Research on the Scrambling and De-scrambling Technique of Pseudo-random Sequences Based on Linear Feedback Shift Register

Jiale Li

College of Mathematics and Physics, Beijing University of Chemical Technology, Beijing, 102202, China
Corresponding author: 2021050172@buct.edu.cn

Abstract:

With the rapid development of communication technology, the security and reliability of signal transmission and anti-interference ability have become a key challenge. Aiming at the problems, this paper deeply studies the scrambling and de-scrambling technique of pseudo-random sequences, and designed the corresponding circuit to better understand the working mode of each step. In this study, the design and implementation of the scrambling and de-scrambling technique of pseudo-random sequences circuit is carried out through Verilog language, and the advantages and disadvantages of the designed circuit are analyzed in detail and the improvement scheme is obtained. In addition, this study also compares and analyzes the advantages and disadvantages of the scrambling and de-scrambling technique of pseudo-random sequences and the scrambling and de-scrambling technique of self-synchronizing, which provides a reliable basis for selecting appropriate technical solutions in practical application scenarios. This study provides theoretical support and reference for the design of communication systems, and looks forward to the future development direction of the scrambling technology, including the development of more efficient algorithms, the exploration of adaptive techniques, and the development of low-power solutions.

Keywords: Verilog; scrambling and de-scrambling technique; pseudo-random sequences; linear feedback shift register; self-synchronizing.

1. Introduction

With the continuous progress of science and technology, communication technology is playing an increasingly important role in production and life around the world. The communication system has achieved a qualitative leap in terms of transmission rate and capacity, which has brought great convenience to people's production and life. However, in this process, the reliability, security and anti-interference ability of signal transmission have become urgent problems in the communication field. Therefore, scrambling code and decoding technology has become an indispensable technical means in digital communication systems. As an effective means to improve communication quality, ensure information security and enhance system performance, scrambling and de-scrambling techniques have been widely used in wireless communication, satellite communication, fiber communication CDMA communication systems, and other fields [1]. For example, in 4G LTE and 5G NR systems, scrambler technology successfully distinguishes the data streams of different users and improves the capacity and user experience of the communication system [2]. However, scrambling and de-scrambling techniques bring many advantages to communication systems but also face certain challenges. How to further improve the reliability, security and anti-interference ability of signal transmission has become a hot topic in the field of communication. As an effective solution, the scrambling and de-scrambling technique of pseudo-random sequences has better anti-interference performance and lower bit error rate, so it has gradually become an important choice for communication system design [1].

In order to deeply understand the scrambling and de-scrambling technique of pseudo-random sequences, this paper will use Verilog language for circuit design and implementation. Through the design and implementation of the pseudo-random sequence dereferencing circuit, the working principle of each step of the scrambling and de-scrambling technique of pseudo-random sequences can be deeply understood. At the same time, aiming at the shortcomings of the designed circuit, an improved scheme is proposed to provide a reference for the design of communication system. In addition, this paper will compare and analyze the advantages and disadvantages of the scrambling and de-scrambling technique of pseudo-random sequences and the scrambling and de-scrambling technique of self-synchronizing. The comparison of the two technologies in terms of performance, complexity and application scenarios, provides a basis for selecting

the appropriate technical scheme in the actual application scenario. It is hoped that this study can provide theoretical support for future communication system design and further promote the development of scrambling and decoding technology.

2. Theoretical Basis

2.1 Scrambling and De-scrambling

Scrambling and de-scrambling technique is the core technology of digital communication systems, which can be used to improve the reliability, security and anti-interference ability of signal transmission. Scrambling code technique effectively reduces the periodicity of the signal by randomizing the original data, making it more difficult to predict and analyze, to improve the reliability of signal transmission [3]. The de-scrambling code technique is responsible for restoring the scrambled signal to the original data and can detect and correct errors, to further improve the accuracy of signal transmission [3].

Scrambling and de-scrambling techniques mainly include two types, namely the scrambling and de-scrambling technique of pseudo-random sequences and the scrambling and de-scrambling technique of self-synchronizing. The scrambling and de-scrambling technique of pseudo-random sequences uses pseudo-random binary sequences (PRBS) generated by linear feedback shift registers(LFSR) to realize data scrambling and de-scrambling. Its periodic and random characteristics help to improve the spectrum characteristics of signals, enhance the anti-fading ability of signals, and improve the security of communication systems [4]. The scrambling and de-scrambling technique of self-synchronizing simplifies the synchronization process, realizes the automatic alignment of the de-scrambling process and the scrambled signal, and does not need precise synchronization between the transmitter and the receiver. This technique is easy to implement and can effectively adapt to time-varying characteristics [5].

In this study, the scrambling and de-scrambling technique of pseudo-random sequences will be taken as the main research goal.

2.2 Scrambling and De-scrambling Technique of Pseudo-random Sequences

The scrambling and de-scrambling technique of pseudo-random sequences is the generation and application of PRBS, and it realizes the data scrambling and unscrambling process. In the scrambling phase, the source data stream is XOR operated with its PRBS with significant periodicity and randomness, thus transforming into a randomized data stream. In this process, the periodicity of the signal is effectively reduced and the reliability of signal transmission is improved [4]. In the de-scrambling phase, the original data is recovered by using the same PRBS at the receiver and the same PRBS at the transmitter for XOR operation [4]. To ensure the correctness of the decoder, the receiver and the transmitter should be synchronized and use the same initial LFSR value and polynomial.

3. Circuit Design and Implementation

In order to design the pseudo-random deranging circuit, the core part of the circuit is studied and analyzed. The scrambling and de-scrambling technique of pseudo-random sequences circuit includes the scrambler and descrambler. The scrambler of the scrambling and de-scrambling technique of pseudo-random sequences is based on LFSR. The input data and LFSR internal register data are XOR-operated to generate a pseudo-random sequence and output the scrambled data [6]. The descrambler of the scrambling and de-scrambling technique of pseudo-random sequences utilizes the characteristics of XOR operation to perform XOR operation between the pseudo-random sequence output by the scrambler and the same LFSR data, so as to recover the original data [6]. The scrambler and descrambler of the scrambling and de-scrambling technique of pseudo-random sequences can use the same module characteristics, and the design only needs to ensure that the two use the same LFSR initial value and polynomial to achieve synchronization and de-scrambling. The preliminary design logic design block diagram of the scrambling and de-scrambling technique of the pseudo-random sequences circuit is shown in Figure.1.

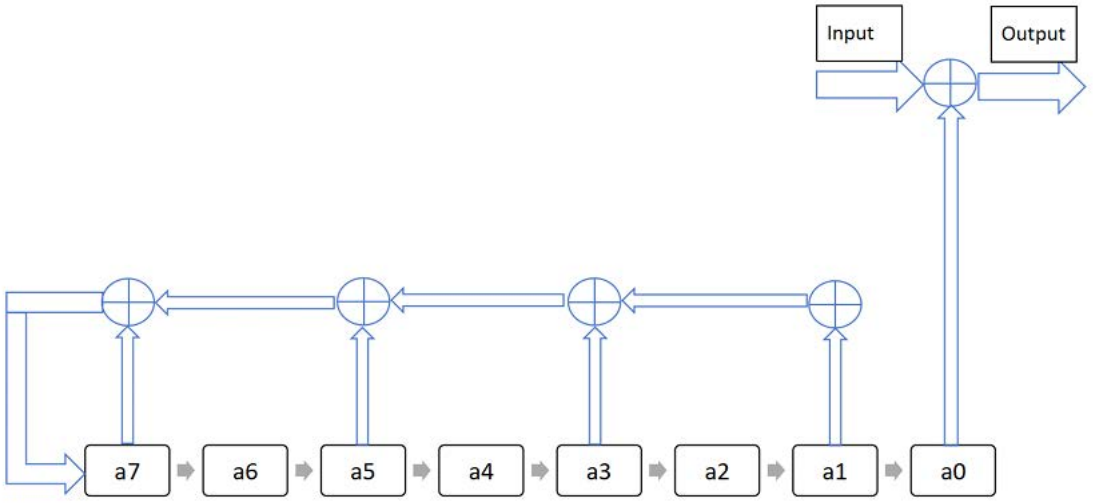

Figure.1 The preliminary design block diagram of pseudo-random sequence de-scrambling

According to the logic of Figure 1, this study uses Verilog language to write the corresponding scrambling and de-scrambling technique of pseudo-random sequences circuit. The circuit is configured with four input ports and an output port. 'clk' is the input clock signal. 'rstn' is the reset signal (effective at low level). 'en' is the enable signal. And 'din' is the input data port. The output port dout is responsible for the output of the processed data. The circuit contains an eight LFSR. The register as shown in figure.1 XOR and shift logic configuration. Completed by the circuit logic function as shown in table 1. The pin of the circuit diagram is shown in figure.2.

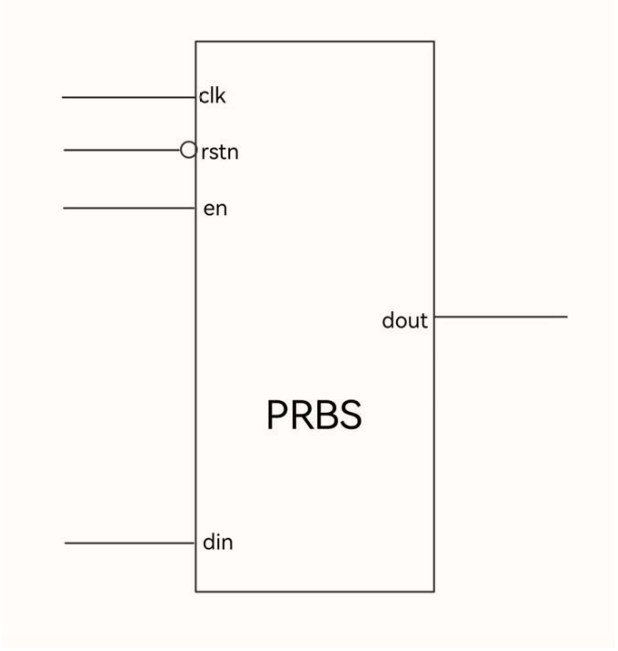

Figure. 2 Pin diagram of the scrambling and de-scrambling technique of pseudo-random sequences circuit

Table 1. Written circuit logic function table

rstn	en	din	dout
0	X	X	0
1	0	0	0
1	0	1	1
1	1	0	right[0]
1	1	1	~right[0]

To verify whether the written circuit can work correctly, the above code is simulated and verified. Start by writing a testbench that refers to the design code. It should cover all functional logic table entries to ensure that there is no omission in the simulation, so as to fully verify the correctness of the coding circuit. After the testbench is written, Modelsim is used for high-precision simulation to capture signal changes, verify whether the circuit behavior accurately matches the design expectation, and obtain the corresponding waveform diagram. By comparing the simulation waveform with the design logic table, the correctness of the circuit output is verified intuitively.

As shown in Figure 3, the written circuit and testbench are compiled successfully, that is, the written circuit design and testbench have no errors.

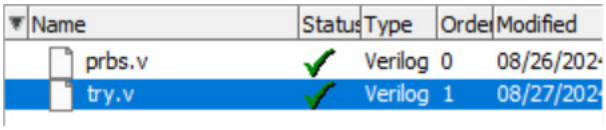

Figure. 3 The Verilog design and testbench compile successfully

As shown in the figure.4, testbench simulation success, each port corresponding simulation results are obtained.

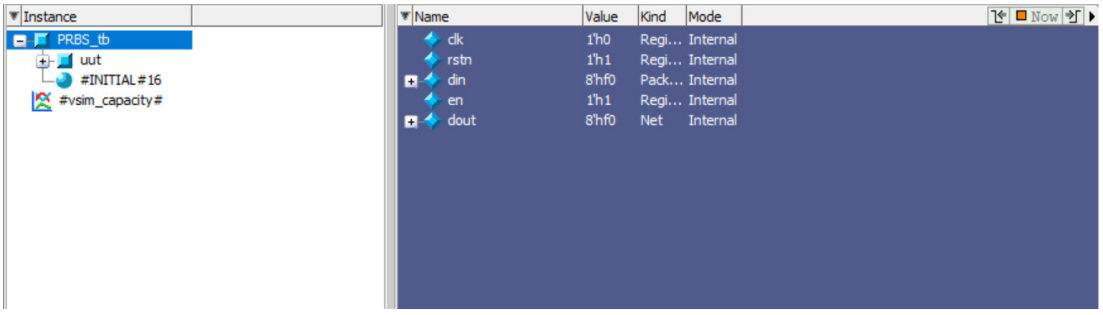

Figure. 4 Testbench simulation is successful

As shown in Figure 5, all ports get the corresponding waveform figure. Comparing and analyzing the waveform in Figure 5, the simulation verifies the completion of the expected operation target. This verifies the correctness of the written scrambling and de-scrambling technique of pseudo-random sequences circuit.

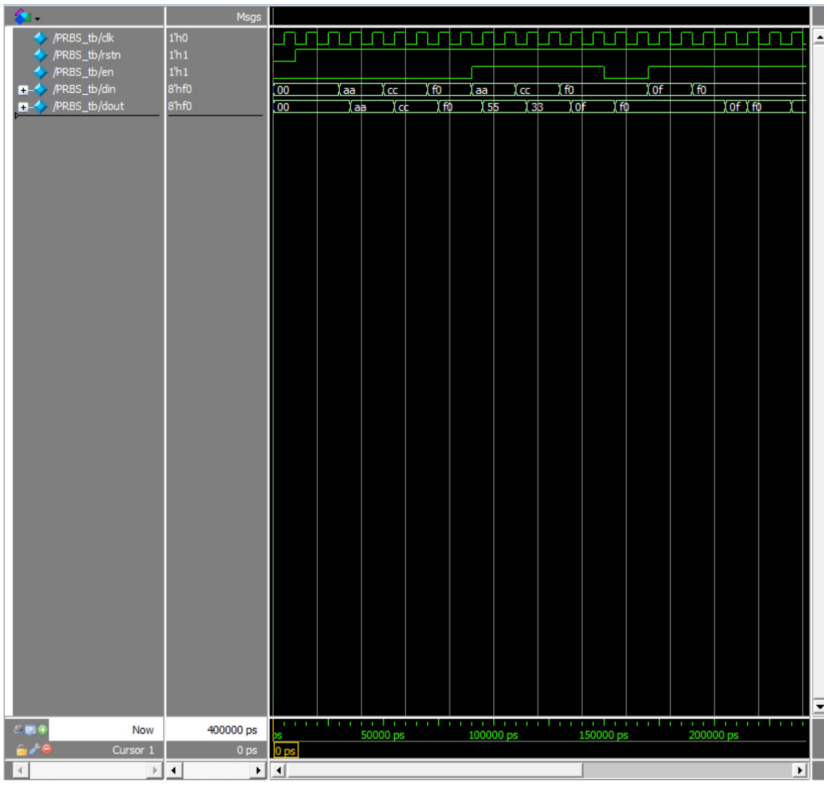

Figure. 5 Testbench simulation result waveform

4. Analysis and Improvement of Scrambling and De-scrambling Technique Circuit Design

The advantages of the existing scrambling and de-scrambling technique of pseudo-random sequences circuits include the ability to generate pseudo-random sequences that conform to specific mathematical laws. By using generate loops, its extensibility allows the generation of PRBS sequences of higher bits. At the same time, the modular design principle of the code ensures the clarity of the structure and easy maintainability. In addition, although multiple always blocks are involved, the design of the technique allows for independent control of each bit, which improves overall resource efficiency while maintaining efficient resource utilization.

The existing scrambling and de-scrambling technique of pseudo-random sequences circuit designs have some performance limitations, and the use of multiple always blocks may lead to performance degradation, especially in high bit rate applications. At the same time, the propagation delay mismatch of clock edges or reset signals may cause timing problems. In addition, because the design of the scrambling and de-scrambling technique of pseudo-random sequences circuit is too simple, the scrambling confidentiality of the original data is not strong, and there may be information security problems. Finally, the technology usually uses serial data input, which limits its ability to process a large number of parallel data, so it cannot effectively scramble and descramble parallel data.

In order to improve the performance of the pseudo-random sequence de-scrambling technology, the subsequent research will be improved from the following aspects. Firstly, the design of LFSR was optimized to improve the unpredictability and linear complexity of the sequence by adding XOR operation and using more random initial data. Second, the number of input and output ports is increased to support parallel data processing. At the same time, the logic design is adjusted to adapt to the increase of input and output bits, so that the circuit has the ability to scramble and decode a large number of parallel data.

5. Comparison with the Scrambling and De-scrambling Techniques of Self-synchronizing

5.1 Scrambling and De-scrambling Technique of Pseudo-random Sequences

The advantages of the scrambling and de-scrambling technique of pseudo-random sequences include that it can effectively broaden the spectrum of the signal, reduce the influence of electromagnetic interference (EMI), and improve the reliability of signal transmission [7]. Pseudo-random sequences can increase the confidentiality of signal transmission, and it is difficult for unauthorized users to predict and copy scrambled sequences, thus improving the security of the communication system [7]. In parallel data transmission lines, the use of scrambling of pseudo-random sequences operation can effectively reduce the interference between lines, thereby improving the quality of signal transmission [7]. The structure of the scrambling and de-scrambling technique of pseudo-random sequences circuit is simple by using Linear LFSR, and its construction and integration process is simple and easy [7]. However, this technique also has drawbacks, such as the strict synchronization of scrambling and de-scrambling operations [8]. At the same time, scrambling and de-scrambling processing is required in the process of scrambling and de-scrambling, which will further increase the complexity and cost of the system [8].

5.2 Scrambling and De-scrambling Technique of Self-synchronizing

The advantage of the scrambling and de-scrambling technique of self-synchronizing is that it does not need precise synchronization between the transmitter and the receiver, and the de-scrambling process can automatically synchronize with the scrambled signal, thus simplifying the system design [7]. In addition, this technique is easy to implement, especially at the hardware level, such as using a nonlinear feedback shift register (NLFSR), and has good adaptability to time-varying characteristics during signal transmission [7]. However, it also has some drawbacks. For example, the spectrum cannot be effectively broadened like pseudo-random sequence scrambling. There is a risk of spectrum leakage [9]. The secrecy is relatively low, and the synchronization mechanism may be easily analyzed and cracked [9]. At the same time, self-synchronization technology requires high signal quality, and the degradation of signal quality may affect the synchronization performance and increase the dereference error rate [9].

5.3 Suitable Scheme for the Actual Situation

To sum up, this study can conclude that the scrambling and de-scrambling technique of pseudo-random sequences and the scrambling and de-scrambling technique of self-synchronizing have their advantages and disadvantages, and are suitable for different scenarios. The scrambling and de-scrambling technique of pseudo-random sequences performs well in terms of spectrum expansion, security, and crosstalk reduction, but it requires a strict synchronization mechanism. The scrambling and de-scrambling Technique of self-synchronizing has the advantages of no

synchronization, easy implementation, and adapting to time-varying characteristics, but it is slightly inferior in spectrum broadening and security.

The two kinds of scrambling and de-scrambling circuits are suitable for different scenarios due to their different characteristics, and the choice should take into account the synchronization requirements, cost, complexity, and performance requirements [10]. The scrambling and de-scrambling technique of pseudo-random sequences is suitable for systems that require accurate synchronization and high performance and confidentiality, such as 4G LTE and 5G NR systems for mobile communication and GPS systems for satellite communication [2]. The scrambling and de-scrambling technique of self-synchronizing is simpler and lower cost, which is suitable for scenarios with limited budget or strict requirements for system complexity, such as Ethernet for LAN communication [2]. According to the actual application requirements, the proper scrambling and de-scrambling technique should be selected to optimize the system's performance and cost-effectiveness.

6. Conclusion

In this study, a simple pseudo-random sequence scrambling circuit is designed by Verilog language and verified by Modelsim simulation. The core principle of the circuit is deeply discussed, including the scrambling and de-scrambling mechanism and the application of LFSR. The effectiveness of LFSR in pseudo-random sequence generation and processing is verified, and the circuit optimization measures are proposed through comprehensive analysis. The research also compares the scrambling and de-scrambling technique of pseudo-random sequences with the scrambling and de-scrambling technique of self-synchronizing and clarifies the advantages, disadvantages, and application scenarios of each technology, which provides decision support for communication system designers. Although the research mainly focuses on the basic level and does not fully involve the complexity and depth of the technology, it verifies the feasibility and practicability of the scrambling and de-scrambling technique of pseudo-random sequences at the circuit implementation level, which provides an important reference for subsequent practical applications and technical optimization.

Looking into the future, the development of scrambling and de-scrambling technology can be explored from three aspects. Firstly, a more efficient scrambling algorithm was developed, and the speed and security were improved by using a complex LFSR structure and fusion cryptography principle. Secondly, the adaptive scrambling and de-scrambling technology is explored to realize the automatic adjustment of parameters to adapt to the channel state and transmission environment, and enhance the reliability of signal transmission. Finally, a low-power scrambling and de-scrambling scheme was developed to meet the needs of energy saving and consumption reduction in communication systems. The scrambling and de-scrambling technology is developing in the direction of more efficient, safer, and more reliable. This research provides the basic technical support for this, and expects to make greater contributions to the innovation and development of the communication field with the continuous progress of technology.

References

[1] Liu Shiqin. Laser network chaotic secure communication key technology research. University of electronic science and technology, 2023.

[2] Zhang Yang. Design and Networking of WCDMA Mobile communication System. Guizhou University, 2009.

[3] LI Changyu. A Trusted Secure Network Data Isolation Exchange System [C]// Tianjin Institute of Electronics. Proceedings of the 38th China (Tianjin) 2024 'IT, Network, Information Technology, Electronics, Instrumentation Innovation Academic Conference. Tianjin Optoelectronic Communication Co., 2024.

[4] Liu Yuming, YAN Shike. Conditional access system based on PRBS . Television Technology, 1997, (11): 25-28.

[5] Chen Tingting. Research and implementation of receiver circuit based on JESD204B protocol. Jiangnan university, 2022.

[6] Yi Maoxiang, ZHANG Hao, Guo Hongwei, et al. Scrambling technique of M-sequence data and its application in SATA. Microelectronics, 2012, 42 (04): 502-505

[7] Zhang Rui, Shao Chao. Comparison of two scrambling methods in Data domain of IEEE802.11 [J]. Journal of Xi 'an University of Posts and Telecommunications, 2012, 17 (04): 48-51

[8] Ruan Junbing. Design of scrambling and de-scrambling based on NB-IoT protocol. Modern Information Technology, 2018, 2 (05): 194-196.

[9] Ou Yangjing, Yao Yafeng, Huo Xinghua, et al. JESD204B agreement since synchronization add one circuit design and implementation of solutions. Journal of Electronic Design Engineering, 2017, 25 (7) : 148-151.

[10] He Dengping, Jiang Caoyong, Li Xiaowen, et al. Simulation and Implementation of Demodulation and de-scrambling Based on FPGA in TD-LTE System. Electronic technology applications, 2013, 39 (5): 4.