11A3-5 (Invited)

Security performance of optical multicoding transmission using a single multiport encoder/decoder

Gabriella Cincotti[1], Gianluca Manzacca[1], Valentina Sacchieri[1], Naoya Wada[2], Xu Wang[2] and Ken-ichi Kitayama[3]

1: Department of Applied Electronics University Roma Tre, via della Vasca Navale 84, I-00146 Rome, Italy,
phone: ++39 0655177399, fax: ++39 0655177026, email: g.cincotti@uniroma3.it
2: National Institute of Information and Communications Technology, 4-2-1, Koganei, Tokyo 184-8795, Japan.
3: Osaka University, 2-1 Yamadaoka, Suita, Osaka 565-0871, Japan.

Abstract

We investigate the confidentiality of an OCDMA P2P transmission, using a single-chip multi-port optical encoder/decoder, as a function of the number of device ports. We consider symmetric bit and block cryptosystems, and investigate the security against brute-force searching attacks.

Introduction

Triple-play services drive an increasing demand for broadband, high-speed access networks, and passive optical networks (PONs) are excellent solutions to meet future demand. A PON has a point to multi point (P2MP) topology, between an optical line terminal (OLT) located at the central office (CO), and *N* optical network units (ONUs) that serve single or multiple residential or business users. Downstream is broadcast and select (B&S), on a single wavelength using time division multiplexing (TDM); destination and source addresses are usually in plain and Ethernet-based traffic frames do not always include encryption of payload. Upstream traffic is scheduled in time division multiple access (TDMA) that does not guarantee data confidentiality. Optical code division multiple access (OCDMA) is receiving increasing attention thanks to its potential to enhance data confidentiality, spectral efficiency and flexibility in asynchronous multiple access networks. In an OCDMA transmission, the mark bits from each user are encoded by a different code; encoded signals can be overlapped both in frequency and time domains and are recognized only by a matched decoder.

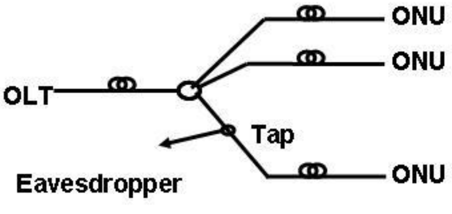

Fig.1: PON topology and eavesdropper attack

Although multiple access interference (MAI) hides transmitted data from each individual user, an accurate analysis of OCDMA network security should consider a point-to-point (P2P) transmission, because an unauthorized user could be able to tap an isolated users signal (see Fig. 1). Secure spectral phased encoding OCDMA have been investigated in literature [1, 2], according to the *Kerckhoff's principle*, that assumes that all the details of the transmission (bit rate, wavelength, etc..) are of public knowledge, and the code is the only *secret key*. We investigate the confidentiality of a P2P OCDMA transmission using a single chip multiport encoder/decoder (E/D), in an arrayed waveguide grating (AWG) configuration [3]. The device has *N* input/output ports and it is able to generate/process *N* phase shifted keyed (PSK) codes simultaneously. The code cardinality *N* is not large enough to guarantee a secure transmission, and for this reason, we consider a *n*-dimensional (*n*-D) configuration, where *n* coherent laser pulses are sent to *n* different input ports. A *n*-D code is recognized

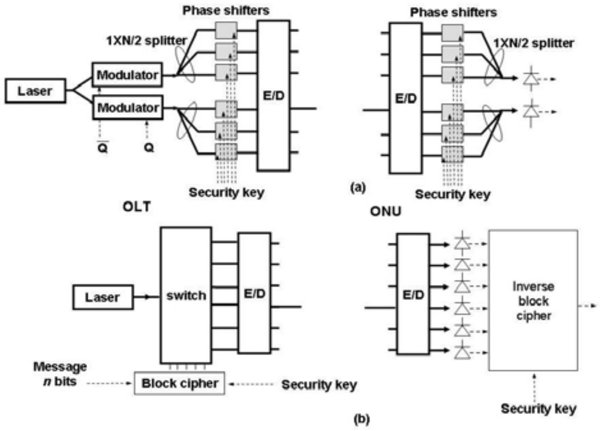

Fig.2:Bit (a) and block (b) cipher architectures

by the same device, detecting *n* autocorrelation peaks (ACPs). On-off keying (OOK) OCDMA is a non-secure transmission, because it can be broken by power detection; for this reason, we consider 2- or multiple-code keying systems.

Bit cipher cryptographic systems

The key space of *n*-D codes is very large, and a device with *N*=100 ports can generate/process more than 10^{29} different codes; but an eavesdropper that possesses a matched decoder can easily break the code. For this reason, we add a new degree of freedom, inserting phase shifters at the encoder input ports, as illustrated in Fig. 2a; this coding scheme corresponds to a spread-spectrum OCDMA, and the private key is the pseudo-random binary phase code. Both mark and space are encoded, so that balanced detection is also possible, to enhance the OCDMA transmission performance. The system security is shown in Fig.3: we consider a *brute-force code searching* attack and evaluate the number of years required to break a code, assuming that an adversary is able to test 10^7 codes per second.

Block cipher cryptographic systems

In this scheme, a block of *n* bits from each user is encoded by a different codeword, sending *n* laser input pulses to different inputs of a multi-port E/D. Figure 2b shows the OLT and ONU architectures: the *message* from each user is mapped into a *n*-bit *ciphertext*, using an electronic cryptographic system, that drives a switch to generate an optical *n*-D code; *n* ACPs detected at outputs of the multi-port E/D at ONU can be seen as *n* marks of the ciphertext than can decrypted into the original message. The electronic encrypting and decrypting systems can have an internal state: in that case they are named *stream ciphers*. The key space potentially comprises all the permutations over *n* bits that are $2^n!$; for instance, if *n*=10, all the possible keys are $5.42\cdot10^{2639}$. Symmetric cyptosystems use only some of all the possible *permutations,* combined with *substitution* to provide *confusion* (to make the relation between key and ciphertext complex) and *diffusion* (to expand the influence of a single plaintext bit over many ciphertext bits).

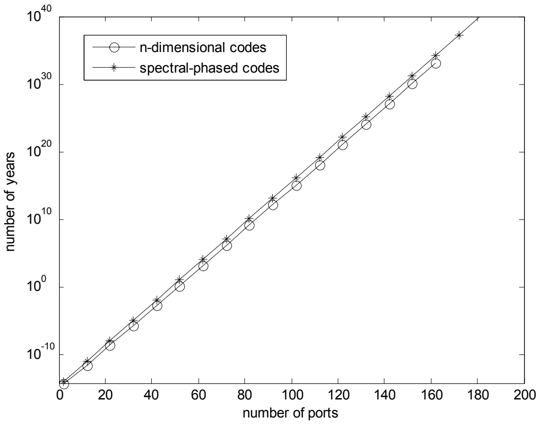

Fig.3:Security versus the number of E/D ports

Data encryption standard (DES) developed by IBM in 1970 encrypts blocks of *n*=64 bits, with 16 multiple iteration, using a key space of 2^{56} elements. Unfortunately in 1998 *Deep Crack* was able to break the system in 4.5 days, and cryptosystems with longer keys have been developed to increase the system confidentiality. According to *Shannon's theorem*, a perfectly secure encryption system requires that entropy of the key space is larger than that of the message space. The system of Fig. 2b corresponds to an *n*-ary transmission, where *n* bits from each user are transmitted simultaneously.

Conclusions

Planar architectures to encode data messages from a multiple access user have been presented, and the P2P transmission confidentiality has been investigated. We presented both bit and block cipher cryptosystems, and compare their performance against brute-force code searching attacks.

To increase data confidentiality, it would be necessary to use time-varying encoding keys; using the *Vernam's one-time pad* scheme, a perfectly secure system can be obtained when the private key is changed every bit or every message block.

References

1 T. H. Shake, IEEE J. Lightwave Tech., vol. 23, 1652-1663 2005..

2 Z. Jiang et al. OthT2, OFC 2006.

3 G. Cincotti, et al., IEEE J. Lightwave Tech., vol.24, 103-112, 2006.