Immunity of information encoded in decoherence-free subspaces to particle loss

Piotr Migdał\textsuperscript{1,2} and Konrad Banaszek\textsuperscript{1}

\textsuperscript{1}Instytut Fizyki Teoretycznej, Wydział Fizyki, Uniwersytet Warszawski, Hoża 69, PL-00-681 Warszawa, Poland

\textsuperscript{2}ICFO–Institut de Ci\`encies Fot\`oniques, 08860 Castelldefels (Barcelona), Spain

(Dated: January 31, 2013)

We demonstrate that for an ensemble of qudits, subjected to collective decoherence in the form of perfectly correlated random SU(d) unitaries, quantum superpositions stored in the decoherence free subspace are fully immune against the removal of one particle. This provides a feasible scheme to protect quantum information encoded in the polarization state of a sequence of photons against both collective depolarization and one photon loss, which can be demonstrated with photon quadruplets using currently available technology.

PACS numbers: 03.67.Hk, 03.67.Pp, 42.50.Ex, 42.50.Dv

\section{I. INTRODUCTION}

Quantum systems are powerful yet fragile carriers of information. The ability to create and manipulate superposition states offers verifiably secure cryptography\cite{1}, reduces the complexity of certain computational problems\cite{2}, and enables novel communication protocols\cite{3}. However, in practical settings one needs to protect the quantum states carrying information against decoherence, i.e. uncontrolled interactions with the environment. This is accomplished by building redundancy into the physical implementation. Compared to the classical case, this task is much more challenging\cite{4} due to limitations in handling quantum information, exemplified boldly by the no-cloning theorem\cite{5}.

When an ensemble of elementary quantum systems decoheres through symmetric coupling with the environment, one can identify collective states that remain invariant in the course of evolution. These states span a so-called decoherence-free subspace (DFS) that is effectively decoupled from the interaction with the environment\cite{6}. More generally, it is possible to identify subspaces that can be formally decomposed into a tensor product of two subsystems, one of which “absorbs” decoherence, while the second one, named a noiseless subsystem or a decoherence-free subsystem, remains intact\cite{7}.

In this paper we consider the DFS for an ensemble of $n$ qudits, i.e. elementary $d$-level systems, composed of states $|\Psi\rangle$ that are invariant with respect to an arbitrary perfectly correlated SU($d$) transformation:

$$\hat{U}^\otimes n |\Psi\rangle = |\Psi\rangle, \quad \hat{U} \in \text{SU}(d).$$

We show that this DFS features an additional degree of robustness, namely that the stored quantum information is immune to the loss of one of the qudits, regardless of the encoding. This result, specialized to the polarization state of single photons for which $d = 2$, offers combined protection against two common optical decoherence mechanisms: photon loss\cite{8} due to reflections, scattering, residual absorption, etc. as well as collective depolarization that occurs inevitably in optical fibers used for long-haul transmission\cite{9,10}. Consequently, we provide here rigorous foundations to a speculation presented in Ref.\cite{11} that DFS-based quantum cryptography can be made tolerant also to photon loss. It is worth noting that another physical realization of the qubit case can be also an ensemble of spin-$1/2$ particles\cite{12} coupled identically to a varying magnetic field.

The paper is organized as follows. First, in Sec.\textsuperscript{II} we briefly review the geometry of the singlet subspace for an ensemble of qubits and we explicitly show the robustness of the four qubit DFS, which spans the logical qubit space. This particular case leads us to a proposal for a proof-of-principle experiment based on currently available photonic technologies that demonstrates the robustness of DFS encoding, presented in Sec.\textsuperscript{III}. The general proof for an arbitrary $d$ that a quantum superposition encoded in an SU($d$) DFS remains immune against the loss of one particle is described in Sec.\textsuperscript{IV}. Finally, Sec.\textsuperscript{V} concludes the paper.

\section{II. SINGLET SUBSPACE FOR QUBITS}

Because of two relevant physical realizations using photons and spin-1/2 particles, we will first discuss the qubit case with $d = 2$. The complete Hilbert space of an ensemble of $n$ qubits, each described by a two-dimensional spin-1/2 space $\mathcal{H}_{1/2}$, can be subjected to Clebsch-Gordan decomposition\cite{13}:

$$\mathcal{H}_{1/2}^\otimes n = \bigoplus_{j=(n \text{ mod } 2)/2}^{n/2} \mathbb{C}^{K_j} \otimes \mathcal{H}_j,$$

where the direct sum is taken with the step of one and $K_j$ are multiplicities of spin-$j$ Hilbert spaces $\mathcal{H}_j$, given explicitly by

$$K_j^n = \frac{2j + 1}{n/2 + j + 1} \binom{n}{n/2 + j}.$$
order to discriminate from the four-qubit DFS defined as products encoding one logical qubit. Let us consider three states main protected from collective depolarization.

\[ |\Xi_1\rangle = |\psi^-\rangle_{12}|\psi^-\rangle_{34}, \]
\[ |\Xi_2\rangle = |\psi^-\rangle_{13}|\psi^-\rangle_{42}, \]
\[ |\Xi_3\rangle = |\psi^-\rangle_{14}|\psi^-\rangle_{23}, \]

where \(|\psi^-\rangle_{ij} = (|01\rangle_{ij} - |10\rangle_{ij})/\sqrt{2}\) is the singlet state of qubits \(i\) and \(j\). These states, shown schematically in Fig. 1, form an overcomplete set in the DFS. For concreteness, let us select \(|\Xi_1\rangle\) and \(|\Xi_3\rangle\) as a non-orthogonal basis. Any state of the logical DFS qubit can be written as a superposition

\[ |\Psi\rangle = \alpha|\Xi_1\rangle + \beta|\Xi_3\rangle, \]

where \(\alpha\) and \(\beta\) are complex amplitudes. Without loss of generality we can assume that the first physical qubit has been lost. The remaining three qubits are described by an equally weighted statistical mixture of two states:

\[ |\Psi^{(0)}\rangle_1 = \alpha|1\rangle_2|\psi^-\rangle_{34} + \beta|\psi^-\rangle_{23}|1\rangle_4, \]
\[ |\Psi^{(1)}\rangle_1 = \alpha|0\rangle_2|\psi^-\rangle_{34} + \beta|\psi^-\rangle_{23}|0\rangle_4, \]

where \(|\rangle_1\) denotes the state of all qubits but the first one. It is easy to see that a collective transformation \(\hat{U} \otimes ^\otimes^3\) leaves the statistical mixture \(\frac{1}{2}|\Psi^{(0)}\rangle_1 \langle |\Psi^{(0)}\rangle + |\Psi^{(1)}\rangle_1 \langle |\Psi^{(1)}\rangle\) intact.

After the loss of the first particle, the initial four-qubit state from Eq. (1) can be recovered through the following procedure. First, one needs to measure in a non-destructive way the \(z\) component of the total pseudospin operator \(\hat{\Sigma}^z = \hat{\Sigma}_1^z + \hat{\Sigma}_2^z + \hat{\Sigma}_3^z\), where \(\hat{\Sigma}^z = |0\rangle_1 \langle 0| - |1\rangle_1 \langle 1|\), in order to discriminate \(|\Psi^{(0)}\rangle\) from \(|\Psi^{(1)}\rangle\). If the result corresponding to \(|\Psi^{(1)}\rangle\) is obtained, we apply a collective rotation \((\hat{\Sigma}^x)^{\otimes^3}\), where \(\hat{\Sigma}^x = |0\rangle_1 \langle 1| + |1\rangle_1 \langle 0|\). This yields the state \(|\Psi^{(0)}\rangle_1\).

\[ (|0\rangle_1 \otimes \mathbb{1}^{\otimes^3} + |1\rangle_1 \otimes (\hat{\Sigma}^x)^{\otimes^3}) (|+\rangle_1 |\Psi^{(0)}\rangle_{1}) = |\Psi\rangle \]

Note that this rotation can be realized as a sequence of three C-NOT gates.

The robustness of DFS to particle loss can be intuitively understood in the following way. DFS states owe their invariance with respect to collective unitary transformation to a very rigid structure. In fact, if we write a DFS state as a superposition in the computational basis for individual qubits, the state of one qubit can be determined unambiguously from the states of the remaining ones. This suggests that the loss of one particle does not destroy any information. Futher, it is always possible to repair the state as there is only one unique way to fit the lost particle such that the singlet symmetry is recovered.

III. EXPERIMENTAL SCHEME

We will now present a proposal a feasible experiment that demonstrates the robustness of DFS encoding using photon quadruplets that can be generated in the process of parametric down-conversion \[10, 14\]. The basis states \(|0\rangle\) and \(|1\rangle\) correspond in this case to horizontal and vertical polarizations of individual photons. Let us consider four-photon states \(|\Xi_k\rangle\), \(k = 1, 2, 3\), defined in Eq. (1) as well as their orthogonal complements in the two-dimensional DFS, which we will denote as \(|\Xi_k^\perp\rangle\). The index \(k\) corresponds to three non-equivalent orderings of the photons and it can be changed by suitable rerouting of the photons. As demonstrated in \[10\], the states \(|\Xi_1\rangle\) and \(|\Xi_3\rangle\) can be discriminated unambiguously by detecting polarizations in the horizontal-vertical basis \((|0\rangle, |1\rangle)\) for photons 12 and in the diagonal basis \((|0\rangle \pm |1\rangle)/\sqrt{2}\) for photons 34. Restricted to the DFS subspace, this strategy yields the standard projective measurement.

It is easy to check that the above individual measurement no longer works if one of the photons is missing. It turns out that this problem can be solved by resorting to collective measurements. Suppose that we interfere photon pairs 12 and 34 on two separate balanced beam splitters, playing the role linear-optics Bell state analyzers \[15\]. The state \(|\Xi_1\rangle\) will yield exactly one photon in each output port of each beam splitter. In contrast, because the orthogonal state \(|\Xi_3^\perp\rangle\) can be written as \[\Xi_3^\perp\rangle = \frac{1}{\sqrt{3}} (|00\rangle_{12} |11\rangle_{34} + |11\rangle_{12} |00\rangle_{34} - |\psi^+\rangle_{12} |\psi^+\rangle_{34}),\]

where \(|\psi^+\rangle_{ij} = (|01\rangle_{ij} + |10\rangle_{ij})/\sqrt{2}\), it will always produce two photons at the same output port for each of the
two beam splitters. If one photon is lost, the states $|Ξ_1\rangle$ and $|Ξ_2\rangle$ will still give distinguishable outcomes: registering two photons at a single output unambiguously heralds $|Ξ_2\rangle$, while registering a photon pair at two different outputs of the same beam splitters detects $|Ξ_1\rangle$. The third photon will emerge separately from the second beam splitter. This detection scheme is summarized in Fig. 2.

An interesting question is whether the scheme described above could be exploited for quantum key distribution. The scalar products between any two states $|Ξ_l\rangle$ and $|Ξ_k\rangle$ with $k \neq l$ are equal to $\langle Ξ_k|Ξ_l\rangle = -\frac{1}{d}$. In the Bloch representation of the two-dimensional DFS, they form a regular triangle inscribed into a great circle on the Bloch sphere, constituting a so-called trine that warrants cryptographic security [11, 16]. To generate a key, the sender Alice could prepare photon quadruplets in one of randomly selected states $|Ξ_1\rangle$, $|Ξ_2\rangle$, or $|Ξ_3\rangle$. The ability to perform a projection onto any pair of orthogonal states $|Ξ_k\rangle, |Ξ_k^\perp\rangle$ would enable the receiving party Bob to tell, in the case when an outcome $|Ξ_k^\perp\rangle$ is obtained, which state has definitely not been prepared by Alice. Such correlations between Alice’s preparations and Bob’s outcomes can be distilled into a secure key.

We have shown that the projective measurement onto $|Ξ_k\rangle, |Ξ_k^\perp\rangle$ can be implemented in a way that tolerates the loss of one photon. In a cryptographic perspective, the crucial issue is to ensure that an eavesdropper Eve does not map the state of intercepted photons outside the DFS, which may enable eavesdropping attacks beyond those already studied [11, 17]. To verify that this is not the case, Bob could perform in principle a full quantum state reconstruction on some of the transmissions, which however would be resource consuming. We conjecture that a sufficient strategy to detect such an attack would be: (i) to detect polarizations of photons emerging after the beam splitters; (ii) for a subset of transmissions to count directly received photons to ensure that no multiphoton states in individual input paths occur; (iii) for another subset of transmissions to apply before the beam splitters random and uncorrelated transformations $U \otimes U$ and $U' \otimes U'$ and check that states $|Ξ_k\rangle$ always yield the correct outcome when Bob used the matching basis for his measurement.

IV. GENERAL PROOF

The reasoning presented in Sec. I can be generalized to any even number of $n > 4$ qubits by considering DFS states given by products of two-qubit singlet states. Such states form an overcomplete set in the DFS [17], which enables one to follow directly the steps described for four qubits. The robustness of DFS encoding can be shown more generally for an ensemble of $n$ qudits, i.e. $d$-dimensional systems. In this case, a DFS satisfying Eq. I exists only when $n$ is a multiple of $d$, which follows from the structure of the Young tableaux for irreducible representations of tensor products of the $SU(d)$ group [18].

As before, for concreteness we will consider removal of the first qudit. Let us consider arbitrary two states $|Ψ\rangle$ and $|Φ\rangle$ from the DFS and expand them in the form analogous to Eq. (3):

$$|Ψ\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle |Ψ(i)\rangle_1, \quad |Φ\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle |Φ(i)\rangle_1$$

where $|i\rangle_1, i = 0, \ldots, d - 1$ is an orthonormal basis in the space of the first qudit, and $|Ψ(i)\rangle_1 = \sqrt{d} |i\rangle |Ψ\rangle$ and $|Φ(i)\rangle_1 = \sqrt{d} |i\rangle |Φ\rangle$ are states of the remaining $n - 1$ qudits. We will first show that the following general property holds:

$$|Ψ\rangle |Φ\rangle_1 = \delta_{ij} \langle Φ|Ψ\rangle.$$

As we will see, this property guarantees that the loss of one particle does not destroy the quantum information encoded in the DFS.

In order to show that for $i \neq j$ the states $|Ψ(i)\rangle$ and $|Ψ(j)\rangle$ are orthogonal as implied by Eq. (10), let us consider the action of a diagonal unitary operator $V^\otimes n$, where $V = \text{diag}(e^{i\phi_0}, \ldots, e^{i\phi_{d-1}})$ with arbitrary phases $\phi_0, \ldots, \phi_{d-1}$ that sum up to zero. Invariance of $|Ψ(i)\rangle_1$ and $|Ψ(j)\rangle_1$ under $V^\otimes n$ implies that in the basis formed by tensor products of states $|0\rangle, \ldots, |d-1\rangle$ they are composed only from terms that have exactly $n/d$ particles in each of these $d$ states. Consequently, projecting the first qudit on orthogonal states $|i\rangle_1$ and $|j\rangle_1$ leaves the remaining qudits in distinguishable states.

In order to verify the case when $i = j$ in Eq. (10) it is convenient to use the transformation of states $|Ψ(i)\rangle_1$ under the action of $U^\otimes (n-1)$. In order to derive this transformation, let us rewrite the invariance condition from Eq. (1) to the form $U^\dagger \otimes 1^\otimes (n-1) |Ψ\rangle = 1 \otimes U^\otimes (n-1) |Ψ\rangle$.

![FIG. 2: An experimental scheme for loss-tolerant detection of a logical qubit encoded in four photons. The projection basis $|Ξ_k\rangle, |Ξ_k^\perp\rangle$, where $k = 1, 2, 3$, is selected by a suitable rerouting of input photons. Pairs of photons are interfered on two balanced beam splitters and photon numbers are counted at their outputs. Combinations of outcomes for individual detectors that correspond to unambiguous identification of $|Ξ_k\rangle$ and $|Ξ_k^\perp\rangle$ are indicated with photon numbers in curly brackets. The ordering within both inner and outer brackets does not matter.](image-url)
and project the first qudit onto $\sqrt{d_i}$, $i=\ldots,d-1$. This yields the identity:

$$\hat{U}^{\otimes(n-1)}|\Psi(i)\rangle_1 = \sqrt{d} (i\hat{U}^\dagger)^i |\Psi(i)\rangle_1 = \sum_{j=0}^{d-1} (j|\hat{U}^\dagger i)^* |\Psi(j)\rangle_1$$

Let us now specialize this result to a special unitary transformation that cyclically shifts the labelling of the basis states:

$$\hat{W} = (-1)^{d-1} \sum_{i=0}^{d-1} |i+1\rangle_i$$

where the addition $i+1$ is understood to be modulo $d$. Using this $W$ in Eq. (11) implies that $|\Psi(i+1)\rangle = (-1)^{d-1} \hat{W}^{\otimes(n-1)}|\Psi(i)\rangle$, i.e. $|\Psi(i)\rangle$ and $|\Psi(i+1)\rangle$ are related by a unitary that is independent of $|\Psi\rangle$. This means that $\langle\Phi(i+1)|\Psi(i+1)\rangle = \langle\Phi(i)|\Psi(i)\rangle$. This fact combined with expanding the scalar product $\langle\Phi|\Psi\rangle$ using Eq. (9) completes the proof of Eq. (10).

With Eq. (10) in hand, further steps are straightforward. A removal of the first qudit maps a state $|\Psi\rangle$ onto a statistical mixture

$$\hat{\tilde{\rho}}_1 = \text{Tr}_1(|\Psi\rangle\langle\Psi|) = \frac{1}{d} \sum_{i=0}^{d-1} |\Psi(i)\rangle_1\langle\Psi(i)|$$

Eq. (10) implies analogously to the SU(2) case the components with different $i$ occupy orthogonal subspaces. Within each subspace the state is fully preserved, which follows from applying Eq. (10) to pairs of states from an arbitrary basis in the DFS. The final step is to show that the state $\hat{\tilde{\rho}}_1$ is invariant with respect to $\hat{U}^{\otimes(n-1)}$. This is a consequence of the fact that both the initial state $|\Psi\rangle$ and the procedure of tracing out a particle are invariant with respect to SU($d$) transformations. Explicitly, the invariance of $\hat{\tilde{\rho}}_1$ can be verified with a calculation based on Eq. (11):

$$\hat{U}^{\otimes(n-1)} \hat{\tilde{\rho}}_1 (\hat{U}^\dagger)^{\otimes(n-1)} = \sum_{i=0}^{d-1} (i|\hat{U}^\dagger)^i |\Psi\rangle \langle\Psi| (\hat{U}^\dagger i)\rangle_1$$

$$= \text{Tr}_1(|\Psi\rangle\langle\Psi|) = \hat{\tilde{\rho}}_1.$$ 

Thus the encoded state is fully preserved.

V. CONCLUSIONS

Concluding, we have shown that DFS encoding is immune to removing one particle. Unfortunately, this property does not seem to generalize in a straightforward manner to the loss of more particles. For example, when two qubits are removed from a four-qubit DFS state, the result will be either a singlet state of the remaining two qubits, or a statistical mixture of the singlet and triplet states which does not preserve the original superposition. This observation holds for any higher even number of qubits. Nevertheless, our result shows how to protect information in the few-photon regime from both collective depolarization and the first-order effects of linear attenuation. We have proposed an experimental demonstration of this combined protection which can provide a robust quantum cryptography protocol.

Finally, let us note that although the proof of robustness against the qudit loss was based on the assumption that Eq. (1) is satisfied for every SU($d$) matrix, the DFS fulfilling this condition protects quantum superpositions from any decoherence mechanism that involves a subset of SU($d$) transformations. Therefore our considerations apply to a range of physical systems, for example higher-spin particles in a magnetic field or multilevel atoms interacting with optical fields.

We acknowledge useful discussions with Rafał Demkowicz-Dobrzański, Harald Weinfurter, Alessio Celi, Marcin Kotowski and Joanna Ziebańska. The work was supported by the Foundation for Polish Science TEAM project cofinanced by the EU European Regional Development Fund, FP7 FET project CORNER (contract no. 213681), Spanish MINECO project FIS2008-00784 (TOM-QATA) and ERC Advanced Grant QUAGATU.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002) [arXiv:quant-ph/0101098v2]; V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, ibid. 81, 1301 (2009) [arXiv:0802.1155v3].
[2] A. Ekert and R. Jozsa, Rev. Mod. Phys. 68, 733 (1996).
[3] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Rev. Mod. Phys. 82, 665 (2010).
[4] D. Gottesman, in Proceedings of Symposia in Applied Mathematics, 68, pp. 13-58 (2010).
[5] W.K. Wootters and W.H. Zurek, Nature 299, 802 (1982).
[6] L.-M. Duan and G.-C. Guo, Phys. Rev. Lett. 79, 1953 (1997) [arXiv:quant-ph/9703040v2]; P. Zanzardi and M. Rasetti, ibid. 79, 3306 (1997) [arXiv:quant-ph/9705041v2]; D. A. Lidar, I. L. Chuang, and K. B. Whaley, ibid. 81, 2594 (1998) [arXiv:quant-ph/9807004v2].
[7] J. Kempe, D. Bacon, D. Lidar, and K. B. Whaley, Phys. Rev. A 63, 042307 (2001) [arXiv:quant-ph/0004064v2].
[8] W. Wasilewski and K. Banaszek, Phys. Rev. A 75,
[9] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Phys. Rev. Lett. 91, 027901 (2003) arXiv:quant-ph/0302111v3; K. Banaszek, A. Dragan, W. Wasilewski, and C. Radzewicz, ibid. 92, 257901 (2004) arXiv:quant-ph/0403024v1.

[10] M. Bourennane, M. Eibl, S. Gaertner, C. Kurtsiefer, A. Cabello, and H. Weinfurter, Phys. Rev. Lett. 92, 107901 (2004) arXiv:quant-ph/0309041v2.

[11] J. C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, Phys. Rev. Lett. 92, 017901 (2004) arXiv:quant-ph/0306199v2.

[12] L. Viola, E. M. Fortunato, M. A. Pravia, E. Knill, R. Laflamme, and D. G. Cory, Science 293, 2059 (2001).

[13] R. H. Dicke, Phys. Rev. 93, 99 (1954).

[14] H. Weinfurter and M. Żukowski, Phys. Rev. A 64, 010102 (2001) arXiv:quant-ph/0103049v1; Y.-X. Gong, X.-B. Zou, X.-L. Niu, J. Li, Y.-F. Huang, and G.-C. Guo, Phys. Rev. A 77, 042317 (2008).

[15] S. L. Braunstein and A. Mann, Phys. Rev. A 51, R1727 (1995).

[16] J. M. Renes, Phys. Rev. A 70, 052314 (2004) arXiv:quant-ph/0402135v3; G. Tabia and B.-G. Englert, Phys. Lett. A, 375, 817 (2011) arXiv:0910.5375v1.

[17] D. W. Lyons and S. N. Walck, Phys. Rev. A 78, 042314, (2008) arXiv:0808.2989v2.

[18] H. F. Jones, Groups, Representations and Physics. (Institute of Physics Publishing, Bristol and Philadelphia, 1998), Chap. 8.