Physical Layer Security: All-Optical Cryptography in Access Networks

Gabriella Cincotti [(1)], *Senior Member, IEEE*, Valentina Sacchieri [(1)], *Student Member, IEEE*
Gianluca Manzacca [(1)], *Student Member, IEEE*, Nobuyuki Kataoka [(2)], *Member, IEEE*
Naoya Wada[(2)], *Member, IEEE*, Naoki Nakagawa[(3)], *Member, IEEE*
and Ken-ichi Kitayama[(3)], *Fellow, IEEE*

[(1)] *Department of Applied Electronics, University of Roma Tre, Rome, Italy* cincotti@uniroma3.it

[(2)] *National Institute of Information and Communications Technology, Tokyo Japan*

[(3)] *Department of Electrical, Electronics and Information Systems, Osaka University, Osaka, Japan*

ABSTRACT
The physical layer security of passive optical networks (PON) is investigated within a rigorous cryptoanalysis framework; we consider different threats and confidentiality attacks and propose different secure optical code division multiple access (OCDMA)-based architectures.
Keywords: security, bit-ciphering, block-ciphering, cryptography, optical code division multiple access (OCDMA), passive optical network (PON).

1. INTRODUCTION

Passive optical networks (PON) are one of the most promising and cost-effective solutions for next generation access networks (NGAN), that can efficiently solve the broadband bottleneck of existing copper infrastructures. The need of data confidentiality is one of the major issues in these systems, due to their simple topology where downstream information is broadcasted from the optical line terminator (OLT) to all the optical network units (ONU), and a malicious user can easily intercept data directed to another user [1].

In an optical code division multiple access (OCDMA) system, each user encodes his messages using a different code, and transmits asynchronously with all the other users at the same wavelength; therefore, encoded signals overlap both in time and frequency, and only the intended receiver with a matched decoder is able to correctly extract the message. Multiple access interference (MAI) noise prevents an eavesdropper to intercept a message, without knowing the proper code, and many theoretical and experimental studies have demonstrated the intrinsic confidentiality of OCDMA system [2-5]. However, it has been observed that OCDMA network security cannot rely only on MAI noise, because it is always possible for an eavesdropper to tap an isolated signal, as shown in Fig. 1. Furthermore, the use of a code-switching scheme, to encode both logical marks and spaces from each user, is recommended to prevent that data confidentiality be broken by power detection. OCDMA-based PON at 10Gb/s has been experimentally demonstrated in field-trial experiments [6].

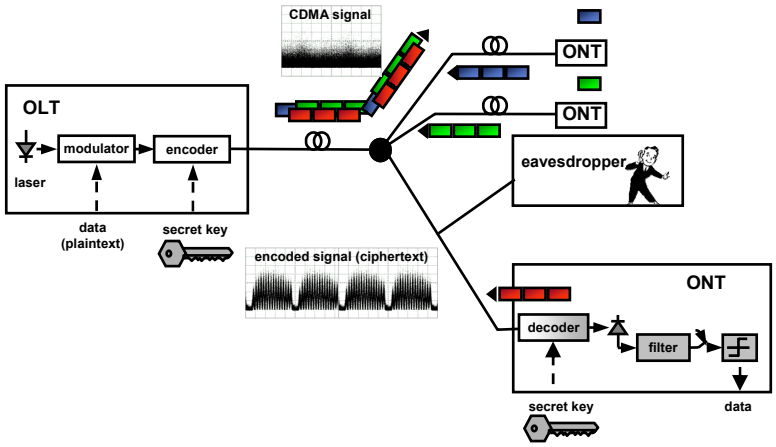

Figure 1. Scheme of an OCDMA-based PON.

In the present paper, we analyze the security performance of different phase shifted keyed (PSK) encoding techniques, using a single multiport encoder/decoder (E/D), that has the unique capability to generate and process a set of different codes simultaneously. We consider both bit- and block ciphering schemes, and, according to the *Kerckhoffs' principle*, we assume that the eavesdropper knows all the parameters of the transmission (bit rate, modulations, wavelength,…) and of the encoding technique (chip rate, code length…), except for the particular code that the user is employing [2-3]. The cryptanalysis is performed against *ciphertext only attacks* (COA), *known plaintext attacks* (KPA) and *chosen plaintext attacks* (CPA).

978-1-4244-2626-3/08/$25.00 ©2008 IEEE

2. ENCODING METHODS

A multiport E/D has an arrayed waveguide grating (AWG) configuration with N input and output ports, as shown in Fig. 2 [7, 8]. When a single laser pulse is sent into one of the input ports, the device generates N optical PSK codes, performing a 1-D encoding. To increase the code cardinality, it is possible to realize a n-dimensional encoding, sending n coherent laser pulses into n different input ports: the n-D codes generated are a coherent sum of n PSK codes.

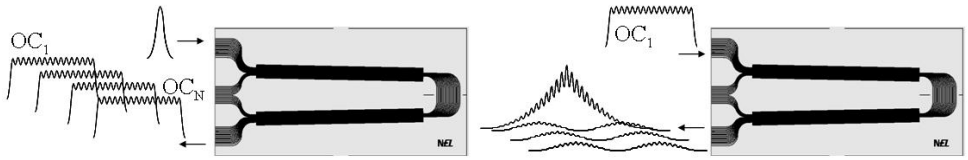

Figure 2. Multiport encoding/decoding device.

The decoding process is performed by the same device, forwarding the code into one of the decoder input ports and measuring the cross-correlation signals at its outputs: the autocorrelation peak (ACP) detected at one port identifies the code; the cross-correlation peak (CCP) between two different codes is about 10 dB lower than the ACP. In case of n-dimensional codes, we measure n ACPs, and their mutual positions among the decoder output ports, unequivocally identifies the code.

We can had a degree of freedom to the encoding process by changing the phases of the coherent laser pulses, by using an array of phase shifters at the encoder input ports, and correspondently at the decoder output ports. Using this device in different configurations, we can perform both bit- and block-ciphering techniques, encrypting the message directly in the physical layer.

2.1 Bit ciphering

Bit ciphering establishes a direct correspondence between bits and optical codes: each bit (both logical zeros and ones) from each user is encoded with a different codeword. For each user, we use a multiport E/D, where $N/2$ ports are used to transmit the logic "1" and the remaining ones to transmit the logic "0". In 1-D encoding, the code space equates the number of the E/D ports, and in the n-D case, the code space is exponentially larger: a device with $N = 100$ ports and $n = 50$ input pulses can generate more than 10^{29} codes. Although enlarging the code cardinality increases data confidentiality, the proposed system cannot be considered completely secure because an eavesdropper that possesses a matched decoder is able to decipher the message.

We can enhance the network security by changing the phases of the coherent laser pulses that are used to generate a n-D code, as shown in Fig. 3. We apply two pseudorandom binary phase codes to all the laser pulses sent into the encoder input ports, and only the intended receiver that knows the phases is able to decrypt the message. In this case, the secret key is the sequence of N phases, that can have values 0 or π, and the code cardinality is 2^N.

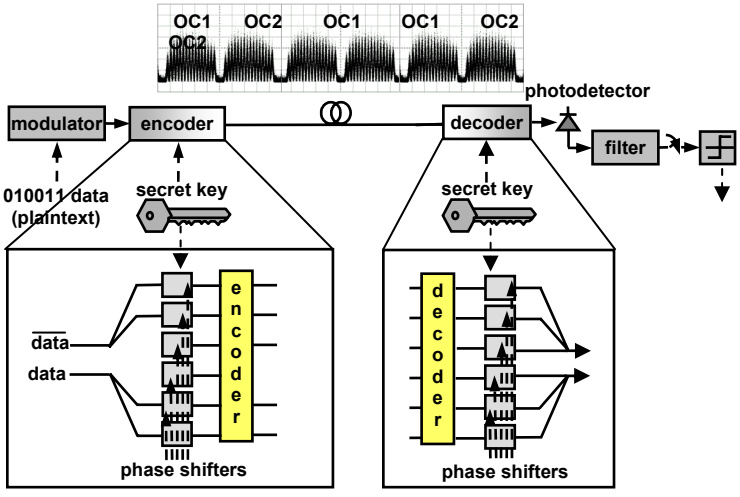

Figure 3. Bit-ciphering scheme.

It is well known that electronic bit-ciphering cannot be considered secure because it can be broken by a differential cryptanalysis. In fact, this technique establishes a fixed correspondence between marks and spaces and two different codes, and an eavesdropper that is able to detect differences between the two codes can break the system confidentiality, without knowing the codes. In the optical domain, differential cryptanalysis can be performed by using a standard a differential phase shift keying (DPSK) receiver [4]. Furthermore, bit-ciphering

is secure against brute-force code searching attacks, but not against known plaintext attacks and chosen plaintext attacks.

2.2 Block ciphering

Block ciphering is widely used in electronic cryptography, and we demonstrated that it can be used also in the optical layer, to increase the degree of confidentiality against all kind of attacks. Data transmitted is divided in sequences of m bits and encoded with an alphabet with at least $M = 2^m$ determinations, that correspond to optical codes; the secret key is not the optical code itself, but the correspondence between an optical code and a bit sequence. In this way, we add two levels of security to data transmission: the eavesdropper has to first detect the optical code, and then he to find the correspondence between the code and the bit sequence.

If we associate a standard 1-D PSK code to each bit sequence, the maximum length of the bit sequence that we can encrypt is $\log_2 N$, and all the possible correspondences between an optical code and a bit sequence are $N!$.

If we use n-D codes, splitting the laser pulse among N input ports of the encoder, the number of codewords is 2^N, the block length is $n = N$ bits, and the all the possible correspondences between optical codes and bit sequences are $2^N!$. We remark that in this case the secret key is the electronic signal that drives the switch and assigns a different n-D code to each n-bit sequence, as shown in Fig. 4. It is also possible to select $n < N$, so that two or more multidimensional codes encrypt the same sequence of bits, to enhance the system confidentiality.

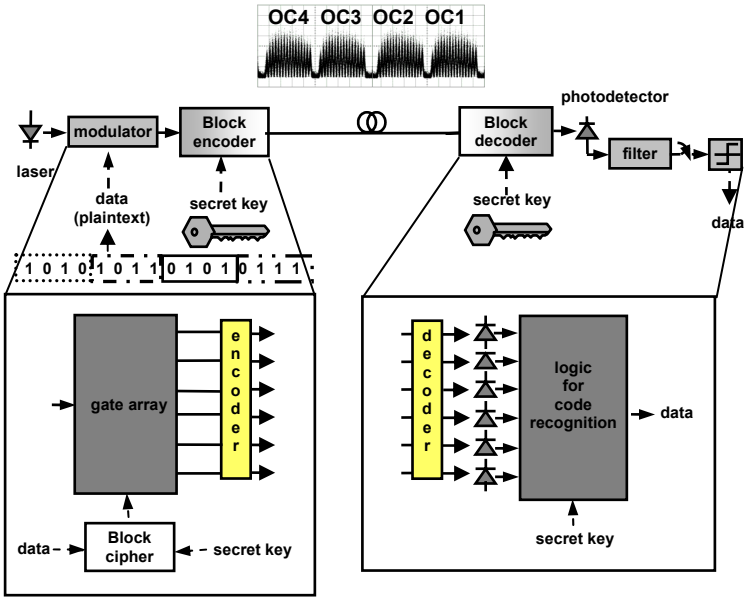

Figure 4. Block-ciphering scheme.

3. DATA SECURITY ANALYSIS

To present a quantitative analysis of the system confidentiality, we start considering the exhaustive key search attack, that is the simplest among the COA. In Fig. 5a, the number of trials needed to break the security is shown as a function of the number N of the E/D ports. We assume that the average number of trials requested to break a code is $K/2$, where K in the overall number of secret keys; in the case of bit-ciphering using n-D codes, it is $K = 2^N$, and for block-ciphering, we have $K = 2^N!$.

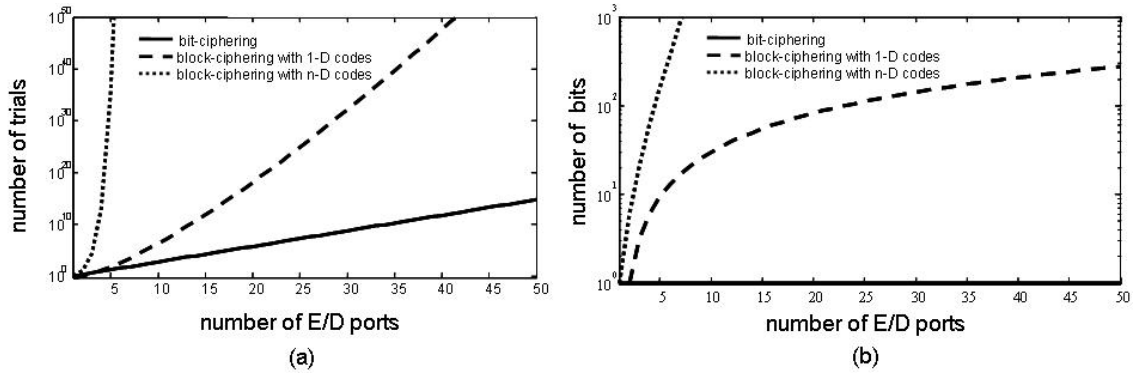

Figure 5. (a) Number of trials needed to break the confidentiality in a COA attack. (b) Number of bit needed to break the confidentiality in a CPA attack.

In a CPA, the adversary has access to the encryption function and can encrypt any plaintext message, trying to determine the secret key. In this case, the lower bound security parameter of modern cryptanalysis is the number of plaintext bits that he or she needs to know to detect the code. In a bit-ciphering scheme, just a single bit allows the adversary to intercept the data; in block-ciphering scheme, instead, the number of message bits required are $(N-1)\log_2 N$, for 1-D codes, and $N(2^N-1)$ for n-D codes, as reported in Fig. 5b.

4. CONCLUSIONS

Physical layer solutions to increase security in optical networks have been presented, performing the encoding and decoding processes with a single multiport encoder/decoder. We have analyzed the performance of bit- and block-ciphering cryptosystems against different kind of security attacks, considering spectral phased, one-dimensional and multidimensional codes.

We demonstrate that bit-ciphering is resistant only against ciphertext attacks, and that block-coding are robust also against known plaintext attacks and chosen plaintext attacks. Furthermore, block encoding allows us to increase the channel capacity of a factor $\log_2 M$.

To enhance data confidentiality, it is possible to use a time varying security keys, according to the Vernam's one-time pad theorem, which states that an unconditionally secure system is obtained when the secret key is changed every transmitted block.

ACKNOWLEDGEMENTS

The work described in this paper was carried out with the support of the BONE-project ("Building the Future Optical Network in Europe"), a Network of Excellence funded by the European Commission through the 7th ICT-Framework Programme.

REFERENCES

[1] V. O'Byrne: Verizons fiber to the premises: lessons learned *in Proc. OFC 2005*, Anaheim, CA, USA, Mar. 2005, paper OWP6.
[2] T. Shake: Security performance of optical CDMA against eavesdropping, *J. Lightwave Technol.*, vol. 23. pp. 655-670, Feb. 2005.
[3] T. Shake: Confidentiality performance of spectral phase encoded optical CDMA, *J. Lightwave Technol.*, vol. 23. pp. 1652-1663, Apr. 2005.
[4] Z. Jiang, *et al.*: Experimental investigation of security issues in O-CDMA, *J. Lightwave Technol.*, vol. 24. pp. 4228-4334, Nov. 2006.
[5] F. Xue, *et al.*: Security issues on spectral-phase-encoded optical CDMA with phase masking scheme, in *Proc. OFC 2006*, Anaheim, CA, USA, Mar. 2006, paper OThT3.
[6] N. Kataoka, *et al.*: Duplex, fully-asynchronous, 10Gbps x 8-userDPSK-OCDMA field trial using a multi-port en/decoder and SSFBG en/decoders, in *Proc. OFC 2008*, San Diego, CA, USA, Feb. 2008, paper PDL.
[7] G. Cincotti, *et al.*: Characterization of a full encoder/decoder in the AWG configuration for code-based photonic routers—Part I: modeling and design, *J. Lightwave Technol.*, vol. 24. pp. 103-112, Jan. 2006.
[8] N. Wada, *et al.*: Characterization of a full encoder/decoder in the AWG configuration for code-based photonic Routers-part II: experiments and applications, *J. Lightwave Technol.*, vol. 24. pp. 113-121, Jan. 2006.
[9] R. Oppliger: *Contemporary Cryptography*, London: Artech House, 2005.