

# A Low Probability of Interception Method Based on Nonlinear Transformation of Channel Transmission Characteristic

Wen Zhao<sup>\*</sup>, Boxiao Li, Ping Tang, Zejian Lu

China Academy of Electronics and Information Technology, 100041, Beijing, China.

**How to cite this paper:** Wen Zhao, Boxiao Li, Ping Tang, Zejian Lu. (2022) A Low Probability of Interception Method Based on Nonlinear Transformation of Channel Transmission Characteristic. *Advances in Computer and Communication*, 3(1), 1-15. DOI: 10.26855/acc.2022.04.001

**Received:** February 18, 2022

**Accepted:** March 15, 2022

**Published:** April 12, 2022

**\*Corresponding author:** Wen Zhao, China Academy of Electronics and Information Technology, 100041, Beijing, China.

**Email:** 3465665538@qq.com

---

## Abstract

To realize the low probability of interception communication system, this paper presents a memory nonlinear model to carry on nonlinear transformation for channel transmission characteristic. When primary signals are transmitted through this kind of system, the quality of signals will be observably deteriorated due to strong memory effect nonlinear distortion. Located at the frequency range where primary signals are, the nonlinearities decrease primary signals' signal to interference ratio (SIR) and memory effect introduce inter-symbol interference (ISI). Hence, with the purpose of encryption, the proposed model is designed to change both amplitude-frequency and phase-frequency characteristics in channel. At receiving end, suffered from bad SIR and ISI, illegal user cannot obtain correct information by I/Q demodulation and sample sentence processing, while authorized users can easily recover the primary signals waveform by proposed inverse nonlinear transformation model and get correct information next. The experiment results are provided to verify encryption effect of our method and analyze the loss of signal to noise ratio (SNR) of authorized user is also discussed for evaluating the impact of encryption method on conventional communication process.

## Keywords

Memory effect nonlinearity, Low probability of interception, Nonlinear transformation of channel state characteristic

---

## 1. Introduction

The remarkable advancement in communication technology has greatly changed the way people live their lives and contributes to a profound impact on social progress. Since encryption methods are the most effective way to achieve data security and protect privacy of legitimate user, it is significant to study on security communication technologies. In 1949, Shannon proposed his famous secure communication model so that the physical layer secure communication issue was the first time studied by quantitative methods based on information theory and statistical theory [1]. Since then, methods of physical layer secure communication have made a lot of progress.

In time-hopping system, in order to lower down probability of interception, authorized user synchronously receive signals with sender according to shared pseudo random sequence [2]. In spread spectrum system, sender converts primary information to spread spectrum sequences by pseudo random sequence and transmits radio-frequency signals through antenna after carrier modulation. For authorized user, dispreading can be completed by the same pseudo random sequence and then primary information is obtained [3-5]. In frequency-hopping system, carrier frequency is

changed by pseudo random sequence in real time so that illegal user cannot track radio-frequency signals synchronously [6, 7]. However, for the communication systems mentioned above, precise and efficient synchronization process is the essential precondition of achieving received signals' quality.

Based on antenna configuration and artificial noise, joint multi-antenna methods maximize authorized user's transfer information rate [8-13]. Antenna configuration can determine secure beamforming direction and select the best transmit antenna to decrease received signals' quality in wiretap channel [14-16]. Meanwhile, as artificial noise is added, illegal user can hardly distinguish where primary signals are located [9, 12]. Whereas when illegal user is near to authorized user, security of this kind of methods are hardly to guarantee, because their encryption don't handle on signals, but make a difference between authorized and illegal user's signals according to distinction of their physical location [12, 17].

Transform domain communication method belongs to initiative anti-interference method. By means of monitoring underutilized spectrum resource in real time, sender dynamically build basis functions basing on transform domain processing, such as discrete Fourier transform, discrete wavelet transform and fractional Fourier transform. These basis functions are applied to modulate information to make radio-frequency signals lying at vacant spectrum. Authorized user generates corresponding basis functions for correlation reception to recover signal waveform [18-20]. However, as distance between transmitting terminal and receiving terminal increasing, basis functions may be change resulting from variation of vacant spectrum. Hence, transform domain communication system may be difficult to adapt to long distance communication situation.

In conclusion, the existing physical encryption methods' performance is affected by some factors. Hence, this paper presents a physical encryption method of implementing nonlinear transformation on channel transmission characteristic. Its basic idea is that encryption at transmitting terminal and decryption at receiving terminal is completed by nonlinear transformation and inverse nonlinear transformation respectively. Compared to other methods, the proposed method doesn't require synchronization step for decryption. Besides that, its encryption performance of proposed method is only related to transformation model and has no concern with user's physical location and communication distance.

The outline of the remainder of this paper is as follows: In Section 2, the structure of memory nonlinear transformation pairs (MNT) is introduced. After that, derivation about MNT's amplitude-frequency nonlinear transformation pairs and their bandwidth control strategy for nonlinear spectral regrowth are studied. Finally, steps of designing phase-frequency nonlinear transformation are given. In Section 3, phase filter for phase-frequency nonlinear transformation is designed and its frequency domain response is shown. And then the proposed MNT model's encryption effect is verified using a QPSK signal. The loss of SNR of authorized user's signal after decryption is shown to analyze whether the proposed encryption method could have harmful influence on authorized user's signal quality. At last, conclusions are drawn in Section 4.

## 2. Memory nonlinear transformation pairs

Resulting from RF devices non-ideal characteristic, memory nonlinear distortions have an influence on amplitude and phase of signals. To be specific, nonlinearities are generated in spectrum as spectral regrowth. Among them, distortions, known as odd-order difference frequency components, are usually located in or near base-wave signals' band, which could reduce SIR. Meanwhile, memory effect causing phase distorted could introduce ISI into signals and decreases demodulation performance in receiving terminal by enhancing the difficulty of sampling and decision. From the point of physical layer security, if models representing non-ideal characteristics are reasonably chosen to design MNT for channel encryption, controllable signal waveform distortion and restoration will be realized. Thus, they can be regarded as encryption process in transmitting terminal and decryption process in receiving terminal, respectively. It means that by disturbing and hiding primary signals, security of communication system is enhanced and low probability of interception is realized.

### 2.1 Structure of nonlinear transformation pair

To realize low probability of interception, there are several restricted conditions when designing MNT:

(a) Strong nonlinearities are generated at the range of base-wave signals. In frequency domain, if primary signals power is lower than nonlinearities, they will be hidden. At this moment, illegal user won't be able to complete decryption for primary signals' center frequency, bandwidth and modulation style are hardly to identify.

(b) Deep memory effect is needed in MNT. The deeper memory effect is, the more serious ISI is brought in, which also contributes to add MNT's complexity and illegal user's decryption difficulty.

(c) Accurate inverse model of MNT is crucial. High complexity of MNT is significant for encryption system's security, but it also makes waveform restoration difficult. Therefore, MNT's inverse model must be accurate enough for authorized user to decrypt received signals.

Now let's discuss whether classical memory nonlinear models, such as Volterra model [21], Hammerstein model [22], are suitable for designing MNT. Asymmetric Volterra model is expressed as

$$y(k) = \sum_{d=1}^D \left[ \sum_{r_1=0}^{N_d-1} \sum_{r_2=r_1}^{N_d-1} \dots \sum_{r_d=r_{d-1}}^{N_d-1} h(r_1, r_2, \dots, r_d) \prod_{j=1}^d x(n-r_j) \right] \quad (1)$$

Where  $x(n)$  and  $y(n)$  is input and output signals of Volterra model. In (1),  $N_d$  is the  $d$ th order maximum memory depth ( $d = 1, 2, 3, \dots, D$ ) and  $h(r_1, r_2, \dots, r_d)$  is kernel coefficient. Literature [23] indicates that inverse Volterra model is still a Volterra model and its expression is

$$y = H_1(x) + \sum_{d=2}^D H_d(x) \quad (2)$$

In (2),  $H_1[x(n)] = \sum_{r_1=0}^{N_1-1} h(r_1)x(n-r_1)$  is linear term of Volterra model. If we assume that

$$z = G_1(y) + \sum_{d=2}^D G_d(y) \quad (3)$$

is the inverse model of equation (2) and  $D' \geq D$ , then

$$\begin{cases} G_1 = H_1^{-1} \\ G_d = -H_1^{-1} H_d H_1^{-1} \quad (d = 2, 3, \dots, D) \end{cases} \quad (4)$$

Considering that Hammerstein model can be treated as a simplified version of Volterra model, its inverse model can also be deduced. Hence, there is no more detailed description in this paper. Equation (1) indicates that number of kernel coefficients of classical nonlinear model rises up rapidly when depth increases.

However, it is can be expected that if MNT is designed using classical nonlinear model, when Condition (a) is met, the number of kernel coefficients must too many and transmitting them as encryption parameters from sender to authorized user is not convenient. Moreover, Equation (4) is not exact solution for inverse Volterra model, because nonlinearities whose order is higher than  $D$  will appear when these two nonlinear systems are cascaded. To sum up, classical nonlinear models cannot be adapt to channel encryption. Therefore, in this paper, amplitude transformation based on power series and phase transformation based on group delay are cascaded together to form a memory nonlinear model as MNT for channel encryption. The structure of proposed model is shown in Figure 1.

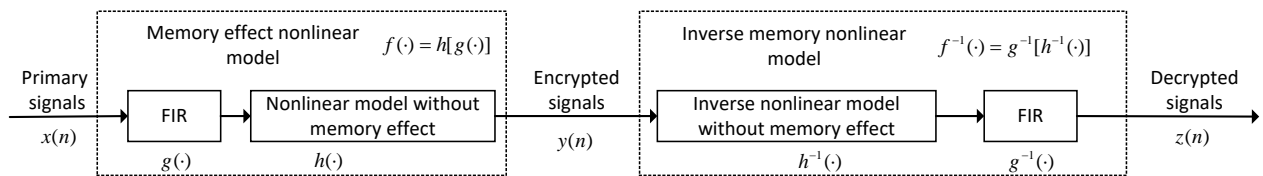


Figure1. Structure of MNT.

MNT includes two parts, amplitude-frequency and phase-frequency nonlinear transformation pair. Assume that  $h(\cdot)$  and  $h^{-1}(\cdot)$  are nonlinear responses which is the inverse of each other respectively. Meanwhile,  $g(\cdot)$  and  $g^{-1}(\cdot)$  are linear time domain responses which is the inverse of each other respectively. If the two conditions below are satisfied,

$$x(n) = h^{-1}\{h[x(n)]\}, \text{ amplitude constraint condition} \quad (5)$$

$$x(n - \tau) = g^{-1}\{g[x(n)]\}, \text{ phase constraint condition} \quad (6)$$

then  $z(n)$  can be expressed as

$$z(n) = f^{-1}\{f[x(n)]\} = g^{-1}\{h^{-1}\{h\{g[x(n)]\}\} = x(n - \tau) \quad (7)$$

where

$$f[x(n)] = h\{g[x(n)]\} = \sum_{d=1}^D a_d \left[ \sum_{r_d=0}^{N_d-1} g(r_d) x(n - r_d) \right]^d \quad (8)$$

In (8),  $d = 1, 2, 3, \dots, D$  is the order of power series model.  $N_d$  is  $d$ th order maximum memory depth.  $a_d$  is coefficient of  $d$ th order power series.  $g(r_d)$  is  $d$ th order coefficient whose memory depth is  $r_d$ . Equation (7) indicates that when constraint conditions (5) and (6) are met, the signals  $z(n)$  authorized user obtaining is the signals  $x(n)$  with delay  $\tau$ . The following Section 2.2, 2.3 and 2.4 will introduce amplitude-frequency and phase-frequency nonlinear transformation pair.

## 2.2 Amplitude-frequency nonlinear transformation pair

If input baseband signals at transmitting terminal are  $x(n)$ , its 3rd order difference frequency components are  $|x(n)|^2 x(n)$ . The output signals  $y(n)$  can be written as

$$y(n) = a x(n) + c x(n) |x(n)|^2 \quad (9)$$

In (9),  $a$  and  $c$  is 1st and 3rd order coefficient of power series model respectively. In order to make the power of base-wave signals  $x(n)$  stay the same when encryption process is carried on, let  $a = 1$ ,  $c > 0$ . Write (9) as a simplified version  $y = x + c |x|^2 x$  and let real and imaginary part of  $x$  and  $y$  be

$$\begin{aligned} x &= i + jq \\ y &= I + jQ \end{aligned} \quad (10)$$

Substitute (10) into (9), we can obtain

$$\begin{aligned} I &= i + c(i^2 + q^2) \\ Q &= q + cq(i^2 + q^2) \end{aligned} \quad (11)$$

Combine two equations in (11), we can get

$$\frac{i}{I} = \frac{q}{Q} \quad (12)$$

Substitute (12) into (11), we can obtain

$$\begin{aligned} I &= i + c \left[ 1 + \left( \frac{Q}{I} \right)^2 \right] i^3 \\ Q &= q + c \left[ 1 + \left( \frac{I}{Q} \right)^2 \right] q^3 \end{aligned} \quad (13)$$

Take (13) as an example,  $I$  can be seen as a function of independent variable  $i$ . Calculate the derivative of  $I$  to  $i$ , we get

$$\frac{dI(i)}{di} = 1 + 3c[1 + (\frac{q}{i})^2]i^2 > 0$$

It means that  $I$  is monotone increasing function of  $i$ , which indicates that there is an inverse function  $i = h^{-1}(I)$  and when the inverse function is the inverse model of equation (9). From (13), we can see that  $Q(q)$  is similar to  $I(i)$ , so we only deduce  $i = h^{-1}(I)$ . The process of calculating the inverse function  $i = h^{-1}(I)$  is equivalent to finding the solution of cubic equation of one variable

$$c[1 + (\frac{Q}{I})^2]i^3 + i - I = 0 \quad (14)$$

According to appendix in this paper, equation (14) has the only real root

$$i = \sqrt[3]{A} + \sqrt[3]{B} = \left[ -\frac{n}{2} + \sqrt{\left(\frac{n}{2}\right)^2 + \left(\frac{m}{3}\right)^3} \right]^{\frac{1}{3}} + \left[ -\frac{n}{2} - \sqrt{\left(\frac{n}{2}\right)^2 + \left(\frac{m}{3}\right)^3} \right]^{\frac{1}{3}}$$

Let

$$t = c[1 + (\frac{I}{Q})^2] \text{ and } s(I) = \left[ \frac{I + \sqrt{I^2 + 4/(27t)}}{2t} \right]^{\frac{1}{3}} \quad (15)$$

The inverse function  $i = h^{-1}(I)$  is

$$i = h^{-1}(I) = s(I) - \frac{1}{3t \cdot s(I)} \quad (16)$$

In conclusion, if authorized user have obtained  $c$ , primary baseband signals can be restored. Therefore, we can take (9) and (16) as nonlinear transformation pair without memory effect to meet amplitude constraint condition in equation (5).

### 2.3 Bandwidth restriction for encrypted signals

Section 2.2 has provided the expression of amplitude-frequency nonlinear transformation. However, 3rd difference frequency components locate not only at baseband signals' position in frequency domain, but also at left and right first adjacent channel. It makes encrypted signals bandwidth being three times of baseband signals' which as a result will lower down spectral efficiency. So in this section, bandwidth restriction method is discussed for encrypted signals.

The primary baseband signals' frequency range is from  $\omega_l$  to  $\omega_h$ . Assume that response function of bandpass filter for removing redundant nonlinear spectral regrowth is  $H(\cdot)$  whose upper and lower cutoff frequency is also set to  $\omega_l$  and  $\omega_h$  respectively. After filtering, the encrypted signals are

$$H[y(n)] = H[ax(n) + cx(n)|x(n)|^2] \quad (17)$$

Since bandpass filter belongs to causal and stable system, linear superposition is satisfied. Then equation (17) can be written as

$$H[y(n)] = aH[x(n)] + cH[x(n)|x(n)|^2] \quad (18)$$

In (18),  $H[x(n)]$ ,  $H[y(n)]$  and  $H[x(n)|x(n)|^2]$  is primary signals, encrypted signals and 3rd order difference frequency components after filter respectively. Now let's analyze their frequency components. The input and output signals in frequency domain can be expressed as

$$x(n) = \sum_{\omega=\omega_l}^{\omega=\omega_h} X(\omega)e^{-j\omega n} + \sum_{\omega=0}^{\omega_l} X(\omega)e^{-j\omega n} + \sum_{\omega=\omega_h}^{2\pi} X(\omega)e^{-j\omega n} \quad (19)$$

$$y(n) = \sum_{\omega=\omega_l}^{\omega_h} Y(\omega)e^{-j\omega n} + \sum_{\omega=0}^{\omega_l} Y(\omega)e^{-j\omega n} + \sum_{\omega=\omega_h}^{2\pi} Y(\omega)e^{-j\omega n} \quad (20)$$

In (19) and (20),  $X(\omega)$  and  $Y(\omega)$  is frequency spectrum of  $x(n)$  and  $y(n)$ , respectively. In the frequency range of  $\omega_l$  to  $\omega_h$ ,

$$\sum_{\omega=\omega_l}^{\omega_h} Y(\omega)e^{-j\omega n} = a \sum_{\omega=\omega_l}^{\omega_h} X(\omega)e^{-j\omega n} + c \sum_{\substack{\omega_1, \omega_2, \omega_3=0 \\ \omega_1+\omega_2-\omega_3 \in [\omega_l, \omega_h]}}^{2\pi} X(\omega_1)X(\omega_2)X(\omega_3)e^{-j(\omega_1+\omega_2-\omega_3)n} \quad (21)$$

In the view that  $X(\omega)$  is primary signals frequency spectrum that has no interference, magnitudes of components whose frequency belongs to  $[\omega_l, \omega_h]$  are very low. Then we can infer that

$$\sum_{\substack{\omega_1, \omega_2, \omega_3=0 \\ \omega_1+\omega_2-\omega_3 \in [\omega_l, \omega_h]}}^{2\pi} X(\omega_1)X(\omega_2)X(\omega_3)e^{-j(\omega_1+\omega_2-\omega_3)n} \approx \sum_{\substack{\omega_1, \omega_2, \omega_3=\omega_l \\ \omega_1+\omega_2-\omega_3 \in [\omega_l, \omega_h]}}^{\omega_h} X(\omega_1)X(\omega_2)X(\omega_3)e^{-j(\omega_1+\omega_2-\omega_3)n} \quad (22)$$

Then equation (21) can be written as

$$\begin{aligned} \sum_{\omega=\omega_l}^{\omega_h} Y(\omega)e^{-j\omega n} &\approx a \sum_{\omega=\omega_l}^{\omega_h} X(\omega)e^{-j\omega n} + c \sum_{\substack{\omega_1, \omega_2, \omega_3=\omega_l \\ \omega_1+\omega_2-\omega_3 \in [\omega_l, \omega_h]}}^{\omega_h} X(\omega_1)X(\omega_2)X(\omega_3)e^{-j(\omega_1+\omega_2-\omega_3)n} \\ &= a \sum_{\omega=\omega_l}^{\omega_h} X(\omega)e^{-j\omega n} + c \sum_{\omega=\omega_l}^{\omega_h} X(\omega)e^{-j\omega n} \left| \sum_{\omega=\omega_l}^{\omega_h} X(\omega)e^{-j\omega n} \right|^2 \end{aligned} \quad (23)$$

According to (23), if authorized user implements inverse nonlinear transformation of (15) and (16), frequency components of restored signals from  $\omega_l$  to  $\omega_h$  are

$$\sum_{\omega=\omega_l}^{\omega_h} X(\omega)e^{-j\omega n} = H[x(n)]$$

It should be pointed out that  $H[y(n)] \neq aH[x(n)] + cH[x(n)]|H[x(n)]|^2$ . The 3rd order components  $cH[x(n)]|H[x(n)]|^2$  means that there are new spectral regrowth generated at  $\omega \notin [\omega_l, \omega_h]$ , while for encrypted signals  $y(n)$ , there are no nonlinearities appearing at the same frequency range after filtering.

To summarize, if there are signals  $z(n)$  making  $H[y(n)] = az(n) + cz(n)|z(n)|^2$ , after decryption, in the range of  $\omega \in [\omega_l, \omega_h]$ , the components are approximately equal to  $\sum_{\omega=\omega_l}^{\omega_h} X(\omega)e^{-j\omega n}$ . The above discussion indi-

cates that after the proposed amplitude-frequency nonlinear transformation in Section 2.2, the encrypted signals can be filtered making their bandwidth equal to primary signals and the following decryption and demodulation at receiving terminal will not be affected remarkably by such filtering approach.

## 2.4 Phase-frequency nonlinear transformation pair

Although primary signals can be hidden after amplitude-frequency nonlinear transformation, the encryption model is too simple to prevent cracking since illegal user can realize decryption by searching. For sake of promoting MNT's complexity, memory effect must be brought into it. From the phase constraint condition, principle of designing phase-frequency nonlinear transformation pair is making the phase encryption filter  $g(\cdot)$  and phase decryption filter  $g^{-1}(\cdot)$  meet the following conditions in  $\omega \in [0, 2\pi]$ .

$$\begin{cases} \text{delay}_g(\omega) \neq \text{const} \\ \text{delay}_g(\omega) + \text{delay}_{g^{-1}}(\omega) = \text{const} \quad (\text{const} > 0) \end{cases} \quad (24)$$

where  $\text{const}$  is set to be a positive constant. Equation (24) means by phase encryption filter whose group delay function is  $\text{delay}(\omega)$ , primary signals  $x(n)$  are distorted by ISI and become encrypted signals  $y(n)$ . In frequency domain, encryption filter makes different frequency components in  $x(n)$  at the same sampling time output at different moments in  $y(n)$ . When  $y(n)$  are received by authorized user, ISI in  $y(n)$  can be eliminated by decryption filter whose group delay function is  $\text{delay}^{-1}(\omega)$  and components with different delays are adjusted to output at same sampling time again in decrypted signals  $\hat{x}(n)$ . The final result is there is a constant delay between  $x(n)$  and  $\hat{x}(n)$ , or say  $\hat{x}(n) = x(n - \text{const})$ .

If primary signals  $x(n)$  are treated as electromagnetic waves of different frequencies, the impact of encryption filter on  $x(n)$  is making scattering effect happen and relative speeds of different frequency waves in  $x(n)$  are changed resulting in  $x(n)$  encrypted and transformed into encryption signals  $y(n)$ . Even if these ‘disorganized’ signals  $y(n)$  are intercepted,  $y(n)$  can hardly be restored to correct waveform since illegal user is lack of group delay function  $\text{delay}(\omega)$ . But authorized user can easily remove scattering effect in  $y(n)$  by corresponding decryption filter and obtain correct information.

The expressions of group delay function include sinusoidal function, rational function and Fourier series [24]. In this paper, sinusoidal function is chosen as example to introduce detailed procedures of designing encryption filter.

(a) Determine encryption filter’s group delay function  $\text{delay}(\omega)$  and decryption filter’s group delay function  $\text{delay}^{-1}(\omega)$ . If at the frequency range  $\omega \in [0, \pi]$ ,

$$\begin{aligned} \text{delay}_g(\omega) &= A \sin(2M\omega) + B \\ \text{delay}_{g^{-1}}(\omega) &= -A \sin(2M\omega) + B \end{aligned} \quad (25)$$

In (25),  $A$  is the amplitude of sinusoidal function.  $M$  is the number of oscillation of sinusoidal function at  $\omega \in [0, \pi]$  and  $B$  is the oscillation center. Because  $g(\cdot)$  and  $g^{-1}(\cdot)$  are both causal filters,  $B > A > 0$ . According to equation (25),

$$\text{delay}_g(\omega) + \text{delay}_{g^{-1}}(\omega) = 2B > 0$$

which satisfies the conditions in (24).

(b) Calculate phase-frequency functions  $\phi_g(\omega)$  and  $\phi_{g^{-1}}(\omega)$ . According to definition of group delay

$$\text{delay}(\omega) = -\frac{d\phi(\omega)}{d\omega}$$

where  $\phi(\omega)$  is phase-frequency function of filter.  $\phi_g(\omega)$  and  $\phi_{g^{-1}}(\omega)$  can be obtained by calculating the integral of  $\text{delay}(\omega)$  to  $\omega$  and  $\text{delay}^{-1}(\omega)$  to  $\omega$ . In order to ensure filter coefficients in time domain belong to real number, the phase-frequency function should meet the following center symmetric conditions as follow.

$$\begin{cases} \phi_g(\omega) = -\phi_g(2\pi - \omega) \\ \phi_{g^{-1}}(\omega) = -\phi_{g^{-1}}(2\pi - \omega) \\ \phi_g(\pi) = \phi_{g^{-1}}(\pi) = 0 \end{cases} \quad (26)$$

Setting  $\phi_g(\pi) = \phi_{g^{-1}}(\pi) = 0$  as initial condition when obtaining  $\phi_g(\omega)$  and  $\phi_{g^{-1}}(\omega)$ , in the range  $\omega \in [0, \pi]$ , we can get

$$\begin{aligned}\phi_g(\omega) &= -\frac{A}{2M}\cos(2M\omega) + B\omega + \frac{A}{2M} - B\pi \\ \phi_{g^{-1}}(\omega) &= \frac{A}{2M}\cos(2M\omega) + B\omega - \frac{A}{2M} - B\pi\end{aligned}\tag{27}$$

Then  $\phi_g(\omega)$  and  $\phi_{g^{-1}}(\omega)$  in the range  $\omega \in [\pi, 2\pi]$  can be determined by (26) and (27).

(c) Calculating frequency domain responses  $G(\omega)$  and  $G^{-1}(\omega)$ . From (27) we can infer that in the range  $\omega \in [0, 2\pi]$ , the expressions of  $G(\omega)$  and  $G^{-1}(\omega)$  are

$$\begin{aligned}G(\omega) &= e^{j\phi_g(\omega)} \\ G^{-1}(\omega) &= e^{j\phi_{g^{-1}}(\omega)}\end{aligned}\tag{28}$$

(d) Calculating time domain responses  $g(\cdot)$  and  $g^{-1}(\cdot)$ . Carrying on fast Fourier transformation (FFT) on  $G(\omega)$  and  $G^{-1}(\omega)$ , filter coefficients in time domain are finally obtained.

In fact, the memory effect of MNT is designed based on group delay function and the kernel coefficients  $g(r_d)$  in equation (7) are corresponding to filter coefficients in time domain. So when encryption transmission is carried out, only the group delay function model and its parameters are need for authorized user. Comparing to using classical nonlinear model to design MNT, complexity of proposed encryption model can be effectively increased which can greatly enhance illegal user's decryption difficulty.

### 3. Results and discussion

In this Section, encryption effect of proposed MNT is discussed. Figure 2 shows procedure of testing the proposed method's encryption effect.

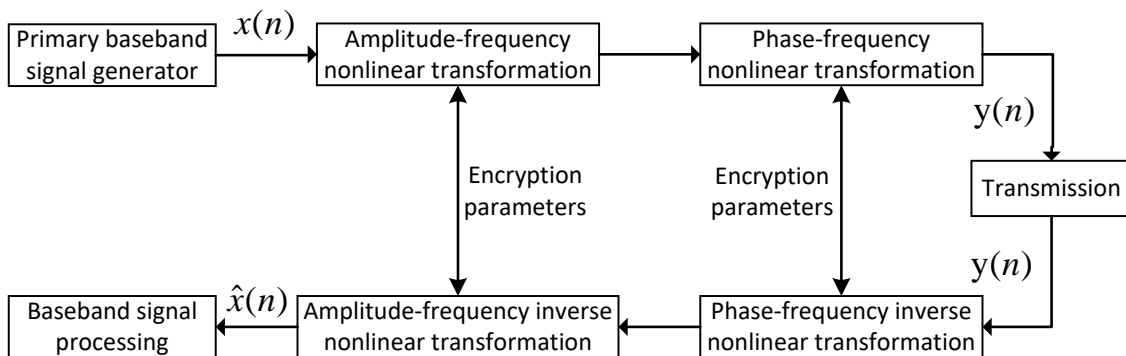


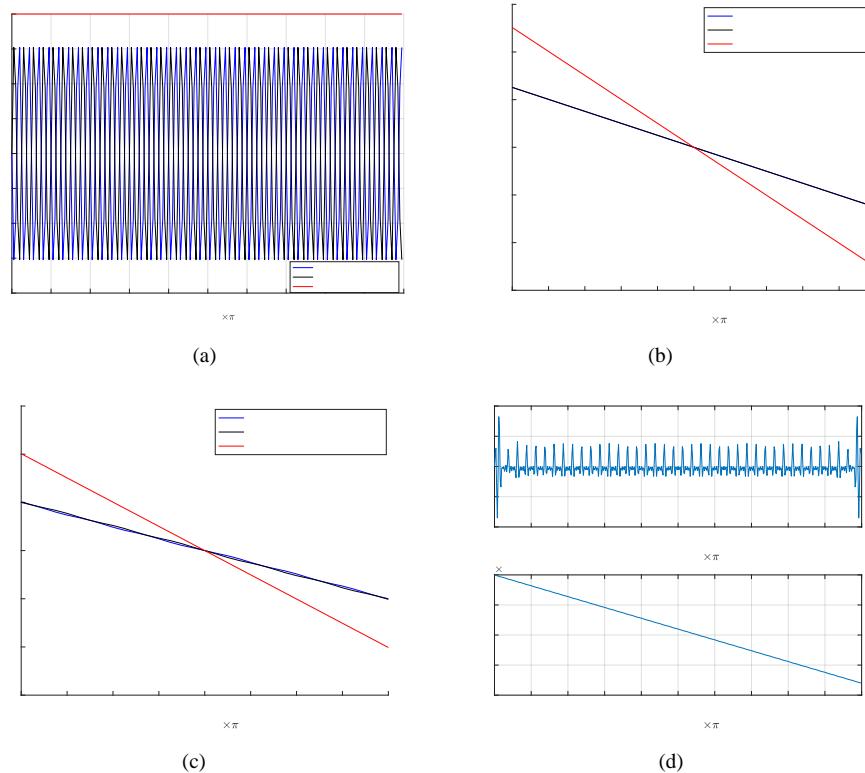
Figure 2. Procedure of testing the proposed method's encryption effect.

At transmitting terminal, primary baseband signals  $x(n)$  are encrypted after amplitude-frequency and phase-frequency nonlinear transformation. Encrypted signals  $y(n)$  are transmitted from sender to authorized user through channel. When authorized user receives  $y(n)$ , basing on corresponding encryption parameters, amplitude-frequency and phase-frequency inverse nonlinear transformation are formed and applied to  $y(n)$ . Finally the restored signals  $\hat{x}(n)$  are obtained for following up baseband signal process to evaluate proposed encryption method's performance.

#### 3.1 Design of phase-frequency nonlinear transformation pair

Firstly, results of designing phase-frequency nonlinear transformation pair are shown. Equation (25) is chosen as group delay function model. The parameters are set as  $A = 160$ ,  $M = 160$ ,  $B = 200$ . The order of filter is 400.

Figure 3 are group delays and frequency domain responses of phase encryption and decryption filter. In the range  $\omega \in [0, \pi]$ , group delay of encryption filter is a sinusoid function of frequency vibrating at center  $B = 200$  with an oscillating frequency of  $M = 160$  and an oscillating amplitude of  $A = 160$ . There is a similar situation in decryption filter except having an opposite oscillating direction. After cascade, their group delay equals to a constant of  $2B = 400$  shown in Figure 3(a). This conclusion can also be inferred from Figure 3(b) and 3(c), which have a linear phase characteristic with negative slope after cascade. In Figure 3(d), the designed filters' amplitude-frequency and phase-frequency characteristics are calculated. Its maximum of pass band damping is less than 0.1dB and its slope of phase-frequency is equal to a negative constant. To sum up, the above results indicate the designed filters have a satisfied characteristic for constructing MNT's phase-frequency nonlinear transformation pair.



**Figure 3. Phase-frequency nonlinear transformation based on sinusoidal function group delay. (a) group delay, (b) phase response from 0 to  $\pi$ , (c) phase response near  $\omega = \pi$ , (d) frequency domain response.**

### 3.2 Verification of the proposed method's encryption effect

Test signal is a QPSK signal with a 200ksym/s symbol rate and 2MHz sampling rate. Its roll-off factor is 1. The amplitude-frequency nonlinear transformation pair's coefficient  $c$  is set to  $2 \times 10^4$  in order to make nonlinearities' power approximately equal to baseband signal. The normalized pass band cut-off frequency is 0.2. The designed filters in Section 3.1 are chosen as MNT's phase-frequency nonlinear transformation pair. The encryption effect is shown in Figure 4.

The spectrum and constellation of QPSK signal intercepted by illegal user are shown in Figure 4(a) and 4(d). From these two figures, we can see nonlinearities cover baseband signals and meanwhile constellation points gather to (0,0). In this case, neither can illegal user find center frequency of baseband QPSK from intercepted signal nor make right decision on sampling judgment. As an authorized user, after amplitude-frequency and phase-frequency nonlinear transformation, the encrypted QPSK is restored to decrypted one since nonlinearities are eliminated and constellation distributes regularly. It can be inferred from above discussion that after MNT encryption, the difference of received signal quality between authorized and illegal user is obvious. Besides that, compared to encrypted signal's spectrum, decrypted QPSK's power changes little. It means communication system based on MNT can achieve satisfied security performance without too much power loss.

### 3.3 Loss of SNR of authorized user’s signal after decryption

In Section 3.2, power of nonlinear distortions is approximately equal to primary baseband QPSK. To illegal user, it is difficult to identify baseband signal’s modulation style and obtain a correct decode result. Nevertheless, while MNT communication system can provide fine security, it is a valuable research whether primary signal’s demodulation performance is worsen during MNT encryption. In Section 2.3, we make an assumption of equation (22), where magnitude of 3rd order nonlinearities generated by frequency components belonging to  $[0, \omega_l]$  or  $[\omega_h, \pi]$  is low enough to be ignored. So it is necessary to analyze the loss of SNR in authorized user’s signal after decryption when bandwidth restriction method is utilized.

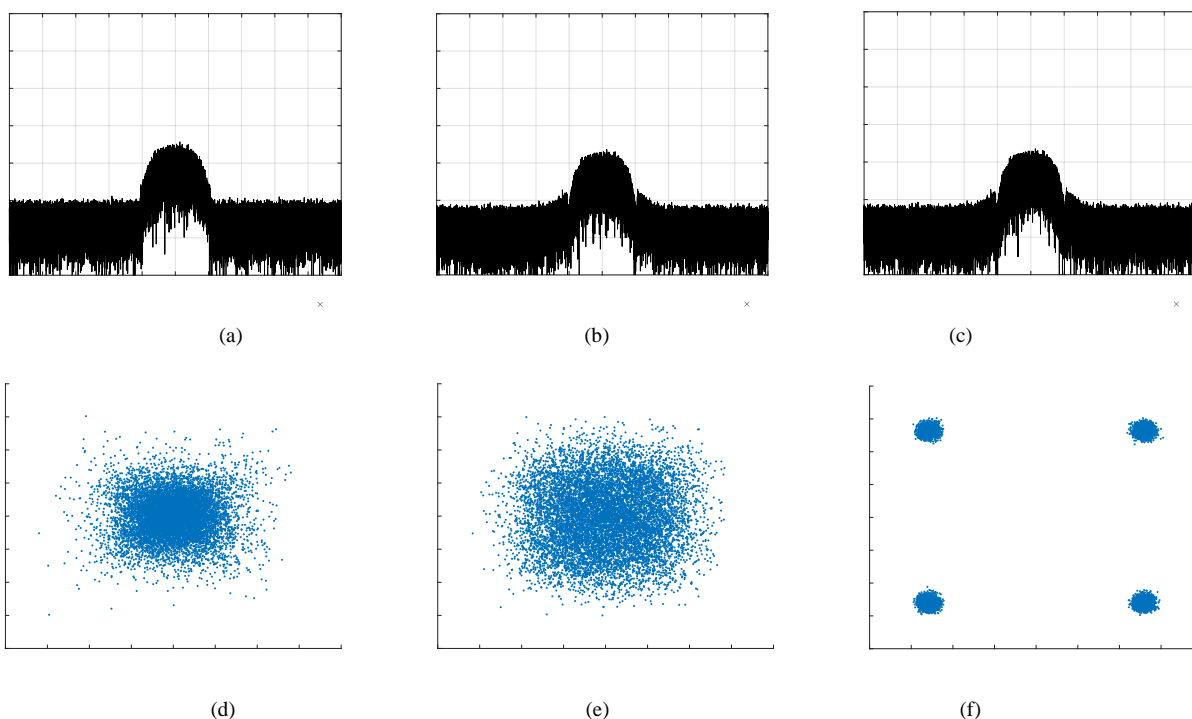


Figure 4. Encryption effect test of QPSK signal. (a) and (d) is power spectrum and constellation of illegal user’s received signal, respectively, (b) and (e) is power spectrum and constellation after inverse amplitude-frequency nonlinear transformation, respectively, (c) and (f) is power spectrum and constellation after inverse phase-frequency nonlinear transformation, respectively.

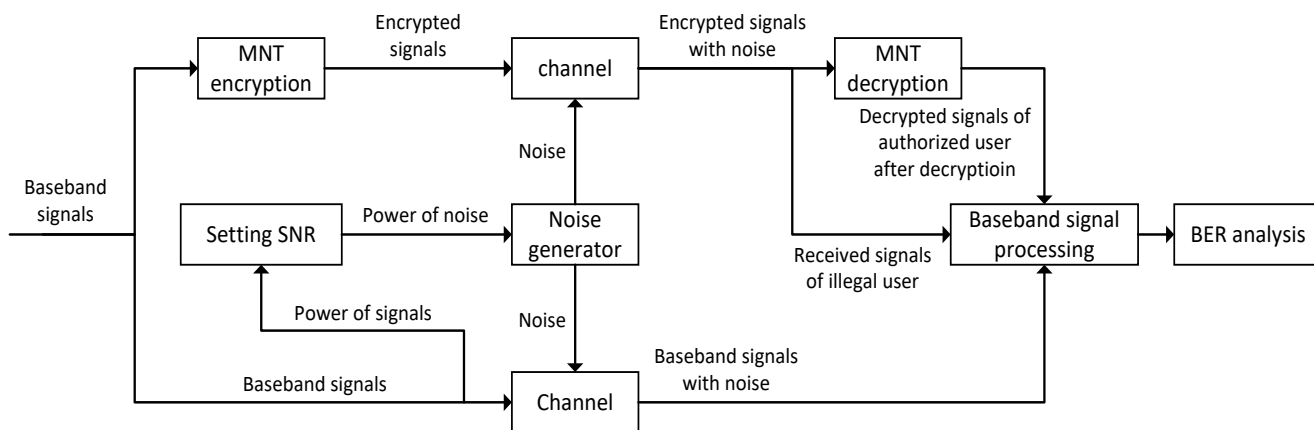


Figure 5. Procedure of BER analysis.

Figure 5 introduces the bit error rate (BER) testing experiment for communication system basing on MNT. The specific process is as follow:

- (a) Calculate primary signal's power  $P_s$ ;
- (b) Set a primary signal's SNR according to  $P_s$  and generate noise with corresponding power  $P_n$ ;
- (c) Calculate BERs of primary signal, authorized user's received signal and illegal user received signal after transmission until all planned SNRs are obtained.

Test signal is a 16QAM signal with a 200ksym/s symbol rate and 2MHz sampling rate. Its roll-off factor is 1. MNT model for encryption is the same as the one used in Section 3.2.

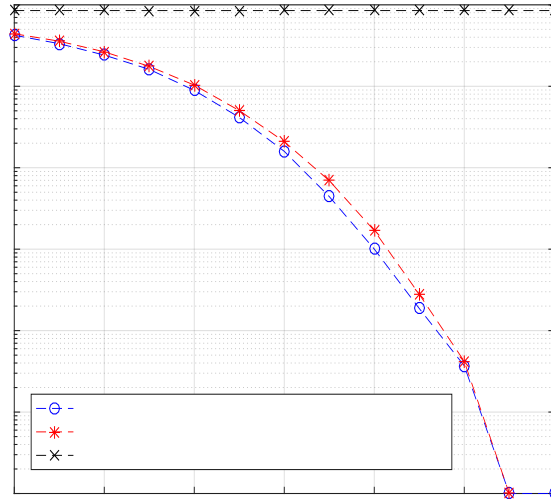


Figure 6. BER of each primary base-wave signal SNR from 0dB to 12dB.

In the same primary signal SNR condition, Figure 6 shows BERs of primary signal, authorized user's received signal and illegal user received signal after transmission. No matter how much primary signal's SNR is, BER of illegal user has no obvious change and remains close to  $10^0$ . It suggests that as an illegal user, received signal's demodulation performance cannot be improved by increasing its SNR at receiving terminal. Therefore, communication system based on MNT can achieve good secure effect as expected.

On the other hand, comparing the BERs between primary 16QAM and authorized user's received 16QAM, they both decrease obviously as SNR increasing and have the same order of magnitude. The result illustrates that after filtering 3rd intermodulation located at the adjacent channel of primary signal by bandwidth restriction method, loss of SNR of received signal after decryption is so little that authorized user can obtain correct information by common demodulation steps.

#### 4. Conclusion

In this paper, an encryption method of nonlinear transformation of channel transmission characteristic is presented for solving physical layer security. The contributions are as follows:

- (1) A nonlinear transformation pair MNT basing on power series model and group delay model is presented for channel encryption. Based on power series model and sinusoid model of group delay, amplitude-frequency and phase-frequency nonlinear transformation are provided to meet amplitude and phase constraint conditions for building MNT with deep memory and strong nonlinear effect. Encryption using proposed MNT can give consideration to communication security and convenience of encryption parameter transmission.

- (2) Based on difference components of 3rd order intermodulation, amplitude-frequency nonlinear transformation pair to baseband signals is provided. Besides, bandwidth restriction for encrypted signals is discussed to increase spectrum efficiency.

- (3) Based on sinusoid function of group delay, phase-frequency nonlinear transformation pair is provided. Its de-

sign steps in frequency domain are introduced and its designing results are shown.

(4) MNT's encryption effect is tested and loss of SNR of authorized user's signal after encryption is shown. From results, security of proposed encryption method is verified and feasibility of bandwidth restriction is proved.

## References

- [1] Shannon, C. E. (1949). Communication theory of secrecy systems [J]. *Bell System Technical Journal*, 1949, 28(4): 656-715.
- [2] Lam, A. W., Sarwate, D. V. (1990). Time-hopping and frequency-hopping multiple-access packet communications [J]. *IEEE Transactions on Communications*, 1990, 38(6): 875-888.
- [3] Win, M. Z., Scholtz, R. A. (2000). Ultra-wide bandwidth time-hopping spread-spectrum impulse radio for wireless multiple-access communications [J]. *IEEE Transactions on Communications*, 2000, 48(4): 679-689.
- [4] Simon, M. K., Omura, J. K., Scholtz, R. A., et al. (1994). *Spread spectrum communications handbook* [M]. New York: McGraw-Hill, 1994.
- [5] Peterson, R. L., Ziemer, R. E., Borth, D. E. (1995). *Introduction to spread-spectrum communications* [M]. New Jersey: Prentice hall, 1995.
- [6] Win, M. Z., Scholtz, R. A. (1998). Impulse radio: How it works [J]. *IEEE Communications letters*, 1998, 2(2): 36-38.
- [7] Win, M. Z., Scholtz, R. A. (2000). Ultra-wide bandwidth time-hopping spread-spectrum impulse radio for wireless multiple-access communications [J]. *IEEE Transactions on Communications*, 2000, 48(4): 679-689.
- [8] Renna, F., Bloch, M. R., Laurenti, N. (2012). Semi-blind key-agreement over MIMO fading channels [J]. *IEEE Transactions on Communications*, 2012, 61(2): 620-627.
- [9] Appendix: Yang, N., Elkashlan, M., Duong, T. Q., et al. (2015). Optimal transmission with artificial noise in MISOME wiretap channels [J]. *IEEE Transactions on Vehicular Technology*, 2015, 65(4): 2170-2181.
- [10] Yang, N., Yan, S., Yuan, J., et al. (2015). Artificial noise: Transmission optimization in multi-input single-output wiretap channels [J]. *IEEE Transactions on Communications*, 2015, 63(5): 1771-1783.
- [11] Zhang, X., Zhou, X., McKay, M. R. (2013). On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels [J]. *IEEE Transactions on Vehicular Technology*, 2013, 62(5): 2170-2181.
- [12] Huang, J., Swindlehurst, A. L. (2011). Cooperative jamming for secure communications in MIMO relay networks [J]. *IEEE Transactions on Signal Processing*, 2011, 59(10): 4871-4884.
- [13] Deng, H., Wang, H. M., Guo, W., et al. (2014). Secrecy transmission with a helper: To relay or to jam [J]. *IEEE Transactions on Information Forensics and Security*, 2014, 10(2): 293-307.
- [14] Wang, X., Zhang, Z., Long, K. (2015). Secure beamforming for multiple-antenna amplify-and-forward relay networks [J]. *IEEE Transactions on Signal Processing*, 2015, 64(6): 1477-1492.
- [15] Gong, X., Yin, H., Dong, F., et al. (2016). Robust beamforming design for secrecy in multiuser peer-to-peer wireless relay networks [J]. *IEEE Systems Journal*, 2016, 12(1): 682-690.
- [16] Wang, C., Wang, H. M., Ng, D. W. K., et al. (2015). Joint beamforming and power allocation for secrecy in peer-to-peer relay networks [J]. *IEEE Transactions on Wireless Communications*, 2015, 14(6): 3280-3293.
- [17] Wang, W., The, K. C., Li, K. H. (2015). Generalized relay selection for improved security in cooperative DF relay networks [J]. *IEEE Wireless Communications Letters*, 2015, 5(1): 28-31.
- [18] Chang, C., Huan, H., Xu, J., et al. (2017). Multidimensional parallel combinatory transform domain communication system [J]. *International Journal of Communication Systems*, 2017, 30(11): e3249.
- [19] Chakravarthy, V., Nunez, A. S., Stephens, J. P., et al. (2005). TDCS, OFDM, and MC-CDMA: a brief tutorial [J]. *IEEE Communications Magazine*, 2005, 43(9): S11-S16.
- [20] Chakravarthy, V., Li, X., Wu, Z., et al. (2009). Novel overlay/underlay cognitive radio waveforms using SD-SMSE framework to enhance spectrum efficiency-part I: theoretical framework and analysis in AWGN channel [J]. *IEEE Transactions on Communications*, 2009, 57(12): 3794-3804.

- [21] Koepl, H. (2009). A Local Nonlinear Model for the Approximation and Identification of a Class of Systems [J]. IEEE Transactions on Circuits & Systems II Express Briefs, 2009, 56(4): 315-319.
- [22] Matsui, M. (1994). Linear cryptanalysis method for DES cipher (III) [C]/Proceedings of the 1994 Symposium on Cryptography and Information Security (SCIS 94), Lake Biwa, Japan. 1994, 27-29.
- [23] Tsimbinos, J. (1995). Identification and compensation of nonlinear distortion [D]. University of South Australia, 1995.
- [24] Zhu, Z., Leung, H., Huang, X. (2013). Challenges in reconfigurable radio transceivers and application of nonlinear signal processing for RF impairment mitigation [J]. IEEE Circuits and Systems Magazine, 2013, 13(1): 44-65.

**Solution of equation (14)**  $c[1+(\frac{Q}{I})^2]i^3+i-I=0$

Making

$$m=1/c[1+(\frac{Q}{I})^2], n=-I/c[1+(\frac{Q}{I})^2]$$

If  $i=u+v$  is supposed as the solution of  $c[1+(\frac{Q}{I})^2]i^3+i-I=0$ , substitute  $m, n$  and  $i$  into it.

Then we can obtain

$$(u+v)(3uv+m)+(u^3+v^3+n)=0 \tag{1}$$

If  $u$  and  $v$  meet the condition  $u^3+v^3=-n$  and  $uv=-m/3$ , Equation (1) is satisfied. According to Vieta theorem,  $u^3$  and  $v^3$  are roots of equation  $e^2+ne-(m/3)^3=0$  and its solution are

$$e=-\frac{n}{2} \pm \sqrt{\left(\frac{n}{2}\right)^2 + \left(\frac{m}{3}\right)^3}$$

or say

$$\begin{cases} u^3 = -\frac{n}{2} + \sqrt{\left(\frac{n}{2}\right)^2 + \left(\frac{m}{3}\right)^3} = A \\ v^3 = -\frac{n}{2} - \sqrt{\left(\frac{n}{2}\right)^2 + \left(\frac{m}{3}\right)^3} = B \end{cases}$$

Since  $uv=-m/3$ ,

$$\begin{cases} u_1 = \sqrt[3]{A} & u_2 = \sqrt[3]{A}\omega & u_3 = \sqrt[3]{A}\omega^2 \\ v_1 = \sqrt[3]{B} & v_2 = \sqrt[3]{B}\omega^2 & v_3 = \sqrt[3]{B}\omega \end{cases}$$

where  $\omega = -1 + \sqrt{3}j/2$ . Then the solutions of equation (1) are

$$\begin{cases} i_1 = u_1 + v_1 = \sqrt[3]{A} + \sqrt[3]{B} \\ i_2 = u_2 + v_2 = \sqrt[3]{A}\omega + \sqrt[3]{B}\omega^2 \\ i_3 = u_3 + v_3 = \sqrt[3]{A}\omega^2 + \sqrt[3]{B}\omega \end{cases} \tag{2}$$

If  $\Delta = \left(\frac{n}{2}\right)^2 + \left(\frac{m}{3}\right)^3$ , There are three possibilities

(a) If  $\Delta > 0$ , There are one real root and two imaginary roots for equation (1).

(b) If  $\Delta = 0$ , There are three real roots and two of them are equal ( $i_2 = i_3$ ) in equation (1).

(c) If  $\Delta < 0$ , There are three real roots.

Considering that  $m = 1/c[1 + (\frac{Q}{I})^2]$  and  $n = -I/c[1 + (\frac{Q}{I})^2]$  which make  $\Delta > 0$ , equation (1) has only one real root

$$i = \sqrt[3]{A} + \sqrt[3]{B} = \left[-\frac{n}{2} + \sqrt{\left(\frac{n}{2}\right)^2 + \left(\frac{m}{3}\right)^3}\right]^{\frac{1}{3}} + \left[-\frac{n}{2} - \sqrt{\left(\frac{n}{2}\right)^2 + \left(\frac{m}{3}\right)^3}\right]^{\frac{1}{3}}$$

If

$$t = c[1 + (\frac{I}{Q})^2] \quad \text{and} \quad s(I) = \left[\frac{I + \sqrt{I^2 + 4/(27t)}}{2t}\right]^{\frac{1}{3}} \quad (3)$$

The inverse function of  $i = h^{-1}(I)$  is

$$i = h^{-1}(I) = s(I) - \frac{1}{3t \cdot s(I)} \quad (4)$$