Intelligent Systems and Computer Technology
D.J. Hemanth et al. (Eds.)
© 2020 The authors and IOS Press.
This article is published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License 4.0 (CC BY-NC 4.0).
doi:10.3233/APC200118

Influence of Noise Channel in Quantum One Time Password Authentication

Mohit Kr sharma [a,1], and Manisha J Nena [b]
[a,b] *Dept of CSE, Defense Institute of Advance Technology, Pune, India*

Abstract. This paper presents an overview of quantum errors and noise channels, their mathematical modeling and its implementation in quantum one time password (QOTP) based user authentication. Quantum noise plays a pivotal role in understanding quantum information theory which is important to build up quantum communication theory. The Kraus operators provide a powerful mathematical tool in understanding and modeling various quantum channels. Use of QOTP provides an impressive method of carrying out user authentication involving quantum operations based on user biometrics. However, the efficiency of this method can be better envisaged by incorporating noise models during qubit transmission.

Keywords. Quantum Noise, Quantum Errors, Kraus Operators, Noise in QOTP

1. Introduction

Classical information theory considers noise as an important factor for calculating the channel capacities. Claude E Shannon has described the same in [1-2] where a probabilistic approach was utilised for measuring information using classical communication.

The same concepts of Shannon information theory can't be applied for quantum communication due to peculiar nature of the quantum channels. However, similar approach can be considered for deriving quantum information theory. Hence, there is a requirement of understanding noise effects on qubits and properties of quantum channels for understanding and modeling qubit interaction with the environment. Such interaction will prove to be a stepping stone in physical realization of user authentication using Quantum One Time Passwords (QOTP).

2. Preliminaries

A qubit is a bit which is in a state 0 and 1 at the same time in some fixed Density Operator**.** Let there be a quantum system with n possible pure states defined by $|\Psi_i\rangle$, $1 \leq i \leq n$ with p_i as probability of getting the state i on measurement[3]. The quantum system, therefore, is an ensemble of states $|\Psi_i\rangle$ with probability p_i , written as $(p_i, |\Psi_i\rangle)$, which allows density operator to be defined as

$$\rho = \sum_i p_i |\Psi_i\rangle\langle\Psi_i| \qquad (1)$$

[1] Mohit KrSharma, Dept of CSE,Defense Institute of Advance Technology,Pune,India
E-mail: majesticbrat@gmail.com

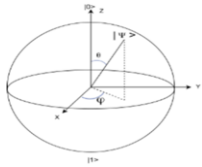


Figure 1. Bloch Sphere

2.1. Density Operators Of Composite Quantum System

AB comprises of two subsystems with individual density operators as ρ^A andρ^B, respectively. The density operator for the composite system is defined asρ^{AB}. Reduced density operator is defined for subsystems of a composite quantum system. ρ^A is reduced density operator for system A and is given by the term$\rho^A = (tr_B \rho^{AB})$. tr_B is a partial trace over system B. Similarly one can define reduced density operator for subsystem B as$\rho^B = (tr_A \rho^{AB})$.

3. Quantum System And Environment

Consider a composite system which consists of a target system T and environment E. Let the density operators defined for T and E be given by ρ^T and ρ^E respectively. Then a closed system will have density operatorρ^{TE}, defined as $\rho^T \; X \; \rho^E$. Once the composite system undergoes a unitary operation, the density matrix of the composed system is transformed as $\rho^{TE'} = \mathrm{U}\rho^{TE}\mathrm{U}^\dagger$. But as we are interested in T, the density operator of the output target system, $\rho^{T'}$, can be termed as [4] the reduced density operator over the environment and can be written as

$$\rho^{T'} = \in (\rho^T) = tr_E(\mathrm{U}\rho^{TE}\mathrm{U}^\dagger) = tr_E[\mathrm{U}\,(\rho^T \; X \; \rho^E)\mathrm{U}^\dagger] \qquad (2)$$

where $\in (\rho^T)$ is the quantum operation $\in$ carried out on target system T.

4. Kraus operators

Once we define ρ^{TE} as $\rho^T \; X \; \rho^E$, the degree of freedom of ρ^{TE} will be equal to the maximum of degree of freedom of the subsystem T and E. Let us consider E to be prepared in initial pure state $|\mathrm{e}_0\rangle\langle\mathrm{e}_0|$ with $|\mathrm{e}_k\rangle$ be the orthonormal basis with k dimensions of E. So we can rewrite equation (2) as

$$\in (\rho^T) = \sum_k \langle \mathrm{e}_k | \mathrm{U}[\rho^T \; X | \mathrm{e}_0\rangle\langle \mathrm{e}_0 |]\mathrm{U}^\dagger | \mathrm{e}_k\rangle \quad = \sum_k \langle E_k | \rho^T | E_k^\dagger\rangle \quad (3)$$

where $E_k = \langle \mathrm{e}_k | \mathrm{U} | \mathrm{e}_0 \rangle$
e_k is orthonormal basis of E, in which noise is present. E_k, called as the Kraus Operator [5][6] will define the noise environment with which T is interacting. Few of the properties of these operators [7] are:-

(a) It is a trace preserving operator i.e. $\sum_k E_k^\dagger E_k = I$, which implies $Tr\,\rho^T = \rho^T \in (\rho^T)$.

(b) These operators define environmental properties and can be used to describe dynamics of target system without considering environmental dynamics.
(c) Thus $\in (\rho^T)$ is an operator which will change the density operator of T from ρ^T to ρ_k^T given by $\frac{E_k^\dagger \rho E_k}{tr(E_k^\dagger \rho E_k)}$ with probability $tr(E_k^\dagger \rho E_k)$.
(d) Kraus operators of a quantum operation are not unique. Different set of operators can cause the same dynamics of the target system

5. Quantum Noise And Channels

Bit flip error:Bit flip error implies flipping the state of the bit with a probability p.

$|0\rangle \rightarrow |1\rangle$ or $|1\rangle \rightarrow |0\rangle$ i.e. $|\psi\rangle \rightarrow \sigma_1 |\psi\rangle$ where $\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Phase Flip Error

Phase flip error causes change in the phase i.e. change in sign.

$|0\rangle \rightarrow |0\rangle$ or $|1\rangle \rightarrow -|1\rangle$ i.e. $|\psi\rangle \rightarrow \sigma_3 |\psi\rangle$ where $\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

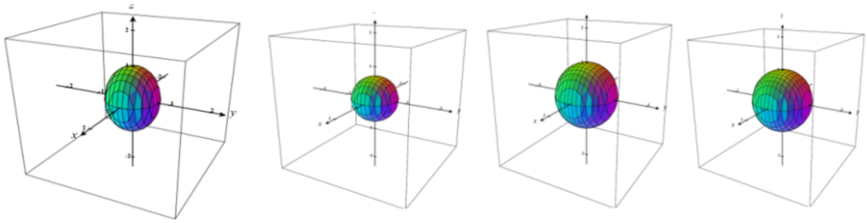
Depolarizing Channels:Channels which cause decoherence in the qubit travelling through it i.e. causing an error to occur with a probability p, are called as depolarizing channels [8]. The error can be bit flip of phase flip or both.

$|0\rangle \rightarrow +\mathrm{i}|1\rangle$ or $|1\rangle \rightarrow -\mathrm{i}|0\rangle$ i.e. $|\psi\rangle \rightarrow \sigma_2 |\psi\rangle$ where $\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

As a result any qubit in a state $|\psi\rangle$ can encounter an error with probability p and is equally likely to transform into either of three states i.e. $\sigma_1 |\psi\rangle$, $\sigma_2 |\psi\rangle$ *or* $\sigma_3 |\psi\rangle$.

Kraus operator thus can be defined as $E_k = \langle \mathrm{e}_k|\mathrm{U}|\mathrm{e}_0\rangle$, $0 \leq k \leq 3$. Thus giving four operators as $E_0 = \sqrt{1-p}$, $E_1 = \sqrt{\frac{p}{3}}\sigma_1$, $E_2 = \sqrt{\frac{p}{3}}\sigma_2$, $E_3 = \sqrt{\frac{p}{3}}\sigma_3$

The Bloch representations for these errors are shown in Figure 2.



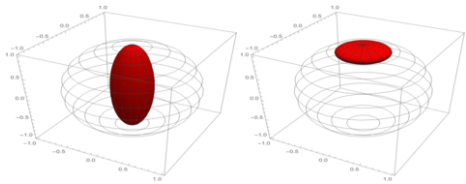
(a)(b) (c)(d)**Figure 2. Bloch Sphere Representation. (a) represents qubit without error. (b) and (c) represents qubit with bit flip error and phase flip error highlighting contraction in *yz* plane and *xy* plane respectively by factor of 1 − 2p. (d) represents qubit in decoherence channel with both the errors.**

Phase dampening channel: In this channel the qubit of the target system doesn't change its value or phase due to noise [8]. The environment qubit which is considered to be in a pure state $|0_E\rangle$ gets scattered off into $|1_E\rangle$ or $|2_E\rangle$ depending on target qubit being $|0_T\rangle$ or $|1_T\rangle$ respectively, with a probability p.The Kraus operators are given as,

$$E_0 = \sqrt{1-p}\ , E_1 = \sqrt{p}\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix} \text{ and } E_2 = \sqrt{p}\begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}$$

Amplitude dampening channel:In amplitude dampening channel, the error occurs with probability p only when the qubit of T is in high state i.e. $|1\rangle$. This error causes the state to change to lower state of $|\psi\rangle$ by releasing a photon which is gained by environment and causes a state change from $|0_E\rangle$ to $|1_E\rangle$[8].The Kraus operators can be written as, $E_0 = \begin{bmatrix}1 & 0\\ 0 & \sqrt{1-p}\end{bmatrix}$ and $E_1 = \begin{bmatrix}0 & \sqrt{p}\\ 0 & 0\end{bmatrix}$

The Bloch sphere representation of qubit undergoing phase dampening and amplitude dampening is highlighted in Figure 3(a) and 3(b) respectively.



(a) (b)

Figure 3. Bloch sphere dampening channel representation [9]

6. Noise inO TP Generation

The use cases utilizes QOTP for carrying out user authentication [10] based on user biometrics. In the uses cases, Case II and Case III involve transmission of qubits once and twice respectively. Noise models can be used accordingly to strengthen the method proposed in the paper.

Fault tolerance **(τ).**The server and user can predetermine in their agreement the acceptable fault tolerance value τ i.e. number of bits which are different from the stored code i.e. number of bits which are '1' in the output of last XOR operation.

Determining p. The server generates random number of entangled qubit pairs, transmits over the quantum medium, and gets it measured at user end. The user shares the results without using biometric code. This allows the server to test the quantum communication medium and determine the value of p.

Transmission Error Case II & III i.e. RIQ_{CM} and RIQ_{CO} proposes transmission of qubits from server to user. This qubit can suffer a bit flip error with a probability p. A qubit may suffer error during single transmission from server to user or during reverse transmission after operation from user to server. If same qubit gets affected the error gets cancelled. However, the worst case scenario of the maximum number of bits which can be flipped in dual transmission is $2p$. Hence, in RIQ_{CM} τ will be p and in $RIQ_{CO,}$ it will be $2p$.

7. Conclusion and Future Work

Understanding of noise in quantum communications holds great importance, especially when quantum operations are more prone to noise as compared to classical operations. The density operators provide a better method of representing mixed states of a quantum system created in laboratory experiments. The noise present in quantum channels can be modeled using Kraus Operators, thus providing a powerful weapon of representing the noise in quantum channel mathematically. Same operators can be used to model noise in carrying out user authentication using QOTP. With further enhancement in study of quantum channels and environment interactions of quantum systems, quantum communication can be achieved more realistically. These methods only involve noise during transmission of qubits, however errors occurring during quantum storage of qubits and quantum operations are also required to be modeled to achieve better efficiency in executing QOTP based user authentication. This highlights requirement of extensive research in the field of quantum noise as future work.

References

[1] C. E. Shannon. Mathematical theory of communication. Bell Syst. Tech. J, **27**:379–423, 623–656, 1948.
[2] C. E. Shannon and W. Weaver. Mathematical Theory of Communication.University of Illinois, Press, 1963.
[3] Gruska J. Quantum computing. 2005. McGraw-Hill London . 1999.
[4] Nielsen, Michael A., and Isaac Chuang. "Quantum computation and quantum information.", 2002: 558-559.
[5] Ruskai, Mary Beth. Optimization of Communication in Noisy Quantum Channels. No. 005, massachusetts univ lowell, 2002.
[6] Daffer, Sonja, Krzysztof Wódkiewicz, and John K. McIver. Quantum Markov channels for qubits. Physical Review A 67.6 (2003): 062312.
[7] Sharma, Vishal. Effect of Noise on Practical Quantum Communication Systems. Defence Science Journal 66.2 (2016): 186-192.
[8] Preskill, John. Lecture notes for physics 229: Quantum information and computation. California Institute of Technology 16 1998.
[9] Jagadish, V. and Petruccione, F., 2019. An invitation to quantum channels. arXiv preprint arXiv:1902.00909
[10] V.D.Ambeth Kumar, V.D.Ashok Kumar, S.Malathi and P.Jagaeedesh, “Intruder Identification using Footprint Recognition with PCA and SVM Classifiers” International Journal of Advanced Materials Research, Vols.1345.2014. 984-985.