This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the ICC 2008 proceedings.

Design of Reconfigurable Multiweight Wavelength-Time Optical Codes for Secure Multimedia Optical CDMA Networks

Nasaruddin and Tetsuo Tsujioka
Graduate School of Engineering, Osaka City University,
3-3-138, Sugimoto, Sumiyoshi-ku, Osaka 558-8585, Japan
Email: nasa@comm.info.eng.osaka-cu.ac.jp and tsujioka@info.eng.osaka-cu.ac.jp

***Abstract*—Multiweight optical codes are one of the alternative designs for differentiated quality-of-service (QoS) in multimedia optical CDMA (OCDMA) networks. In this paper, we address the design of reconfigurable multiweight wavelength-time optical codes that lead to secure multimedia transmission in OCDMA networks. The proposed multiweight wavelength-time optical codes are constructed based on quasigroups (QGs) for wavelength hopping and one-dimensional multiweight optical orthogonal codes (MWOOCs) for time spreading, then called QG/MWOOCs. Both QGs and MWOOCs are randomly generated by computer search. As a result, the proposed QG/MWOOCs have many different code set groups which differ in both time and wavelengths positions. Furthermore, a secure network is suggested by employing reconfigurable encoders/decoders array waveguide gratings (AWGs)-based, which allow the users to change their codewords patterns to protect against eavesdropping. Finally, the degree of security which may provide by the proposed scheme is analyzed. The results show that the proposed scheme offers both differentiated QoS and differentiated quality-of-security (QoSec) in multimedia OCDMA networks.**

I. Introduction

Recently, there has been renewed interest in optical code division multiple access (OCDMA) system due to its potential for reconfigurability multi-user (codes), privacy and security in transmission, asynchronous access, and ability to support multimedia services [1]. OCDMA system is suited well for access networks, because it is easy to assign channels in the system. Such networks should be able to accommodate more users and to support various types of services including image, data, video and so on. Furthermore, public networks are subject to eavesdropping. In the future, a combination of secure transmission and large bandwidth availability in fiber optic for various OCDMA applications is becoming an issue of great importance. Several works have examined the degree and types of security which may be provided by OCDMA systems [1]–[3], [8]. Although OCDMA can provide a very large code space for secure communications, it may not provide a high degree of data of confidentiality (DOC).

As a core of an OCDMA system, various different types of optical codes have been proposed and studied for various OCDMA technologies: one-dimensional (1D) codes which spread in time [4]–[6] or in frequency [7] and two-dimensional (2D) codes which spread in both time and wavelength [8]–[13]. The 2D codes can provide more flexible and greater capacity than 1D codes, but insufficient for good DOC [1], [2]. Moreover, multilength and/or multiweight codes were introduced for supporting multimedia applications in 1D OCDMA systems [4]–[7]. For 2D OCDMA system, double-weight signatures pattern codes were proposed with autocorrelation constraint being relaxed in order to improve the code cardinality [11], [12]. Varying code weight is one way to ensure quality-of-service (QoS) of critical services. However, those 1D or 2D codes were well-defined coding structures that produced a fixed code set with relative simple elements among codewords (e.g., prime sequences and algebraically structures). They can be easily observed by an eavesdropper. Recent analyses of OCDMA security solutions reported that code reconfiguration is becoming one of technological challenges involving the secure OCDMA system [1]–[3], [13]. Therefore, novel reconfigurable code schemes are required for a greater security in today's real-time and multimedia applications.

This paper investigates a novel scheme for providing secure multimedia OCDMA networks based on reconfigurable multiweight wavelength-time (W-T) optical codes. A multiweight W-T optical code is a collection of binary (0, 1) matrices with the same code length but may have different code weights, where the total number of "1s" gives the code weight and also defines the number of wavelengths with their corresponding time spreading positions. The proposed multiweight W-T optical codes are constructed by using quasigroups (QGs) for wavelength hopping and 1D multiweight optical orthogonal codes (MWOOCs) for time spreading, then called QG/MWOOCs. For good randomness of codes, random method is chosen for generating both QGs and MWOOCs, where set of QGs and code set for MWOOCs are randomly generated by computer search. This is to ensure that an eavesdropper could not improve its interception performance by making use of the code structure in the interception process. As a result, the proposed QG/MWOOCs have many different code set groups which differ in both time and wavelength positions for given code parameters for code reconfiguration. Therefore, the DOC can be increased by frequently allowing changes codeword *patterns* for every user in the network. The bit error probability of the proposed codes is also analyzed numerically. It shows that the proposed codes could provide differentiated QoS. To realize the proposed coding scheme,

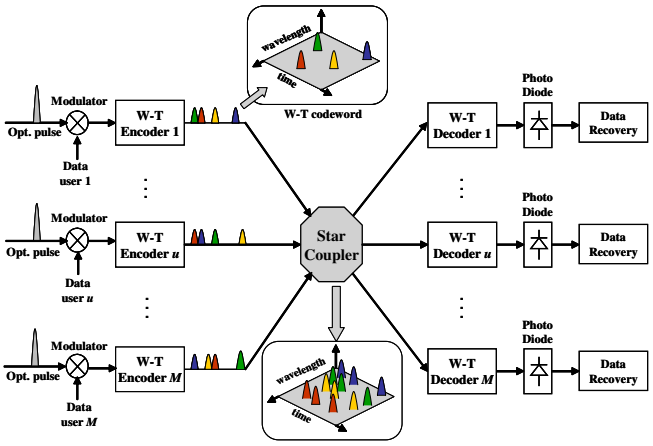

Fig. 1. A typical wavelength-time OCDMA network.

a flexible encoder/decoder (endec) is constructed by adding switches and programmable controller units into array waveguide grating (AWG)-based OCDMA endec. Then, a secure multimedia network is obtained in which codeword patterns are changed to protect the network from eavesdropping. Finally, the probability of breaking a certain codeword in the proposed scheme is studied theoretically. The result shows that the proposed scheme can decrease the probability of blocking a certain codeword by allowing the network to use several different codewords patterns to provide multi-level security in a secure multimedia OCDMA network.

The rest of the paper is organized as follows. A wavelength-time OCDMA system is presented in Section II. In Section III, random algorithms for designing reconfigurable QG/MWOOCs, cardinality, and their performance are discussed. A secure network and security analysis are presented in Section IV. Finally, we conclude with a brief summary of results.

II. Wavelength-Time OCDMA System

Figure 1 shows a typical W-T OCDMA network. There are M users in the network where any pair of transmitter and receiver wants to send data through a star coupler. Every user is assigned with a matrix (0, 1) codeword from a code set of W-T codes. At transmitter side, the laser source produces very short optical pulses which are encoded by using an optical encoder. W-T endec is used tunable delay lines and tunable-filters as in [8]. However, AWGs with delay lines in [9] is a more practical alternative for W-T endecs. Then data at active transmitters using an ON-OFF keying (OOK) optical modulation (OM) are first encoded with the desired matrix codeword. After encoding and modulating processes, active transmitters are superimposing their transmissions through the star coupler and are then distributed to each receiver. At receiver side, the decoder is matched the desired matrix codeword. The output of photo detector is fed to a threshold detector for data recovery. Such a system should be able to support multimedia services which require different performance, different QoS, and different power.

III. Proposed Reconfigurable Code Design

The concept of reconfigurable QG/MWOOCs design is first generating g different sets of a QG of order m and g different code sets of an MWOOC, then constructing matrices that contain either nothing or one pulse in time slot by permutation of wavelengths which are provided by g sets of a QG onto the nonzero time slots of the codewords of an MWOOC.

Definition 1: An MWOOC, C_{MWOOC}, is a collection of binary (0, 1) sequences with the same code length but different code weights in a code set, generally, denoted by (n, W, λ, Q) where n, W, λ, and Q are the code length, a set of code weights $W = \{w_1, \ldots, w_L\}$, maximum correlation value, and a set of fraction of codewords $Q = \{q_1, \ldots, q_L\}$, respectively, where L is the number of different code weights.

Definition 2: A QG/MWOOC, C, is characterized by the tuple $(m \times n_{\mathrm{MWOOC}}, W, \lambda, Q)$ matrices consisting of "0s" and "1s", where m denotes the number of available wavelengths. The maximum correlation value for the proposed QG/MWOOCs is according to the correlation value of MWOOCs that is bounded by one.

A. Quasigroups Generation

A QG is a set of elements with one binary operation whose multiplication table or Cayley table forms a Latin square. It has unique solutions, where each element will appear exactly once in each row and exactly once in each column of Cayley table. Each row and each column are a permutation of m elements. Then the structure of the Cayley table forms an $m \times m$ Latin square because it is made up of m distinct elements. Furthermore, the QGs have also been shown as an alternative for generating 2D optical codes [13] and are more flexible than prime sequences in [8], [10] in terms of the number of available wavelengths because the order number of QGs is applicable for any positive integer.

The random search algorithm for generating QGs is modified from [14].

1) Choose positive integer of order m.
2) Define number of different sets, g, for a QG of order m.
3) Obtain an $m \times m$ set of $\mathrm{S}[m \times m] = (h_{ir})$.
4) Assign a random integer $h \in \{0, 1, \ldots, m-1\}$ to $h_{i0}, h_{i1}, \ldots, h_{i(m-1)}$ for $i = 0, \ldots, m-1$.
5) Repeat step 3) until no pair of entries in the same column of $\mathrm{S}[m \times m]$ is equal.
6) Repeat step 2) and change random seed until g different sets are generated.

The algorithm has been simulated by using a computer. For example, two different sets of QGs of order 8 and 5 can be found in Table II and Fig. 2, respectively.

B. One-Dimensional MWOOCs Generation

The random search algorithm for generating and reconfiguring MWOOCs can be described as follows.

1) Choose positive integers of $W = \{w_1, w_2, \ldots, w_L\}$ and $|C_{\mathrm{MWOOC}}| = \{|C_{\mathrm{MWOOC},w_1}|, |C_{\mathrm{MWOOC},w_2}|, \ldots, |C_{\mathrm{MWOOC},w_L}|\}$ for L different code weights.

TABLE I
EXAMPLES OF TWO AND THREE DIFFERENT WEIGHTS OF MWOOCS WITH TWO DIFFERENT CODE SET GROUPS.

Code $(n_{\mathrm{MWOOC}}, W)_s$	Code set group	
	$s=1$	$s=2$
(9, {3, 2})	(0,5,6) (0,2)	(0,1,4) (0,7)
(41, {6, 3})	(0,1,3,8,14,24) (0,4,19)	(0,4,10,17,26,40) (0,8,20)
(29, {5, 3, 2})	(0,12,14,20,25) (0,7,26) (0,28)	(0,1,3,12,25) (0,15,23) (0,19)
(51, {6, 4, 2})	(0,1,3,7,15,28) (0,11,29,46) (0,10)	(0,4,14,27,48,49) (0,12,31,36) (0,9)

2) The code length n_{MWOOC} must be satisfy

$$n_{\mathrm{MWOOC}} \geq \sum_{l=1}^{L} w_l(w_l-1)q_l|C_{\mathrm{MWOOC}}| + 1. \quad (1)$$

3) Search true random integers of all possible w_l-set by a computer. The w_l-set of "1s" positions for the tth codeword can be represented by

$$(0, b_{1,t_l}, b_{2,t_l}, \ldots, b_{w_l-1,t_l}) \bmod n_{\mathrm{MWOOC}}, \quad (2)$$

where $t_l = 1, \ldots, |C_{\mathrm{MWOOC},w_l}|$, $l = 1, \ldots, L$ and $|C_{\mathrm{MWOOC},w_l}|$ is the number of codewords for code weight w_l. Without loss of generality, we assume all $b_{0,t_l} = 0$.

4) Sort all possible w_l-set codewords and check the used intervals of them as

$$d_{jk,t_l} = b_{k,t_l} - b_{j,t_l} \text{ and } d_{jk,t_l} \neq d_{j'k',t'_l}, \quad (3)$$

for $d_{jk,t_l} \in D_{w_l}$ and $d_{j'k',t'_l} \in D_{w_{l'}}$, where $t_l = 1, 2, \ldots, |C_{\mathrm{MWOOC},w_l}|$, $t'_l = 1, 2, \ldots, |C_{\mathrm{MWOOC},w_{l'}}|$, $j = 0, 1, \ldots, k-1$, $k = 1, 2, \ldots, w_l - 1$, $j' = 0, 1, \ldots, k'-1$ and $k' = 1, 2, \ldots, w_{l'} - 1$. The D_{w_l} is a collection of used intervals by all codewords with weight w_l such that there is no repeated interval within a codeword and among codewords. An analysis of the D_{w_l} and correlation values can be found in [Eqs. (14)–(16), 6].

5) If all constraint parameters are found, stop searching. Otherwise go back to step 3). Changing random seed until g different code sets are generated.

We have simulated the algorithm by using a computer. Several examples of the corresponding codes for $L = 2$ or $W = \{w_1, w_2\}$, $|C_{\mathrm{MWOOC},w_1}| = |C_{\mathrm{MWOOC},w_2}| = 1$, $\lambda = 1$, $Q = \{q_1, q_2\} = \{1/2, 1/2\}$, and for $L = 3$ or $W = \{w_1, w_2, w_3\}$, $|C_{\mathrm{MWOOC},w_1}| = |C_{\mathrm{MWOOC},w_2}| = |C_{\mathrm{MWOOC},w_3}| = 1$, $\lambda = 1$, $Q = \{q_1, q_2, q_3\} = \{1/3, 1/3, 1/3\}$, are shown in Table I, where every code has two different code set groups ($g = 2$). We denote the codes for short by $(n_{\mathrm{MWOOC}}, W)_s$, where $s = 1, \ldots, g$. Using these two- or three-weight of MWOOCs, two- or three-weight of the QG/MWOOCs can be constructed for supporting two- or three-service simultaneously in the networks.

TABLE II
TWO DIFFERENT SETS OF QUASIGROUP OF ORDER 8, WHERE (*) IS UNUSED COLUMN FOR CONSTRUCTING QG/MWOOCS.

QG_1							(*)	QG_2							(*)
6	4	5	0	7	1	2	~~3~~	3	5	2	7	6	4	0	~~1~~
3	1	0	5	2	4	7	~~6~~	1	7	0	5	4	6	2	~~3~~
1	3	2	7	0	6	5	~~4~~	2	4	3	6	7	5	1	~~0~~
4	6	7	2	5	3	0	~~1~~	4	2	5	0	1	3	7	~~6~~
7	5	4	1	6	0	3	~~2~~	5	3	4	1	0	2	6	~~7~~
0	2	3	6	1	7	4	~~5~~	0	6	1	4	5	7	3	~~2~~
5	7	6	3	4	2	1	~~0~~	7	1	6	3	2	0	4	~~5~~
2	0	1	4	3	5	6	~~7~~	6	0	7	2	3	1	5	~~4~~

$\longleftarrow w_1 \longrightarrow$

$\leftarrow w_L \rightarrow$

C. Reconfigurable QG/MWOOCs Construction

The algorithm for reconfigurable QG/MWOOCs can be described as follows.

1) Generate g sets of a QG of order m for wavelength hopping, where the last column in each set is omitted such that there is no repeated pair of integers between rows for correlation of one, as shown in Table II.
2) Using the generated MWOOCs for time spreading, then QG/MWOOCs are constructed by permutation of w_l elements (wavelengths) in each set of QGs onto the "1s" positions of the codewords of MWOOCs, where $w_l \leq m$ and $l = 1, \ldots, L$. A QG$_s$/MWOOC, C, can be obtained with two patterns: time spreading $C_{0,l}$ and wavelength hopping $C_{1,l}$.
3) For reconfigurable code, the other code set groups of QG$_{s'}$/MWOOC can be obtained by using the different set of a QG$_{s'}$ with the same order m and different code set group of MWOOC$_{s'}$, for $s' \neq s$, then repeat step 2).

Example : Let two sets of QG of order 5 as shown in Fig. 2 are used to construct and reconfigure QG/MWOOCs. Suppose QG_1 and a $(9, \{3, 2\})_1$ MWOOC in Table I are used to construct the first code set group QG_1/MWOOC, where the $(9, \{3, 2\})_1$ MWOOC has two codewords with w_l-set notations; $\{(0, 5, 6), (0, 2)\}$ and binary notations; $\{(100001100), (101000000)\}$. Now, each row of QG_1 is used as a seed for a part of new matrices, but the last column in each of QG (*) is omitted in the permutation to preserve the correlation of one. For $w_1 = 3$, the first three elements in each row are used in the permutations as shown in Fig. 2 (a), then do the same way for $w_2 = 2$. The first code set group for a $(5 \times 9, \{3, 2\}, 1, \{1/2, 1/2\})$ QG_1/MWOOC is constructed as shown in Table III. By doing so for QG_2 and using the $(9, \{3, 2\})_2$ MWOOC as shown in Fig. 2 (b), the second code set group for the $(5 \times 9, \{3, 2\}, 1, \{1/2, 1/2\})$ QG_2/MWOOC is obtained, where both code set groups are different in both time and wavelength positions as shown in Fig. 2.

D. Cardinality

The cardinality of 1D MWOOCs is given by

$$|C_{\mathrm{MWOOC}}| \leq \frac{n_{\mathrm{MWOOC}} - 1}{\sum_{l=1}^{L} q_l w_l (w_l - 1)}. \quad (4)$$

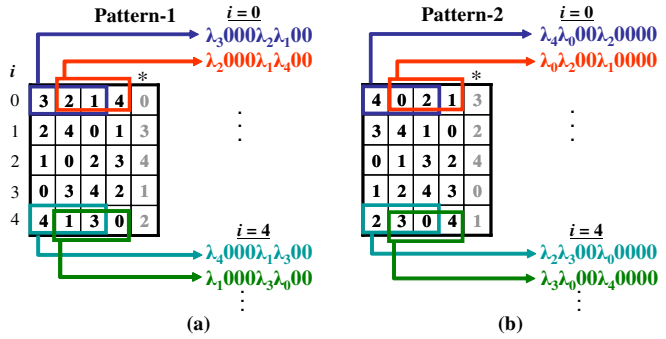

Fig. 2. An illustration of the QG_s/MWOOC construction (a) QG_1 and MWOOC codeword:100001100 (b) QG_2 and MWOOC codeword:110010000.

TABLE III
A $(5 \times 9, \{3,2\}, 1, \{25/50, 25/50\})$ QG_1/MWOOC WITH 1D MWOOC CODEWORDS: (100001100) AND (101000000).

Weight w_l	$C_{0,l}$	$C_{1,l}$		
		$i=0$	...	$i=4$
$l=1$ $w_1=3$	$\lambda_0 0000 \lambda_0 \lambda_0 00$	$\lambda_3 0000 \lambda_2 \lambda_1 00$	...	$\lambda_4 0000 \lambda_1 \lambda_3 00$
	$\lambda_1 0000 \lambda_1 \lambda_1 00$	$\lambda_2 0000 \lambda_1 \lambda_4 00$	...	$\lambda_1 0000 \lambda_3 \lambda_0 00$
	$\lambda_2 0000 \lambda_2 \lambda_2 00$	$\lambda_1 0000 \lambda_4 \lambda_3 00$	...	$\lambda_3 0000 \lambda_0 \lambda_4 00$
	$\lambda_3 0000 \lambda_3 \lambda_3 00$	$\lambda_4 0000 \lambda_3 \lambda_2 00$	...	$\lambda_0 0000 \lambda_4 \lambda_1 00$
	$\lambda_4 0000 \lambda_4 \lambda_4 00$			
$l=2$ $w_2=2$	$\lambda_0 0 \lambda_0 000000$	$\lambda_3 0 \lambda_2 000000$	...	$\lambda_4 0 \lambda_1 000000$
	$\lambda_1 0 \lambda_1 000000$	$\lambda_2 0 \lambda_1 000000$	...	$\lambda_1 0 \lambda_3 000000$
	$\lambda_2 0 \lambda_2 000000$	$\lambda_1 0 \lambda_4 000000$	...	$\lambda_3 0 \lambda_0 000000$
	$\lambda_3 0 \lambda_3 000000$	$\lambda_4 0 \lambda_3 000000$	...	$\lambda_0 0 \lambda_4 000000$
	$\lambda_4 0 \lambda_4 000000$			

While the cardinality for a QG/MWOOC, $|C|$, is composed by the cardinality of time spreading pattern, $|C_0|$, and the cardinalty of wavelength hopping pattern, $|C_1|$, which are given by

$$|C_0| = m|C_{\text{MWOOC}}| \le m\frac{n_{\text{MWOOC}}-1}{\sum_{l=1}^{L} q_l w_l(w_l-1)}, \tag{5}$$

$$\begin{aligned} |C_1| &= m(m-1)|C_{\text{MWOOC}}| \\ &\le \frac{m(m-1)(n_{\text{MWOOC}}-1)}{\sum_{l=1}^{L} q_l w_l(w_l-1)}, \text{ and} \end{aligned} \tag{6}$$

$$|C| = |C_0| + |C_1| \le \frac{m^2(n_{\text{MWOOC}}-1)}{\sum_{l=1}^{L} q_l w_l(w_l-1)}. \tag{7}$$

E. Bit Error Probability

Performance of an OCDMA system is primarily affected by multiple access inteference (MAI) from the other users. Here, we consider only MAI from the other users as a main factor to degrade system performance. Suppose there are $M = \{M_{w_1}, \ldots, M_{w_L}\}$ users with L different services in a network. A user with weight w_1 could be interfered by the other users with weights of $W = \{w_1, \ldots, w_L\}$ at one hit. Without considering any noise and hard-limiter, the bit error probability for a user with weight w_l of the proposed

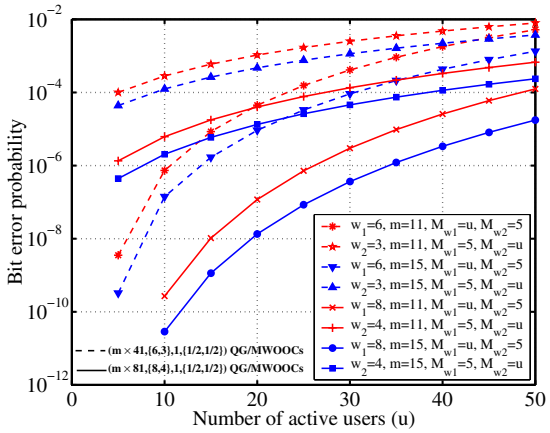

Fig. 3. Bit error probability versus the number of active users for $(m \times 41, \{6,3\}, 1, \{1/2, 1/2\})$ QG/MWOOCs (dashed lines) and $(m \times 81, \{8,4\}, 1, \{1/2, 1/2\})$ QG/MWOOCs (solid lines) with $m = 11$ (red color) and $m = 15$ (blue color).

QG/MWOOCs is given by

$$\begin{aligned} P_{\text{E}}, w_l &= \frac{1}{2} - \frac{1}{2} \sum_{I_1+I_2+\ldots+I_L=0}^{w_l-1} \left\{ \frac{(M_{w_l}-1)!}{I_l!(M_{w_l}-1-I_l)!} \right. \\ &\quad \cdot (p_{l,l})^{I_l} (1-p_{l,l})^{M_{w_l}-1-I_l} \\ &\quad \cdot \prod_{\substack{l'=1 \\ l' \ne l}}^{L} \frac{M_{w_{l'}}!}{I_{l'}!(M_{w_{l'}}-I_{l'})!} \\ &\quad \left. \cdot (p_{l,l'})^{I_{l'}} (1-p_{l,l'})^{M_{w_{l'}}-I_{l'}} \right\}, \end{aligned} \tag{8}$$

where I_l is the number of the interferers with matrices of weight w_l and $p_{l,l'}$ is the average number of "hits" between matrix of weight w_l and matrix of $w_{l'}$ from QG/MWOOCs. The average probability $p_{l,l'}$ is modified from [10] as

$$p_{l,l'} = \frac{1}{m} q_{0,l,l'} + \frac{m-1}{m} q_{1,l,l'}, \tag{9}$$

where $q_{0,l,l'}$ and $q_{1,l,l'}$ are the probability of getting one hit between the desired matrix codeword originated from C_0 and C_1, respectively, and can be obtained as

$$q_{0,l,l'} = \frac{w_l w_{l'}(|C_{\text{MWOOC}}|m-1)}{2n_{\text{MWOOC}}(|C|-1)}, \tag{10}$$

and

$$q_{1,l,l'} = \frac{w_l w_{l'}(|C_{\text{MWOOC}}|m-1) + (w_{l'}-1)^2}{2n_{\text{MWOOC}}(|C|-1)}, \tag{11}$$

respectively. The decision threshold for users is set to the code weight w_l for optimal operation.

Bit error probability of the double-weight QG/MWOOCs by employing $(41, \{6,3\})$ MWOOC in Table I and $(81, \{8,4\})$ MWOOC with one of code set groups of $\{(0,2,6,13,21,31,45,61), (0,9,12,46)\}$ for $m = 11$ and 15, repectively, is evaluated by using (8). The bit error probability versus number of active users is plotted in Fig. 3. In the figure, we varied the number of active users with w_l, $M_{w_l} = m$,

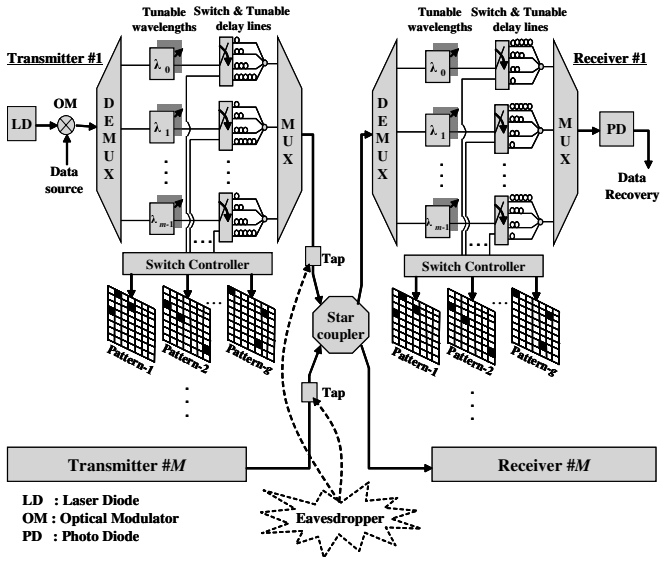

Fig. 4. Proposed secure wavelength-time OCDMA network.

and fixed $M_{w_l} = 5$ users. The performance worsens as the number of active users increases. Users with large code weight always perform better than those with smaller code weight. This implies that the differentiation bit error performance is mainly dependent on the code weight. In addition, the bit error probability is improved when n_{MWOOC}, W or m increases. Therefore, the proposed codes enable a network to support different QoS requirements for multimedia applications.

IV. Security Analysis

A. Proposed Secure OCDMA Network

To enhance security at the physical level of multimedia OCDMA networks, changing the user's codewords is a major approach to protect the eavesdropper [1]–[3]. We here propose a secure W-T OCDMA network based on reconfigurable endecs as shown in Fig. 4. Each encoder is composed of an AWG demultiplexing (demux), tunable wavelength filters, switches and tunable delay lines which are controlled by a programmable switch controller, and an AWG multiplexing (mux). The g patterns of a user's codeword will store in the controller's memory. The encoding is performed by the links from the demultiplexing to the multiplexing. Each delay line has a unique configuration according to g groups of an MWOOC in time spreading. The switch controller will also arrange the wavelengths (by "on" or "off" switch) to appear at corresponding time-slot according to the assigned matrix codeword. So it can support multiweight or different number of wavelengths for the user's codewords in the network. The decoder is similar to the encoder where it is required to re-arrange the wavelengths and time spreading in reverse order. If the users' code can change rapidly at different patterns, the eavesdropper's ability to break data confidentiality could be very limited. Note that a synchronous control mechanism is required when codeword patterns are changed, so that there is no data loss or no degradation of the system.

Let two code set groups of $(5\times 9, \{3,2\}, 1, \{25/50, 25/50\})$ QG/MWOOC in the example are used in the network. A user may have two different patterns of codewords, where he can change the codeword patterns twice in the network against eavesdropping. For example, two codeword patterns for a user with weight $w_1 = 3$ are $(\lambda_3 0000 \lambda_2 \lambda_1 00)_1$ and $(\lambda_4 \lambda_0 00 \lambda_2 0000)_2$ from pattern 1 and 2, respectively, as shown in Fig. 2. While two codeword patterns for a user with weight $w_2 = 2$ are $(\lambda_3 0 \lambda_2 000000)_1$ and $(\lambda_4 000000 \lambda_0 0)_2$ from pattern 1 and 2, respectively. Although the eavesdropper may tap a coded transmission of a particular user to derive the transmitter's codeword as shown in Fig. 4, he would not improve its interception performance by making use of the proposed coding structure.

In the conventional 2D coding schemes, the number of possible codewords generated is $|C|$ with a fixed code set for given code parameters. An eavesdropper would have to guess *only* on the $|C|$ patterns in order to tune in on any given transmission. On the other hand, the proposed scheme is designed for a *much larger* of possible matrices patterns and the ability to dynamically change the codewords, which makes eavesdropping practically impossible in a brute force attack. Suppose g patterns for a user's codeword and $|C|$ active users are employed in the network, an eavesdropper will observe $g|C|$ patterns of codewords. Then the number of patterns that can be arranged in the network, U, is obtained by the hypergeometric distribution [3]

$$U = \frac{(|C|g)!}{g!^{|C|}}. \tag{12}$$

A short code with two different code sets of $(5 \times 9, \{3,2\}, 1, \{25/50, 25/50\})$ QG/MWOOC with $g = 2$ and $|C| = 50$ gives a very large value of $U \approx 8.2 \times 10^{142}$.

B. Probability of Breaking a Codeword

Basically secure system should be based solely on the fact that particular one or more codewords being used by a user are unknown to the eavesdropper. This is well known as *Kerckhoffs' principle*, where the eavesdropper may know everything about the system except particular codeword that each user employs. So the security enhancement in this paper is to make eavesdropping difficult to capture the used codeword by a user. In the proposed coding, there are m available wavelengths, multiweight $W = \{w_1, \ldots, w_l, \ldots, w_L\}$, and g different patterns of code sets, where $m \geq w_l$. The probability of breaking a certain codeword is the probability of choosing a proper hopping pattern times the probability of having the right spreading pattern [8] and is given by

$$P_{\text{break conv},l} = \frac{(m-w_l)!}{m!} \times \frac{1}{w_l}, \tag{13}$$

for $l = 1, \ldots, L$. Now, observing that g different patterns of codeword for each user are independent, the probability of breaking all patterns of a certain user's codeword in the proposed scheme can be written as

$$P^g_{\text{break prop},l} = \left\{ \frac{(m-w_l)!}{m!} \times \frac{1}{w_l} \right\}^g. \tag{14}$$

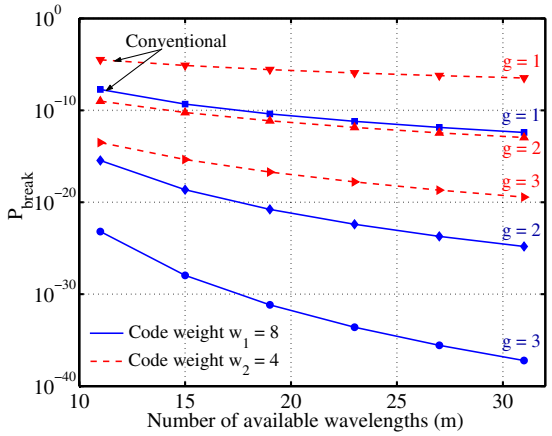

Fig. 5. Probability of breaking a codeword versus the number of available wavelengths for double-weight QG/MWOOCs ($w_1 = 8$ and $w_2 = 4$) with different number of code set patterns.

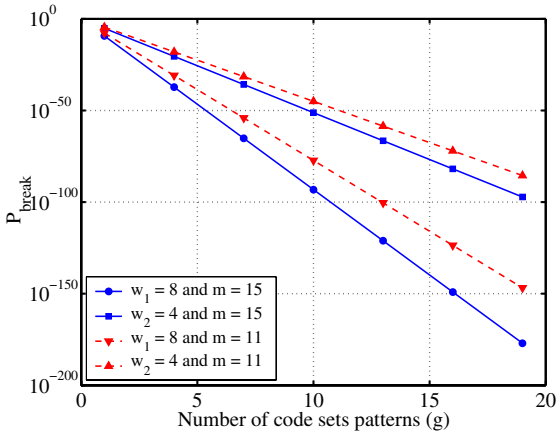

Fig. 6. Probability of breaking a codeword versus the number of different code set patterns for double-weight QG/MWOOCs ($w_1 = 8$ and $w_2 = 4$) with $m = 11$ and 15.

Figure 5 shows the probability of breaking a certain codeword versus the number of available wavelengths (m) for double-weight QG/MWOOCs ($w_1 = 8$ and $w_2 = 4$) with $g = 1$, 2 and 3, respectively. The probability of breaking a codeword decreases as m, W or g increases. Furthermore, the proposed scheme can increase some degree of DOC compared to the conventional scheme with a fixed code set ($g = 1$). In Fig. 6, the probability of breaking a codeword versus the number of different code sets for double-weight QG/MWOOCs ($w_1 = 8$ and $w_2 = 4$) is plotted for $m = 11$ and 15, where the probability of breaking a codeword decreases as g increases. If a QG of order m can provide all possible of $g_{\max} = \prod_{k=1}^{m} k!$ different sets, they can be used for a long time to change the codeword patterns in the network. Moreover, from Figs. 4 and 5, P_{break} for larger code weight performs lower than that for smaller code weight. Therefore, the proposed scheme has features that can provide differentiated QoS and differentiated quality-of-security (QoSec).

V. Conclusion

A novel scheme for secure multimedia OCDMA networks based on reconfigurable multiweight wavelength-time optical codes has proposed in this paper. Random search algorithms for designing reconfigurable QG/MWOOCs have been described in detail. The proposed QG/MWOOCs can provide many different code set groups for given code parameters. Furthermore, the proposed codes enable a network to support different QoS because the performance is mainly dependent on the code weight. To enhance data of confidentiality, a secure wavelength-time OCDMA network has been suggested by employing the proposed coding scheme and reconfigurable AWGs-based encoders/decoders, where each user is assigned with several patterns of codeword. The degree of security of the proposed scheme has been analyzed theoretically. The results have shown that the proposed scheme could provide a very large codeword patterns and different confidentiality of services which depend on the selected numbers of available wavelengths, code weights, and code set groups. Therefore, the proposed scheme can provide not only multi-level QoS, but also multi-level QoSec in multimedia OCDMA networks.

Acknowledgement

This work was partly supported by the ICOM Electronics Communication Engineering Promotion Foundation, Japan.

References

[1] P. R. Prucnal, *Optical code division multiple access: Fundamentals and applications*, Boca Raton: Taylor & Francis, 2006.

[2] T. H. Shake, "Security performance of optical CDMA against eavesdropping," *J. Lightw. Technol.*, vol. 23, no. 2, pp. 655–670, Feb. 2005.

[3] J. M. Castro, I. B. Djordjevic, and D. F. Geraghty, "Novel super structured Bragg gratings for optical encryption," *J. Lightw. Technol.*, vol. 24, no. 4, pp. 1875–1885, Apr. 2006.

[4] G. C. Yang, "Variable-weight optical orthogonal codes for CDMA network with multiple performance requirements," *IEEE Trans. Commun.*, vol. 44, no. 1, pp. 47–55, Jan. 1996.

[5] I. B. Djordjevic, B. Vasic and J. Rorison, "Design of multiweight unipolar codes for multimedia optical CDMA applications based on pairwise balanced designs," *J. Lightw. Technol.*, vol. 21, no. 9, pp. 1850–1856, Sep. 2003.

[6] Nasaruddin and T. Tsujioka, "Multiple-length variable-weight optical orthogonal codes for supporting multirate multimedia services in optical CDMA networks," *IEICE Trans. Commun.*, vol. E90-B, no. 8, pp.1968–1978, Aug. 2007.

[7] E. Inaty, H. M. H. Shalaby, P. Fortier, and L. A. Rusch, "Multirate optical fast frequency hopping CDMA system using power control," *J. Lightw. Technol.*, vol. 20, no. 2, pp. 166–177, Feb. 2002.

[8] L. Tancevski and I. Andovic, "Hybrid wavelength hopping/time spreading schemes for use in massive optical networks with increased security," *J. Lightw. Technol.*, vol. 14, no. 12, pp. 2636–2647, Dec. 1996.

[9] K. Yu, J. Shin, and N. Park, "Wavelength-time spreading optical CDMA systems using wavelength multiplexers and mirrorred fiber delay line," *IEEE Photon. Technol. Lett.*, vol. 12, no. 9, pp. 1278–1280, Sep. 2000.

[10] W. C. Kwong, G. C. Yang, V. Baby, C. -S. Bres, and P. R. Prucnal, "Multiple-wavelength optical orthogonal codes under prime-sequence permutations for optical CDMA," *IEEE Trans. Commun.*, vol. 53, no. 1, pp. 117–123, Jan. 2005.

[11] W. C. Kwong and G. C. Yang, "Image transmission in multicore-fiber code-division multiple-access Networks," *IEEE Commun. Lett.*, vol. 2, no. 10, pp. 285–287, Oct. 1998.

[12] —, "Double-weight signature pattern codes for multicore-fiber code-division multiple-access Networks," *IEEE Commun. Lett.*, vol. 5, no. 5, pp. 203–205, May. 2001.

[13] Nasaruddin, T. Tsujioka and S. Hara, "A code reconfiguration design for two dimensional OCDMA system to enhance security," in *Proc. IEEE WOCN 2007*, Singapore, Jul. 2007.

[14] R. Bartak, "On generators of random quasigroup problem," *Proc. of ERCIM*, pp. 264–278, Uppsala, Sweden, 2005.