Applied Computer Letters (ACL)

DOI: http://doi.org/10.7508/acl.01.2023.11.14

ISSN: 2377-6242 (Print)
ISSN: 2377-8156 (Online)

ARTICLE

THE IMPORTANCE OF TRUE RANDOM NUMBER TO NETWORK COMMUNICATION SECURITY

Ying Xu

School of Mechanical Electronic & Information Engineering, China University of Mining and Technology-Beijing, Beijing 10010, China
****Corresponding Author Email: 2010490303@student.cumtb.edu.cn***

ARTICLE DETAILS

Article History:

Received 1 January 2022
Accepted 28 January 2022
Available online 9 March 2023

ABSTRACT

In today's network communication environment, random number has a very wide range of applications. Such as identity authentication and digital signature, RFID label ownership transfer need to use random numbers. Generating key is one of the main uses of random number and its importance for network communication security is self-evident. In order to further study the importance of true random numbers to network communication security, this paper compares pseudo-random numbers with true random numbers by comparison, and finds that true random numbers are more difficult to crack than pseudo-random numbers, which better meets the requirements of network communication security for random numbers. True random number is more advantageous to ensure the security of network communication and has very important significance for maintain the security of network communication.

KEYWORDS

True random numbers, cryptography, network communication security, keys

INTRODUCTION

With the rapid development of communication technology, network communication security becomes more critical. The best means to maintain network security is cryptography. In the use of cryptography, random number is widely used both in the algorithm to generate keys and in the cryptographic protocol to randomly initialize specific variables. For example, random numbers can be applied to digital signature, identity authentication [1], etc. Random numbers can be roughly divided into two categories: pseudo-random numbers and true random numbers. The generation of pseudo-random numbers is mainly through mathematical algorithms, while the generation of true random numbers is mainly through physical random. Hao et al. applied pseudorandom number generator to information encryption processing and designed a lightweight electronic tag ownership transfer protocol based on the pseudorandom number generator [2]. Lu et al. designed a configurable, lightweight and high-throughput true random number generator [3] based on a configurable asynchronous feedback ring oscillator composed of and/or gates and xOR gates. Xue et al. introduced several random number generators and compared their applications in the security level [4]. According to the references, most people's research is biased to quantitative research, and most of them focus on the design of random number generator and its application in information security systems.

This paper mainly studies the importance of random numbers to the security of network communication, and focuses on true random number to study how it is important to the security of network communication. Compared with pseudo-random numbers, it is found that true random numbers are independent in time, uniform in space, unpredictable and unrepeatable, and random in statistics [5]. The superiority of true random number shows that it is more important in the application of network communication security. This paper studies the importance of true random numbers in network communication security, which has theoretical value for the application of true random numbers in information security systems in the future.

1. RANDOM NUMBER SECURITY FOR NETWORK COMMUNICATION OVERVIEW

The security conditions required for the storage and transmission of various communication data in the network environment refer to the security of network information [6]. Nowadays, with the rapid development of network communication technology, some network communication security problems need to be solved urgently. Random numbers are the cornerstone of cryptography. When analyzing the security of random numbers, we should consider all aspects of true and false random numbers and the requirements of network communication security on random numbers.

1.1 Network Communication Security Problem and Countermeasure Analysis

The main threat to network communication security is human factors. For example, to use the identity of the user, so as to illegally intercept, obtain data, and even analyze, tamper with the user information; or

Table 1: Comparison of two encryption methods

Way of encryption	Whether the encryption key is the same as the decryption key	Safety	Consumption	Algorithm
Symmetrical encryption	Yes	Low	Low	DES AES、IDEA
Asymmetric encryption	No	High	High	RSA DSA、Diffie-Hellman

monitor and steal the content of the communication when the user is conducting network communication [7]. These network communication security problems have a serious impact on the user's normal network work and life, at least the loss of personal property, serious disclosure of state secrets. In order to solve the security problem of network communication, it is necessary to select the appropriate encryption method. Encryption methods mainly fall into two categories: symmetric encryption and asymmetric encryption [8]. The two encryption methods are matched as shown in Table 1.

Symmetric encryption has low security. If the key is stolen, the ciphertext will be cracked. Asymmetric encryption has a high cost, but the public key used for encryption and the private key used for decryption are a key pair. Even if the ciphertext and public key are known, the ciphertext cannot be cracked, which greatly improves the security. Therefore, asymmetric encryption is widely used, such as digital signature, public statement, mail sending and receiving [8], etc. No matter what kind of encryption method, the security of an encryption algorithm is based on the security of the key. The secure key must be generated by a random number. The higher the security of the random number, the higher the security of the key.

1.2 Comprehensive Index Analysis of Pseudorandom Number and True Random Number

The security of random numbers is closely related to the security of key, which is directly related to the quality of network communication security. Random numbers can be divided into two categories: pseudo-random numbers and true random numbers [9].

Pseudorandom numbers are generally generated by computer algorithm, and are divided into uniformly distributed random numbers, normally distributed random numbers and lognormal distributed random numbers, among which uniformly distributed random numbers are particularly important [10]. Pseudo-random number generation methods based on uniform distribution include linear congruency method, middle square method, and random number function of calling high-level languages [11]. Pseudo-random number generation is efficient but periodic. Application of pseudorandom number in network communication security Although the period is large enough to extract part of the sample can not effectively calculate the rest of the random sequence, but if the random seeds and algorithms are known, the random sequence can be easily calculated, so the security of pseudorandom number is low.

Truly random number can obtain random data from hardware by sampling chaotic system. For example, high-speed true random number generator based on thermal noise oscillator, lightweight and efficient true random number generator based on ring oscillator, etc. True random number is obtained by some random events outside. Its randomness is a kind of physical randomness without cycle. Although its generation cost is high, even if the truly random number generation method is obtained, it cannot predict the random sequence, so it has high security. Pseudo-random numbers are matched with true random numbers as shown in Table 2: True random numbers are not as easy and efficient to generate as pseudo-random numbers, but their random numbers are of high quality and cannot be cracked theoretically.

1.3 Network Security Requirements for Random Numbers

The repeatability of pseudorandom number brings great threat to network security. Nowadays, with the rapid development of network communication technology, it is no longer realistic to use pseudorandom number to ensure the security of network communication. To ensure secure network communication, the random numbers used must be difficult or even impossible to crack. Compared with pseudo-random numbers, true random numbers cannot be predicted or repeated, which greatly improves the security of network communication. True random numbers must be used in situations with high security requirements, such as e-commerce, LAN, computer software [10], etc. In the long run, truly random numbers play an important role in maintaining the security of network communication.

2. TRUE RANDOM NUMBER GENERATOR AND ITS IMPORTANCE TO NETWORK COMMUNICATION SECURITY

2.1 True Random Number Generator

Random number generator, namely the method of generating random numbers, can be divided into two categories: pseudo-random number generator and true random number generator [3]. Pseudorandom number generator (PRNG) is a mathematical algorithm that obtains pseudorandom numbers with statistical characteristics through fixed and repeated calculation. True random number generator (TRNG) is a kind of physical random by using uncertain physical sources to obtain true random sequence. Typical steps of true number generator are as follows: first extract random signals from physical source (entropy source), then sample random signals to generate random sequence, and finally use post-processing module to improve sequence quality. Among the entropy sources such as thermal noise, nuclear decay and cosmic radiation [4], thermal noise is the most widely used. In recent years, new true random number generators have emerged in an endless stream, and portability has become a major advantage. Two types of true random number generators are described below: traditional true random number generators based on thermal noise oscillators and new true random number generators based on ordinary smartphone cameras [3, 12].

2.1.1 True random number generator based on thermal noise oscillator

There are three main circuit design methods of true number generator based on thermal noise: metastable sampling, thermal noise amplification and ring jitter [13], among which true random number generator based on ring jitter has been widely studied by predecessors. This kind of true random number generator can generate true random sequence efficiently, and provide high quality true random number continuously for key generation, so as to effectively ensure the security of network communication. In this paper, a high speed true random number design based on thermal noise oscillator is introduced：

Table 2: Comparison between pseudo-random numbers and true random numbers

Random number	Periodicity	Safety	Generation difficulty	Generating efficiency
Pseudo-random numbers	Yes	Low	Low	High
True random number	No	High	High	Low

The random source of the oscillator-based random number generator is phase noise or jitter in the CMOS ring oscillator, which is mainly caused by the thermal noise of the transistor in the ring oscillator [12]. This kind of true random number generator uses a high and low frequency oscillator to sample the noise source, that is, a low frequency oscillator with jitter is sampled through a D flip-flop to a high frequency oscillator with a fixed period. Oscillator jitter is the source of uncertainty at each sampling time [14], so that the output sequence is physically random and a truly random number sequence is generated.

Hardware is the best source of high-quality random numbers, and the best method to generate random numbers by computer is to transform the unpredictable physical random sequence from the outside into the input initial sets of a real random number generator. It is inherently random and can quickly generate random sequences for high security purposes. However, the cost of using such hardware is very high and it is not suitable for the application of personal network communication encryption.

2.1.2 True random number generator based on ordinary smartphone camera

True number generator based on thermal noise oscillator can generate true random sequence more efficiently, but it needs expensive professional peripheral hardware equipment, and can not be popularized in a short time. In recent years, some new true random number generators have been proposed. In this paper, we will discuss a new portable true random number generator based on the common smart phone camera. This kind of true random number generator does not require high hardware facilities and is portable and easy to operate. It is suitable for the security and encryption of network communication at the personal level. The true random number generator structure is shown in Figure 1.

The operator presses his thumb on both the image sensor and the flash at the same time. The light from the flash is evenly attenuated, resulting in a raw image with a moderate signal-to-noise ratio on the image sensor. The original random number sequence can be obtained by extracting the red pixel of the original image and conducting a series of post-processing on the gray level. The moderate signal-to-noise ratio of the image ensures the good randomness of the scattered particle noise of photocurrent. After testing, this method can produce truly random number sequences with good randomness [15].

The concept of true random number generator is novel and portable, which effectively solves the problem of high hardware requirements of true random number generator, but the disadvantage is that it is difficult to generate random sequences continuously.

2.2 Security Analysis of True Random Numbers in Network Communication Security

From the above introduction of true random number generator, we can know that even if the true random number generator is operated repeatedly, due to the physical randomness of the entropy source, it is impossible to input exactly the same entropy source, so that the true random number sequence cannot be reproduced. Random numbers used in encryption must satisfy the following three basic characteristics:

(1) Unpredictability: random sequence cannot be predicted before it is generated, that is, random sequence cannot be deduced by generating method and random source;

(2) Cannot be repeated: random sequences cannot be periodic, that is, repeated random sequences cannot appear, and the results produced by repeated experiments cannot be repeated;

(3) Can pass random statistical test: Random numbers that meet encryption requirements must pass random statistical test, which commonly include frequency test, follow characteristic test and run test [15].

The security of communication data transmission and storage in the network environment is collectively referred to as network information security [10]. Cryptography is the most effective weapon to ensure the security of network communication. Random number is the cornerstone of cryptography. The quality of random number determines the encryption strength.

In view of the above characteristics, although the traditional pseudorandom number can increase the period to make it unpredictable to a certain extent, the random sequence can be repeated once its seed and generation algorithm are known. This feature of pseudorandom number brings great security risks to network communication. True random numbers are independent in time, uniform in space, random in statistics, and unrepeatable and unpredictable. The superiority of true random number shows that it is more important in the application of network communication security. Therefore, although the above traditional true random number generator involves high hardware requirements and high cost, the new true random number generator reduces the hardware requirements and the generation efficiency of random sequence, but it still cannot prevent the increasing importance of true random number in network communication security.

2.3 The Development Prospect of True Random Number for Network Communication Security

True random number has the advantages of unpredictability and cannot be repeated. In Applied Cryptography, an authoritative work on computer security, there are a total of 61 cryptographic protocols, including more than 40 protocols using random numbers [15]. In the environment of network communication, with the rapid improvement of computer performance, the research into random number generation algorithms is gradually deepening, and the use of true random number generation algorithm has become a trend. When maintaining the security of network communication, using true random number to encrypt the security of network communication can effectively improve the security of software, protocol and service using true random number generator.

3. CONCLUSION

With the rapid improvement of computer performance, the security of some pseudo-random number generation algorithms is threatened. Once the pseudo-random sequence is cracked, the software, protocols, and services based on the pseudo-random number generator are no longer secure. By analyzing network communication security problems and countermeasures, this paper comprehensively considers the requirements of network communication security on random numbers, and compares pseudo-random numbers with true random numbers in terms of generation methods, quality of random numbers, cost of generation and efficiency. It can be seen that true random numbers are not as efficient as pseudo-random numbers in terms of generation, but their quality is much higher than that of pseudo-random numbers. Since the randomness of true random number is a kind of physical randomness, which is unpredictable and cannot be reproduced, the key generated by using true random number cannot be cracked theoretically. True random numbers must be used in situations requiring high security intensity, such as e-commerce, computer software, local area network, etc. True random number greatly reduces the probability of security risks in network communication and improves the security level of network communication. Therefore, true random number has high application value in ensuring the security of network communication.

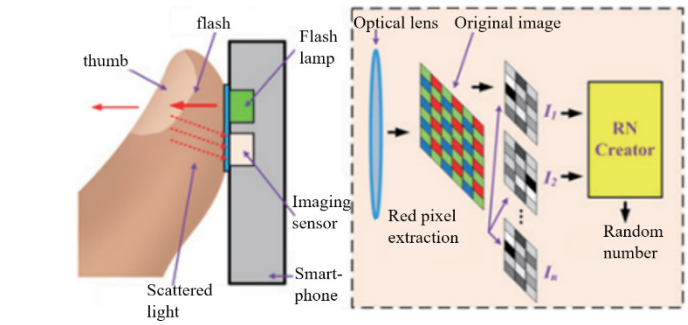

Figure 1: Schematic diagram of portable TRNG based on image sensor (reference figure)

ACKNOWLEDGEMENT

China University of Mining and Technology-Beijing College Student

Innovation training project. This was supported by the special Funds for basic scientific Research for central universities. School-level project number: 202204087

REFERENCES

[1] Huang, F. 2008. Research on the Security of Random Numbers in Network Environment. Science and Technology Information (Science Teaching and Research), (16), 391-393.

[2] Hao, W., LV, L. 2022. RFID Tag Ownership Transfer Protocol based on Pseudorandom Number Generator. Microcomputer application, 38(11), 11-14.

[3] Lu, Y., Han, Q., Liu, X., Yao, L. 2023. True Random Number Generator Based on Configurable Asynchronous Feedback Ring Oscillator[J/OL]. Journal of Electronic Measurement and Instrumentati on:1-9[2023-02-13].

[4] Xue, Y., Lv, S., Guo, S. 2003. Random Number Generator Analysis and Its Application in Security Information System. Computer Engineering, (03), 42-44.

[5] Su, G., Lv, S., Yang, Z., Xue, Y. 2002. Application of Randomness of True Random Number Generator to Information Security. Computer Engineering, (06), 114-115.

[6] Wei, K. 2022. Application of Data Encryption Technology in Computer Network Communication Security. China New Communication, 24(24), 1-3.

[7] Zhang, M. 2022. Application of Data Encryption Technology in Computer Network Information Security. Journal of Jiamusi Vocational College, 38(12), 152-154.

[8] Li, B. 2021. Discussion on asymmetric encryption and its Application. Information Recording Materials, 22(01), 214-215.

[9] Zhao, K. 2021. Random Number Research and Application Based on VFP. Journal of Shangqiu Vocational and Technical College, 20(04), 74-78.

[10] Wu, F. 2006. Several Methods for Generating Random Numbers and Their Applications. Numerical Computation and Computer Applications, (01), 48-51.

[11] Yang, W., Wu, G. 2007. Several Pseudorandom Number Generators and Their Applications in WEB. Microcomputer application, (02), 57-60+6.

[12] Wei, Z., Fu, L., Wang, X., et al. 2018. A High Speed truly Random Number Design Based on Thermal Noise Oscillator. Application of Electronic Technology, 44(10), 29-31+36.

[13] Ou, H., Zhao, J., Yu, H., Hu, X., Li, Q. 2011. Research on True Random Number Generator Based on Oscillator. Communication Technology, 44(12), 153-155+158.

[14] Wang, P., Li, Z., Li, G., Cheng, X., Zhang, H. 2019. Design of True Random Number Generator Based on Voltage-controlled Oscillator. Acta Electronica Sinica, 47(02), 417-421.

[15] Liu, Y., Tang, Z. 2018. Brief Introduction of a New Portable True Random Number Generator. Computer Products and Circulation, (09), 112+115.