Providing Adaptive Quality of Security in Quantum Networks

Baokang Zhao, Ziling Wei, Bo Liu, Jinshu Su
School of Computer
National University of Defense Technology
Changsha, Hunan, CHINA
bkzhao@nudt.edu.cn, {wziling1017, liub0yayu }@gmail.com, sjs@nudt.edu.cn

Ilsun You
School of Information Science
Korean Bible University
Seoul, Korea
isyou@bible.ac.kr

***Abstract*—Recently, several Quantum Key Distribution (QKD) networks, such as Tokyo QKD, SECOQC, have been built to evaluate the quantum based OTP(One Time Pad) secure communication. As an ideal unconditional secure technique, OTP requires the key rate the same as the information rate. However, comparing with high speed information traffic (Gbps), the key generation rate of QKD is very poor(Kbps). Therefore, in practical QKD networks, it is difficult to support numerous applications and multiple users simultaneously. To address this issue, we argue that it is more practical to provide quality of security instead of OTP in quantum networks. We further propose ASM, an Adaptive Security Selection Mechanism for quantum networks based on the Analytic Hierarchy Process (AHP). In ASM, services can select an appropriate encryption algorithm that satisfies the proper security level and performance metrics under the limit of the key generation rate. We also implement ASM under our RT-QKD platform, and evaluate its performance. Experimental results demonstrate that ASM can select the optimal algorithm to meet the requirement of security and performance under an acceptable cost.**

Keywords- Quantum Key Distribution; Quality of security; Analytic Hierarchy Process

I. INTRODUCTION

Quantum Key Distribution (QKD) technology [1], based on fundamental principles of quantum physics, can generate unconditional security keys between two communication parties. Information theoretically secure cipher communication can be achieved when the obtained key is used with one-time-pad encryption method [2]. In recent years, the practical QKD is rapidly developed and high speed system has been approached with about hundreds of kbps security key rate [3]. In 2009, the first live demonstration of a working QKD network took place in Vienna with several kbps security key rate [4]. In 2010, Tokyo QKD network has been approached with about 100 kbps key rate in one single optical link [5]. In January 2013, we constructed our first real-time QKD system, RT-QKD, and developed several quantum secure applications, including a quantum secure phone: Qphone [6].

During our developing of quantum security based application, we found there is a significant rate gap between the information rate and quantum key generation rate, i.e., the information rate has nearly 400Gbps for single fiber, yet the quantum key generation key of a single fiber is nearly 100kbps. Though the QKD system has been improved rapidly, the key generation rate is still limited with the performance of the quantum communication devices. However, regarding real applications, the bandwidth requirements are high. For instance, a real time high definition video conference needs more than 400 kbps.

To address this problem, we argue that it is more practical to provide quality of security for different kind of applications. Quality of Security (QoS) means satisfying the various security demands with limited security key source. In QoS enabled QKD networks, the QKD generated key can be used for many cryptographic algorithms, such as OTP, AES, RSA, etc. Moreover, these keys can be further used in VANET [21], cloud computing[22], signature [23], secure network[24], disk encryption[25], etc. Security is provided as services with different levels, i.e., OTP can be regarded as highest security level. Based on the requirement of user applications, the QKD network provides the appropriate encryption algorithm for different applications and users.

In this paper, we propose ASM, An adaptive Security Mechanism Selection in Quantum Communication system, which can satisfy the requirement of applications under given the key source. We use the Analytic Hierarchy Process (AHP) to solve the problem. In this work, we also implement ASM under the RT-QKD platform and estimate ASM in this paper. Our estimations demonstrate that our solution can select the optimal algorithm under an acceptable cost.

The rest of the paper is organized as follows. In section II, we briefly introduce the Analytic Hierarchy Process (AHP). In section III, the proposed ASM approach is proposed. Next, we evaluate the functional and performance of our solution in section IV. Finally, we draw the conclusion in section V.

II. ANALYTIC HIERARCHY PROCESS

The AHP is a structured technique for organizing and analyzing complex decisions. Based on mathematics and psychology, it was developed by Thomas L. Saaty in the 1970s and has been extensively studied and refined since then [6].

It has particular application in group decision making, and is used around the world in a wide variety of decision situations,

QSHINE 2015, August 19-20, Taipei, Taiwan

DOI 10.4108/eai.19-8-2015.2260982

in fields such as government, business, industry, healthcare, and education. Rather than prescribing a "correct" decision, the AHP helps decision makers find one that best suits their goal and their understanding of the problem. It provides a comprehensive and rational framework for structuring a decision problem, for representing and quantifying its elements, for relating those elements to overall goals, and for evaluating alternative solutions.

The procedure of AHP for decision making can be divided into four parts [7] [8].

- Users of the AHP first decompose their decision problem into a hierarchy of more easily comprehended sub-problems, each of which can be analyzed independently. The elements of the hierarchy can relate to any aspect of the decision problem.
- Once the hierarchy is built, the decision makers systematically evaluate its various elements by comparing them to one another two at a time, with respect to their impact on an element above them in the hierarchy. In making the comparisons, the decision makers can use concrete data about the elements, but they typically use their judgments about the elements' relative meaning and importance. It is the essence of the AHP that human judgments, and not just the underlying information, can be used in performing the evaluations.
- The AHP converts these evaluations to numerical values that can be processed and compared over the entire range of the problem. A numerical weight or priority is derived for each element of the hierarchy, allowing diverse and often incommensurable elements to be compared to one another in a rational and consistent way. This capability distinguishes the AHP from other decision making techniques.
- In the final step of the process, numerical priorities are calculated for each of the decision alternatives. These numbers represent the alternatives' relative ability to achieve the decision goal, so they allow a straightforward consideration of the various courses of action.

III. THE PROPOSED SOLUTION DESIGN

In this section, we show the design of ASM. In ASM, it can select an appropriate encryption algorithm that satisfies the user’s requirement and the limit of the key generation rate, based on the AHP. There are five steps in ASM.

A. *Selecting the available encryption algorithms.*

The first step is selecting the available encryption algorithms. The principle of selecting is based on the key generation rate. If the key can satisfy the algorithm’s demand, we consider the algorithm is an available algorithm. In order to select the available algorithms, we introduce the mainstream encryption algorithms. The mainstream encryption algorithms contain DES, 3DES, AES, RSA, ECC and OTP. We compare these algorithms and get the result which is shown in Table 1. In Table 1, we process the time, security and resource cost by classification based on the features of each algorithm. For example, the higher layer of the speed; the lower cost of encryption time. Therefore, if the size of data is too large, OTP cannot consider an available encryption algorithm.

TABLE 1 THE MAINSTREAMS ALGORITHMS

Name	Key length (bits)	Speed	Security	Resource Cost
DES [9]	56	7	1	3
3DES [9]	118,168	6	3	5
AES [10]	128,192,256	9	5	2
RSA [10]	1024	2	7	5
ECC [11]	160	1	7	2
OTP [12]	Same to data	7	9	9

B. *Modeling the problem as a hierarchy*

The second step is modeling the problem as a hierarchy containing the decision goal, the alternatives for reaching it, and the criteria for evaluating the alternatives. Before modeling the problem, we should define the problem and determine its goal. Through the above analysis, we could know the problem is selecting the appropriate encryption algorithm to satisfy the applications’ requirement under given the key sources. Therefore, the goal of the problem is selecting an encryption algorithm. The hierarchy of ASM is shown in Fig. 1 [13].

We introduce the three layers as follow.

- Goal. Selecting an available encryption algorithm. As the key length can be ensure according to the algorithm choose, we just need to select the algorithm.
- Criteria. As the key length is considered in step A, we just need to consider the security, timeliness and the cost.
- Alternatives. In this layer, it contains the mainstreams algorithms.

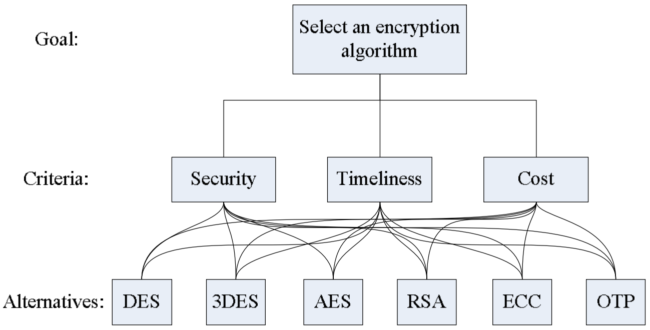


Figure 1 The hierarchy of ASM

C. *Establishing priorities among the elements*

The third step is establishing priorities among the elements of the hierarchy by making a series of judgments based on pairwise comparisons of the elements. Once the hierarchy has been constructed, the participants analyze it through a series of pairwise comparisons that derive numerical scales of measurement for the nodes. The criteria are pairwise compared against the goal for importance. The alternatives are pairwise compared against each of the criteria for preference. The comparisons are processed mathematically, and priorities are derived for each node. Then, we should explain the pairwise compared scheme. That is, we should use a scale to indicate the weightiness of element u_i and u_j for criteria C .Table 2 exhibits the scale [14].

TABLE 2 SCALE OF RELATIVE IMPORTANCES

Intensity of Importance (a_{ij})	Definition
1	Equal importance
3	Weak importance of u_i over u_j
5	Essential importance of u_i over u_j
7	Demonstrated importance of u_i over u_j
9	Absolute importance of u_i over u_j
2,4,6,8	Intermediate values between the two adjacent judgments
1,1/2,1/3,…,1/9	If u_i has one of the above nonzero numbers assigned to it when compared with u_j , then u_j has the reciprocal value when compared with u_i .

For criteria C , we can get a decision matrix which is shown in (1) based on the pairwise compared scheme.

$$A=\left[a_{ij}\right]_{n\times n} \qquad (1)$$

In the equation, a_{ij} and n denote the performance value of the *i-th* element in terms of the *j-th* element and the number of the elements respectively.

In this problem, let u_1,u_2,u_3 denote the criteria which including security, timeliness and cost. We take a real time application named iptux as an example. Therefore, we can get the decision matrix A based on the pairwise compared scheme [15].

$$A=\begin{bmatrix} 1 & 1/2 & 3 \\ 2 & 1 & 5 \\ 1/3 & 1/5 & 1 \end{bmatrix}$$

In this matrix, as timeliness is between to be classified as “equal importance” and “weak importance” than security for iptux, the value a_{12} is $1/2$. Similarly, we can get other values of the matrix. Therefore, timeliness is the most important criteria and cost is the least important for iptux.

D. Extracting the relative importance

The fourth step is extracting the relative importance implied by the previous comparisons. That is, how important are the three alternatives when they are considered in terms of the hardware expandability criterion? Therefore, we must compute the different criteria’s relative importance. We could denote it as a vector, $W=\left(\omega_1,\omega_2,\cdots,\omega_n\right)^T$.

In our solution, the relative importance will be computed using eigenvalue method. That is, we could compute the eigenvalue of maximum, which is denoted $\lambda_{\max}$ [16]. Then, we could get the vector W by the equation (2).

$$AW=\lambda_{\max}W \qquad (2)$$

In our example, we compute $\lambda_{\max}=3.0037$. And, we get $W=(0.334,0.631,0.118)^T$ by (2).

E. Synthesizing these judgments and checking the consistency

The fifth step is synthesizing these judgments to yield a set of overall priorities for the hierarchy and checking the consistency of the judgments. Though the above analysis, we can get an element weight vector which is a set of elements to an element which is in the upper layer. However, our goal is that we want to get the alternatives’ elements to the goal layer’s weights. Next, we introduce the method.

Let $W^{(k-1)}=(\omega_1^{(k-1)},\omega_1^{(k-1)},\cdots,\omega_{n_{k-1}}^{(k-1)})^T$ denote the weight vector which is the *(k-1)_th* layer to the goal layer. Let $P_j^{(k)}=(P_{1j}^{(k)},P_{2j}^{(k)},\cdots,P_{n_kj}^{(k)})^T$ denote the weight vector which is the *k_th* layer to the *(k-1)_th* layer’s *j_th* element. Let denote the weight vector which is the *k-th* layer to the whole elements of *(k-1)_th* layer’s. Therefore, the weight vector which is the *(k-1)_th* layer to the goal layer is $W^{(k)}=(\omega_1^{(k)},\omega_1^{(k)},\cdots,\omega_{n_k}^{(k)})^T=P^{(k)}W^{(k-1)}$. Based on the vector $W^{(k)}$, the alternative which is the maximum value is the appropriate alternative.

As the judgments are relying on subjective judgments, we should check the consistency of the judgments. That is, we should avoid a case that is “absolute importance of A over B , absolute importance of B over C and absolute importance of C over A ”. If all the comparisons are perfect consistent, then the following relation should always be true for any combination of comparisons take from the judgment matrix: $a_{ij}=a_{ik}a_{kj}$. However, perfect consistency rarely occurs in practice. In the AHP the pairwise comparisons in a judgment matrix are considered to be adequately consistent if the corresponding consistency ratio (CR) is less than 10%. The CR is calculated as follows. First the consistency index (CI) needs to be estimated and $CI_j^{(k)}$ is the consistency index which the *j_th* elements of *(k-1)_th* layer influenced by the elements of *k_th* layer. It calculated by $CI=\frac{\lambda_{\max}-n}{n-1}$, and $\lambda_{\max}$ is the maximum eigenvalue of the matrix. Next, the consistency ratio CR is obtained by dividing the CI value by the Random Consistency index (RCI) as given in Table 3. And the layer’s $CI^{(k)}$, $RCI^{(k)}$ and $CR^{(k)}$ can be calculated by (3). If

$CR^{(k)} < 0.1$, the judgments are considered to be adequately consistent [13].

$$\begin{aligned} CI^{(k)} &= (CI_1^{(k)}, CI_2^{(k)}, \cdots, CI_{n_{k-1}}^{(k)})W^{(k-1)} \\ RI^{(k)} &= (RI_1^{(k)}, RI_2^{(k)}, \cdots, RI_{n_{k-1}}^{(k)})W^{(k-1)} \qquad (3) \\ CR^{(k)} &= CR^{(k-1)} + \frac{CI^{(k)}}{RI^{(k)}}, k = 3, 4, \cdots, s \end{aligned}$$

TABLE 3 RCI VALUES FOR DIFFERENT VALUES OF n

n	1	2	3	4	5	6	7	8
RCI	0	0	0.58	0.89	1.12	1.26	1.36	1.41
n	9	10	11	12	13	14	15	
RCI	1.46	1.49	1.52	1.54	1.56	1.58	1.59	

In our example, we could get the decision matrix and the weight vector which is the criteria layer to the goal layer, as shown in Table 4.

TABLE 4 THE MATRIX OF CRITERIA TO GOAL

A	u_1	u_2	u_3	$W^{(2)}$
u_1	1	1/2	3	0.334
u_2	2	1	5	0.631
u_3	1/3	1/5	1	0.118
$\lambda_{\max} = 3.0037; CI = 0.00185; RI = 0.58; CR^{(2)} = 0.00319 < 0.1$				

Similarly, we could get the decision matrix and the weight vector which is the alternative layer to the criteria layer. In table 5, it shows the decision matrix and the weight vector which is the alternative layer to the criteria layer's element u_1.

TABLE 5 THE MATRIX OF ALTERNATIVE TO u_1

B_1	P_1	P_2	P_3	P_4	P_5	P_6	$P_1^{(3)}$
P_1	1	1/2	1/5	1/7	1/7	1/9	0.0315
P_2	2	1	1/2	1/3	1/3	1/5	0.0668
P_3	5	2	1	1/2	1/2	1/3	0.1235
P_4	7	3	2	1	1	1/2	0.2089
P_5	7	3	2	1	1	1/2	0.2089
P_6	9	5	3	2	2	1	0.3603
$\lambda_{\max} = 6.0403; CI_1^{(3)} = 0.00806; RI_1^{(3)} = 1.26; CR_1^{(3)} = 0.00640 < 0.1$							

Therefore, the weight of alternatives is shown in (4).

$$W^{(3)} = P^{(3)}W^{(2)} = \begin{pmatrix} 0.0315 & 0.2128 & 0.1757 \\ 0.0668 & 0.1425 & 0.1033 \\ 0.1235 & 0.3584 & 0.2957 \\ 0.2089 & 0.0445 & 0.1033 \\ 0.2089 & 0.0291 & 0.2957 \\ 0.3603 & 0.2128 & 0.0263 \end{pmatrix} \begin{pmatrix} 0.334 \\ 0.631 \\ 0.118 \end{pmatrix} = \begin{pmatrix} 0.1655 \\ 0.1244 \\ 0.3023 \\ 0.1100 \\ 0.1230 \\ 0.2577 \end{pmatrix} \quad (4)$$

The consistency of final decision is shown in (5).

$$\begin{aligned} CI^{(3)} &= \left(CI_1^{(3)}, CI_2^{(3)}, CI_3^{(3)}\right)W^{(2)} \\ &= \begin{pmatrix} 0.00806 & 0.0232 & 0.01128 \end{pmatrix} \begin{pmatrix} 0.334 \\ 0.631 \\ 0.118 \end{pmatrix} = 0.0187 \quad (5) \end{aligned}$$

$$CR^{(3)} = CR^{(2)} + \frac{CI^{(3)}}{RI^{(3)}} = 0.00319 + \frac{0.0187}{1.26} = 0.018 < 0.1$$

As $CR^{(3)} < 0.1$, we could know the consistency of the judgments is rational. As 0.3022 is the maximum of the weight vector, the third one is the appropriate algorithm. That is, AES is the optimum algorithm which is used to encrypt the message of iptux.

IV. EVALUATION

In our work, the experiments are based on the RT-QKD platform, a system including the quantum device, the post processing and the applications. The composition of experimental environment is shown in Fig. 2. Alice and Bob are using the personal computer (PC). The parameters of the PC are shown in Table 6.

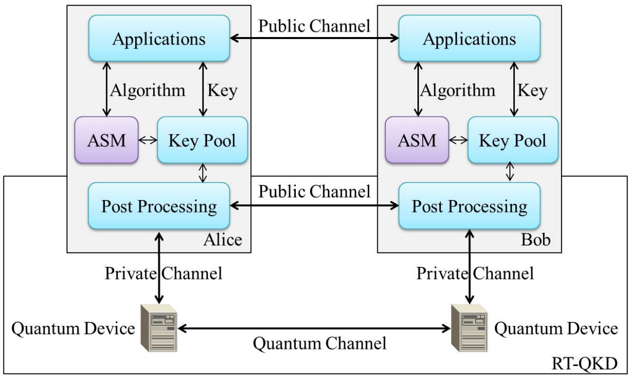


Figure 2 The composition of experimental environment

TABLE 6 THE PARAMETERS OF THE PC

Processor	Intel Core i5-3210M 2.50 GHz
Memory	4G DDR3
OS	Linux(Fedora 14)
Kernel version	2.6.35
Bandwidth	100Mbps

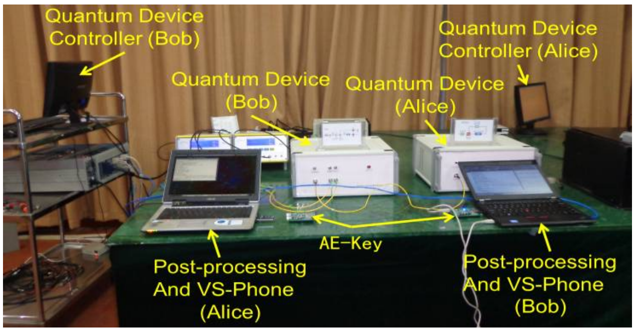
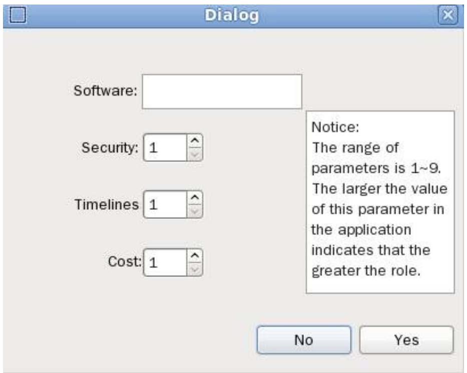

Quantum Device Controller (Bob)
Quantum Device Controller (Alice)
Quantum Device (Bob)
Quantum Device (Alice)
AE-Key
Post-processing And VS-Phone (Alice)
Post-processing And VS-Phone (Bob)

Figure 3 The composition of experimental environment

In our work, we evaluate the functional and performance.

The goal of functional evaluation is testing the feasibility of ASM. We design software that implements ASM. The interface of the software is shown in Fig. 4. At first, users can configure the parameters including the name of the application and the layer of security, timeliness and cost. Then, ASM will select the appropriate algorithm which is suitable the application. At last, the application can transmit the message safely using the encryption algorithm and the unconditional secure key. In our test, we configure and run three applications at the same time, which named VISOR_Phone [17], iptux and FileZilla [18]. The result demonstrates that these applications can run normal at the same time.



Dialog

Software:

Security: 1

Timelines 1

Cost: 1

Notice:
The range of parameters is 1~9.
The larger the value of this parameter in the application indicates that the greater the role.

Figure 4 The interface of the ASM

The performance evaluation contains the time complexity, the space complexity and the optimization.

At first, we evaluate the time complexity. The time complexity contains two parts, computing the weight of elements and the consistency of the judgments. In order to compute the weight of elements, we should compute the equation $W^{(k)} = (\omega_1^{(k)}, \omega_1^{(k)}, \cdots, \omega_{n_k}^{(k)})^T = P^{(k)}W^{(k-1)}$. We assume the mumble of rules that related to the goal is n, the mumble of schemes for selecting is m. We can know that $P^{(k)}$ is a $m \times n$ matrix and $W^{(k-1)}$ is a $n \times 1$ matrix. Therefore, the time complexity of matrix multiplication is $O(2mn)$. In ASM, n and m are fixed, $n = 3$ and $m = 6$. In order to compute the consistency of the judgments, we should compute the matrix's maximal eigenvalue. In our solution, we use the power method [19] to solve the eigenvalue. Assuming the matrix A is $n \times n$, the time complexity is $O(n^2)$. In ASM, the order of A is fixed, $n = 3$. Through the above analysis, the time complexity is acceptable.

Then, we evaluate the space complexity. The space complexity is the storage of matrix. Assuming is a $m \times n$ matrix, the space complexity is $O(mn)$. As the matrix of ASM is reciprocal matrices, the space complexity is $O(mn/2)$. In ASM, the order of matrix is 4. Therefore, the cost of space can be negligible.

At last, we evaluate the optimization. In order to evaluate the optimization, we set the experimental scenes as follow.

- VISOR_Phone: we take a three-minute call using the VISOR_Phone. We use the steganography to transmit the sensitive message at the same time. Therefore, these sensitive messages should be encrypted by encryption algorithm.
- iptux: We send a 2Mbits file which is sensitive to the other one using iptux. Similarly, the file should be encrypted by encryption algorithm.
- FileZilla: We send a 5Mbits file to the FTP server using FileZilla. Similarly, the file should be encrypted by encryption algorithm.

Based on the features of these applications, we can get the conclusion as follow.

- VISOR_Phone : security is the most important criteria. Cost is the least important criteria.
- iptux: timeliness is the most important criteria. Cost is the least important criteria.
- VISOR_Phone : security is the most important criteria. Timeliness is the least important criteria.

Based on ASM, we select the appropriate algorithm of applications is shown Table 7. In order to verifying the optimization, we implement six algorithms which named DES, 3DES, AES, RSA, ECC and OTP with the three applications. Then, we test the security, timeliness and cost. In our experiment scene, we use the time of break, the time of encryption and the cost of key to substitution the security, timeliness and cost. The result of is shown as Fig. 5. At last, we compute the optimize algorithm using linear programming [20]. The result demonstrates that the algorithm which selected by ASM is optimal. Therefore, we could summarize that the algorithm is optimal which is selected by ASM.

I. Conclusion

In this paper, we propose ASM, An adaptive Security Mechanism Selection in Quantum Communication system. In ASM, it can select an appropriate encryption algorithm that satisfies the user's requirement and the limit of the key generation rate, based on the Analytic Hierarchy Process. We implement ASM in RT-QKD, and demonstrate that our solution can select the optimal algorithm under an acceptable cost.

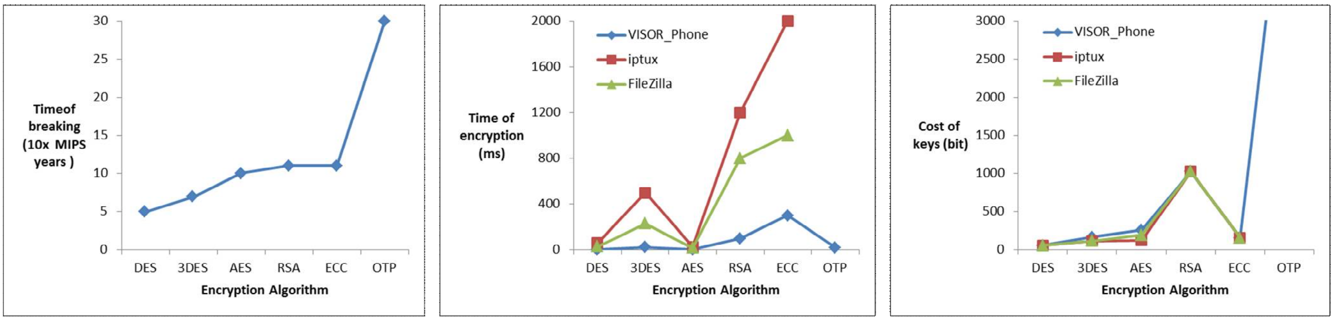


Figure 5 The cost of different algorithms

TABLE 7 THE APPROPRIATE ALGORITHM OF APPLICATIONS

Application	Algorithm
VISOR_Phone	OTP
iptux	AES
FileZilla	ECC

ACKNOWLEDGMENTS

This work is partially supported by the grants of the project of National Science Foundation of China under grant No. 61202488. The work is also in part supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (2014R1A1A1005915).

REFERENCES

[1] Liu B, Zhao B, Zou D, et al. A Real-Time Privacy Amplification Scheme in Quantum Key Distribution, Information and Communication Technology. Springer Berlin Heidelberg, 2013: 453-458.

[2] Fujiwara M, Ishizuka H, Miki S, et al. Field demonstration of quantum key distribution in the Tokyo QKD Network [C]//Quantum Electronics conference & Lasers and Electro-Optics, 2011, IEEE, 2011:507-509.

[3] Xiaoyu Wu, et al. The design of 3G Terminal Data Confidentiality Services [J]. Journal of DAQING Petroleum Institute, 2011, 35(2):95-98.

[4] Irvine C, Levin T. Quality of security service[C]//Proceedings of the 2000 workshop on New security paradigms. ACM, 2001: 91-99.

[5] Liu B, Zhao B, Wei Z, et al. QPhone: A Quantum Security VoIP Phone [C]//Proceeding of the ACM SIGCOMM 2013 conference on SIGCOMM, ACM, 2013:477-478

[6] Ishizaka A, Labib A, Review of the main developments in the analytic hiersarchy process [J]. Expert Systems with Applications, 2011, 38(11):14336-14345.

[7] Saaty T L, Vargas L G. How to Make a Decision[M]//Models, Methods, Concepts & Applications of the Analytic Hierarchy Process. Springer US, 2012: 1-21.

[8] Subramanian N, Ramanathan R. A review of applications of Analytic Hierarchy Process in operations management[J]. International Journal of Production Economics, 2012, 138(2): 215-241.

[9] Singh S P, Maini R. Comparison of data encryption algorithms[J]. International Journal of Computer Science and Communication, 2011, 2(1): 125-127.

[10] Miller F P, Vandome A F, McBrewster J. Advanced Encryption Standard[J]. 2009.

[11] Orlando G. Reliable elliptic curve cryptography computation: U.S. Patent 8,155,307[P]. 2012-4-10.

[12] Horstmeyer R, Judkewitz B, Vellekoop I, et al. Physical key-protected one-time pad[J]. arXiv preprint arXiv:1305.3886, 2013.

[13] Triantaphyllou E, Mann S H. Using the analytic hierarchy process for decision making in engineering applications: some challenges[J]. International Journal of Industrial Engineering: Applications and Practice, 1995, 2(1): 35-44.

[14] Saaty T L. Decision making with the analytic hierarchy process[J]. International Journal of Services Sciences, 2008, 1(1): 83-98.

[15] Vargas L G. Models, methods, concepts & applications of the analytic hierarchy process[M]. Springer US, 2012.

[16] Ahn S C, Horenstein A R. Eigenvalue ratio test for the number of factors[J]. Econometrica, 2013, 81(3): 1203-1227.

[17] Wei Z, Xu L, Liu B, et al. VISOR: A Pratical VoIP Steganography Platform[C]//Mobile Ad-hoc and Sensor Networks (MSN), 2011 Seventh International Conference on. IEEE, 2011: 370-372.

[18] Sanford M, Woodraska D, Xu D. Security Analysis of FileZilla Server Using Threat Models[C]//SEKE. 2011: 678-682.

[19] WANG L, CHU M T. On the global convergence of the high-order power method for rank-one tensor approximation[J]. preprint, North Carolina State University, 2013.

[20] Bazaraa M S, Jarvis J J, Sherali H D. Linear programming and network flows[M]. Wiley. com, 2011.

[21] Lewis N, Bayu A, Youngho Pk, and Kyung H. A fine-grained privacy preserving protocol over attribute based access control for vanets. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 6(2):98–112, June 2015.

[22] Shaojing Fu, Dongsheng Wang, Ming Xu, Jiangchun Ren: Cryptanalysis of Remote Data Integrity Checking Protocol Proposed by L. Chen for Cloud Storage. IEICE Transactions 97-A(1): 418-420 2014

[23] Sangeetha J, Akash G, and Chandrasekaran P. A new certificateless blind signature scheme. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 5(1):122–141, March 2014.

[24] Yaping Liu, Zhihong Liu, Baosheng Wang, Qianming Yang: SIR: A Secure Identifier-Based Inter-Domain Routing for Identifier/Locator Split Network. IEICE Transactions 96-B(7): 1742-1752. 2013

[25] Johannes G and Tilo M. Analysing android's full disk encryption feature. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 5(1):84–100, March 2014.