Research on optical security based on simulated noise induced encryption scheme

Shi Wang1, Zili Zou1, Tiantian Xing1, Junhua Wang2, Zeng Wang2 and Fei Jiang1

1College of Information Communication, National University of Defense Technology, Wuhan Hubei, China
2Systems Engineering Research Institute, Academy of Military Sciences, Beijing, China

*Corresponding author e-mail: wmpeterwm@163.com

Abstract. The security of a noise-induced optical encryption scheme with two dimensional keys is examined by a series of statistical analysis. We introduce the cross correlation function (CCF) and mutual information (MI) approach to estimate the time-delay information, which is considered as the most important physical key in the secure strategy. Subsequently, the other key can be cracked by using the independent component analysis (ICA) method. Meanwhile, the plaintext can be extracted with a small deviation.

1. Introduction
The increasing demands of information sharing and high-speed data interconnection put forward higher requirements for the security of reliable data transmission at the physical layer [1]. A variety of optical communication security strategies based on optical domain encryption are proposed [2-8]. These methods, including broadband optical chaos signal generation [2-5], optical code division multiplexing access (OCDMA) technology [6,7] and XOR encryption [8,9] are developed to resist information theft attack in the environment of high-speed data transmission at the physical layer. Recently, a novel optical encryption method has been proposed based on interference noise cancellation [10]. The system structure is more compact compare with the aforementioned techniques, and the key parameters are easily controllable. Meanwhile the key space can be sufficiently large because of the two-dimensional variable parameters. Different from the digital encryption methods, the analog noise has the properties of broadband and nonperiodic, which is very suitable in designing secure communication systems.

According to the descriptions in [10], the receiver could not properly digitize the encrypted noise-like signal without decryption, thus the original plaintext message will not be intercepted by the eavesdropper through subsequent processing techniques. However, to analyze an analog encryption system, direct digitization is not the only cryptanalysis method. The analog signal can still be intercepted, quantized and stored (although the quantization precision may be restricted). Offline analysis is then feasible. And such offline cryptanalysis techniques are widely used in cracking chaos based communication schemes [11-13].

This paper reports a security analysis of the analog noise-induced encryption scheme proposed in [10]. Several statistical methods are adopted to extract the key parameters as well as the plaintext of the encryption scheme. The cross-correlation function (CCF) and mutual information (MI) approach...
are use for estimating the time-delay which is the key parameter of the system. With the knowledge of time-delay, the phase of the noise signal is obtained, independent component analysis (ICA) is then adopted to estimate the amplitude of the noise. Meanwhile the plaintext signal can also be extracted. A modified configuration is also proposed to resist the aforementioned statistical attacks. A pseudo-random number sequence (PRNS) with low frequency is introduced into the system. As a result, the statistical dependence of the encrypted signal and the encryption keys is interrupted.

The remainder of this paper is organized as follows. Interception system and attack strategy are briefly introduced in section 2. In section 3 and section 4, the phase and the amplitude of the noise signal are cracked successively. In section 5, a security enhanced scheme is proposed and verified. Finally the last section concludes the paper.

2. Interception system setup

In this case, we propose an interception configuration based on the original transmission system. The recommended settings are shown in figure 1. The transmitter consists of two optical paths with different wavelengths. Interference noise signal is carried by the channel 1 (C₁), cancellation noise is carried by channel 2 (C₂). \( C₁(t) = k[S(t-T) + N(t-T)] \), \( C₂(t) = N(t) \). The receiver consists of a WDM filter, a variable optical attenuator and a tunable time-delay line. The values of the attenuate factor \( k \) and the time-delay \( T \) can be adjusted according to the setup at the transmitter side. The interception part is similar to the authorized receiver, however the initial value of the key parameters are set as \( k' = 1 \), \( T' = 0 \), as demonstrated in Fig. 1 by dashed frame. Two photodetectors are adopted to capture the signals of the two paths simultaneously. A digital sampling oscilloscope (DSO) is used to store the signals of the two paths as time series \( E₁(i) \) and \( E₂(i) \), \( i = 1, 2, 3, \ldots \). Then the time series can be post-processed in a computer.

![Figure 1. Interception configuration built on the original transmission system in [10].](image)

VOA: variable optical attenuator, MZ: Mach-Zehnder modulator, TDL: tunable delay line, OC: optical coupler, SSMF: standard single mode fiber, DCF: dispersion compensate fiber, EDFA: erbium-doped fiber amplifier, WDM: wavelength division multiplexer, PD: photodetector, EC: electrical combiner.

The simulation of the data transmission process is conducted by the VPI transmission software and the cryptanalysis is performed by MATLAB. A Gaussian noise with limited bandwidth is used as the mask signal \( N(t) \). The data rate of the signal is 10Gbps. The sampling rate of the DSO is set as \( Fₛ = 80 \) Gsample/s. The time-delay \( T = 10 \) ns, and the attenuate factor \( k = 0.8 \).

3. Time-delay extraction

As stated in [10], time-delay is the major key in the system, since the bit error rate (BER) is extremely sensitive to the mismatch of time-delay. The brute force attack against the time-delay is hard to conduct due to the large variation range of \( T \). However, statistical analysis, including CCF and MI, can be used to directly extract the value of \( T \) without exhausting the whole key space. Similar techniques are widely used in breaking the inner time-delay of chaotic systems [11, 12].

For two time series \( v₁(i) \) and \( v₂(i) \), the CCF \( C(s) \) is defined as
In which $\langle \cdot \rangle$ is the time average, $F_s$ is the sampling rate of the time series. The MI $M(s)$ is defined as

$$M(s) = \sum_{v_1(i), v_2(i-sF_s)} P(v_1(i), v_2(i-sF_s)) \ln \frac{P(v_1(i))P(v_2(i-sF_s))}{P(v_1(i), v_2(i-sF_s))},$$

(2)

The probability distribution function of $v_1(i)$ is $P(v_1(i))$, $P(v_1(i), v_2(i-sF_s))$ is the joint probability distribution function.

Figure 2. Cross correlation function $C(s)$ (a) and mutual information $M(s)$ (b) of the captured transmitted signal $E_1(i)$ and $E_2(i)$.

Figure 3 displays that both CCF and MI have obvious peaks at $s=T$ for $E_1(i)$ and $E_2(i)$ when the signal to noise ratio $R=0$dB (here the noise means the mask signal $N(t)$, not the channel noise). Thus indicates the effectiveness of the statistical attack strategy against the time-delay.

Figure 3 shows that both CCF and MI have obvious peaks at $s=T$.

Figure 3(a) shows the peak value at $s=T$ in background $Q_{CCF}$. Green lines corresponding to the background mean and the standard deviation. (b) The peak size at $s=T$ in background $Q_{MI}$. (c) BER of direct-decoding (without decryption).

Figure 3(a) shows the peak value of background $Q_{CCF}$ in $C(s)$ when the relevant time-delay $T=10$ns, and Fig. 3(b) shows the peak size at $T=10$ns in background $Q_{MI}$ in $M(s)$.

The backgrounds $Q_{CCF}$ and $Q_{MI}$ are defined as

$$Q_{CCF} = [P_{CCF}(R), \bar{P}_{CCF}(R)]$$

$$P_{CCF}(R) = mean\{C_R(s)\} - SD\{C_R(s)\}$$

$$\bar{P}_{CCF}(R) = mean\{C_R(s)\} + SD\{C_R(s)\},$$

(3)
\[ Q_{MI} = [P_{MI}(R), \overline{P}_{MI}(R)], \]
\[ P_{MI}(R) = \frac{\text{mean}\{M_R(s)\} - \text{SD}\{M_R(s)\}}{\text{mean}\{M_R(s)\} - \text{SD}\{M_R(s)\}}, \]
\[ \overline{P}_{MI}(R) = \frac{\text{mean}\{M_R(s)\} + \text{SD}\{M_R(s)\}}{\text{mean}\{M_R(s)\} - \text{SD}\{M_R(s)\}}, \]

where SD is the standard deviation. The backgrounds are calculated for each \( R \). The peak value of relevant time-delay \( T \) in the CCF and MI is defined as
\[ P_{CCF}(R) = C_R(T), \quad P_{MI}(R) = \frac{M_R(T)}{\text{mean}\{M_R(s)\} - \text{SD}\{M_R(s)\}}. \]

The corresponding bit-error-rates (BERs) of direct-decoding (without decryption) under different \( R \) are shown in Fig. 3 (c). If \( R \) is small, the encryption effect is satisfactory. However, the peak in CCF is clearly observed. When \( R \) increases, the peak size in CCF decreases, the encryption effect degrades significantly. In MI, the peak is obvious even if we increase \( R \). These results mean that the time-delay information can be extracted under all circumstances, and the system is not safe without certain modification.

4. Attenuate factor estimation and plaintext extraction
ICA has been utilized in many areas due to its potential applications, including biomedical signal processing, speech enhancing, optical communication, etc. [14, 15] The principle is formulated as follows: observable signals \( x(i) = [x_1(i), x_2(i), \ldots, x_n(i)]^T \) are modeled as \( x(i) = Ay(i) \), where \( y(i) = [y_1(i), y_2(i), \ldots, y_n(i)]^T \) is a vector of source signals, \( A \) is a \( n \times n \) non-singular unknown matrix, namely the mixing matrix. Each row of \( A \) corresponds to a mixing vector. The mixing vector consists of a series factors that determine the extent to which each source signal affects a given observation signal. The objective is to estimate \( A \) and \( y(i) \) assuming that \( y_1, y_2, \ldots, y_n \) are statistically independent.

In this system, the observed signals are written as \( x(i) = [x_1(i), x_2(i)]^T = [E_1(i), E_2(i-TFs)]^T \), the mixing matrix can be written as
\[ A = \begin{bmatrix} k & k \\ 0 & 1 \end{bmatrix}. \]

The source signals which need to be estimated are assumed to be \( y(i) = [y_1(i), y_2(i)] \). With the knowledge of \( T \), we can estimate the attenuate factor \( k \) directly by using ICA.

The ICA tries to search the linear transformation \( W \) that makes the separated components of the observed signals as statistically independent as possible. Such process can be written as \( u(i) = Wx(i) \). In this research, we use the FastICA [16] algorithm to find the de-mixing matrix \( W \), which is an estimate of \( A^{-1} \).

Figure 4 shows the effectiveness of the separating process using ICA. The captured encrypted signal \( E_1(i) \) is shown in Fig. 4(a), and the mask signal with compensated time-delay \( E_2(i-TFs) \) is shown in Fig. 4(b). The message signal can be extracted successfully, as shown in Fig. 4(c), and the separated mask signal is shown in Fig. 4(d). Meanwhile the de-mixing matrix \( W \) is estimated. The attenuate factor \( k = 0.8 \) is then obtained with a small error due to the additive channel noise, the estimated value is \( k' = 0.8064 \).
Figure 4. The separating results of ICA: (a) the captured encrypted signal $E_1(i)$, (b) the mask signal with compensated time-delay $E_2(i-TFs)$, (c) the extracted message signal $y_1(i)$, (d) the separated mask signal $y_2(i)$.

5. Conclusion
In summary, we have studied the cryptanalysis strategies against an analog noise-induced optical encryption scheme with two dimensional physical keys. CCF and MI can be used to estimate time-delay information. With such information, the attenuate factor and the plaintext can be extracted simultaneously by ICA. These results mean that the system can be cracked with the transmitted signals only. How to guarantee the security level and keep the system structure as simple as possible is the aim of our future works.

References
[1] M. P. Fok et al., “Optical layer security in fiber-optic network,” IEEE Trans. Inf. Forensics Security 6(3), 725–736 (2011).
[2] A. Argyris et al., “Chaos-based communications at high bit rates using commercial fibre-optic links,” Nature 438, 343-346 (2005).
[3] M. Sciamanna et al., “Physics and applications of laser diode chaos,” Nat. Photonics 9, 151-162 (2015).
[4] A. Wang et al., “Optical heterodyne generation of high-dimensional and broadband white chaos,” IEEE J. Sel. Top. Quant. 21, 1800710 (2015).
[5] C. Xue et al., “Key distribution based on synchronization in bandwidth-enhanced random bit generators with dynamic post-processing,” Opt. Express 23, 14510-14519 (2015).
[6] Z. Gao et al., “Rapid programmable/code-length-variable, time-domain bit-by-bit code shifting for high-speed secure optical communication,” Opt. Lett. 36, 1623-1625 (2015).
[7] H. Zhu et al., “Optical steganography of code-shift keying OCDMA signal based on incoherent light source,” IEEE Photonics J. 7, 6801607 (2015).
[8] X. Zhang et al., “High-speed all-optical encryption and decryption based on two-photon absorption in semiconductor optical amplifiers,” IEEE J. Optical communications and networking 7, 276-285 (2015).
[9] P. Cao et al., “Physical layer encryption in OFDM-PON employing time-variable keys from ONUs,” IEEE Photonics J. 6, 7901006 (2014).
[10] B. Wu et al., “Analog noise protected optical encryption with two-dimensional key space,” Opt. Express 22, 14568-14574 (2014).
[11] V. S. Udaltsov et al., “Cracking chaos-based encryption systems ruled by nonlinear time delay differential equations,” Phys. Lett. A 308, 54-60 (2003).
[12] M. D. Prokhorov et al., “Reconstruction of time-delayed feedback systems from time series,” Physica D 203, 209-223 (2005).