

Communicating Using Non-maximally Entangled states





Sujan Vijayaraj ¹ S Balakrishnan ² K Senthilnathan ²

¹ School of Electronics Engineering, Vellore Institute of Technology, Vellore, India

² Department of Physics, School of Advanced Sciences, Vellore Institute of Technology, Vellore, India

ABSTRACT. We propose a novel quasi-quantum secure direct communication scheme using non-maximally entangled states. The proposed scheme is simple to implement using existing techniques and significantly reduces the number of leaked bits. As a result long sequences or the whole sequence of data can be communicated at once before error checking for a potential eavesdropper. The qubit efficiency of the proposed protocol is found to be 40 %.

INTRODUCTION. In this work [1], a two qubit entangled state, $(\varepsilon|00\rangle + |11\rangle)/\sqrt{\varepsilon^2 + 1}$ is used by Alice to communicate to Bob. The state can be prepared by rotating the pump polarization with respect to the vertical or horizontal by an angle Θ [2]. ε is the degree of entanglement where $0 < \varepsilon \leq 1$ and $\varepsilon = \tan \Theta$. Our protocol does not require entangled states with fixed ε , which is favorable for practical communication. We can alternatively denote the two qubit entangled state as $|\Psi\rangle = \alpha|00\rangle + \beta|11\rangle$, which is prepared by Alice. The rest of the protocol is denoted in the form of a table below, where Alice, whose operations are denoted on the left side in gold color, intends to send n bits of information to Bob. Bob’s operations are on the right side and denoted in blue color. Note that in the first step, Alice sends one of the qubit in the entangled state to Bob, while she retains the other. Skewed probability amplitudes in non-maximally entangled states can be used to arrive at the intended measurement result on Bob’s side. Incidentally, randomly complemented bits are introduced in the sequence due to the inherent nature of the prepared states. The percentage of bits to be complemented as such is controlled by the sender.

Prepares $ \Psi\rangle$ and sends one of the qubits (n times)	
Measures in R/D basis, shares the choice of bases	Measures in R/D basis, shares the choice of bases
Sifted bits: P, preserves the other bits: A	Measures in R/D basis, shares the choice of bases
Checks if P=Q; if error rate > 25 percent, communication is terminated, else sends $A \oplus P$	
	Calculates $(A \oplus P) \oplus Q$ which is approximately A
Announces position of bits to complemented in P	

ADVANTAGES.

- Non-maximally entangled states are robust to specific decoherence models [3]
- Bits deciphered by Eve (the malicious third party) when she uses compatible basis will also be wrong by a probability of $|\beta|^2$ (assuming 1 as the error bit)
- Allows long sequence of data to be transmitted at once
- Alice can keep a track on the result of Bob’s qubit due to the correlation, therefore no bits are lost in spite of change in β

QUBIT EFFECIENCY. The theoretical qubit efficiency of a protocol is defined as

$$\eta = \frac{c}{q + b}$$

where c is the number of bits received by Bob, q is the number of qubits transmitted by Alice and b is the number of classical bits exchanged between Alice and Bob [4]. Here $c = 1$, $q = 1$ and $b = 1 + 0.5 = 1.5$, where b includes the basis exchanged and the position of bits to be complemented. Thus $\eta = 0.4$ and the efficiency of the proposed protocol is 40 %.

CONSIDERATIONS. When Bob announces his subset of sifted bits, it is possible for Eve to gather some information about the sifted bits. This can be neglected by assuming the small size of the subset of bits compared to the whole sequence. To wholly avoid this, Alice can use decoy bits in between the sequence of bits she sends to Bob. They can follow the same error checking process by comparing the decoy bits, and discard them afterwards. By doing so, the length of the message sequence is preserved and transmitted to Bob.

CONCLUSION. In the proposed quasi-QSDC scheme, different bases are used along with entangled states to achieve secure communication. This scheme can also be favorable for transmitting qubits as non-maximally entangled states, as it is difficult to retain maximally entangled states during transmission in practical scenarios. One half of the sequence of bits is sent by generating sifted bits and the other half uses a cipher with the sifted bits. The position of bits to be complemented is announced by Alice at the end. The scheme also shows how secure communication can be achieved with non-maximally entangled states without losing any qubits, but at the cost of post processing the bits on the receiver side.

REFERENCES.

1. Vijayaraj, S., Balakrishnan, S., Senthilnathan, K.: Quasi-quantum secure direct communication scheme using non-maximally entangled states. arXiv preprint arXiv:1912.03498 (2019)
2. White, A. G., James, D. F., Eberhard, P. H., Kwiat, P. G.: Nonmaximally entangled states: production, characterization, and utilization. Phys. Rev. Lett. 83(16), 3103 (1999)
3. Wang, X. W., Tang, S. Q., Yuan, J. B., Kuang, L. M.: Nonmaximally entangled states can be better for quantum correlation distribution and storage. Int. J. Theor. Phys. 54(5), 1461-1469 (2015)
4. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. 85(26), 5635 (2000)