} e^{i\phi_{kl}}|k\rangle^{A_p}|l\rangle^{B_p}$. Whenever we measure the eigenvalue that corresponds to this state (see Ref. [10]), the atomic states are projected onto the state

$$\alpha\gamma e^{-i\phi_{00}}|0\rangle^{A_a}|0\rangle^{B_a} + \beta\gamma e^{-i\phi_{10}}|1\rangle^{A_a}|0\rangle^{B_a} + \alpha\delta e^{-i\phi_{01}}|0\rangle^{A_a}|1\rangle^{B_a} + \beta\delta e^{-i\phi_{11}}|1\rangle^{A_a}|1\rangle^{B_a}. \tag{4}$$

This is equivalent to the unitary transformation

$$|k\rangle^{A_a}|l\rangle^{B_a} \to e^{-i\phi_{kl}}|k\rangle^{A_a}|l\rangle^{B_a}. \tag{5}$$

Such a transformation is not factorizable into local transformations that would act separately onto the atoms $A$ and $B$ due to the fact that the state $\frac{1}{2}\Sigma_{k,l=0}^{1} e^{i\phi_{kl}}|k\rangle^{A_p}|l\rangle^{B_p}$ is assumed to be maximally entangled. For instance, when the qubits are both prepared in the first eigenstate of the Hadamard basis, $|\psi\rangle^{A_a}|\phi\rangle^{B_a} = \frac{1}{\sqrt{2}}(|0\rangle^{A_a} + |1\rangle^{A_a})\frac{1}{\sqrt{2}}(|0\rangle^{B_a} + |1\rangle^{B_a})$, they are transformed, after the completion of the full process, to the state $\frac{1}{2}\Sigma_{k,l=0}^{1} e^{-i\phi_{kl}}|k\rangle^{A_p}|l\rangle^{B_p}$ which is maximally entangled.

Let us consider the special case $\phi_{00} = \phi_{01} = \phi_{10} = -\phi_{11} = 1$, then the unitary transformation $|k\rangle^{A_a}|l\rangle^{B_a} \to e^{-i\phi_{kl}}|k\rangle^{A_a}|l\rangle^{B_a}$ is nothing else than the conditional $\pi$ phase gate.

For now obvious reasons, in what follows, we shall refer to the gates that characterize transformations of the type $|k\rangle^{A_a}|l\rangle^{B_a} \to e^{-i\phi_{kl}}|k\rangle^{A_a}|l\rangle^{B_a}$ (with $\Sigma_{k,l=0}^{1} e^{i\phi_{kl}}|k\rangle^{A_p}|l\rangle^{B_p}$ being a maximally entangled state) under the name maximally entangling conditional phase (MECP) gates. In the following sections we shall show how to realize qudit realizations of such gates for $d$ an arbitrary dimension.

It has been shown that an arbitrary 2-qubit unitary coupling can always be factorized into products of local unitary transformations and conditional phase gates [11]. The flying-qubit scheme makes it thus possible in principle to generate arbitrary couplings between the two distant two-level atoms through the manipulation of the photons (flying-qubits) emitted by these atoms.

Let us now consider the required measurements that are necessary for implementing the qubit MECP gate. It is well known that it is impossible to perform a complete Bell states measurement with linear optics [12]. Despite of the impossibility to realize in practice with simple optical components (beam splitters, phase shifters, and so on) a measurement that is diagonal in the Bell basis, it is nevertheless possible to

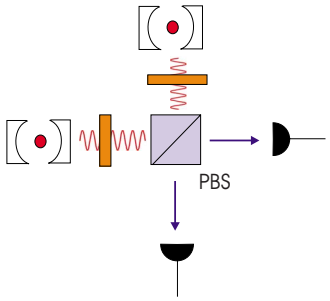


FIG. 1. (Color online) Flying-qubit scheme realized with photons emitted by atoms in cavities that are mixed in a beam splitter before undergoing a joint measurement resulting in a measurement of the states $|hv \pm vh\rangle$, $|hh\rangle$, and $|vv\rangle$.

realize a measurement of which two eigenstates are Bell states and which two eigenstates are factorizable [12].

Such a measurement can be realized, in the case that the degrees of freedom that correspond to the qubits are photonic polarizations, by sending the two polarization encoded photons through a beam splitter resulting in a measurement of the states $|hv \pm vh\rangle$, $|hh\rangle$, and $|vv\rangle$.

Passing the photons through a beam splitter after applying the map

$$U^{A_p} = |h\rangle\langle A_0| + |v\rangle\langle A_1|,$$

$$U^{B_p} = |h\rangle\langle B_0| + |v\rangle\langle B_1|, \tag{6}$$

as shown in Fig. 1 reduces then to a measurement of the states $|\Phi_i\rangle$ defined by

$$|\Phi_1\rangle \equiv |A_0\rangle|B_0\rangle,$$

$$|\Phi_2\rangle \equiv |A_1\rangle|B_1\rangle,$$

$$|\Phi_3\rangle \equiv \frac{1}{\sqrt{2}}[|A_0\rangle|B_1\rangle + |A_1\rangle|B_0\rangle],$$

$$|\Phi_4\rangle \equiv \frac{1}{\sqrt{2}}[|A_0\rangle|B_1\rangle - |A_1\rangle|B_0\rangle], \tag{7}$$

where the states $|A_i\rangle$ ($|B_i\rangle$) describe the photon originating from the atom in the $A$ ($B$) region.

When the outcome of the measurement corresponds to a factorizable eigenstate ($|\Phi_1\rangle$ or $|\Phi_2\rangle$), the effective unitary transformation of the two two-level atoms is factorizable. It is thus easy to reinitialize the atoms by implementing the local inverse transformations and to repeat the whole process. This is the reason why the qubit scheme is called in Ref. [8] "repeat-until-success quantum computing." In practice, the two outcomes corresponding to Bell states ($|\Phi_3\rangle$ or $|\Phi_4\rangle$) and the two outcomes corresponding to factorizable states are all observed with equal probability of 25%. The whole scheme must thus be repeated 2 times in average before a Bell state is obtained. Indeed, the number of repetitions before we successfully obtain a Bell state is equal to $(\frac{1}{2})+2(\frac{1}{2})^2+3(\frac{1}{2})^3+\cdots$, a series which is the Taylor expansion of the function $x/(1-x)^2$ around 0 evaluated in $x=\frac{1}{2}$. It rapidly converges to 2.

## III. FROM FLYING QUBITS TO FLYING QUDITS, WITH *d* ARBITRARY

### A. Flying-qudit scheme in prime dimensions

Before we generalize the qubit scheme to pairs of qudits, with $d$ an arbitrary dimension higher than 2, we shall first focus on a special case, when $d$ is a prime number. Subsequently we shall generalize this construction to arbitrary dimensions $d$ due to the factorization property that will be established in the next section.

Before we treat the case where $d$ is a prime number, let us first point out that in the qubit case, we introduced at the beginning of the preceding section three (photonic) bases: The $A$, $B$, and computational bases.

These bases are pairwise equally balanced. The natural generalization of the equal balance is called mutual unbiasedness: 2-qudit bases are said to be mutually unbiased whenever the modulus of the in products between states from different bases is always equal to $\frac{1}{\sqrt{d}}$. For instance, when $d=2$ there exists a well-known set of three mutually unbiased bases that presents many applications in quantum information. Those bases are the eigenbases of the Pauli spin operators. When they are represented on the Bloch sphere they correspond to antipodal pairs of points along the $X$, $Y$, and $Z$ directions,

$$|0\rangle_X = \frac{1}{\sqrt{2}}(|0\rangle_Z + |1\rangle_Z),$$

$$|1\rangle_X = \frac{1}{\sqrt{2}}(|0\rangle_Z - |1\rangle_Z),$$

$$|0\rangle_Y = \frac{1}{\sqrt{2}}(|0\rangle_Z + i|1\rangle_Z),$$

$$|1\rangle_Y = \frac{1}{\sqrt{2}}(|0\rangle_Z - i|1\rangle_Z) \tag{8}$$

Here the $Z$ basis plays the role of the computational basis. The states of those bases can be physically implemented by spin-up and spin-down states along three orthogonal directions $X$, $Y$, and $Z$, for instance, by a Stern-Gerlach filtering process. They can also be realized by filtering photonic polarizations. For instance, if the computational basis corresponds to linearly polarized photons along two coplanar and orthogonal directions $(0, \frac{\pi}{2})$, the two other mutually unbiased polarization bases correspond to linear diagonal $(\frac{\pi}{4}, \frac{3\pi}{4})$ and circular (left, right) polarizations.

It is easy to check from Eq. (1) that the relation between the $A$ and computational bases for the photon from the region $A$ is similar to the relation between $X$ and $Z$ bases on the Bloch sphere. Similarly, the $B$ basis and the computational basis of the $B$ photon are oriented relative to each other just as the $Z$ and $Y$ bases (the order matters). As we see, three

mutually unbiased spin bases are involved in the flying-qubit scheme. We shall now generalize the qubit construction to prime-dimensional Hilbert spaces. In order to do so, we shall construct generalized Bell states that are mutually unbiased relatively to the products of states from the local $A$ and $B$ computational bases. We shall show this by making use of well-known properties of mutually unbiased bases and of certain specific properties of finite fields. Despite of the fact that we shall refer to certain properties of finite fields without necessarily establishing them firmly in order to give to the reader some clues concerning our derivation, all of our results will be proven integrally and self-consistently.

As is well known, for all dimensions $d$ larger or equal to 2, one can always find at least three mutually unbiased bases. An explicit expression for $d+1$ of them (in even and odd prime power dimensions $d=p^m$ with $p$ prime) is, for instance, derived in Refs. [13,14].

In even prime dimension (the qubit case) we presented such a triplet of bases in the preceding section.

In odd prime dimensions, a straightforward generalization of the $X$-, $Y$-, and $Z$-qubit bases can be found making use of the results presented in Ref. [15]. The first of them is the computational basis, $|e_k\rangle$, $k=0,\ldots,d-1$; the second one is its discrete Fourier transform, $|f_k\rangle=(\frac{1}{\sqrt{d}}\Sigma_{j=0}^{d-1}\gamma_d^{kj}|e_j\rangle)$; and the third one is defined as follows: $|g_k\rangle=(\frac{1}{\sqrt{d}}\Sigma_{j=0}^{d-1}\gamma_d^{aj^2}\gamma_d^{kj}|e_j\rangle)$, with $a$ chosen at our convenience between all integers strictly comprised between 0 and $d$, and $\gamma_d$ is the $d$th root of unity $e^{2\pi i/d}$. It is worth noting that for this choice of $\gamma_d$, the following identities are satisfied: $\gamma_d^{kj}=\gamma_d^{kj}$, $\forall\ k,j\in Z$ and $\gamma_d^k\gamma_d^j=\gamma_d^{k+j}$, $\forall\ k,j\in Z$, where all the powers of $\gamma$ are taken modulo $d$.

Moreover, the addition and multiplication between integers modulo $d$ are known to form a finite field when $d$ is a prime number. This is due among others to the fact that every element of the field (every integer between 0 and $d-1$) different from 0 (the neutral element for the addition) possesses an invert multiplicative element. This property is realized by modulo $d$ operations only when $d$ is a prime number.

In order to prove that the three bases defined above are mutually unbiased relatively to each other, we shall make use of the properties of Gauss sums. These sums are a discrete generalization of the integral of Gaussian functions. They can be derived in odd prime power dimensions $d=p^m$, making use of the properties of finite fields with $d$ elements $\mathcal{G}(p^m)$ (see, e.g., Eq. 5, p. 2, Ref. [16]) in which case they are expressed through the following identity:

$$\Big|\sum_{k\in\mathcal{G}(p^m)} e^{2\pi i/p\ \mathrm{Tr}(ak^2+bk)}\Big|=\sqrt{p^m} \tag{9}$$

with $a\neq 0$, $\mathrm{Tr}(\eta)=\eta+\eta^p+\eta^{p^2}+\cdots+\eta^{p^{m-1}}$, $\eta\in\mathcal{G}(p^m)$, the Galois field with $p^m$ elements.

In odd prime dimensions ($m=1$, $d=p$), the field operations reduce to the usual operations modulo $p$, the elements of the field are integers comprised between 0 and $d-1$ and the field-theoretical trace of an element $\eta$ can be shown to be equal to $\eta$. Besides, $\gamma_d=e^{2\pi i/d}$, with $d$ odd and prime and there is no other divider of 0 regarding the modulo $d$ multiplication except 0 itself. In particular, $a$ does not divide 0 with $a$ an integer strictly comprised between 0 and $d$. This allows us to prove by a direct computation the identity (9) in odd prime dimensions. Then,

$$\begin{aligned}
\Big|\sum_{k=0}^{d-1}\gamma_d^{(ak^2+bk)}\Big|^2 &= \Big(\sum_{k=0}^{d-1}\gamma_d^{(ak^2+bk)}\Big)\Big(\sum_{k'=0}^{d-1}\gamma_d^{(-ak'^2-bk')}\Big)\\
&= \Big(\sum_{k,k'=0}^{d-1}\gamma_d^{(ak^2+bk-ak'^2-bk')}\Big)\\
&= \Big(\sum_{k'=k+j;k,j=0}^{d-1}\gamma_d^{[-ak^2+bk-a(k+j)^2-b(k+j)]}\Big)\\
&= \Big(\sum_{k,j=0}^{d-1}\gamma_d^{(2akj-bj-aj^2)}\Big)=\Big(\sum_{j=0}^{d-1}d\,\delta_{2aj0}^{Kr}\gamma_d^{(-bj-aj^2)}\Big)\\
&= d\Big(\sum_{j=0}^{d-1}\delta_{j0}^{Kr}\gamma_d^{(-bj-aj^2)}\Big)=d\gamma_d^0=d
\end{aligned} \tag{10}$$

In the previous derivation, we implicitly made use of the fact that in odd prime dimension $d$ and with $a$ strictly comprised between 0 and $d$, $a$ is not a divider of 0 modulo $d$, and also of the cyclic cancellation $\Sigma_{k=0}^{d-1}\gamma_d^{kl}=d\,\delta_{l0}^{Kr}$, valid in any dimension [14]. It is easy to prove the latter identity making use of the properties of the truncated geometrical series, $(1-\gamma_d^l)\Sigma_{k=0}^{d-1}\gamma_d^{kl}=1-\gamma_d^{ld}=0$, and $1-\gamma_d^l\neq 0$ unless $l=0$ in which case $\Sigma_{k=0}^{d-1}\gamma_d^{kl}=d$.

Let us now prove, making use of the Gauss identity in (9) and (10), that the second and the third bases are mutually unbiased relatively to each other. We have $|\langle f_{k'}|g_k\rangle|=|(\frac{1}{d}\Sigma_{j=0}^{d-1}\gamma_d^{-k'j}\gamma_d^{aj^2}\gamma_d^{kj})|=|(\frac{1}{d}\Sigma_{j=0}^{d-1}\gamma_d^{aj^2+(k-k')j})|=\frac{1}{\sqrt{d}}$, in virtue of the identity (10).

In order to generalize the qubit case to higher dimensions $d=p$ with $p$ odd and prime, we must observe that the states $|f_k\rangle$ generalize the $X$ basis while the states $|g_k\rangle$ generalize the $Y$ basis. This will allow us to generalize the $A$- and $B$-qubit bases defined in Eq. (1), keeping in mind that, as noted before, (i) the relation between the $A$ and computational basis for the photon from the region $A$ is similar to the relation between $X$ and $Z$ bases; (ii) the $B$ basis and the computational basis of the $B$ photon are oriented relative to each other just as the $Z$ and $Y$ bases. Replacing the states of the qubit $Z$ (computational) basis by the qudit $|e_k\rangle$ states, the states of the qubit $X$ basis by the qudit $|f_k\rangle$ states, and the states of the qubit $Y$ basis by the qudit $|g_k\rangle$ states, the definition of the qudit generalized $A$ and $B$ bases are straightforward,

$$|A_k\rangle=|f_k\rangle=\left(\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\gamma_d^{kj}|e_j\rangle\right),$$

$$|B_k\rangle=|g_k^{-1}\rangle=\left(\frac{1}{\sqrt{d}}\gamma_d^{-ak^2}\sum_{j=0}^{d-1}\gamma_d^{-kj}|e_j\rangle\right)\quad\text{with}\ \ a\neq 0. \tag{11}$$

The symbol $|g_k^{-1}\rangle$ means that the $B$ basis is to the computational basis $e$ what the computational basis $e$ is to the third

mutually unbiased basis (MUB) (the $g$ basis).

We can now prove that the generalized Bell states $|B_{ij}\rangle$ constructed with the $A$ and $B$ bases are mutually unbiased relatively to the 2-qudit product states of the computational basis states, which is the required property in order to generate entanglement thanks to flying qudits, $|B_{ij}\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\gamma_d^{jk}|A_k\rangle|B_{k+i}\rangle$ ($\gamma_d = e^{2\pi i/d}$), so that, making use of (10),

$$|\langle e_m e_n|B_{ij}\rangle| = \frac{1}{\sqrt{d^3}}|\sum_{k=0}^{d-1}\gamma_d^{jk}\langle e_m e_n|A_k B_{k+i}\rangle|$$
$$= \frac{1}{\sqrt{d^3}}|\sum_{k=0}^{d-1}\gamma_d^{jk}\gamma_d^{mk}\gamma_d^{-a(k+i)^2}\gamma_d^{-n(k+i)}| = 1/d. \tag{12}$$

If it is possible experimentally to repeat the flying-qubit scheme in odd prime dimension $d$, so as to say (1) to duplicate the level of a $d$ level atom at the level of a flying photon (with $d$ levels perhaps as angular momentum) and (2) to measure a pair of photons in a basis in which at least one eigenstate is a qudit Bell state and other eigenstates are factorizable, then a qudit computer in odd prime dimension $d$ with distant single photon sources would obviously be realizable. We mean hereby that it would be concretely possible to implement a maximally entangling conditional phase gate that generalizes its qubit counterpart.

Indeed, let us assume that two distant two-level atoms are prepared in the factorizable state $|\psi\rangle^{A_a}|\phi\rangle^{B_a} = \sum_{k,l=0}^{d-1}\alpha_k|k\rangle^{A_a}\gamma_l|l\rangle^{B_a}$, and that each of them emits a photon which is entangled with the $d$ levels of the atom, $|\psi\rangle^{A_a}|\phi\rangle^{B_b} \to \sum_{k,l=0}^{d-1}\alpha_k|k\rangle^{A_a}|k\rangle^{A_p}\gamma_l|l\rangle^{B_a}|l\rangle^{B_p}$.

Let us then measure the two photons in a joint, 2-qudit, measurement that possesses at least an eigenstate of the form $|B_{ij}\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\gamma_d^{jk}|A_k\rangle|B_{k+i}\rangle$ ($\gamma_d = e^{2\pi i/d}$) that is maximally entangled and equally balanced relatively to the computational basis (due to equal balance, this state can always be written in the form $\frac{1}{d}\sum_{k,l=0}^{d-1}e^{i\phi_{kl}}|k\rangle^{A_p}|l\rangle^{B_p}$) and obtain the corresponding eigenvalue so that the atomic states are projected onto the state $\sum_{k,l=0}^{d-1}\alpha_k\gamma_l e^{-i\phi_{kl}}|k\rangle^{A_a}|l\rangle^{B_a}$. This is equivalent to the unitary transformation

$$|k\rangle^{A_a}|l\rangle^{B_a} \to e^{-i\phi_{kl}}|k\rangle^{A_a}|l\rangle^{B_a}. \tag{13}$$

Such a transformation is maximally entangling. For instance, when the qudits are both prepared in the first state of the Hadamard basis (or generalized $X$ basis, the $f$ basis in our notations), $|\psi\rangle^{A_a}|\phi\rangle^{B_a} = \frac{1}{\sqrt{d}}(\sum_{k=0}^{d-1}|k\rangle^{A_a})\frac{1}{\sqrt{d}}(\sum_{l=0}^{d-1}|l\rangle^{B_a})$, they are transformed, after the completion of the full process, to the state $\frac{1}{d}\sum_{k,l=0}^{d-1}e^{-i\phi_{kl}}|k\rangle^{A_a}|l\rangle^{B_a}$ which is maximally entangled.

Obviously all of this process resorts to the implementation of a maximally entangling phase conditional (MECP) gate that generalizes to higher (odd prime in this case) dimensions the flying-qubit scheme.

Moreover, a flying-qudit scheme would even be possible for arbitrary value of $d$ as we shall now show.

### B. Flying-qudits process, with $d$ arbitrary

#### 1. Factorization into elementary flying-qudit schemes with d prime

In order to generalize to arbitrary dimension $d$ the construction of the preceding sections that were valid in even and odd prime dimensions, two ingredients are needed:

(i) When the dimension $d$ factorizes into a product of two dimensions $d_1$ and $d_2$ ($d = d_1 d_2$), we define generalized qudit Bell states in such a way that they factorize into products of qu$d_1$it Bell states and qu$d_2$it Bell states.

(ii) If we find bases of qu$d_1$it Bell states and qu$d_2$it Bell states that are mutually unbiased relatively to the products of states from the local $A$ and $B$ qu$d_1$it and, respectively, qu$d_2$it computational bases, their products are mutually unbiased relatively to the products of states from the local $A$- and $B$-qudit computational bases (with $d = d_1 d_2$).

Let us now prove the factorization properties (i) and (ii).

#### 2. Property (i): Factorization of Bell states

A way to define factorizable Bell states is first to define the qudit Bell state $|B_{00}^{AB}\rangle$ as $\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}|a_k^A\rangle|b_k^B\rangle$, where $|a_k^A\rangle$ and $|b_k^B\rangle$ factorize versus the tensorization $d_1$ times $d_2$. Obviously such a state is factorizable,

$$\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}|a_k\rangle|b_k\rangle = \frac{1}{\sqrt{d_1 d_2}}\sum_{k=0}^{d_1-1}\sum_{k'=0}^{d_2-1}|a_k^1\rangle|a_{k'}^2\rangle|b_k^1\rangle|b_{k'}^2\rangle$$
$$= \frac{1}{\sqrt{d_1}}\sum_{k=0}^{d_1-1}|a_k^1\rangle|b_k^1\rangle\frac{1}{\sqrt{d_2}}\sum_{k'=0}^{d_2-1}|a_{k'}^2\rangle|b_{k'}^2\rangle.$$

Besides, the Bell states $|B_{i,j}^{AB}\rangle$ are obtained from the state $|B_{00}^{AB}\rangle$ by letting displacement operators act on it, $|B_{ij}^{AB}\rangle = (V_i^j)^B|B_{00}^{AB}\rangle$, where the displacement operators are defined [14] in such a way that they factorize

$$V_{i_1 i_2}^{j_1 j_2} = V_{i_1}^{j_1}V_{i_2}^{j_2}, \tag{14}$$

where $i_1$ and $j_1$ ($i_2$ and $j_2$) vary from 0 to $d_1 - 1$ ($d_2 - 1$) and

$$V_{i_{1,2}}^{j_{1,2}} = \sum_{k=0}^{d_{1,2}-1}\gamma_{d_{1,2}}^{(kj_{1,2})}|k + i_{1,2}\rangle\langle k|; i_{1,2}, j_{1,2}: 0 \cdots d_{1,2} - 1 \tag{15}$$

(here addition and multiplication are defined modulo $d_{1,2}$ while $\gamma_{d_{1,2}}$ is the $d_{1,2}$th root of unity $e^{2\pi i/d_{1,2}}$).

Given that the generalized Bell states are obtained from the Bell state $|B_{00}^{AB}\rangle$ by letting act on it tensorial products of displacement operators, the maximal entanglement of the Bell basis is guaranteed by construction.

It is worth noting that other possible generalizations of Bell states can possibly be considered [14], in particular when the dimension is a power of a prime; in our approach we privileged one of them that presents the advantage that although the 2-qudit subsystems in a Bell state are maximally entangled, the $d_1$ and $d_2$ subsytems inside the qudit subsystems are not entangled with each other (the full state factorizes into a product of a 2-qu$d_1$it Bell state and a 2-qu$d_2$it Bell state).

#### 3. Property (ii): Factorization of mutual unbiasedness

The validity of the property (ii) is established as follows: Obviously the computational basis in dimension $d=d_1d_2$ factorizes into a product of local computational bases. Besides, let us choose the $a$ and $b$ bases in accordance with the special choice defined at the level of Eq. (11). We obtain the primed Bell states defined by $|B'^{AB}_{ij}\rangle=(V^j_i)^B|B'^{AB}_{00}\rangle$, where $|B'^{AB}_{00}\rangle=\frac{1}{\sqrt{d}}\Sigma_{k,k'=0}^{d-1}|A^1_k\rangle^A|A^2_k\rangle^A|B^1_{k'}\rangle^B|B^2_{k'}\rangle^B$. Such states factorize into products of local Bell states as a consequence of the property (i) and the local (local relatively to the tensorization $d_1$ times $d_2$) Bell states are known to be mutually unbiased relatively to the product of the $A$ and $B$ local computational basis states $|e^1_k\rangle^A|e^1_k\rangle^B$ and $|e^2_k\rangle^A|e^2_k\rangle^B$. The primed Bell states $|B'^{AB}_{ij}\rangle$ are thus mutually unbiased relatively to the $A$-$B$ computational basis because when $d=d_1d_2$, $\frac{1}{\sqrt{d}}=\frac{1}{\sqrt{d_1}}\frac{1}{\sqrt{d_2}}$. Roughly speaking, as Bell states, computational states, as well as mutual unbiasedness factorize relatively to the tensorization $d_1$ times $d_2$, the Bell states are mutually unbiased relatively to the computational basis.

The generalization to arbitrary dimension follows in a straightforward manner, due to the fact that all integers can always be expressed as products of prime numbers. A key ingredient for generalizing the qubit-flying scheme is that the Bell states $|B'^{AB}_{ij}\rangle$ obtained by displacing the Bell states $|B'^{AB}_{00}\rangle$ are maximally entangled because so is $|B'^{AB}_{00}\rangle$, and because the displacement operators factorize into local operators in the $A$ and $B$ regions. One can then show how to implement a MECP gate following exactly the same steps as in the prime-dimensional case.

We obtain a MECP gate that obeys Eq. (13).

## IV. A FEASIBLE GENERALIZATION: $m$ ENTANGLED QUBITS

As we have shown in the preceding section, generalizations to arbitrary dimensions higher than 2 (3, 4, 5, 6, and so on) of the flying-qubit scheme are in principle possible. Nevertheless, presently, only the case of composite qubit systems is realizable experimentally because the process requires to measure qudit Bell states and, presently, this is only feasible when $d=2$. Therefore the many-qubit case will be treated separately in this section.

As a consequence of factorizability, we now know that when a qudit consists of $m$ qubits (then $d=2^m$) it is possible to implement the MECP gate onto $2^m$ dimensional qudits by acting onto $m$ pairs of qubits separately. The trick is simply to consider two groups of $m$ atomic qubits that we label from 1 to $m$ at each side and to repeat the flying-qubit procedure $m$ times between pairs of equally labeled qubits. In Fig. 2, we sketch the process that consists of realizing in parallel $m$ flying-qubit processes. Of course this requires to project flying qubits (photons) onto Bell states (each horizontal arrow refers to the elementary process represented in Fig. 1 and horizontal circles refer to the missing $m-4$ processes that were not explicitly represented), a process which does not always work, but atoms are stable and once the entanglement of a pair is made, they are not likely to disentangle easily so that we could still have some insurance to entangle the other atoms before decoherence disentangles the two atoms.

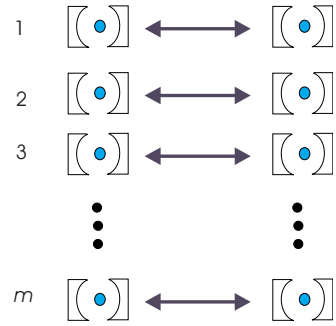


FIG. 2. (Color online) Maximal entanglement of a pair of $2^m$-dimensional qudits by acting onto $m$ pairs of qubits separately.

On average the number of iterations required for implementing a generalized phase conditional gate between two groups of $m$ atoms is an increasing function of $m$. We shall now show how to derive a recursive relation between the average repetition times necessary in order to successfully implement $m$ gates in parallel (so to say between the average repetition times $\langle T^m\rangle$ necessary in order to succeed in measuring $m$ times a Bell state during a repeat-until-success procedure in which $m$ pairs of atoms are present).

Our reasoning goes as follows: In order to implement successfully the 2-qubit MECP gate, we must implement successfully 2 times the 1-qubit MECP gates, a process that can be decomposed in three elementary nonoverlapping processes: (i) The two MECP gates are successfully realized at the first attempt (the probability therefore is equal to 1/4); (ii) at the first attempt only one of the individual gates is successfully realized (the probability therefore is equal to 2 times 1/4); (iii) none of the gates is successfully realized.

The contribution of the process (i) to the average time is $\frac{1}{4}$. The contribution of the process (ii) to the average time is $\frac{1}{2}(1+\langle T^1\rangle)$ where $\langle T^1\rangle$ is the average time necessary for successfully implementing the gate onto the second pair of qubits. The contribution of the process (iii) to the average time is $\frac{1}{4}(1+\langle T^2\rangle)$ because the first attempt failed completely so that we must still implement the gates for the pair of qubits which requires by definition an average time $\langle T^2\rangle$. Setting all of this together we obtain $\langle T^2\rangle=\frac{1}{4}+\frac{2}{3}(1+\langle T^1\rangle)+\frac{1}{4}(1+\langle T^2\rangle)$.

The reasoning can be generalized to the implementation of $m$ gates, and we arrive to the recursive relation

$$\langle T^m\rangle=\sum_{j=0}^{m}C^m_j(1/2)^m(\langle T^j\rangle+1)\quad(\text{where}\langle T^0\rangle=0),\quad(16)$$

by separating the process into elementary independent processes where $m-j$ gates were successfully implemented after one attempt (or equivalently there were $j$ failures).

The average number of iterations is, for instance, equal to 2 when $m=1$ (in accordance with the estimation made in Ref. [8] and with our alternative derivation at the end of the section devoted to the original flying-qubit scheme), $(\frac{8}{3})$ when $m=2$, and to $(\frac{22}{7})$ when $m=3$.

In Fig. 3, we plot the average repetition time when $m$ varies from 2 to 20 that were obtained by solving the recur-

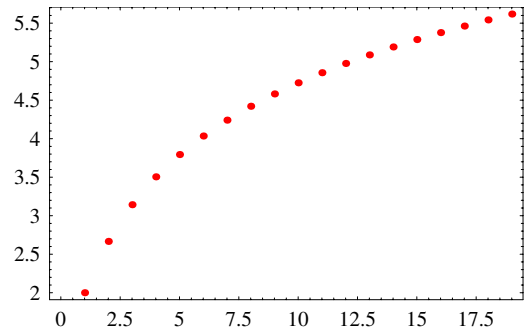


FIG. 3. (Color online) Graph of the average iteration (repetition time) for entangling $m$ pairs of qudits plotted in function of $m$.

sive relation. Using this relation, we can express the average value $\langle T^m \rangle = \frac{s_m}{\Pi_{i=1}^{m}(2^i-1)}$ where the sequence $s_m$ takes the values 2, 8, 66, 1104, 37 050, etc., for $m=1,2,\ldots$. The value obtained for $m=50$ is equal to 6.990 977 903 42.

The average time of repetition is obviously much shorter than 100, 50 times the repetition time corresponding to one pair of qubits ($m=1$). This is an encouraging result in relation with the scalability of the flying-qudit scheme. The reason why the number of iterations necessary for entangling a pair of $m$ qubits is necessarily less than $m$ times the time required for entangling one pair is that the operations can be treated in parallel.

It is expected that for large $m$ the scaling is logarithmic, and not linear as we would get for tasks to perform in series. In order to motivate this hypothesis, we shall consider situations such that $m$ is relatively large (say larger than $m_0$, taken large enough) so that $\langle T^m \rangle$ is large enough.

Let us assume in a first time that the time necessary for implementing $m$ gates in parallel is exactly equal to $\langle T^m \rangle$. The chance is high that during the time $\langle T^m \rangle m+1$ gates are successfully implemented because the probability that this does not occur is very low [it is close to $(\frac{1}{2})^m$]. Therefore $\langle T^{m+1} \rangle$ is likely to remain close to $\langle T^m \rangle$, and in a first approximation, $\langle T^{m+1} \rangle - \langle T^m \rangle \approx (\frac{1}{2})^{\langle T^m \rangle} \langle T^1 \rangle = 2(\frac{1}{2})^{\langle T^m \rangle}$, a small number when $\langle T^m \rangle$ is sufficiently large.

The assumption that the time necessary for implementing successfully $m$ gates in parallel is of course somewhat crude; actually it is not so easy to compute the distribution of times necessary for implementing successfully $m$ gates in parallel.

If, for instance, we would consider that this time is homogeneously distributed between say $[\langle T^m \rangle - 2, \langle T^m \rangle + 2]$ or, alternatively, $[\langle T^m \rangle - 3, \langle T^m \rangle + 3]$ we would get that

$$\langle T^{m+1} \rangle - \langle T^m \rangle \approx \alpha \left( \frac{1}{2} \right)^{\langle T^m \rangle}, \tag{17}$$

where $\alpha \approx 1.4$ We estimated numerically the value of this factor and found that it remains confined in the interval [3.338 51, 3.597 62] and slowly increases when $m$ varies from 5 to 50, which suggests that we can safely upper bound $\langle T^{m+1} \rangle - \langle T^m \rangle$ by say $4(\frac{1}{2})^{\langle T^m \rangle}$.

We can in a next step transform the bound obeyed by the difference $\langle T^{m+1} \rangle - \langle T^m \rangle$ into a differential equation of the form $2^{\langle T^m \rangle} d\langle T^m \rangle < 4dm$. Integrating over $m$ for $m$ larger than $m_0$, we find $2^{T^m} - 2^{T^{m_0}} < 4 \ln 2(m-m_0)$. This shows that for large $m$ the average implementation time grows logarithmically and not linearly, in good qualitative agreement with the numerical results that we obtained through the (exact) recursive relation. It is easy to understand why the average repetition time increases logarithmically and not linearly: When the task is realized in parallel the probability is high that it is successfully achieved more or less at the same time at each sublevel. The probability that the task is not realized at one sublevel after a time $T$ decreases exponentially in a function of $T$. Therefore, the rate of increase of $\langle T^m \rangle$ as a function of $m$ constantly decreases for increasing $m$.

## V. CONCLUSIONS

We have shown that in principle the flying-qubit scheme can be generalized to arbitrary dimensions. In particular, our analysis established that the $m$-qubit scheme reduces to the parallel implementation of the original flying-qubit scheme [8] so that it is feasible experimentally, because the 2-qubit scheme is presently feasible (see Refs. 8, 12–15 of Ref. [8]). The time necessary for implementing the MECP gate onto a pair of $2^m$-dimensional systems is on average largely inferior to $m$ times the time necessary for entangling one pair of qubits, which shows that this approach is promising from the point of view of scaling [17].

We have made use in our derivation of the fact that when we prepare a Bell state in which a $m$-qubit state (in a region $A$) is maximally entangled with another $m$-qubit state (in a region $B$), the full Bell state factorizes into $m$ products of maximally entangled qubits, a result that is counterintuitive at first sight but is intimately related to entanglement swapping. Thus, beside scalability, this factorization property is another advantage of our approach: The whole scheme is practically feasible although all atoms remain far away from each other, while no photon coincidence detections of order higher than two are required.

All our analysis shows that such operations with insurance are well suited for dealing with composite systems. It can be shown that the 2-qudit MECP gate coupled to local qudit transformations would allow us to generate arbitrary $2d$ times $2d$ unitaries. When $d$ differs from 2 this is a direct consequence of the main theorem of Ref. [18], where it has been proven that any unitary interaction that entangles two qudits (so to say that does not preserve the factorization of all initially factorizable 2-qudit states) can generate, when it is combined to local (1-qudit) unitaries, arbitrary $m$-qudit gates (unitaries). Actually in the qubit case this is a well-known property of the MECP or Ising gate [11] that has been systematically exploited in, for instance, the conception of the one-way quantum computer [19]. Although certain arbitrary $m$-qudit unitaries could appear to be difficult to implement concretely making use of the flying-qudit approach, our scheme makes it possible to let interact degrees of freedom that otherwise would remain decoupled; considered so, we believe that it could provide an economic and tractable manner for generating useful interactions between distant atoms that could find interesting applications in quantum computing.

Finally it is worth noting that it could be possible in principle to realize the flying-qutrit scheme with three-level atoms that emit photons of classical orbital momentum equal to 1. Several progresses were already achieved in the past with such photons (for instance, 2-qutrits entanglement). It is possible presently [20] to produce experimentally such entangled ternary quantum systems (qutrits) for quantum key distribution. The qutrits are encoded into the orbital angular momentum of photons, namely Laguerre-Gaussian modes with azimuthal index l, +1, 0, and −1, respectively. The orbital angular momentum is controlled with phase holograms. Moreover, combining flying qubits and qutrits does not seem to be an impossible task, opening new possibilities in the flying-qudit approach.

One of the authors (T.D.) acknowledges support from the Flemish Fund for Scientific Research (FWO), the ICT Impulse Program of the Brussels Capital Region (Project Cryptasc), the IUAP program of the Belgian government, the Solvay Institutes for Physics and Chemistry and the Quantum Laboratory at NUS, as well as technical help from Samuel Colin (Perimeter Institute), and fruitful discussions with Wee Kang Chua (Quantum Laboratory) about the subject. Two of the authors (D.K., L.C.K.) acknowledge support by the National Research Foundation and Ministry of Education, Singapore. We are pleased to thank A. Beige and Y-L. Lim (Imperial College) who drew our attention on the interest of the subject and suggested to one of the authors (T.D.) to analyze the qubit scheme at the light of the properties of finite (Galois) fields.

[1] E. Knill, R. Laflamme, and G. Milburn, Nature (London) **409**, 46 (2001).

[2] D. Gottesman and I. L. Chuang, Nature (London) **402**, 390 (1999).

[3] M. I. Dyakonov, in *Future Trends in Microelectronics. Up the Nano Creek*, edited by S. Luryi, J. Xu, and A. Zaslavsky (Wiley, New York, 2007), pp. 4–18; see also M. I. Dyakonov, e-print arXiv:quant-ph/0610117v1.

[4] It has been shown that a quantum computer begins to be competitive relatively to presently existing classical computers when it is implementable on at least [3] $10^{12}$ qubits due to the fact that 300 digit numbers corresponds to more or less a 1000-bit number, and that its factorization through Shore's algorithm implies a need for a $10^{12}$ to $10^{18}$ qubit realistic computer that incorporates error correction mechanisms [3].

[5] N. Yoran and B. Reznik, Phys. Rev. Lett. **91**, 037903 (2003); M. A. Nielsen, e-print arXiv:quant-ph/0402005; D. E. Browne and T. Rudolph, Phys. Rev. Lett. **95**, 010501 (2005).

[6] E. Knill, R. Laflamme, and G. Milburn, e-print arXiv:quant-ph/0006120.

[7] T. B. Pittman, B. C. Jacobs, and J. D. Franson, Phys. Rev. Lett. **88**, 257902 (2002); J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning, Nature (London) **426**, 264 (2003).

[8] Y.-L. Lim, A. Beige, and L.-C. Kwek, Phys. Rev. Lett. **95**, 030505 (2005); see also Y-L. Lim, A. Beige, and L-C. Kwek, e-print arXiv:quant-ph/0408043.

[9] Y.-L. Lim, S.-D. Barret, A. Beige, P. Kok, and L.-C. Kwek, Phys. Rev. A **73**, 012304 (2006).

[10] I. E. Protsenko, G. Reymond, N. Schlosser, and P. Grangier, Phys. Rev. A **66**, 062306 (2002); G. Reymond, N. Schlosser, I. Protsenko, and P. Grangier, Philos. Trans. R. Soc. London, Ser. A **361**, 1527 (2003).

[11] D. P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).

[12] N. Lutkenhaus, J. Calsamiglia, and K.-A. Suominen, Phys. Rev. A **59**, 3295 (1999).

[13] T. Durt, e-print arXiv:quant-ph/0401046.

[14] T. Durt, J. Phys. A **38**, 5267 (2005).

[15] I. D. Ivonovic, J. Phys. A **14**, 3241 (1981).

[16] H. C. Rosu, M. Planat, M. Saniga, AIP Conf. Proc. **734**, 315 (2004)

[17] In Ref. [8], the scalability of the 2-qubit process was already addressed in relation with the so-called cluster state quantum computer [19].

[18] J.-L. Brylinski and R. Brylinski, e-print arXiv:quant-ph/0108062.

[19] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).

[20] S. Groeblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, e-print arXiv:quant-ph/0511163.