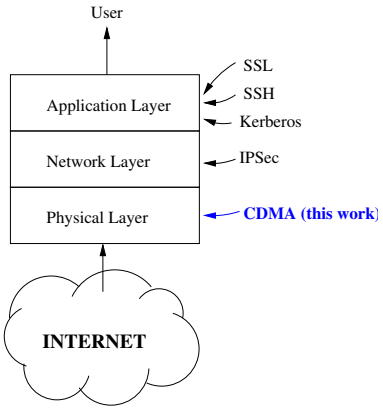
CDMA Time-hopping Optical Network with Enhanced Security

A. A. Ortega[1], V. A. Bettachini[2]
J. I. Alvarez-Hamelin[1,2]
[1]ITBA (Instituto Tecnológico de Buenos Aires)
[2]CONICET (Consejo Nacional de Investigaciones Científicas y Técnicas)
aortega@alu.itba.edu.ar, {vbettachini,ihameli}@itba.edu.ar

ABSTRACT: *A method to provide cryptographically secure point-to-point and point-to-multipoint communication using an encrypted Bloom filter is implemented on a time-hopping CDMA optical fiber network. A novel Hamming-weight minimization coding algorithm optimises the performance of the encrypted Bloom filter in terms of end-user bandwidth utilisation over previous proposals. The system has a total channel utilisation of up to 29% for* **128** *simultaneous users, up to* **20** *km apart, served by a single passive optical hub, or longer distances if served by an active hub.*

Keywords: Security, Bloom Filter, Encryption, communication, Algorithm



Simplified OSI network model

1 Introduction

Communication methods currently employed in access optical networks are inherently insecure, as signals are broadcast to all users (e.g., as in Passive Optical Networks, PONs), and do not provide privacy from a sufficiently motivated eavesdropper. To avoid attacks to privacy, end points can implement security measures on the network logical layer protocols (see Fig.); however, these are often neglected. Implementation of security measures is mandatory to stablish secure Virtual Private Networks (VPNs) over public optical networks to serve privacy minded users.
Previous works address the privacy problems with solutions based on logical layer protocols to create a VPN-capable system. For instance Ref. [8] proposed the use of direct-sequence Code Division Multiple Access (CDMA) and Walsh coding. However, Walsh or similar codes cannot provide a large enough code space to be used in a strong secure cryptosystem [11]. An alternative approach that provides privacy in the logical layer applies the Advanced Encryption Standard (AES, see [3]) to data, then sent by direct sequence CDMA with a short code length [14]. Altough this method offers privacy and high channel utilisation, it is limited to point-to-point communication.

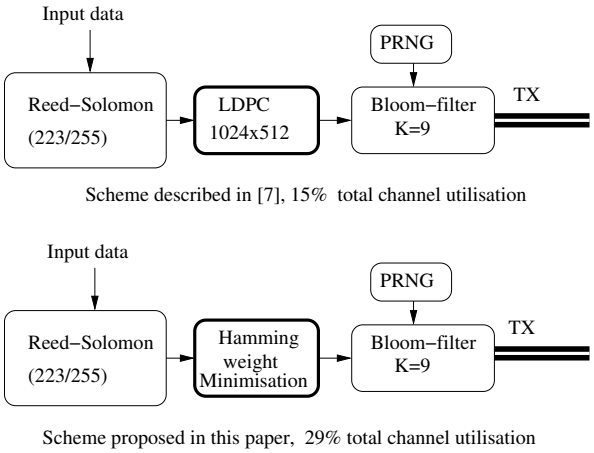


Figure 1: Comparison of coding stages proposed in [10] and in this paper. Channel utilisation correspond to 128 simultaneous end users.

A workaround to the shortcomings of security in the logical layer is to implement measures in the physical layer. A proposal in this sense provided all-optical VPN emulation using dynamic wavelength reflection or multiple fiber Bragg grating (FBG) reflectors [13]. However use of optical filters implies a fixed network configuration requiring physical access to reconfigure it in order to stablish VPNs. Another physical layer approach was presented in Ref. [7], but shares the same limitations of logical-layer based solutions, it provides only point-to-point communication and a reduced key space.
The scheme presented in this paper implements security at the physical layer, allowing point-to-point and point-to-multipoint communication, and does not require physical access to create VPNs, as channels can be re-configured remotely. Our proposal addresses the security problem through time-hopping CDMA, where the position (or slot) of each bit of the data stream is selected by a Pseudo Random Bit Sequence (PRBS). The security of this system relies on the implementation of the PRBS which must be cryptographically secure. Its only requirement is a secure shared-key distribution between end users.
This paper is organised as follows: Section 2 presents the basis of this proposal, section 3 presents the network physical and logical architecture; section 4 gives a detailed description of Hamming-weight minimisation, section 5 discusses security advantages, and finally, the last section 6 is devoted to numerical simulations implementation and results.

2 Overview

The scheme reported in [10] provided confidentiality to optical access networks using a time-hopping CDMA scheme at the physical layer. In this case the end user needs an pre-shared key provided by the transmitter. Note that this leads to point-to-multipoint communication if multiple users received the same pre-shared key. The network configuration allowed the setup of VPNs among users, in which each user transmits data in frame slots assigned by a cryptographically secure PRBS. As these sequences are non-orthogonal, collisions will occur between streams; thus the system requires heavy use of Forward Error Correction (FEC, see [6] and references therein) to provide low Bit Error Rates (BER) better than 10^{-8}. With this FEC the total usable medium utilisation was 15.7% when all of 128 end-users were transmitting simultaneously. In that proposal, FEC was performed by Low-Density Parity Check (LDPC) and Reed-Solomon algorithms. These are particularly intensive in the use of hardware resources and also significantly reduce the bandwidth available to the user.
In this paper we extend our previous proposal in terms of hardware simplicity and performance by eliminating the LDPC stage, and using instead a zero-minimising algorithmic coding stage, i.e., Hamming weight minimization (see section 4). This stage decreases the FEC overhead, yielding an increase of the system total bandwidth utilisation up to 29% of the medium capacity (15.7% in [10]).

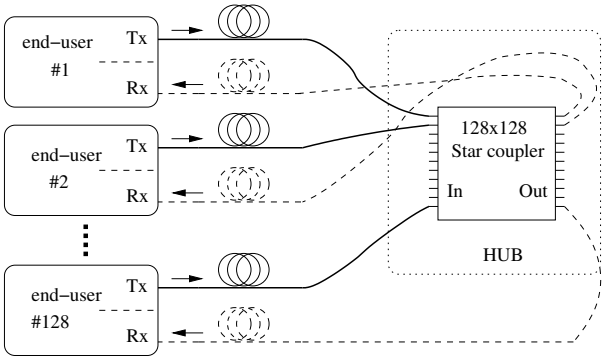


Figure 2. A star coupler is the basis of the optical network architecture for a $10\ \mathrm{km}$ reach.

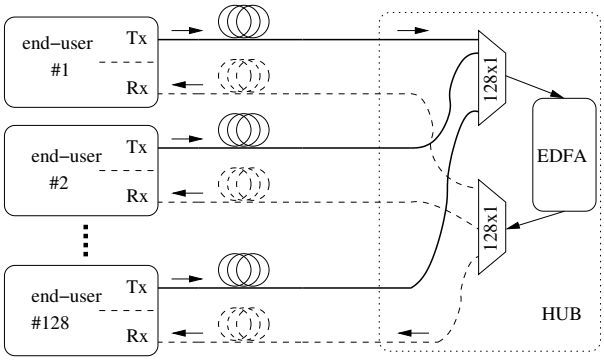


Figure 3. For reaches exceeding $10\ \mathrm{km}$ the network architecture requires amplification provided by an EDFA.

3 Network architecture

The physical layer structure is similar to that of a PON star topology operating with On-Off Keying (OOK) modulation operating at a $1550\ \mathrm{nm}$ single wavelength. A single central hub redistributes traffic from each end-user to all the rest, allowing point-to-multipoint as well as point-to-point communications of up to 128 end users. A hub function can be fulfilled by a single 128x128 passive star coupler, as shown in Fig. 2, where end users can be located up to $10\ \mathrm{km}$ away from the hub. This scenario assumes a $2\,\mathrm{dBm}$ transmitter power, $6\,\mathrm{dB}$ fiber attenuation for two $10-\mathrm{km}$ stretches, an insertion loss of approximately $25\,\mathrm{dB}$ for the 128x128 star coupler, and a receiver sensitivity of $-28\,\mathrm{dBm}$. Alternatively, if longer distances need to be served, power budget constraints can be addressed by using a hub with an Erbium Doped Fibre Amplifier (EDFA) and a pair of 1x128 optical splitters, as shown in Fig. 3. The EDFA gain is required to exceed $27\,\mathrm{dB}$.

Time-hopping CDMA is implemented by each end user by writing every bit of its stream in a determined position, or bit slot, inside a data frame. This position is chosen randomly by the end user PRBS generator (PRNG). As discussed in section 2, this leads to collisions. Since the modulation format is OOK, only transmitted ‘1’s can interfere with ‘0’s. This behaviour can be modelled as a Z-channel because the superposition of individual light pulses representing ‘1’s can only be identified as a ‘1’, but a received ‘0’ is an unmistakable sign of the absence of pulses in a given time slot. We found that the Bloom filter [2] provides a convenient structure to correct for errors in this type of channel. This technique is borrowed from hashing algorithms and is used to test whether an element is member of a given set. The way that we implement this algorithm relies on copying every bit in K slots of the transmitted frame. On the receiving end it is sufficient to receive a single ‘0’ out of K copies in order to correctly retrieve the original transmitted ‘0’, whereas collisions have no effect on ‘1’s.

Improvements in channel utilisation over the design presented on [10] are due to the different coding stage, where a Hamming-weight minimisation algorithm (see section 4) is used to reduce collisions instead of LDPC. Synchronisation is only needed at the bit-slot level in contrast to TDMA where it is also performed at frame level. The

Data	Input HW= 0 to 3	Expanded HW=2
0	000	00011
1	001	00110
2	010	00101
3	011	01100
4	100	01010
5	101	01001
6	110	10001
7	111	10010

Table 1. Hamming minimisation table for 3-bit symbols

standard hard-decision Reed-Solomon (223/255) stage is still used. A BCH algorithm could be used instead of the Reed-Solomon stage as an alternative for better performance in terms of bandwidth utilisation [6].

4 Hamming weight minimization

This scheme based on time-hopping CDMA relies on symbol interference for confidentiality as data from other end users effectively acts as noise. Symbol interference, as discussed in section 2, causes errors that need to be corrected. As these errors reduce the usable channel bandwidth, it is desirable to decrease interference to a point where it still provides security while maximising bandwidth usage. In order to decrease interference it is not advisable to modify the cryptographically secure random generator, since it would compromise the security of the whole system by introducing predictability in the symbol positions (e.g., using orthogonal codes as in Ref. [8].) Instead, a strategy based on the fact that an optical channel can be modelled as a Z-channel is pursued.
Hamming-weight of a symbol is the number of bits '1', which is directly related to interferences in the Z-channel. The Hamming-weight minimisation algorithm consists on coding every binary symbol into an equivalent longer one, having more '0's and less '1's than in the original symbol. Applying a Hamming-weight minimising algorithm thus decreases interference. Intuitively, a longer symbol would decrease the channel bandwidth; but as numerical simulations shown (see section 6) as intersymbol interference decreases the FEC overhead can also decrease, compensating for the increase in symbol length and yielding a net bandwidth gain. Normal binary symbols of length L have variable Hamming weight, with L/2 being the average, zero being the minimum and L being the maximum weight. We propose decreasing this Hamming weight (HW) to HW=2 a small number, as a good compromise between interference reduction and symbol length. Additionally, for security purposes we use a fixed Hamming weight for all symbols. This causes a slight loss of bandwidth but makes it impossible to infer any information about the transmitted symbol by analysing statistics of the transmitted data.

4.1 How the Hamming weight is minimised

The symbol expansion can be implemented as a lookup table (see table 1), where a symbol, of length L, is used as the index. The coded symbol has a length N>L. For practical implementation purposes it is desirable for L to be either 8 or 16 bits, so the table will have either 256 or 65536 entries. We apply the Hamming weight minimisation to symbols of 8 or 16 bits of length, thus it is needed a 256 or 65535 output symbols with a HW=2, respectively. To encode a 16-bits input symbol and HW=2, output symbols of 363 bits long are needed. Note that the number of unique symbols with HW=2 and N=363 is not exactly 65536 but 65703, so the expansion table is not unique. The ordering of the symbol conversion is not important as long as the same table is used in all the nodes trying to communicate.

4.2 Symbol insertion into the Bloom filter

Once the symbol expansion has been performed it is inserted into the frame upon which the Bloom-filter algorithm is applied, and becomes the frame to transmit. For instance, a 16-bit input symbol gets expanded to a 363 output symbol which, in turn, is inserted into a frame 4700 slots long (M=4700 bits). The K parameter of the Bloom filter represents the number of insertions per bit, K=9 means that actually 9 insertions are needed. As every output symbol has a HW=2, every symbol needs exactly 18 bits '1's insertions at pseudo-random positions inside the data frame (bits '0's need no insertions at all because Z-channel is used). Figure 4 illustrates the case for K=3 and HW= 2.

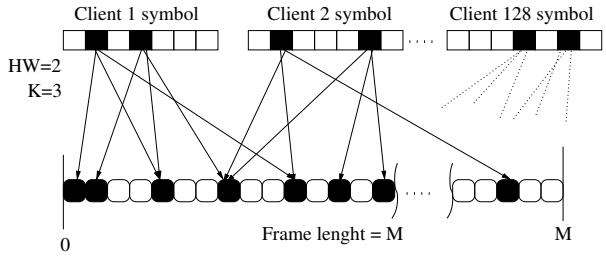


Figure 4. Symbol insertion into the Bloom filter

This shared data structure where the correct bit positions are only known to the communicating end users is called the *encrypted Bloom filter*. Symbol insertion is the stage where system security is enabled by selection of the symbol position inside the Bloom-filter data structure, according to a cryptographically secure PRNG. The seed of this generator is derived from a key or password that is shared between all the end users that want read/write access to the private channel. The Bloom filter copies K, the fixed Hamming weight HW, and frame length M are selected to maximise the error correction capacity at the designed coded symbol length N and number of simultaneous end users.

4.3 Decoding

The frame upon which the Bloom-filter algorithm is applied is modulated into an OOK optical signal, and collides with signals from other users. The destination node uses the synchronised PRNG to decode it and obtain the expanded symbol.
By their very nature Bloom filters never produce false negatives, meaning that a '1' bit can always be recovered with no errors. However, it can produce false positives. As the Bloom filter contains K copies of the data at random locations, all the '0' bit copies must have collided with '1's to cause an error, actually working as the first error-correction stage. The expanded symbol is decoded using an inverted expansion table to recover the original symbol. With a large number of users transmitting simultaneously, not all errors will be corrected by the Bloom filter. The remaining errors can be corrected by using standard FEC to achieve a required BER. Our FEC stage uses a Reed-Solomon algorithm in a 223/255 configuration.

5 Security considerations and cypher strength

There are several aspects of security to a communication channel: Authentication, reliability, confidentiality, and integrity. The scheme presented in this paper uses CDMA to provide confidentiality, reliability, and integrity between two or more parties, and is equivalent to a shared-key symmetric encryption scheme where the shared key is used to initialise the PRNG. Additional aspects like authentication can be implemented using logical-layer protocols. We specifically designed the proposed system taking into consideration attacks of the sort presented in Ref. [11].
As system security relies on the strength of its PRNG, special care must be observed in the selection and implementation of a suitable cryptographically strong algorithm. The proposed PRBS is non-linear, e.g., as in a self-shrinking generator [4]. Additionally the user's key is never broadcast to the network, so key distribution must be performed beforehand using a secure channel.
We address an additional vulnerability inherent to optical systems arranged as a star network: CDMA algorithms depend on interference for confidentiality. However, in an optical star-topology there are locations where little or no interference among users is present, for instance, next to the transmitter output of an end user the signal power is high and can be singled out from the background noise. Note that even if the hypothetical eavesdropper can locate and observe the bits of the transmitted symbol, they cannot infer any information. As positions within the data frame can overlap, the eavesdropper will observe a symbol with a HW between 1 and HW$\times$K, but it is not possible to reconstruct the right order of the bits without the PRNG seed.
Most encryption algorithms rely on XORing (the case of the RC4 encryption algorithm), a combination of substituting/scrambling of the bits before transmission (AES and DES encryption algorithms), or more complex transformations (RSA or Elliptic Curve algorithms), see Ref. [5]. However, these techniques necessarily modify the Hamming weight of every symbol in a way that is not optimal for our CDMA scheme as it increases intersymbol interference. As

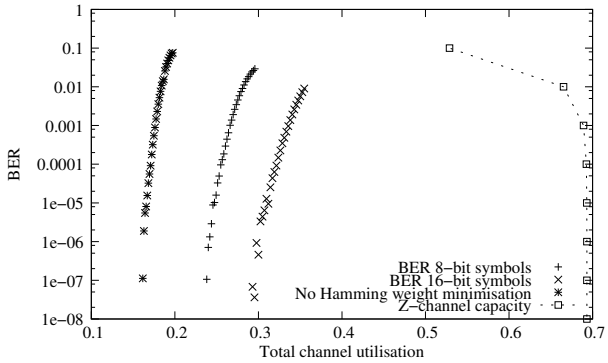


Figure 5: Utilisation of the 10 Gbps channel. Each one of the 123 to 158 users transmitted 1 Gbit of data. Note the improvement in bandwidth utilisation compared to that in [10].

the presented algorithm relies on time-hopping CDMA, it effectively encrypts symbols while maintaining the desirable low Hamming weight, increasing total bandwidth utilisation as shown in Fig. 5.
In contrast to TDMA, in our scheme the eavesdropper needs to intercept every optical fibre to reliably identify each end user as they are anonymised after passing through the central hub.

6 Numerical simulation

We tested through numerical simulation the performance of the proposed scheme in terms of BER for each set of data frame and Bloom filter parameters. To generate each data point we simulated the transmission of one gigabit of random data by a single user, and its interference from the remaining end users. Special care was taken to generate realistic expanded-symbols interference from these remaining end users.
The software has modules for the Bloom filter, error correction algorithms (Reed solomon and scrambling), and simulation of the optical channel. Each stage performs a single operation and are totally interchangeable (see Fig. 1). All modules were implemented using the C++ language and compiled to native code. Individual modules act as filters so they can be combined via UNIX pipes. The Hamming weight minimisation stage is included inside the Bloom filter module. The Reed-Solomon and scrambling stages are actually two separated software modules configured independently. This is followed by simulation of the optical layer.

6.1 Data flow

The modules are chained via their standard input/outputs, and simulation begins when a binary data block (random bits) is feed to the first module, that is, the reed-solomon enconder. The output of this encoder is feed to the next one, the scrambler. In this way the original data is transformed in each stage and succesively pass through all modules until the end of the stack is reached, that is the reed-solomon decoder.
At this stage the system compares the original input with the output, and finally calculates and reports the BER. Normally 1×10^9 bits or more needs to be simulated for each client. As up to 128 clients has to be simulated in each run, computational resources needed for simulation are considerable. The software provides a client-server model in which calculations are shared among multiple nodes.
All modules of the software simulator are available under an open GPL license [9].

6.2 Optical Simulation Parameters

The physical simulation module was used to provide an estimate of the BER performance for a $10\ \mathrm{Gbps}$ optical channel operating at $1550\ \mathrm{nm}$ using an active hub, that is, the configuration depicted in Figure 3 with an EDFA and two 1x128 optical splitters. Simulation steps were as follows: RZ upstream traffic coming from all end users is assumed to arrive at the 128×1 splitter with perfect time synchronisation.The '0'-bit slots contain a small CW optical intensity given by the transitter extinction ratio, assumed to be $16\ \mathrm{dB}$. Each on-line transmitter adds its '0'-bit optical intensity yielding a base power level. Each '1'-bit adds a super-Gaussian ($m = 4$) pulse, duty cycle $1/3$, to the

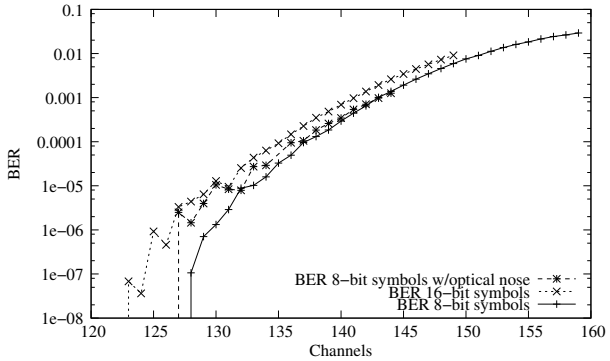


Figure 6. BER of the 10 Gbps channel vs. amount of active end users.

base power level. Upstream and downstream merged traffic suffers from attenuation due to splitter, fiber, and splice losses. The power budget is balanced by an EDFA with 27 dB constant gain. Amplified spontaneous emission from the EDFA is modelled by white Gaussian noise, with intensity proportional to the amplifier noise figure. The input optical signal at the receiver is filtered (2nd order low-pass Butterworth filter, 25 GHz bandwidth) and photodetected assuming a standard PD responsivity (see section 4.4.3 of [1]). White Gaussian noise accounting for thermal and shot noise is then added to the photocurrent, and electrical filtering is applied (2nd order low-pass Butterworth filter, 14 GHz bandwidth).

6.3 Simulation results

As performance varies with symbol length, simulations were performed for 8- and 16-bits lengths. Channel utilization increased in comparison to that provided by the algorithm in [10] by approximately 90% when using the more efficient 16-bit symbol length, and 66% using the simpler 8-bit symbol length as can be appreciated in Figure 5. In any case, it can be appreciated the loss of channel utilisation compared with the theoretical maximum given by Tallini et al. for the Z-channel: $C_Z = \log_2 \left(1 + (1-p)p^{p/(1-p)}\right)$, where p is the probability of error [12]. This penalty is paid as a compromise to gain security and reliability.
In order to predict the BER upon variation of the number of active end users, we performed simulations with and without the effects of the optical channel (Fig. 6). It can be seen that for the optimal parameters, if the number of end users exceeds 128 the BER increases sharply. In comparison with an AES scheme, our system provides additional functionalities like reliability and anonymity.

7 Conclusions

We proposed an enhanced time-hopping CDMA network architecture capable of supporting both point-to-point and point-to-multipoint communication of up to 128 end users. By using a Hamming-weight minimisation algorithm together with an encrypted Bloom filter algorithm we provide confidentiality, reliability, and integrity between two or more end users in an optical channel using a simple error correction stage. By means of numerical simulation we found a gain in the bandwidth utilisation of 90% relative to the scheme presented in [10], increasing total channel bandwidth utilisation to 29%.

References

[1] G. P. Agrawal. *Fiber-Optic Communication Systems*. John Wiley & Sons, New York, USA, second edition, 1997.

[2] B. H. Bloom. Space/time trade-offs in hash coding with allowable errors. *Commun. ACM*, 13(7):422–426, July 1970.

[3] Joan Daemen, Joan Daemen, Joan Daemen, Vincent Rijmen, and Vincent Rijmen. Aes proposal: Rijndael, 1998.

[4] W. Meier and O. Staffelbach. The self-shrinking generator. In A. De Santis, editor, *Advances in Cryptology-EUROCRYPT'94*, pages 205–214. Springer, Berlin, 1994.

[5] Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 1st edition, 1996.

[6] T. K. Moon. *Error Correction Coding: Mathematical Methods and Algorithms*. John Wiley & Sons, New York, USA, 2005.

[7] F. Mosso, J.F. Barrera, M. Tebaldi, N. Bolognini, and R. Torroba. All-optical encrypted movie. *Opt. Express*, 19(6):5706–5712, 2011.

[8] N. Nadarajah, E. Wong, and a. Nirmalathas. Implementation of multiple secure virtual private networks over passive optical networks using electronic CDMA. *IEEE Photonics Technology Letters*, 18(3):484–486, February 2006.

[9] A. A. Ortega, V. A. Bettachini, and J. I. Alvarez-Hamelin. Ecc-chain simulator, http://code.google.com/p/eccchain/, 2008.

[10] A. A. Ortega, V. A. Bettachini, J. I. Alvarez-Hamelin, and D. F. Grosz. Point-to-point and point-to-multipoint cdma access network with enhanced security. In *Access Networks and In-house Communications, OSA Technical Digest (CD), paper ATuB6*, Toronto, Canada, June 2011.

[11] T.H. Shake. Security performance of optical cdma against eavesdropping. *IEEE Journal of Lightwave Technology*, 23:655–670, February 2005.

[12] L. G. Tallini, S. Al-Bassam, and B. Bose. On the capacity and codes for the z-channel. In *Proc. IEEE International Symposium on Information Theory (ISIT'02)*, page 422, Lausanne, Switzerland, June 2002.

[13] P. Torres, L.C.G. Valente, and M.C.R. Carvalho. Security system for optical communication signals with fiber bragg gratings. 50:13–16, January 2002.

[14] Z. Wang, L. Xu, J. Chang, T. Wang, and P. R. Prucnal. Secure optical transmission in a point-to-point link with encrypted cdma codes. *IEEE Photonics Technology Letters*, 22(19):1410 –1412, oct. 2010.