A Quantum Key Distribution protocol for qu*d*its with better noise resistance

Zoé AMBLARD
XLIM Laboratory
University of Limoges

François ARNAULT
XLIM Laboratory
University of Limoges

April 27, 2015

The Ekert91 protocol [1] uses pairs of entangled qubits to exchange keys and checks for the violation of a Bell inequality in order to detect eavesdropping. The violation value of a Bell inequality is known to be one of the factors that lead to a better noise resistance [2]. It is indeed linked to the threshold fraction of unbiased noise which has to be admixed to the state used in the protocol in order to erase the non-classicality of the correlations. In a real experiment, it is almost impossible to obtain a perfectly noiseless channel. An inequality admitting a good threshold of noise is consequently needed to be able to perform the checks even in a noisy environment. But as the two parties running the protocol are unable to distinguish between a perturbation caused by a noisy channel and an adversary, tolerating a big amount of noise eventually leads to a security breach.

For this reason, the two parties must use an inequality whose violation value reaches a compromise between noise resistance and security.

In their article [3] introducing a generalization of the Ekert91 protocol for any dimension d (called the N-DEB protocol), Durt, Kaszlikowski, Chen and Kwek use the generalized CHSH inequality described in [4] to obtain better noise resistance than for the qubit case.

We describe here a new protocol hdDEB which generalize our protocol h3DEB [5] in any dimension $d \geqslant 3$. It uses an homogeneous Bell inequality called hCHSH-d which belongs to the family of Bell inequalities introduced in [6].The amount of violation achieved by hCHSH-d with specific entangled states being better than for the generalized CHSH, our protocol hdDEB allows more tolerance to noise than N-DEB.

Devices called multiport beam splitters [7] (or ditters), are mentioned in [3] as one way to handle measurements of qudits. Our protocol hdDEB is analysed in view of the use of ditters to implement measurements. As the inequality hCHSH-d involves some products of observables which do not commute, each observable being implemented by a ditter coupled with a measurement

in the computational basis, we first show how these products can also be implemented by another single ditter. Once we have made clear that our protocol is indeed fully implementable in practice, we study the eventual impact of these product measurements over the security against a family of cloning attacks described in [3]. As these new measurements do not affect the form of the cloner required for this attack, we derive a security criterion for our protocol which takes the form of an upper bound over the value of the violation.

We finally provide for each $d = 3, 4, 5$ a set of parameters (basis, entangled state and homogeneous Bell inequality) which ameliorates the noise threshold of N-DEB while ensuring the security of our protocol against the same family of cloning attacks than in N-DEB.

d	3	4	5
N-DEB	1.436	1.448	1.455
hdDEB	1.505	1.546	1.574

Table 1: Violations obtained with N-DEB and hdDEB for $d = 3, 4, 5$

A detailed version of this work can be found in attachment below.

References

[1] A. K. Ekert. Quantum cryptography based on bell's theorem. *Physical Review Letters*, 67:661, 1991.

[2] Harald Weinfurter and Marek Żukowski. Four-photon entanglement from down-conversion. *Phys. Rev. A*, 64:010102, Jun 2001.

[3] T. Durt, D. Kaszlikowski, J.L. Chen, and L.C. Kwek. Security of quantum key distribution with entangled qudits. *Physical Review A*, 69:032313, 2004.

[4] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu. Bell inequalities for arbitrarily high-dimensional systems. *Phys. Rev. Lett.*, 88:040404, 2002.

[5] F. Arnault and Z. Amblard. A qutrit quantum key distribution protocol with better noise resistance. quant-ph/1404.4199, 2014.

[6] F. Arnault. A complete set of multidimensional bell inequalities. *Journal of Physics A*, 45:255304, 2012.

[7] M. Ẑukowski, A. Zeilinger, and M.A. Horne. Realizable higher-dimensional two-particle entanglements via multiport beam splitters. *Physical Review A*, 55:2564, 1997.

Attachment : A Quantum Key Distribution protocol for qu*d*its with better noise resistance

Abstract

The Ekert quantum key distribution protocol [1] uses pairs of entangled qubits and performs checks based on a Bell inequality to detect eavesdropping. The N-DEB protocol [3] uses instead pairs of entangled qu*d*its to achieve better noise resistance than the Ekert protocol. It performs checks based on a Bell inequality for qu*d*its found in [4] and which we will refer to as the CGLMP-d. In this paper, we present the generalization of our protocol h3DEB [5] for qu*d*its. This protocol also uses pairs of entangled qu*d*its, but achieves even better noise resistance than N-DEB and is showed to be secure against the same family of cloning attacks than N-DEB. This gain of performance is obtained by using another inequality called here hCHSH-d, which was discovered in [6]. For each party, the hCHSH-d inequality involves $2d$ observables. We explain how the parties can measure these observables and thus are able to check the violation of hCHSH-d. In the presence of noise, this violation allows the parties to ensure the secrecy of the key because it guarantees the absence of a local Trojan horse attack. The advantage of our proposed scheme is that it results in an increased resistance to noise while remaining secure against individual attacks.

1 Introduction

The Ekert91 protocol [1] exploits pairs of entangled states to exchange keys, and uses Bell inequalities to detect eavesdropping. Some of the measurement results obtained by the two parties Alice and Bob are perfectly correlated, providing key bits. Other measurement results must exhibit quantum behaviour if there is no alteration of the quantum channel, and this permits to detect eavesdropping by testing a Bell inequality violation.

The amount of quantum violation is an important characteristic in key distribution protocols because a larger violation is one of the factors that lead to a better noise resistance [2]. Some progress has been made to increase this amount of violation with the use of parties with higher dimension or specific entangled states. One can also consider choosing different Bell inequalities to detect eavesdropping.

In their article introducing the N-DEB protocol [3], Durt, Kaszlikowski, Chen and Kwek use d-dimensional quantum systems (qu*d*its), and the CGLMP-d inequality to obtain better noise resistance than for the Ekert'91 protocol.

Our work makes one step further by using a recent discovered Bell inequality (here called hCHSH-d), which belongs to the family of homogeneous Bell inequalities introduced in [6]. The amount of violation which can be achieved with entangled states is even better than for the CGLMP-d. Consequently, the protocol we derive is more tolerant to noise than N-DEB.

Devices called multiport beam splitters [7] (or ditters), are mentioned in [3] as one way to handle measurements of qu$d$its. Our new protocol hdDEB described in this article is analysed in view of the use of ditters to implement measurements. A crucial point here will be that some products of observables, each implemented by a ditter coupled with a measurement in the computational basis, can also be implemented by another single ditter. This is needed for our protocol as the inequality hCHSH-d involves such products.

The paper is organized as follows. It begins with some reminders and precisions about measurements with ditters in Section 2, where we also consider the use of ditters for implementing the product of observables. Then Section 3 recalls the N-DEB protocol. After that, Section 4 introduces the Bell inequality hCHSH-d we use and defines our new protocol hdDEB. In Section 5, we study the security of our protocol against individual attacks and we show that our protocol hdDEB reaches a compromise between resistance to noise and security. Finally, the paper concludes about the advantage of hdDEB providing better resistance to noise.

2 Prerequisites

In what follows, all the sums will be taken modulo d. Our protocol use qu$d$its and observables with d outcomes which we label for readability $1, \omega, ..., \omega^{d-1}$ where ω is the d^{th} root of unity $\omega = e^{\frac{2i\pi}{d}}$. The observables used by the two parties Alice and Bob will be denoted respectively by A_i and B_j for some indexes i and j. We will also use the correlation functions :

$$E(A_i B_j) = \sum_{a,b=1,\omega,...,\omega^{d-1}} P(A_i = a, B_j = b)\, ab.$$

2.1 Measurements with ditters

A ditter is parameterized by a d-uplet $(\varphi_0, \varphi_1, ..., \varphi_{d-1})$ of phase shifts. For readability we put $\theta_j = \exp(i\varphi_j)$ (for $j = 0, 1, ..., d-1$) and $\Theta = (\theta_0, ..., \theta_{d-1})$. The ditter performs over a qu$d$it the following unitary transformation :

$$U_\Theta := HD_\Theta = \frac{1}{\sqrt{d}} \sum_{k,l=0}^{d-1} \omega^{kl} \theta_l \left|k\right\rangle \left\langle l\right|$$

where the matrices H and D_Θ are $H = (\omega^{kl})_{0 \leq k,l \leq d-1}$ and $D_\Theta = \text{diag}(\theta_0, ..., \theta_{d-1})$.

After the transformation performed by the ditter, a measurement in the computational basis is made using d detectors. This measurement is represented by the observable

$$Z = \sum_{k=0}^{d-1} \omega^k \left|k\right\rangle \left\langle k\right|.$$

As we assumed the d possible outcomes to be labeled by complex roots of unity, we use unitary observables. Thus, the measurement obtained by the combination of the ditter and the detectors corresponds to the following observable

$$Z_\Theta := D_{\Theta^*} H^\dagger Z H D_\Theta = \sum_{k=0}^{d-1} \theta_k \theta_{k+1}^* \left|k+1\right\rangle \left\langle k\right| \tag{1}$$

which gives us, in the particular case where $\theta_j = \theta^j$:

$$Z_\Theta = \theta^{d-1} \left|0\right\rangle \left\langle d-1\right| + \sum_{k=0}^{d-2} \theta^* \left|k+1\right\rangle \left\langle k\right|. \tag{2}$$

2.2 Products of incompatible observables

Suppose that we have two measurement devices (each one represented by a ditter and a measurement in the computational basis), which implement the observables Z_Θ and Z_Λ described by Equation (1), with $\Theta = (\theta_0, \theta_1, ..., \theta_{d-1})$ and $\Lambda = (\lambda_0, \lambda_1, ..., \lambda_{d-1})$. Then we need to implement the product observable $Z_\Theta^i Z_\Lambda^j$ for $i = 1, ..., d-2$ and $j = d-i-1$.

Proposition 1. *Let define the d-uplet of phase shifts* $\Gamma = (\gamma_0, \gamma_1, ..., \gamma_{d-1})$. *For any* $i = 1, ..., d-2$ *and* $j = d-i-1$, *the observable* $Z_\Theta^i Z_\Lambda^j$ *verifies :*

$$Z_\Theta^i Z_\Lambda^j = Z_\Gamma^\dagger = \sum_{k=0}^{d-1} \gamma_{k+1} \gamma_k^* \left|k\right\rangle \left\langle k+1\right|$$

with

$$\forall k = 0, ..., d-1 \qquad \gamma_k = \theta_k \theta_{k+1} ... \theta_{k-i-1} \lambda_{k-i} \lambda_{k-i+1} ... \lambda_k.$$

Proof. From Equation (1), we write :

$$\begin{aligned} Z_\Theta^i Z_\Lambda^j &= (\sum_{k=0}^{d-1} \theta_k \theta_{k+i}^* \left|k+i\right\rangle \left\langle k\right|) \times (\sum_{l=0}^{d-1} \lambda_l \lambda_{l+j}^* \left|l+j\right\rangle \left\langle l\right|) \\ &= \sum_{l=0}^{d-1} \theta_{l+j} \theta_{l+i+j}^* \lambda_l \lambda_{l+j}^* \left|l+i+j\right\rangle \left\langle l\right| \\ &= \sum_{k=0}^{d-1} \theta_{k-i} \theta_k^* \lambda_{k+1} \lambda_{k-i}^* \left|k\right\rangle \left\langle k+1\right|. \end{aligned}$$

The generalized Pauli matrix Z in dimension d verifies $Z^d = I_d$. The matrix Z being unitary, it also verifies $I_d = Z Z^\dagger$, which gives $Z^{d-1} = Z^\dagger$.

For any observable Z_Ω we have $Z_\Omega^{d-1} = D_\Omega^* H^\dagger Z^\dagger H D_\Omega = Z_\Omega^\dagger$. In order to rewrite a product observable as a new ditter measurement of the form $Z_\Gamma^\dagger = \sum_{k=0}^{d-1} \gamma_{k+1}\gamma_k^* |k\rangle \langle k+1|$, we need $\gamma_{k+1}\gamma_k^* = \theta_{k-i}\theta_k^* \lambda_{k+1}\lambda_{k-i}^*$. One of the possible solutions is :

$$\forall k = 0, ..., d-1 \qquad \gamma_k = \theta_k \theta_{k+1} ... \theta_{k-i-1} \lambda_{k-i} \lambda_{k-i+1} ... \lambda_k.$$

□

From Proposition 1, we conclude that any product observable $Z_\Theta^i Z_\Lambda^j$ is implementable by a ditter and a detector, with the detector performing a measurement corresponding to the observable $Z^\dagger$ instead of Z.

3 The N-DEB protocol

We will recall the N-DEB protocol introduced in [3].

3.1 The d-dimensional inequality used in N-DEB

For a given value of d, the N-DEB protocol uses the d-dimensional inequality introduced in [4] which is referred in N-DEB as the generalized CHSH and which we will call in our paper the CGLMP-d inequality. The maximally entangled state

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj\rangle \tag{3}$$

is known to violate this inequality with the four bases used in N-DEB. For these bases, we will use the same denomination "optimal bases" as in [3]. The violation values for $d = 3, 4, 5$ are summarized in the following table :

d	v_d	N_d
3	1.436	0.304
4	1.448	0.309
5	1.455	0.313

Table 2: Violation value of the CGLMP-d inequality with the maximally entangled state for $d = 3, 4, 5$

.

3.2 The N-DEB procedure

Alice uses four observables A_a with $a = 0$ to 3, corresponding to ditter measurements with phase shift $(1, \theta^a, \theta^{2a}, ..., \theta^{(d-1)a})$. Bob use four observables

B_b with $b = 0$ to 3, corresponding to ditter measurements with phase shift $(1, \theta^{-b}, \theta^{-2b}, ..., \theta^{-(d-1)b})$. The following steps are repeated until Alice and Bob obtained a shared key of desired length.

1. Alice and Bob obtain an entangled pair of states in the maximally entangled state defined in (3).

2. Alice draws randomly a value for $a \in \{0, 1, 2, 3\}$ and makes the measurement corresponding to the observable A_a whereas Bob draws randomly a value for $b \in \{0, 1, 2, 3\}$ and makes the measurement corresponding to the observable B_b.

3. When $a = b$, the results obtained by Alice and Bob are perfectly correlated. Indeed, the two ditters used by Alice and Bob perform on the shared maximally entangled state the transformation $(H \otimes H)(D_\Theta \otimes D_{\Theta^*})$ with $\Theta = (1, \theta^a, \theta^{2a}, ..., \theta^{(d-1)a})$. But it is easy to check that:

$$(H \otimes H)(D_\Theta \otimes D_{\Theta^*})(\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj\rangle) = \frac{1}{\sqrt{d}} \sum_{\substack{k,k'=0 \\ k+k' \equiv 0[d]}}^{d-1} \left|kk'\right\rangle. \qquad (4)$$

   Consequently, in this case where $a = b$, Alice and Bob obtain a new dit for the shared key.

4. When $a \neq b$, Alice and Bob can use a fraction of their joint measurements to detect eavesdropping by checking a configuration of maximal violation of the CGLMP-d.

4 The hdDEB protocol

We will now describe our protocol. It achieves better noise resistance because it uses an homogeneous Bell inequality, which has a larger violation factor than CGLMP-d.

4.1 Violation of the inequality hCHSH-d

Depending on the entangled state that we want to use in our protocol, we can choose an inequality belonging to the set of homogeneous Bell inequalities described in [6] and which will be called hCHSH-d. It has also been shown in [6] that the homogeneous Bell inequalities are satisfied under the hypothesis of local realism, and that they form a complete set. An homogeneous Bell inequality for two parties can in general be written

$$\mathrm{Re}(\frac{\rho}{d^2 \cos(\frac{\pi}{d})} E(T)) \leqslant 1 \qquad (5)$$

where $\rho = \mathrm{e}^{\frac{i\pi}{d}}$ and T is an homogeneous polynomial in some measurements Alice and Bob can make. We call T a *Bell operator*.

A feature of the homogeneous Bell inequalities is that T involve some products of observables (for example $A_1^3 A_2$, $A_1^2 A_2^2$ and $A_1 A_2^3$ for Alice in the case $d = 5$) which become incompatible when considered as quantum observables. The outcomes of such a product of course cannot be meant to be the products of outcomes of incompatible observables. In Proposition 1, we show that if we use the unitary observables Z_Θ defined in (1) for the A_i previously described, the product is also a unitary observable which outcomes can be obtained with a single measurement. We also conclude that we can perform this product measurement in terms of a new ditter operation and a final detection in the computational basis.

The local realistic elements A_1^{d-1}, $A_1^i A_2^j$ (for $i = 1, ..., d-2$ and $j = d-i-1$) and A_2^{d-1} for Alice have to be replaced by the observables

$$Z^\dagger_{\Theta_A}, \quad Z^\dagger_{\Gamma_{ij_A}}, \quad Z^\dagger_{\Lambda_A}$$

where the $Z^\dagger_{\Gamma_{ij_A}}$ is a product observable as described in Proposition 1 and Θ_A, Λ_A are the parameters corresponding to the optimal bases. Similarly, the party Bob has to use the observables $Z^\dagger_{\Theta_B}$, $Z^\dagger_{\Gamma_{ij_B}}$, $Z^\dagger_{\Lambda_B}$.

After substituting these observables to the variables in a Bell operator T, a quantum state $|\psi\rangle$ violates the homogeneous Bell inequality associated to T with a violation factor $v \geqslant 1$ if it verifies (compare to (5)) :

$$\frac{1}{d^2 \cos(\frac{\pi}{d})} \mathrm{Re}(\langle\psi| \rho T |\psi\rangle) = v \quad \text{for } \rho = \mathrm{e}^{\frac{i\pi}{d}} . \tag{6}$$

4.2 The hdDEB procedure

As for the NDEB protocol described in [3], we denote $\mathscr{A}_a = A_0^{d-1-a} A_1^a$ with $a = 0, 1, 2, .., d-1$ the observable parameterized by phase shift $(1, \theta^a, .., \theta^{(d-1)a})$, and $\mathscr{B}_b = B_0^{d-1-b} B_1^b$ with $b = 0, 1, 2, .., d-1$ the observable parameterized by $(1, \theta^{-b}, \theta^{-(d-1)b})$. Each of these observables is expected to be implemented with a single ditter from Proposition 1.

1. Alice and Bob obtain an entangled pair of states in the d-dimensional entangled state $|\psi\rangle := \sum_{j=0}^{d-1} \delta_j |jj\rangle$ with $\delta_j \in \mathbb{C}$ for some $j = 0, ..., d-1$.

2. Alice draws randomly a value of a and performs her measurement in the basis associated to the observable $\mathscr{A}_a$ whereas Bob draws randomly a value of $\mathscr{B}_b$ and performs his measurement in the basis associated to B_b.

3. When $a = b$, the results obtained by Alice and Bob are perfectly correlated and they obtain a new dit for the shared key. For completeness, a proof of this statement is given in Appendix A.

4. For some choices of a and b Alice and Bob collect the issues of their measurements in order to detect eavesdropping by checking a violation of the homogeneous Bell inequality hCHSH-d considered.

4.3 Choice of the inequality and resistance to noise for $d = 3, 4, 5$

With the four "optimal bases" described in [3], the maximally entangled states don't allow to reach the largest violations. We consider several non-maximally entangled states which, when used with their corresponding homogeneous Bell inequalities, reach largest violations. A precise derivation of the case $d = 3$ can be found in [5].

We compare the violations for the following states $|\psi_d\rangle$ with $d = 3, 4, 5$:

$$|\psi_3\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle).$$

$$|\psi_4\rangle = \frac{1}{2}(|00\rangle + |11\rangle + |22\rangle + |33\rangle).$$

$$|\psi_5\rangle = \frac{1}{\sqrt{5}}(|00\rangle + |11\rangle + |22\rangle + |33\rangle - i\,|44\rangle).$$

We use the homogeneous inequalities associated to each $|\psi_d\rangle$:

$$\frac{1}{d^2\cos(\frac{\pi}{d})}\mathrm{Re}(\rho E(T_d)) \leqslant 1 \tag{7}$$

with

$$\begin{aligned} T_3 = -\big[&(\omega-4)(A_1^2B_1^2) + (\omega+2)(A_1^2B_1B_2) + (\omega-1)(A_1^2B_2^2) \\ &+ (\omega+5)(A_1A_2B_1^2) + (\omega+2)(A_1A_2B_1B_2) + (\omega+1)(A_1A_2B_2^2) \\ &+ (\omega+5)(A_2^2B_1^2) + (\omega+2)(A_2^2B_1B_2) + (\omega-1)(A_2^2B_2^2)\big]. \end{aligned}$$

$$\begin{aligned} T_4 = &-(3\omega+1)(A_1^3B_1^3) - (\omega+1)(A_1^3B_1^2B_2) - 5(\omega-1)(A_1^3B_1B_2^2) \\ &- (3\omega-1)(A_1^3B_2^3) + (\omega+1)(A_1^2A_2B_1^3) - (\omega+3)(A_1^2A_2B_1^2B_2) \\ &- (\omega+1)(A_1^2A_2B_1B_2^2) - (3\omega+1)(A_1^2A_2B_2^3) + (3\omega+1)(A_1A_2^2B_1^3) \\ &+ (5\omega+1)(A_1A_2^2B_1^2B_2) - (7\omega+1)(A_1A_2^2B_1B_2^2) + 3(\omega+1)(A_1A_2^2B_2^3) \\ &- 5(\omega+1)(A_2^3B_1^3) + (\omega-1)(A_2^3B_1^2B_2) + (\omega+1)(A_2^3B_1B_2^2) \\ &- (\omega-1)(A_2^3B_2^3). \end{aligned}$$

For conveniency, the Bell operator T_5 is derived in Appendix B.

These states and the Bell operators corresponding to their inequalities were chosen because they reach the best compromise between noise resistance and security against individual attacks, as it will be explained in Section 5.

We summarize each choice of entangled state and Bell operator in the following table :

$\|\psi_d\rangle$	T_d	v_d	N_d
$\|\psi_3\rangle$	T_3	1.505	0.336
$\|\psi_4\rangle$	T_4	1.546	0.353
$\|\psi_5\rangle$	T_5	1.574	0.365

Table 3: Violation value of the hCHSH-d inequality depending on the entangled state and its Bell operator

5 An alternative version of hdDEB secure against individual attacks

5.1 An optimal cloning-based attack for the N-DEB and hdDEB protocols

A cloning-based attack uses a cloning machine (also known as cloner) to copy an input state. Because of the no-cloning theorem, the clonage is imperfect and the adversary aims to design an optimal cloner which copies a specific set of states as accurately as possible. Depending on the properties of the input state or the family of the cloner, the state can be reproduced with a certain amount of fidelity F_A defined in [3] by

$$F_A = \langle\psi| \rho |\psi\rangle \tag{8}$$

where ψ is the initial pure state, and ρ the density of the clone (not necessarily pure).

In [3] is described a cloning-based attack which uses a phase-covariant qu$d$it cloning machine. This cloner acts with the same accuracy on each states of the optimal bases used in the N-DEB protocol. All these states are copied with the same fidelity F_A depending on the value of d :

d	3	4	5	6	7	8	9	∞
F_A	0.7753	0.7342	0.7080	0.6898	0.6762	0.6657	0.6573	0.5

Proposition 2. *The $2d$ bases considered in our protocol are copied with maximal fidelity when using the optimal phase-covariant cloner described in [3].*

Proof. Four of our bases are the same optimal bases than from [3]. The $2(d-2)$ remaining bases have vectors of the form :

$$\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{i\gamma_j} |j\rangle.$$

But the cloner described in [3] is optimal for all states of the form :

$$\sum_{j=0}^{d-1} \delta_j |jj\rangle \text{ for all } \delta_j \text{ verifying } |\delta_j|^2 = \frac{1}{d}.$$

Consequently, this cloner is also the optimal asymmetric qu*d*it cloner when considering our $2d$ bases. □

5.2 The violation of an homogeneous Bell inequality as a sufficient condition for security

The violation factor is considered very important for the security of the key distribution protocol. The presence of noise is usually modeled by the replacement of the initial entangled state by a mixture

$$N\frac{I}{d} + (1-N) |\psi\rangle \langle\psi| \tag{9}$$

where N is the proportion of noise. The point is that the presence of noise decreases the experienced violation to $(1-N)v$ and that the protocol is considered useless when the initial state entanglement cannot be detected anymore. With this criterion, it has been shown that a protocol is resistant to the presence of noise up to a threshold :

$$N = 1 - 1/v. \tag{10}$$

When using a noisy channel described by (9), the fidelity (as defined in (8)) between the input state $|\psi\rangle$ and the output state is given by

$$F_N = \langle\psi| \rho' |\psi\rangle = -\frac{d-1}{d}N + 1$$

where $\rho' = N\frac{I}{d} + (1-N) |\psi\rangle \langle\psi|$. The presence of noise N does not erase the non-classicality of the correlations as long as it stays below the value given by (10). Hence, it is possible to use a channel for secure key distribution if its fidelity satisfies

$$F_N > \frac{d-1}{dv} + \frac{1}{d}. \tag{11}$$

Suppose that an adversary Eve uses an optimal cloner which copy an input state with fidelity F_A and introduces a minimal amount of error $1 - F_A$ indistinguishable from an unbiased noise.

Eve's attacks won't be detected as long as $F_A \geqslant F_N$. Hence, the security of the protocol against individual cloning attacks is guaranteed if we have $\frac{d-1}{dv} + \frac{1}{d} > F_A$. This is equivalent to $v < \frac{d-1}{dF_A - 1}$.

By replacing F_A for each $d = 3, 4, 5$, we obtain the conditions :

d	Security criterion
3	$v < 1.508$
4	$v < 1.549$
5	$v < 1.575$
6	$v < 1.593$
7	$v < 1.607$
8	$v < 1.618$
9	$v < 1.627$
∞	$v < 2$

5.3 Comparison between N-DEB and hdDEB under the same security criterion

By looking at Table 1 and Table 2, we notice that for each $d = 3, 4, 5$ the violation values of CGLMP-d and hCHSH-d are below the security criterion, which ensure the security of the N-DEB and hNDEB protocols against this family of optimal cloning attacks. But it is also noticeable that, for each $d = 3, 4, 5$, there is a wide gap between the violation values attainable by CGLMP-d and the maximal value tolerated by the security threshold. This gap can be closed by the use of our inequality CGLMP-d which reaches largest violation values :

d	$v_{\text{N-DEB}}$	$v_{\text{h}d\text{DEB}}$	Security criterion
3	1.436	1.505	$v < 1.508$
4	1.448	1.546	$v < 1.549$
5	1.455	1.574	$v < 1.575$

Moreover, this exploitable gap between $v_{\text{N-DEB}}$ and the security criterion increases with the dimension d. From this we conclude not only that our protocol tolerates a higher error rate in the channel than N-DEB while remaining secure against the same family of attacks, but also that this amelioration grows for a higher d.

6 Conclusion

Our goal was to generalize our protocol h3DEB [5] in any dimension d. By using the homogeneous Bell inequality hCHSH-d which reaches a better violation factor than the CGLMP-d in dimension $d = 3, 4, 5$, our new protocol hdDEB obtain a better threshold of noise resistance than N-DEB.

As the inequality hCHSH-d involves products of observables which become incompatible for quantum states, an important fact is the possibility to implement with slightly modified ditters the single observable corresponding to these products. We showed in 4.2 that all the observables needed to compute the violation of an homogeneous Bell inequality, including these products of observables, can be implemented by replacing the final measurement with observable Z by a measurement with observable $Z^\dagger$. Physically, this replacement corresponds just to a permutation of the detectors.

The gain in noise resistance of our protocol over N-DEB is due to the use of the inequality hCHSH-d.This inequality detects violations of local realism when some measurements are multiplicatively related. By using ditters measurements which respect this multiplicative constraints, the parties running the protocol are able to exploit its larger violation capabilities.

The use of $2d$ bases instead of four has the drawback of decreasing the effective dit transfer rate (the probability to obtain a key dit decreases from $\frac{1}{4}$ to $\frac{1}{2d}$) and it makes our protocol more complex ($2(d-2)$ supplementary devices), which can be a potential source of added noise. In the other hand, our protocol tolerates a higher threshold of noise than the one in the N-DEB protocol.

In the paper [3], the security of the protocol N-DEB against the optimal individual attack was investigated and it was possible to conclude that a violation of the CHSH-d inequality was a sufficient condition to guarantee the security against individual attacks. We study here the security of our protocol hdDEB against the same optimal individual attack and we conclude that our protocol is also secure against this cloning attack.

For the same level of security against individual attacks, we consequently obtain a better noise resistance than N-DEB and this amelioration is more and more visible when d increases.

Acknowledgement. One of the author (Z.A.) was partially supported by Thales Alenia Space during this work.

Appendix A

We show that in the hdDEB procedure, when $a = b$, the results obtained by Alice and Bob are perfectly correlated.

Let first define the d-dimensional entangled state $|\psi\rangle := \sum_{j=0}^{d-1} \delta_j |jj\rangle$ with $\delta_j \in \mathbb{C}$ for some $j = 0, ..., d-1$.

The two ditters used by Alice and Bob perform on the state $|\psi\rangle$ the transformation $(H \otimes H)(D_\Theta \otimes D_{\Theta^*})$, with $\Theta = (1, \theta^a, \theta^{2a}, ..., \theta^{(d-1)a})$. We use the notations :

$$HD_\Theta := \frac{1}{\sqrt{d}} \sum_{k,l=0}^{d-1} \omega^{kl} \theta_l |k\rangle \langle l|$$

where the matrices H and D_Θ are $H = (\omega^{kl})_{0 \leq k,l \leq d-1}$ and $D_\Theta = \mathrm{diag}(\theta_0, \theta_1, ..., \theta_d)$.
We write :

$$\begin{aligned}(H \otimes H)(D_\Theta \otimes D_{\Theta^*}) &= (HD_\Theta) \otimes (HD_{\Theta^*}) \\ &= \frac{1}{d}\Big(\sum_{k,l=0}^{d-1} \omega^{kl} \theta_l |k\rangle \langle l| \otimes \sum_{k',l'=0}^{d-1} \omega^{k'l'} \theta_{l'} \left|k'\right\rangle \left\langle l'\right|\Big) \\ &= \frac{1}{d}\Big(\sum_{k,l,k',l'=0}^{d-1} \omega^{kl+k'l'} \theta_l \theta_{l'} \left|kk'\right\rangle \left\langle ll'\right|\Big)\end{aligned}$$

By applying this transformation to the state $|\psi\rangle$, we obtain :

$$(HD_\Theta \otimes HD_{\Theta^*})\Big(\sum_{j=0}^{d-1} \delta_j |jj\rangle\Big) = \frac{1}{d}\Big(\sum_{j=0}^{d-1} \sum_{k,k'=0}^{d-1} \delta_j \omega^{j(k+k')} \left|kk'\right\rangle\Big)$$

From $1 + \omega + \omega^2 + ... + \omega^{d-1} = 0$ we finally find :

$$(HD_\Theta \otimes HD_{\Theta^*})\Big(\sum_{j=0}^{d-1} \delta_j |jj\rangle\Big) = \Big(\sum_{j=0}^{d-1} \delta_j\Big)\Big(\sum_{\substack{k,k'=0 \\ k+k' \equiv 0[d]}}^{d-1} \left|kk'\right\rangle\Big)$$

Appendix B

In order to obtain the violation $v \simeq 1.574$, we use the entangled state

$$|\psi_5\rangle = \frac{1}{\sqrt{5}}(|00\rangle + |11\rangle + |22\rangle + |33\rangle - i\,|44\rangle).$$

with the following Bell operator :

$$
\begin{aligned}
T_5 = {} & (2\omega^3 - 3\omega + 6)(A_1^4 B_1^4) - (4\omega^2 + 6\omega + 5)(A_1^4 B_1^3 B_2) \\
& + (7\omega^3 - \omega^2 + 2\omega - 3)(A_1^4 B_1^2 B_2^2) + (\omega^3 + \omega^2 - 4\omega - 3)(A_1^4 B_1 B_2^3) \\
& + 2(\omega^3 + \omega^2 + 3\omega)(A_1^4 B_2^4) - (\omega^3 + 4\omega^2 + 3\omega + 2)(A_1^3 A_2 B_1^4) \\
& - (5\omega^3 + 3\omega^2 + 3\omega + 4)(A_1^3 A_2 B_1^3 B_2) - (2\omega^3 + 3\omega^2 + 2\omega - 2)(A_1^3 A_2 B_1^2 B_2^2) \\
& + (-2\omega^3 + \omega^2 + 1)(A_1^3 A_2 B_1 B_2^3) + (4\omega^2 - 2\omega + 3)(A_1^3 A_2 B_2^4) \\
& + (-\omega^2 + 3\omega + 3)(A_1^2 A_2^2 B_1^4) + (2\omega^3 + 7\omega^2 + \omega)(A_1^2 A_2^2 B_1^3 B_2) \\
& - (4\omega^3 + 6\omega^2 + 5\omega + 5)(A_1^2 A_2^2 B_1^2 B_2^2) - (3\omega^3 + 2)(A_1^2 A_2^2 B_1 B_2^3) \\
& + (5\omega^3 + \omega + 4)(A_1^2 A_2^2 B_2^4) + (-2\omega^3 - 4\omega^2 + 1)(A_1 A_2^3 B_1^4) \\
& + (\omega^3 + \omega^2 + \omega + 2)(A_1 A_2^3 B_1^3 B_2) + (\omega^3 + 3\omega + 1)(A_1 A_2^3 B_1^2 B_2^2) \\
& - (7\omega^3 + 7\omega^2 + 4\omega + 7)(A_1 A_2^3 B_1 B_2^3) - (3\omega^3 + 2)(A_1 A_2^3 B_2^4) \\
& + (-2\omega^3 + 2\omega^2 + 3\omega + 2)(A_2^4 B_1^4) - (3\omega^3 + 1\omega^2 + 3\omega + 3)(A_2^4 B_1^3 B_2) \\
& - (2\omega^3 + 3\omega + 5)(A_2^4 B_1^2 B_2^2) - (4\omega^3 + 5\omega^2 + 2\omega + 4)(A_2^4 B_1 B_2^3) \\
& - (4\omega^3 + 6\omega^2 + 5\omega + 5)(A_2^4 B_2^4).
\end{aligned}
$$