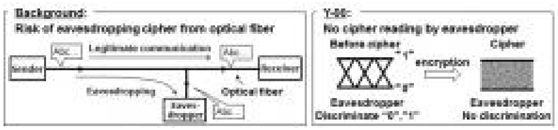
The world's fastest Y-00 stream cipher transmission at 40 Gbit/sec over 120 km

March 6 2012, By Adarsh Sandhu



Fumio Futami at Tamagawa University, Quantum ICT Research Institute, announced the world first transmission of the stream cipher by Yuen 2000 protocol (Y-00) at the bit rate of 40 Gbit/sec over 120 km.

Y-00 is a physical cipher that has a possibility to avoid the decipher and hence it is a promising candidate to realize secure networks. The key to success of high capacity transmission was the use of wavelength division multiplexing (WDM) scheme. Four lights with different wavelengths each carrying 10-Gbit/sec Y-00 encrypted optical signals were multiplexed into an optical fiber to attain the aggregate capacity of 40 Gbit/sec. In the experiment, it has been proved that the transmission capacity of Y-00 signals was increased by employing the WDM scheme. The capacity can be further increased with use of more number of lights with different wavelengths. The result made a step closer to practical use of Y-00 stream cipher in the real network services.

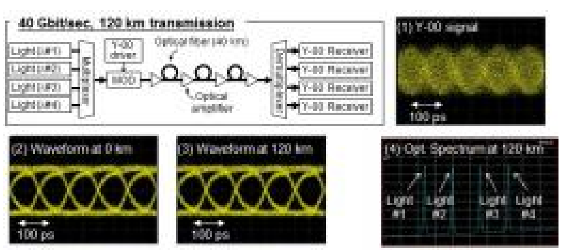
The details will be presented in the Optical Fiber Communication

Conference and Exposition and National Fiber Optic Engineers Conference (OFC/NFOEC) held in Los Angeles on March 6th, 2012. The title of the talk is “40 Gb/s (4 x 10 Gb/s) Y-00 protocol for secure optical communication and its transmission over 120 km.

Tamagawa University is advancing the research on developing a cipher that is capable of disabling the decipher and realizing secure communications. The University aims at practical use of the cipher in a network to realize the unbreakable system.

The quantum noise randomized stream cipher, Y-00, the University is developing is categorized into the multi-level intensity modulation from the viewpoint of modulation scheme. That is, it features that Y-00 requires no excess bandwidth. Therefore, the transmission capacity has been expected to increase with the WDM scheme that multiplexes the lights in wavelength. The scheme is widely utilized in the modern optical fiber communication for high capacity transmissions.

F. Futami successfully applied the WDM scheme to Y-00 encrypted optical signal transmission and demonstrated the Y-00 transmission experiment at the aggregate capacity of 40 Gbit/sec over a 120-km optical fiber transmission line with optical fiber amplifiers. The transmission distance was not limited by the technical limit, but by the amplifiers available for the experiment.



Currently, data that are not encrypted is traveling across the networks. Such data can be easily eavesdropped by taping the data from the optical fibers. Actually we succeeded in demonstration of eavesdropping data in our university network. Some data such as the personal information and the proprietary information is encrypted by the mathematical cryptography. The mathematical cryptography features practical implementation, however, there's the possibility of decipher since its security level is mainly dependent on the computational complexity, that is, the difficulty of vast amount of numerical calculations. For higher security, it is effective that a physical cipher is employed for the data in optical fibers. The University has been engaged in both the theoretical and experimental researches on a physical cipher, so called, Y-00. A fundamental idea of Y-00 protocol to avoid decipher is to mask the Y-00 signal level by noise. As shown in Figure, it disables an eavesdropper to discriminate the correct level of Y-00 signal and to read the cipher text itself, resulting in the failure of eavesdropping. A Y-00 encrypted optical signal is theoretically proved that there's no mathematical algorithm of cryptanalysis, and has a possibility of realizing the unbreakable security level. In the experimental researches, it has been demonstrated that cipher communication at 10 Gbit/sec over 360 km and Y-00 prototype transceivers in our University in-service GbE network. Those results are the evidences that Y-00 has compatibility with the current optical fiber communication systems. Furthermore, it was experimentally observed noise masking of Y-00 signal level that achieves high security level. Y-00 is the most promising candidate as the practical physical cipher applicable to the optical signals in the optical fiber transmission line. Consequently, the practical use of Y-00 is expected.

Today, data transmission volumes in the network are rapidly growing. Therefore, there is demand for Y-00 to enable higher capacity than the highest capacity of 10 Gbit/sec so far experimentally demonstrated.

An experiment of WDM transmission of Y-00 was demonstrated by using four lights of Y-00 that have different wavelengths. Each light carries 10 Gbit/sec data. Four lights were input to an optical fiber resulting in the transmission of total 40 Gbit/sec data in a fiber. The transmission distance was 120 km. After the transmission, four lights were demultiplexed in wavelength and Y-00 signals were received in Y-00 receivers to investigate the signal qualities. A waveform of Y-00 signal in Fig.1, which corresponds to one measured by an eavesdropper, did not show the signal intensity levels which disabled correct discrimination. On the other hand, the waveforms (Figs. 2 and 3) measured by the legitimate user before and after the transmission were correctly received. Moreover, the signal quality of the waveform after 120-km transmission was the same as that before transmission. The spectrum shown in Fig. 4 after the transmission revealed no harmful interactions among the lights with different wavelengths. The quantitative evaluations showed the evidence of high quality transmission.

Provided by Tamagawa University

Citation: The world’s fastest Y-00 stream cipher transmission at 40 Gbit/sec over 120 km (2012, March 6) retrieved 1 May 2024 from https://phys.org/news/2012-03-worlds-fastest-y-stream-cipher.html