Quantum Information and Computation, Vol. 9, No. 11&12 (2009) 0950–0962

DETERMINISTIC QUANTUM DISTRIBUTION OF A d-ARY KEY

A. EUSEBI *
Dipartimento di Matematica ed Informatica, Università di Camerino
I-62032 Camerino, Italy

S. MANCINI †
Dipartimento di Fisica, Università di Camerino
I-62032 Camerino, Italy

Received March 2, 2008
Revised July 23, 2009

We present an extension to a d-ary alphabet of a recently proposed deterministic quantum key distribution protocol. It relies on the use of mutually unbiased bases in prime power dimension d, for which we provide an explicit expression. Then, by considering a powerful individual attack, we show that the security of the protocol is maximal for $d = 3$.

Keywords: Quantum Key Distribution, Generalized Pauli Operators, Mutually Unbiased Bases, Galois fields.
Communicated by: B Kane & H Zbinden

1. Introduction

Quantum Key Distribution (QKD) is recognized to complement the One Time Pad to a secure system for reliable transfer of confidential information [1]. A paradigm for QKD (not exploiting entanglement) is the pioneering BB84 protocol [2]. It allows two remote parties (Alice and Bob) to share a secret key by a *unidirectional* use of a quantum channel (supplemented by a public authenticated classical channel).

Protocols like BB84 have a *probabilistic* character, in the sense that, on each use of the quantum channel, the sender (Alice) is not sure that the encoded symbol will be correctly decoded by the receiver (Bob). Tipically, this only happens with probability 1/2.

Recently a new generation of protocols has been introduced making the QKD process *deterministic* [3, 4, 5, 6]. In this case Alice is sure about the fact that Bob will exactly decode the symbol she has encoded. This paradigm shift has been realized by a *bidirectional* use of the quantum channel. These new generation protocols are more versatile than the old generation ones and are supposed to outperform them.

As much as like extensions of BB84 to larger alphabets have been developed [7, 8], there is a persistent aim to also extend the protocol of [6] to larger alphabets, that is to higher dimensions. A construction has been recently devised for a tri-dimensional alphabet [9, 10], and then another for a continuous infinite-dimensional alphabet [11].

*e-mail address: anita.eusebi(at)unicam.it
†e-mail address: stefano.mancini(at)unicam.it

Here we present a protocol that realizes an extension of the deterministic protocol of [6] to a d-ary alphabet. Since our construction is based on Mutually Unbiased Bases (MUB) [12, 13, 14, 15], it holds only for prime power dimensions d. We will provide an explicit expression for MUB encompassing powers of both even and odd primes, by correcting the one given in [16].

We then consider a powerful individual attack on the forward and backward path of the quantum channel and we show that the security for $d = 3, 4, 5$ is higher than that at $d = 2$ and is maximal for $d = 3$.

2. Qudits and Mutually Unbiased Bases

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 *Mutually Unbiased Bases* (MUB) if the absolute value of the inner product of any two vectors from different bases is $1/\sqrt{d}$ [12, 13, 14, 15].

It is known that in $\mathcal{H}_d$, when d is prime power, there exists a maximal set of $d+1$ MUB [12, 13, 14, 15]. Here, we focus on this case.

From now on we assume that $d = p^m$, with p a prime number and m positive integer, and 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.

Thus, for every $k, k' = 0, 1, \ldots, d$ and every $t, t' = 0, 1, \ldots, d-1$, the following equality holds:

$$\left|\langle v_t^k | v_{t'}^{k'} \rangle\right| = \frac{1}{\sqrt{d}} (1 - \delta_{k,k'}) + \delta_{t,t'}\delta_{k,k'}, \tag{1}$$

where δ stands for the Kronecker delta.

We deal with the Galois field $G = \mathbb{F}(p^m)$ of d elements. We denote by $\oplus$ and $\odot$ respectively the addition and the multiplication in the field G (by $\ominus$ and $\oslash$ the subtraction and the division in G). Usually, an element of G is represented by a m-tuple $(g_0, g_1, \ldots, g_{m-1})$ of integers modulo p. According to this representation, $\oplus$ corresponds to the componentwise addition modulo p.

Following [16], we identify G with $\{0, 1, \ldots, d-1\}$, paying attention to distinguish the operations in the field from the usual ones. Namely, we identify $(g_0, g_1, \ldots, g_{m-1})$ with the integer $g = \sum_{n=0}^{m-1} g_n p^n$. This allows us to consider the vector label t in $|v_t^k\rangle$ as an element of G.

Let us denote the p-th root of unity by

$$\omega = e^{i2\pi/p}. \tag{2}$$

It is proved in [16] that

$$\omega^j \cdot \omega^l = \omega^{j \oplus l} \quad \text{with } j, l \in G \tag{3}$$

and

$$\sum_{j=0}^{d-1} \omega^{j \odot l} = d\,\delta_{l,0} \quad \text{with } l \in G. \tag{4}$$

We choose $\{|v_t^0\rangle\}_{t=0,\ldots,d-1}$ as the computational basis and use the explicit formula given in [16] to express the vectors of any other basis in the following compact way:

$$|v_t^k\rangle = \frac{1}{\sqrt{d}} \sum_{q=0}^{d-1} \omega^{\ominus q \odot t} (\omega^{(k-1)\odot q \odot q})^{\frac{1}{2}} |v_q^0\rangle, \tag{5}$$

where $k = 1, \ldots, d$ and $t = 0, 1, \ldots, d-1$. In particular for $k = 1$:

$$|v_t^1\rangle = \frac{1}{\sqrt{d}} \sum_{q=0}^{d-1} \omega^{\ominus q \odot t} |v_q^0\rangle. \tag{6}$$

As it is pointed out in [16], for p odd the square root coincides with the division of the exponent by 2 in G and it is uniquely determined. On the contrary, for $p = 2$ it is necessary to unambiguosly determine the square root's sign. This is given by (see Appendix)

$$(\omega^{(j-1)\odot q \odot q})^{\frac{1}{2}} = \prod_{\substack{n=0 \\ q_n \neq 0}}^{m-1} i^{(j-1)\odot 2^n \odot 2^n} \omega^{(j-1)\odot 2^n \odot (q \bmod 2^n)}. \tag{7}$$

With this in mind, the expression (5) satisfies the condition (1) of MUB, for d any prime power, both even and odd (see Appendix for the proof). Hence, in the following we will make use of (5) without distinguishing the two cases.

3. The protocol

Moving from the protocol of [6], 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 has to encode a symbol belonging to a d-ary alphabet $A = \{0, \ldots, d-1\}$ in such a way that Bob will be able to unambiguously decode it (deterministic character of the protocol). The alphabet A can be identified with the Galois field G. Moreover, let us consider the unitary transformations V_0^a for $a \in A$, defined by

$$V_0^a \, |v_t^0\rangle = \omega^{t \odot a} |v_t^0\rangle, \tag{8}$$

which can be regarded as the generalized Pauli Z operators.

Then, Alice encoding operation will be the shift operation realized by the operator V_0^a with $a \in A$ on all the MUB but the computational one, that is for $k > 0$:

$$V_0^a \, |v_t^k\rangle = \frac{1}{\sqrt{d}} \sum_{q=0}^{d-1} \omega^{\ominus q \odot (t \ominus a)} (\omega^{(k-1)\odot q \odot q})^{\frac{1}{2}} |v_q^0\rangle = |v_{t \ominus a}^k\rangle. \tag{9}$$

In such a case, Bob receiving back the state $|v_{t\ominus a}^k\rangle$ can unambiguously determine a by means of a projective measurement onto the k-th basis. In fact, he will get the value

$$b = t \ominus a \tag{10}$$

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.

Notice at the above point 2. the deterministic character of the protocol given by the possibility for Alice, besides to decide when to encode, to determine the message (key) sequence, since she knows that Bob will unambigously decode each character of the message (key).

4. Security of the protocol

Among individual attacks the most elementary one is the *Intercept-Resend*. Suppose Eve, to learn Alice's operation, performs projective measurements on both paths of the traveling qudit, randomly choosing the measuring basis. She will steal the whole information for each message mode run, indipedently from the chosen basis. However, in each control mode run with coincident bases for Alice and Bob, she can guess the correct basis with probability $1/d$, and in this case she is not detected at all. If otherwise Eve chooses the wrong basis, she still has a probability $1/d$ to evade detection on the forward path and probability $1/d$ on the backward path, leading to an overall probability $1/d^2$ to remain undetected. This means that the double test of Alice and Bob reveals Eve with probability $(d^2-1)(d-1)/d^4$, including the cases of non-coincident bases.

We are going to prove the security of the protocol against a more powerful individual attack. Quite generally, in individual attacks Eve lets the carrier of information interact with an ancilla system she has prepared and then try to gain information by measuring the ancilla. In this protocol she has to do that two times, in the forward path (to gain information about the state Bob sends to Alice) and in the backward path (to gain information about the state Alice sends back to Bob, hence about Alice's transformation). Moreover, by using the same ancilla in the forward and backward path, Eve could benefit from quantum interference effects (see Fig. 1).

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:

$$|v_{t_1}^1\rangle|v_{t_2}^1\rangle \xrightarrow{C\{V_0^l\}_{l\in A}} |v_{t_1}^1\rangle V_0^{l=t_1}|v_{t_2}^1\rangle = |v_{t_1}^1\rangle|v_{t_2\ominus t_1}^1\rangle. \tag{11}$$

We remark that, in this definition, 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) will 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

$$|v_{t_1}^1\rangle|v_{t_2}^1\rangle \xrightarrow{(C\{V_0^l\}_{l\in A})^{-1}} |v_{t_1}^1\rangle V_0^{\ominus t_1}|v_{t_2}^1\rangle = |v_{t_1}^1\rangle|v_{t_2\ominus(\ominus t_1)}^1\rangle = |v_{t_1}^1\rangle|v_{t_2\oplus t_1}^1\rangle, \tag{12}$$

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

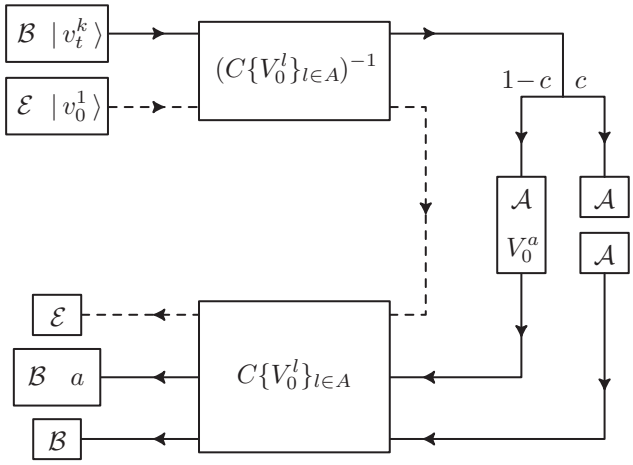

Fig. 1. The scheme summarizing our protocol. Labels $\mathcal{B}$ and $\mathcal{E}$ stand for Bob's and Eve's qudit systems respectively. Label $\mathcal{A}$ denotes Alice's operation on Bob's qudit. $(C\{V_0^l\}_{l\in A})^{-1}$ and $C\{V_0^l\}_{l\in A}$ represent the eavesdropping operations on the forward and backward path respectively.

4.1. *Message Mode*

Now, let us analyze in detail the transformations of the quantum states on an entire message mode run.

Attack on the forward path.

The initial Bob state is one of the d^2 states $|v_t^k\rangle$, with $k = 1, \ldots, d$ and $t = 0, \ldots, d-1$. Then, Eve initially prepares the ancilla state $|v_0^1\rangle_{\mathcal{E}}$ in the dual basis and performs the controlled operation. Hence, we get

$$|v_t^k\rangle_{\mathcal{B}}|v_0^1\rangle_{\mathcal{E}} \xrightarrow{(C\{V_0^l\}_{l\in A})^{-1}} \sum_{h=0}^{d-1}\langle v_h^1|v_t^k\rangle|v_h^1\rangle_{\mathcal{B}}|v_0^1\rangle_{\mathcal{E}} = \sum_{h=0}^{d-1}\langle v_h^1|v_t^k\rangle|v_h^1\rangle_{\mathcal{B}}|v_h^1\rangle_{\mathcal{E}}. \tag{13}$$

Encoding.

The Bob's qudit state undergoes the shift V_0^a with $a \in A$, then from (13) we get

$$\xrightarrow{V_0^a} \sum_{h=0}^{d-1} \langle v_h^1 | v_t^k \rangle | v_{h\ominus a}^1 \rangle_{\mathcal{B}} | v_h^1 \rangle_{\mathcal{E}}. \tag{14}$$

Attack on the backward path.

The state (14) undergoes a $C\{V_0^l\}_{l\in A}$ operation, hence we have

$$\xrightarrow{C\{V_0^l\}_{l\in A}} \sum_{h=0}^{d-1} \langle v_h^1 | v_t^k \rangle | v_{h\ominus a}^1 \rangle_{\mathcal{B}} | v_{h\ominus(h\ominus a)}^1 \rangle_{\mathcal{E}} = \sum_{h=0}^{d-1} \langle v_h^1 | v_t^k \rangle | v_{h\ominus a}^1 \rangle_{\mathcal{B}} | v_a^1 \rangle_{\mathcal{E}} = | v_{t\ominus a}^k \rangle_{\mathcal{B}} | v_a^1 \rangle_{\mathcal{E}}. \tag{15}$$

Then, Eve measures her ancilla system by projecting in the dual basis, according to the chosen initial ancilla state.

We notice that the controlled operations performed by Eve, as well as her final measurement, left unchanged Bob's qudit state. Hence, Bob's measurement by projection in the k-th basis to which the initial state belonged, always allows him to obtain the symbol a Alice has encoded [see (10)].

On the other hand, Eve gets $|v_a^1\rangle$ with probability 1 as the result of her measurement. Therefore, she is able to exactly determine the encoded symbol a as well and she steals the whole information, quantified in bits,

$$I_{\mathcal{E}} = \log_2 d \tag{16}$$

on each message mode run.

4.2. *Control Mode*

We would like to evaluate the probability $P_{\mathcal{E}}$ Alice and Bob have to reveal Eve on each control mode run. Alice and Bob only compare the results of their measurements when, by public discussion, they agree on the used basis.

Let us focus on the case Alice and Bob use the same basis k, keeping in mind that it happens with probability $1/d$. The situation is different for $k = 1$ and $k \neq 1$, due to the Eve's choice of using the dual basis for her ancilla.

1) For $k = 1$, on the forward path we have

$$|v_t^1\rangle_{\mathcal{B}} | v_0^1 \rangle_{\mathcal{E}} \xrightarrow{(C\{V_0^l\}_{l\in A})^{-1}} |v_t^1\rangle_{\mathcal{B}} | v_t^1 \rangle_{\mathcal{E}}. \tag{17}$$

Alice, measuring in the dual basis, gets $\bar{t}$ with probability 1 and projects into $|\bar{t}\rangle_{\mathcal{B}}$. On the backward path we have

$$|v_t^1\rangle_{\mathcal{B}} | v_t^1 \rangle_{\mathcal{E}} \xrightarrow{C\{V_0^l\}_{l\in A}} |v_t^1\rangle_{\mathcal{B}} | v_{t\ominus t}^1 \rangle_{\mathcal{E}} = |v_t^1\rangle_{\mathcal{B}} | v_0^1 \rangle_{\mathcal{E}}. \tag{18}$$

Bob, in turn, by measuring in the dual basis gets t with probability 1. Thus, Alice and Bob have perfect correlation and $P_{\mathcal{E}} = 0$.

2) For $k = 2, \ldots, d$, we get on the forward path

$$|v_t^k\rangle_{\mathcal{B}}|v_0^1\rangle_{\mathcal{E}} = \sum_{h=0}^{d-1}\langle v_h^1|v_t^k\rangle|v_h^1\rangle_{\mathcal{B}}|v_0^1\rangle_{\mathcal{E}} \xrightarrow{(C\{V_0^l\}_{l\in A})^{-1}} \sum_{h=0}^{d-1}\langle v_h^1|v_t^k\rangle|v_h^1\rangle_{\mathcal{B}}|v_h^1\rangle_{\mathcal{E}}. \tag{19}$$

By expressing the vectors of the dual basis in terms of the basis k used by Bob, we rewrite the right hand side of (19) as

$$\sum_{h=0}^{d-1}\langle v_h^1|v_t^k\rangle \sum_{s=0}^{d-1}\langle v_s^k|v_h^1\rangle|v_s^k\rangle_{\mathcal{B}}|v_h^1\rangle_{\mathcal{E}}. \tag{20}$$

At this point Alice measures in the basis k. The result of her measurement is to project into $|v_{t'}^k\rangle$, whatever $t' \in A$ is, with probability

$$\sum_{h=0}^{d-1}|\langle v_h^1|v_t^k\rangle\langle v_{t'}^k|v_h^1\rangle|^2 = \sum_{h=0}^{d-1}|\langle v_h^1|v_t^k\rangle|^2|\langle v_{t'}^k|v_h^1\rangle|^2 = \sum_{h=0}^{d-1}\frac{1}{d^2} = \frac{1}{d} \tag{21}$$

according to definition of MUB.

Among the d possibilities we distinguish two cases.

a) $t' = t$, occurring with probability $1/d$, for which the resulting state from (20) is

$$\sqrt{d}\sum_{h=0}^{d-1}\langle v_h^1|v_t^k\rangle\langle v_t^k|v_h^1\rangle|v_t^k\rangle_{\mathcal{B}}|v_h^1\rangle_{\mathcal{E}} = \frac{1}{\sqrt{d}}\sum_{h=0}^{d-1}|v_t^k\rangle_{\mathcal{B}}|v_h^1\rangle_{\mathcal{E}}. \tag{22}$$

We have now to apply the $C\{V_0^l\}_{l\in A}$ operation of the backward path. Thus, (22) transforms as follows

$$|v_t^k\rangle_{\mathcal{B}}\frac{1}{\sqrt{d}}\sum_{h=0}^{d-1}|v_h^1\rangle_{\mathcal{E}} = \sum_{h'=0}^{d-1}\langle v_{h'}^1|v_t^k\rangle|v_{h'}^1\rangle_{\mathcal{B}}\frac{1}{\sqrt{d}}\sum_{h=0}^{d-1}|v_h^1\rangle_{\mathcal{E}} \tag{23}$$

$$\xrightarrow{C\{V_0^l\}_{l\in A}} \sum_{h'=0}^{d-1}\langle v_{h'}^1|v_t^k\rangle|v_{h'}^1\rangle_{\mathcal{B}}\frac{1}{\sqrt{d}}\sum_{h=0}^{d-1}|v_{h\ominus h'}^1\rangle_{\mathcal{E}} = |v_t^k\rangle_{\mathcal{B}}\frac{1}{\sqrt{d}}\sum_{r=0}^{d-1}|v_r^1\rangle_{\mathcal{E}}, \tag{24}$$

where $r = h \ominus h'$.

It results that Eve's attack does not alter the eigenvector $|v_t^k\rangle_{\mathcal{B}}$. Hence, Bob upon his measurement will get t with probability 1. Then, neither Alice nor Bob outwit Eve's attacks.

b) $t' \neq t$, occurring with probability $(d-1)/d$, for which Alice, getting a state different from the one initially sent by Bob, outwits Eve in the forward path. Hence, in this case, we do not need to explicitly evaluate the state change in the backward path.

In summary, from the analyzed cases, we have:

- $1/d$ the probability with which Bob and Alice measure in the same basis k;
- $(d-1)/d$ the probability of Bob choosing the initial state $|v_t^k\rangle$ from any basis but the dual one, that is $k \neq 1$;

- $(d-1)/d$ the probability that the state $|v_t^k\rangle$ sent by Bob gives a measurement result $|v_{t'}^k\rangle$ with $t' \neq t$ to Alice.

We then conclude that the probability for Alice and Bob to outwit Eve on each control mode run is

$$P_{\mathcal{E}} = \frac{1}{d} \cdot \frac{d-1}{d} \cdot \frac{d-1}{d} = \frac{(d-1)^2}{d^3} \,. \tag{25}$$

In Fig. 2 we show the behavior of $P_{\mathcal{E}}$ versus the order d of the alphabet. Interestingly enough, the values of $P_{\mathcal{E}}$ at $d = 3, 4, 5$ are higher than that at $d = 2$. In particular, $P_{\mathcal{E}}$ has a maximum at $d = 3$ showing that this dimension represents the optimal compromise between two different trends. On the one hand, the probability $(d-1)^2/d^2$ of revealing Eve in each successful control mode run (that is when the bases of Alice and Bob coincide) increases towards 1 when increasing the dimension d. On the other hand, the efficiency of the whole control process decreases according to the probability $1/d$ for each control mode run to succeed.

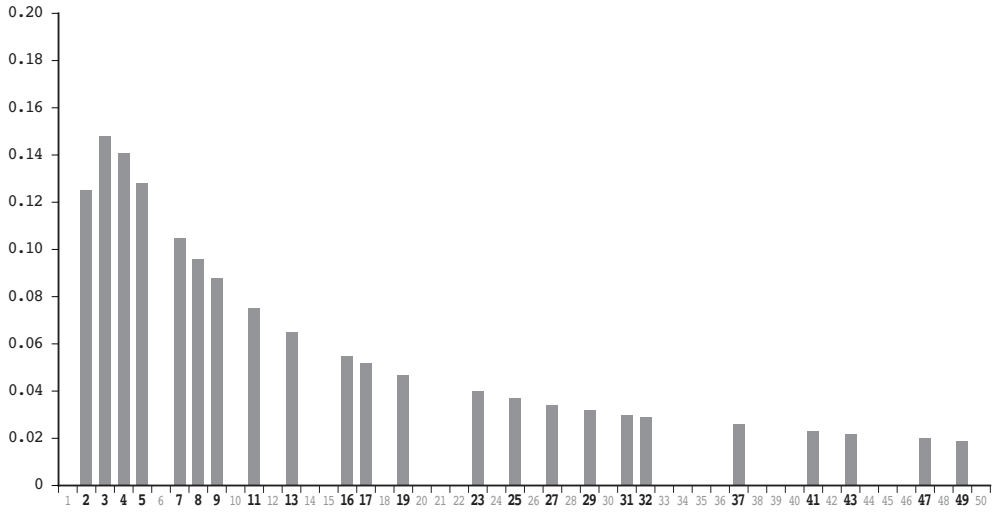

Fig. 2. The probability $P_{\mathcal{E}}$ versus the dimension d (bars correspond to prime power numbers).

5. Concluding remarks

We have proposed a deterministic cryptographic protocol working with a d-ary alphabet and exploiting a bidirectional quantum channel. When considering an attack performed by means of controlled operations on both directions of the quantum channel, we have found that Eve can steal the total amount of information $I_{\mathcal{E}}$ (see (16)), while the probability $P_{\mathcal{E}}$ to outwit her presents a maximum for $d = 3$ (see (25)).

Contrarily to probabilistic protocols, the deterministic nature of this protocol also allows the realization of Quantum Direct Communication (QDC) between legitimate users [3, 4, 5, 6]. In this case Alice and Bob (after authentication) can communicate directly the meaningful message without encryption. However, for this kind of communication only an asymptotic

security can be proven. In fact, if we assume that Eve wants to perform her attack on each message mode run, without having been detected in the previous control mode runs, then the probability is given by following geometric series:

$$(1-c)+c(1-P_{\mathcal{E}})(1-c)+c^2(1-P_{\mathcal{E}})^2(1-c)+\ldots=\frac{1-c}{1-c(1-P_{\mathcal{E}})}. \tag{26}$$

Thus, being $I_{\mathcal{E}}$ the quantity of information that Eve eavesdrops in a single attack, the probability that she successfully eavesdrops an amount of information I is

$$\left(\frac{1-c}{1-c\big(1-P_{\mathcal{E}}\big)}\right)^{I/I_{\mathcal{E}}}, \tag{27}$$

with $I_{\mathcal{E}}$ and $P_{\mathcal{E}}$ given in (16) and (25) respectively.

We observe that such a probability exponentially decreases towards 0 as a function of I for each given dimension d. So, (27) expresses the asymptotic security of the direct communication use of the protocol.

However, in this case the probability for Alice and Bob to detect Eve before she can eavesdrop a fixed amount of information, that is the complement of probability in (27), is maximal for $d = 2$.

It is interesting to notice that the optimal dimension depends on the specific task of the protocol (QKD or QDC). Therefore, we believe that this work might open up new horizons for deterministic cryptographic protocols involving finite dimensional systems.

Acknowledgments

We are grateful to T. Durt for correspondence on the subject of MUB and to M. Lucamarini, R. Piergallini and C. Toffalori for interesting discussions and a careful reading of the ms.

References

1. Physics World (March 1998).
2. C. H. Bennett and G. Brassard, Proc. of IEEE Int. Conf, on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984).
3. A. Beige, B.-G. Englert, C. Kurtsiefer, H. Weinfurter J. Phys. A: Math. Gen. **35**, L407 (2002).
4. K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
5. Q.-Y. Cai and B.-W. Li, Chin. Phys. Lett. **21**, 601 (2004).
6. M. Lucamarini and S. Mancini, Phys. Rev. Lett. **94**, 140501 (2005).
7. H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
8. N. Cerf, M. Bourennane, A. Karlsonn and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
9. J. S. Shaari, M. Lucamarini and M. R. B. Wahiddin, Phys. Lett. A **358**, 85 (2006);
10. J. S. Shaari and M. R. B. Wahiddin, Phys. Lett. A **361**, 445 (2007).
11. S. Pirandola, S. Mancini, S. Braunstein and S. Lloyd, Nat. Phys. **4**, 726 (2008).
12. I. D. Ivanovic, J. Phys. A **14**, (1981) 3241.
13. W. K. Wootters and B. D. Fields, Ann. Phys. **191**, 363 (1989).
14. S. Bandyopadhyay, P. O. Boykin, V. Roychowdhuri and F. Vatan, Algorithmica **34**, 512 (2002).
15. A. Klappenecker and M. Rötteler, Finite Fields and Applications, 137, Lecture Notes in Comput. Sci., **2948**, Springer, Berlin, (2004).
16. T. Durt, J. Phys. A: Math. Gen. **38**, 5267 (2005).

Appendix A

In [16] it has been provided expression (5) for MUB's vectors as potentially utilizable also in even prime power dimensions (besides odd prime powers). However, the recipe to do that contains some imprecisions, though the underlying idea based on the group properties of the Generalized Pauli Operators is essentially valid.

Then, we are going to give hereafter a correct proof of MUBness for even prime powers in order to have expression (5) really useful.

By referring to [16], let us denote by V_l^j the operators given by the composition of the shifts in the computational and the dual basis, that is

$$V_l^j = V_0^j \cdot V_l^0 = \sum_{t=0}^{d-1} \omega^{(t\oplus l)\odot j} |t \oplus l\rangle\langle t|. \tag{A.1}$$

This set of operators coincides with the Generalized Pauli Group (see [14]). The V_l^j's are d^2 unitary transformations which satify the following composition law

$$V_l^j \cdot V_{l'}^{j'} = \omega^{(l\odot j')} V_{l\oplus l'}^{j\oplus j'}, \tag{A.2}$$

and, up to phases, they form $d+1$ commuting subgroups of d elements that have only the identity in common. The k-th subgroup, with $k = 0, \ldots, d$, admits $\{|v_t^k\rangle\}_{t=0,\ldots,d-1}$ as diagonalizing basis. Its elements are denoted by U_l^k with $l = 0, \ldots, d-1$, and they are required to satisfy:

$$U_{l\oplus l'}^k = U_l^k \cdot U_{l'}^k, \tag{A.3}$$

$$U_l^k = \sum_{t=0}^{d-1} \omega^{t\odot l} |v_t^k\rangle\langle v_t^k|, \tag{A.4}$$

$$U_l^k = V_l^{(k-1)\odot l} \quad \text{up to a phase which is 1 for } l = 0. \tag{A.5}$$

It is important to point out that (A.2), (A.3), (A.4) and (A.5) must be guaranteed at the same time. In [16], the following relation is obtained from them:

$$U_l^k = (\omega^{\ominus(k-1)\odot l\odot l})^{\frac{1}{2}} V_l^{(k-1)\odot l} \tag{A.6}$$

In the odd prime power case such expression is completely determined and the phase is a p-th root of unity. In fact the square root can be interpreted as the division of the exponent by 2 in the Galois field G.

This is no longer true in the even prime power case. In this case the phase is not a 2-nd root of unity but a 4-th root of unity, that is it can also assume the values $\pm i$, other than ± 1. Moreover, the sign of it is still undetermined. The determination of such sign provided in [16] is uncorrect.

Below we correctly develop the last step of (32) in [16] getting the right sign, and consequently the square root's sign in (5), as indicated in (7).

First of all, we observe that for $p = 2$ we have $\omega = -1$.

In [16] it has been implicitly chosen the determination of the square root of $\omega^{(k-1)\odot 2^n \odot 2^n}$ as to be $i^{(k-1)\odot 2^n \odot 2^n}$. Then, we have:

$$U_l^k = \prod_{n=0}^{m-1} U_{l_n \odot 2^n}^k = \prod_{n=0}^{m-1} \left(U_{2^n}^k\right)^{l_n} = \left(\prod_{\substack{n=0 \\ l_n \neq 0}}^{m-1} i^{(k-1)\odot 2^n \odot 2^n}\right)\left(\prod_{\substack{n=0 \\ l_n \neq 0}}^{m-1} V_{2^n}^{(k-1)\odot 2^n}\right). \tag{A.7}$$

Let $n_0, n_1, \ldots n_h$ be the indices n_j such that $l_{n_j} = 1$. By taking into account (A.2), the second product can be rewritten as follows.

$$\begin{aligned}\prod_{\substack{n=0 \\ l_n \neq 0}}^{m-1} \left(V_{2^n}^{(k-1)\odot 2^n}\right) &= \left(\prod_{j=1}^{h} \omega^{(k-1)\odot(2^{n_0}\oplus 2^{n_1}\oplus\ldots\oplus 2^{n_{j-1}})\odot 2^{n_j}}\right) V_{(2^{n_0}\oplus\ldots\oplus 2^{n_h})}^{(k-1)\odot(2^{n_0}\oplus\ldots\oplus 2^{n_h})} \\ &= \left(\prod_{\substack{n=0 \\ l_n \neq 0}}^{m-1} \omega^{(k-1)\odot 2^n \odot (l \bmod 2^n)}\right) V_l^{(k-1)\odot l}. \end{aligned} \tag{A.8}$$

Then, we have:

$$U_l^k = \left(\prod_{\substack{n=0 \\ l_n \neq 0}}^{m-1} i^{(k-1)\odot 2^n \odot 2^n} \omega^{(k-1)\odot 2^n \odot (l \bmod 2^n)}\right) V_l^{(k-1)\odot l}. \tag{A.9}$$

This gives the correct determination of square root's sign in the phase as in (7), which can be rewritten as

$$\prod_{\substack{n=0 \\ l_n \neq 0}}^{m-1} i^{(k-1)\odot 2^n \odot 2^n} \omega^{(k-1)\odot 2^n \odot (l \bmod 2^n)} = \prod_{n=0}^{m-1} (-1)^{\sum_{h=0}^{n-1} l_n l_h (k-1)\odot 2^n \odot 2^h} i^{l_n (k-1)\odot 2^n \odot 2^n}. \tag{A.10}$$

Now, by referring to (3), we remark that an analogous property does not hold for powers of i with exponents in G. The reader can easily check that

$$i^j \cdot i^l = (-1)^{jl} i^{j\oplus l} = (-1)^{j_0 l_0} i^{j\oplus l}. \tag{A.11}$$

From (A.10) and (A.11) it follows that

$$(\omega^{(k-1)\odot l \odot l})^{1/2} (\omega^{(k'-1)\odot l \odot l})^{1/2} = \phi(k, k', l)\, (\omega^{((k-1)\oplus(k'-1))\odot l \odot l})^{\frac{1}{2}}, \tag{A.12}$$

where we have defined

$$\phi(k, k', l) = (-1)^{\sum_{n=0}^{m-1} l_n ((k-1)\odot 2^n \odot 2^n)((k'-1)\odot 2^n \odot 2^n)}. \tag{A.13}$$

By assuming $k' = k$ in (A.12), we get the conjugate of $(\omega^{(k-1)\odot q \odot q})^{\frac{1}{2}}$ as

$$\phi(k, k, q)\, (\omega^{(k-1)\odot q \odot q})^{\frac{1}{2}}. \tag{A.14}$$

Consequently, the correct expression for the inner products $\langle v_{t'}^{k'} | v_t^k \rangle$ with $k, k' \geq 1$ is the following (which does not coincide with (28) in [16]):

$$\langle v_{t'}^{k'} | v_t^k \rangle = \frac{1}{d} \sum_{q=0}^{d-1} \phi(k, k', q)\, \phi(k', k', q)\, \omega^{q\odot(t\oplus t')} (\omega^{((k-1)\oplus(k'-1))\odot q \odot q})^{\frac{1}{2}}. \tag{A.15}$$

In order to explicitly prove the MUB condition, we state the following elementary properties of the function ϕ:

$$\phi(k,k',0) = 1 \tag{A.16}$$
$$\phi(k',k,q) = \phi(k,k',q) \tag{A.17}$$
$$\phi(k,k',q)\,\phi(k,k',q') = \phi(k,k',q\oplus q') \tag{A.18}$$
$$\phi(k,k,q) = \omega^{(k-1)\odot q\odot q} \tag{A.19}$$

The first and the second one come from the very definition of ϕ, the third one comes from the fact that $q_n + q'_n \bmod 2 = (q\oplus q')_n$ and the fourth one from (A.12) for $k' = k$.

We also need to verify that the following equality, corresponding to (37) in [16],

$$\big(\omega^{(k-1)\odot q\odot q}\big)^{\frac{1}{2}}\big(\omega^{(k-1)\odot q'\odot q'}\big)^{\frac{1}{2}} = \omega^{(k-1)\odot q\odot q'}\big(\omega^{(k-1)\odot(q\oplus q')\odot(q\oplus q')}\big)^{\frac{1}{2}} \tag{A.20}$$

holds with the correct determination of square root's sign given by (A.10) (this does not happen with wrong determination of the sign given in [16]).

Let us consider the left hand side. It turns out to be

$$\begin{aligned}&\big(\omega^{(k-1)\odot q\odot q}\big)^{\frac{1}{2}}\big(\omega^{(k-1)\odot q'\odot q'}\big)^{\frac{1}{2}}\\ &\quad= (-1)^{\left(\sum_{n=0}^{m-1} q_n q'_n (k-1)\odot 2^n\odot 2^n\right)+\left(\sum_{n=0}^{m-1}\sum_{h=0}^{n-1}(q_n q_h + q'_n q'_h)(k-1)\odot 2^n\odot 2^h\right)}\\ &\qquad\qquad\times\prod_{n=0}^{m-1} i^{(q\oplus q')_n (k-1)\odot 2^n\odot 2^n}.\end{aligned} \tag{A.21}$$

For the right hand side, we have:

$$\begin{aligned}&\omega^{(k-1)\odot q\odot q'}\big(\omega^{(k-1)\odot(q\oplus q')\odot(q\oplus q')}\big)^{\frac{1}{2}}\\ &\quad= (-1)^{\left(\sum_{n=0}^{m-1}\sum_{h=0}^{m-1} q_n q'_h (k-1)\odot 2^n\odot 2^h\right)+\left(\sum_{n=0}^{m-1}\sum_{h=0}^{n-1}(q\oplus q')_n (q\oplus q')_h (k-1)\odot 2^n\odot 2^h\right)}\\ &\qquad\qquad\times\prod_{n=0}^{m-1} i^{(q\oplus q')_n (k-1)\odot 2^n\odot 2^n}.\end{aligned} \tag{A.22}$$

At this point, (A.20) derives from the following equality mod 2:

$$\begin{aligned}&\left(\sum_{n=0}^{m-1}\sum_{h=0}^{m-1} q_n q'_h 2^n\odot 2^h\right)+\left(\sum_{n=0}^{m-1}\sum_{h=0}^{n-1}(q\oplus q')_n (q\oplus q')_h 2^n\odot 2^h\right)\\ &\qquad= \left(\sum_{n=0}^{m-1} q_n q'_n 2^n\odot 2^n\right)+\left(\sum_{n=0}^{m-1}\sum_{h=0}^{n-1}(q_n q_h + q'_n q'_h)2^n\odot 2^h\right).\end{aligned} \tag{A.23}$$

Finally, we can prove the MUB condition for even prime power.

From (A.15), by using in the order (A.17), (A.18), (A.20) and (A.19), and then relabelling the sum indices, we have

$$\langle v_{t'}^{k'}\,|\,v_t^k\rangle\langle v_t^k\,|\,v_{t'}^{k'}\rangle = \frac{1}{d^2}\sum_{q,h=0}^{d-1}\phi(k,k',h)\,\phi(k,k,h)\,\omega^{(k-1)\odot q\odot q}\omega^{(k'-1)\odot q\odot q} \times \omega^{h\odot(t\oplus t')}\omega^{((k-1)\oplus(k'-1))\odot q\odot(q\oplus h)}\big(\omega^{((k-1)\oplus(k'-1))\odot h\odot h}\big)^{\frac{1}{2}}.$$

Now, by collecting the terms without q and then using (4), the previous expression can be rewritten as

$$\frac{1}{d^2}\sum_{h=0}^{d-1}\phi(k,k',h)\,\phi(k,k,h)\,\omega^{h\odot(t\oplus t')}\big(\omega^{((k-1)\oplus(k'-1))\odot h\odot h}\big)^{\frac{1}{2}}\sum_{q=0}^{d-1}\omega^{((k-1)\oplus(k'-1))\odot q\odot h} = \frac{1}{d}\sum_{h=0}^{d-1}\phi(k,k',h)\,\phi(k,k,h)\,\omega^{h\odot(t\oplus t')}\big(\omega^{((k-1)\oplus(k'-1))\odot h\odot h}\big)^{\frac{1}{2}}\delta_{((k-1)\oplus(k'-1))\odot h,0}.$$

At this point we can arrive, by separating the cases $k\neq k'$ and $k=k'$ and then using (A.16), (A.18) and (4), at the following:

$$\frac{1}{d}(1-\delta_{k,k'})\phi(k,k',0)\,\phi(k,k,0)+\frac{1}{d}\delta_{k,k'}\sum_{h=0}^{d-1}\phi(k,k,h)\,\phi(k,k,h)\,\omega^{h\odot(t\oplus t')} = \frac{1}{d}(1-\delta_{k,k'})+\frac{1}{d}\delta_{k,k'}\sum_{h=0}^{d-1}\omega^{h\odot(t\oplus t')} = \frac{1}{d}(1-\delta_{k,k'})+\delta_{k,k'}\delta_{t,t'}. \tag{A.24}$$

This gives (1), q.e.d.