International Journal of Advanced Engineering and Technology
ISSN: 2456-7655
Impact Factor: RJIF 5.54
www.newengineeringjournal.com
Volume 1; Issue 5; November 2017; Page No. 35-42

A quantum encryption method in wireless sensor networks

Sheng Guo[1], Shuo Yao[2], Yinyin Zhang[3], Jingya Xiang[4], Zhengying Cai[5*]
[1, 3, 5] College of Computer and Information Technology, China Three Gorges University, Yichang, China
[2, 4] School of Foreign Language, China Three Gorges University, Yichang, China

Abstract
This article focuses on the topics of the quantum encryption method in wireless sensor networks. First, from the aspect of the nature separation and the secure, we studied the secure model. Second, the security of the quantum protocol was studied for Wireless Sensor Networks by three points that are the environment, privacy protection and the quantum system. Third, the security of the quantum communication protocol was analyzed by three sides, which are the side of the improved, the protocol matrix and the probabilisti. Four, the analysis results show that this method is so good for the wireless sensor networks.

Keywords: wireless sensor networks, network security, quantum encryption, BB84 protocol

1. Introduction

1.1 Related Work

Recently the security of Wireless sensor networks gained more and more attention. Fan, Hu, Luan, Dong (2017) [2] introduced DisLoc: A Convex Partitioning Based Approach for Distributed 3-D Localization in Wireless Sensor Networks. Sasaki, Miyaji, Uehara (2017) [3] presented Energy Budget Formulation in Progress-Based Nearest Forwarding Routing Policy for Energy-Efficient Wireless Sensor Networks. Rajeswari, Bhagyaveni (2017) [4] proposed MAP Based V-BLAST Transmission to Improve Network Lifetime in Virtual MIMO Based Wireless Sensor Networks. Omairi, Ismail, Danapalasingam, Ibrahim (2017) [5] described Power Harvesting in Wireless Sensor Networks and Its Adaptation With Maximum Power Point Tracking: Current Technology and Future Directions. Yu, Zhang, Yao, Li, (2016) [6] produced R3: A Lightweight Reactive Ring based Routing Protocol for Wireless Sensor Networks with Mobile Sinks. Mehmood, Lloret, Sendra (2016) [7] studied A secure and low-energy zone-based wireless sensor networks routing protocol for pollution monitoring. Mou, Wang (2015) discussed Reference State Tracking in Distributed Leader-Following Wireless Sensor Networks with Limited Errors. Kim (2017) [9] displayed Two-Stage Model for Security Network-Constrained Market Auction in Pool-Based Electricity Market. Shin, Wang, Gu (2015) made a modle A First Step Toward Network Security Virtualization: From Concept To Prototype. Xiang, Al-Dubi, Liu, Chu (2015) [12] modelled Frontier technologies of trust computing and network security. Kohira, Mitsuhashi, Yahiro, Ikeda (2016) [13] put forward Solution for Virtualization to Ensure Optimal Network Security Environment. Wang, Shi, Xiang, Li (2016) [14] researched Efficient Network Security Policy Enforcement with Policy Space Analysis. Pearce, Zeadally (2015) [15] talked about Ancillary Impacts of Multipath TCP on Current and Future Network Security.

Some researchers proposed encryption method for wireless sensor networks. Wang, Xu, Song (2017) [16] created Research on the improved algorithm for image quantum encryption in multimedia networks. Shi (2017) adopted Verifiable Quantum Encryption and its Practical Applications. Wang, She, Huang, Ouyang (2016) [18] applied Optimal Symmetric Ternary Quantum Encryption Schemes. Anonymous (2017) [19, 20] built Ottawa displays high-dimensional quantum encryption. Anonymous (2017) [19, 20] considered Optical signals measured from space could enable quantum encryption network. Smith (2016) [21] draw quantum leap quantum encryption. Shenoy, Aravinda, Srikanth, Home (2017) [22] indicated Can the use of the Leggett-Garg inequality enhance security of the BB84 protocol?. Khokhlov (2016) [23] illustrated Scheme of the arrangement for attack on the protocol BB84. Zhao, Zhu, Quan (2015) featured A Novel Basis Splitting Eavesdropping Scheme in Quantum Cryptography Based on the BB84 Protocol. Gleim, AV; Egorov, VI; Nazarov, YV; Smirnov, SV; Chistyakov, VV; Bannik, OI; Anisimov, AA; Kynev, SM; Ivanova, Collins (2016) exhibited Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference. Li, Yin, Wang, Qian, Chen, Guo, Han (2015) made a research on Randomness determines practical security of BB84 quantum key distribution. Li, Chen, Pan, Sun, Li, Li (2016) implied Security analysis of BB84 protocol in the collective-rotation noise channe. Sun, Djordjevic, Neifeld (2016) [11] sketched Secret Key Rates and Optimization of BB84 and Decoy State Protocols Over Time-Varying Free-Space Optical Channels.

1.2 Organization of the Article

In section 2, it includes the secure model of Wireles Wires Sensor Network. Section 3 gives the introduction of security of the quantum protocol. Section 4 simply describes the designning of protocol. Section 5 is about the security analysis of the quantum communication protocol. And section 6 is the summary of the thesis.

2. The Secure Model of Wireles Wires Sensor Network

To consider classical registers as a special case of quantum registers is useful in a few situations. Denote by $\left|\hat{\mu}\right\rangle^{\mathrm{M}}$, $\hat{\mu}\in\hat{\mathrm{M}}$, the associated orthogonal states. H^{M} is used to denote the state space for the classical part. The initial random state is $\left|\hat{\mu}\right\rangle^{\mathrm{M}}\left|\Psi(\hat{\mu})\right\rangle$ with probability $\rho(\hat{\mu})$. And p is denoted the associated density matrix. The POVM that returns $(\hat{\mu},\hat{\lambda})$ is $\mathrm{E}_{\hat{\upsilon}}=\mathrm{P}_{\hat{\mu}}\mathrm{E}_{\hat{\lambda}|\hat{\mu}}$ where $\mathrm{P}_{\hat{\mu}}$ is the projection on the state $\left|\hat{\mu}\right\rangle^{\mathrm{M}}$. Before all, we have

$$\rho(\hat{\upsilon})=Tr(\mathrm{E}_{\hat{\upsilon}}p)=\rho(\hat{\mu})\left\langle\Psi(\hat{\mu})\right|\mathrm{E}_{\hat{\lambda}|\hat{\mu}}\left|\Psi(\hat{\mu})\right\rangle,$$

which is corresponding with (1). In the proof, the extended operator formalism will be only needed to use the simple rule $\mathrm{E}_{\upsilon}=\Sigma_{\upsilon|\kappa(\upsilon)=\kappa}\mathrm{E}_{\upsilon}$, which is valid for any deterministic function κ of $\upsilon=(\mu,\lambda)$. This rule will be used in a context where E_{υ} is not used to compute a probability. In such a context, without the extended operator formalism, it is hard to explain this rule, at least from the point of view of author.

Nevertheless, using the extended operator formalism at every step is not expected.

PROPOSITION 3. *Suppose* $\upsilon=(\mu,\lambda)$ *be a view on* $\hat{\upsilon}$ *that abides by C*1 *and C*2. *The POVM on* $\mathrm{H}^{Q}\otimes\mathrm{H}^{\mathrm{M}}$ *linked with* $\upsilon=(\mu,\lambda)$ *is* $\mathrm{E}_{\upsilon}=\mathrm{E}_{(\mu,\lambda)}=\mathrm{P}_{\mu|\lambda}\mathrm{E}_{\lambda|\mu}$ *where*

$$\mathrm{P}_{\mu|\lambda}=\sum_{\hat{\mu}|\mu(\hat{\mu},\hat{\lambda})=\mu}\mathrm{P}_{\hat{\mu}}$$

PROOF. Based on condition C1, there is

$$\begin{aligned}\mathrm{E}_{\upsilon}=\mathrm{E}_{(\mu,\lambda)}&=\sum_{\hat{\mu}|\mu(\hat{\mu},\hat{\lambda})=\mu}\sum_{\hat{\lambda}|\lambda(\hat{\mu},\hat{\lambda})=\lambda}\mathrm{P}_{\hat{\mu}}\mathrm{E}_{\hat{\lambda}|\hat{\mu}}\\&=\sum_{\hat{\mu}|\mu(\hat{\mu},\hat{\lambda})=\mu}\mathrm{P}_{\hat{\mu}}\sum_{\hat{\lambda}|\lambda(\hat{\mu},\hat{\lambda})=\lambda}\mathrm{E}_{\hat{\lambda}|\hat{\mu}}\end{aligned}$$

Based on condition C2, there is

$$\mathrm{E}_{\upsilon}=\sum_{\hat{\mu}|\mu(\hat{\mu},\hat{\lambda})=\mu}\mathrm{P}_{\hat{\mu}}\mathrm{E}_{\lambda|\mu}=\mathrm{P}_{\mu|\lambda}\mathrm{E}_{\lambda|\mu}.$$

This is the end of the proof.

Let M and M' be any two operators on H^{Q}. To make the next equation sufficiently general for the purpose, these operators are needed. In the proof, the following equation will be helpful to pass from the standard to the extended operator formalism.

$$\begin{aligned}Tr(\mathrm{E}_{\upsilon}MpM')&=Tr(\mathrm{P}_{\mu|\lambda}\mathrm{E}_{\lambda|\mu}MpM')\\&=\rho(\mu:\lambda)Tr_{Q}(\mathrm{E}_{\lambda|\mu}Mp_{\mu|\lambda}M')\quad(5)\end{aligned}$$

The second equality contains the main content of this rule, and the first equality is a direct result of Proposition 3. In the special case $M=M'=I_{\mathrm{E}}$, for $Tr(\mathrm{E}_{\upsilon}p)=\rho(\upsilon)$, in essence, the rule is Proposition 2. In Proposition 2, the condition $\mu(\hat{\mu},\lambda)=\mu$ restricts the sum over $\hat{\mu}$ in the definition of $p_{\mu|\lambda}$. This restriction is performed via the projection $\mathrm{P}_{\mu|\lambda}$ on p in the extended operator formalism, which is the basic point of formula (5). And the factor $\rho(\mu:\lambda)$ is added (in the nonextended formalism) to make good for the fact that $p_{\mu|\lambda}$ is normalized.

PROOF OF FORMULA (5). Note that $Tr=Tr_{Q}\,Tr_{\mathrm{M}}$, in other words, the trace operation Tr is equivalent to a partial trace over H^{M} followed by a trace over H^{Q}. The operators $\mathrm{E}_{\lambda|\mu}$, M and M' exchange with Tr_{M} and $\mathrm{P}_{\mu|\lambda}$ since the former operator on H^{Q} while the latter operate on H^{M}. Hence, acting on the left-hand-side, $\mathrm{P}_{\mu|\lambda}$ and Tr_{M} can be first performed. If p is expanded as a sum over $\hat{\mu}$, what can be obtained is that the restriction on $\hat{\mu}$ coming with the projection $\mathrm{P}_{\mu|\lambda}$ (the same restriction as in Proposition 2) followed by the partial trace Tr_{M} maps ρ into $\rho(\mu:\lambda)\ p_{\mu|\lambda}$. For the fact that $p_{\mu|\lambda}$ is renormalized, the factor $\rho(\mu:\lambda)$ being needed to make good. After taking $\rho(\mu:\lambda)$ in evidence, there leaves with the right-hand side.

3 Security of quantum protocol

Suppose that Alice transmits some classic binary string $\pi\in\{0,1\}^{N}$ to Bob over a channel, either quantum or classical. Let $\Omega\subseteq\{1\ldots N\}$ be any subset of the positions. In short, with the exception of a small probability of error, Ω is the set of positions $\imath$ where Bob's bit $\varepsilon[\imath]$ and Alice's bit $\pi[\imath]$ are presumed identical. In quantum protocols, there is a typical situation that Alice and Bob need to be indicated that the number of errors is small in some subset $\mathrm{E}\subseteq\Omega$ and yet they cannot perform a test on E for the bits in E must keep private. For solving this problem, they pick two random subsets T and E, so that the bits in T can be used for a test while at the same time the bits in E keep private. Every position $\imath\in\Omega$ is added either in T (initially empty) with probability ρ_{T}, or in E (initially empty) with probability ρ_{E}, or is ignored with probability $1-\rho_{\mathrm{T}}-\rho_{\mathrm{E}}$. (In the protocol, the case $\rho_{\mathrm{T}}+\rho_{\mathrm{E}}=1$ will be addressed, but here is a bit more general.)

LEMMA 2. Consider some positions Ω and a set of errors ζ on Ω. (In the above situation, the string e is $\pi[\Omega]\oplus\varepsilon[\Omega]$.) Suppose T and E be two random subsets of D, so that every position $\imath\in\Omega$ is in T with probability ρ_{T}

or in E with probability ρ_{E} or discarded with probability $1-\rho_{\mathrm{T}}-\rho_{\mathrm{E}}$. For $\mathrm{X}\in\{\mathrm{T},\mathrm{E}\}$, let η_{X} be the size of X and ϑ_{X} be the number of errors in X (the weight of $\zeta[\mathrm{X}]$). Using P_{T} to denote the event that $\vartheta_{\mathrm{T}} < j\rho_{\mathrm{T}}\eta_{\Omega}$ where is some fixed parameter that stands for the tolerated error rate. Using P_{E} to denote the event that $\vartheta_{\mathrm{E}} < (j+b)\rho_{\mathrm{T}}\eta_{\Omega}$ where b > 0 is any positive real number. There is

$P_{\mathrm{T}} \Rightarrow_{u} (b,\eta_{\Omega})P_{\mathrm{E}}$ (6)

where

$$\mathrm{u}(b,\eta_{\Omega}) = \exp\left(\frac{-b^2\min\{\rho_{\mathrm{T}}^2,\rho_{\mathrm{E}}^2\}}{2s+b}\eta_{\Omega}+\frac{2b^2\rho_{\mathrm{E}}^2}{(2j+b)^2}\right)$$

The term $2b^2\rho_{\mathrm{E}}^2/(2j+b)^2$ is seprated from η_{Ω}. When η_{Ω} is large, it can be ignored. As for the above situation, the fact that E and T are not distinguishable until after the transmission is only used in the the lemma. Apart from E and T, an upper bound $\mathrm{u}(b,\eta_{\Omega})$ on $\Pr(P_{\mathrm{T}}\wedge P_{\mathrm{E}})$ is provided for every variable fixed. And it still holds if averaging over the other variables. Excluding the situation that not averaging over η_{Ω}, for the upper bound $\mathrm{u}(b,\eta_{\Omega})$ itself depends on η_{Ω}. The following lemma, a variation on Chernoff's lemma, which is a standard tool to cope with large numbers (e.g., see Kearns [1989]), and is also the basic tool used to prove the fictive test lemma.

LEMMA 3 (CHERNOFF). *Let* $\mathrm{X}_1 \ldots \mathrm{X}_{\mathrm{n}}$ *be n independent Bernoulli variables and* $\mathrm{Z} = \Sigma_{i=1}^{n}\mathrm{X}_{\mathrm{i}}$ *respectively. If* $\Pr(\mathrm{X}_{\mathrm{i}}=1)=\rho$ *for* $1 \le i \le n$, *then for all* $0 \le \Delta\rho \le 1$, *there is*

$$\Pr(\mathrm{Z} \ge \mathrm{n}(\rho+\Delta\rho)) \le \exp(-2n(\Delta\rho)^2), \qquad (7)$$

$$\Pr(\mathrm{Z} \le \mathrm{n}(\rho-\Delta\rho)) \le \exp(-2n(\Delta\rho)^2). \qquad (8)$$

The following is the basic idea of the proof. ϑ_{Ω}, the number of errors in Ω, is either (1) larger or equal to $\lceil(\mathrm{j}+b/2)\eta_{\Omega}\rceil$ or (2) smaller or equal to $\lfloor(j+b/2)\eta_{\Omega}\rfloor$. The probability of P_{T} and the probability of P_{E} respectively in the first case and in the second case is small. In other words, the probability of $P_{\mathrm{T}}\wedge P_{\mathrm{E}}$ is small in both cases.

First, there comes the case where $\vartheta_{\Omega} \ge \lceil(\mathrm{j}+b/2)\eta_{\Omega}\rceil$. Only if ϑ_{T} which is the number of errors in T is strictly smaller than $j\rho_{\mathrm{T}}\eta_{\Omega}$ will the condition P_{T} hold. The above the probability of $\vartheta_{\mathrm{T}} \le j\rho_{\mathrm{T}}\eta_{\Omega}$ will be a constraint. Every $\iota \in \Omega$, especially every position ι with $\zeta[\iota]\neq 0$, belongs to T with probability ρ_{T}, which is to say, each of the $\vartheta_{\Omega} \ge (\mathrm{j}+b/2)\eta_{\Omega}$ errors is put in *T* with probability ρ_{T}. A conservative assumption can be made that $\vartheta_{\Omega} = \lceil(\mathrm{j}+b/2)\eta_{\Omega}\rceil$, since the probability will only be decreased by a larger value for ϑ_{Ω}. Suppose $\mathrm{Z} = \vartheta_{\mathrm{T}}$ be the number of errors in *T*. By using inequality (8), an upper bound on $\Pr(\vartheta_{\mathrm{T}} \le j\rho_{\mathrm{T}}\eta_{\Omega})$ can be obtained. Substitute η by ϑ_{Ω} and ρ by ρ_{T} in (8), a value for $\Delta\rho$ will be found. Hence, there is

$$j\rho_{\mathrm{T}}\eta_{\Omega} \le \vartheta_{\Omega}(\rho_{\mathrm{T}}-\Delta\rho), \qquad (9)$$

And in this way, $\vartheta_{\mathrm{T}} \le j\rho_{\mathrm{T}}\eta_{\Omega}$ implies $\vartheta_{\mathrm{T}} \le \vartheta_{\Omega}(\rho_{\mathrm{T}}-\Delta\rho)$. Besides, $\Pr(\vartheta_{\mathrm{T}} \le j\rho_{\mathrm{T}}\eta_{\Omega})$ can be restrained by (8). If $(\mathrm{j}+b/2)\eta_{\Omega} = j\rho_{\mathrm{T}}\eta_{\Omega}/(\rho_{\mathrm{T}}-\Delta\rho)$, (9) can be obtained for $(\mathrm{j}+b/2)\eta_{\Omega} \le \vartheta_{\Omega}$. $\Delta\rho = b\rho_{\mathrm{T}}/(2j+b)$ is the solution for $\Delta\rho$. These values applied with Chernoff's lemma can lead to that ρ_{T} is smaller than $j\rho_{\mathrm{T}}\eta_{\Omega}$ (and thus smaller than $\vartheta_{\Omega}(\rho_{\mathrm{T}}-\Delta\rho)$ with a probability smaller or equal to

$$\exp\left(\frac{-2b^2\rho_{\mathrm{E}}^2}{(2j+b)^2}\vartheta_{\Omega}\right)$$

Now, using the fact $(\mathrm{j}+b/2)\eta_{\Omega} \le \vartheta_{\Omega}$ can get

$$\Pr(\mathrm{P_T}) \le u_{\mathrm{T}}(b,\eta_{\Omega}) \overset{\text{def}}{=} \exp\left(\frac{-b^2\rho_{\mathrm{E}}^2}{2j+b}\eta_{\Omega}\right)$$

The second case $\vartheta_{\Omega} \le \lfloor(j+b/2)\eta_{\Omega}\rfloor$ is similar to the first case. The difference is that inequality (7) is used instead of inequality (8) and $\rho=\rho_{\mathrm{E}}$ is used instead of $\rho=\rho_{\mathrm{T}}$. When ϑ_{E} which is the number of errors in *E* is larger than $(\mathrm{j}+b)\rho_{\mathrm{E}}\eta_{\Omega}$, the event P_{E} occurs. Even if ϑ_{Ω} which is the total number of errors in *D* is smaller than $\lfloor(j+b/2)\eta_{\Omega}\rfloor$, $\vartheta_{\Omega} = \lfloor(j+b/2)\eta_{\Omega}\rfloor$ can be assumed. Now, $\Delta\rho$ is found, so that $\vartheta_{\Omega}(\rho_{\mathrm{E}}+\Delta\rho) \le (\mathrm{j}+b)\rho_{\mathrm{E}}\eta_{\Omega}$ can be obtained. Since $\vartheta_{\Omega} \le (\mathrm{j}+b/2)\eta_{\Omega}$, if $(\mathrm{j}+b/2)\eta_{\Omega} = (\mathrm{j}+b)\rho_{\mathrm{E}}\eta_{\Omega}/(\rho_{\mathrm{E}}+\Delta\rho)$, the seeked inequality can be got. This equation has the solution $\Delta\rho = b\rho_{\mathrm{E}}/(2j+b)$ like in the first case. By using (7), ϑ_{T} which can be got is larger than $(\mathrm{j}+b)\rho_{\mathrm{T}}\eta_{\Omega}$ (and thus larger than $\vartheta_{\Omega}(\rho_{\mathrm{E}}+\Delta\rho)$) with a probability smaller or equal to

$$\exp\left(\frac{-2b^2\rho_{\mathrm{E}}^2}{(2j+b)^2}\vartheta_\Omega\right)$$

Here, unlike the first case, $(\mathrm{j}+b/2)\eta_\Omega = \eta_\Omega$ doesn't exist. $(\mathrm{j}+b/2)\eta_\Omega - 1 \le \eta_\Omega$ is the only inequality existing. Do as in the first case, apart from an additional positive term $\frac{-2b^2\rho_{\mathrm{E}}^2}{(2j+b)^2}$ in the exponent. Thus, there is

$$\Pr(\overline{P}_{\mathrm{E}}) \le u_{\mathrm{E}}(b,\eta_\Omega) \stackrel{\mathrm{def}}{=} \exp\left(\frac{-b^2\rho_{\mathrm{E}}^2}{2j+b}\eta_\Omega + \frac{2b^2\rho_{\mathrm{E}}^2}{(2j+b)^2}\right)$$

Then,

$$\Pr(P_{\mathrm{T}} \wedge \overline{P}_{\mathrm{E}}) \le u(b,\eta_\Omega) = \max\{u_{\mathrm{T}}(b,\eta_\Omega), u_{\mathrm{E}}(b,\eta_\Omega)\}$$

This is the end of the proof.

4. Designing of Communication Protocol

4.1 The BB84 Protocol

On the well known protocol proposed by Bennett and Brassard [1984] (see also Bennett *et al*. [1992]), the protocol analyzed is a variation.

Step 1. *Alice's Preparation*. Bob was sent *N* two dimensional quantum systems from Alice to prepare individually in one of the four states in BB84 picked at accident. For concreteness, the BB84 states denoted by $\Psi(0,+)$, $\Psi(1,+)$, $\Psi(0,\times)$ and $\Psi(1,\times)$ are equivalent to photons polarized at 0, 90, 45, and -45 degrees respectively. Of course, if Alice uses any other realization of the BB84 states, the proof remains the same. The state of the photons prepared by Alice is $\Psi(\pi,\alpha) \stackrel{def}{=} \Psi(\pi[1],\alpha[1]) \otimes \cdots \otimes \Psi(\pi[N],\alpha[N])$. The state $|\Psi(a,e)\rangle$ is a state for the photons in *E* that encodes the bits $a[\imath]$ in the bases $e[\imath]$ for each $\imath \in \mathrm{E}$, for any string of bits $a \in \{0,1\}^{\mathrm{E}}$ and string of bases $e \in \{+,\times\}^{\mathrm{E}}$ (see Appendix M).

Step 2. *Bob's Measurement*. Bob uses either the rectilinear basis $\{\Psi(0,+), \Psi(1,+)\}$ or the diagonal basis $\{\Psi(0,\times), \Psi(1,\times)\}$ chosen at random to measure each photon. If both the conditions that Bob detects a photon at position $\imath$ and the associated outcome as $\perp$ are met, then $\imath$ is said to be a detected position. The following notations are adopted:

— $\alpha \in \{+,\times\}^N$: Alice's string of bases.

— $\pi \in \{0,1\}^N$: Alice's string of bits.

— $\beta \in \{+,\times\}^N$: Bob's string of bases.

— D: the set of detected positions, that is, the set of positions $\imath$ with $\varepsilon[\imath] \neq \perp$.

— $\varepsilon \in \{0,1,\perp\}^N$: Bob's string of outcomes.

Step 3. *Choosing the Tested Bits*. A subset of positions $\delta \subseteq \{1 \ldots N\}$ is picked at random by Bob: every position $\imath$ is put in the set δ (initially empty) with probability ρ_{T}.

Some notations. The set of positions $\imath$ where $\alpha[\imath] = \beta[\imath]$ is denoted by $A \subset D$. Generally, for every $\imath \in A$, there is $\pi[\imath] = \varepsilon[\imath]$ except for errors in the transmission. We denote by $\mathrm{T} = \delta \cap A = \{\imath \in \delta \mid \alpha[\imath] = \beta[\imath]\}$ the set of tested positions.

Step 4. *Counting the Errors*. δ and β are announced by Bob; α and $\pi[\delta]$ are announced by Alice; and $\varepsilon[\delta]$ is announced by Bob. The value $\vartheta_{\mathrm{T}} = \vartheta_{\mathrm{T}}(\pi,\varepsilon)$ and the Hamming distance between π and ε on T are noted by Alice and Bob.

Remark. In validation constraints, the value ϑ_{T} will be used for error-correction.

Step 5. *Error Correction*. The positions in *R* are discarded. To define the key, the set $\mathrm{E} = A - \delta = \{\imath \notin \delta \mid \alpha[\imath] = \beta[\imath]\}$ will be used. Let $\eta_{\mathrm{E}} = |\mathrm{E}|$. Alice and Bob should share the string $\pi[\mathrm{E}]$ which is called the raw key, if no error occurred. Alice calculates and announces the *syndrome* $\sigma = \mathrm{Y} \bullet \pi[\mathrm{E}]$ to Bob for error correction, in which Y is a $\theta \times \eta_{\mathrm{E}}$ parity check matrix, and "$\bullet$" is the binary matrix multiplication modulo 2 (see also Appendix M). θ, *the* redundant bits about the raw key $\pi[\mathrm{E}]$ is contained in the syndrome σ. The value θ relies on ϑ_{T} (see the validation constraints). By using this information, Bob corrects the errors in $\varepsilon[\mathrm{E}]$ and obtains the raw key $\pi[\mathrm{E}]$. In the next part, more about error correction is provided.

Step 6. *Key Extraction*. Alice and Bob share the string $\pi[\mathrm{E}]$ which is called the raw key at this point. After error correction, Alice uses a $\cdots$ binary matrix K to define a (final) key. The value of *m* will depend on ϑ_{T}. The key $\hat{\varpi} = \mathrm{K} \bullet \pi[\mathrm{E}]$ is computed by Alice and Bob. At this stage, the protocol comes to an end in practice.

The key $\hat{\varpi} = \mathrm{K} \bullet \pi[\mathrm{E}]$, which attracts the interest of Eve, is a function of the string π chosen by Alice. An interactive reconciliation procedure in which the parity check matrix Y is a function of the error positions is performed by Alice and Bob in another variation. The number of redundant bits needed in practice can certainly be reduced by such an approach where the matrix Y depends on the error positions. Nevertheless, the privacy proof is made more complicated.

4.2 Mutual Information

In terms of *Mutual information* or *Shannon's entropy*, privacy is often expressed often. In one small subsection, it is impossible to do justice the concepts of mutual information and Shannon's entropy. Here listed some simple formulas. Let X, Θ, and Λ be any three random variables. Let $\rho(\chi,\gamma)=\Pr(\mathrm{X}=\chi\wedge\Theta=\gamma)$, $\rho(\chi)=\Pr(\mathrm{X}=\chi)$, $\rho(\gamma)=\Pr(\Theta=\gamma)$, $\rho(\chi\mid\gamma)=\Pr(\mathrm{X}=\chi\mid\Theta=\gamma)$, $\rho(\chi,\gamma,\kappa)=\Pr(\mathrm{X}=\chi\wedge\Theta=\gamma,\wedge\Lambda=\kappa)$ etc.

Definition 7. The mutual information between X and Θ is given by

$$\sum_{\chi,\gamma}\rho(\chi,\gamma)\log_2\left(\frac{\rho(\chi,\gamma)}{\rho(\chi)\rho(\gamma)}\right)=\mathrm{I}(\mathrm{X};\Theta)$$

Definition 8. The Shannon entropy of X is given by

$$\mathrm{H}(\mathrm{X})=\mathrm{I}(\mathrm{X};\mathrm{X})=-\sum_{\chi}\rho(\chi)\log_2\rho(\chi).$$

Definition 9. The conditional Shannon entropy of X given Θ is given by

$$\mathrm{H}(\mathrm{X}\mid\Theta)=-\sum_{\chi,\gamma}\rho(\chi,\gamma)\log_2\rho(\chi\mid\gamma).$$

In the following, $\mathrm{I}(\mathrm{X};\Theta)=\mathrm{H}(\mathrm{X})-\mathrm{H}(\mathrm{X}\mid\Theta)$ can be easily verified:

Note that $\mathrm{I}(\mathrm{X};\Theta)$ is the expected value of $\log_2(\rho(\chi,\gamma)/\rho(\chi)\rho(\gamma))$:

$$\mathrm{E}\left(\log_2\left(\frac{\rho(\chi,\gamma)}{\rho(\chi)\rho(\gamma)}\right)\right)=\mathrm{I}(\mathrm{X};\Theta)$$

Similarly, there is

$$\mathrm{H}(\mathrm{X})=\mathrm{E}(-\log_2\rho(\chi)) \quad \text{and}$$
$$\mathrm{H}(\mathrm{X}\mid\Theta)=\mathrm{E}(-\log_2\rho(\chi\mid\gamma)).$$

Thus, one obtains

$$\begin{aligned}\mathrm{H}(\mathrm{X})-\mathrm{H}(\mathrm{X}\mid\Theta)&=\mathrm{E}(-\log_2\rho(\chi))-\mathrm{E}(-\log_2\rho(\chi\mid\gamma))\\&=\mathrm{E}(-\log_2\rho(\chi)+\log_2\rho(\chi\mid\gamma))\\&=\mathrm{E}\left(\log_2\left(\frac{\rho(\chi,\gamma)}{\rho(\chi)\rho(\gamma)}\right)\right)=\mathrm{I}(\mathrm{X};\Theta)\end{aligned}$$

By symmetry one has also $\mathrm{I}(\mathrm{X};\Theta)=\mathrm{H}(\mathrm{X})-\mathrm{H}(\mathrm{X}\mid\Theta)$.

Definition 10. The conditional mutual information between X and Θ given an event ϕ is

$$\sum_{\chi,\gamma,\kappa}\rho(\chi,\gamma\mid\phi)\log_2\left(\frac{\rho(\chi,\gamma\mid\phi)}{\rho(\chi\mid\phi)\rho(\gamma\mid\phi)}\right)=\mathrm{I}(\mathrm{X};\Theta\mid\phi)$$

Definition 11. The conditional mutual information between X and Θ given Λ *is*

$$\begin{aligned}\sum_{\chi,\gamma,\kappa}\rho(\chi,\gamma\mid\kappa)\log_2\left(\frac{\rho(\chi,\gamma\mid\kappa)}{\rho(\chi\mid\kappa)\rho(\gamma\mid\kappa)}\right)&\overset{\text{def}}{=}\mathrm{I}(\mathrm{X};\Theta\mid\Lambda)\\&=\sum_{\kappa}\rho(\kappa)\mathrm{I}(\mathrm{X};\Theta\mid\Lambda=\kappa).\end{aligned}$$

One can verify that

$$\mathrm{I}(\mathrm{X};\Lambda)+\mathrm{I}(\mathrm{X};\Theta\mid\Lambda)=\mathrm{I}(\mathrm{X};\Theta,\Lambda) \qquad (11)$$

Many other formulas of the same kind can be obtained. For instance,

$$\mathrm{I}(\mathrm{X};\Theta\mid\Lambda)+\mathrm{I}(\mathrm{X};\Lambda)+\mathrm{I}(\Theta;\Lambda)-\mathrm{I}(\mathrm{X},\Theta;\Lambda)=\mathrm{I}(\mathrm{X};\Theta).$$

For

$$\frac{\rho(\chi,\gamma\mid\kappa)}{\rho(\chi\mid\kappa)\rho(\gamma\mid\kappa)}\times\frac{\rho(\chi,\kappa)}{\rho(\chi)\rho(\kappa)}\times\frac{\rho(\gamma,\kappa)}{\rho(\gamma)\rho(\kappa)}\times\frac{\rho(\chi,\gamma)\rho(\kappa)}{\rho(\chi,\gamma,\kappa)}=\frac{\rho(\chi,\gamma)}{\rho(\chi)\rho(\gamma)}.$$

5. Security Analysis of Quantum Communication Protocol

Originally, the basic mechanisms of Section 3 are applied to the modified protocol in this section. Then, basic formula that will be useful later in the proof will be provided. Assume that H^{A} is Alice's original system. By and large, Eve–Bob is free to use an extra system $\mathrm{H}^{B}=\mathrm{H}^{\mathrm{E}}$ when s/he receives control over H^{A}. Without loss of generality, the extra system $\mathrm{H}^{B}=\mathrm{H}^{\mathrm{E}}$ is not needed. For that the POVM formalism has already been used to describe Eve– Bob's measurement. Besides, in the POVM formalism, this extra system is implicit.

$\hat{\lambda}=(D,\varepsilon,o)$ is the overall measurement outcome. There is $\hat{c}=(\tilde{b},a,R,g,\hat{K})$, in which $\hat{K}$ stands for the random bits that will be used to generate *K* (and possibly *F* if a random error-correcting code is used). The string β is a function of δ and $\tilde{\beta}$. $\hat{\mu}=(\tilde{\beta},\alpha,\delta,\mathrm{E},\pi[\mathrm{E}],\mathrm{K},\mathrm{Y},\sigma)$ is the string of classical announcements received by Eve–Bob. $\lambda=\hat{\lambda}=(D,\varepsilon,o)$ is Eve–Bob's quantum outcome, in which ε represents the outcome of the measurement performed by Eve–Bob on H^{A} to pass the test, and o is the measurement performed by Eve–Bob on the residual system after the first measurement. $\upsilon=(\mu,\lambda)$ is Eve–Bob's view.

It's obivious that *v* abides by conditions C1 and C2. Without loss of generality, consider conservatively that the operator $\mathrm{E}_{\lambda|\mu}$ on H^{A} has rank one that is, $\mathrm{E}_{\lambda|\mu}=\left|G_{\mu,\lambda}\right\rangle\left\langle G_{\mu,\lambda}\right|$ for

some nonnormalized state $\left|G_{\mu,\lambda}\right\rangle$. The initial random state is $\left|\hat{\mu}\right\rangle^{\mathrm{M}}\left|\Psi(\pi,\alpha)\right\rangle$ with probability $\rho(\hat{\mu})$ (which probability will not need to compute). Denote by ρ the corresponding density matrix. There is $\mathrm{E}_{\upsilon} = \mathrm{P}_{\mu|\lambda}\ \mathrm{E}_{\lambda|\mu}$. Denote by the trace over H.

The first basic formula is for $\rho(\upsilon)$. According to Proposition 2, there is

$$\rho(\upsilon) = \rho(\mu:\lambda)\ Tr_A(^{\mathrm{E}_{\lambda|\mu}}\ p_{\mu|\lambda}). \qquad (14)$$

Calculate $p_{\mu|\lambda}$ as explained in Section 3 (see remark after Proposition 2). When $\left|\Psi(\hat{\mu})\right\rangle$ is prepared uniformly at random and the states with $\mu_\lambda = \mu$ is only kept, the density matrix $\rho_{\mu|\lambda}$ is obtained. Recall that $\mu_\lambda \overset{def}{=} \mu(\hat{\mu},\lambda)$. Consider $\hat{\mu}$ as the outcome of a random experiment, on which the random variable μ_λ (with parameter λ) is defined. In the protocol, there is $\Psi(\hat{\mu}) = \Psi(\pi,\alpha)$. Besides, for given μ and λ, that the constraint $\mu_\lambda =$ $\mu = (\tilde{\beta},\alpha,\delta..\sigma)$ on (π,α) corresponds to the three constraints **a** = α, $\pi[\overline{\mathrm{E}}] = \pi[\overline{\mathrm{E}}]$ and $\mathrm{Y}\bullet\pi[\mathrm{E}]$ = *s* can be checkd, in which $\overline{\mathrm{E}}$ = {, 1, . . ., *N* } $-\mathrm{E}$. Note that, the set E and the matrix Y are uniquely determined for given μ and λ, so that E and Y can be interpreted as in the above constraints. Let

$$\mathrm{M}_\sigma = \{a \in \{0,1\}^{\mathrm{E}} \mid \mathrm{Y}\bullet\alpha = \sigma\}$$

There is that $p_{\mu|\lambda}$ is the product $\left|\Psi_{\overline{\mathrm{E}}}\right\rangle\left\langle\Psi_{\overline{\mathrm{E}}}\right| \otimes \tilde{p}_\sigma$, in which

$$\left|\Psi_{\overline{\mathrm{E}}}\right\rangle = \left|\Psi(\pi[\overline{\mathrm{E}}],\alpha[\overline{\mathrm{E}}])\right\rangle \quad (15)$$

is the pure state for the photons in $\overline{\mathrm{E}}$ = {, 1, . . ., *N* } $-\mathrm{E}$. And $\tilde{p}_\sigma$ are equivalent to a uniform distribution over the states $\left|\Psi(a,\alpha[\overline{\mathrm{E}}])\right\rangle$ with $a \in \mathrm{M}_\sigma$.

$$\tilde{p}_\sigma = \left|\mathrm{M}_\sigma\right|^{-1} \sum_{a\in C_\sigma} \left|\Psi(a,\alpha[\overline{\mathrm{E}}])\right\rangle\left\langle\Psi(a,\alpha[\overline{\mathrm{E}}])\right| \quad (16)$$

The state

$$\tilde{G}_{\mu,\lambda} = \underbrace{\left\langle\Psi_{\overline{\mathrm{E}}}\right|}_{On\overline{E}}\ \underbrace{G_{\mu,\lambda}}_{On\{1,\ldots,N\}} \quad (17)$$

naturally appears in the computation of $\rho(\upsilon)$ for $p_{\mu|\lambda}$ is equivalent to the pure state $\Psi_{\overline{\mathrm{E}}}$ on $\overline{\mathrm{E}}$. Recall $\mathrm{E}_{\lambda|\mu} = \left|G_{\mu,\lambda}\right\rangle\left\langle G_{\mu,\lambda}\right|$. The component in $\overline{\mathrm{E}}$ of $G_{\mu,\lambda}$ is used in the inner product with $\Psi_{\overline{\mathrm{E}}}$, so that $\tilde{G}_{\mu,\lambda}$ is the residual state for the photons in E (see Section 3.3). There is

$$\begin{aligned} Tr_A(\mathrm{E}_{\lambda|\mu}\ \rho_{\mu|\lambda}) &= \left\langle G_{\mu,\lambda}\right|\ p_{\mu|\lambda}\left|G_{\mu,\lambda}\right\rangle \\ &= \underbrace{\left\langle\tilde{G}_{\mu,\lambda}\right|\tilde{p}_\sigma\left|\tilde{G}_{\mu,\lambda}\right\rangle}_{On\overline{E}} \quad (18) \end{aligned}$$

By using (14) and (18), there is

$$\rho(\upsilon) = \rho(\mu:\lambda)\left\langle\tilde{G}_{\mu,\lambda}\right|\tilde{p}_\sigma\left|\tilde{G}_{\mu,\lambda}\right\rangle \quad (19)$$

Now prove the generalization of (18). Assume M and M' be any two operators on the state space. The generalization of (18) is

$$Tr_{\mathrm{A}}(\mathrm{E}_{\lambda|\mu}\ p_{\mu|\lambda}\ M') = \left\langle\tilde{G}_{\mu,\lambda}\right|M\tilde{p}_\sigma M'\left|\tilde{G}_{\mu,\lambda}\right\rangle. \qquad (20)$$

Recall that $p_{\mu|\lambda}$ is equavilent to the pure state $\Psi_{\overline{\mathrm{E}}}$ on $\overline{\mathrm{E}}$ (and to $\tilde{p}_\sigma$ on E) and $\mathrm{E}_{\lambda|\mu} = \left|G_{\mu,\lambda}\right\rangle\left\langle G_{\mu,\lambda}\right|$. Likewise, M and M' are only defined on E by hypothesis. Hence, the residual state $\tilde{G}_{\mu,\lambda}$ on E will be returned by the inner product between $\Psi_{\overline{\mathrm{E}}}$ and $G_{\mu,\lambda}$ as in (19). Therefore, (20) is obtained.

By using the same technique, it is easy to calculate $\rho(\varpi,\upsilon)$. That *k* is added to the view is the only difference. It is as if the new syndrome was (σ,ϖ) rather than *s* only. There is

$$\rho(\varpi,\upsilon) = \rho(\mu,\varpi:\lambda)\left\langle\tilde{G}_{\mu,\lambda}\right|\tilde{p}_{\sigma,\varpi}\left|\tilde{G}_{\mu,\lambda}\right\rangle. \qquad (21)$$

$\tilde{p}_\sigma$ is used to define the normalized density matrix $\tilde{p}_{\sigma,\varpi}$ via (16). Except that

$$\mathrm{M}_{\sigma,\varpi} = \{a \in \{0,1\}^{\mathrm{E}} \mid \mathrm{T}\bullet\alpha = \sigma \wedge \mathrm{K}\bullet a = \sigma\}$$

is used instead of M_σ. $\rho(\mu,\varpi:\lambda)$ in (21) is the probability that $(\mu,\varpi)_\lambda = (\mu,\varpi)$, in which $(\mu,\varpi)_\lambda$ is a function of $\hat{\mu}$. $\hat{\mu}$ is defined in the protocol when $\lambda = (D,\varepsilon,o)$ is fixed, in the light of Section 3 (see remark after Proposition 2). Seeing from the point of view that $(\mu,\varpi)_\lambda$ is a random variable defined on $\hat{\mu}$. For a given λ, the value of this random variable can be gotten by first obtaining $\mu = \mu(\hat{\mu},\lambda)$ and then ϖ using $\varpi = \mathrm{K}\bullet\pi[\mathrm{E}]$,. By

definition, $\rho(\mu:\lambda)$ is the probability of obtaining μ in this computation. $2^{-\varsigma}$ is the probability of every ϖ independently of the view $\upsilon=(\mu,\lambda)$. Thus, there is

$$\rho(\mu,\varpi:\lambda) = 2^{-\varsigma}\ \rho(\mu:\lambda) \quad (22)$$

6. Conclusion

Here, we made these experiments in order to verify its security from the environment, the privacy protection and the appcation of the quantum protocol and we find it is safe for us to use it. And we discuss the problem of designing and modifying the protocol. At this time, we do some analysis to prove the improved and the security of the protocol. Although the analysis is successful, but it is not so prefect like the analysis, it has not been made real experiment for the modified protocol, it need to be tested in actual work. In further research, we will do more works and try our best to modidy the protocol and do better security in the protocol.

7. Acknowledgments

This research was supported by the National Natural Science Foundation of China (No. 71471102), and Yichang University Applied Basic Research Project in China (Grant No. A17-302-a13).

8. References

1. Wallenius J, Dyer JS, Fishburn PC, Steuer RE, Zionts S, Deb K, *et al*. Multiple criteria decision making, multiattribute utility theory: recent accomplishments and what lies ahead [J], Management Science, 2008; 54(7):1336-1349.
2. Fan J, Hu YD, Luan TH, Dong MX. DisLoc: A Convex Partitioning Based Approach for Distributed 3-D Localization in Wireless Sensor Networks [J], Ieee Sensors Journal, 2017; 17(24):8412-8423.
3. Sasaki S, Miyaji Y, Uehara H. Energy Budget Formulation in Progress-Based Nearest Forwarding Routing Policy for Energy-Efficient Wireless Sensor Networks [J], Ieice Transactions on Information and systems, E100D 2017; (12):2808-2817.
4. Rajeswari K, Bhagyaveni MA. MAP Based V-BLAST Transmission to Improve Network Lifetime in Virtual MIMO Based Wireless Sensor Networks [J], National academy science letters-India. 2017; 40(6):409-414.
5. Omairi A, Ismail ZH, Danapalasingam KA, Ibrahim M. Power Harvesting in Wireless Sensor Networks and Its Adaptation With Maximum Power Point Tracking: Current Technology and Future Directions [J], Ieee Internet of things journal. 2017; 4(6):2104-2115.
6. Yu S, Zhang BX, Yao Z, Li C. R3: A Lightweight Reactive Ring based Routing Protocol for Wireless Sensor Networks with Mobile Sinks [J], KSII Transactions on internet and information systems. 2016; 10(12):5442-5463.
7. Mehmood A, Lloret J, Sendra S. A secure and low-energy zone-based wireless sensor networks routing protocol for pollution monitoring [J], wireless communications & mobile computing. 2016; 16(17):2869-2883.
8. Mou JP, Wang J. Reference State Tracking in Distributed Leader-Following Wireless Sensor Networks with Limited Errors [J], journal of communications and networks. 2015; 17(6):602-608.
9. Kim MK. Two-Stage Model for Security Network-Constrained Market Auction in Pool-Based Electricity Market [J], journal of electrical engineering & technology. 2017; 12(6):2196-2207.
10. Shin S, Wang HP, Gu GF. A First Step Toward Network Security Virtualization: From Concept To Prototype [J], ieee transactions on information forensics and security. 2015; 10(10):2236-2249.
11. Sun XL, Djordjevic IB, Neifeld MA. Secret Key Rates and Optimization of BB84 and Decoy State Protocols Over Time-Varying Free-Space Optical Channels [J], ieee photonics journal, 2016; 8(3).
12. Xiang Y, Al-Dubi A, Liu L, Chu XW. Frontier technologies of trust computing and network security [J], concurrency and computation-practice & experience. 2015; 27(12):2907-2909.
13. Kohira S, Mitsuhashi K, Yahiro S, Ikeda S. Solution for Virtualization to Ensure Optimal Network Security Environment [J], fujitsu scientific & technical journal. 2016; 52(2):35-40.
14. Wang X, Shi WQ, Xiang Y, Li J. Efficient Network Security Policy Enforcement With Policy Space Analysis [J], ieee-acm transactions on networking. 2016; 24(5):2958-2970.
15. Pearce C, Zeadally S. Ancillary Impacts of Multipath TCP on Current and Future Network Security [J], ieee internet computing. 2015; 19(5):58-65.
16. Wang B, Xu J, Song HB. Research on the improved algorithm for image quantum encryption in multimedia networks [J], computers & electrical engineering, 2017; 62:414-428.
17. Shi RH. Verifiable Quantum Encryption and its Practical Applications [J], international journal of theoretical physics. 2017; 56(4):1208-1217.
18. Wang YQ, She K, Huang RF, Ouyang Z. Optimal Symmetric Ternary Quantum Encryption Schemes [J], international journal of theoretical physics. 2016; 55(11):4709-4722.
19. Anonymous. Ottawa displays high-dimensional quantum encryption [J], photonics spectra. 2017; 51(11):20-20.
20. Anonymous. Optical signals measured from space could enable quantum encryption network [J], photonics spectra. 2017; 51(10):33-33.
21. Smith E. quantum leap quantum encryption [j], journal of the institute of telecommunications professionals. 2016; 10:15-20.
22. Shenoy HA, Aravinda S, Srikanth R, Home D. Can the use of the Leggett-Garg inequality enhance security of the

BB84 protocol? [J], Physics Letters A. 2017; 381(31):2478-2482.
23. Khokhlov DL. Scheme of the arrangement for attack on the protocol BB84 [J], Optik. 2016; 127(18):7083-7087.
24. Zhao N, Zhu CH, Quan DX. A Novel Basis Splitting Eavesdropping Scheme in Quantum Cryptography Based on the BB84 Protocol [J], chinese physics letters, 2015; 32(8).
25. Gleim AV, Egorov VI, Nazarov YV, Smirnov SV, Chistyakov VV, Bannik OI, *et al*. Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference [J], Optics Express. 2016; 24(3):2619-2633.
26. Li HW, Yin ZQ, Wang S, Qian YJ, Chen W, Guo GC, Han ZF. Randomness determines practical security of BB84 quantum key distribution [J], Scientific Reports, 5() 2015.
27. Li J, Chen YH, Pan ZS, Sun FQ, Li N, Li LL. Security analysis of BB84 protocol in the collective-rotation noise channel [J], acta physica sinica, 2016; 65(3).