HAL open science

A Real-Time Privacy Amplification Scheme in Quantum Key Distribution

Bo Liu, Bo Liu, Baokang Zhao, Dingjie Zou, Chunqing Wu, Wanrong Yu, Ilsun You

To cite this version:

Bo Liu, Bo Liu, Baokang Zhao, Dingjie Zou, Chunqing Wu, et al.. A Real-Time Privacy Amplification Scheme in Quantum Key Distribution. 1st International Conference on Information and Communication Technology (ICT-EurAsia), Mar 2013, Yogyakarta, Indonesia. pp.453-458, 10.1007/978-3-642-36818-9_50 . hal-01480204

HAL Id: hal-01480204

https://inria.hal.science/hal-01480204v1

Submitted on 1 Mar 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

A Real-time Privacy Amplification Scheme in Quantum Key Distribution

Bo Liu[1], Bo Liu, Baokang Zhao[1]*, Dingjie Zou, Chunqing Wu, Wanrong Yu

[1]Department of Computer Science
National University of Defense Technology
Changsha, Hunan, CHINA
{liub0yayu@gmail.com}, {boliu,bkzhao,chunqingwu}@nudt.edu.cn

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

Abstract..QKD (Quantum Key Distribution) technology, based on the laws of physics, can create an unconditionally secure key between communication parties. In recent years, researchers draw more and more attention to the QKD technology. Privac amplification is a very significant procedure in QKD system. In this paper, we propose the real-time privacy amplification (RTPA) scheme which converts the weak secret string W to a uniform key that is fully secret from Eve. We implement RTPA scheme based on CLIP (Cvqkd Ldpc experImental Platform) which is connected to the real quantum communication systems. Experimental results show that, our proposed RTPA scheme is very efficient when the bit error rate of quantum channel is lower than 0.06.

Keywords: QKD, privacy amplification, security

1 Introduction

Quantum Key Distribution (QKD) [1, 2] is technology for solving the key distribution problem. QKD system, based on the laws of physics, rather than the computational complexity of the mathematical problems assumed by current cryptography methods, can create an unconditionally secure key between communication parties. These keys are generated over unsecured channels, where may exist an active computationally unbounded adversary Eve.

After the procedure of information reconciliation [3], Alice and Bob have own almost uniform keys with comparative low BER (Bit Error Rate). But Eve may have partial knowledge about the keys by eavesdropping or other ways.

[1] The Corresponding author: Dr. Baokang Zhao, School of Computer Science, National University of Defense Technology.CHINA.

Therefore, in order to gain the absolutely security keys, we must ensure the keys are privacy amplified. Privacy amplification (PA) [4] is a technology, through a public channel, to improve the information confidentiality. Privacy amplification converts the weak secret string W to a uniform key that is fully secret from Eve.

Privacy amplification technology typically applies a random and public hash function to shorten the weak secret key and reduce the amount of information obtained by Eve as much as possible. By sacrificing partially key information of Alice and Bob, privacy amplification makes the knowledge obtained by Eve been meaningless.

Though the majority researches (such as [5, 6]) about privacy amplification focusing on the theoretical study and proof of security, implementing an efficient privacy amplification scheme in QKD system has been more and more significant.

In this paper, we propose a real-time privacy amplification scheme (RTPA) and implement RTPA in CLIP system [7], which is connected to the quantum communication system. After extensive experiments, the performance and the detail analysis are described in Section III. Experimental results show the efficiency of our proposed RTPA scheme for generating unconditional security keys in quantum cryptography.

2 The Proposed RTPA Scheme

2.1 Privacy Amplification Protocol

After analyzed and researched the classical and quantum privacy amplification theoretical study in [4, 8, 9, 10] and etc., we approach the RTPA protocol (Real-time Privacy Amplification Protocol).

We assume that the key information of Alice and Bob after information reconciliation is W and its length is N, the length of key information used for reconciliation, confirmation and etc. is K, the length of key information may obtained by Eve is T, the security parameter is S, and the final key length is R. We describe the RTPA protocol as follows:

- Alice and Bob select the security parameter S, according to the quantum key state, key length N and other information;
- Alice generates the description information about hash function randomly, the seed string $Seed$ and the shift string $Shift$. $Seed$ and $Shift$ send to Bob through the public channel;
- Alice and Bob construct the hash function f, $f \in F$, $F:\{0,1\}^N \rightarrow \{0,1\}^R$, $R = N - T - K - S$;
- Alice and Bob gain the final key y, $y = f(W)$.

In RTPA protocol, hash function f is randomly chosen from class H_3 of universal$_2$. The hash function is described by Toeplitz matrix construction method [11, 12, 13]. After applying the privacy amplification procedure, the final key is unconditionally safe to Eve.

2.2 The RTPA Scheme

The RTPA scheme mainly consists three parts: Hash function construction, data communication and privacy amplification. The architecture of RTPA is shown in Figure 1.

Hash function construction

As shown in Figure 1, the parameter controller carries out the security parameter S and controls the generation of $Shift$ and $Seed$ based on the quantum channel states. Then, the hash function construction module constructs Toeplitz hash function scaling $N \times R$.

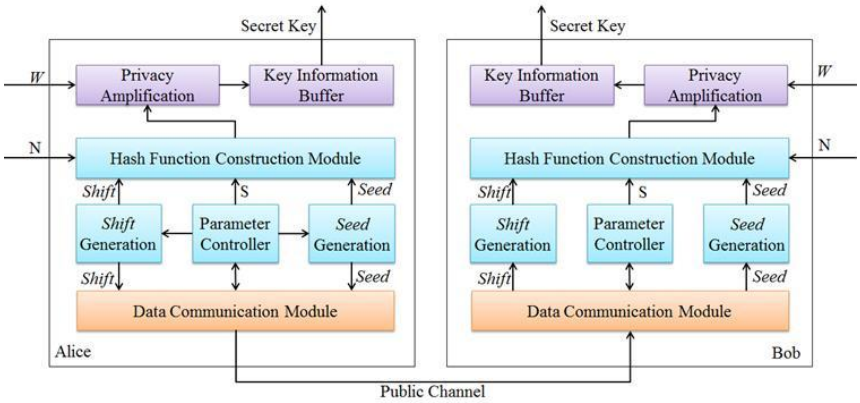

Fig. 1. The Architecture of RTPA

- **Data communication**
  In this part, Alice sends $Shift$ and $Seed$, the description information of hash function , to Bob through a public channel.
- **Privacy amplification**
  Privacy amplification is applied to convert W to an absolutely secret key with length R. These keys used for quantum cryptography are stored in the Key information buffer.

3 Experimental Results And Analysis

The RTPA scheme is implemented in CLIP [7] which is connected to the real quantum communication system. The experimental environment is shown in Figure 2.

We conducted extensive experiments to evaluate the performance of RTPA. We analyzed the privacy amplification overhead, average bit error rate (avBER) of key information.

3.1 Privacy Amplification Overhead

Various hash function constructed for different input key lengths, will lead to different time overhead per privacy amplification process. While the input key length should be long enough in order to gain an absolutely security key, the privacy amplification overhead will be very high. In this experiment, we test the privacy amplification overhead of different hash function scale. The result is shown in Figure 3.

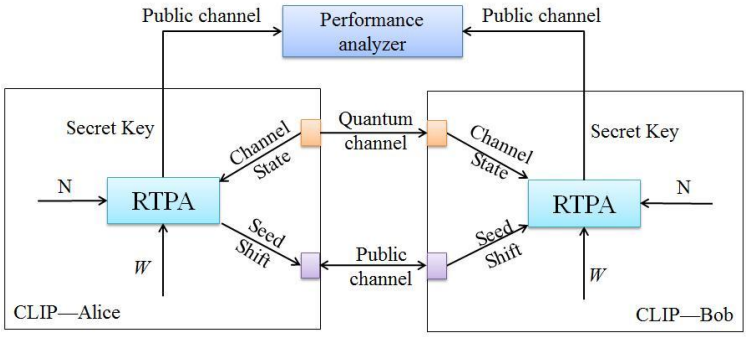

Fig. 2. The experimental environment of RTPA

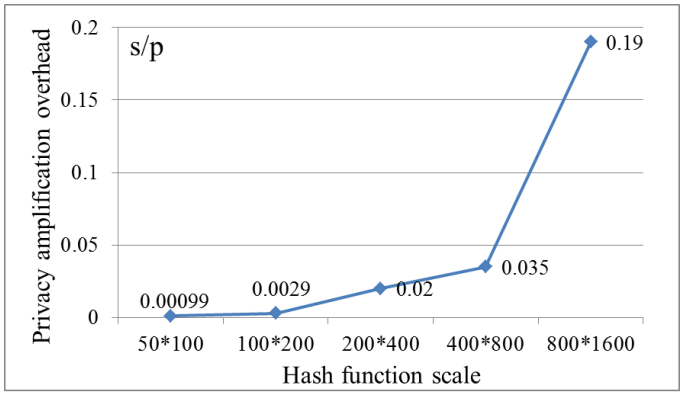

Fig. 3. The privacy amplification overhead of various hash function scales

For example, it will cost 0.19s/p (second per amplification process) when converting a key from 1600 bits to 800bits. Though costing 9.5 times overhead than the scale of 200*400, the security of keys is enhanced by thousands of times. The hash function scale should be balanced between the security demands and the time overhead.

3.2 Average Bit Error Rate

After the procedure of information reconciliation, Alice and Bob have own almost uniform keys with comparative low BER (Bit Error Rate). When applying hash func-

tion to these keys, it may generate quite different strings for Alice and Bob. Therefore, we test the average Bit Error Rate for the final keys with different quantum channel Bit Error Rates.

As it shown in Figure 4, privacy amplification can work effectively when the BER of quantum channel is lower than 0.06. When the BER of quantum channel ranges from 0.06 to 0.10, the information reconciliation procedure still works effectively, the BER after information reconciliation is close to zero, but the BER after privacy amplification is very high. And it doesn't meaningless when the quantum channel BER is higher than 0.10.

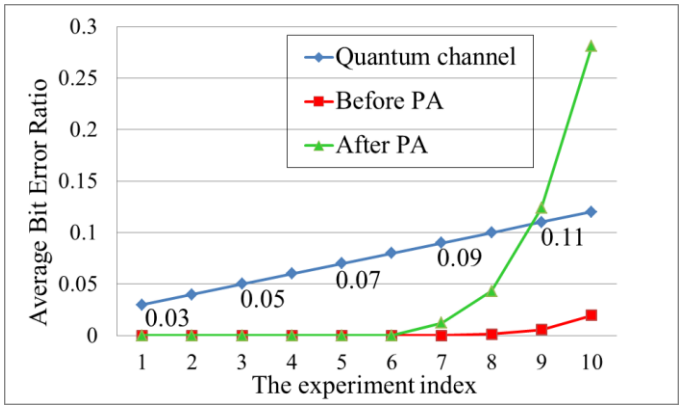

Fig. 4. The Average Bit Error Ratios with different scenes

4 Conclusion

In this paper, we approached the privacy amplification protocol and proposed the RTPA scheme, a real-time quantum privacy amplification procedure in QKD systems. To evaluate the performance of RTPA, we built a prototype QKD system based on CLIP [7]. Experimental results showed the efficiency of our proposed RTPA scheme when the bit error rate of quantum channel is lower than 0.06. The results showed that the performance of RTPA is greatly affected by the quantum channel BER and the information reconciliation. In order to gain an efficient performance, we must enhance the performance of information reconciliation to gain a low BER of key information before privacy amplification.

5 Acknowledgment

The work described in this paper is partially supported by the grants of the National Basic Research Program of China (973 project) under Grant No.2009CB320503, 2012CB315906;the National High Technology Research and Development Program("863"Program) of China under Grant No. 2011AA01A103, the project of National Science Foundation of China under grant No. 61070199, 61003301, 61103189,

61103194, 61103182, 61202488; the Research Fund for the Doctoral Program of Higher Education of China uner Grant No. 20124307120032, and supported by Program for Changjiang Scholars and Innovative Research Team in University of the Ministry of Education("Network Technology",NUDT), the Innovative Research Team in University of Hunan Province("Network Technology",NUDT), and the Innovative Research Team of Hunan Provincial natural science Foundation(11JJ7003).

References

1. C.H. Bennett and G. Brassard, Quantum Cryptography: Public Key Distribution and Coin Tossing, inProc. IEEE Int. Conf. Comput., Syst., Signal Process., 1984, pp. 175–179.（QKD）
2. A. K. Ekert, Quantum cryptography based on Bell theorem, Phys. Rev. Lett., vol. 67, pp. 661–663, 1991.（QKD）
3. G. Brassard and L. Salvail, Secret-key reconciliation by public discussion, EUROCRYPT '93, LNCS, Vol. 765, pp. 410–423. Springer-Verlag, 1994.
4. C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer. Generalized privacy amplification. IEEE Transactions on Information Theory, 41(6):1915-1923, 1995.
5. Yodai Watanabe, Privacy amplification for quantum key distribution, 2007, J. Phys. A: Math. Theor. 40(2007) F99–F104
6. Renato Renner, Robert König, Universally Composable Privacy Amplification Against Quantum Adversaries, Theory of Cryptography, Lecture Notes in Computer Science Volume 3378, 2005, pp 407-425
7. D. Zou, B. Zhao, C. Wu, B. Liu, W. Yu, X. Ma, H. Zou, CLIP: A Distributed Emulation Platform for Research on Information Reconciliation. NBiS 2012: 721-726
8. N. Chandran, B. Kanukurthi, R. Ostrovsky, and L. Reyzin. Privacy amplification with asymptotically optimal entropy loss. In Proceedings of the 42nd Annual ACM Symposium on Theory of Computing, pages 785–794, 2010.
9. Yevgeniy Dodis and Daniel Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In Proceedings of the 41st Annual ACM Symposium on Theory of Computing, page 601610, 2009.
10. T. Horváth, L. B. Kish and J. Scheuer, Effective privacy amplification for secure classical communications, EPL, Volume 94, Number 2, April 2011 , pp. 28002-28007(6)
11. Y. Mansour, N. Nisan and P. Tiwari, The computational complexity of universal hashing. Theoret. Comput. Sci., 107 (1993), pp. 121–133.
12. H. Krawczyk. LFSR-based hashing and authentication. Advances in Cryptology — CRYPTO '94. Lecture Notes in Computer Science, vol. 839, Springer-Verlag, pp 129–139, 1994.
13. Chi-Hang Fred Fung, Xiongfeng Ma, and H. F. Chau, Practical issues in quantum-key-distribution postprocessing, Phys. Rev. A 81, 012318 (2010).