# A public-key based secure quantum-communication protocol using entangled qubits

**S Murugesh**

Department of Physics, Indian Institute of Space Science and Technology - Thiruvananthapuram - 695547, India

E-mail: murugesh@iist.ac.in

**Abstract.** We propose a quantum algorithm that crucially involves the receiver's public-key to establish secure communication of an intended message string, using shared entangled-qubits. The public-key in question is a random bit string that proclaims the sequence of measurement basis used by the receiver. As opposed to known quantum key distribution protocols, wherein a random key string is generated at the end of the communication cycle, here the sender's intended bit string itself is communicated across securely. The quantum outlay for the proposed protocol is limited to the sender and receiver sharing pairs of entangled qubits, prepared in *a priori* known states, besides unitary manipulations and measurements that the sender and receiver individually perform on their respective qubits, within their confines.

## 1. Introduction

With the imminent challenge to present day classical encryption posed by quantum computing algorithms[1], several quantum key distribution (QKD) protocols proposed over the last few decades[2, 3, 4, 5, 6, 7, 8], and their practical implementation, has found a strong impetus[9, 10]. Broadly, QKD algorithms fall into two varieties - 'prepare-and-measure' and 'entanglement-based'. A reliable quantum channel to transport single photons in polarization states, entangled or otherwise, forms the primary technological challenge in implementation. Where channel noise and intrusions are within tolerable limits, error correction codes and entanglement distillation techniques help in restoring fidelity of the transmitted qubits[11, 12, 8, 13]. Besides transport of qubits and error correction, their manipulation and measurement within the respective laboratories of the sender (Alice) and receiver (Bob) completes the quantum cost of implementation. Along with the aforementioned quantum outlay, availability of an uncorrupted (although insecure) public channel forms another minimal, yet critical, requirement. As it stands, land based optical fiber networks that channel photons between relays spread over a distance of two thousand kilometers, and further by dedicated satellites connecting similar distances has been reported, demonstrating successful implementation of the BB84 protocol[2, 10, 14]. On the other hand, entangled

photons have been reliably exchanged *via* optical fibers for a distance of nearly two hundred and fifty kilometers[15, 16].

The QKD protocols being pursued share at least one common feature: in truth they are key *generation* protocols, as no predetermined key is exchanged or distributed. Instead, a random bit string is generated at the end of the protocol, ideally known only to the intended receiver and sender, from which a *shared key* is then realized. Shared key protocols carry certain inherent limitations, besides their range of applicability. For instance *identity authentication* is a fundamental challenge in shared key cryptosystems, usually circumvented by resorting to classical cryptography to establish initial communication[17, 18, 19]. Alternately, a wide variety of situations common to modern day engagements - multi party exchanges, transactions between untrustworthy participants, digital signature and non-repudiability, to name a few - are conveniently serviced by public-key algorithms[20, 21]. Indeed, it can be argued that the rapid growth and acceptance of the internet over the last thirty years can be singularly attributed to public-key protocols, and the spectrum of engagements wherein it's use is both handy and indispensable.

By adding a layer of non-orthogonal states and measurement basis to the quantum teleportation protocol by Bennet *et al.*[22], we propose an algorithm wherein Bob's public-key is vitally used by Alice in securely communicating her intended sequence of message bits. Here, Bob's public-key is a random bit string (say, of length $N$) which shall proclaim the sequence of his choice of measurement basis for successive qubits. As opposed to QKD algorithms, wherein the key is generated only at the end of execution of the protocol, the proposed public-key algorithm allows for secure communication of a predetermined string. When used along with the receiver's public-key, this effectively resolves the issue of identity authentication. The algorithm presented here has some salient differentiators from the regular public-key algorithms, and QKD protocols: i) While Bob's public-key is critical in establishing secure communication, the proposal here does not involve a private-key. ii) The message bits themselves can be transmitted securely, as opposed to *key generation* in QKD algorithms. The protocol involves entangled qubits and measurements in non-orthogonal basis. The message itself is never encrypted *per se*, nor are any encrypted qubits transferred over a quantum channel consequently, as is usually the case with entanglement based protocols[5]. Bob shares entangled qubits with Alice, who remotely manipulates the qubits in her possession. Before making measurements on his qubits, in his predetermined and publicized sequence of basis choices, Bob performs specific unitary operations on his qubits as advised by Alice over a public channel. As will be seen, the security of the communication is ensured by the fact that the unitary operations advised by Alice do not in any way reveal Bob's measurement outcomes.

## 2. Using entangled qubits, qubits in non-orthogonal states, and the receiver's public-key, to securely communicate a chosen bit string

### *2.1. Prerequisites*

In order to accomplish the algorithm, Alice and Bob start with a set of pairs of entangled qubits in known initial states, either of them having one qubit from each pair. Quantum channels are invariably noisy, and attempts at infiltration are precautionary assumptions taken by default. After satisfactorily performing the necessary fidelity checks and purification, we shall assume that they are still left with $N$ such reliable entangled pairs. Without loss of generality, let each pair be prepared in the Bell state $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. If the fidelity checks are satisfactory, they will have no further need for a quantum channel beyond this point, as is the case with entanglement-based protocols[13]. In addition to the entangled qubits, Alice shall also have with her another set of $N$ qubits in states $|\psi_i\rangle$, $i = 1, 2, ..N$, each prepared randomly in any one of the four states - $|0\rangle$, $|1\rangle$, and $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Thus, Alice has a total of $N$ pairs of qubits to work with - the first one of each pair in an un-entangled pure state $|\psi_i\rangle$ known to her (and her only), and the second qubit entangled with its counterpart in Bob's laboratory in the state $|\beta_{00}\rangle$.

Let $\{a_1a_2a_3....a_N\}$ $(a_i = 0, 1)$, be the message string Alice intends to send across to Bob, and $\{b_1b_2b_3....b_N\}$ $(b_i = 0, 1)$ be Bob's public-key string. $b_i$ essentially declares the measurement basis Bob would choose for his $i$'th qubit - 0(1) implying $B_0 = Z(B_1 = X)$ basis. Adhering to convention, we will choose $|0\rangle$ ($|1\rangle$) to represent the bit 0 (1) in the $Z$ basis, and $|+\rangle(|-\rangle)$ to represent bit 0 (1) in the $X$ basis all along. I.e., a measurement on $|0\rangle$ and $|1\rangle$ in the $Z$ basis leads to outcomes 0 and 1, respectively.

### *2.2. Implementation sequence*

Secure communication can now be established by the following steps:

I. From her first pair of qubits, Alice prepares her first qubit in state $|\psi_1\rangle$, a random choice from one of the four states - $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Her second qubit is in an entangled state $|\beta_{00}\rangle$ with Bob's qubit. The combined state of the three qubit system is then

$$|\Psi\rangle = |\psi_1\rangle|\beta_{00}\rangle. \tag{1}$$

In steps II and III, Alice teleports $|\psi_1\rangle$ across to Bob using the regular teleportation algorithm[22, 23], stopping short of conveying the measurement outcomes on her two qubits:

II. Alice's two qubits are subject to a CNOT operation, with the first (un-entagled) qubit in state $|\psi_1\rangle$ as the control bit.
III. Her first qubit is then transformed by a Hadamard operation $(H \otimes I)$.

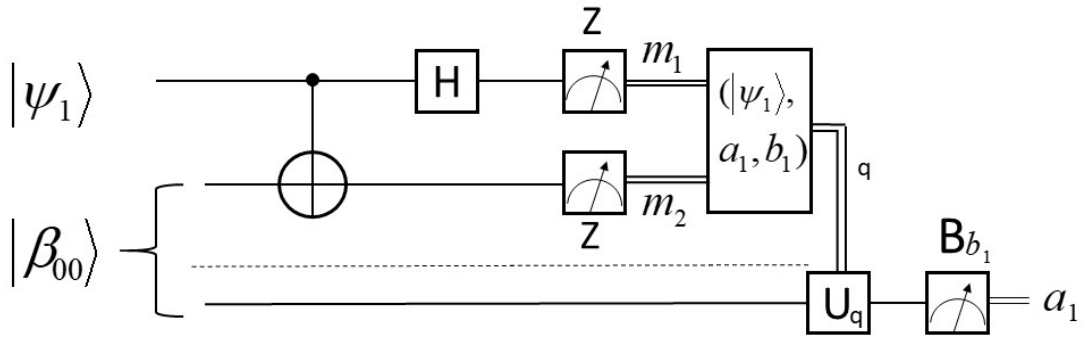


**Figure 1.** Circuit to implement the public-key secure communication protocol. Alice prepares her first qubit in the state $|\psi_1\rangle$, which could be any one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Her second qubit and Bob's qubit are entangled in a Bell state $|\beta_{00}\rangle$. $a_1$ is Alice's intended message bit, and $b_1$ denotes Bob's declared measurement basis. Knowing $\{m_1, m_2, a_1, b_1, |\psi_1\rangle\}$ Alice determines from tables 1, 3, and 4, the unitary transformation $U_q$ Bob should perform to get the correct outcome $a_1$ upon measurement in the $B_{b_1}$ basis ($B_0 = Z$, and $B_1 = X$).

**Table 1.** Possible states of Bob's qubit, $|\phi\rangle_B$, post Alice's measurement of her two qubits. $|\psi_1\rangle$ is the initial state of Alice's first qubit, and $(m_1, m_2)$ are her measurement results.

| | $(m_1, m_2)$ | | | |
|---|---|---|---|---|
| $\|\psi_1\rangle$ | (0,0) | (0,1) | (1,0) | (1,1) |
| $\|0\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ |
| $\|1\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ |
| $\|+\rangle$ | $\|+\rangle$ | $\|+\rangle$ | $\|-\rangle$ | $\|-\rangle$ |
| $\|-\rangle$ | $\|-\rangle$ | $\|-\rangle$ | $\|+\rangle$ | $\|+\rangle$ |

Writing $|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$ in general, the state of the three qubits at this stage is

$$|\Psi\rangle = \frac{1}{2}\Big[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) \\ +|10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\Big] \quad (2)$$

IV. She then performs measurements in, say, the $Z$ basis on her two qubits, yielding the results $(m_1, m_2)$, where $m_i = 0, 1$.

The circuit shown in figure 1. illustrates the flow of the algorithm. From (2), post Alice's measurement on her two qubits, given the specific choice of $|\psi_1\rangle$, Bob's qubit collapses into one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ (up to an insignificant phase). Table 1 lists the state of Bob's qubit after these two measurements with outcomes $(m_1, m_2)$, for each possible initial state of Alice's qubit, $|\psi_1\rangle$.

V. Knowing $|\psi_1\rangle$ and $(m_1, m_2)$, Alice determines the state of Bob's qubit, $|\phi\rangle_B$, from table 1.

**Table 2.** State of Bob's qubit due to the four unitary transformations $U_q$, $q = 1, ..4$. A choice of $U_q$ acting on any of the four possible $|\phi\rangle_B$ states transforms it to the corresponding state in the table (up to an insignificant overall phase).

| | $U_q$ | | | |
|---|---|---|---|---|
| $\|\phi\rangle_B$ | $I$ | $\sigma_y$ | $R_+$ | $R_-$ |
| $\|0\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|-\rangle$ | $\|+\rangle$ |
| $\|1\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|+\rangle$ | $\|-\rangle$ |
| $\|+\rangle$ | $\|+\rangle$ | $\|-\rangle$ | $\|0\rangle$ | $\|1\rangle$ |
| $\|-\rangle$ | $\|-\rangle$ | $\|+\rangle$ | $\|1\rangle$ | $\|0\rangle$ |

However, without Alice's measurement results, Bob (or any intrusive third-party) has no knowledge of the state of his qubit. As can be seen from table 1, Bob's qubit is equally likely to be in any one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ for each of the four possible measurement outcomes. Indeed, the reduced density matrix for Bob's qubit post Alice's measurements is $\rho_B = \frac{1}{2}I$, implying that Bob can gain no information about $|\psi_1\rangle$ as yet from his qubit.

In the next step Alice has to convey her intended message bit $a_1$ securely over to Bob. From Bob's public-key bit $b_1$, Alice is aware of the basis in which Bob is about to perform his measurement. With the knowledge of the current state of Bob's qubit, and $b_1$, Alice's task then reduces to instructing Bob, over a public channel, to perform an appropriate unitary transformation on his qubit before proceeding with the measurement in the pre-announced basis $B_{b_1}$. Effectively, this is a set of automorphisms on the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and can be accomplished by the four unitary operations

$$U_1 = I, \tag{3a}$$

$$U_2 = \sigma_y, \tag{3b}$$

$$U_3 = R_+ \equiv \frac{1}{\sqrt{2}}(I + i\sigma_y), \tag{3c}$$

$$U_4 = R_- \equiv \frac{1}{\sqrt{2}}(I - i\sigma_y), \tag{3d}$$

up to an overall phase. Table 2 lists the possible resultant states of Bob's qubit $|\phi\rangle_B$ after these four operations.

In order to get the correct outcome $a_1$ in the $B_{b_1}$ basis, knowing the state of his qubit $|\phi\rangle_B$, Alice should advise Bob to perform an appropriate unitary transformation, $U_q$, prior to his measurement. Tables 3 and 4 chart these unitary operation for $Z$ and $X$ basis, respectively.

VI. From tables 3 and 4, Alice identifies the unitary operation, $U_q$, Bob should be advised to perform before going ahead with his measurement in the basis $B_{b_1}$ as planned. For example, let Alice's message bit $a_1 = 1$, Bob's basis bit $b_1 = 0$ (i.e., measurement basis is $B_0 = Z$), and $|\phi\rangle_B = |+\rangle$. From table 3 then, Alice determines $U_q$ to be $R_-$ in order for Bob to obtain the measurement result '1′.

**Table 3.** Identifying the correct unitary transformation Alice should advise Bob to perform, given the current state of Bob's qubit $|\phi\rangle_B$ and the message bit $a_1$, if Bob were to use $Z$ measurement basis (i.e., $b_1 = 0$). For $a_1 = 0(1)$ the intended final state is $|0\rangle\,(|1\rangle)$

| | $\|\phi\rangle_B$ | | | |
|---|---|---|---|---|
| $a_1$ | $\|0\rangle$ | $\|1\rangle$ | $\|+\rangle$ | $\|-\rangle$ |
| 0 | $I$ | $Y$ | $R_+$ | $R_-$ |
| 1 | $Y$ | $I$ | $R_-$ | $R_+$ |

**Table 4.** Identifying the appropriate unitary transformation, if Bob were to use $X$ measurement basis ($b_1 = 1$). For $a_1 = 0\,(1)$, the intended final state is $|+\rangle(|-\rangle)$

| | $\|\phi\rangle_B$ | | | |
|---|---|---|---|---|
| $a_1$ | $\|0\rangle$ | $\|1\rangle$ | $\|+\rangle$ | $\|-\rangle$ |
| 0 | $R_-$ | $R_+$ | $I$ | $Y$ |
| 1 | $R_+$ | $R_-$ | $Y$ | $I$ |

VII. Over a public channel, Alice instructs Bob to perform the unitary operation $U_q$, identified in step VI before going ahead with his measurement.
VIII. Finally, after performing the unitary transformation $U_q$, as instructed, Bob measures his qubit in the pre-disclosed basis $B_{b_1}$.

Steps I-VIII are repeated till all the message bits $\{a_i\}$ are communicated across.

## 3. Discussion

Besides Bob's key declaring the final measurement basis bit $b_1$, the only other information any potential evesdropper has possible access to all along is the unitary operation that Bob is instructed to perform - $U_q$, over a public channel. In particular, after sharing the entangled qubits, all subsequent unitary operations and measurements happen within the confines of Alice's and Bob's respective laboratories. From tables 3 and 4, it is however evident that for any choice of $b_1$ and the final unitary operation $U_q$, the outcomes 0 and 1 (or, the final states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$) are equally likely, thus giving away no information regarding $a_1$. This is critical in ensuring that the communication stays secure.

It must be noted that no true encryption of the message bit takes effect at any stage *per se*, typical of an entanglement based protocol. The shared entangled qubits are utilized in teleporting only a random state $|\psi_1\rangle$, known exclusively to Alice. The message bit $a_1$ is invoked only at step VI to determine the final unitary operation $U_q$. In fact, prior to performing this final transformation, Bob's qubit carries no information, whatsoever, regarding the message bit $a_1$.

As pointed out earlier, the proposed public-key protocol does not involve a private-key to decrypt the received message. This, however, does not pose a limitation in the sender and receiver establishing their mutual identities. For instance, upon completion of the exchange, Bob could send back a subset of the received message string following the same protocol, using Alice's public-key, thereby mutually establishing identity. Additionally, engaging a trusted third party certification infrastructure would accomplish the objectives of digital signature and non-repudiability. We suspect lack of a private-key will in any way limit the range of engagements that can normally be accomplished by a regular Diffie-Hellman public-key cryptosystem.

Very recently alternate quantum public-key protocols have been proposed, built around the difficulty in distinguishing superposed states[24], and those based on hardness of inverting one-way functions[25, 26, 27]. However, the scheme presented here differs fundamentally from these cited protocols, while also limiting the technological cost to what is already demanded, or being pursued, in the implementation of known QKD protocols.

## 4. Conclusion

To summarize, with an added layer of non-orthogonal states and measurements to the teleportation protocol by Bennet *et al.*, we have proposed a quantum algorithm that employs the receiver's public-key to achieve secure communication. As with any entanglement based protocol, no encrypted signal of the message, either classical or quantum, is ever exchanged. The proposed protocol differs from known QKD algorithms in at least three notable ways: i) *It critically incorporates the receiver's declared public-key*, which facilitates a wide variety of engagements among players, beyond enabling secure communication, ii) While Bob's public-key is critical to ensure secure communication, *it does not involve a private-key*, and iii) *The intended message bits themselves could be communicated securely*, as opposed to QKD algorithms wherein a random bit string is generated only at the end of the protocol. This last aspect, although, may not be anything more than a novelty restricted to prototypical applications, since in reality further checks and error correction methods employed at the end of the exchange will result in loss of a fraction of the communicated message bits. In practice, the set $\{a_i\}$ will likely be a random pre-decided string of bits, securely communicated employing the receiver's public-key, from which a shared-key can then be reliably constructed.

## References

[1] Shor P W 1997 *SIAM Journal of ComputingNature* **26** 1484
[2] Bennett C H and Brassard G 1984 *Proc. of the IEEE International Conference on Computers, Systems and Signal Processing* 175
[3] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[4] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 *J. Cryptol.* **5** 3
[5] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[6] Ekert A K, Rarity J G, Tapster P R and Palma G M 1992 *Phys. Rev. Lett.* **69** 1293
[7] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[8] Pirnadola S, Andersen U L, Banchi L, Berta M, Bunandar D, Colbeck R, Englund D, Gehring T, Lupo C, Ottaviani C, Pereira J L, Rizavi M, Shaari J S, Tomamichel M, Usenko V C, Vallone G, Villoresi P and Wallden P 2020 *Adv. Opt. Photonics* **12** 1012
[9] Xu F, Ma X, Zhang Q, Lo H K and Pan J W 2020 *Rev. Mod. Phys* **92** 025002
[10] Chen Y A, Zhang Q, Chen T Y, Cai W Q, Liao S K, Zhang J, Chen K, Yin J, Ren J G and Chen Z 2021 *Nature* **589** 214
[11] Bennett C H, Brassard G, Popescu S, Schumacher B, Smolin J A and Wootters W K 1996 *Phys. Rev. Lett.* **76** 722
[12] Horodecki M, Horodecki P and Horodecki R 1997 *Phys. Rev. Lett.* **78** 574
[13] Wolf R 2021 *Quantum Key Distribution* 2nd ed (*Lecture Notes in Physics* vol 2) (Heidelberg: Springer)
[14] Lu C Y, Cao Y, Peng C Z and Pan J W 2022 *Rev. Mod. Phys.* **94** 035001
[15] Neumann S P, Buchner A, Bulla L, Brohmann M and Ursin R 2022 *Nature Comm.* **13** 1
[16] Neumann S P, Selimovic M, Bohmann M and Ursin R 2022 Experimental entanglement generation for quantum key distribution beyond 1 gbit/s e-print arXiv:2107.07756v4
[17] Wegman M N and Carter J L 1981 *J. Comput. Syst. Sci.* **22** 265–279
[18] Ekert A, Gisin N, Huttner H, Inamori H and Weinfurter H 2000 Quantum cryptography *The Physics of Quantum Information* ed Bouwmeester D, Ekert A and Zeilinger A (Berlin: Springer-Verlag) chap 2, p 21
[19] Dutta A and Pathak A 1922 *Quantum Inf. Process.* **21** 369
[20] Diffie W and Hellman M E 1976 *IEEE Trans. Inf. Theory* **22** 644
[21] Katz J and Lindell Y 2020 *Introduction to Modern Cryptography* (Chapman & Hall/CRC)
[22] Bennett C H, Brassard G, Crépeau C, Jozsa R, peres A and Wootters W 1993 *Phys. Rev. Lett.* **70** 1895
[23] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge University Press)
[24] Hhan M, Morimae T and Yamakawa T 2022 e-print arXiv:2210.05978v1
[25] Kitagawa F, Morimae T, Nishimaki R and Yamakawa T 2023 e-print arXiv:2304.01800v1
[26] Barooti K, Malavolta G and Walter M 2023 Cryptology ePrint Archive, Report 2023.306
[27] Grilo A B, Sattath O and Vu Q H 2023 Cryptology ePrint Archive, Report 2023.345