ISSN 2186-6570

Experimental Demonstration of a Driver Circuit using a 20-bit Digital-to-Analog Converter for Key Exchange in a Y-00 Quantum Noise Stream Cipher

Fumio Futami, and Ken Tanizawa

Quantum ICT Research Institute, Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan

Tamagawa University Quantum ICT Research Institute Bulletin, Vol.10, No.1, 13-15, 2020

©Tamagawa University Quantum ICT Research Institute 2020
All rights reserved. No part of this publication may be reproduced in any form or by any means electrically, mechanically, by photocopying or otherwise, without prior permission of the copy right owner.

Experimental Demonstration of a Driver Circuit using a 20-bit Digital-to-Analog Converter for Key Exchange in a Y-00 Quantum Noise Stream Cipher

Fumio Futami, and Ken Tanizawa
Quantum ICT Research Institute, Tamagawa University
6-1-1 Tamagawa Gakuen, Machida, Tokyo, 194-8610, Japan
E-mail: futami@lab.tamagawa.ac.jp

***Abstract*—Y-00 quantum stream cipher (Y-00 cipher) is a direct data encryption system, in which a key for encryption and decryption is shared in advance with legitimate users. The Y-00 cipher can also be used for key exchange in which an existing key is replaced with a new one. However, the key exchange rate in these systems is generally relatively low. High-resolution digital-to-noise converters (DACs) with low sampling speeds are readily available. Such DACs generate signals with levels to realize a large amount of noise masking, thus providing high-level secrecy for a key exchange when the Y-00 cipher is used. In this work, we demonstrate the first driver circuit that uses a 20-bit DAC to successfully generate electrical signals at 1,048,676 amplitude levels of electrical signals at a data rate of 100 kb/s, for performing key exchange with the Y-00 cipher system.**

***Index Terms* — Y-00 quantum stream cipher, key exchange physical cipher, 20-bit DAC, noise masking, ciphertext, secure optical communication.**

I. Introduction

High security to protect eavesdropping in an optical transport layer is essential. In this regard, the Y-00 quantum stream cipher (Y-00 cipher) [1-3] is a promising candidate. This cipher is a symmetric key cryptosystem in which the key is shared between legitimate users before they start their communication using the Y-00 cipher. The Y-00 cipher features quantum noise, which covers the cipher signals of multi-level modulation to prevent an eavesdropper from correctly discriminating the cipher signal levels. The security measure of the Y-00 cipher is a noise masking number defined as the ratio of the noise to the minimum distance between the signals [4]. This distance can be reduced by increasing the number of signal levels. These multi-level signals are digitally generated using a digital-to-analog converter (DAC). The number of signal levels corresponds to the number of bits (NOB) of the DAC. A tradeoff exists between the sampling speed of the DAC and the number of bits, that is, its resolution. In other words, a high-speed DAC has a low resolution, whereas a high-resolution DAC has a low speed. To date, the Y-00 cipher has mainly been used for data encryption in optical communication systems [5-12]. These systems employ high-speed DACs with limited resolution to generate high-data-rate cipher signals. In addition to data encryption, the Y-00 cipher provides a key exchange function in which a key shared in advance is replaced with another key. Compared with the data encryption rate for high-capacity transmission, the key exchange rate is generally much lower because key exchange does not occur frequently. Consequently, a low-speed but high-resolution DAC is applied to generate signals suitable for key exchange in the Y-00 cipher system.

In this work, we focus on the implementation of a driver circuit for generating electrical signals with a larger number of amplitude levels than those of signals for high-capacity data communication. First, a driver circuit that employs an existing DAC with a resolution of 20 bits is implemented. This circuit is then used to experimentally demonstrate 1,048,676 amplitude levels of electrical signals at a rate of 100 kb/s for driving an optical modulator to generate a Y-00 cipher for key exchange.

II. Key Exchange Scheme for Y-00 Cipher System

A key to encrypt and decrypt the Y-00 cipher is shared between legitimate users before they start their communication using the cipher. Upon receipt of a request for key exchange during cipher communication, the key is updated by the Y-00 cipher, as shown in Fig. 1. While data are being transmitted securely using key #1 of the Y-00 cipher, another key, key #2, is encrypted by key #1 in the Y-00 transmitter (TX). Then, the encrypted key #2 is transmitted to a legitimate user and decrypted by key #1 to recover key #2 in the Y-00 receiver (RX). After key #2 is shared between the legitimate users, key #1 is replaced with key #2 at the same time after synchronizing with the head of key #2. Figure 1 shows an example in which key #2 is transmitted in a different transmission line. This key can also be shared using the same transmission line and a wavelength division multiplexing scheme in which the Y-00 signals of the data are transmitted at a wavelength that differs from that at which key #2 is exchanged.

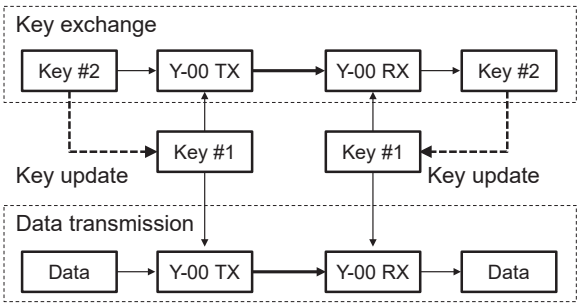

Fig. 1. Example of a key exchange system for the Y-00 cipher system.

III. Influence of Basis Number on Noise Masking

The noise masking number of the intensity modulation of the Y-00 cipher caused by quantum noise or shot noise is related to parameters such as the number of bases (M), signal frequency (ν_0), signal bandwidth (R), and the maximum and minimum signal power. The number M corresponds to the NOB of a DAC. The maximum power level P_{2M} has the highest signal power, and the minimum power level P_1 has the lowest. To effectively generate a higher noise masking number for the lower power level signals in the IM Y-00 cipher, a DC offset is intentionally added to the minimum power level signal. Details of IM Y-00 are provided elsewhere [10]. Using the parameters and the ratio of the maximum power to the minimum power, $r = P_{2M} / P_1$, the noise masking number of an IM Y-00 signal with a basis comprising pairs of binary signals "0" and "1" is given by

$$\Gamma_{IM} = \frac{(2M-1)(r+1)e}{r-1}\sqrt{\frac{2R}{P_0 h\nu_0}} \quad (1)$$

where e is the elementary charge, P_0 is the average optical power, and h is Planck's constant [10]. Considering that the number of bases is high, the probability of correct signal detection in a single time slot is approximately expressed using only Γ_{IM} as

$$Prob_{Single} \approx erf\left[\frac{1}{\Gamma_{IM}\sqrt{2}}\right] \quad (2)$$

where erf[·] is the error function [10].

A larger M leads to a larger Γ_{IM}, and a larger Γ_{IM} yields a lower $Prob_{single}$. The NOB generally decreases as the sampling speed of the DAC increases. An existing DAC with a sampling speed in excess of 10 GSample/s for high-capacity Y-00 cipher data transmission contains a maximum of 12 bits (e.g., the Keysight M8190A 12 GSa/s arbitrary waveform generator). To overcome this limitation, a scheme that employs two DACs with configurations that are coarsely and finely tuned, respectively, was proposed [7] and a Y-00 cipher signal with 17-bit signal levels at a baud rate of 12 Gbaud/s was achieved [8]. Compared with the data transmission rate of the Y-00 cipher, the required key exchange rate is generally lower. Therefore, the generation of a multi-level signal suitable for key exchange requires higher resolution (rather than high-speed operation) to increase M. The use of a single DAC simplifies the configuration of the Y-00 transmitter.

Here, we briefly discuss the impact of the signal bandwidth (R) and optical signal power (P_0) on the quantum noise masking number. A decrease in the signal bandwidth causes the noise masking number to decrease in proportion to the square root of the signal bandwidth, as shown in Eq.(1). The signal quality generally depends on the signal-to-noise ratio in the signal bandwidth. When the signal bandwidth is decreased, the signal power also decreases and P_0/R remains constant to achieve the same signal quality, assuming that the thermal noise in the receiver circuit is ignored. Consequently, the quantum noise masking number increases in proportion to the number of bases, M, from Eq.(1), and the probability of correct signal detection in Eq.(2) decreases.

IV. Experimental Demonstration

Here, we demonstrate the implementation of a Y-00 cipher driver circuit using an existing DAC with 20-bit resolution. A schematic of the driver circuit is shown in Fig. 2. A 256-bit key is employed as a seed key, and binary data in the form of a pseudorandom bit sequence (PRBS) is used as the second key for exchange.

In pseudorandom number generation (PRNG), a linear feedback shift register (LFSR) expands the 256-bit key length to generate a pseudorandom number of a running key with a key length of 2^{256}–1. Binary data and the basis selection signal of a block of the 19-bit running key are combined to generate an electrical signal for driving an E/O modulator.

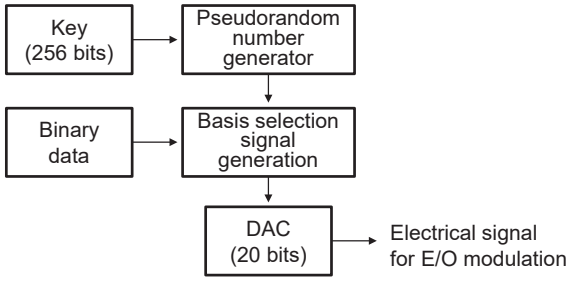

Fig. 2. Schematic of a driver circuit using a 20-bit DAC in a Y-00 cipher transmitter.

First, the NOB of the DAC is set to 3 bits and electrical signals with eight amplitude levels are generated at 100 kbit/s. The waveform of the signals with a duration of 50 ms is shown in Fig. 3, in which the eight levels are clearly observed. Next, the NOB is increased to 5 bits and the resulting waveform of the electrical signal is shown in Fig. 4, in which the 32 amplitude levels of the signals are still observable. Finally, the NOB of the DAC is set to its maximum resolution of 20 bits, resulting in an electrical signal waveform with 1,048,576 amplitude levels (Fig. 5). The peak-to-peak amplitude of the signal was 9.5 V, and the difference in the amplitude of the neighboring signals was calculated to be 9.0 μV. This difference is prohibitively small in that it prevents the different levels from being distinguished. Γ_{IM} is calculated to be ~ 4,400 using R = 100 kbit/s, r = 2, M = 524,288(19 bits), P_0 = 0.02 μW, in the wavelength range of 1.55 μm.

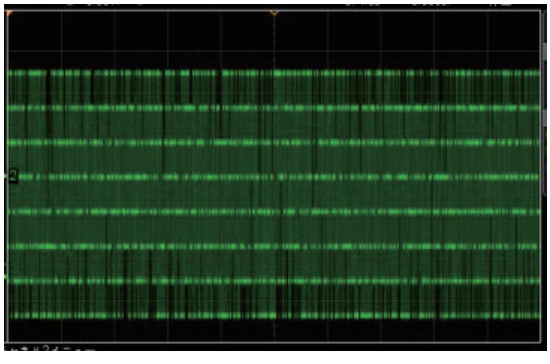

Fig. 3. Electrical signal waveform with eight amplitude levels when the NOB of the DAC is set to 3. (H: 5 ms/div, V: 3 V/div)

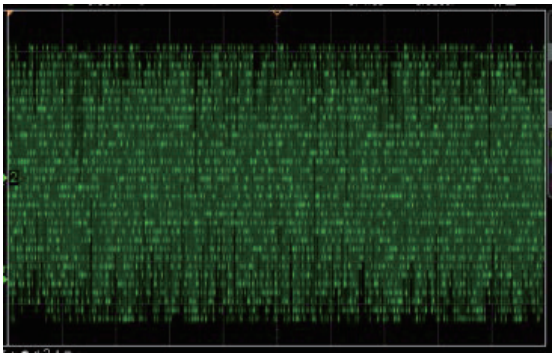

Fig. 4. Electrical signal waveform with 32 amplitude levels when the NOB of the DAC is set to 5. (H: 5 ms/div, V: 3 V/div)

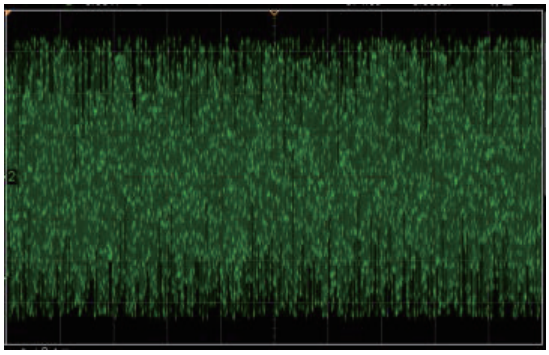

Fig. 5. Electrical signal waveform with 1,048,576 amplitude levels when the NOB of the DAC is set to 20. (H: 5 ms/div, V: 3 V/div)

V. Summary

We implemented a driver circuit using a 20-bit DAC to generate Y-00 cipher signals. This circuit was used to experimentally demonstrate a Y-00 cipher system with electrical signals with 1,048,676 amplitude levels and a key exchange rate of 100 kb/s. This work can be extended to demonstrate a Y-00 cipher system with a key exchange function using the developed driver circuit. A secure communication system based on this driver circuit would be applicable to both optical fiber communication and free space optical communication.

References

[1] G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, "Secure communication using mesoscopic coherent states," *Phys. Rev. Lett*., vol.22, 227901, 2003.

[2] O. Hirota, M. Sohma, M. Fuse, and K. Kato, "Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme," *Phys. Rev. A*, 72, 022335, 2005.

[3] K. Kato and O. Hirota, "Quantum quadrature amplitude modulation system and its applicability to coherent state quantum cryptography," SPIE conference on quantum communication and imaging III. SPIE Proc. vol-5893, 2005.

[4] O. Hirota, "Practical security analysis of a quantum stream cipher by the Yuen 2000 protocol," *Phys. Rev. A*, 76, 032307, 2007.

[5] F. Futami, and O. Hirota, "100 Gbit/s (10 × 10 Gbit/s) Y-00 cipher transmission over 120 km for secure optical fiber communication between data centers," in *Proc. OECC/ACOFT2014*, MO1A2, 2014.

[6] F. Futami, K. Guan, J. Gripp, K. Kato, K. Tanizawa, C. Sethumadhavan, and P. J. Winzer, "Y-00 quantum stream cipher overlay in a coherent 256-Gbit/s polarization multiplexed 16-QAM WDM system," *Optics Express*, vol. 25, no. 26, pp. 33338-33349, 2017.

[7] K. Tanizawa and F. Futami, "Digital coherent PSK Y-00 quantum stream cipher with 2^{17} randomized phase levels," *Opt. Express*, vol. 27, pp. 1071-1079, 2019.

[8] K. Tanizawa and F. Futami, "Single channel 48-Gbit/s DP-PSK Y-00 quantum stream cipher transmission over 400- and 800-km SSMF," *Opt. Express*, vol. 27, pp. 25357-25363, 2019.

[9] F. Futami, K. Tanizawa, K. Kato, and O. Hirota, "1,000-km transmission of 1.5-Gb/s Y-00 quantum stream cipher using 4096-level intensity modulation signals," in *Proc., Conference on Lasers and Electro‐Optics (CLEO 2019)*, SW3O.4, 2019.

[10] F. Futami, K. Tanizawa and K. Kato, "Y-00 Quantum-Noise Randomized Stream Cipher Using Intensity Modulation Signals for Physical Layer Security of Optical Communications," *J. Lightwave Technol.*, vol. 38, no. 10, pp. 2774-2781, 2020.

[11] F. Futami, K. Tanizawa, A. Bekkali, and H. Fujita, "Secure Free-Space Optical Transmission of Y-00 Quantum Stream Cipher with 4096-Level Intensity Modulated Signals," in *Proc. 14th Pacific Rim Conference on Lasers and Electro-Optics (CLEO-PR 2020)*, 2020.

[12] M. Nakazawa, M. Yoshida, T. Hirooka, and K. Kasai, "QAM quantum stream cipher using digital coherent optical transmission," *Opt. Express*, vol.22, no.4, pp.4098-4107, 2014.