A Logical Method to Estimate Reliability of Quantum Communication Channels

Jabbar Abbas[*] and Ranjana Abhang[**]
[*]Department of Applied Sciences, University of Technology, Baghdad-Iraq.
[**]Department of Physics, A. Garware College, Karve Rd, Pune 4, India.
[*]E-mail: jabbar1969@math.com
[**]E-mail: ranjanaabhang@ yahoo.com

Abstract

In this paper, we propose mathematical framework "Fuzzy three-valued measure and logical fuzzy integral" based on the three-valued logic. Then, we establish a simple model for representing quantum states and vagueness in transmission caused by noise, and we apply the proposed mathematical framework as a logical method to estimate reliability of quantum communication channels approximately.

Keywords: Quantum cryptosystem, Fuzzy measure, fuzzy integral, Three-valued logic.

1. Introduction

A qubit $|\Psi\rangle = a\,|0\rangle + b\,|1\rangle$ in quantum information system is extension of classical concept "bit", where $|0\rangle$ and $|1\rangle$ are basis of a two dimensional quantum system with two orthogonal states, a and b are probabilistic amplitudes in c (complex numbers). Then, one qubit can have infinite number of values in contrast with classical one bit.

In this paper, we focus on analyzing quantum information system, especially, quantum cryptosystems. It is well known that quantum cryptosystems such as bb84 protocol [1] enable us to detect eavesdropping of encryption key because in quantum state, it can be observed only once unless eavesdropper use the same quantum basis as sender's, or use orthogonal quantum basis against sender's. In quantum cryptosystems, errors in transmission are utilized actively because they are caused by eavesdropping. In practice, however, eavesdropping is not the only source of errors in transmission. Imperfections of source, channels, and detectors may also produce errors. In this paper, we propose the mathematical framework (fuzzy three-valued measure and logical fuzzy integral) to estimate quantum cryptosystems approximately.

2. Fuzzy three-valued measure and logical fuzzy integral

2.1 fuzzy three-valued measure:

Classical logic allows just two truth values, true (t) or false (f). Kleene's three-valued logic was originally designed to accommodate undecided mathematical statements. The third value represents an "unknown" value (u) to indicate a state of partial vagueness. This informal reading suggests two natural orderings, concerning "degree of truth" and "amount of vagueness". If degree of truth is the issue, not knowing a classical truth value to assign to a sentence is better than knowing the sentence is false, while knowing it is true is better yet. Then in the 'truth' ordering, false is less than unknown which is less than true. On the other hand, 1 and 0 can be interpreted as true and false, respectively. Then, 1/2 is the middle value in [0, 1], and can be interpreted as unknown whether true or false. Therefore, it is the vaguest state. Based on this fact, the partial ordering relation with respect to vagueness on [0, 1] is denoted by $\mathbf{p}_V$.

Remark:

Hereafter, to simplify notation, we assume a finite universe of discourse $X = \{1, 2, ..., i, ..., n\}$ instead of $X = \{x_1, x_2, ..., x_i, ..., x_n\}$.

Definition 1:

Let $X = \{1, ..., i, ..., n\}$ be the universe of discourse and B be a subset of X . Then, we define the characteristic function of an element i in X as follows:

$$q_B(i) = \begin{cases} 1 \ \text{ iff } i \text{ memberof } B, \\ \frac{1}{2} \ \text{ iff unknown whether } i \text{ memberof } B \text{ or not}, \\ 0 \, \text{iff } i \text{ nonmemberof } B. \end{cases}$$

We consider the meaning of the three values, 1, 0 and 1/2, which are taken by the above characteristic function. It is valid and natural that there is a relationship among 1, 0 and 1/2. That is, "nonmember (0)" and "unknown (1/2)" are comparable to each other. And similarly "member (1)" and "unknown (1/2)" are comparable to each other. Furthermore, "unknown (1/2)" is the most ambiguous state. The partial ordering relation with respect to ambiguity is denoted by $\mathbf{p}_A$. Let X be the universe of discourse and $B \in 3^X$ (where 3^X means the power set of X, which is based on three-valued characteristic function as in definition 1).

Then the interpretation and notation of the element i of X is as follows:

(i) If i is member of B $(q_B(i)=1)$, then the element i is interpreted as the true element and represented as i^T in B.

(ii) If i is nonmember of B $(q_B(i)=0)$, then the element i is interpreted as the false element and represented as i^F in B.

(iii) If i is unknown whether member of B or not $q_B(i)=1/2)$, then the element i is interpreted as the unknown whether true or false element and represented as i^U in B.

Although the relationship between partial ordering relation with respect to ambiguity ($\mathbf{p}_A$) and partial ordering relation with respect to vagueness ($\mathbf{p}_V$) is a numerical relation, we apply and extend this relation to sets of the power set of the universe of discourse.

Definition 2:

Let X be the universe of discourse and $B_1, B_2 \in 3^X$. Then, $B_1 \mathbf{p}_A B_2$ holds iff $q_{B_1}(i) \mathbf{p}_A q_{B_2}(i)$ holds, $\forall i \in 2^X$.

Fig.(1) shows that hasse diagram of partially ordered set $\langle 3^X, \mathbf{p}_A \rangle$ for $n=2$.

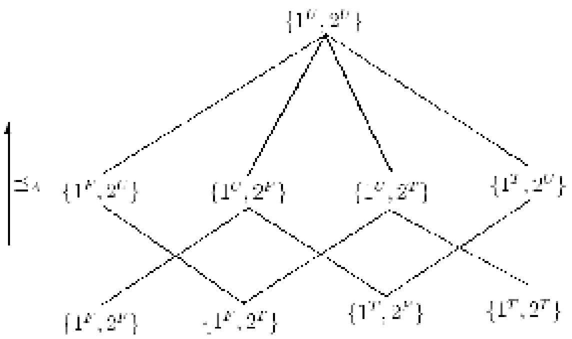


Fig.(1) Hasse diagram of partially ordered set
á3^X ,$\mathbf{p}_A$ ñ *for n = 2.*

Based on the definitions mentioned above, we propose the following definition of fuzzy three-valued measure.

Definition 3:

A fuzzy three-valued measure (g_t) on the universe of discourse x is a normed set function g_t: $3^X :\to [0,1]$, which satisfies the following requirement if:

$B_1, B_2 \in 3^X$ and $B_1 \mathbf{p}_A B_2$ then $g_t(B_1) \mathbf{p}_A g_t(B_2)$.

2.2 logical fuzzy integral:

In the previous subsection, we mentioned the interpretation of the truth-value 1/2, expresses unknown whether true (1) or false (0). In this subsection, we propose fuzzy integral model based on the three-valued logic of a measurable function (h) with respect to fuzzy three-valued measure (g_t). Let $X=\{1,...,i,...,n\}$ be the universe of discourse which is defined as the set of usual fuzzy integral inputs, these inputs values are $h(i) \in [0,1], i=1,...,n.$ in the new fuzzy integral model (logical fuzzy integral), the input values are divided into true (t), false (f), and unknown (u) as shown in figure 4. That is, the $i-$th true input value is $h(i^T) \in [0,1]$, false $h(i^F) \in [0,1]$, and unknown $h(i^U) \in [0,1]$. Where $h(i^T)+h(i^F)+h(i^U)=1$ and $h(i^T)=0$ or $h(i^F)=0$ for each i. In this case, when the number of original input values is n, it is a set of $3n$ inputs. Let the universal set of logical fuzzy integral inputs be

$$X^* = \{1^T, ..., n^T, 1^F, ..., n^F, 1^U, ..., n^U\} \quad ......(1)$$

and

$h : X^{*} \rightarrow [0,1]$ .... (2)

They are converted from $x_i = h(i)$ into $h(i^T)$, $h(i^F)$, $h(i^U)$, as shown in Fig.(2). The functions of figure 2 are r^T, r^F, r^U called as "conversion functions":

$$r^T(x) = \begin{cases} (x-0.5)\times 2 & \text{if } x \geq 0.5 \\ 0 & \text{if } x < 0.5 \end{cases}$$

$$r^F(x) = \begin{cases} 0 & \text{if } x \geq 0.5 \\ (0.5\text{-}x) & \text{if } x < 0.5 \end{cases}$$

$$r^U(x) = 1 - |x - 0.5| \times 2 \quad \text{.............................} (3)$$

And the input value is set as follows:

$h(i^T) = r^T(x_i)$, $h(i^F) = r^F(x_i)$,

$h(i^U) = r^U(x_i)$ .... (4)

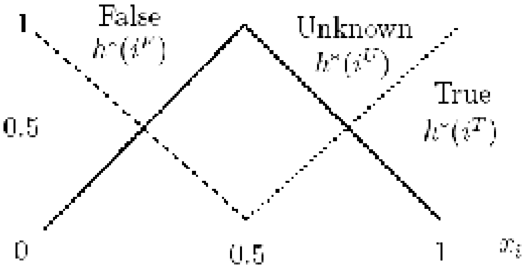


Fig.(2).

Definition 4:

The subset of X^{*}containing the complementary element [i^T or i^U is called the complementary element for i^T (the same with other combinations)] is called the complementary set, and the subset of X^{*}not containing the complementary elements is called the non-complementary set.

Definition 5:

The non-complementary set with the n elements is called basic set. This is, the basic set is the set which contains only one out of i^T, i^F, and i^U and for all $i, (i = 1,\ldots,n)$.

For example, if $n = 5$ then $\{1^{\mathrm{T}}, 2^{\mathrm{F}}, 3^{\mathrm{T}}, 4^{\mathrm{U}}, 5^{\mathrm{F}}\}$ is basic set. The set of the basic sets of X^{*} is denoted by B.

Fuzzy measure value (m^T, m^F, m^U) is assigned for each of t, f, and u. The fuzzy measure values are assigned as follows:

(1) All the fuzzy measure values, m^T, m^F, m^U of the non-complementary set which is not a basic set and complementary set not containing the basic set are 0. For example, when n=3, $\mu^T(\{1^T, 2^F\}) = 0$, $\mu^U(\{1^U, 2^T, 2^F\}) = 0$.

(2) The fuzzy measure values of basic set B are assigned from the following equation:

$m^T = r^T(g_t(B))$, $m^F = r^F(g_t(B))$,

$\mu^U = r^U(g_t(B))$ .... (5)

Where $g_t(B)$ is the fuzzy three-valued measure of the basic set B, and r^T, r^F, r^U are conversion functions as shown in equation (3).

(3) Let c be the complementary set which includes basic set and contains at most two out of i^T, i^F, and i^U for some i. The set of all complementary sets is denoted by Λ. The fuzzy measure value of those set containing three elements for any i is assumed to be 0 for the sake of convenience. C is calculated from the fuzzy measure value of the two basic sets covering c. For the calculation, the superscripts t, f, u are omitted because i^T, i^F, i^U are common. To calculate $m(\mathrm{C})$, c is divided into two basic sets, B_1 and B_2, where $B_1, B_2 \in 3^X$ and $B_1 \cup B_2 = \mathrm{C}$. $m(\mathrm{C}) = m(B_1) + m(B_2)$. for example, if $n = 2, \mathrm{C} = \{1^T, 2^T, 2^U\}$ then $B_1 = \{1^T, 2^T\}, B_2 = \{1^T, 2^U\}$, and:

$$m(\{1^T, 2^T, 2^U\}) = m(\{1^T, 2^T\}) + m(\{1^T, 2^U\}).$$

If there can be many combination of B_1 and B_2, the mean value is calculated by the following equation.

$$\mu(\mathrm{C}) = \frac{\sum\limits_{\{(B_1,B_2)|B_1 \cup B_2 = \mathrm{C}\}} \mu(B_1) + \mu(B_2)}{|(B_1, B_2) \,|\, B_1 \cup B_2 = \mathrm{C}|} \quad \text{.....} (6)$$

Definition 6:

Let $g_t : 3^X \rightarrow [0,1]$ be a fuzzy three-valued measure and $h : X \rightarrow [0,1]$ be a measurable function. The logical fuzzy integral of h with respect to g_t is defined by the following equations:

$$z^T = \sum_{j=1}^{2n} [h(s_j^{p_j}) - h(s_{j+1}^{p_{j+1}})] \mu^T(\{s_1^{p_1}, \ldots, s_j^{p_j}\}) \quad \text{.........} (7)$$

$$z^F = \sum_{j=1}^{2n} [h(s_j^{p_j}) - h(s_{j+1}^{p_{j+1}})]\mu^F(\{s_1^{p_1},...,s_j^{p_j}\}) \quad \cdots (8)$$

$$z^U = \sum_{j=1}^{2n} [h(s_j^{p_j}) - h(s_{j+1}^{p_{j+1}})]\mu^U(\{s_1^{p_1},...,s_j^{p_j}\}) \quad \cdots\cdots (9)$$

Where z^T, z^F, z^U are the output values, m^T, m^F, m^U are fuzzy measure values for each of t, f, u, and $h(s_1^{p_1}),...,h(s_j^{p_j}),...,h(s_{2n}^{p_{2n}})$ are the input values of h (after conversion), such that $h(s_1^{p_1}) \geq ... \geq h(s_j^{p_j}) \geq ... \geq h(s_{2n}^{p_{2n}}) \geq 0$ for all $s_1,...,s_{2n} \in X^*$ and $p_1,..., p_{2n} \in \{\mathrm{T, F, U}\}$. Note that there are at least n terms in the sequence $\{h(i^T), h(i^F), h(i^U)\}_{i \in X}$ that are zero. Hence there are only n terms of h in the present case.

The output of the logical fuzzy integral expresses those restored to values (x_i) of [0, 1] by applying r^{-1} of equation (3) from z^T, z^F, z^U which is result of logical fuzzy integral. That is, the result of logical fuzzy integral equal to value $1 - \frac{1}{2}z^U$, if the number of input variables (x_i) which have the values $x_i \geq 0.5$ greater or equal to the number of input variables (x_i) which have values $x_i < 0.5$, and $z^F = 0$. Otherwise the result of logical fuzzy integral equal to value $\frac{1}{2}z^U$.

3 a logical method to estimate reliability of quantum communication channels

3.1 an algebra in quantum states with two orthogonal basis:

The bit is the fundamental concept of classical computation and classical information. Quantum computation and quantum information are built upon an analogous concept, the *quantum bit*, or *qubit* for short. Just as a classical bit has a state "either 0 or 1" a qubit also has a state. Two possible states for a qubit are the states $|0\rangle$ and $|1\rangle$, which correspond to the states 0 and 1 for a classical bit. The difference between bits and qubits is that a qubit can be in a state other than $|0\rangle$ or $|1\rangle$. It is also possible to form linear combinations of states, often called *superpositions*:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (10)$$

The numbers a and b are complex numbers, although for many purpose not much is lost by thinking of them as real numbers. Put another way, the state of a qubit is a vector in a two-dimensional complex vector space. The special states $|0\rangle$ and $|1\rangle$ are known as *computational basis states*.

Definition 7:

Let $|0\rangle$ and $|1\rangle$ be two orthogonal basis characterized by $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ and $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix} \in C^2$. then, state vector is superposition of $|0\rangle$ and $|1\rangle$. It is represented in

$|\Psi\rangle = a\ |0\rangle + b\ |1\rangle$, where $a\ , b \in C$ satisfy $|\,a\,|^2 + |\,b\,|^2 = 1$.

***Definition* 8:**

Let $|\Psi_A\rangle = a_A|0\rangle + b_A|1\rangle$ and $|\Psi_B\rangle = a_B|0\rangle + b_B|1\rangle$ be superpositions. Then, we define an ordering $\mathbf{p}_Q$ between $|\Psi_A\rangle$ and $|\Psi_B\rangle$ as follows :

$$|\Psi_A\rangle\ \mathbf{p}_Q\,|\Psi_B\rangle \text{ iff } |\beta_A|^2 \leq |\beta_A|^2 \quad \ldots\ldots\ldots (11)$$

Note that $\leq$ is usual ordering in real number. For example, let:

$$|\Psi_A\rangle = \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle, |\Psi_B\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

then, $|\Psi_A\rangle\ \mathbf{p}_Q\,|\Psi_B\rangle$ holds because $|b_A|^2 = \frac{1}{4} \leq \frac{1}{2} = |b_B|^2$ holds.

***Definition* 9:**

Let $|\Psi_A\rangle$ and $|\Psi_B\rangle$ be superpositions. The binary operations $\wedge_Q$ and $\vee_Q$ are defined as follows :

$$|\Psi_A\rangle \wedge_Q |\Psi_B\rangle = |\Psi_A\rangle \text{ iff } |\Psi_A\rangle\,\mathbf{p}_Q\,|\Psi_B\rangle \qquad (12)$$

$$|\Psi_A\rangle \vee_Q |\Psi_B\rangle = |\Psi_B\rangle \text{ iff } |\Psi_A\rangle\,\mathbf{p}_Q\,|\Psi_B\rangle \qquad (13)$$

***Definition* 10:**

Let $|\Psi\rangle = a\ |0\rangle + b\ |1\rangle$, be a superposition. Then we define a unary Operation $\sim_Q$ as follows :

$$\sim_Q|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (14)$$

For example, we illustrate examples of definition 12 and definition 13 using

$|\Psi_A\rangle = \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle$ and

$|\Psi_B\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{2}|1\rangle$, as follows:

- $|\Psi_A\rangle \wedge_Q |\Psi_B\rangle = |\Psi_A\rangle$,
- $|\Psi_A\rangle \vee_Q |\Psi_B\rangle = |\Psi_B\rangle$
- $\sim_Q |\Psi_A\rangle = -\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$
- $\sim_Q |\Psi_B\rangle = |\Psi_B\rangle$.

If we can give physical meaning to operations $\wedge_Q$ and $\vee_Q$, and $\sim_Q$ we can treat a set of superpositions Q as kleene algebra.

3.2 Partial ordering relation with respect to superpositions:

Hereafter, $|\frac{1}{2}\rangle$ stands for four superpositions $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$, $-\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and $-\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$, all of which have probability $\frac{1}{2}$ for both $|0\rangle$ and $|1\rangle$. then we define below a fundamental partial ordering relation among $|0\rangle$,$|1\rangle$ and $|\frac{1}{2}\rangle$.

Definition 11:

We define a partial ordering relation with respect to superpositions (will be denoted by $\mathbf{p}_Q$) as follows :

$|i\rangle = |i\rangle$, for all $i \in \{0, \frac{1}{2}, 1\}$

$|i\rangle = |\frac{1}{2}\rangle$, for all $i \in \{0,1\}$.

Fig.(3) shows the partial ordering relation with respect to superpositions $(\langle\{|0\rangle, |\frac{1}{2}\rangle, |1\rangle, \mathbf{p}_Q\rangle)$.

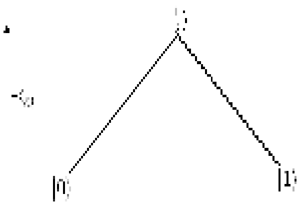


Fig. (3) Partial ordering relation with respect to superpositions (<{|0>, $|\frac{1}{2}$ >}, $\mathbf{p}_Q$ >).

The partial ordering relation with respect to superpositions ($\mathbf{p}_Q$) can be extended to n-dimensional tensor product follows:

Definition 12:

Let $|k_1,k_2,...,k_n\rangle = |k_1\rangle \otimes .... \otimes |k_n\rangle$ and $|k_1,k_2,...,k_n\rangle = |k_1\rangle \otimes .... \otimes |k_n\rangle$ be tensor products where $k_i, l_i \in \{0, \frac{1}{2}, 1\}$ and the definition of $\otimes$ is usual one. Then $|k_1,k_2,...,k_n\rangle \, \mathbf{p}_Q |l_1,l_2,....l_n\rangle$ holds if and only if $|k_i\rangle \, \mathbf{p}_Q |l_i\rangle, \forall i$ holds.

Fig.(4) shows the hasse diagram of partial ordering relation $\mathbf{p}_Q$ in case that $n = 2$.

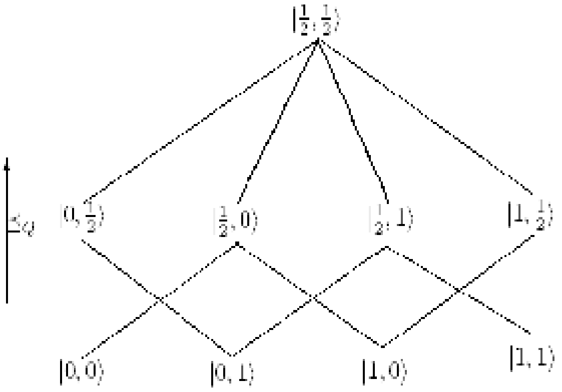


Fig. (4) Hasse daiagram of partial ordering relation $\mathbf{p}_Q$ in case that n =2.

3.3 encryption key distribution of bb84 cryptography protocol:

Bb84 cyptography protocol was proposed by bennett and brassard in 1984 [1]. Bb84 protocol make a series of bit message that represent encryption key in quantum channel unable to decipher using *verman cipher* (see [11] for details) and principle of quantum mechanics, that is, observation (eavesdropping) cause the collapse of superpositions into basis. Here, we assume quantum communication environment as shown in Fig.(5). That is, two kinds of direction of polarization ($\oplus -$polarization, $\otimes -$polarization) are used. $\otimes -$ polarization is at an angle 45° to $\oplus -$polarization. We below consider relations among $|0\rangle_{\oplus}, |1\rangle_{\oplus}, |0\rangle_{\otimes}$, $|1\rangle_{\otimes}$. Clearly, $|0\rangle_{\oplus} = \frac{1}{\sqrt{2}}(|0\rangle_{\oplus} + |1\rangle_{\oplus})$ and $|0\rangle_{\otimes} = \frac{1}{\sqrt{2}}(|0\rangle_{\oplus} - |1\rangle_{\oplus})$ hold. That is $|0\rangle_{\otimes}$ and

$|1\rangle_{\otimes}$ are superposition of $|0\rangle_{\oplus}$ and $|1\rangle_{\oplus}$. Conversely, $|0\rangle_{\oplus}$ and $|1\rangle_{\oplus}$ are also superposition of $|0\rangle_{\otimes}$ and $|1\rangle_{\otimes}$.

In no noise environment, if alice sends a photon using $\oplus-$filter ($\otimes-$filter) and bob receives it using $\oplus-$detector($\otimes-$detector), then bit value can be communicated
Correctly.

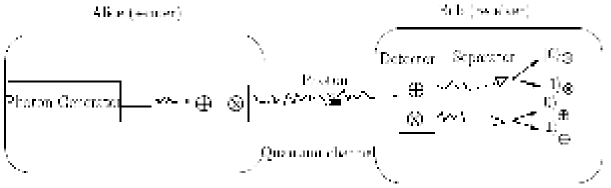


Fig. (5) Quantum communication environment.

However, if alice sends a photon using $\oplus-$filter ($\otimes-$ filter) and bob receives it using $\oplus-$detector ($\otimes-$detector), then bob receives incorrectly bit value with probability 50%. Based on the fact, bb84 protocol make eavesdropping be detected. (for more details, see literature such as [2], [6], and [11]). According to above, we formulate bb84 protocol in ambiguity (vague and noisy) environment. We consider the following tuple: (signal alice sent, signal bob detected) "signal alice sent" take a value as follows:

0: alice sent $|0\rangle_{\oplus}$ or $|0\rangle_{\otimes}$ without noise.

1: alice sent $|1\rangle_{\oplus}$ or $|1\rangle_{\otimes}$ without noise.

$\frac{1}{2}$: alice sent noisy state.

Similarly, "signal bob received" take a value as follows:

0: bob detected $|0\rangle_{\oplus}$ or$|0\rangle_{\otimes}$.

1: bob detected $|1\rangle_{\oplus}$ or$|1\rangle_{\otimes}$.

$\frac{1}{2}$: bob could not detect alice's signal.

All tuples representing (signal alice sent, signal bob detected) are sets of$\{0,\frac{1}{2},1\}^2$, and partially ordered set with respect to ambiguity $\langle\{0,\frac{1}{2},1\}^2,\mathbf{p}_A\rangle$ is shown in Fig.(6). This relation is isomorphic to partial ordering relation with respect to $\mathbf{p}_Q$, as shown in Fig.(6). In unvague and no noise environment, the tuple (signal alice sent, signal bob detected) must be one of (0, 0), (0, 1), (1, 0), and (1, 1). However, in vague and noise environment, it does not hold true.

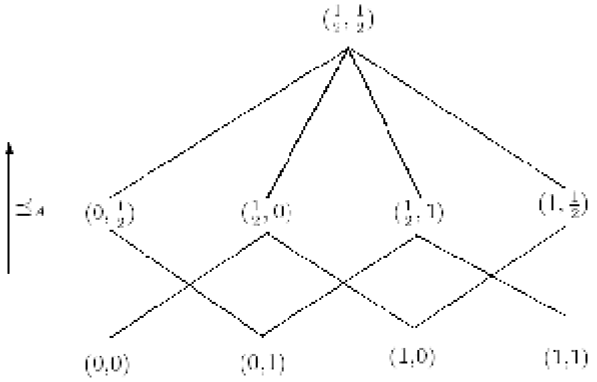


Fig. (6) Hasse diagram of poset $<\{0, \frac{1}{2}, 1\}^2, \underline{\mathbf{p}}_A>$.

Based on our proposals, fuzzy three-valued measure and logical fuzzy integral can both represent unknown state of quantum system and provide us an approximate method to estimate quantum cryptosystems. We describe correspondence between the sets of $\{0,\frac{1}{2},1\}^2$, and the sets of 3^X by replace (0,0) with $\{1^F,2^F\}$, (0, 1) with $\{1^F,2^T\}$, (1, 0) with $\{1^T,2^F\}$, (1, 1) with $\{1^T,2^T\}$, (0, 1/2) with $\{1^F,2^U\}$, (1/2 , 0) with $\{1^U,2^F\}$, (1/2, 1) with $\{1^U,2^T\}$, (1, 1/2) with $\{1^T,2^U\}$ and (1/2, 1/2) with $\{1^U,2^U\}$. Accordingly, we can generate sets of 3^X and partial ordering set $\langle\{0,\frac{1}{2},1\}^2,\mathbf{p}_A\rangle$ as shown in figure 6 corresponds with partial ordering set $\langle 3^X,\mathbf{p}_A\rangle$ for $n=2$, as shown in figure 1.

3.4 illustrative example (practical example)

In this section, we illustrate on a simple example the method for reliability estimation in a noisy quantum communication channel from alice to bob, using fuzzy three-valued measure and logical fuzzy integral. We assign fuzzy three-valued measure (g_t) to sets, which are represented (signal alice sent, signal bob detected). According to the following criteria:

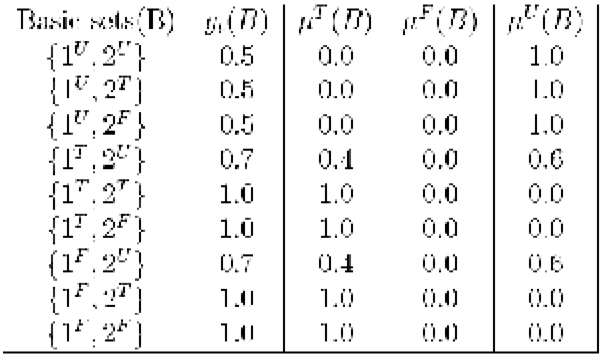
- (0, 0), (0, 1), (1, 0), and (1, 1) are assigned 1. The reason is that we can operate bb84 protocol correctly because alice and bob can send and detect bit information correctly.

- (0, 1/2) and (1, 1/2) are assigned 0.7. The reason is that bob is receiver and can inform his impossibility of detection to alice. These cases are not the worst.
- (1/2, 0) and (1/2, 1) are assigned 0.5. The reason is that bob can not judge alice's trouble because he detects 0 or 1.these cases are the worst.
- (1/2, 1/2) is assigned 0.5 because clearly it means the worst case.

The assignments of fuzzy three-valued measures gt by criteria mentioned above are also shown in table 1. A measurable function $h(i) = 100 - i$ is an availability function, where i means percentage of error rate of alice's photon generator and bob's photon detector. Therefore, we can apply logical fuzzy integral to estimate reliability of quantum communication channel from alice to bob as follows:

When alice's error rate is 3% and bob 6%, availability of them are $x_1 = h(1) = 0.97$ and $x_2 = h(2) = 0.94$, respectively. From equation (3), $h(1^T) = 0.94$, $h(1^F) = 0$, $h(1^U) = 0.06$, $h(2^T) = 0.88$, $h(2^F) = 0$, $h(2^U) = 0.12$. Then, after sorting of values h with decreasing order ($h(1^T) = 0.94$, $h(2^T) = 0.88$, $h(2^U) = 0.12$, $h(1^U) = 0.06$, $h(1^F) = 0$, $h(2^F) = 0$), the output corresponding to the basic set $B = \{1^T, 2^T\}$ is calculated as follows: $g_t(\{1^T, 2^T\}) = 1$ so $m^T(\{1^T, 2^T\}) = 1$, $m^F(\{1^T, 2^T\}) = 0$, $m^U(\{1^T, 2^T\}) = 0$ from equation (5). The fuzzy measure values (m^T, m^F, m^U) of other basic sets are shown in Table (1).

Table(1)
Assignments of g_t and fuzzy measure values of basic sets.



Basic sets(B)	$g_t(B)$	$\mu^T(B)$	$\mu^F(B)$	$\mu^U(B)$
$\{1^U, 2^U\}$	0.5	0.0	0.0	1.0
$\{1^U, 2^T\}$	0.5	0.0	0.0	1.0
$\{1^U, 2^F\}$	0.5	0.0	0.0	1.0
$\{1^T, 2^U\}$	0.7	0.4	0.0	0.6
$\{1^T, 2^T\}$	1.0	1.0	0.0	0.0
$\{1^T, 2^F\}$	1.0	1.0	0.0	0.0
$\{1^F, 2^U\}$	0.7	0.4	0.0	0.6
$\{1^F, 2^T\}$	1.0	1.0	0.0	0.0
$\{1^F, 2^F\}$	1.0	1.0	0.0	0.0

Next,

$m^T(\{1^T, 2^T, 2^U\}) = m^T(\{1^T, 2^T\}) + m^T(\{1^T, 2^U\}) = 1.4$

also

$m^F(\{1^T, 2^T, 2^U\}) = m^F(\{1^T, 2^T\}) + m^F(\{1^T, 2^U\}) = 0,$

$m^U(\{1^T, 2^T, 2^U\}) = m^U(\{1^T, 2^T\}) + m^U(\{1^T, 2^U\}) = 0.6$

now, $m^T(\{1^T, 1^U, 2^T, 2^U\}) = 0.7$ is the mean of

$m^T(\{1^T, 2^T\}) + m^T(\{1^U, 2^U\}) = 1$ and

$m^T(\{1^T, 2^U\}) + m^T(\{1^U, 2^T\}) = 0.4.$

Also, $m^F(\{1^T, 1^U, 2^T, 2^U\}) = 0$ is the mean of

$m^F(\{1^T, 2^T\}) + m^F(\{1^U, 2^U\}) = 0$ and

$m^F(\{1^T, 2^U\}) + m^F(\{1^U, 2^T\}) = 0,$

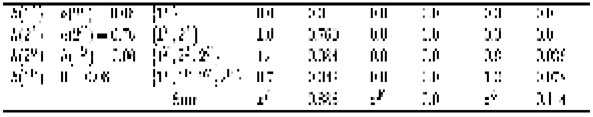
$m^U(\{1^T, 1^U, 2^T, 2^U\}) = 1.3$ is the mean

$m^U(\{1^T, 2^T\}) + m^U(\{1^U, 2^U\}) = 1$ and

$m^U(\{1^T, 2^U\}) + m^U(\{1^U, 2^T\}) = 1.6.$

The calculation of logical fuzzy integral is shown in Table (2). The result of logical fuzzy integral is 0.943 (by $1 - \frac{1}{2} z^U$). This is an approximate reliability in a noisy quantum communication channel from alice to bob evaluated by their criteria according to their situation.

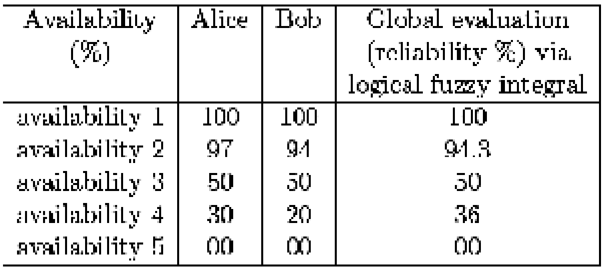
Table (2)
Calculation of logical fuzzy integral.



Alternative			A	$\mu^T(A)$	Product	$\mu^F(A)$	Product	$\mu^U(A)$	Product
[illegible]	[illegible]	[illegible]	$\{1^T\}$	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	$\{1^T, 2^T\}$	1.0	[illegible]	0.0	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	$\{1^T, 2^T, 2^U\}$	[illegible]	[illegible]	0.0	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
			Sum	z^T	[illegible]	z^F	[illegible]	z^U	[illegible]

A table showing the global evaluation (reliability estimation of quantum communication channels) via logical fuzzy integral of different percentages of availability of alice’s photon generator and bob’s photon detector is given in Table (3).

Table (3)
Global evolution table.



Availability (%)	Alice	Bob	Global evaluation (reliability %) via logical fuzzy integral
availability 1	100	100	100
availability 2	97	94	94.3
availability 3	50	50	50
availability 4	30	20	36
availability 5	00	00	00

4. Conclusions

In this paper, first we have established a simple model for representing quantum states and vagueness in transmission caused by noise and so on, and showed that it forms kleene algebra. Secondly, we have applied the proposed mathematical framework (fuzzy three-valued measure and logical fuzzy integral) to estimate quantum cryptosystems approximately.

The framework would be an effective tool for analyzing more complex quantum systems although we have illustrated a simple example in this paper.

References

[1] Bennet C. H. And Brassard G., "quantum cryptography: public key distribution and coin tossing’", proc. Ieee conference on computers, systems and signal processing, bangalore, India, pp.175-179, 1984.

[2] Brooks M. (ed.), "quantum computing and communications", springer-verlag london berlin heidelberg, 1999.

[3] Cgnoli R., "injective de morgen algebra and kleene algebra", proc. Amer. Math. Soc., Vol. 47, pp. 269-278, 1975.

[4] Denneberg D., "non-additive measure and integral", kluwer academic publisher, 1994.

[5] Grabisch M., Murofushi T., and sugeno m. (eds.), "fuzzy measures and integrals", physic-verlag, 2000.

[6] Gruska J., "quantum commputing", macgraw-hill publishing, 1999.

[7] Ishikawa M., and et al., "thresholding based image segmentation aided by kleene algebra", ieice trans. Inf. Syst., Vol.e82-d, No.5 .pp.962-967, 1999.

[8] Klir G.J. and Floger T.A., "fuzzy sets, uncertainty, and information", prentice hall, englewood cliffs, new jersey, 1988.

[9] Fitting M., "kleene’s logic", generalized. J. Log. Comput, 1(6), pp: 797-810, 1991.

[10] Fitting M. And Orlowska E. (eds.), "beyond two: theory and applications of multiple valued logic", physic-verlag, 2003.

[11] Nielsen M. A. And chuang I. L., "quantum computation and quantum information", cambridge university press, 2000.

[12] Takahagi E., "fuzzy three-valued switching function using choquet integral", journal of advanced computational intelligence and intelligent informatics, Vol.7, No.1, pp. 47-52, 2003.

[13] Tomoyuki Araki, "a simple model for estimating quantum communication channels", 6th international workshop on boolean problems, technische university, sep.22-24, 2004.

[14] Wang Z. And Klir G.J., "fuzzy measures theory", plenum press, new york, 1992.

[15] Zadeh, L. A., "fuzzy sets", inf. Control, Vol. 8, pp. 338-353, 1965.

الخلاصة

نقترح في هذا البحث إطارا رياضي" قياس ضبابي ثلاثي القيم وتكامل ضبابي منطقي" مبني على المنطق الرياضي ذو القيمتيين. ثم ننشأ نموذج بسيط لتمثيل الحالات الكمية والغموض في الإرسال المتسبب بالضوضاء، ونطبّق الإطار الرياضي المقترح كطريقة منطقيّة لتقدير معولية قنوات الإتصال الكمّي بشكل تقريبي.