(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 November 2008 (20.11.2008)

PCT

(10) International Publication Number
WO 2008/140290 A2

(51) International Patent Classification:
H04L 9/08 (2006.01)

(21) International Application Number:
PCT/MY2008/000038

(22) International Filing Date: 9 May 2008 (09.05.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 20070734 11 May 2007 (11.05.2007) MY

(71) Applicants *(for all designated States except US)*: **MIMOS, Berhad** [MY/MY]; Technology Park of Malaysia, Bukit Jalil, 57000 Kuala Lumpur (MY). **INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA** [MY/MY]; Jalan Gombak, 53100 Kuala Lumpur (MY).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **WAHIDIN, Mohamed, Ridza** [MY/MY]; 12, Lorong Limau Dua, Bangsar Park, 59000 Kuala Lumpur (MY). **SHAARI, Jesni, Bin, Shamsul** [MY/MY]; No 19, Jalan T/K 2/4, Taman Kinrara, Seksyen 2, Puchong, 47100 Selangor (MY). **LUCAMARNI, Marco** [IT/IT]; Department of Physics, University of Camerino, I-62032 Camerino (IT).

(74) Agent: **MOHAN, K.**; Adastra Intellectual Property SDN BHD, Suite 2B, Level 7, Menara Dato Onn, 45 Jalan Tun Ismail, Putra World Trade Centre, 50480 Kuala Lumpur (MY).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Continued on next page]

(54) Title: QUDITS IN TWO WAY DETERMINISTIC QUANTUM KEY DISTRIBUTION

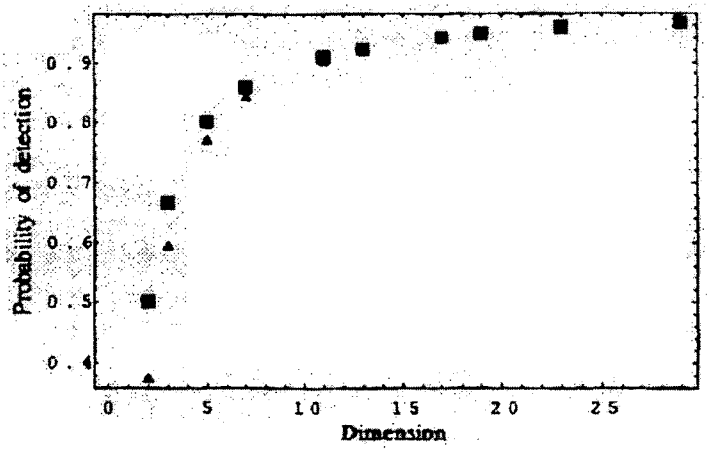

FIG. 1

(57) Abstract: The present invention relates to a qudits in two way deterministic quantum key distribution wherein it involved a two way transmission where qubits are sent to and from between communicating parties while information is encoded by unitary transformers on the qubits. A protocol sees U1 sending to U2 a state that U1 prepared and wherein U2 would then encode the said received protocol with unitary transformation. U2 would then thereafter send the encoded state back to U1 who would then measure or decode the sent state deterministically. In order to ensure the security of the protocol, a control mode used and is randomly done with a certain probability wherein instead of encoding. U2 would do a projective measurements on the qudit received whilst U1 measures the qudit sent by U2.

WO 2008/140290 A2

ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

QUDITS IN TWO WAY DETERMINISTIC QUANTUM KEY DISTRIBUTION

FIELD OF THE INVENTION

The present invention relates to a qudits in two way deterministic quantum key distribution.

BACKGROUND OF THE INVENTION

In the prior art the use of qubit was basically the leader in quantum key distribution (QKD) in the BB84 protocol. A higher dimensional system was used wherein the protocol was extendable to the use of qutrits, exhibiting a higher level of security. The two way deterministic protocols emerged with development in various protocols. This involved a two way transmission where qubits are sent to and from between communicating parties while information is encoded by unitary transformers on the qubits.

Generalization to exhaustive use of all the MUB in both the qubit and qutrit case involves nontrivial extensions due to he nonexistence of the unitary universal NOT gate as well as a non go theorem.

In the present invention, the inventors have introduced the use of d (d being a prime number) dimensional quantum system (qudit) in a two way deterministic scheme. Further to this, a generalized protocol is considered using an encoding recipe for unitary efficiency. The security was compared and efficiencies of the protocols both in the context of theoretical as well as practical efficiencies were recorded.

SUMMARY OF THE INVENTION

The present invention relates to a qudits in two way deterministic quantum key distribution wherein it involved a two way transmission where qubits are sent to and from between communicating parties while information is encoded by unitary

transformers on the qubits. A protocol sees U1 sending to U2 a state that U1 prepared and wherein U2 would then encode the said received protocol with unitary transformation. U2 would then thereafter send the encoded state back to U1 who would then measure or decode the sent state deterministically and wherein in order to ensure the security of the protocol, a control mode used and is randomly done with a certain probability wherein instead of encoding, U2 would do a projective measurements on the qudit received whilst U1 measures the qudit sent by U2. In a noisy channel, the measure of security is essentially translated into the robustness of the protocol.

A secure key can be distilled with the use of standard error correction and privacy amplification procedures only when the information shared between U2 and U1 is greater than the lesser of the information shared between U2 and U3. U3 substitute the noisy channel between U1 and U2 and attack only certain fractions of the qudits to glean some information whilst inducing a lesser amount of error in the control mode. In a full fraction attack by U3, U3 would destroy the information in the qudit when U3 measures it in a different basis that that which U1 has prepared.

BRIEF DESCRIPTION OF THE FIGURE

Figure 1 shows a graph plotted to show the probability of detection for the generalized protocol (square points) and non-generalized protocol (triangular points) against the number of dimensions.

DETAILED DESCRPTION OF THE PRESENT INVENTION

In the present invention two users would be used as to better describe the protocol. Wherein the said two users would be referred as User 1 or U1 and User 2 or U2. Subsequent users would be referred as U3, U4 and etc.

In the present invention it would be notice that a protocol sees U1 sending to U2 a state that U1 prepared (also referred as forward path). U2 would then encode the said received protocol with unitary transformation. U2 would then thereafter send the

encoded state back to U1 (also referred as backward path) who would then measure or decode the sent state deterministically.

According to the present invention, in order to ensure the security of the protocol, a control mode is necessary. This is randomly done with a certain probability where instead of encoding U2 would do a projective measurements on the qudit in the forward path whilst U1 measures the qudit in the backward path. In the instances wherein U2 choice of basis coincides with U1's , the measurements should correlate. If this is not the case, an eavesdropper would be detected.

In the case the present invention only use *d* basis, a U3 may correctly guess only 1/*d* times and avoids detection. However, in the case that U3 makes a mistake, she gets to evade detection in both the forward and backward path with probability $1/d^2$. on average U3 would be detected with probability $Pr(Eve) =[(d-1)/d](d^2-1)/(d^2)$.

However, in a realistic setup with a noisy channel, the measure of security is essentially translated into the robustness of the protocol; i.e., how much of error could be tolerated before communication becomes insecure. A secure key can be distilled with the use of standard error correction and privacy amplification procedures only when the information shared between U2 and U1, I_{AB}, is greater than the lesser of the information shared between U2 and U3, I_{AE} , or U1 and U3, I_{BE}, ($I_{AB} > \min(I_{AE}, I_{BE})$).

In such instance, it could be considered that U3 substitute the noisy channel between them with a perfect one and attack only certain fractions of the qudits to glean some information whilst inducing a lesser amount of error in the control mode. A full fraction attack would induce an error amounting to $e = ((d-1)/d)^2$. In other words U3 needs to attack and achieve $I_{AB} \leq \min (I_{AE}, I_{BE})$. For the purpose of describing the present invention, it is considered that the information shared between the parties, wherein for U2 and U3, the information shared is given as:

$$I_{AB} = 1 - (2d-1)/(d^2) \log_d (2d-1)/d^2) - ((d-1)/(d))^2 \log_d (d-1)/d^2 \qquad (1$$

Wherein, $I_{AE} = 1$ for a full fraction attack by U3, the case is quite different for I_{BE} as U3 would destroy the information in the qudit when U3 measures it in a different basis that that which U1 has prepared. U3's chances of having equal results with U1 about U2's encoding is only $(2d-1)/d^2$ and U3's uncertainty of U1's result becomes as shown below:-

$$H(B) = (2d-1)/(d^2) \log_d (2d-1)/(d^2) + (d-1)^2/(d^2) \log_d (d-1)/(d^2) \qquad (2)$$

It is straightforward to see that with $I_{BE} = 1 - H(B)$, only when U3 attacks all the qudits would be $I_{BE} = I_{AB}$. In considering the case when we generalize to d+ 1 basis we refer to for a reliable recipe for blind encoding to achieve a protocol of unitary efficiency. U1 would send to U3 *d* qudits of differing bases and U2 would encode with any of the d^d possible transformations.

$$(V\frac{d-a}{1}U\frac{a}{d+1})(U\frac{d-b}{2}U\frac{k}{d+1}). \quad .(U\frac{d-k}{d}U\frac{k}{d+1})|\varphi_{t_1}^1\varphi_{t_2}^2 \quad .\varphi_{td}^d \qquad (3)$$

Wherein a, b, ..., k are different values to encode onto the relevant qudits, Uj is the unitary transformation to shift a state in any basis except *j*th and φ^i belongs to *d* different MUB. In an IR attack, U3 has the chances of d / (d+1) making a mistake and the probability to avoid detection in both the forward and backward path is $1/d^2$. The probability on the whole to detect U3 would be $Pr(Eve_{generalized}) = (d-1)/d$.

In term of efficiency of the protocol, it could be considered that only the transmission mode as opposed to the control mode. In the theoretical framework where a channel is considered to be noiseless and lossless, this is not unjustifiable as one may minimize greatly the probability of the control mod, leading to a negligible number of qudits to be discarded. With respect to the practical efficiency, we consider the transmittance of the channel to be T. With the distance between U2 and U1 being L, every qudit would have to travel a distance of 2L. For the generalized protocol, considering every round of communication, the practical efficiency amounts to the

overall probability that all the qudits arrive at the end of the round trip: $\varepsilon' = T^{2d}$. As in a realistic setup, wherein

$$T < 1, \lim_{d \to \infty} \varepsilon^i = 0$$

The practical efficiency is literally zero. Given the fact that probability of detecting U3 for both the protocol asymptotically approaches 1 as *d* increases.

$$\lim_{d \to \infty} \Pr(Eve) = \lim_{d \to \infty} \Pr(Eve_{generalized}) = 1$$

It is therefore concluded that the generalized two way protocols become less efficient with increasing dimensions in realistic cases where the transmittance is less than perfect.

CLAIMS

1. A qudits in two way deterministic quantum key distribution wherein it involved a two way transmission where qubits are sent to and from between communicating parties while information is encoded by unitary transformers on the qubits characterized in that wherein a protocol sees U1 sending to U2 a state that U1 prepared and wherein U2 would then encode the said received protocol with unitary transformation and wherein U2 would then thereafter send the encoded state back to U1 who would then measure or decode the sent state deterministically and wherein in order to ensure the security of the protocol, a control mode used and is randomly done with a certain probability wherein instead of encoding, U2 would do a projective measurements on the qudit received whilst U1 measures the qudit sent by U2.

2. A qudits in two way deterministic quantum key distribution as claimed in Claim 1 wherein with a noisy channel, the measure of security is essentially translated into the robustness of the protocol.

3. A qudits in two way deterministic quantum key distribution as claimed in Claim 1 wherein a secure key can be distilled with the use of standard error correction and privacy amplification procedures only when the information shared between U2 and U1 is greater than the lesser of the information shared between U2 and U3.

4. A qudits in two way deterministic quantum key distribution as claimed in Claim 3 wherein U3 substitute the noisy channel between U1 and U2 and attack only certain fractions of the qudits to glean some information whilst inducing a lesser amount of error in the control mode.

5. A qudits in two way deterministic quantum key distribution as claimed in Claim 1 wherein in a full fraction attack by U3, U3 would destroy the information in

the qudit when U3 measures it in a different basis that that which U1 has prepared.

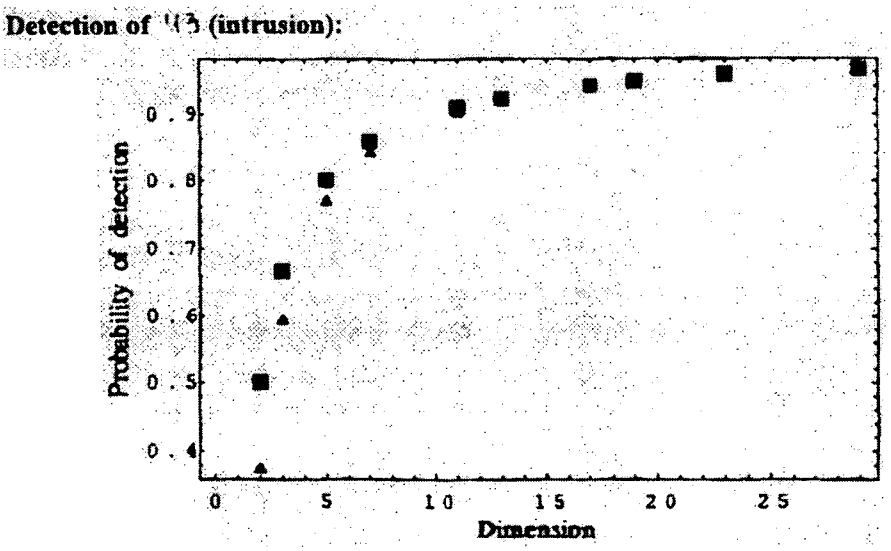
Detection of
(intrusion):
Probability of detection
0.9
0.8
0.7
0.6
0.5
0.4
0
5
10
15
20
25
Dimension

FIG. 1