e-ISSN 2320 –7876 www.ijfans.org
Vol.11, Iss.7, 2022
 UGC CARE Listed (Group -I) Journal

Secure Communication Based on the Uncertainty of Underwater Noise Channel

Kanne Naveen[1], Dr. Amol Kumbhare [2]

[1]*Research Scholar, Department of Electronics & Communication Engineering,*

Dr. APJ Abdul Kalam University Indore, India

[2] *Associate Professor, Department of Electronics & Communication Engineering,*

Dr. APJ Abdul Kalam University Indore, India

1. ***Corresponding author**: kanne.naveen@gmail.com*

2. *kumbhareamol82@gmail.com*

Abstract: Aiming at the impact of underwater noise uncertainty on information transmission and the security problems faced by communications in noise channels, a secure communication scheme based on the uncertainty of underwater noise channels is proposed. The scheme consists of an interactive key extraction protocol based on Godel coding and a confidentiality enhancement protocol based on $r-$cyclic Toeplitz matrix. In the process of key extraction, Godel coding is introduced to reduce the number of comparisons of key sequences; when calculating the secret-enhanced key length, the uncertainty of underwater noise is considered, which has stronger practical significance. The experimental results show that under the condition of meeting the security of the protocol, the total number of bits transmitted is 119940 bits, the lower bound of the total length of the key string generated after confidentiality enhancement is 117331 bits, and the upper bound of the amount of information about the key string by the adversary It is 2609 bits, the required time is 11.99s, and the proposed $(nt+s)\times(nt+s)$order $r-$cyclic Toeplitz matrix reduces the storage space of $(nt+s)-1$ bit compared with the traditional Toeplitz matrix of the same order.

Keywords: Underwater noise, uncertainty, Toeplitz matrix, confidentiality enhancement

I. Introduction

With the development of information technology and the development and utilization of the marine environment, marine information communication has become more and more important. At present, marine information mainly uses sound waves to communicate underwater [1]. Due to the openness of the underwater acoustic channel and the variability of the marine environment, marine information communication is faced with various security and attack problems [1-2], and in the complex and changeable marine environment, the interference of various noises will affect the information. Transmission has a great impact [3]. According to the sounding mechanism, the sound sources of marine environmental noise can be divided into the following four categories: marine dynamic noise, marine biological noise, man-made noise and marine thermal noise [4]. The uncertainty of noise has brought serious interference to the transmission of marine information. How to conduct confidential communication of transmitted information under the condition of uncertain underwater noise and ensure the integrity, confidentiality and robustness of information has become a major challenge for marine information security technology.

Aiming at the problem of confidential communication of marine information, this paper, based on the unpredictability of underwater noise in the binary symmetric communication channel, introduces Godel coding [5], and proposes an interactive cryptographic based on Godel coding under the premise of ensuring security. Key extraction protocol for key agreement and authentication extraction. At the same time, in order to improve the storage efficiency of confidentiality enhancement [6-7], the r-cyclic Toeplitz matrix [8-9] is applied to the confidentiality enhancement, and a confidentiality enhancement protocol based on the r-cyclic Toeplitz matrix is proposed, which makes the matrix storage space Compared with the traditional Toeplitz matrix, the storage space is greatly reduced, thus forming a secure communication scheme based on the uncertainty of the underwater noise channel, making the adversary unable to obtain enough information to calculate the key, ensuring the security and reliability of the scheme .

II. Related Information

2.1.Godel Coding

Godel coding is introduced by Godel in the proof of Godel's incompleteness theorem [5]. Based on the principle of prime number decomposition, a one-to-one correspondence is established between sequences and natural numbers. Given a finite sequence $(z_1, z_2, z_3, \dots, z_n)$, let $y = enc(z_1 z_2 \dots z_n) = p_1^{z_1} p_2^{z_2} \dots p_n^{z_n} = \prod p_i^{z_i} (1 \le i \le n, p_i \ne 1)$, Then this coding method is called Godel coding, and y is called the sequence $(z_1, z_2, z_3, \dots, z_n)$ corresponds to the Godel number, where p_i represents the i-th different from small to large Prime number.

2.2.Confidentiality enhancement

Confidentiality enhancement was originally proposed by Bennett [6] and was further promoted in literature [10]. Confidentiality enhancement means that when the legitimate communication parties A and B share a partial secret string S, and the adversary Eve knows part of the

information about S, through the global hash function [11-13], A and B can obtain an almost complete secret. The key string S ', and the amount of information about S' that the adversary Eve knows decreases exponentially. Definition 1 [14] Assuming that A and B share an N bit key string S, the random variable V means that it contains all the information about S that Eve knows. For any $\alpha = 2$ or $\alpha = \infty$, there are subsets $\{P_S|H_\alpha(S) \geq \beta\}$ to form the $\psi_{N,\alpha,\beta}$ set. Let l be any positive integer, $\varepsilon, \delta > 0$, then there is a $(N, \psi, l, \varepsilon, \delta)$ confidentiality enhancement protocol on the non-authenticated channel that satisfies the following properties.

1) *Correctness and confidentiality*: Let the adversary Eve accept a specific value $V = v$ that satisfies $P_{S|V} \in \psi$ when passive attack can only be used for eavesdropping, A and B will get a l bit key string S' make $S_A^{'} = S_B^{'} = S^{'}$ at the end of the agreement, and $H(S^{'}|C, V = v) \geq l - \varepsilon$ holds, where C represents the exchange information on the channel. In this case, the confidentiality enhancement is considered to be successful.
2) *Stubbornness:* Let$P_{S|V=v} \in \psi$, then any possible attack strategy against the adversary Eve, A and B both reject the result of the agreement, or the probability of success of confidentiality enhancement is at least $1 - \delta$.

2.3.Global hash function

The global hash function is an important tool to realize confidentiality enhancement, which is defined as follows [13]. Suppose the function $G: X \to Y$, $X = \{0,1\}^n, Y = \{0,1\}^l, n > l, \forall g \in G$, where g is a randomly selected function from G that obeys a uniform distribution, $|X|$ And $|Y|$ denote the number of elements in set X and set Y, respectively. For $\forall x_1, x_2 \in X$ and $x_1 \neq x_2$, the probability of $g(x_1) = g(x_2)$ does not exceed $\frac{1}{|Y|}$, that is

$$P\{g(x_1) = g(x_2)|x_1 \neq x_2\} \leq \frac{1}{|Y|}$$

There are three kinds of global hash functions used to realize confidentiality enhancement, namely modular arithmetic [15], finite field multiplication [10] and Toeplitz matrix [15-16]. Toeplitz matrix is the most widely used due to its good storage performance.

2.4.Toeplitz matrix

A general Toeplitz matrix of order $s \times n$ satisfies$T_{i,j} = T_{i+\varpi,j+\varpi}$, where $1 \leq i, i + \varpi \leq s, 1 \leq j, j + \varpi \leq n$, that is, each matrix from top left to bottom right elements on the diagonal line are the same. The specific representation of the Toeplitz matrix is

$$T(D) = \begin{pmatrix} D_n & D_{n-1} & \cdots & D_2 & D_1 \\ D_{n+1} & D_n & \cdots & D_3 & D_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ D_{n+s-2} & D_{n+s-1} & \cdots & D_s & D_{s-1} \\ D_{n+s-1} & D_{n+s-2} & \cdots & D_{s+1} & D_s \end{pmatrix}_{s \times n}$$

The r−cyclic Toeplitz matrix can be expressed as

$$R_r(D) = \begin{pmatrix} D_0 & D_1 & D_2 & \cdots & D_{n-1} \\ rD_{n-1} & D_0 & D_1 & \cdots & D_{n-2} \\ rD_{n-2} & rD_{n-1} & D_0 & \dots & D_{n-3} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ rD_1 & rD_2 & rD_3 & \cdots & D_0 \end{pmatrix}_{n\times n}$$

When $r = 1$, it is a cyclic Toeplitz matrix; when $r\ -1$, it is an oblique cyclic Toeplitz matrix; when $r = 0$, it is an upper triangular Toeplitz matrix [8].

III. Interactive key extraction protocol based on Godel coding

3.1.Protocol design

The interactive key extraction protocol based on Godel coding includes two parts: key agreement and authentication extraction. Select q elements in the finite field$GF(q)$, where q is a prime number. Node A and Node B respectively select Q_1 and Q_2 as signs in advance. Among them, $Q_1, Q_2 \in GF(q), Q = (Q_1{+}Q_2)mod(q)$, then $Q\varepsilon GF(q)$, and Q is the secret number of node A and node B.

In the following, the interactive key agreement protocol based on Godel coding will be described in detail.

First, node A and node B simultaneously obtain n-bit key strings $S_A = x_1x_2 \dots x_n, S_B = y_1y_2 \dots y_n$, on the binary symmetric channel, and perform XOR operations on the adjacent two bits of the key strings respectively obtained, and The following two adjacent bits cannot overlap with any one of the preceding adjacent bits. Combine all the results after XOR to form the key sequence $Z_A = \left(z_1, z_2, \dots, z_{\frac{n}{2}}\right), Z_B = \left(z_1^{'}, z_2^{'}, \dots, z_{\frac{n}{2}}^{'}\right)$ and z', and then calculate them separately Del number Ge_A and Ge_B, node B sends the calculated Ge_B to node A. In order to verify whether the passed Ge_B is correct, calculate $G_A = Q \times Ge_B, G_B = Q \times Ge_B$ by the secret number Q known to only node A and node B, send G_A to node B, if $G_A = G_B$, send it to node A feedback message "Yes", if $Ge_A \neq Ge_B$, send the key sequence Z_A, otherwise stop. Node B compares z_i with $z_i^{'}(1 \leq i \leq n/2)$, if $z_i \neq z_i^{'}$, record the corresponding subscripts to form a set I, and send I to node A, so that node A knows that the XOR results are different and node A and node B both set the position where the XOR result is different to 1, so that the bit strings of both sides are as the same as possible.

Repeat the above key agreement protocol t times to obtain the key strings □□ and □□ of □□ bit respectively. At this time, □□ and □□ will still be different in a small probability. Therefore, it is necessary to authenticate the public string after key negotiation and extract a completely consistent security key.

Let □□(□) = $\sum_{□=I}^{2|□|}$ □□ □□, where □□ and □□ represent the i-th position of the string length □ and □ respectively, and |□| represents the number of elements in the set □, based on the interaction of Godel coding the key authentication extraction. First, □ and $h(h \neq$ □) are arbitrarily selected from the real finite field □□□($2^{□□}$) (R stands for real number), $□_{II}$ is the interactive key agreement based on Godel coding, after t times, different XORs The result is set to all bits of 1. Node A and node B calculate the identifiers □□□□, □□□□′ and □□□□, respectively. The message authentication on the channel is carried out through the comparison between identifiers, and finally the hash function □ is selected arbitrarily from the hash function family to check whether the public key string □□ and □□ of the finally obtained nt bit are equal.

If $□_□ ≠ □_□$, stop the protocol; otherwise, node A and node B act on the public key string through the global hash function g in confidentiality enhancement to extract the final security key $□_□ = □_□ = □$. The global hash function g satisfies$□_{□□□}(□) = □□□□$. Among them, □ is randomly selected from □ that obeys a uniform distribution, cir is a binary r-cyclic Toeplitz matrix, □ is the key string $□_□$ or $□_□$, and □ is the first l digit of the result of the hash function.

3.2.Protocol analysis

3.2.1. Adversary model and attack method

The adversary model discussed in this article satisfies the following conditions:

i. The adversary has unlimited computing power;
ii. The adversary's eavesdropping channel is not limited to a fading channel;
iii. The channel is a binary symmetric channel, and the bit error rate of both parties in legal communication is λ. The bit error rate of the eavesdropping channel is θ, and the error bit rate of the adversary's estimated information is θ ′.

This article mainly discusses the following two attack methods.

1) Replacement attack: The adversary randomly selects a check block from the set of check blocks it owns, and sends it directly to node B without any error correction.
2) Imitation attack: The adversary randomly selects a check block from the check block set, and then randomly corrects the selected check block according to the error bit rate $□'$ of the estimated information. Since the adversary does not know the specific location of the error bit, the error correction is random and probabilistic. The interactive key agreement protocol based on Godel coding is executed □ times, and there are □ check blocks in total. In the interactive key extraction protocol based on Godel coding, each time the adversary eavesdrops on the check block □ sent by node A to node B, it is compared with the check block $□''$ that he owns. Assuming that the number of error bits found each time is $□_□$, after multiple eavesdropping, a total of num check blocks are eavesdropped on, then

$$□' = (1 - □)\left[\frac{\sum_{□=1}^{□□□} □_□}{□□□\left(\frac{□}{2}\right)}\right]$$

3.2.2. Security analysis and proof

From the key agreement protocol, if $□_□ ≠ □'_□$, the adversary can know $□_{2□-1} = □_{2□} = 11$. If$□_□ = □'_□$, the adversary's $□''_□$ is different from the node A and node B's $□_□$ and$□'_□$, then the probability that the adversary correctly guesses the two digits is $1/2$. If the adversary's $□''_□$ is the same as the $□_□$ and $□'_□$ of node A and node B, then the probability that the two eavesdropped by the adversary are the same as node A and node B is $(1 - □)^2, □[□_□ ≠ □'_□] = 2□(1 - □), □[□_□ = □'_□] = 1 - 2□ + 2□^2$, in summary, the probability of the adversary's correct eavesdropping on the corresponding two bits is $2□(1 - □) + (1 - 2□ + 2□^2)\left[\frac{1}{2}2□(1 - □) + (1 - □)^2\right]$, which is $2□(1 - □)(1 - 2□ + 2□^2)(1 - □)$, let $□ = 2□(1 - □)(1 - 2□ +$

$2□^2)(1-□)$, so the average number of bits that the adversary can correctly eavesdrop on the n bit key string is at most $□□^{□/2}$ $(0<□^{\frac{□}{2}}+□<1)$.

Next, prove that the probability that the adversary knows $□^{\frac{□}{2}}+□$bit is negligible.

Theorem 1. Let $□ \subset \{1,2,3,\ldots,□\}$, Satisfy $□\left[|□|\geq□\left(□^{□/2}+□\right)\right]\leq□^{\frac{-□□^2□^{-□/2}}{3}}$. Proof. Let $\bar{□}_□$ denote the i-th random variable, $\bar{□}_□=1$ denote the adversary's eavesdropping of the correct value of the i-th bit, and $\bar{□}_□=0$ means that the adversary's eavesdropping of the i-th bit is wrong. where, $\bar{□}_1,\bar{□}_2,\ldots,\bar{□}_□$ are independent Poisson events and $□(\bar{□}_□)=□$, then the expectation of $\sum_{□=1}^{□}\bar{□}_□$is $□(\sum_{□=1}^{□}\bar{□}_□)=□□$. According to Markov's inequality, for any $□>0,□>0$, formula (1) is applied to $□^{□\,\bar{□}}$ to obtain the general Chernoff bound of the random variable □, which can be obtained by the multiplicative Chernoff theorem. The more convenient and commonly used Chernoff bound is obtained, that is, for any $0\leq□\leq1$, the formula (2) is satisfied.

$$□[\bar{□}\geq□]=□\left[□^{□\bar{□}}\geq□^{□□}\right]\leq\frac{□\left(□^{□\bar{□}}\right)}{□^{□□}} \tag{1}$$

$$□[\sum_{□=1}^{□}\bar{□}_□\geq(1+□)□□]\leq□^{\frac{-□□□^2}{3}} \tag{2}$$

So,

$$□\left[|□|\geq□\left(□^{□/2}+□\right)\right]=□\left[\sum_{□=1}^{□}\bar{□}_□\geq□□^{\frac{□}{2}}\left(1+□□^{-\frac{□}{2}}\right)\right]\leq□^{\frac{-□□^2□^{-□/2}}{3}}$$

When the adversary has its own key string $□''_□$, compared with the key string $□_□$ transmitted by node □ $\left(1\leq□\leq\frac{□}{2}\right)$, the uncertainty of the corresponding two bits $□_{2□-1}□_{2□}$ can be estimated by Theorem 2.

Theorem 2: $\bar{□}=\{00,01,10,11\}$, $\bar{□}\in\bar{□}$ is a random variable corresponding to two bits $□_{2□-1}□_{2□}$, where the bit error rate of the adversary's eavesdropping channel is □, then the adversary is uncertain about the nt bit key string The degree is $□(\bar{□}|\bar{□})=□(\bar{□}=0)□(\bar{□}|\bar{□}=0)+□(\bar{□}=1)\,□(\bar{□}\,|\bar{□}=1)$.

Prove that the random variable Y has the following three cases: 1) When the check digits sent by A and B are not equal, that is, $□_□\neq□'_□$, at this time the adversary knows $□_{2□-1}□_{2□}=11$, then $\bar{□}=\Delta$; 2) When A and When the check digits sent by B are equal, it is $□_□=□'_□$. If the check digit $□_□=□'_□$ that the adversary eavesdropped, then $\bar{□}=0$; 3) When the check digits sent by node A and node B are equal, that is $□_□=□'_□$, If the check digit $□''_□\neq□_□$ eavesdropped by the adversary, then $\bar{□}=1$.

For case 1), it is clear that $□(\bar{□}\,|\bar{□}=□)=0$; for case 2) and case 3), let's assume that node □ sends $□_□=1,□_{2□-1}□_{2□}=10$ ($□_{2□-1}□_{2□}$ is $00,01$, situation is same at 11), because when $□_□=0$, the probability of case 2) and case 3) is same as that of $□_□=1$. For situation 2), the adversary only receives 01 or 10, that is, either both are correct or both are wrong, then

$$□[\bar{□}=0]=□^2+(1-□)^2 \tag{3}$$

The probability that the adversary receives $□_{2□-1}□_{2□}=10$ is

$$\square[10|\bar{\square}=0]=\frac{(1-\square)^2}{[\square^2+(1-\theta)^2]}$$

(4)

The probability that the adversary receives $\square_{2\square-1}\square_{2\square}=01$ is

$$\square[01|\bar{\square}=0]=\frac{\square^2}{\square^2+(1-\square)^2}$$

(5)

For case 3), the adversary only accepts 00 or 11. At this time, the adversary receives $\square_{2\square-1}\square_{2\square}$ only one bit is correct, so

$$\square[\bar{\square}=1]=2\square(1-\square)$$

(6)

The probability that the adversary receives $\square_{2\square-1}\square_{2\square}=00$ is

$$\square[00|\bar{\square}=1]=\frac{\square(1-\square)}{2\square(1-\square)}=\frac{1}{2}$$

(7)

The probability that the adversary receives $\square_{2\square-1}\square_{2\square}=11$ is

$$\square[11|\bar{\square}=1]=\frac{\square(1-\square)}{2\square(1-\square)}=\frac{1}{2}$$

(8)

Use Renyi entropy [17] to express the uncertainty of information, as shown in equations (9)~(11).

$$\square(\bar{\square}|\bar{\square}=0)=\frac{(1-\square)^2}{\square^2+(1-\square)^2}\square\square\frac{\square^2+(1-\square)^2}{(1-\square)^2}+\frac{\square^2}{\square^2+(1-\square)^2}\square\square\frac{\square^2+(1-\square)^2}{\square^2}$$

(9)

$$\square(\bar{\square}|\bar{\square}=1)=-\frac{1}{2}\square\square\frac{1}{2}-\frac{1}{2}\square\square\frac{1}{2}=1$$

(10)

$$\square(\bar{\square}|\bar{\square}=\Delta)=0$$

(11)

In summary, we have

$$\begin{aligned}\square(\bar{\square}|\bar{\square})&=\square(\bar{\square}=0)\square(\bar{\square}|\bar{\square}=0)+\square(\bar{\square}=1)\square(\bar{\square}|\bar{\square}=1)+\square(\bar{\square}=\Delta)\square(\bar{\square}|\bar{\square}=\Delta)\\&=\square(\bar{\square}=0)\square(\bar{\square}|\bar{\square}=0)+\square(\bar{\square}=1)\square(\bar{\square}|\bar{\square}=1)\\&=\left[\square^2+(1-\square)^2\right]\left[\frac{(1-\square)^2}{\square^2+(1-\square)^2}\square\square\frac{\square^2+(1-\square)^2}{(1-\square)^2}\right.\\&\left.+\frac{\square^2}{\square^2+(1-\square)^2}\square\square\frac{\square^2+(1-\square)^2}{\square^2}\right]+2\square(1-\square)\end{aligned}$$

Therefore, the adversary's uncertainty of the $\square\square$ $\square\square\square$ key string is $\frac{\square\square}{2}\square(\bar{\square}|\bar{\square})$.

3.3.Protocol characteristics

3.3.1. Authentication

The Godel coding-based interactive key authentication and extraction protocol verifies whether the channel is secure by whether the identifiers are equal, and uses a hash function to verify whether the public string obtained by node A and node B after t times of key negotiation is consistent, and Extract the completely consistent high-secret key string K.

3.3.2. High efficiency

The interactive key agreement protocol based on Godel coding judges whether it is necessary to send the key sequence □□ by whether the Godel numbers are consistent. It can be seen from the nature of Godel coding that if the calculation result of the two parties in communication is □□□ = □□□, it means that □□ = □□′, the key sequence □□ does not need to be sent; only when □□□ ≠ □□□, the key sequence □□ needs to be sent for comparison, so Reduce the number of comparisons of key sequences, reduce communication overhead, and improve communication efficiency. In addition, from the operating rules of modular arithmetic [18-19], we know

$$□_1□_2□□□ □ = [(□_1 □□□ □)(□_2 □□□ □)]□□□ □$$
$$(□_1 + □_2) □□□ □ = (□_1 □□□ □ + □_2 □□□ □) □□□ □$$

When calculating □□□ and □□□, by using modulo operation in advance, the data storage space problem caused by exponential operation can be reduced. In the process of extracting the key authentication, by introducing the modulus operation of □, the operation efficiency of the exponent can be improved. In addition, all calculations in this paper are based on binary symmetrical channels. Therefore, all non-binary results must be modulo arithmetic.

This paper does not check whether the key strings □□ and □□ are the same in the key agreement protocol, but in the key authentication extraction protocol, the authentication is performed by collecting □ such key strings, and the hash function is used to complete the key Checking whether the strings are the same reduces the number of authentications and further improves communication efficiency.

Let N be the number of times the complete protocol is executed until the key string K is established. Theorem 3 gives the expected value of □′, which further proves the efficiency of the protocol.

Theorem 3 Let □′be a random variable of the number of executions, until node A and node B establish a public key string of length nt bit, then the expected value of N'is $(1 - □)^{□□□ - \frac{□□}{2}}$.

Proof. Suppose the bit error rate of both parties in legal communication is □, and the bit error rate of the adversary's eavesdropping channel is □. $□_1$ means that node B can correctly receive the key sequence A sent by node A $□_□ = (□_1, □_2, \dots, □_{□/2})$ event, $□_2$ means that node A and node B get the same event of the □□ bit key string.

$$□ = \frac{\sum_{□=1}^{□} |□|_□}{□□/2} \quad (12)$$

In the key agreement protocol, there are

$$□(\Omega_1) = (1 - □)^{\frac{□□}{2}} \quad (13)$$

The number of check bits of node A and node B in the t-th key agreement protocol is the same $\frac{□}{2} - |□|_□$, and the probability that the □ bit key strings of node A and node B are the same is

$$((1 - □)^2)^{\frac{□}{2} - |□|_□} = (1 - □)^{□ - 2|□|_□} \quad (14)$$

Therefore, after t times of execution of the interactive key agreement protocol based on Godel coding is completed, the probability that the □□ bit key string obtained by node A and node B is the same is

$$\square(\Omega_2|\Omega_1) = \frac{\prod_{\square=1}^{\square}(1-\square)^{\square-2|\square|_{\square}}}{(1-\square)^{\frac{\square\square}{2}}} = (1-\square)^{\frac{\square\square}{2}-2\sum_{\square=1}^{\square}|\square|_{\square}} = (1-\square)^{\frac{\square\square}{2}-\square\square\square}$$

(15)

Let

$$\square = (1-\square)^{\frac{\square\square}{2}-\square\square\square}$$

(16)

But

$$\square(\square') = \frac{1}{\square}$$

(17)

So $\square(\square') = (1-\square)^{\frac{\square\square}{2}-\square\square\square}$.

It can be seen from Section 3.2.1 that the bit error rate of both parties in legal communication is □, and the bit error rate of the adversary's eavesdropping channel is □, and the probability of correct eavesdropping on the key sequence $\square_{\square} = (\square_1, \square_2, \dots, \square_{\square/2})$ is $(1-\square)^{\square\square/2}$, when the protocol is executed N′ times, the probability of being eavesdropped by the adversary is $1-\left[1-(1-\square)^{\frac{\square\square}{2}}\right]^{\square'}$, when the protocol is executed N′ times, the secret is established When the key string is K, the communication channel between node A and node B is equivalent to a noise-free channel, because after executing the protocol N' times, both parties have established the same and consistent key string, and the adversary's eavesdropping channel can be equivalent to one For the new binary symmetrical channel, the new bit error rate $\overline{\square}$ satisfies $(1-\overline{\square})^{\square\square/2} = 1-1-\left[1-(1-\square)^{\frac{\square\square}{2}}\right]^{\square'}$, we can get $\overline{\square} = 1-\left\{1-\left[1-(1-\square)^{\frac{\square\square}{2}}\right]^{\square'}\right\}^{2/\square\square}$, where N′ is the expected value in Theorem 3.

From the above analysis, the original $(\square > 0, \square > 0)$ channel can be equivalent to the $(\square = 0, \overline{\square} > 0)$ channel, that is, a noise-free legal communication channel and an eavesdropping channel with a lower bit error rate. Even if the bit error rate of the eavesdropping channel is lower than the bit error rate of both parties in the legal communication, the adversary still cannot avoid the extremely small bit error rate caused by noise.

3.3.3. Anti-active attack

Combining the analysis in Section 3.2.1, theorem 4 can be obtained.

Theorem 4 Node A and Node B share the common string of □□ bits, and the error bit rate of the adversary's estimated information is □′. In each check block, the number of bits inconsistent between the adversary and node A and node B is Ω_1, then the adversary takes the first The

maximum probability of a successful attack in one way is $(1-\square')^{\square/2}$, and the maximum probability of an adversary's active attack in the second way is $\frac{1}{\sum_{\Omega_1}^{\frac{\square}{2}} \square_{\frac{\square}{2}}^{\Omega_1}} \square'^{\Omega_1}(1-\square')^{\frac{\square}{2}-\Omega_1}$.

Prove that if the adversary adopts an alternative attack method for active attack, since the error bit rate of the adversary's estimated information in the binary symmetric channel is $\square'$, and the length of each check block is $\square/2$, the check block selected by the adversary same probability as node A and node B is $(1-\square')^{\square/2}$, that is, the maximum probability that the adversary adopts the first method to actively attack successfully is $(1-\square')^{\square/2}$.

If the adversary adopts an imitation attack to actively attack, he does not know how many inconsistent bits are in each parity block, and can only guess randomly, and the probability of correctly guessing the number of inconsistent bits is $\frac{1}{\sum_{\Omega_1=0}^{\square/2} \square_{\square/2}^{\Omega_1}}$, So the probability of correctly guessing and correcting the inconsistent bits is

$$\frac{1}{\sum_{\Omega_1=0}^{\frac{\square}{2}} \square_{\frac{\square}{2}}^{\Omega_1}} \frac{1}{\square_{\frac{\square}{2}}^{\Omega_1}} \square_{\frac{\square}{2}}^{\Omega_1} \square'^{\Omega}(1-\square')^{\frac{\square}{2}-\Omega_1}$$

(18)

Organized

$$\frac{1}{\sum_{\Omega_1}^{\frac{\square}{2}} \square_{\frac{\square}{2}}^{\Omega_1}} \square'^{\Omega_1}(1-\square')^{\frac{\square}{2}-\Omega_1}$$

(19)

Therefore, the maximum probability that the adversary adopts the second method to actively attack successfully is $\frac{1}{\sum_{\Omega_1=0}^{\frac{\square}{2}} \square_{\frac{\square}{2}}^{\Omega_1}} \square'^{\Omega_1}(1-\square')^{\frac{\square}{2}-\Omega_1}$.

IV. Confidentiality enhancement protocol based on r−circular Toeplitz matrix

The core of confidentiality enhancement is to construct a global hash function. At present, what is widely used for security enhancement is the global hash function based on the general Toeplitz matrix. The general $\square \times \square$ order Toeplitz matrix requires $(\square + \square - 1)$ bit storage space. In order to improve storage efficiency, this paper uses n order r−cyclic Toeplitz matrix for confidentiality enhancement and only requires n bits of storage space and parameter r information. . At the same time, the uncertainty of noise is taken into account in the confidentiality enhancement protocol, which makes the protocol have higher practical value, and obtains the maximum length of the extracted key and the upper bound of the amount of information about the key by the adversary.

4.1.r−cyclic Toeplitz matrix

Any Toeplitz matrix can be embedded in a cyclic matrix [20], and it can also be embedded in an r-cyclic Toeplitz matrix. In order to improve the storage efficiency of confidentiality

enhancement, a general $□ \times □□$ order Toeplitz matrix is expanded into an $(□□ + □) \times (□□ + □)$ order r−cyclic Toeplitz matrix $(□ < □□)$. The specific representation is

$$□□□ = \begin{pmatrix} □_1 & □_2 \\ □_3 & □_4 \end{pmatrix}_{(□□+□)\times(□□+□)}$$

Where $□_1, □_2, □_3, □_4$ are respectively

$$□_1 = \begin{pmatrix} □_□ & □_{□+1} & \cdots & □_{□+□□-1} \\ □□_{□-1} & □_□ & \cdots & □_{□+□□-2} \\ \cdots & \cdots & \cdots & \cdots \\ □□_1 & □□_2 & \cdots & □_{□□} \end{pmatrix}_{□\times□□}$$

$$□_2 = \begin{pmatrix} □_0 & □_1 & \cdots & □_{□-1} \\ □_{□+□□-1} & □_0 & \cdots & □_{□-2} \\ \cdots & \cdots & \cdots & \cdots \\ □_{□□+1} & □_{□□+2} & \cdots & □_0 \end{pmatrix}_{□\times□□}$$

$$□_3 = \begin{pmatrix} □□_0 & □□_1 & \cdots & □_{□□-1} \\ □□_{□-1} & □□_0 & \cdots & □_{□□-2} \\ \cdots & \cdots & \cdots & \cdots \\ □□_{□+1} & □□_□ & \cdots & □□_0 \end{pmatrix}_{□□\times□□}$$

$$□_4 = \begin{pmatrix} □_{□□} & □_{□□+1} & \cdots & □_{□+□□-1} \\ □_{□□-1} & □_{□□} & \cdots & □_{□+□□-2} \\ \cdots & \cdots & \cdots & \cdots \\ □□_1 & □□_2 & \cdots & □_□ \end{pmatrix}_{□□\times□}$$

Extend the $□□ \times 1$ order public string $□ = (□_1, □_2, \ldots, □_{□□})^□$, the extracted key $\bar{□} = \begin{pmatrix} □ \\ 0 \end{pmatrix}_{(□□\times□)\times1}$ calculation formula is as follows

$$\bar{□} = □□□\ \bar{□} \tag{20}$$

where, $\bar{□} = (□_1, □_2, \ldots, □_{□□+□})$. Take the first $□$ digits of $\bar{□}$ as the final key $□$ after confidentiality enhancement, namely $□ = (\bar{□})_□$, and

$$□_□ = □□□_{□1}\ \bar{□}_{11} \oplus □i□_{□2}\ \bar{□}_{21} \oplus \ldots \oplus □□□_{□(□□+□)}\ \bar{□}_{(□□+□)1}$$

where, $\oplus$ represents the exclusive OR operation, $□□□_{□□}$ represents the element in the i-th row and the j-th column of the matrix $□□□$, and $\bar{□}_{□1}$ represents the element in the j-th row and the first column of the vector $\bar{□}$, which can be obtained by fast Fourier transform [20]

$$□□□□ = □□□□(□□)□ \tag{21}$$

where, $□$ is a $(□□ + □)$-dimensional vector, $□ = (□_0, □_1, \ldots, □_{□□+□-1}), □ = (□_{□'}), □_{□'} = □^{□'}_{□□+□}, □_{□□+□} = □^{-\frac{2□□}{□□}+□}$, by the formula (20) and (21) can be obtained

$$□ = □^{-1}□□□□(□□)□\ \bar{□} = □^{-1}(□□.*\ □\bar{□}) \tag{22}$$

where, $(.*)$ represents the Hadamard product, that is, $(□.*\ □)_□ = □_□□_□$.

In this paper, the r-circular Toeplitz matrix is used in the security-enhanced global hash function because the r-circular Toeplitz matrix depends on the first row of matrix elements and the parameter r. For the traditional $(□□ + □) \times (□□ + □)$-order Toeplitz matrix, $2(□□ + □) - 1$ bit is required to describe the entire matrix completely, while the $(□□ + □) \times (□□ + □)$-order r-cyclic Toeplitz matrix in this article only needs $(□□ + □)$ bit and The parameter $□$ can completely describe the entire matrix, thereby reducing the storage space of the matrix.

4.2.Noise uncertainty based on propagation distance

Underwater environment communication is much more complicated than terrestrial environment communication. In order to quantitatively analyze the uncertainty of underwater noise, this paper adopts the Markov chain Monte Carlo (MCMC) method [21] to capture the uncertainty of noise. The MCMC method is suitable for non-standard multi-variable forms, can realize dynamic simulation, and is usually used to obtain the probability distribution of underwater acoustic parameters. The model parameter space is explored by generating several independent parallel Markov chains, and the sample information is constantly updated to make the Markov chain converge in the high probability density area, which is the maximum posterior estimation in the Bayesian method [4]. Assuming that the application domain of underwater communication $\square \in \square$, the distance domain $\square \in \square'$, and the environmental domain $\square \in \square$.

Noise itself is a kind of random process. This article regards noise as a random variable $\square$ belonging to the application domain $\square$. Available from Bayesian theory

$$\square(\square|\square) = \frac{\square(\square|\square)\square(\square)}{\square(\square)}\square\square(\square)\square(\square) \tag{23}$$

where, $\square(\square)$ is the normalization factor, and $\square(\square|\square)$ is the likelihood function of $\square(\square|\square)$. If the data vector in the distance domain is expressed as $\square = \square'(\square) + \square$, where $\square'(\square) = \square(\square)\overline{\square}$, $\square$ is the error term that obeys the normal distribution $(0, \overline{\square})$, and $\overline{\square}$ is the covariance. Then the likelihood function is

$$\square(\square, \overline{\square}, \overline{\square}) = \frac{1}{\square^{\overline{\square}}|\overline{\square}|}\exp\left\{-[\square - \square(\square)\,\overline{\square}\,]^{\Theta}\,\overline{\square}^{-1}[\square - \square(\square)\,\overline{\square}\,]\right\} \tag{24}$$

where, $\overline{\square}$ represents the number of data points, the superscript Θ is the conjugate transpose, the transfer function $\square(\square)$ can be obtained from the underwater acoustic propagation model [4], $\overline{\square}$ is the underwater noise source, and the uncertainty of the data can be obeyed independent and identically distributed error $\overline{\square} = \square\square$ is described. When $\frac{\square \log \square}{\square\overline{\square}} = 0$,

$$\overline{\square}_{\square\square} = \frac{\square^{\square}\square(\square)}{\|\square(\square)\|^2} \tag{25}$$

Substituting equation (25) into equation (24), the likelihood function becomes

$$\square(\square, \square) = \frac{1}{\square^{\overline{\square}}\square^{\overline{\square}}}\exp\left(-\frac{\Phi(\square)}{\square}\right) \tag{26}$$

where, the objective function is

$$\Phi(\square) = \|\square\|^2 - \frac{|\square^{\square}\square(\square)|^2}{\|\square(\square)\|^2} \tag{27}$$

Therefore, the product is calculated by formula (26), and the covariance is regarded as a redundant parameter.

$$\square(\square) = \int_0^{\infty}\square(\square, \square)\square(\square)\square\square \tag{28}$$

where, $\square(\square) = \frac{1}{\square}$, so the likelihood function can be written as equation (29).

$$□(□) = \frac{(□-1)!}{□^{□}Φ(□)^{□}}$$

(29)

Formula (30) can be obtained from the above derivation and the Bayesian model averaging method.

$$□(□|□) = ∫ □(□, □|□)\,□□ = ∫ □(□|□, □)□(□|□)□□$$

(30)

If □ contains all the uncertainties, and all the information in □ is mapped to □, then there is □(□|□, □) = □(□|□).

Traditional statistics describing noise include probability density function, mathematical expectation, variance or power spectrum and other statistics. The power spectrum is uniform noise, that is, white noise, which is not suitable for complex dynamic underwater environmental noise. At present, in the uncertainty research of underwater numerical simulation, the variance of the variable is generally defined as a measure of uncertainty [21], but the variance is not a general uncertainty measurement function and has limitations. Therefore, this article will introduce information entropy in information theory to quantitatively analyze the uncertainty of noise. For a continuous variable □, the information entropy □ is defined as [22]

$$□(□) = -∫ □(□)□□□(□)□□$$

(31)

From equation (30) and equation (31), the information entropy of the applied domain noise variable u can be obtained as

$$□_{□}(□) = H\big(□(□|□)\big) = -∫ □(□|□)□□□(□|□)□□$$

(32)

4.3.Lower bound of key length after confidentiality enhancement

Corollary 1 [10] Let $□_{□□}$ be an arbitrary probability distribution, let □ be a specific value of □ observed by the adversary, if the adversary's Renyi entropy □(□|□ = □)) of □ is at least □, and node A and node B chooses □ = □(□) as its key, where □ is randomly selected from the global hash function class from □ to $\{0,1\}^{□}$, □ ∈ □, then

$$□(□|□, V = □) ≥ □_2(□|□, □ = □) ≥ □ - □□\big(1 + 2^{□-□}\big) ≥ □ - \frac{2^{□-□}}{□□2}$$

According to the literature [10], □(□|□) > □(□). According to Theorem 2, □ = $\frac{□□}{2}$□(□|□) > $\frac{□□}{2}$□(□), according to Corollary 1

$$□(□|□, □ = □) ≥ □ - □□\left(1 + 2^{□-\frac{□□□(□)}{2}}\right) ≥ □ - \frac{2^{□-\frac{□□□(□)}{2}}}{□□2}$$

(33)

Let $□' = \frac{□□}{2}□(□) - □$, from the above analysis, when $□ < \frac{□□}{2}□(□)$, the adversary's uncertainty about the key □ is close to the maximum, that is, the adversary's probability distribution about the key □ is close to Evenly distributed, node A and node B can obtain the key □ at this time, which satisfies equation (34).

$$\square \geq \frac{\square\square}{2}\square(\square) + \frac{2^{\square-\frac{\square\square\square(\square)}{2}}}{\square\square 2}$$

(34)

The amount of mutual information between the information known by the adversary and the final key is

$$\square(\square, \square\square) = \square(\square) - \square(\square|\square\square) \leq \frac{2^{\square-\square'}}{\square\square 2}$$

(35)

That is, the amount of information that the adversary knows about the key K is at most $\frac{2^{\square-\square'}}{\square\square 2}$, and it decreases exponentially with $\frac{\square\square}{2}\square(\square) - \square$.

Theorem 5 For any integer $\square\square$, there exists a positive number $\square' < 1$ and $\square$ that makes $(1 - \square_{\square}(\square) - \square)\square\square - \wp$ a positive integer, where $\square_{\square}(\square)$ is the noise calculated in Section 4.2 The uncertainty of $\wp$ is the safety factor. A confidentiality enhancement agreement can be executed on an insecure channel. The specific parameters are as follows

$$\left(\square\square, \square_{\square\square,2,\square'\square\square}, (1 - \square_{\square}(\square) - \Gamma)\square\square - \wp, \frac{2^{\square-\frac{\square\square\square(\square)}{2}}}{\square\square 2}, \square\right)$$

where, $\square = \max\left(\left(1-\square'\right)^{\square/2}, \left(\frac{1}{\sum_{\Omega_1=0}^{\frac{\square}{2}}\square_{\frac{\square}{2}}^{\Omega_1}}\right)\square'^{\Omega_1}\left(1-\square'\right)^{\frac{\square}{2}-\Omega_1}\right)$, $\square'$ the error bit rate of the estimated information is the number of bits in each check block that the adversary is inconsistent with node A and node B, $\square$ is the final key length extracted, and $\square(\square)$ is the Renyi entropy of the original part of the secret string $\square$, $\square\square$ is the common string obtained during key negotiation between node A and node B.

Proof. Let V be the random variable of the information about the original string S that the adversary eavesdropped on. A certain $\square \in \square$ can be known from Definition 1, $\square_2(\square|\square = \square) \geq \square'\square\square$, and $\square_{\square}(\square)$ can be known from Eq. (32)

$$\square = (1 - \square_{\square}(\square) - \Gamma)\square\square - \wp$$

(36)

From Corollary 1:

$$\square_2(\square|\square, \square = \square) \geq \square - \frac{2^{\square-\frac{\square\square\square(\square)}{2}}}{\square\square 2}$$

(37)

That is, $\square = \frac{2^{\square-\frac{\square\square\square(\square)}{2}}}{\square\square 2}$ in Definition 1. According to Theorem 4, the maximum probability of an adversary's active attack is

$$\square = \max\left(\left(1-\square'\right)^{\frac{\square}{2}}, \left(\frac{1}{\sum_{\Omega_1=0}^{\frac{\square}{2}}\square_{\frac{\square}{2}}^{\Omega_1}}\right)\square'^{\Omega_1}\left(1-\square'\right)^{\frac{\square}{2}-\Omega_1}\right)$$

In summary, the corresponding parameter values in Definition 1 can be obtained, and the confidentiality enhancement agreement in Theorem 5 can be obtained.

V. Experimental results and analysis

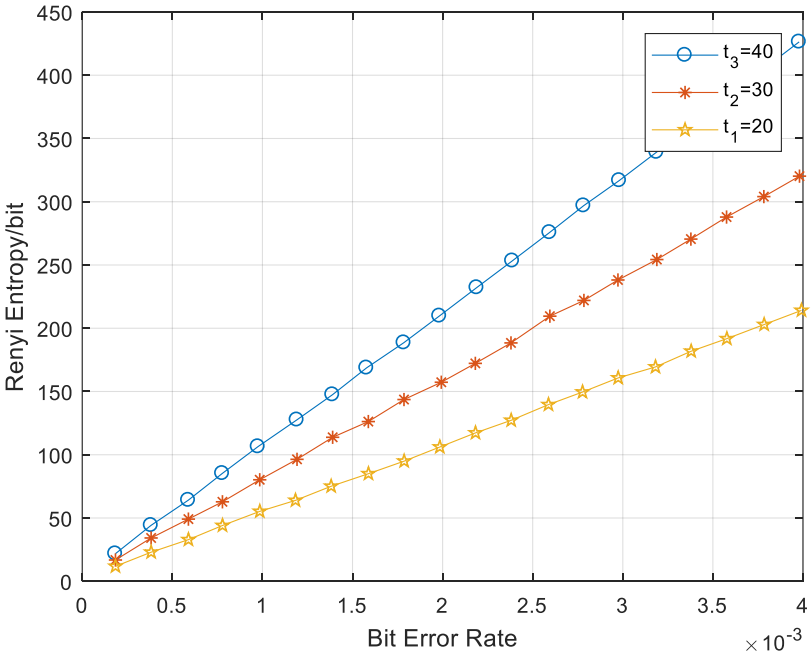

Figure 1. Adversary's uncertainty about the □□ bit key string information

Let the number of bits transmitted in each key negotiation process be □ = *300*, and the number of key negotiation times □ are respectively □*1* = *20*, □*2* = *30*, □□□ □*3* = *40*. The experimental results of the uncertainty of the adversary's information acquisition are shown in Figure 1.

The three curves in Figure 1 all correspond to the uncertainty of the adversary's □□ bit key string information when the number of key negotiation times is different under the condition of □ = *300*. Among them, the horizontal axis represents the adversary's bit error rate in the underwater noise channel, and the vertical axis represents the adversary's Renyi entropy of the nt bit key string information, that is, the uncertainty of the information. It can be seen from Figure 1 that the fitting degrees of the three curves are all approximately linear functions, and the Renyi entropy of the adversary's information increases with the increase of the bit error rate and the number of key negotiations, indicating that multiple key negotiations can be Increase the uncertainty of the adversary to the key string and make the key more secure.

Table 1: Expected value of the number of key execution agreements N'

Frequency	□ = *0.001*	□ = *0.0015*	□ = *0.002*
□*1* = *20*	19.99	89.41	399.81
□*2* = *30*	89.11	841.18	7940.54

$□_3 = 40$	396.23	7887.04	156994.80

When the bit error rate □ of node A and node B and the number of key negotiation times t take different values, the expected value of the number of times the key is established to execute the agreement N'is shown in Table 1.

It can be concluded from Table 1 that the expected value of □′ is related to the bit error rate □, the number of times □, and the length of the key string □. When $□ = 0.001$, the execution efficiency of the agreement is the highest. In underwater acoustic communication, the maximum data transmission rate can reach 10 kbit/s [23]. When $□ = 300, □ = 20, □' = 19.99$, the total number of bits transmitted by the key agreement is 119940 bits, and the lower bound of the total length of the key string generated after confidentiality enhancement is 117331 bits. The upper bound is 2609 bits, and the required time is 11.99s. It shows that under the current technical conditions, the agreement is feasible.

VI. Conclusion

In this paper, an interactive key extraction protocol based on Goelian coding and a confidentiality enhancement protocol based on the r-cyclic Toeplitz matrix under the uncertainty of ocean noise are designed to form a secure communication scheme based on the uncertainty of the underwater noise channel. Theoretical analysis and experimental results show that this scheme is not only safe and reliable, but also has high communication efficiency and low communication overhead. At the same time, it reduces the storage space of the matrix, improves the storage efficiency of confidentiality enhancement, and obtains the confidentiality enhancement key string lower bound of the length and the upper bound of the adversary's information about the key string.

References:

[1] Han, Guangjie, et al. "Secure communication for underwater acoustic sensor networks." IEEE communications magazine 53.8 (2015): 54-60.
[2] Diamant, Roee, Paolo Casari, and Stefano Tomasin. "Cooperative authentication in underwater acoustic sensor networks." IEEE Transactions on Wireless Communications 18.2 (2018): 954-968.
[3] Jiang, Shengming. "State-of-the-art medium access control (MAC) protocols for underwater acoustic networks: A survey based on a MAC reference model." IEEE communications surveys & tutorials 20.1 (2017): 96-131.
[4] El-Banna, Ahmad A. Aziz, Kaishun Wu, and Basem M. ElHalawany. "Application of Neural Networks for Dynamic Modeling of an Environmental-Aware Underwater Acoustic Positioning System Using Seawater Physical Properties." IEEE Geoscience and Remote Sensing Letters (2020).
[5] Godel, Kurt. On formally undecidable propositions of Principia Mathematica and related systems. Courier Corporation, 1992.

[6] Robert, Jean-Marc. "IBM TJ Watson Research Laboratory." Advances in Cryptology: Proceedings of CRYPTO'85. Vol. 218. Springer, 2007.
[7] Tan, Vincent YF, and Masahito Hayashi. "Analysis of remaining uncertainties and exponents under various conditional Renyi entropies." IEEE Transactions on Information Theory 64.5 (2018): 3734-3755.
[8] Chen, Xiaoting, Zhaolin Jiang, and Jianmin Wang. "Determinants and inverses of fibonacci and lucas skew symmetric toeplitz matrices." Journal of Advances in Mathematics and Computer Science (2016): 1-21.
[9] Bini, Dario A., and Beatrice Meini. "On the exponential of semi-infinite quasi-Toeplitz matrices." Numerische Mathematik 141.2 (2019): 319-351.
[10] Bennett, Charles H., and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing." arXiv preprint arXiv:2003.06557 (2020).
[11] Yin, Bo, et al. "Energy-efficient filtering for skyline queries in cluster-based sensor networks." Computers & Electrical Engineering 40.2 (2014): 350-366.
[12] Hayashi, Masahito. "Security analysis of $\varepsilon $-almost dual universal 2 hash functions: Smoothing of min entropy versus smoothing of Renyi entropy of order 2." IEEE Transactions on Information Theory 62.6 (2016): 3451-3476.
[13] Bennett, Charles H., et al. "Generalized privacy amplification." IEEE Transactions on Information theory 41.6 (1995): 1915-1923.
[14] Renner, Renato, and Stefan Wolf. "The exact price for unconditionally secure asymmetric cryptography." International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2004.
[15] Berta, Mario, Omar Fawzi, and Volkher B. Scholz. "Quantum-proof randomness extractors via operator space theory." IEEE Transactions on Information Theory 63.4 (2016): 2480-2503.
[16] Arnon-Friedman, Rotem, Renato Renner, and Thomas Vidick. "Simple and tight device-independent security proofs." SIAM Journal on Computing 48.1 (2019): 181-225.
[17] Tan, Vincent YF, and Masahito Hayashi. "Analysis of remaining uncertainties and exponents under various conditional Renyi entropies." IEEE Transactions on Information Theory 64.5 (2018): 3734-3755.
[18] Asif, Shahzad, et al. "A fully RNS based ECC processor." Integration 61 (2018): 138-149.
[19] Kraft, James S., and Lawrence C. Washington. An introduction to number theory with cryptography. Chapman and Hall/CRC, 2018.
[20] Hayashi, Masahito, and Toyohiro Tsurumaru. "More efficient privacy amplification with less random seeds via dual universal hash function." IEEE Transactions on Information Theory 62.4 (2016): 2213-2232.
[21] Bardenet, Rémi, Arnaud Doucet, and Chris Holmes. "On Markov chain Monte Carlo methods for tall data." The Journal of Machine Learning Research 18.1 (2017): 1515-1557.
[22] Sun, Tao, Hongwei Zhang, and Yuan Wang. "The application of information entropy in basin level water waste permits allocation in China." Resources, conservation and recycling 70 (2013): 50-54.

[23] Amar, Alon, Gilad Avrashi, and Milica Stojanovic. "Low complexity residual Doppler shift estimation for underwater acoustic multicarrier communication." IEEE Transactions on Signal Processing 65.8 (2016): 2063-2076.