applied sciences

MDPI

Article

Analysis and Research on Secondary LT Coding Anti-Eavesdropping Scheme Based on LT Code Degree-1

Lizheng Wang [1], Fanglin Niu [1,*], Jingjing Jin [2] and Ling Yu [1]

[1] School of Electronics and Information Engineering, Liaoning University of Technology, Jinzhou 121001, China; wlz0831@163.com (L.W.); dx_yl@lnut.edu.cn (L.Y.)
[2] China Mobile Communications Group Limited, Chaoyang 122000, China; jinjingjing_cy@ln.chinamobile.com
* Correspondence: dx_niufl@lnut.edu.cn

Abstract: Fountain code can significantly increase eavesdroppers' untranslated efficiency in the wireless communication eavesdropping channel. The secondary LT coding anti-eavesdropping scheme with fountain code degree-1 is the subject of a theoretical investigation in this paper. The fact that its channel security capacity is greater than that of traditional LT code is first deduced from an information-theoretic standpoint, and the impact of source symbol length on decoding complexity and decoding overhead is then examined. The experimental results show that, compared with the traditional anti-eavesdropping twice fountain code, selecting long source symbols for double LT coding, when the main channel is better than the eavesdropping channel, can ensure that the eavesdropper has a higher untranslated efficiency, and can effectively reduce the fountain code decoding complexity and the number of encoded symbols sent by the source to improve the efficiency of information transmission.

Keywords: LT code; anti-eavesdropping; physical layer security; eavesdropping channel; delete channel

Citation: Wang, L.; Niu, F.; Jin, J.; Yu, L. Analysis and Research on Secondary LT Coding Anti-Eavesdropping Scheme Based on LT Code Degree-1. *Appl. Sci.* **2023**, *13*, 11296. https://doi.org/10.3390/app132011296

Academic Editor: Chilukuri K. Mohan

Received: 2 August 2023
Revised: 11 October 2023
Accepted: 12 October 2023
Published: 14 October 2023

1. Introduction

Wireless communication has taken over as the primary form of modern communication due to the quick development of mobile communication technology. It is essential to ensure the security of information transmission since the open channel environment of wireless networks makes it simple for unlawful eavesdroppers to obtain information. The majority of conventional anti-eavesdropping methods use cryptosystems; however, as the computing power of computers and other devices has steadily increased, the security of these secrecy systems has come under threat. As a result, the conventional secret key mechanism in wireless communications is facing significant difficulties.

Since the establishment of Shannon's information-theoretic security model [1] and the introduction of the wireless eavesdropping channel model [2] by Wyner, the secrecy capabilities of degraded eavesdropping channels has been defined based on information theory, which has laid the foundation for information theory for the development of physical layer security (PLS) technology. According to the definition of confidential capacity, confidential communication can be realized during the transmission of the eavesdropping channel when the channel capacity of the main channel is higher than the channel capacity of the eavesdropping channel. PLS now serves as a guarantee for wireless communications' information security transmission problems. Successively, the literature [3] investigated how secure communication can be performed over fading broadcast channels. According to the literature [4], a capacity realization encoding approach is suggested for the secure rate-limiting feedback link's eavesdropping channel, where the receiver can also feedback the random rate and provide an independently generated key to accomplish secrecy capacity. The literature [5] provides an overview of wireless communication's physical layer technologies, network architecture, and resource management. It also goes into detail on the ideal design of energy-saving wireless networks, which can actually drastically lower

the network's overall energy usage. Based on this, the literature [6] developed a methodical strategy for big data-sensing wireless networks with improved wireless service quality and innovative mobile applications, increasing the potential of wireless communication.

The majority of PLS technologies in use today aim to increase security capabilities. By enhancing the gap in signal quality between legitimate receivers and eavesdroppers, for instance, artificial noise, collaborative relaying, and other techniques can raise the rate of signal receipt for legitimate receivers. As an illustration, the literature [7] suggests a secure communication beamforming scheme based on signal-to-noise ratio, which aims to eliminate artificial noise at the legitimate receiving end by minimizing the signal-to-noise ratio of the unreliable relay nodes, maximizing its signal-to-noise ratio, and achieving the goal of preventing information eavesdropping. The literature [8] suggests an opportunistic fountain coding mechanism based on coordinated routing, in which each relay node does not have to restore all of the original packets but instead chooses a virtual node for packet forwarding and re-encodes the unrestored and restored packets of a single relay, improving the performance of multi-hop networks' transmission delay and reducing the decoding complexity.

Physical layer coding can significantly improve eavesdroppers' untranslated efficiency in noisy channels. Fountain code is an anti-eavesdropping code appropriate for physical layer communication. The longer the source coding symbol length, the smaller the decoding overhead, even near to 1. In the eavesdropping channel, there is a difference between the legitimate receiver and the eavesdropper in receiving the correct coding symbol, which is utilized as an anti-eavesdropping code to make it difficult for the eavesdropper to obtain the source information from it. In the literature [9], a coset precoding method is based on enhanced fountain codes to achieve strong communication security. Coset precoding prevents eavesdroppers from intercepting confidential information from leaked bits, and the main channel and the eavesdropping channel are both memoryless binary erasure channels. The literature [10] proposes a structure of repairable fountain codes in distributed storage systems, where random symbols are first added to the message, and then the message is encoded through the connection of Gabidulin codes and repairable fountain codes (RFCs) to design secure and repairable vector RFCs, i.e., the code symbols are distributed over storage nodes in order to theoretically achieve complete security. An improved distributed fountain coding method that has been suggested in the literature [11] uses a joint iterative optimization algorithm to optimize the degree distribution of sources and relays, improving the overall performance of all sources while also ensuring the reliability of the network by adding cooperative relays to mitigate the effects of undesirable channel conditions. The literature [12] uses rateless fountain code, Raptor code, equalizer, and chaotic interleaving technology in multi-user large-scale multiple-input multiple-output (MIMO) systems to enhance Bit Error Rate (BER) performance and throughput of a MIMO-Orthogonal Frequency Division Multiplexing-based system over multipath fading channels. In addition, the literature [13] on Industrial Wireless Sensor Networks (IWSNs) suggests a secure cooperative transmission strategy for IWSNs based on fountain codes, which combines cooperative jamming in the physical layer with fountain coding in the application layer, and designs a cooperative jamming method based on constellation rotation, so that the quality of the signals received by the eavesdropper deteriorates and the secrecy of the transmission is guaranteed. The literature [14] also proposes a recursive finite feedback online fountain code for the Underwater Acoustic Network system (UANs) that can lower bandwidth and energy consumption and restrict the number of feedback packets by decoding the progress threshold. This UANs data transmission mechanism improves in terms of overhead, computational complexity, and efficiency.

This is because digital fountain codes, which are more suited for wireless deletion channels because of their low decoding overhead, may efficiently conserve network resources and cut down on transmission delay. The Luby Transform (LT) code was first presented by Luby [15] in 2002, and it enhances LT code performance by increasing the likelihood that degree-1 coded packets with robust soliton distribution will be encoun-

tered during the decoding iterations. Later, a Shift-LT code (SLT code) was put forth in the literature [16], where the source side uses feedback data to modify the RSD degree distribution, which significantly reduces the compiled code complexity, memory usage, and overall energy consumption. Next, the literature [17] introduces a feedback LT coding scheme that, by adjusting the variable nodal degree, reduces the encoding time and average overhead, accelerates the convergence of the symbol BER curve, and significantly enhances the anti-eavesdropping effect. According to the literature [18], this fountain coding scheme can achieve a high intermediate decoding rate by using feedback information to predict the decoder state and dynamically adjusting the non-uniform symbol selection distribution. The literature [19,20] suggested modifying the LT code degree-1 and Online Fountain Codes without a build-up phase, respectively, by modifying the quantity of degree-1 coded symbols, doing away with the stacking phase, enhancing Belief Propagation (BP) decoding performance, and making sure that the received coded symbols are recovered as soon as possible. The degree distribution of the robust soliton distribution is then optimized in literature [21], and it is suggested to reorder the degree distribution from large to small in order to delay the emergence of degree-1 symbols. As a result, the decoding process is delayed, which is helpful for increasing the untranslated rate of the eavesdropper. According to the literature [22], an anti-eavesdropping method for the SLT-LT joint code is based on a collection of random symbols. The sender chooses a group of random symbols to send to the legitimate receiver as known symbols and cascades these random symbols with the message symbols to form the source symbols for cascade coding, which increases the eavesdropper's untranslated rate. The literature [23] devised an anti-eavesdropping channel coding method for the degree-1 symbols of LT code to LT coding again, so as to further improve the untranslated rate of eavesdroppers.

The communication information transfer rate can be efficiently increased thanks to the decreased decoding overhead. In this paper, the secondary LT coding anti-eavesdropping scheme for LT code degree-1 is analyzed theoretically from the security capacity, complexity, and decoding overhead. From the experimental results, it can be seen that this scheme can effectively reduce the coding complexity, and when used in the case of longer source symbols, it can effectively reduce the decoding overhead and improve the efficiency of the eavesdropper's untranslated rate.

The remaining portions of the research are structured as follows: The LT code and the secondary LT coding scheme based on LT code degree-1 are described in Section 2. The performance analysis of the secondary LT coding scheme is presented in Section 3. The associated simulation analysis is done in Section 4. The paper's conclusion is presented in Section 5.

2. LT Code Anti-Eavesdropping Method

2.1. LT Code

(1) LT Code Encoding

The source first packs k symbols into packets, which are then randomly encoded by the robust soliton distribution (RSD) degree distribution function into an infinite number of coded symbols. Then, Alice continuously sends these coded symbols to Bob through the main channel, Bob receives these coded symbols and performs BP decoding until enough coded symbols are received to recover the source information, Bob sends an ACK feedback to Alice to notify Alice of the completion of the decoding, and Alice immediately stops sending coded symbols after receiving the feedback. Additionally, the performance of the encoding method is directly impacted by the selection of the RSD degree distribution. Therefore, it is crucial to carefully consider how to design the degree distribution function.

(2) Deletion of LT Code Coding Matrix in the channel

According to Luby's theory [15], the Ideal Solitary Distribution (ISD) $\rho(d)$ and the enhancement factor $\tau(d)$ after normalization make up the Robust Soliton Distribution

(RSD) degree distribution function, and their corresponding mathematical formulas are as follows:

$$\rho(d) = \begin{cases} 1/k & d = 1 \\ \frac{1}{d(d-1)} & d = 2, 3, \cdots, k' \end{cases} \tag{1}$$

$$\tau(d) = \begin{cases} \frac{s}{k} \cdot \frac{1}{d} & d = 1, 2, 3, \cdots, (k/s) - 1 \\ \frac{s}{k} \ln(s/\delta) & d = k/s \\ 0 & d > k/s \end{cases} \tag{2}$$

where k represents the number of original symbols of the source, d represents the degree of encoded symbols, $s = c \ln(k/\delta)\sqrt{k}$, c is a constant ($c > 0$), and δ represents the maximum failure probability of decoding.

The RSD degree distribution function is normalized as follows:

$$\mu(d) = \frac{\rho(d) + \tau(d)}{z} \quad d = 1, 2, \cdots, k \tag{3}$$

where $z = \sum_d (\rho(d) + \tau(d))$.

The source symbols are grouped and d symbols from each group of k symbols are randomly selected for an XOR operation to obtain the LT coded symbols. The LT encoding matrix G is obtained according to the probability distribution function of Equation (3) as shown below:

$$G = \begin{pmatrix} 0 & 1 & \cdots & 0 & \cdots \\ 1 & 0 & \cdots & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & 0 & \cdots & 1 & \cdots \end{pmatrix}_{k \times \frac{a}{1 - P_{AB}}} \tag{4}$$

where "1" indicates the location of the corresponding selected source, p_{AB} denotes the main channel deletion probability, and a denotes the number of correctly decoded symbols participating in LT. The value of a is not fixed because LT encoding has a codeless rate, but it satisfies $a \geq k$.

$C = M \times G$ is the LT code encoding symbol. If a accurate symbols are needed for LT decoding, considering the impact of channel deletion probability, the actual number of encoding symbols received by the destination node is $m = \frac{a}{1 - P_{AB}}$.

2.2. Eavesdropping Channel Model

The three components of the eavesdropping channel are the source (Alice), the legitimate receiver (Bob), and the eavesdropper (Eve). The main (legal) channel is the one between Alice and Bob, whereas the eavesdropping channel is the one between Alice and Eve. Bob adopts the BP decoding method, while Alice uses LT code as the anti-eavesdropping channel coding. Bob continuously delivers the coded symbols to Alice across the main channel, and sends an ACK feedback to inform Alice of the completion of decoding when Bob recovers the source information. Due to the wireless channel's openness, we presume that Eve has obtained every decoding rule shared by Alice and Bob. While both are legally transmitting information, Eve can effectively steal the source information through the eavesdropping channel, and the same BP decoding is used. Figure 1 then displays the LT code eavesdropping channel model.

When Bob consistently gets enough coded symbols, BP decoding can be used to quickly recover the source information. The security of information transmission can be ensured as long as Bob receives enough coded symbols and finishes decoding before Eve. However, there is a higher probability of information leaking if Eve steals more coded symbols before Bob does.

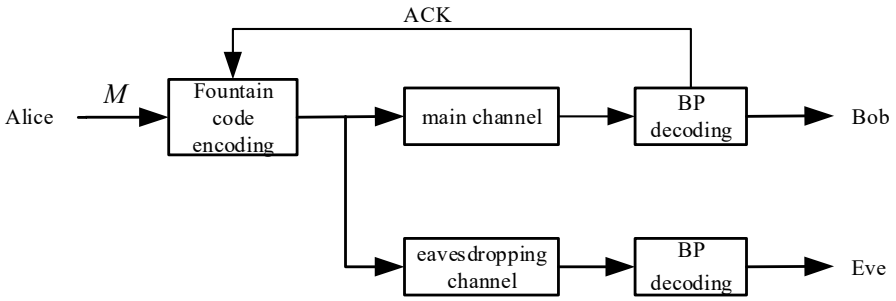

Figure 1. Eavesdropping channel model based on fountain code.

The channel security capacity is:

$$\begin{aligned} C_{S_{LT}} &= 1 - P_{AB} - (1 - P_{AE}) \\ &= P_{AE} - P_{AB} \end{aligned} \tag{5}$$

2.3. Anti-Eavesdropping Method Based on Degree-1 Secondary LT Coding

Based on the anti-eavesdropping channel premise of Figure 1, the source first LT encodes the overall symbols and then continues LT encodes the degree-1 symbols produced by it again, as shown in the literature [23]. The method is known as double LT code because it goes through two LT encoding processes. Figure 2 depicts its scheme model.

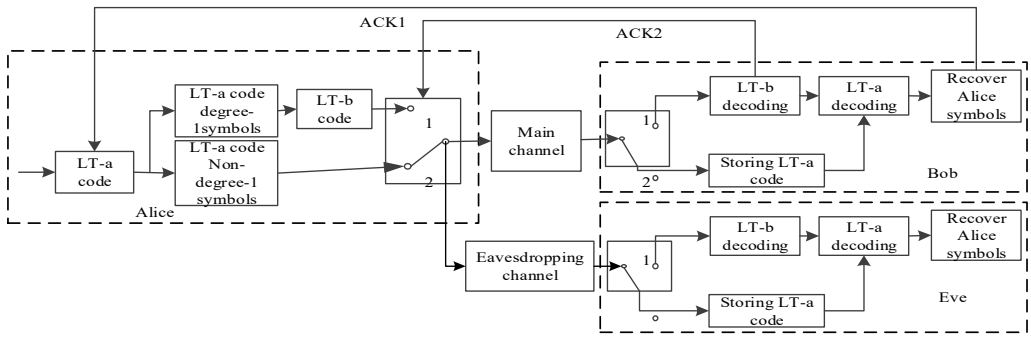

Figure 2. Double LT code anti-eavesdropping model based on degree-1.

In Figure 2, the source Alice first sends the LT-a code under the deletion channel from G of Equation (4), and sends the non-degree-1 encoding symbol of the LT-a code to Bob through the main channel. Bob receives it and stores it for later use. Meanwhile, Alice performs a secondary LT encoding of degree-1 symbols of the LT-a code, gets the LT-b code and continues to send it to Bob. When Bob receives the LT-b code, LT-b decoding begins, and continues until ACK2 is sent to Alice at the conclusion of decoding. Alice receives the feedback and instead sends a non-degree-1 symbol code of the LT-a code to Bob. At this point, Bob executes LT-a decoding using the recovered degree-1 symbols and the received LT-a code. Alice instantly stops transmitting any encoded data after the feedback message ACK1 is sent to it once all the decoding is finished. Meanwhile, during Bob's decoding process, Eve eavesdrops on the encoded symbols through the eavesdropping channel, and similarly decodes the degree-1 symbols after the LT-b code is decoded along with the LT-a code. However, due to the randomness of the fountain code, there is a difference between the main channel and the eavesdropping channel environments, which creates uncertainty in the eavesdropper's decoding, causing a difference in the degree-1 symbols decoded by Bob and Eve, and an even greater difference when continuing to decode with the LT-a code. The probability of Eve not yet completing the decoding increases when Bob finishes the decoding.

3. Program Performance Analysis

In this section, we examine the security capacity, decoding complexity, and decoding overhead for the double LT method to assess the security and reliability of system information transmission.

3.1. Security Capacity

The number of symbols sent by the source is k, and the channel deletion probability of the main channel and the wiretap channel are P_{AB} and P_{AE}, respectively, which are transmitted through a binary memoryless deletion channel. The channel security capacity C_s is described as maximizing the information transmission rate while ensuring security and is denoted as $C_s = \max R$.

As can be seen from 2.3, the double LT scheme is divided into two decoding stages. The first phase is the decoding of degree-1 symbols, in which Alice encodes degree-1 symbols to create the LT-b code (U-sequence) and sends it to Bob. Bob then receives the source symbols to obtain U_{Bob}. According to Shannon's Information Theory [1], Bob's information transmission rate R_{U_Bob} is:

$$R_{U\_Bob} = I(U; U_{Bob}) = 1 - P_{AB} \tag{6}$$

In the second stage, Alice encodes k symbols to form an LT-a code (S_U sequence) and sends it to Bob, and by utilizing the degree-1 symbol sequences that have been decoded in the first stage to be decoded together, Bob's information transmission rate R_{S_Bob} is satisfied:

$$\begin{aligned} R_{S\_Bob} &= I(S_U; S_{U\_Bob}) \times R_{U\_Bob} \\ &= I(S_U; S_{U\_Bob}) \times (1 - P_{AB}) \\ &= (1 - P_{AB})^2 \end{aligned} \tag{7}$$

Similarly, the eavesdropper eavesdrops through the eavesdropping channel to get Eve's information transmission rate R_{S_Eve} as:

$$R_{S\_Eve} = (1 - P_{AE})^2 \tag{8}$$

Setting parameter $S_r = (1 - P_{AE})/(1 - P_{AB})$, the safe rate R of the system is satisfied:

$$\begin{aligned} C_{S_{double\_LT}} &= \max R = R_{Bob} - R_{Eve} \\ &= (1 - P_{AB})^2 - (1 - P_{AE})^2 \\ &= (1 - P_{AB})^2 - {S_r}^2 (1 - P_{AB})^2 \\ &= (1 - P_{AB})^2 \left(1 - {S_r}^2\right) \end{aligned} \tag{9}$$

Due to $(1 - P_{AB})^2 > 0$, achieving $C_s > 0$ merely requires completing ${S_r}^2 < 1$. This ensures that the security capacity is greater than zero, thus guaranteeing the secure transmission of information. Then, to satisfy ${S_r}^2 < 1$, that is, $S_r < 1$, that is, $1 - P_{AE} < 1 - P_{AB}$, yields $P_{AB} < P_{AE}$. Therefore, in summary, we only need to satisfy that $P_{AB} < P_{AE}$, the legal channel environment is superior to the eavesdropping channel, and then necessarily $C_s > 0$, that is, the security capacity exists and is higher.

Next, the security capacity of the double LT code is simplified:

$$\begin{aligned} C_{S_{double\_LT}} &= (1 - P_{AB})^2 - (1 - P_{AE})^2 \\ &= ((1 - P_{AB}) + (1 - P_{AE})) \times (1 - P_{AB} - (1 - P_{AE})) \\ &= (P_{AE} - P_{AB})(2 - P_{AB} - P_{AE}) \end{aligned} \tag{10}$$

Since better channel conditions are taken into account in this paper's practical applications, both P_{AB} and P_{AE} take values less than 0.5; then, $2 - P_{AB} - P_{AE} > 1$, which results in $C_{S_{double\_LT}} > C_{S_{LT}}$. Even though the channel state condition of the eavesdropping channel is better than that of the legitimate channel, it still satisfies the larger security capacity of

the double LT method, which can theoretically be shown to have a larger security capacity than the traditional LT code.

3.2. Decoding Complexity

(1) Double LT fountain code decoding complexity

The fountain code uses the $\mu(d)$ distribution to obtain the coding matrix and the XOR computation to obtain the coded symbols, and the number of XOR calculations determines the size of the complexity of the compiled code. A computational approach to coding complexity is suggested in the literature [22]. The decoding complexity E is therefore correlated with the average degree $\overline{d}$ and the number of decoding symbols m_1. The following is the mathematical expression:

$$E = m_1 \cdot (\overline{d} - 1) \tag{11}$$

Due to the low decoding overhead of the fountain code, the number of decoded symbols $m_1 = k + e$, and e can be an arbitrarily small number greater than zero. Then, from Equation (11), the decoding complexity E_{LT} of LT code is obtained:

$$E_{LT} = (k+e)\left(\overline{d_{LT}} - 1\right) \approx k\left(o\left(\ln\frac{k}{\delta}\right) - 1\right) \tag{12}$$

The E_{double_LT} complexity in the double LT approach is divided into two sections, LT-a code and LT-b code:

$$E_{double\_LT} = E_{LT-a} + E_{LT-b} \tag{13}$$

LT-a, the first LT encoding process needs to complete decoding for k symbols, and the decoding complexity E_{LT-a} can be obtained from Equation (12):

$$E_{LT-a} = k(\overline{d_{LT}} - 1) \tag{14}$$

LT-b is the secondary LT encoding for the $k \cdot u(1)$ degree-1 symbols in LT-a after extraction, and the decoding complexity E_{LT-b} can be obtained from Equation (12):

$$E_{LT-b} = k \cdot u(1)(\overline{d_{LT-b}} - 1) \tag{15}$$

where $\overline{d_{LT-b}}$ denotes the average degree of participation of $k \cdot u(1)$ symbols in the LT-b code and $u(1)$ is the probability of the degree-1 symbols.

In summary, substituting (14) and (15) into Equation (13) yields the decoding complexity E_{double_LT}:

$$\begin{aligned} E_{double\_LT} &= E_{LT-a} + E_{LT-b} \\ &= k\left(\overline{d_{LT_{(k)}}} - 1\right) + k \cdot u(1)\left(\overline{d_{LT_{(k \cdot u(1))}}} - 1\right) \\ &= k\left(o\left(\ln\tfrac{k}{\delta}\right) - 1\right) + k \cdot u(1)\left(o\left(\ln\left(\tfrac{k \cdot u(1)}{\delta}\right)\right) - 1\right) \end{aligned} \tag{16}$$

Obviously, from Equations (12) and (16), it can be seen that the decoding complexity of the double LT method is increased by $o\left(k \cdot u(1) \ln\left(\frac{k \cdot u(1)}{\delta}\right)\right) - k \cdot u(1)$ compared to the LT code, and increases with the increase in the k value.

(2) Comparison of decoding complexity of double LT fountain code with two other fountain codes

a. For the DEMR-LT fountain code [21], a twice LT code cascade coding was performed, and the decoding complexity is expressed as follows:

$$\begin{aligned} E_{DEMR\_LT} &= E_{LT} \cdot E_{LT_{(\frac{k}{1-P_{AB}})}} \\ &= k\left(\overline{d_{LT}} - 1\right) \cdot k\left(\overline{d_{LT_{(\frac{k}{1-P_{AB}})}}} - 1\right) \end{aligned} \tag{17}$$

Equation (17) shows that E_{DEMR_LT} increases with the increase in P_{AB}. When $P_{AB} = 0$, Equation (17) shows that:

$$E_{DEMR\_LT} = \left(k \cdot \left(\overline{d_{LT}} - 1\right)\right)^2 \tag{18}$$

In Equation (18), $k\left(\overline{d_{LT}} - 1\right)$ denotes the LT coding complexity, i.e., the number of XOR calculations during the coding process, k is chosen to be large in LT coding, and the number of XOR calculations is much larger than 2, which can be obtained from (18).

$$E_{DEMR\_LT} \gg 2k\left(\overline{d_{LT_{(k)}}} - 1\right) \tag{19}$$

In Equation (16), $u(1) \ll 1$, then, $k \cdot u(1)\left(\overline{d_{LT_{(k \cdot u(1))}}} - 1\right) \ll k\left(\overline{d_{LT_{(k)}}} - 1\right)$.

$$\begin{aligned} E_{double\_LT} &= k\left(\overline{d_{LT_{(k)}}} - 1\right) + k \cdot u(1)\left(\overline{d_{LT_{(k \cdot u(1))}}} - 1\right) \\ &\ll 2\left(\overline{d_{LT_{(k)}}} - 1\right) \end{aligned} \tag{20}$$

Comparing Equations (19) and (20), it is clear that $E_{double\_LT} \ll E_{DEMR\_LT}$ and the double LT fountain code is much smaller than the decoding complexity of the DEMR-LT fountain code.

b. For the SLT-LT fountain code [22], the same twice fountain code cascade coding is performed with the length of the participating decoded symbols as $k + n$ and $P_{AB} = 0$. The decoding complexity is expressed as follows:

$$\begin{aligned} E_{SLT\_LT} &= E_{SLT} \cdot E_{LT} \\ &= k\left(\overline{d_{SLT}} - 1\right) \cdot k\left(\overline{d_{LT}} - 1\right) \end{aligned} \tag{21}$$

$k\left(\overline{d_{SLT}} - 1\right)$ denotes the SLT coding complexity. With the same principle of Equation (19), the number of XOR calculations is much larger than 2. From Equation (18), it is then:

$$\begin{aligned} E_{SLT\_LT} &= E_{SLT} \cdot E_{LT} \\ &\gg 2 \cdot k\left(\overline{d_{LT}} - 1\right) \end{aligned} \tag{22}$$

From Equations (20) and (22), it follows that, $E_{double\_LT} \ll E_{SLT\_LT}$.

From the above analysis, it can be seen that the complexity of double LT is much lower than that of the other two methods for the same twice fountain code encoding.

3.3. Effect of the Length of the Source Symbol on the Decoding Overhead

In the decoding process, the ratio of the number of symbols m required to recover the source information to the original number of symbols k of the source is known as the decoding overhead ε, whose mathematical expression is:

$$\varepsilon = m/k \tag{23}$$

The number of overhead symbols needed to decode k symbols in LT code, according to the literature [15], is:

$$m_{LT} = k + o\left(\sqrt{k}\cdot \ln^2\left(\frac{k}{\delta}\right)\right) \tag{24}$$

where δ denotes the maximum decoding failure probability and δ is fixed.

The decoding overhead ε_{LT} is obtained from Equations (23) and (24).

$$\varepsilon_{LT} = 1 + o\left(\sqrt{k}\cdot \ln^2\left(\frac{k}{\delta}\right)\right)/k \tag{25}$$

Since LT-a in double LT is the LT code, the decoding overhead $\varepsilon_{LT-a} = \varepsilon_{LT}$.

LT-b decoding is LT encoding and decoding of $k\mu(1)$ degree-1 symbols, and the decoding overhead ε_{LT-b} is obtained from Equation (25):

$$\varepsilon_{LT-b} = \mu(1) + o\left(\sqrt{k\mu(1)}\cdot \ln^2\left(\frac{k\mu(1)}{\delta}\right)\right)/k \tag{26}$$

The total of LT-a code and LT-b code constitutes the double LT decoding overhead. The decoding overhead ε_{double_LT} of the double LT code method is obtained by adding (25) and (26):

$$\varepsilon_{double\_LT} = 1 + u(1) + \frac{o\left(\sqrt{k}\cdot \ln^2\left(\frac{k}{\delta}\right)\right) + o\left(\sqrt{k\cdot u(1)}\cdot \ln^2\left(\frac{k\cdot u(1)}{\delta}\right)\right)}{k} \tag{27}$$

The larger k is, the smaller $u(1)$ is from Equation (3), and the smaller $\left(o\left(\sqrt{k}\cdot \ln^2\left(\frac{k}{\delta}\right)\right) + o\left(\sqrt{k\cdot u(1)}\cdot \ln^2\left(\frac{k\cdot u(1)}{\delta}\right)\right)\right)/k$ is in Equation (27). Comparing Equations (25) and (27), $u(1) > 0$, obviously, $\varepsilon_{double\_LT} > \varepsilon_{LT}$.

It is clear from the aforementioned derivation that ε_{double_LT} is greater to ε_{LT}. However, as k rises, ε_{double_LT} moves closer to ε_{LT}.

4. Simulation Results and Discussion

The eavesdropping channel model structure is shown in Figure 2, the source is Alice, the legal receiver is Bob, and the eavesdropper is Eve. Assuming that Eve obtains all the decoding rules of Bob, and Bob is BP decoding, we can use this as the background for simulation experiments through matlab. The transmission group number is 5000, the source's original symbol number is k, and the values for the RSD degree distribution are $c = 0.03$ and $\delta = 0.05$. From Section 3.1, it is concluded that the experiment's values for channels P_{AB} and P_{AE} are less than 0.5.

4.1. Comparison of the Number of Symbols Sent by the Source

Under erase channel conditions, fountain codes are used as anti-eavesdropping codes, and the number of symbols sent by the source directly affects the message transmission rate. The scheme double LT of this paper is compared with the literature [21,22], respectively, to observe the effect of main channel variation on the number of encoded symbols sent by the source.

As can be seen in Figure 3, the number of encoded symbols sent by the source increases for all four schemes as P_{AB} increases. The number of double LT is smaller than in the literature [21,22] and larger than LT codes, respectively.

Double LT is the result of LT encoding its degree-1 symbols again on the basis of LT codes, and the number of double LT is slightly larger than that of LT codes. In contrast, the literature [21] encodes LT again for length $\frac{k}{1-P_{AB}}$ encoded symbols, and the literature [22] for length $\frac{k-n}{1-P_{AB}}$ encoded symbols, which increases the number of encoded symbols required for decoding more substantially. Therefore, comparing the number of encoded symbols sent by the source, double LT is smaller than the literature [21,22].

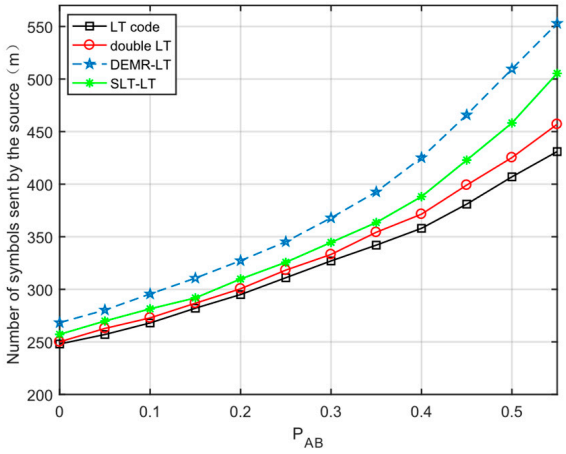

Figure 3. Effect of P_{AB} variation on the number of encoded symbols sent by the source.

4.2. Eve Untranslated Rate and Erase Channel Relationship

The scheme of this paper is compared with LT codes, in the literature [21,22], respectively, to observe the change in the eavesdropper $P_{eve\_undecode}$ under different schemes.

(1) Comparison of the effect of simultaneous changes in the main channel and the eavesdropping channel on the eavesdropper untranslated probability.

Compare the change in the eavesdropper $P_{eve\_undecode}$ under different schemes when $P_{AB} = P_{AE}$ is increased simultaneously.

From the experimental results in Figure 4, it can be seen that the probability of deletion in the channel is smaller as $P_{AB} = P_{AE}$ increases, and all four schemes increase with $P_{AB} = P_{AE}$. When the probability of deletion in the channel then reaches a certain value, the $P_{eve\_undecode}$ of the four schemes begins to have a decreasing trend. When $P_{AB} = P_{AE} > 0.18$, the $P_{eve\_undecode}$ of this paper's scheme is larger than in the literature [21] and LT codes, but smaller than the literature [21].

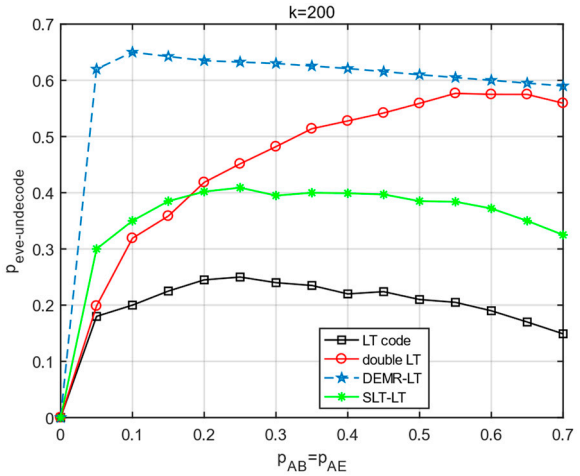

Figure 4. The effect of changes in the main channel and the eavesdropping channel on $P_{eve\_undecode}$.

(2) Comparison of the effect of the main channel change for the eavesdropper untranslated probability.

When $P_{AE} = 0.3$, P_{AB} increases, comparing the change in the eavesdropper $P_{eve\_undecode}$ under different schemes.

As can be seen from the experimental results in Figure 5, all four schemes decrease with increasing P_{AB}. The $P_{eve\_undecode}$ of the scheme in this paper is greater than the LT codes. Compared with the other three schemes, $P_{AB} \leq 0.28$ and the $P_{eve\_undecode}$ of this paper is smaller than the literature [21,22]; at $0.28 < P_{AB} < 0.32$, the $P_{eve\_undecode}$ of this

paper is larger than the literature [22]; at $0.32 \leq P_{AB}$, the $P_{eve\_undecode}$ of this paper is larger than the literature [21,22]. However, the $P_{eve\_undecode}$ of this paper's scheme is always greater than the LT codes, regardless of how the main channel is changed.

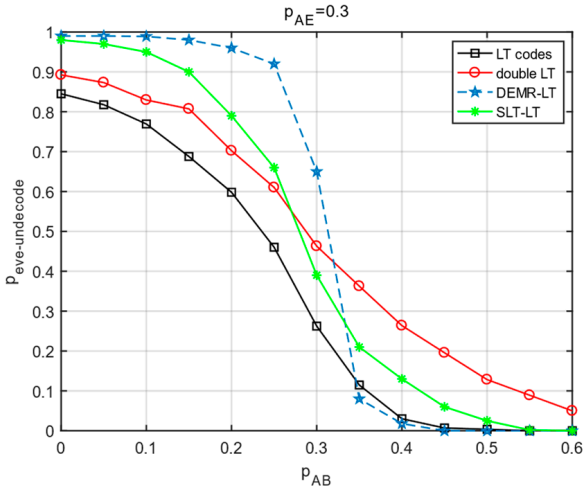

Figure 5. Curve of the main channel variation versus eavesdropper $P_{eve\_undecode}$.

(3) Comparison of the effect of the eavesdropping channel change for the eavesdropper untranslated probability.

When $P_{AB} = 0.3$ and P_{AE} increases, compare the change in the eavesdropper $P_{eve\_undecode}$ under different schemes.

As can be seen from the experimental results in Figure 6, all four schemes increase with the increase in P_{AE}. The $P_{eve\_undecode}$ of double LT codes are all greater than those of the LT codes. When P_{AE} is low, the $P_{eve\_undecode}$ of double LT is greater than that of the literature [21,22], and when P_{AE} increases to a certain value, the $P_{eve\_undecode}$ of double LT increases at a lower value than that of the literature [21,22], in that order.

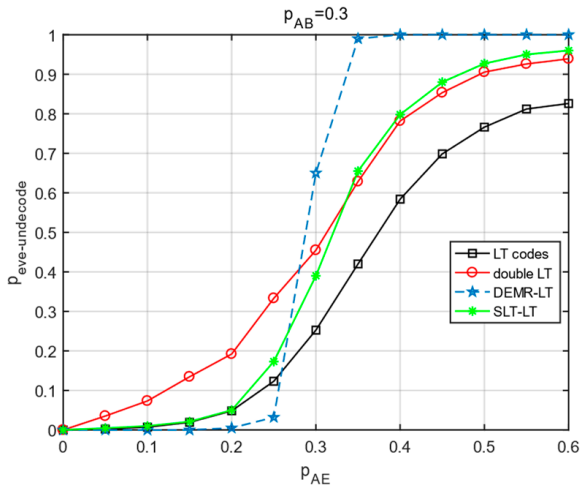

Figure 6. Curve of the eavesdropping channel variation versus eavesdropper $P_{eve\_undecode}$.

From the above experimental results, it can be seen that both double LT and the literature [21,22] are encoded by twice fountain code, which is equivalent to the receiver sending ACK to the source two times, increasing the number of times to intercept the eavesdropper to continue decoding, so the anti-eavesdropping effect is better than LT codes.

The coding schemes in the literature [21,22] both encode the overall source symbols with twice fountain codes, and as can be seen in Section 3.2, their coding complexity increases substantially. The number of encoded symbols required to be sent by the source

for decoding also increases substantially, as can be seen in Figure 3. Double LT requires a relatively low number and complexity of encoded symbols to be sent by the source for decoding since only degree-1 symbols are encoded for the second time. Compared with [21,22] schemes, although Eve's $P_{eve\_undecode}$ is not the highest, when the eavesdropping channel deletion probability is low and the eavesdropping channel is better than the main channel, then the double LT scheme can enable Eve to achieve a high untranslated rate. Therefore, this paper's scheme, double LT, also has a high application value.

4.3. Double LT Anti-Eavesdropping Capability Versus the Number of Original Symbols of the Source k

In double LT coding, the source symbol k is chosen to vary from 100 to 1000, and the effect of k on the decoding overhead ε is observed. Other experimental conditions are the same as above. The experimental results are shown in Figure 7.

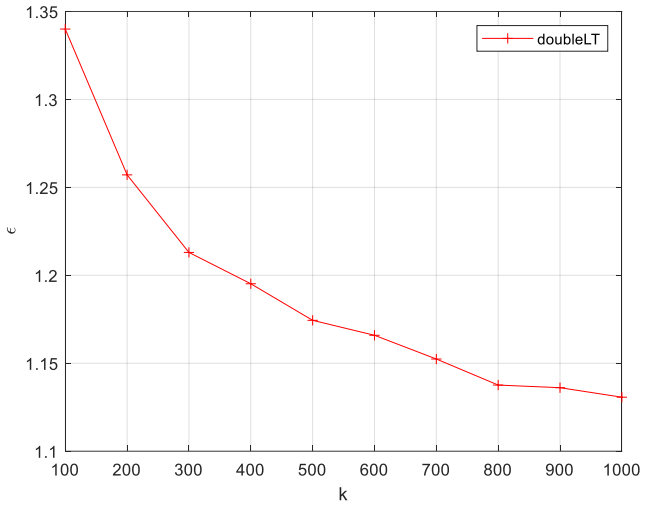

Figure 7. Relation curve between k and ε.

From Figure 7, it can be seen that double LT decreases with the increase in k. The experimental results are the same as the theoretical analysis in Section 3.3. Although the $\varepsilon_{dounble\_LT}$ of double LT is larger than the ε_{LT} of LT codes, the double LT $\varepsilon_{dounble\_LT}$ for $k = 1000$ is only 1.1427, which can be seen in the lower decoding overhead of long double LT.

Variation in the untranslated probability $P_{eve\_undecode}$ of Eve is under the variation in channel deletion probability for double LT with different code lengths. If the main channel deletion probability $P_{AB} = 0.3$, k is chosen to be 2000, 200, and 50, respectively. Observe the effect of the change in the deletion probability of the eavesdropping channel P_{AE} on $P_{eve\_undecode}$. The experimental results are shown in Figure 8.

From Figure 8, it can be seen that under the condition that the main channel $P_{AB} = 0.3$ remains constant, as the eavesdropping channel P_{AE} increases, the eavesdropper $P_{eve\_undecode}$ also grows larger, and at higher P_{AE}, $P_{eve\_undecode}$ gradually flattens out and will converge to 1. In the range where P_{AE} is (0,0.25), the change in k in the double LT scheme can have a small effect on the eavesdropper $P_{eve\_undecode}$, but it also has a certain anti-eavesdropping function. P_{AE} is (0.25, 0.5), and the eavesdropper's $P_{eve\_undecode}$ increases substantially as the source message length k increases in the double LT scheme.

Set the eavesdropping channel deletion probability $P_{AE} = 0.3$, and observe the effect of the main channel P_{AB} change on $P_{eve\_undecode}$. The experimental results are shown in Figure 9.

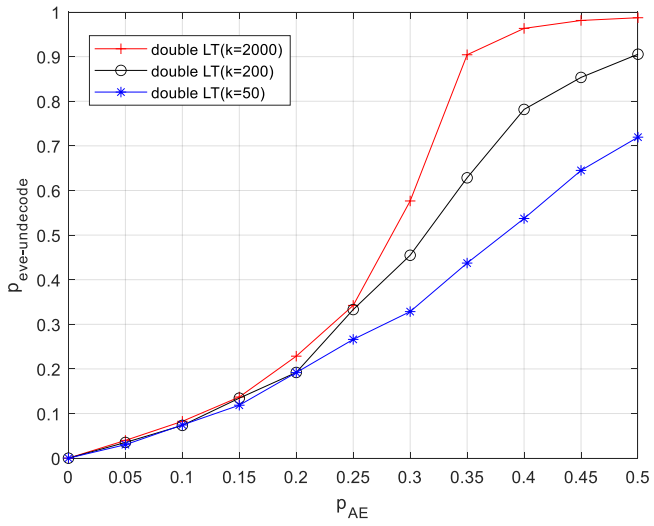

Figure 8. The effect of a change in the probability of eavesdropping channel deletion P_{AE} on $P_{\text{eve\_undecode}}$.

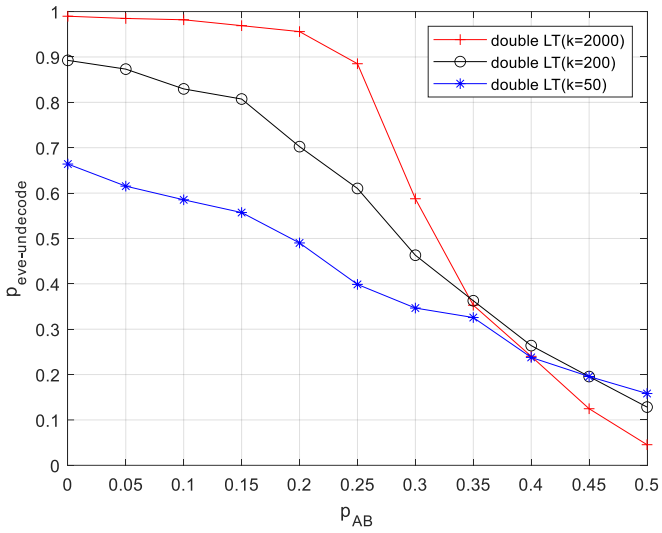

Figure 9. The effect of a change in the probability of main channel deletion P_{AB} on $P_{\text{eve\_undecode}}$.

From Figure 9, it can be seen that the eavesdropper's $P_{\text{eve\_undecode}}$ decreases as the main channel P_{AB} increases, regardless of what value k is. P_{AB} is (0, 0.35), and in the double LT scheme, as k increases, the eavesdropper's $P_{\text{eve\_undecode}}$ increases substantially. After $P_{AB} \geq 0.35$, $P_{\text{eve\_undecode}}$ begins to decrease as k increases.

The experimental results show that as the source message length k increases, the RSD has a higher degree-1 probability and a higher number of degree-1 symbols, increasing the secondary LT code source length. LT code uses BP decoding, which can only be decoded by receiving a large enough number of symbols. If Eve receives an insufficient number of symbols to be decoded in the process of BP decoding of LT encoded symbols of degree-1, there exists a large number of degree-1 symbols that can not be decoded, and the next step of BP decoding can not be carried out, resulting in an increase in the untranslated rate. However, when P_{AB} is slightly larger than P_{AE}, Eve receives a larger number of correctly encoded symbols than Bob, and can decode as long as it receives enough encoded symbols, the advantage of a long double LT is not present, and $P_{\text{eve\_undecode}}$ begins to decrease as k increases. Therefore, double LT with a larger number k of original symbols of the source is suitable to be used more effectively under conditions where the main channel is better or slightly worse than the eavesdropping channel.

5. Conclusions

From the above theoretical analysis and experimental results, it can be seen that the double LT method increases the number of times to intercept the eavesdropper's continued decoding due to the twice LT coding, effectively improves the channel security capacity, and improves the effect of anti-eavesdropping. Since this method performs secondary LT encoding on a smaller number of degree-1 symbols in the LT code, it reduces the number of encoded symbols required to be sent by the source for decoding and the complexity of coding compared to other secondary LT coding schemes. When the main channel is better or slightly worse than the eavesdropping channel conditions, due to the increase in the original symbols with the source, this effectively increases the number of symbols for the secondary LT coding degree-1. The number of symbols decoded by the eavesdropper is reduced, which improves the untranslated rate of the eavesdropper, and at the same time reduces the number of encoded symbols that need to be sent from the source for decoding, so the use of the long codes of the double LT code has a better effect in anti-eavesdropping.

Author Contributions: Conceptualization, L.W.; Methodology, L.W.; Software, L.W.; Validation, L.W.; Formal analysis, L.W.; Investigation, L.W.; Resources, L.W.; Data curation, L.W.; Writing—original draft, L.W., F.N. and J.J.; Writing—review & editing, L.W., J.J. and L.Y.; Visualization, L.W. and F.N.; Supervision, F.N.; Project administration, F.N. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Liaoning Provincial Education Department Fund (LJKMZ20220965, LJKZ0624).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: Author Niu, F. was employed by the Liaoning University of Technology. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
2. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
3. Liang, Y.; Poor, H.V.; Shamai, S. Secure communication over fading channels. *IEEE Trans. Inf. Theory* **2008**, *54*, 2470–2492. [CrossRef]
4. Ardestanizadeh, E.; Franceschetti, M.; Javidi, T.; Kim, Y.-H. Wiretap channel with secure rate-limited feedback. *IEEE Trans. Inf. Theory* **2009**, *55*, 5353–5361. [CrossRef]
5. Feng, D.; Jiang, C.; Lim, G.; Cimini, L.J., Jr.; Feng, G.; Li, G.Y. A survey of energy-efficient wireless communications. *IEEE Commun. Surv. Tutor.* **2012**, *15*, 167–178. [CrossRef]
6. Bi, S.; Zhang, R.; Ding, Z.; Cui, S. Wireless communications in the era of big data. *IEEE Commun. Mag.* **2015**, *53*, 190–199. [CrossRef]
7. Sarma, S.; Kuri, J. SNR based secure communication via untrusted amplify-and-forward relay nodes using artificial noise. *Wirel. Netw.* **2018**, *24*, 127–138. [CrossRef]
8. Peng, T.; Lambotharan, S.; Zheng, G.; Shikh-Bahaei, M. Opportunistic Fountain Coding with Coordinative Routing. *IEEE Wirel. Commun. Lett.* **2022**, *11*, 851–855. [CrossRef]
9. Yi, M.; Ji, X.; Huang, K.; Wen, H.; Wu, B. Achieving strong security based on fountain code with coset pre-coding. *IET Commun.* **2014**, *8*, 2476–2483. [CrossRef]
10. Kumar, S.; Rosnes, E.; i Amat, A.G. Secure repairable fountain codes. *IEEE Commun. Lett.* **2016**, *20*, 1491–1494. [CrossRef]
11. Shao, H.; Zhu, H.; Bao, J. Analysis and Design of Enhanced Distributed Fountain Codes in Multiple Access Networks with Cooperative Relay. *Symmetry* **2022**, *14*, 2026. [CrossRef]
12. Kasban, H.; Hashima, S.; Nassar, S.; Mohamed, E.M.; El-Bendary, M.A.M. Performance enhancing of MIMO-OFDM system utilizing different interleaving techniques with rate-less fountain raptor code. *IET Commun.* **2022**, *16*, 2479–2491. [CrossRef]
13. Sun, L.; Ren, P.; Du, Q.; Wang, Y. Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks. *IEEE Trans. Ind. Inform.* **2015**, *12*, 291–300. [CrossRef]
14. Liu, X.; Du, X.; Zhang, J.; Han, D.; Jin, L. ROFC-LF: Recursive Online Fountain Code With Limited Feedback for Underwater Acoustic Networks. *IEEE Trans. Commun.* **2022**, *70*, 4327–4342. [CrossRef]

15. Luby, M. LT codes. In Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science, Vancouver, BC, Canada, 19 November 2002; IEEE Computer Society: Washington, DC, USA, 2002; p. 271.
16. Hagedorn, A.; Agarwal, S.; Starobinski, D.; Trachtenberg, A. Rateless coding with feedback. In Proceedings of the IEEE INFOCOM 2009, Rio de Janeiro, Brazil, 19–25 April 2009; IEEE: New York, NY, USA, 2009; pp. 1791–1799.
17. Sun, W.; Wang, H.; Zhu, K.; Wang, J.; Tang, Z. A Novel Encoding Scheme for Regular Variable-Node Degree LT Codes. *Acta Electron. Sin.* **2014**, *42*, 1918.
18. Hashemi, M.; Cassuto, Y.; Trachtenberg, A. Fountain codes with nonuniform selection distributions through feedback. *IEEE Trans. Inf. Theory* **2016**, *62*, 4054–4070. [CrossRef]
19. Cai, P.; Zhang, Y.; Pan, C.; Song, J. Online fountain codes with unequal recovery time. *IEEE Commun. Lett.* **2019**, *23*, 1136–1140. [CrossRef]
20. Huang, J.; Fei, Z.; Cao, C.; Xiao, M. Design and analysis of online fountain codes for intermediate performance. *IEEE Trans. Commun.* **2020**, *68*, 5313–5325. [CrossRef]
21. Zhang, H.; Niu, F.; Yu, L.; Zhang, S. LT Codes with Double Encoding Matrix Reorder Physical Layer Secure Transmission. *J. Sens.* **2022**, *2022*, 6106786. [CrossRef]
22. Zhang, S.; Niu, F.; Yu, L.; Zhang, Y. Design of Anti-Eavesdropping Scheme for SLT-LT Codes Based on Random Symbol Sets. *IEEE Access* **2022**, *10*, 57880–57892. [CrossRef]
23. Jin, J.; Niu, F.; Yu, L.; Wang, D. Design of secondary LT code information security Transmission based on the symbols of degree 1. *Chang. Inf. Commun.* **2021**, *34*, 51–55.