On a quantum two-way deterministic and d-dimensional cryprographic scheme

Anita Eusebi
School of Science and Technology, University of Camerino
anita.eusebi@unicam.it

Stefano Mancini
School of Science and Technology, University of Camerino
stefano.mancini@unicam.it

The pioneering protocol for Quantum Key Distribution (QKD) is known to be the BB84. This allows two remote parties (Alice and Bob) to share a secret key by a *unidirectional* use of a quantum channel. It has a *probabilistic* character, that is, on each use of quantum channel, the sender (Alice) is not sure that the encoded symbol will be correctly decoded by the receiver (Bob).

In the last decade a new generation of protocols has been introduced realizing QKD processes in a *deterministic* way: in this case Alice is sure about the fact that Bob will exactly decode the symbol she has encoded. This paradigm shift can been realized by a *bidirectional* use of the quantum channel, as in the LM05 protocol [Phys. Rev. Lett. 94, 140501 (2005)].

Here, we present a protocol that realizes an extension of the LM05 protocol to a d-ary alphabet. Since our construction is based on *Mutually Unbiased Bases* (MUB), it holds only for prime power dimensions $d = p^m$, with p prime number and m positive integer.

Let us consider a qudit, i.e., a d-dimensional quantum system, and indicate with $\mathcal{H}_d$ the associated Hilbert space. A set of orthonormal bases in $\mathcal{H}_d$ is called a set of MUB if the absolute value of the inner product of any two vectors from different bases is $1/\sqrt{d}$ (MUBness condition).

We denote the $d+1$ MUB of $\mathcal{H}_d$ by $|v_t^k\rangle$, with $k = 0, 1, \ldots, d$ and $t = 0, 1, \ldots, d-1$ labelling the basis and the vector in it respectively. Hence, we choose $\{|v_t^0\rangle\}_{t=0,\ldots,d-1}$ as the computational basis and use the explicit formula for MUB's vectors to express the vectors of any other basis in the following compact way:

$$|v_t^k\rangle = \frac{1}{\sqrt{d}} \sum_{q=0}^{d-1} \omega^{\ominus q \odot t} (\omega^{(k-1)\odot q \odot q})^{\frac{1}{2}} |v_q^0\rangle \,, \tag{1}$$

where $k = 1, \ldots, d$, $t = 0, 1, \ldots, d-1$, ω is the p-th root of unity $e^{i2\pi/p}$ and the circled operations are in the Galois fields $G = \mathbb{F}(p^m)$ of d elements.

For d even the correct determination of the square root's sign is:

$$(\omega^{(j-1)\odot q \odot q})^{\frac{1}{2}} = \prod_{\substack{n=0 \\ q_n \neq 0}}^{m-1} i^{(j-1)\odot 2^n \odot 2^n} \omega^{(j-1)\odot 2^n \odot (q \bmod 2^n)} \,. \tag{2}$$

This determination corrects the one given in [J. Phys. A: Math. Gen. 38 (2005)] and makes the MUBness condition hold for d any prime power, both even and odd (see Appendix in [1] for the even case).

The description of the protocol is the following. We consider Bob sending to Alice a qudit state randomly chosen from the set $\{|v_t^k\rangle\}_{t=0,\ldots,d-1}^{k=1,\ldots,d}$ of MUB. Then, whatever is the state, Alice encodes a symbol a belonging to a d-ary alphabet $A = \{0, \ldots, d-1\}$ (identifiable with the Galois

field G) by applying the following shift operator V_0^a (which can be regarded as a generalized Pauli Z operator):

$$V_0^a \, |v_t^k\rangle = \frac{1}{\sqrt{d}} \sum_{q=0}^{d-1} \omega^{\ominus q \odot (t \ominus a)} (\omega^{(k-1) \odot q \odot q})^{\frac{1}{2}} |v_q^0\rangle = |v_{t \ominus a}^k\rangle \, . \tag{3}$$

In such a case, Bob receiving back the state $|v_{t\ominus a}^k\rangle$ realizes a projective measurement onto the k-th basis and he get the value $b = t \ominus a$, from which, knowing t, he can extract a. Then, the protocol runs as follows:

1. Bob randomly prepares one of the d^2 qudit states $|v_t^k\rangle$, with $k = 1, \ldots, d$ and $t = 0, \ldots, d-1$, and sends it to Alice.

2. Alice, upon receiving the qudit state has two options.

a) With probability $c \neq 0$, she performs a measurement by projecting over a randomly chosen basis among the d bases with $k = 1, \ldots, d$ (*Control Mode*). She then sends back to Bob the resulting state.

b) With probability $1 - c$, she encodes a symbol $a \in A$ by applying the unitary operator V_0^a (*Message Mode*). She then sends back to Bob the resulting state.

3. Bob, upon receiving back the qudit state, performs a measurement by projecting over the basis to which the qudit state initially belonged.

4. At the end of the transmission, Alice publicly declares on which runs she performed the control mode and on which others the message mode. In the first case, Alice announces the bases over which she measured. Then, by public discussion, a comparison of Alice's and Bob's measurements results is performed over coincident bases. In the ideal case (noiseless channels and no eavesdropping) their results must coincide. In the message mode runs, Bob gets the encoded symbol a as discussed above.

Then, we prove the security of the protocol against a powerful individual attack. Eve lets the carrier of information interact with an ancilla system she has prepared. Then, she tries to gain information in the forward path about the state Bob sends to Alice and in the backward path about the state Alice sends back to Bob, hence about Alice's transformation, by measuring her ancilla.

In particular, we consider the unitary transformation describing the attack as controlled shifts $\{V_0^l\}_{l\in A}$, where the controller is the traveling qudit, while the target is in the Eve's hands. That is, $C\{V_0^l\}_{l\in A} : \mathcal{H}_d \otimes \mathcal{H}_d \to \mathcal{H}_d \otimes \mathcal{H}_d$ defined as follows:

$$|v_{t_1}^1\rangle |v_{t_2}^1\rangle \xrightarrow{C\{V_0^l\}_{l\in A}} |v_{t_1}^1\rangle V_0^{l=t_1} |v_{t_2}^1\rangle = |v_{t_1}^1\rangle |v_{t_2\ominus t_1}^1\rangle. \tag{4}$$

Notice that the controller as well as the target states are considered in the dual basis for the sake of simplicity. Other choices (except the computational basis) give the same final results.

Then, we consider Eve intervening in the forward path with $(C\{V_0^l\}_{l\in A})^{-1}$, defined by

$$|v_{t_1}^1\rangle |v_{t_2}^1\rangle \xrightarrow{(C\{V_0^l\}_{l\in A})^{-1}} |v_{t_1}^1\rangle V_0^{\ominus t_1} |v_{t_2}^1\rangle = |v_{t_1}^1\rangle |v_{t_2\ominus(\ominus t_1)}^1\rangle = |v_{t_1}^1\rangle |v_{t_2\oplus t_1}^1\rangle, \tag{5}$$

and with $C\{V_0^l\}_{l\in A}$ in the backward path.

The protocol is summarized in the following scheme, where the label $\mathcal{A}$ denotes Alice's operation on Bob's qudit, so the labels $\mathcal{B}$ and $\mathcal{E}$ stand for Bob's and Eve's qudit systems respectively.

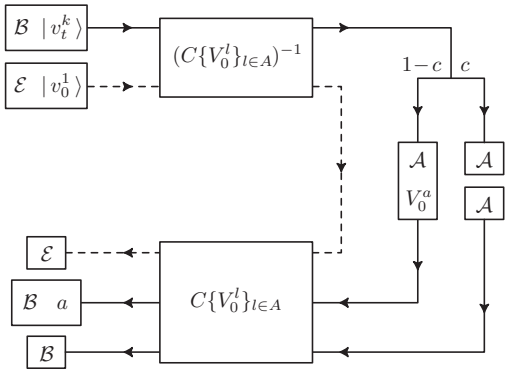

Fig. 1

By analizing the message mode and the control mode processes, we obtain that

$$I_{\mathcal{E}} = \log_2 d \quad \text{and} \quad P_{\mathcal{E}} = \frac{(d-1)^2}{d^3}\,, \tag{6}$$

where $I_{\mathcal{E}}$ is the information that Eve is able to steal on each encoding run and $P_{\mathcal{E}}$ is the probability that Alice and Bob have to reveal Eve on each control run. Then, the security of the protocol is maximal for $d = 3$.

In Fig. 2 we show the behavior of $P_{\mathcal{E}}$ versus the dimension d (the bars correspond to prime power numbers).

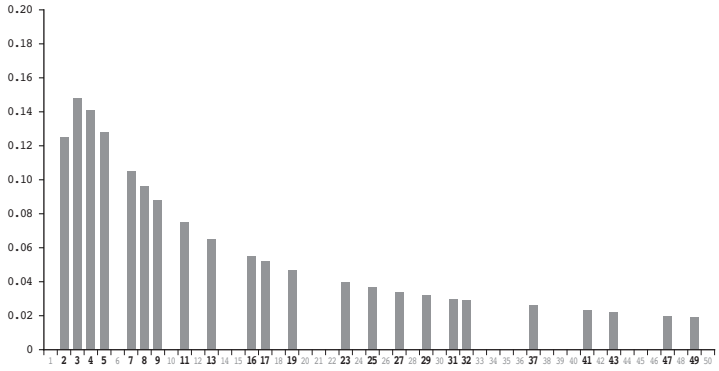

Fig. 2

At this point, we propose an innovative way of realizing the control process to guarantee the security of the protocol [2]. Instead of the usual quantum measurement as in the previous case, we introduce the control by means of a suitable unitary transformation applied by Alice. Such an operator should realize a permutation of vectors within each basis, to allow Bob a reliable data gathering, but not cyclic shift, to differ from the encoding.

An operator W, satisfying such conditions, can be defined as acting on the MUBs in the following way:

$$W\,|v_t^k\rangle = |v_{\ominus t}^k\rangle\,. \tag{7}$$

Notice that it works only when d is an odd prime power dimension. In fact, for $d = 2^m$ the W operator reduces to the identity , which is not acceptable. It seems reasonable to suppose

that it does not exist any transformation of this kind when d is a power of 2, and moreover that W is the only kind of operator with the required properties when d is an odd prime.

Then, the new protocol differs from the previous one only for the Alice's action in the control mode.

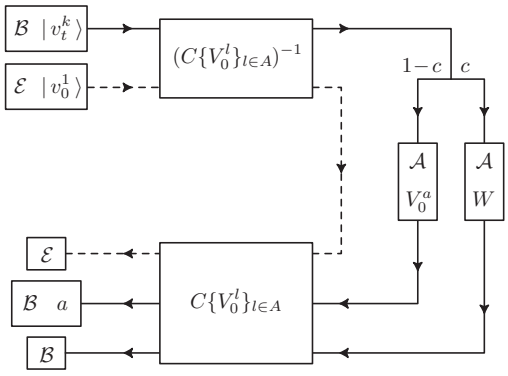

Fig. 3

In this case we obtain that

$$P_{\mathcal{E}} = \frac{(d-1)^2}{d^2}\,. \tag{8}$$

Notice that this quantity is largely greater than the analogous obtained with control strategy based upon measurement. Essentially that happens because here only Bob perfoms a measurement (at the end of path) and he knowns what is the correct basis over which to project (that is the one to which the initial qudit state belonged).

In conclusion, we get an improvement of the security, which we prove to increase with the alphabet order d.

We show in Fig. 4 the behavior of $P_{\mathcal{E}}$ as fuction of the order d of the alphabet. The bars correspond to odd prime power numbers.

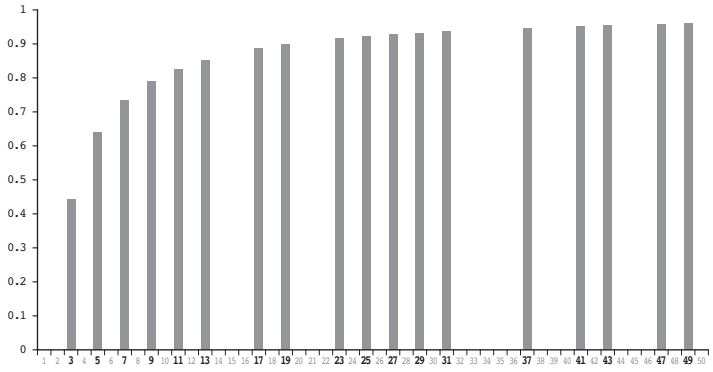

Fig. 4

Finally, we also address the issue of Quantum Direct Communication (QDC) and see that in this case the optimal dimension is $d = 3$.

[1] A. Eusebi and S. Mancini, *Deterministic quantum distribution of a d-ary key*, Quantum Inf. & Comp. **9**, 950 (2009). [2] A. Eusebi and S. Mancini, *Improving the Control Strategy in two-way deterministic cryptographic protocols*, arXiv:1005.1222v1, submitted to IJQI.