Encryption via Entangled states belonging to Mutually Unbiased Bases

M. Revzen\(^{1}\) and F. C. Khanna\(^{2}\)

\(^{1}\)Department of Physics, Technion - Israel Institute of Technology, Haifa 32000, Israel
\(^{2}\)Department of Physics, University of Alberta, Edmonton, Alberta, Canada T6G 2J1

(Dated: September 11, 2008)

We consider particular entanglement of two particles whose state vectors are in bases that are mutually unbiased (MUB), i.e. "that exhibit maximum degree of incompatibility" (J. Schwinger, Nat. Ac. Sci. (USA), 1960). We use this link between entanglement and MUB to outline a protocol for secure key distribution among the parties that share these entangled states. The analysis leads to an association of entangled states and states in an MUB set: both carry the same labels.

PACS numbers: 03.65-w,03.67Dd,89.70.+c

I. INTRODUCTION

Two orthonormal vector bases, \(B_1, B_2\), are said to be mutually unbiased (MUB) iff

\[
\forall |u_1\rangle, |u_2\rangle \in B_1, B_2 \text{ resp. } |\langle u_1 | u_2 \rangle| = \text{constant,} \quad (1.1)
\]

i.e. the absolute value of the scalar product of vectors from different bases is independent of the vectorial labels within either basis. This implies that if the state vector is measured to be in one of the states e.g. \(|u_1\rangle\) of the base \(B_1\), it is equally likely to be in any of the states \(|u_2\rangle\) of the base \(B_2\). The first to emphasize that there are more than two such bases "that exhibit maximum degree of incompatibility" i.e. more than just the pair of conjugate bases such as \(|x\rangle\), (spatial coordinates) and \(|k\rangle\) (momentum representation basis) was Schwinger [1].

The infomation theoretic oriented term "mutually unbiased bases" (MUB) is due to Wootters [2]. Wootters and coworkers [3, 4] related the MUB's to lines in phase space: the vector/state that satisfy the equation,

\[
(p - b x)|1; b, c\rangle = c|1; b, c\rangle, \quad -\infty < c, b < \infty, \quad (1.2)
\]

This state may be viewed as lines in phase space in as much as the Wigner function of such state is given by (cf. Eq. (2), Appendix A),

\[
W_{1,b,c}(q,p) = \delta(p - bq - c), \quad (1.3)
\]

One may check directly that the vectors form an MUB set:

\[
|\langle 1; b, c | 1; b', c\prime \rangle| \text{ independent of } c, c' \text{ for } b \neq b'.
\]

The phase space geometry of MUB introduced by Wootters [2], may be seen as follows. Two lines (cf. Eq. (1.3)) parametrized with the same \(b\) but distinct \(c\) can never intersect. Two lines with distinct \(b\)'s intersect once.

Entanglement has been of great interest in theoretical physics since its first presentation by Einstein Podolsky and Rosen [5] where they consider an entangled two particles' state given by (the normalization is not specified)

\[
|2\rangle_{EPR} = \int dx_1 dx_2 \delta(x_1 - x_2) |x_1\rangle |x_2\rangle. \quad (1.5)
\]

The ensuing studies led to the immense development of quantum information theory [6-8] and, concomitantly, cryptography. On general grounds the sensitivity of quantum mechanical cryptographic protocols to eavesdroppers is anchored in a fundamental nature of quantum mechanics: a measurement e.g. by an eavesdropper) disturbs the system, i.e. leaves a trace (unless the state is an eigenstate of the operator representing the measurement). An essential ingredient is the use of non orthogonal states, e.g. vectors from distinct MUB. Indeed this was the basis of the pioneering protocol of encryption [9].

A protocol wherein cryptographic security is based on entanglement was put forward by Ekert, [10]. Here, too, noncompatible (i.e. belonging to distinct MUBs) bases are used. This idea involved qubits. It was extended with improved security to higher dimensional systems (qudits) [11-13]. The maximal number of MUB was shown [14] to be \(d+1\). Ivanovic, [15] demonstrated that for \(d=p\) (a prime) the set (i.e. \(d+1\) bases) allows what is probably most efficient means for the determining the density matrix of an arbitrary state. This may be viewed as a facet in the study of \(d\)-dimensional quantum mechanics. It attracted a large body of research work with several cogent reviews [16-19]. These studies now involve abstract algebra and projective geometry:
A central issue is the unsolved problem of the number of MUB for dimensionality, d, which is not a power of a prime. Of particular interest for the present work are the articles by Planat and coworkers [22, 23] who studied entangled states in conjunction with MUB sets similar to ours (see also [18, 23]).

In the present work we consider an interrelation between MUB and EPR like entanglement. Our considerations are for continuous variables (i.e. $d \to \infty$) allowing us, thereby, to bypass some of the intricate problems that do arise in the finite dimensional case. In particular we have Hermitian (i.e. measureable) operators that classify the MUB. We consider in the next section the one particle observable, $(\hat{p}-\hat{b}\hat{x})$, whose measurement projects on to Wootters’ [2, 4] ”line in phase space” state. The projection is elaborated in appendix A. A two-particle state is built via an EPR [3] like entanglement. (The corresponding finite dimensional case is considered in appendix B.) In the succeeding section we give a secure protocol for (quantum) key distribution which, we believe, is conceptually simpler than available in the literature (see also [18, 25]).

We now give a protocol for a secure encryption. We consider an encrypted one bit message from A to B given that they share two entangled states ($\alpha = 1, 2$) cf. Eq. (2.3) both having the same values for the parameters $b$ and $c$. In this case, of common values of $b$ and $c$, we assume that neither party requires the actual values of the parameters. (For the cases where the entangled states differ in their eigenvalues, $c$, Alice has to use the difference of these values to affect the encryption.) The measurements relevant to this are the two particle observables $\hat{R}_1, \hat{R}_2$, Eq. (17) discussed in Appendix C. The protocol is as follows: Alice measures for both states the quantity $(\hat{p}_1 - b_1\hat{x}_1)$. She may choose any $b_1$ but use it for both states. She records the two values she gets: $c_1$ and $c_1'$. She now sends, by classical communication channel, a value $\lambda$ to Bob’s port. Upon receiving Alice’s message Bob subjects his second particle to the unitary transformation $e^{i\lambda\hat{X}_2}$. This shifts his state from $c_2' = c - c_1'$ to $c_2' + \lambda$ (cf. Appendix A). Now he measures the correlation among his two states,

$$\langle 1; b_2, c_2 | 1; b_1, (c_2' + \lambda) \rangle = \delta(c_2 - c_2' - \lambda). \quad (3.1)$$

Thus if Alice chooses to communicate $+1$ she sends $\lambda = c_1' - c_1$, if she chooses to communicate zero she sends $\lambda \neq c_1' - c_1$. This procedure is secure in as much as Alice and Bob can at any time check, via classical communication channels, whether the observed value is indeed the intended one: An eavesdropper must use the same MUB measurement (i.e. the same $b_1$ chosen by A) and observe the same value $c_1$ in order not to leave a trace. In the case considered here both quantities range over unlimited numbers leaving him/her a small chance of avoiding detection.

III. THE ENCRYPTION PROTOCOL

We now give a protocol for a secure encryption. We consider an encrypted one bit message from A to B given that they share two entangled states ($\alpha = 1, 2$) cf. Eq. (2.3) both having the same values for the parameters $b$ and $c$. In this case, of common values of $b$ and $c$, we assume that neither party requires the actual values of the parameters. (For the cases where the entangled states differ in their eigenvalues, $c$, Alice has to use the difference of these values to affect the encryption.) The measurements relevant to this are the two particle observables $\hat{R}_1, \hat{R}_2$, Eq. (17) discussed in Appendix C. The protocol is as follows: Alice measures for both states the quantity $(\hat{p}_1 - b_1\hat{x}_1)$. She may choose any $b_1$ but use it for both states. She records the two values she gets: $c_1$ and $c_1'$. She now sends, by classical communication channel, a value $\lambda$ to Bob’s port. Upon receiving Alice’s message Bob subjects his second particle to the unitary transformation $e^{i\lambda\hat{X}_2}$. This shifts his state from $c_2' = c - c_1'$ to $c_2' + \lambda$ (cf. Appendix A). Now he measures the correlation among his two states,

$$\langle 1; b_2, c_2 | 1; b_1, (c_2' + \lambda) \rangle = \delta(c_2 - c_2' - \lambda). \quad (3.1)$$

Thus if Alice chooses to communicate $+1$ she sends $\lambda = c_1' - c_1$, if she chooses to communicate zero she sends $\lambda \neq c_1' - c_1$. This procedure is secure in as much as Alice and Bob can at any time check, via classical communication channels, whether the observed value is indeed the intended one: An eavesdropper must use the same MUB measurement (i.e. the same $b_1$ chosen by A) and observe the same value $c_1$ in order not to leave a trace. In the case considered here both quantities range over unlimited numbers leaving him/her a small chance of avoiding detection.

IV. CONCLUSIONS AND REMARKS

Mutual unbiased bases may be characterized by observables that are diagonal in each of them (hence cannot be so in any two distinct bases). Einstein, Podolsky
and Rosen (EPR) like entanglement of eigenfunctions of such observables has the property that measuring one particle of the entangled pair to be in a particular state (of the set of MUB bases’ states) projects its (entangled) mate to another member state, generally in another basis. This attribute allowed us to outline a secure (albeit technically complicated) protocol for encryption. The analysis led to the consideration of what might be termed mutually unbiased entangled pairs bases. The basis vectors in two particles systems are (maximally) entangled pairs whose labels are those of the MUB states used in the entanglement.

Appendix A: The Projection Procedure

We consider the Hermitian operator \((\hat{p} - b \hat{x})\). We denote its eigenfunctions by \(|1; b, c\rangle\):

\[
(\hat{p} - b \hat{x})|1; b, c\rangle = c|1; b, c\rangle.
\]

We refer to the operator as the MUB operator (MUB-O). Its eigenvalues for fixed \(b\) form a complete orthonormal basis where the various vectors in a given basis are labeled by \(c\). The definition of the MUB-O implies that [4],

\[
\langle x|1; b, c\rangle = \frac{1}{\sqrt{2\pi}} e^{i 2\pi x^2/cx}.
\]

The normalization is obtained in [4]. The MUB related entanglement that we consider is given in Eq. (2.2). Measuring at the A port an arbitrary MUB-O, e.g. with a basis label \(b_1\) and observing, say, \(c_1\), the projected state at the port B (before normalization) is:

\[
\langle 1; b_1, c_1|2; b, c\rangle = \frac{1}{2\pi} \int dx e^{i 2\pi x^2/cx}|x\rangle = \frac{1}{\sqrt{2\pi}}|1; b_2, c_2\rangle,
\]

with \(b_2 = b - b_1\); \(c_2 = c - c_1\). Thus the second particle is projected into a sharply defined, MUB labeled, state.

Appendix B: Entanglement of MUB states at Finite dimensionality

Our method may be applied in the finite dimensional space to the case where the states’ label are finite field variables. This case for dimensionality \(d\), with \(d = p^n\), \(p\) an odd prime [18, 22, 23, 25]. The MUB are given by, using our notation, \((\omega_p = e^{2\pi i/n})\):

\[
|1; b, c\rangle = \frac{1}{\sqrt{d}} \sum_{n \in \mathbb{F}_d} \omega_p^{n^2 + cn}|n\rangle.
\]

Here \(b, c, n \in \mathbb{F}_d\), \(\mathbb{F}_d\) is Galois field of \(d\) dimension. \(|n\rangle\) denotes a vector in the computational basis (labelled with an element of the field); and \(tr[\alpha] = \alpha + \alpha p + \alpha p^2 + \ldots + \alpha p^{n-1}\). The trace, \(tr\), is a mapping with \(\alpha \in \mathbb{F}_d\); \(tr\alpha \in \mathbb{F}_p\).

Now a basic property of trace is: \(tr[\alpha + \beta] = tr[\alpha] + tr[\beta]\).

Appendix C: Structure of the Entangled States

The determination, at the A (Alice’s) port, of the two particle eigenvalue of the entangled state associated with the single particle MUB labeled by \(b\) - i.e. the determination of \(c\) of Eq. (2.2) - requires operators whose measurement gives the eigenvalue while leaving the desired entangled state intact. The operators that characterize the (single particle) MUB are \(\hat{p} - b \hat{x}\), Eq. (2.2). Here \(b\) signifies the basis. To form an entangled state we require two \textit{non-commuting} operators for each of the two particles. These are \(\hat{p}_1 - b_1 \hat{x}_1\), \(\hat{p}_1 - b_2 \hat{x}_1\); \(b_1 + b_2 = b\), \(b_1 \neq b_2\), for the first particle and \(\hat{p}_2 - b_1 \hat{x}_2\), \(\hat{p}_2 - b_2 \hat{x}_2\); \(b_1 + b_2 = b\), \(b_1 \neq b_2\), for the second. These operators allow the definition of two \textit{commuting} two particles’ operators,

\[
\hat{R}_1 = \hat{p}_1 - b_1 \hat{x}_1 + \hat{p}_2 - b_2 \hat{x}_2; \quad \hat{R}_2 = \hat{p}_1 - b'_1 \hat{x}_1 + \hat{p}_2 - b'_2 \hat{x}_2.
\]

The common eigenfunctions of these are, \textit{necessarily} [26], entangled. The eigenfunctions of \(\hat{R}_1\), \(\hat{R}_2\) are given by Eq. (2.2), the eigenvalue is \(c\). Thus the required operators are \(\hat{R}_1, \hat{R}_2\). To gain some insight to these states we evaluate the Wigner function for the entangled state parametrized by \(b\) and \(c\),

\[
W_{(2,b,c)}(q_1, q_2, p_1, p_2) = \delta(q_2 - q_1)\delta(p_1 + p_2 - bq_1 + c).
\]

Expressing thereby the relation of the entangled state to the MUB state bearing the same parameters. One of the authors (FCK) thanks NSERC for financial support. MR thanks the theoretical physics Institute for support during the stay at the University of Alberta.
We are unaware of any existing proof for this, rather obvious, observation. We may state the corresponding result for the finite dimension as follows. Let two operators on system $\alpha$ be $A, B$, with $AB = cBA$, $c \neq 1$. Let two operators on $\beta$ be $U, V$, with $UV = dVU$. Let the product of the $c$ numbers $cd = 1$. We have now that $AU$ commute with $BV$. The statement is that the common eigenfunction of $AU$ and $BV$ is necessarily entangled.