Cryptographic Key Generation Using Conventional Single-Mode Fiber and an Optical Time Domain Reflectometer

Yuto Sagae, Atsushi Nakamura, Takayoshi Mori, Yusuke Koshikiya, and Kazuhide Nakajima
Access Network Service Systems Laboratories, NTT Corporation
yuto.sagae@ntt.com

Abstract: Generation of cryptographic key is demonstrated by conventional equipment for an optical network. Random bit sequences obtained from an optical time domain reflectometry of a single-mode fiber satisfies a quality of randomness as cryptographic keys. © 2024 The Author(s)

1. Introduction

The physical characteristics of light have been enthusiastically investigated for utilization in secure communications [1–3]. Random behaviors of light, e.g., phase fluctuations in lasers, amplified spontaneous emissions, and the vacuum state, have been used for generating random bit sequences [2]. Physically generated random bits are more often applied to cryptography as random keys than a deterministic pseudo-random bit sequence (PRBS), thanks to their unpredictability. Random keys have been utilized in an authentication technique called fast identity online (FIDO), which enables password-less authentication [4]. FIDO utilizes a pair of cryptographic keys, a private key and a public key, i.e., public-key cryptography, and these keys are retained in a user device and a FIDO server, respectively. One can expect secure and convenient authentication in FIDO. However, inconvenience will likely be perceived in using multiple pieces of device because each piece of device is necessary to be registered with FIDO independently to prepare the pair of keys uniquely for the device. This issue is an obstacle to utilizing FIDO, so demand has emerged for techniques to share the private key for use with multiple devices [5].

In this paper, we show a FIDO scheme in which a network operator generates and retains private keys with the user information. This model realizes the private key sharing among the user devices, and so user inconvenience will be relaxed. We demonstrated that a random characteristic of an optical fiber enables generation of private keys. Bit sequences were obtained from a random behavior of the backscattered light of a single-mode fiber (SMF) using an optical time domain reflectometer (OTDR). Unpredictability and non-repeatability of the bit sequences, which are required in cryptographic keys [2], were evaluated. Tests of NIST SP 800-22 Rev.1a [6] were also conducted.

2. Authentication procedure and key generation setup by OTDR

Figure 1(a) shows the concept of authentication based on standardized FIDO. When a user registers with a FIDO service, the user device generates a new key pair: 256-bit public and private keys. The private key is produced from random bit sequences, and the public key is calculated by hashing the private key. The private key is stored in the user device, and the corresponding public key is located in a FIDO server with information identifying the device. The server sends a challenge asking the user to encrypt the signature. The user responds with the signature encrypted by the private key. Authentication is complete when the encrypted signature is successfully decrypted by the public key, and then the user device can access web services. When multiple pieces of device are used, the key pairs need to be prepared for each device, which deteriorates usability of FIDO. Figure 1(b) describes the concept of FIDO enabling the private key sharing. The private key is generated by existing equipment for an optical network, for which we considered an OTDR and a transmission line, and stored with the user information in the private key storage located in a facility of the network operator. The network operator and the FIDO sever authenticate the user by FIDO. This architecture prepares the private key related not to the user device but to the user itself. Thus, multiple pieces of

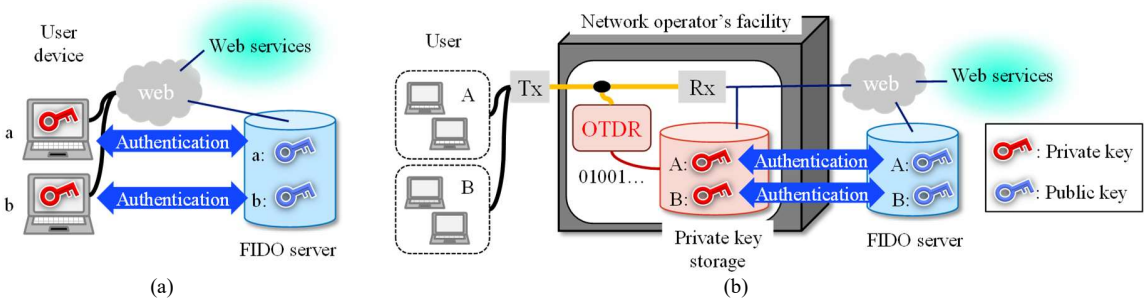

Fig. 1. Authentication schemes of (a) standardized FIDO and (b) FIDO for private key sharing.

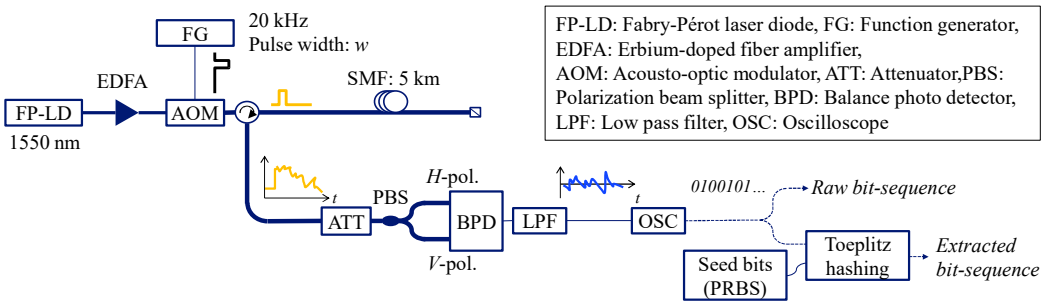

Fig. 2. Experimental setup for producing the raw and the extracted bit sequences.

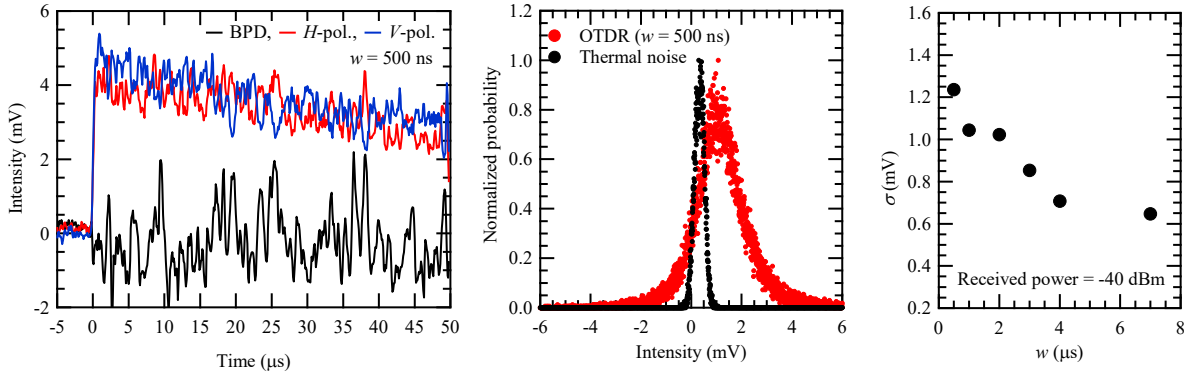

Fig. 3. (a) the OTDR waveforms of the output of BPD, the *H*- and *V*-polarization port, (b) the histogram of the received intensity for a OTDR waveform and thermal noise, and (c) *w* dependence of the standard deviation in the histogram.

user device can be equally used for authentication. Furthermore, any obstacles in installing the considered FIDO should be minimized by utilizing the existing equipment.

Figure 2 describes the experimental setup for generating the keys using OTDR measurements. A Fabry-Pérot laser diode (FP-LD) operating at 1550 nm was used to generate the test light. The optical power of the test light was amplified by an erbium-doped fiber amplifier (EDFA) up to 24 dBm to obtain a sufficient power level of backscattered light compared with the electrical noise. The test light was pulsed using an acousto-optic modulator (AOM) driven by a function generator (FG). The test pulse was launched into a 5-km-long SMF, and a backscattered light with an average power over −40 dBm was extracted through a circulator. The optical power of the backscattered light monotonically decreased due to the attenuation of the SMF, and it could deteriorate the randomness of the OTDR waveform. Thus, a balanced photo detector (BPD) was incorporated with a polarization beam splitter (PBS) to divide the backscattered light into *H*- and *V*-polarization states. When the polarization dependent loss was negligible, the power change due to the attenuation was eliminated. After filtering undesired high frequency components using a low-pass filter (LPF), the signal was digitized with an oscilloscope having a vertical resolution of 12 bits, and the sampling frequency was 10 MHz. We generated raw bit sequences from a waveform in 0–50 μs, which covered the whole length of the SMF. To improve the randomness of the bit sequence, we utilized a randomness extractor using Toeplitz-matrix hashing [7]. The seed bits were a PRBS generated based on the Mersenne Twister [8], and we obtained the seed bits for each time of the processing. The compression ratio of the extracted bit sequence to the raw bit sequence was set at $H_\infty/B\times0.9$, where H_∞ and B were the obtained minimum entropy and the bit resolution.

3. Experimental results

Figure 3(a) shows examples of observed results for the pulse width of 500 ns. The red and blue lines represent the OTDR waveforms for *H*- and *V*-pol., respectively. The black line indicates the difference in the two waveforms, which were output from the BPD. t = 0 μs corresponds to the time of the pulse input. the monotonical intensity reduction of the waveforms at each polarization port due to the attenuation and random fluctuation was found. The random factor resulted from the longitudinal variation of the Rayleigh backscattering coefficient and the interferometric component [9]. Only random fluctuation was obtained successfully in the output of the BPD. We divided whole intensity range into 2^{12} levels, and a set of 12-bit associated with each intensity level is assigned for

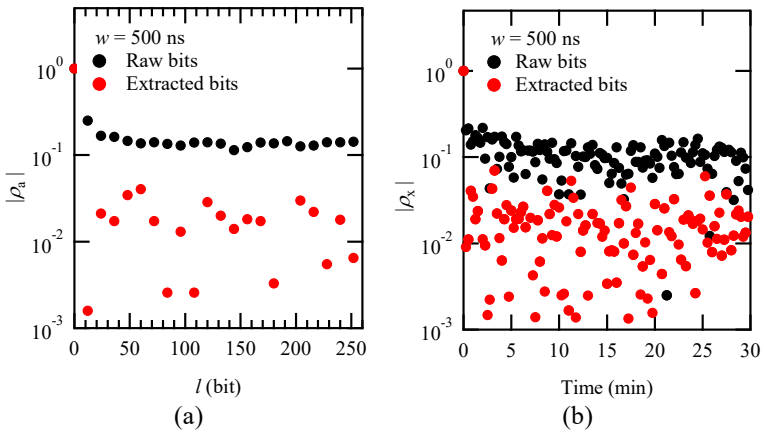

Fig. 4. (a) auto-correlation $|\rho_a|$ of a OTDR waveform and (b) cross-correlation $|\rho_x|$ between successively obtained OTDR waveforms.

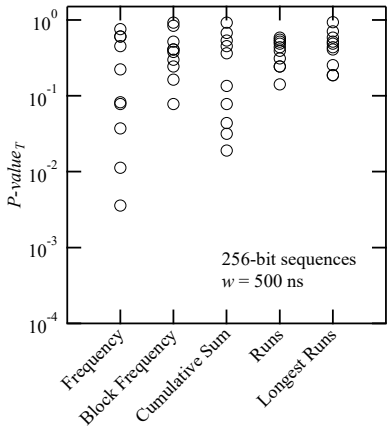

Fig. 5. *P-value*$_T$ results of the randomness tests.

each sampling point. Figure 3(b) is a histogram of the intensity of the observed waveforms. The vertical axis was normalized using the maximum probability. The red and black lines represent the results of the OTDR waveform with the BPD and the thermal noise, respectively. Each histogram was derived from 120 waveforms observed for 30 minutes and a 15-second interval. The standard deviation σ of the intensity fluctuation in the OTDR waveform of 1.2 mV was larger than that of the thermal noise of 0.2 mV. Therefore, the observed intensity fluctuation was mainly caused by the backscattered light. The w dependence of σ is shown in Figure 3(c). The average power of the backscattered light was adjusted at −40 dBm by the attenuator (ATT) in all pulse-width setups. σ increased as w decreased because the longitudinal resolution was increased. Therefore, a smaller w realizes acquisition of bits from a wider range of intensity, which results in improvement of randomness in obtained bit sequences.

We produced raw bit sequences from OTDR waveforms with w = 500 ns. An average H_∞ of 6.7 bits was found, and the compression ratio was less than 0.5 for the extracted bit sequences. We obtained 2048 bits from an OTDR waveform. The auto-correlation ρ_a in an obtained bit sequence and the cross-correlation ρ_x between bit sequences obtained from successive OTDR measurements were calculated to evaluate unpredictability and non-repeatability, respectively. Figure 4(a) and 4(b) are the absolute value of the $|\rho_a|$ and $|\rho_x|$. The open and filled circles represent values of the raw and the extracted bit sequences. A lag of 0 bit was set for $|\rho_x|$. The standard deviation of the correlations for the uniform bit sequences with the number of bits N was $1/\sqrt{N}$ [10], which was found to be 0.022 where $N = 2048$ as in this experiment. The standard deviation of ρ_a and ρ_x derived from the extracted bit sequences was 0.020 and 0.022, respectively, comparable with the ideal value. Thus, unpredictability and non-repeatability were achieved in bit sequences obtained by the OTDR and the extractor.

Finally, we evaluated the quality of randomness using the NIST SP800-22 Rev.1a test suite [6] for the extracted bit sequences. We prepared 1280 bit-sequences with a length of 256 bits from 120 OTDR waveforms observed in a 15-second interval. The test was conducted ten times, and 128 sequences were used for each test. We chose five types of tests that were able to evaluate the 256-bit sequences. Figure 5 summarizes the evaluated *P-value*$_T$. Every *P-value*$_T$ was found to be over 0.0001, which is recommended for uniformly distributed sequences [6]. Therefore, the obtained bit sequences from the OTDR measurements had sufficient randomness.

3. Conclusion

A sufficient quality of randomness as cryptographic keys was confirmed in 256-bit sequences obtained from a random behavior of the backscattered light of SMF incorporated with the randomness extractor. We can expect that a FIDO scheme enabling private key sharing is feasible with existing network equipment and relaxes inconvenience regarding a limitation among user devices.

3. References

[1] H-K. Lo et al., *Nature Photon*., **8**, 595 (2014).
[2] M. H-Collantes et al., *Rev. Mod. Phys.*, **89**, 1, 015004 (2017).
[3] M. Fuse et al., *ECOC*, We.4.P027 (2005).
[4] S. Machani et al., "FIDO UAF Architectural Overview," FIDO alliance (2020).
[5] FIDO alliance, "How FIDO Addresses a Full Range of Use Cases," white paper (2022).
[6] A. Rukhin et al., *NIST special publication* 800-22 Rev. 1a (2010).
[7] L. Trevisan, *J. ACM*, **48**, 4, 860 (2001).
[8] M. Matsumoto et al., *ACM TOMACS*, **8**, 1, 3 (1998).
[9] A. Smirnov et al., Sensors, **23**, 14, 6390 (2023).
[10] C. R. S. Williams et al., *Opt. Exp.*, **18**, 23, 23584 (2010).