Experimental Demonstration of An Efficient Correlation Attack Method in 300km QAM/QNSC Transmission

Mingrui Zhang, Yajie Li, Kongni Zhu, Shuang Wei, Yuang Li, Yongli Zhao, and Jie Zhang

State Key Laboratory of Information Photonics and Optical Communications

Beijing University of Posts and Telecommunications, Beijing, 100876, China

**jie.zhang@bupt.edu.cn*

Abstract: We propose an efficient correlation attack based on low-order demodulation to recover the seed keys in QNSC. Experiment results prove its high success possibility and low computational complexity in 300km QAM/QNSC transmission.

1. Introduction

Physical-layer security in optical networks is crucial as it faces threats that aim to disrupt services or gain unauthorized access to data [1]. Quantum noise stream cipher (QNSC) is proposed to protect these messages from eavesdropping in optical communication system [2]. It allows high transmission rates and distances since the encoding is performed in digital signal processing (DSP). The security is produced by the noise in the transmission system including quantum noise and amplifier spontaneous emission (ASE) noise. Meanwhile, QNSC requires the transmitter and the receiver to share a stream cipher that is generated from a linear feedback shift register (LFSR).

However, QNSC might be attacked due to the mathematical properties of an LFSR-based stream cipher. Especially, the correlation attack (CA) is a powerful specific attack against random stream ciphers. It is a kind of known plaintext attacks that targets the seed keys (the LFSR's initial state that is used to generate the stream cipher). The security of QNSC under CA has been analyzed in [3-5]. The results in our previous work find that the security of the whole system depends on the cycle to refresh seed key and the correlation between incepted running key, original running key and seed key [3]. However, due to the distribution characteristics of constellation points in quadrature amplitude modulation (QAM) based QNSC, Eve is able to improve the correlation between incepted running key and original running key by introducing low-order demodulation. This presents new advantage for attacking the QNSC system with correlation attacks. Therefore, it is necessary to conduct an attack analysis under CA based on low-order demodulation in QNSC system.

In this paper, we propose a high success probability CA targeting QNSC and give an experiment of attack analysis on 300km QAM/QNSC transmission system. Low-order demodulation is established in our proposed CA. The experiment demonstrates that the proposed CA performs better attack success possibility and lower computational complexity than traditional CA.

2. Principle of QAM/QNSC attack analysis

2.1. Generation principle of QAM/QNSC

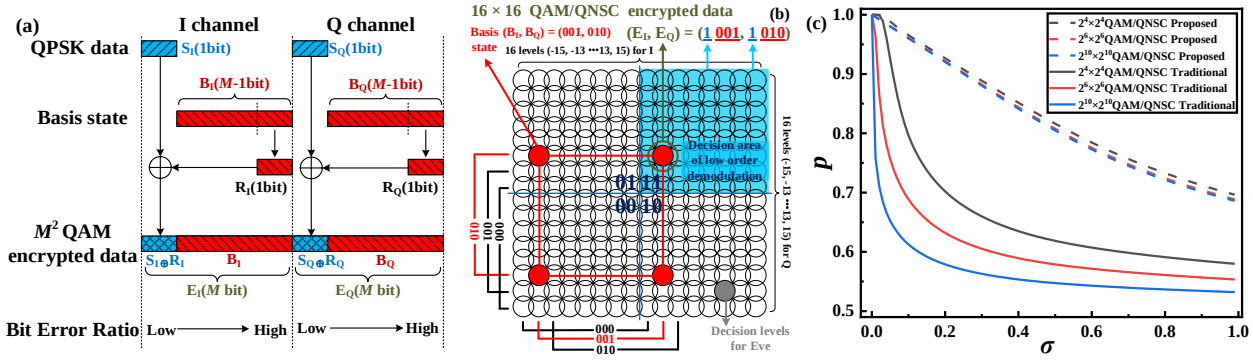

Fig. 1 (a) Generation principle of QNSC, (b) definition of low-order demodulation, and (c) p for different noise standard deviation σ.

Generator based on LFSR and non-linear function is used to generate the keys. The nonlinear function breaks the linear relationship between the output of LFSR and the running key, which brings challenge to CA. The q is defined

as the correlation between the output of registers and the output of nonlinear function [3]. The final generated running keys are used as the basis states for encryption and decryption.

The number of constellation points of QAM/QNSC signal is $2^M \times 2^M$. Therefore, the M+M encrypted symbols hide the 2-bit (I+Q) original data and the decision level of QNSC signal for Eve is covered by quantum noise or other noise such as amplifier spontaneous emission (ASE) noise without shared basis. As an example, the constellation of 16×16 QAM/QNSC is shown in Fig. 1(b), where QPSK (1 bit for I and Q, respectively) data is encrypted by using 2×2^3 basis states (3 bits for I and Q, respectively). We use 2-bit information data $S_I = 0$, $S_Q = 1$ and 6-bit basis $B_I = (b_{I3}b_{I2}b_{I1}) = 001$, $B_Q = (b_{Q3}b_{Q2}b_{Q1}) = 010$ to generate 8-bit encrypted data $E_I = (S_I \oplus b_{I2}b_{I1}, B_I) = 1001$, $E_Q = (S_Q \oplus b_{Q2}b_{Q1}, B_Q) = 1010$. Respectively, lower bits of B_I and B_Q are regarded as R_I and R_Q, which has the same length as S_I and S_Q.

2.2. CA based on low-order demodulation

Our previous work calculated the bit error ratio for different bit positions in a symbol of QAM/QNSC. The results show that the effect of noise on bit position increases as bit position decreases. Low-order demodulation is proposed to obtain the bit of lowest bit error ratio within the symbol. Hence, the obtained bit of lowest bit error ratio has higher correlation with the original running key, compared with traditional high order demodulation. The noise masking Γ is defined as $\Gamma = 2\sigma / \Delta$, σ is the standard deviation of noise, Δ is the minimum hamming distance in constellation diagram. It is commonly considered as an evaluation index of security in QNSC system [6]. Fig. 1(c) shows the p for different σ by traditional high order demodulation and proposed low-order demodulation. The p is defined as the probability that each bit of intercepted sequence equals with the original running key. The results show that the introduction of low-order demodulation strengthen the correlation between intercepted sequence and the original running key. Yet p can still decrease to 0.5 with the help of deliberate signal randomization and deliberate error randomization [3].

In CA on QNSC, the objective of Eve is to obtain the initial state of LFSR (the seed keys). The steps of CA are as follows. 1) We assume that Eve has already known the structure of key generator and the DSP rules. Besides, publicly available parameters M and σ are used by Eve to calculate p [3]. 2) Eve performs the same DSP with Bob and intercepts the sequences with a specific length L. It is worth noting that L decreases in same number of intercepted symbols while low-order demodulation is applied. The intercepted key is interfered by the quantum noise, which shows correlation with the seed keys. 3) Using q, p, and the intercepted sequences, a CA is launched by Eve to find the seed keys. 4) If Eve gets both the seed keys and the structure of key generator, the key stream can be generated to decode the message exactly like Bob.

To achieve CA, Eve employs the hypothesis testing theory. Suppose the seed keys' length of attacked register is g, we need to separate all 2^g possible seed keys into two hypotheses (H1: seed keys; H2: non-seed keys). The miss probability p_m and the false probability p_f are preset to define the abilities of Eve. The p_m represents the probability that the true seed keys are misplaced in H2. Besides, the p_f represents the probability that each false seed key is misplaced in H1. Therefore, we can see that higher p_m can bring less possible elements in H1 and p_f can bring more possible elements in H1, theoretically. The number of elements in H1 is N. Eventually, the attack success possibility (ASP) will be 100% if there is only one seed key separated into H1. Besides, ASP will be 0% if all the seed keys (i.e., 2^g) are separated into H1. Therefore, the ASP is defined as $ASP = 1 - (\log_2 N) / g$.

3. Experimental setup and results analysis

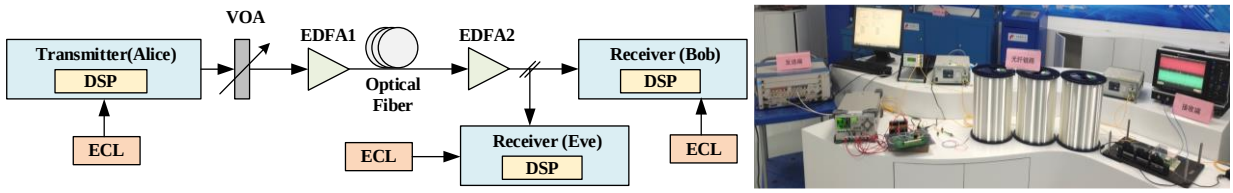

Fig.2 The system of QAM/QNSC

Fig. 2 shows the experiment's flow-process of the $2^M \times 2^M$ QAM/QNSC. An external cavity laser (ECL) sends a beam at 1550 nm with 11 dBm power into an I/Q modulator. At transmitter, the I and Q data are converted by an arbitrary waveform generator (AWG) to an electrical signal at the sampling rate of 10-GSa/s after DSP. Amplified by the I/Q modulator driver (MD), the signal is loaded onto the optical carrier. Then, the optical signal goes across the variable optical attenuator and is amplified by an erbium-doped fiber amplifier (EDFA) into 0 dBm and transmitted through a 300 km SSMF. At the receiver, the received optical signal is amplified into 0dBm, and then detected by a coherent optical receiver which is combined with an ECL. The detected I/Q signals are captured by a 40-GSa/s real-time

oscilloscope. Eve can temporarily intercept the signal from Bob to launch the CA.

ASP of CA for Eve is shown in Fig. 3(a). Different colors represent different values of *ASP*. We can see the *ASP* is approaching 0 as the growth of σ while L is fixed. Hence a higher σ weakens the correlation between intercepted sequences and seed keys, which makes it more difficult to extract the seed keys through CA. Meanwhile, the increase of L leads to the growth of *ASP*. In addition, with fixed L and σ, the proposed CA based on low-order demodulation has a higher *ASP* compared with traditional CA. For instance, when L is 240, q=0.75, p_f=0, p_m=0.05, and σ=0.2, the *ASP* is 0.392 and 1 for traditional and proposed CA, respectively.

Fig. 3(b) indicates that a higher order of QAM and a higher σ can result in a lower *ASP*. A higher modulation order of QAM significantly decrease p in traditional CA and *ASP* approaches 0 while M is 6, 10, and 14 for σ is 0.75, 0.5, and 0.25, respectively. Meanwhile, due to the higher p, *ASP* of proposed CA is higher than *ASP* of traditional CA while M and σ is fixed. Besides, *ASP* of proposed CA maintains around 0.172, 0.364, and 0.728 while M$\geqslant$6 for σ is 0.75, 0.5, and 0.25. The results indicate that CA based on low-order demodulation performs better *ASP* than traditional CA especially in high M situation. Furthermore, increasing symbol length M while $M\geqslant 6$ is no longer an available approach to enhance the security level against our proposed CA. However, maintaining high-level σ by increasing symbol length M while $M\leqslant 6$ or decreasing optical power is still an effective way to reduce the *ASP* of our proposed CA.

Fig. 3(c) shows the time cost (*TC*) of CA using Intel® Core™ i7-8750H CPU. In traditional CA, the theoretical computational complexity of CA is $C = o(2^g \cdot L \cdot M)$. While L=240 and g=12, the *TC* is 4.04, 12.12, and 20.2 for M is 2, 6, 10. Meanwhile, the computational complexity is $C = o(2^g \cdot L)$ in proposed CA. While L=240 and g=12, the *TC* is 2.02, 2.12, and 2.08 for M is 2, 6, 10. Updating the seed keys periodically is still an approach to immune CA. Yet, the result shows that CA based on low-order demodulation has lower computational complexity than traditional CA. Hence, the seed key needs to be refreshed more frequently under our proposed CA.

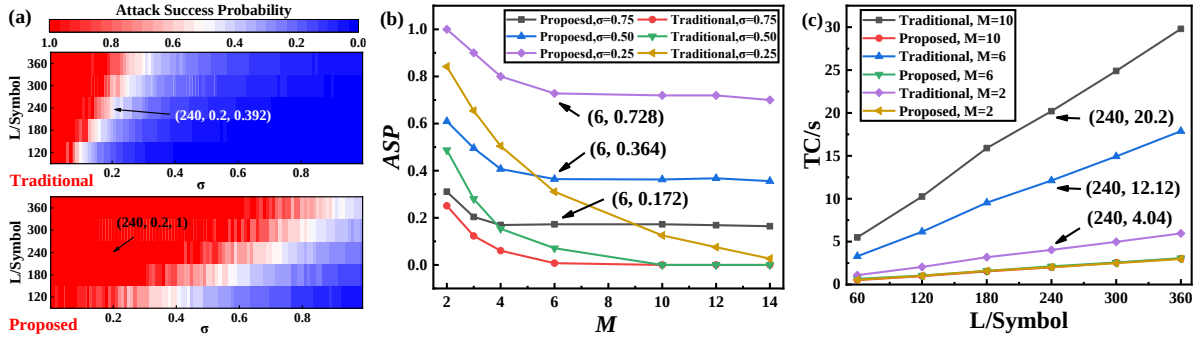

Fig. 3 (a) ASP of two CA, (b) *ASP* for M and (c) *TC* of two CA.

4. Conclusions

In this paper, we conduct an experiment of attack analysis on LFSR-based QAM/QNSC transmission system under CA based on low-order demodulation. The experiment demonstrates that our proposed CA performs better *ASP* and lower computational complexity than traditional CA.

5. Acknowledgment

This work is supported by NSFC Projects (Grant No.: 61831003, 62021005), the Fundamental Research Funds for the Central Universities, Beijing Natural Science Foundation (4232011) and BUPT Excellent Ph.D. Students Foundation (CX2023228).

6. References

[1] N. Skorin-Kapov, et al., "Physical-layer security in evolving optical networks," IEEE Commun. Mag. **54**, 110-117, (2016).

[2] O. Hirota, et al., "Quantum stream cipher by the Yuen 2000 protocol: Design and experiment by an intensity-modulation scheme." Phys. Rev. A **72**, 022335, (2005).

[3] M. Zhang, et al., "Security analysis of a QAM modulated quantum noise stream cipher under a correlation attack," Opt. Express **30**, 40645–40656, (2022).

[4] T. Iwakoshi, et al., "Analysis of Y00 protocol under quantum generalization of a fast correlation attack: Toward information-theoretic security." IEEE Access **8**, 23417-23426, (2020).

[5] T. Iwakoshi, et al., "Y00 quantum noise randomised cipher; theoretical and experimental background." IET Quant. Comm., 1-10, (2023).

[6] M. Nakazawa, et al., "QAM quantum stream cipher using digital coherent optical transmission," Opt. Express **22**, 4098–4107, (2014).