Efficient Almost Strongly Universal Hash Function for Quantum Key Distribution

Extended Abstract

Bo Liu[1], Baokang Zhao[1(✉)], Chunqing Wu[1], Wanrong Yu[1], and Ilsun You[2]

[1] School of Computer Science,
National University of Defense Technology, Changsha, Hunan, China
liubo.eecs@gmail.com,
{bkzhao,wuchunqing,wryu}@nudt.edu.cn
[2] School of Information Science, Korean Bible University, Seoul, Korea
isyou@bible.ac.kr

Abstract. Quantum Key Distribution (QKD) technology, based on principles of quantum mechanics, can generate unconditional security keys for communication parties. Information-theoretically secure (ITS) authentication, the compulsory procedure of QKD systems, avoids the man-in-the-middle attack during the security key generation. The construction of hash functions is the paramount concern within the ITS authentication. In this extended abstract, we proposed a novel Efficient NTT-based ε-Almost Strongly Universal Hash Function. The security of our NTT-based ε-ASU hash function meets $\varepsilon \leq L(n+1)/2^{n-2}$. With ultra-low computational amounts of construction and hashing procedures, our proposed NTT-based ε-ASU hash function is suitable for QKD systems.

Keywords: Almost strongly universal hash · Quantum key distribution

1 Introduction

With the rapid development of computing technologies, the importance of secure communication is growing daily [21–24]. Unlike conventional cryptography which based on the computational complexity, Quantum Key Distribution (QKD) can achieve the unconditional security communication [1, 2, 18–20]. By transmitting security key information with quantum states, the final key generated by QKD system is information-theoretically secure (ITS), which is guaranteed by the non-cloning theorem and measuring collapse theorem in quantum physics [3, 4]. Nowadays, QKD has been one of the research focuses around the world. In recent years, the famous QKD network projects mainly include SECOQC in Europe [5], UQCC in Tokyo [6] and NQCB in China [7] and so on.

ITS authentication is the compulsory procedure of QKD system and also the key procedure which ensures the security of generated keys between communication parties [4, 8]. Otherwise, QKD is vulnerable to the man-in-the-middle attack [9–11]. The main challenge about the research of ITS authentication is the construction of hash functions which are suitable for ITS authentication with less security key [9, 12–14].

I. Khalil et al. (Eds.): ICT-EurAsia 2015 and CONFENIS 2015, LNCS 9357, pp. 282–285, 2015.
DOI: 10.1007/978-3-319-24315-3_29

Usually, ε-Almost Strongly Universal (ε-ASU) hash functions can be used to construct ITS authentication schemes in a natural way. Majority construction schemes focus on the ε-ASU_2 hash function families, such as Wegman-Carter's and Krawczyk's construction schemes [13, 14]. Nowadays, the photon transmission frequency has reached to about ten GHz [15, 16]. With heavy computational amounts, ITS authentication schemes which based on ε-ASU_2 hash functions cannot meet the high performance requirement of QKD systems [9, 13, 17].

In this extended abstract, with NTT technology, we proposed a novel Efficient ε-Almost Strongly Universal Hash Function. With the special features of number-theoretic transforms (NTT) technology, our ε-ASU hash function family is constructed in the prime ring $\boldsymbol{Z}_p^L$. In order to construct the NTT-based ε-ASU hash function efficiently, we assume that $L = 2^{\lambda}$, and the prime number $p = \upsilon L + 1$. We assume that the set of all messages is R, where $R \in \boldsymbol{Z}_p^L$ with length of L, and the length of authentication tag is n, where $n = \beta\lceil \log_2 p \rceil$. The security of our NTT-based ε-ASU hash function meets $\varepsilon \le L(n+1)/2^{n-2}$ and the consumed key length of ITS authentication scheme is less than $3n + 1$.

2 NTT-Based Almost Strongly Universal Hash Function

Since the construction has to consume a very long key, Gilles's NTT-based almost universal hash function is not suitable for ITS authentication [18]. With a partially known security key and a LFSR structure [13], a random bit stream can be generated to construct the NTT-based almost strongly universal (NASU) hash functions.

Let $\boldsymbol{R}$ be the set of messages, where $\boldsymbol{R} \in \boldsymbol{Z}_p^L$. We take only the first β elements of the hashing result. Let $f(x)$ be an irreducible polynomial with degree $\beta\lceil \log_2 p \rceil$ of $GF(2)$ and $\boldsymbol{s_{init}} = \left(s_0, s_1, \cdots, s_{\beta\lceil \log_2 p \rceil - 1}\right)^T$ be an initial state of the LFSR structure defined by the feedback function $f(x)$. $\boldsymbol{s_{init}}$ and $f(x)$ are both generated from the partially known key with length of $2\beta\lceil \log_2 p \rceil + 1$. Let $\boldsymbol{f} = \left(f_0, f_1, \cdots, f_{\beta\lceil \log_2 p \rceil - 1}\right)^T$ be the coefficient vector of $f(x)$ and $\boldsymbol{s}_{[i-\beta\lceil \log_2 p \rceil, i-1]} = \left(s_{i-\beta\lceil \log_2 p \rceil}, s_{i-\beta\lceil \log_2 p \rceil + 1}, \cdots, s_{i-1}\right)^T$, where $i \ge \beta\lceil \log_2 p \rceil$.

Thus, we can gain the random bit

$$s_i = \boldsymbol{s}_{[i-\beta\lceil \log_2 p \rceil, i-1]}{}^{\tau} \boldsymbol{f} \bmod 2. \tag{1}$$

Let $1 \le \beta \le L$ and $K = \left(2^0, 2^1, \cdots, 2^{\lceil \log_2 p \rceil - 1}\right)$. For $\boldsymbol{C}, \boldsymbol{R} \in \boldsymbol{Z}_p^L$, let $h_C(\boldsymbol{R}) = \left(F^{-1}(C \cdot R)\right)_{0,1,\cdots,\beta-1}$ be the inverse NTT of their component-wise product, taking only the β first elements of the result. Assume that $u = \lceil \log_2 p \rceil$, we define that the set

$$H_{p,L,\beta,\boldsymbol{s},\boldsymbol{f}} = \left\{ h_C : C_i = K\boldsymbol{s}_{[(i+\beta)u,(i+\beta+1)u-1]} \bmod p, \forall i \right\} \tag{2}$$

is an almost strongly universal family of hash functions with $\varepsilon \le (L + 2L\beta\lceil \log_2 p \rceil + 2)/2^{\beta\lceil \log_2 p \rceil}$. Assume that $n = \beta u$, we have $\varepsilon \le (L + 2nL + 2)/2^n$.

3 Potential Advantages

Comparing with ASU_2 hash functions, our proposed NASU hash functions have the following potential advantages:

(a) NASU hash functions can be easily constructed with a partially known security key and a LFSR structure.
(b) With the special features of number-theoretic transforms (NTT) technology, the computational amounts of our NASU hashing procedure is much less than Krawczyk's scheme and other ASU_2 hash functions.
(c) Treating the elements of input messages as non-binary integers of the ring $\boldsymbol{Z}_p^L$, our proposed NTT-based ε-ASU hash function is very suitable for ITS authentication in QKD systems.

In the future, we will explore the detailed security proof of NASU hash functions and its deployment within the QKD system.

References

1. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N., Dušek, M., Lütkenhaus, N., Peev, M.: The security of practical quantum key distribution. Rev. Mod. Phys. **81**, 1301–1350 (2009)
2. Wang, L., Chen, L., Ju, L., Xu, M., Zhao, Y., Chen, K., Chen, Z., Chen, T.-Y., Pan, J.-W.: Experimental multiplexing of quantum key distribution with classical optical communication. Appl. Phys. Lett. **106**, 081108 (2015)
3. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, New York (Year)
4. Ma, X., Fung, C.-H.F., Boileau, J.C., Chau, H.F.: Universally composable and customizable post-processing for practical quantum key distribution. Comput. Securtiy **30**, 172–177 (2011)
5. Leverrier, A., Karpov, E., Grangier, P., Cerf, N.J.: Unconditional security of continuous-variable quantum key distribution. arXiv preprint arXiv:0809.2252 (2008)
6. Sasaki, M., Fujiwara, M., et al.: Field test of quantum key distribution in the Tokyo QKD Network. Opt. Express **19**, 10387–10409 (2011)
7. http://www.quantum2011.org/
8. Ma, X.: Practical Quantum key Distribution post-processing (2011)
9. Abidin, A.: Authentication in Quantum Key Distribution: Security Proof and Universal Hash Functions. Department of Electrical Engineering, vol. Ph.D. Linkoping University (2013)
10. Pacher, C., Abidin, A., Lorunser, T., Peev, M., Ursin, R., Zeilinger, A., Larsson, J.-A.: Attacks on quantum key distribution protocols that employ non-ITS authentication. arXiv preprint arXiv:1209.0365 (2012)
11. Ioannou, L.M., Mosca, M.: Unconditionally-secure and reusable public-key authentication. arXiv preprint arXiv:1108.2887 (2011)
12. Portmann, C.: Key Recycling in Authentication. arXiv preprint arXiv:1202.1229 (2012)
13. Krawczyk, H.: LFSR-based hashing and authentication. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 129–139. Springer, Heidelberg (1994)

14. Wegman, M.N., Carter, J.L.: New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci. **22**, 265–279 (1981)
15. Wang, S., Chen, W., Guo, J.: YIn, Z., Li, H., Zhou, Z., Guo, G., Han, Z.: 2 GHz clock quantum key distribution over 260 km of standard telecom fiber. Opt. Lett. **37**, 1008–1010 (2012)
16. Tanaka, A., Fujiwara, M., et al.: High-speed quantum key distribution system for 1-Mbps real-time key generation. IEEE J. Quant. Electron. **48**, 542–550 (2012)
17. Carter, J.L., Wegman, M.N.: Universal classes of hash functions. In: Proceedings of the Ninth Annual ACM Symposium on Theory of Computing, pp. 106–112. ACM (Year)
18. Liu, B., Zhao, B., Wei, Z., et al.: Qphone: a quantum security VoIP phone. In: Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM. ACM, pp. 477–478 (2013)
19. Liu, B., Zhao, B., Liu, B., et al.: A security real-time privacy amplification scheme in QKD system. J. UCS. **19**(16), 2420–2436 (2013)
20. Sun, S., Jiang, M., Ma, X., Li, C., Liang, L.: Hacking on decoy-state quantum key distribution system with partial phase randomization, Scientific Reports (2013)
21. Liu, Y., Peng, W., Jinshu, S.: A study of IP prefix hijacking in cloud computing networks. Secur. Commun. Netw. **7**(11), 2201–2210 (2014)
22. Roland, R., Zhdanova, M., Repp, J.: Security compliance tracking of processes in networked cooperating systems. J. Wirel. Mob. Netw., Ubiquitous Comput., Dependable Appl. (JoWUA) **6**(2), 21–40 (2015)
23. Kotenko, I.: Guest editorial: security in distributed and network-based computing. J. Wirel. Mob. Netw., Ubiquitous Comput., Dependable Appl. (JoWUA) **6**(2), 1–3 (2015)
24. Skovoroda, A., Gamayunov, D.: Securing mobile devices: malware mitigation methods. J. Wirel. Mob. Netw., Ubiquitous Comput., Dependable Appl. (JoWUA) **6**(2), 78–97 (2015)