QKD Communication Protocol for Authentication Mechanism of Cloud Network

Zuriati Ahmad Zukarnain

Department of Communication Technology and Networks, Faculty of Computer Science and Information Technology

Head the High Performance of Computing Section, UPM

Founder of ZA Quantum Sdn Bhd

OUTLINE

- Introduction
- Challenges
- Background
- Previous Research
- Proposed Scheme
- Result
- Conclusion
- Selected References

INTRODUCTION

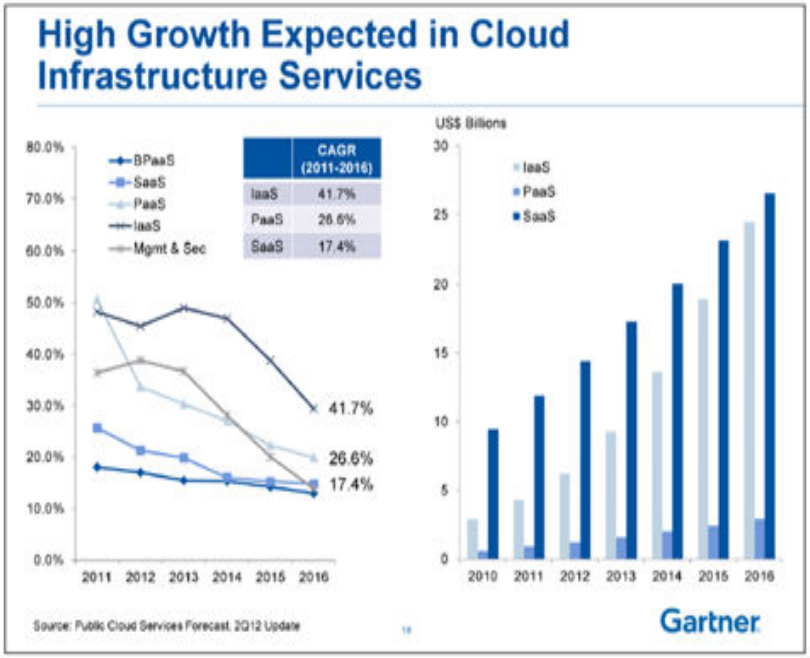
- The aim of this study was to propose unique communication protocol for Authentication Mechanism of Cloud Network in replacing the key distribution technique based on public key infrastructure to achieve unconditional security in cloud.
- Cloud infrastructure provides many benefits in terms of low cost and accessibility of data. Ensuring the security aspect is a major factor in the cloud infrastructure.

CHALLENGES

- Currently, there are certain issues pertaining on Public Key Infrastructure (PKI) in cloud systems.
- It is obviously shown, there is no sufficient secured procedure to move private keys between clouds client.
- To ensure the session is secure, a new scheme that use an appropriate number of photons that can be selected as the bits of the cryptographic key that both the sender and receiver will use.

BACKGROUND

- **Cloud Network**



- According to Gartner Prediction, one third of user data will be in cloud by 2016 **(http://www.gartner.com/it/page.jsp?id=2060215)**

- Cloud computing describes a computing concept where software services, and the resources they use, operate as (and on) a virtualised platform across many different host machines, connected by the Internet or an organization's internal network.

BACKGROUND

- **Authentication**
  - Basic idea of authentication is a process determining whether someone or something is, in fact, who or what it is declared to be
  - Mainly standard cryptography is authentication
  - The authentication scheme is based on client-server architecture

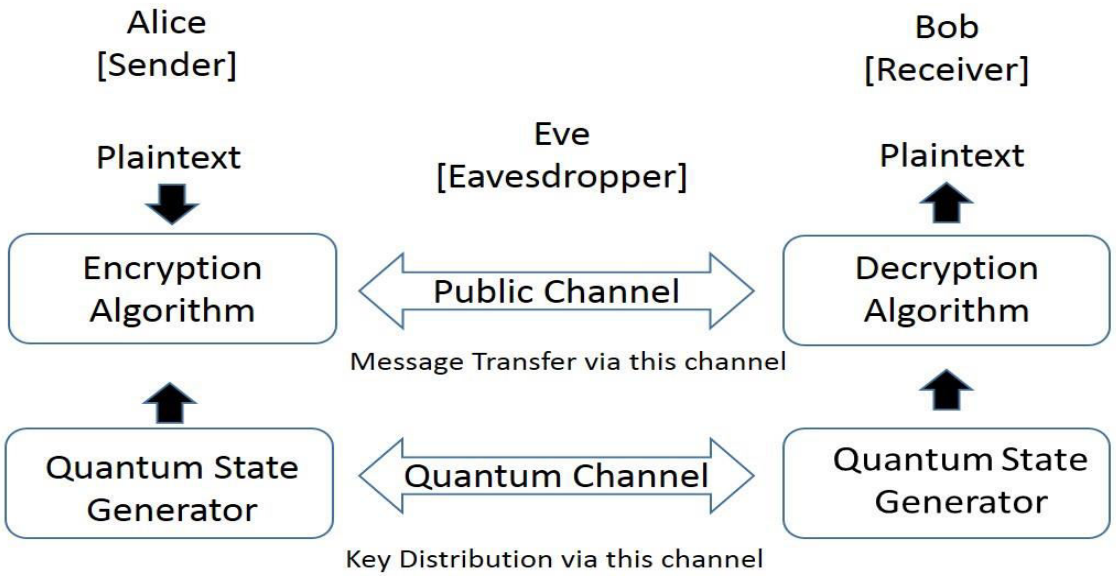
BACKGROUND

The Main contribution of Quantum Cryptography

- It solved the key distribution problem.
- Unconditionally secure key distribution method proposed by:
- Charles Bennett and Gilles Brassard in 1984.
- The method is called BB84.
- Once key is securely received it can be used to encrypt messages transmitted by conventional channels.

BACKGROUND

Concept Of Quantum Key Distribution



ADVANTAGES IN QUANTUM SECURITY

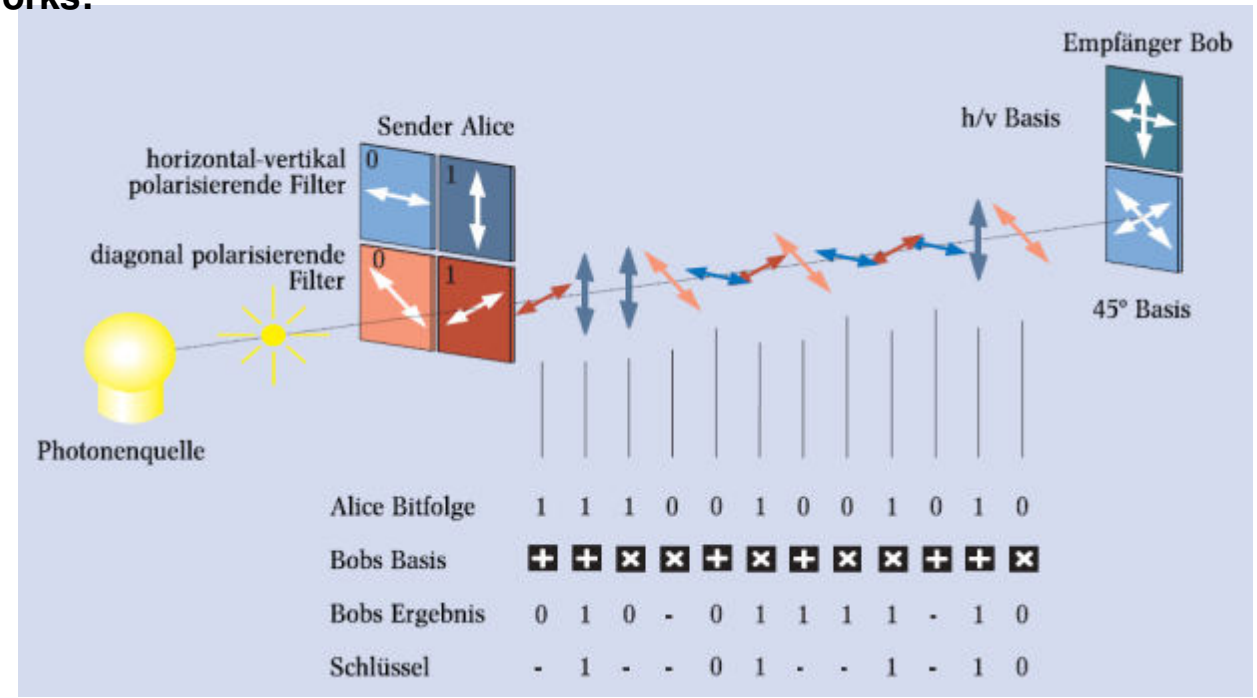
- Provably Secure
- Evidence of Tampering
  - Alice & Bob can find out when Eve tries to eavesdrop.
- Attention that Quantum cryptography means just the exchange of keys
- Actual transmission of data is done with classical algorithms

ADVANTAGES IN QUANTUM SECURITY

Ingredients: 1) One photon ⟶ no copying,
2) Two non orthonormal bases sets
3) Insecure classical channel; Internet

What it does: Secure distribution of **a key**, *can't be used to send messages*

How it works:



Physikalische Blätter 55, 25 (1999)

PREVIOUS RESEARCH

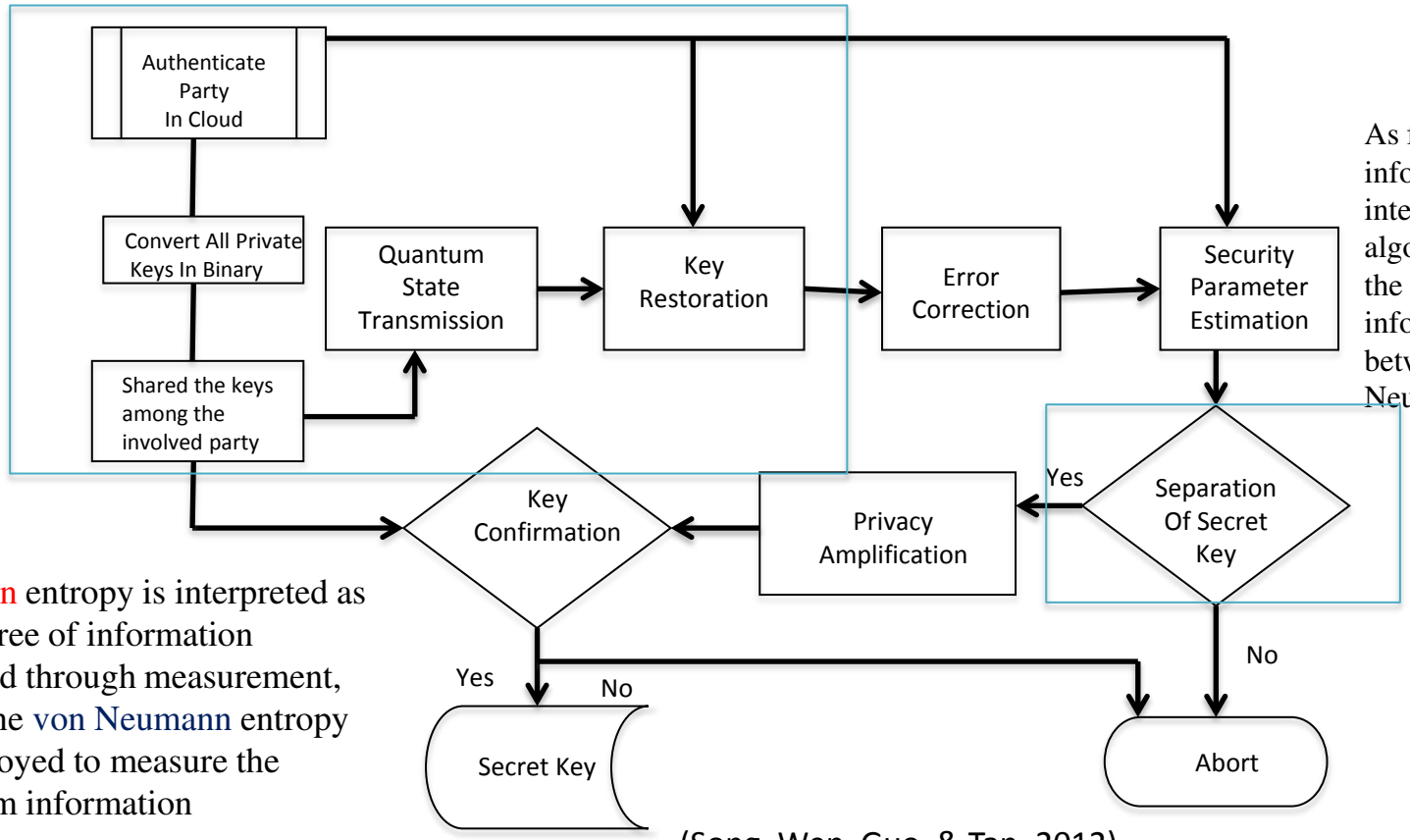
- (Gilbert & Weinstein, 2014).
  - Two solution one-time pad and quantum key distribution (QKD)
- (Hwang, Lee, & Li, 2007)
  - provably secure three party authentication using QKD been introduced. Their focus is on large networks.
- (Goorden, Horstmann, & Mosk, 2013)
  - They introduce quantum secure authentication with classical key that provides a solution of quantum readout. Basically the quantum readout happens in physical keys that easily can be exploits. Thus, by approaching the classical key, they still need to combine the classical channel and quantum channel.
- (Padmavathi, Madhavi, & Nagalakshmi, 2013)
  - V.Padmavathi, M.Madhavi and N.Nagalaksmi in proposed to use group signature base. The group signature base will be verify by third party so called as Trusted Center to distribute the key among members.

PREVIOUS RESEARCH

- (Yuan, Zhou, Zhang, Yang, & Xing, 2012)
  - Multi-party Quantum Key Distribution (MQKD) is actually a key distribution protocol that establish a common key among a number of users
- (Shor & Preskill, 2008)
  - Shows that the BB84 protocol that being introduced by Bennet and Brassard in 1984 is secure and reliable.
- (Mai, Nguyen, Sfaxi, & Ghernaouti-hélie, 2006).
  - As all eavesdropping can be detected, quantum cryptography is considered as a promising key distribution means towards long term unconditionally secure cryptosystems

PROPOSED SCHEME

Proposed Phase



As for quantum information, the intelligence of quantum algorithms is achieved with the principle of minimum information distance between Shannon and von Neumann entropy.

Shannon entropy is interpreted as the degree of information accessed through measurement, while the von Neumann entropy is employed to measure the quantum information

(Song, Wen, Guo, & Tan, 2012)

PROPOSED METHOD

$$p(a) = \sum_b p(a,b), p(b) = \sum_a p(a,b) \quad \text{(Equation1)}$$

The base equation of Shannon's theorem is denoted in equation (1). This is the probability of the key being created by a and b.

$$I(a,b) = S\big(p(a)\big) + S\big(p(b)\big) - S\big(p(a,b)\big) \quad \text{(Equation 2)}$$

For sharing the information, it could be interpreted as in equation (2) where it will involve the Shannon theory in mutual exclusion information sharing.

$$p(a) = \sum_b p(a,b,c), p(b), p(c) = \sum_a p(a,b,c) \quad \text{(Equation 3)}$$

For creating a secret key, it could be interpreted as in equation (3) where it will involve the Shannon theory in mutual exclusion information sharing.

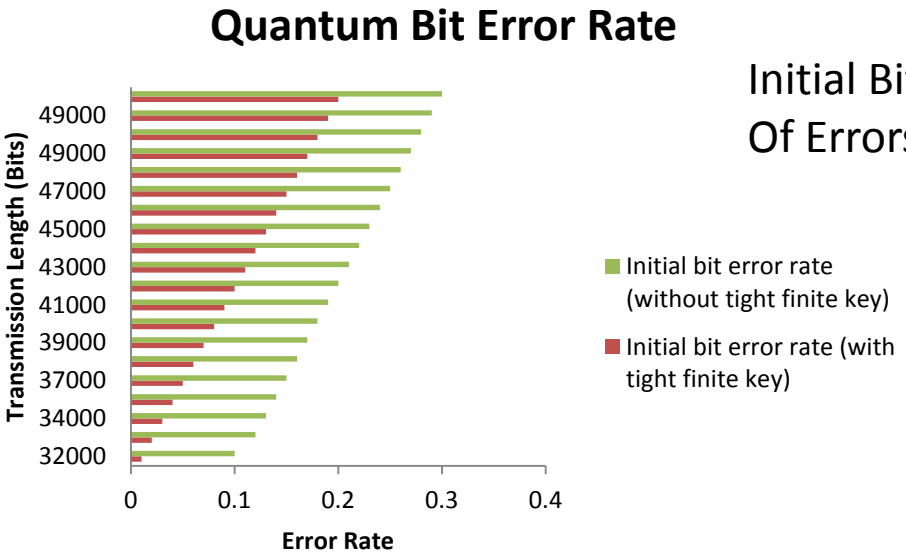
$$I(a,b,c) = S\big(p(a)\big) + S\big(p(b)\big) + S(p(c) - S\big(p(a,b,c)\big)\big) \quad \text{(Equation 3)}$$

Multi-parties that will involve three parties that can share the information

Simulation Setup

- Our simulator is develop on C# platform
- Protocol BB84
- The parameter setup is refer to *Walenta, N. et al.: A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. New J. Phys. 16, 1, 013047 (2014)*
- We choose the size of key for each kind of experiment base on general, post-processing key size (>= 10^5 bits), as required in finite-key scenarios analysed in appendix, and limits imposed by the hardware in terms of memory size and throughput. (Walenta et al., 2014)

QUANTUM BIT ERROR RATE



Initial Bit Error Rate, IBER = Number Of Errors / Total Number Of Bits Sent

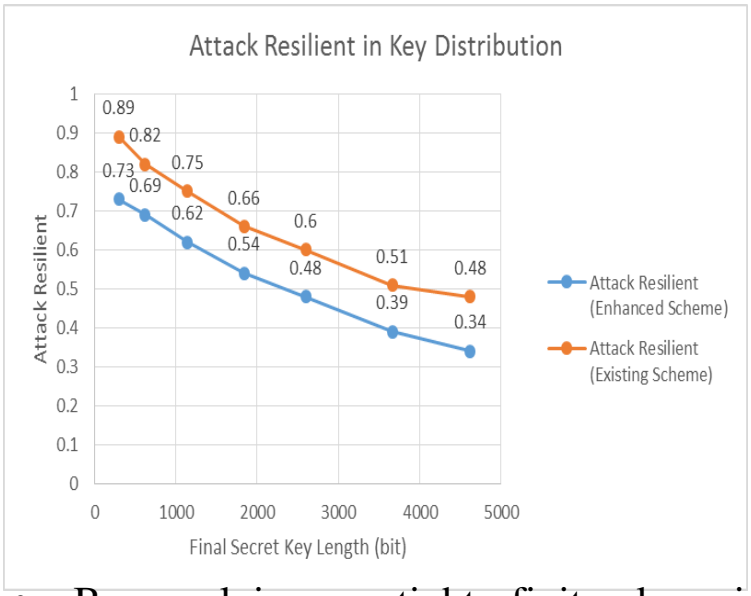
Experiment Setting	
Minimum Total Numbers of Bits Sent	32000 bit
Maximum Total Numbers of Bits Sent	49000 bit
Minimum Number of Errors (Enhanced Scheme)	320 bit
Maximum Number of Errors (Enhanced Scheme)	8330 bit
Minimum Number of Errors (Existing Scheme)	3200 bit
Maximum Number of Errors (Existing Scheme)	13230 bit

A quantum bit error rate is defined as the rate at which errors occur in a transmission system

The result shows our proposed method are better than existing method.
Error rate reduce to almost 10%.

Number of Errors = Initial key – Final Key
Total Number of Bits sent = Transmission Length (Bits)

RESULT



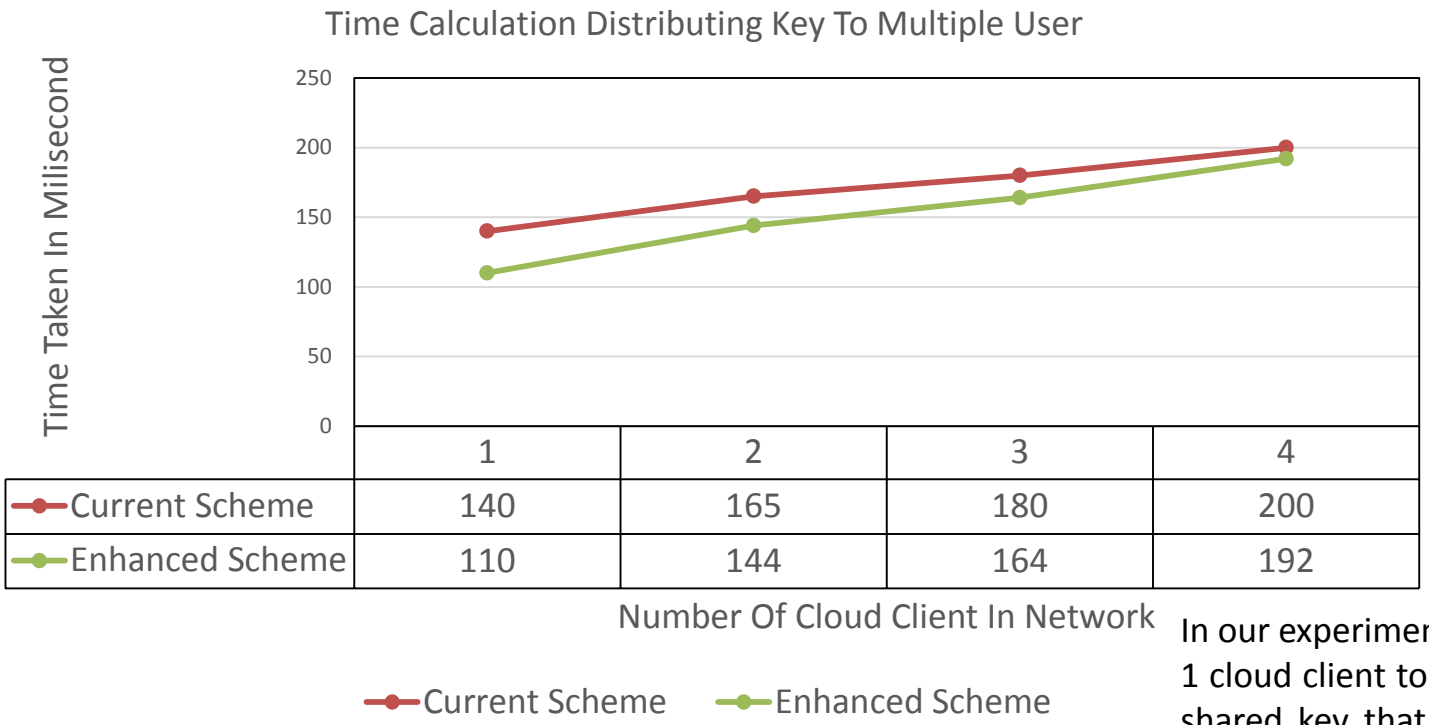
- By applying a tight finite key in quantum key distribution, the problem of the man in the middle attack can be solved.
- We categorized it as resilience to attack.
- In comparing the enhanced scheme with the existing scheme there is a high impact on the proposed method.

$$resilience\ to\ attack = \frac{\text{Initial Key length} - \text{Final Key Length}}{\text{Initial Key Length}}$$

Experiment Setting	
Minimum Initial Key Length	1000 bit
Maximum Initial Key Length	7000 bit
Minimum Final Secret Key Length (Enhanced Scheme)	196 bit
Maximum Final Secret Key Length (Enhanced Scheme)	1200 bit
Minimum Final Secret Key Length (Existing Scheme)	102 bit
Maximum Final Secret Key Length (Existing Scheme)	1100

(Furrer, Franz, Berta, & Leverrier, 2012)

RESULT



	1	2	3	4
Current Scheme	140	165	180	200
Enhanced Scheme	110	144	164	192

Time Taken For Distributing Key To Multiple User = Start Time – End Time

In our experiment, we are test from 1 cloud client to 4 cloud clients. It is a secret shared key that been distribute among the users.

Time taken to distribute a key among a cloud client in the network also reducing with our enhanced scheme

CONCLUSION

- From the result, it shows that our proposed method could improve the error rate.
- The bit error rate is actually a bit error divided by a total number of transferred bits during a studied interval.
- This is due to any noise, interference, distortion or bit synchronization during the transmission of the initial key that error rate can be slightly reduce the error rate by implementing our new scheme.
- In other words it can push aside any interference during the key transmission.

QUANTUM KEY DISTRIBUTION (VIDEO)

SELECTED PUBLICATION

- Buhari, A., Zukarnain, Z. A., Subramaniam, S. K., Zainuddin, H., & Saharudin, S. (2012). A SIMPLE POST QUANTUM SCHEME FOR HIGHER KEY RATE MULTIPARTY QUANTUM KEY DISTRIBUTION. *International Journal of Network Security & Its Applications*, *4*(5), 1..
- Khalid, Roszelinda, and Zuriati Ahmad Zulkarnain. "Enhanced Tight Finite Key Scheme for Quantum Key Distribution (QKD) Protocol to Authenticate Multi-Party System in Cloud Infrastructure." *Applied Mechanics and Materials*. Vol. 481. 2014.
- Khalid, Roszelinda, et al. "Multi-Party System Authentication for Cloud Infrastructure by Implementing QKD." *Computational Intelligence and Efficiency in Engineering Systems*. Springer International Publishing, 2015. 195-207.

SELECTED REFERENCES

[1]G. Gilbert and Y. S. Weinstein, “Introduction to Special Issue on quantum cryptography,” *Quantum Inf. Process.*, vol. 13, no. 1, pp. 1–4, Jan. 2014.

[2]T. Hwang, K. Lee, and C. Li, “Provably Secure Three-Party Authenticated Quantum Key Distribution Protocols,” *IEEE Trans. Dependable Secur. Comput.*, vol. 4, no. 1, pp. 71–80, Jan. 2007.

[3]C. Science, “Building Trust In Cloud Using Public Key Infrastructure,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 3, no. 3, pp. 26–31, 2012.

[4]S. Goorden, M. Horstmann, and A. Mosk, “Quantum-Secure Authentication with a Classical Key,” *arXiv Prepr. arXiv …*, 2013.

[5]V. Padmavathi, M. Madhavi, and N. Nagalakshmi, “An Approach to Secure Authentication Protocol with Group Signature based Quantum Cryptography,” *Int. J. Innov. Technol. Explor. Eng.*, vol. 2, no. 2, pp. 105–107, 2013.

[6]H. Yuan, J. Zhou, G. Zhang, H. Yang, and L. Xing, “Efficient Multiparty Quantum Secret Sharing of Secure Direct Communication Based on Bell States and Continuous Variable Operations,” *Int. J. Theor. Phys.*, vol. 51, no. 11, pp. 3443–3451, Jun. 2012.

SELECTED REFERENCES

[7]M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, “Tight finite-key analysis for quantum cryptography.,” *Nat. Commun.*, vol. 3, no. may 2011, p. 634, Jan. 2012.

[8]P. W. Shor and J. Preskill, “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol,” *Phys. Rev. Lett.*, no. 1, 2008.

[9]T. Mai, T. Nguyen, M. A. Sfaxi, and S. Ghernaouti-hélie, “802 . 11i Encryption Key Distribution Using Quantum Cryptography,” *J. Netw.*, vol. 1, no. 5, pp. 9–20, 2006.

[10]R. Sharma and A. De, “A new secure model for quantum key distribution protocol,” *… Inf. Syst. (ICIIS), 2011 6th …*, vol. 1984, pp. 462–466, 2011.

[11L. Gyongyosi and S. Imre, “Information geometric security analysis of differential phaseâ€shift quantum key distribution protocol,” *Secur. Commun. Networks*, 2012.

[12]A. Karlsson, M. Koashi, and N. Imoto, “Quantum entanglement for secret sharing and secret splitting,” *Phys. Rev. A*, vol. 59, no. 1, pp. 162–168, Jan. 1999.

THANK YOU
FOR
YOUR ATTENTION