Quadratic-Congruence Carrier-Hopping Prime Code for Multicode-Keying Optical CDMA

Wing C. Kwong, Cheng-Yuan Chang†, Hung-Ta Chen†, and Guu-Chang Yang†

Department of Engineering, Hofstra University, Hempstead, NY 11549, USA
†Department of Electrical Engineering, National Chung-Hsing University, Taichung 402, Taiwan

Abstract—In this paper, we study a new family of carrier-hopping prime codes (CHPCs), so-called quadratic-congruence CHPC (QC-CHPC), with expanded code cardinality by relaxing the maximum cross-correlation function to two (i.e., λc = 2). An application of the new code is for multicode keying in wavelength-time optical code-division multiple access (O-CDMA), in which each user is assigned $M = 2^m$ code matrices to represent $m$ data bits per symbol. The advantages are that 1) a lower baud multicode-keying O-CDMA system can support a higher bit rate and 2) user’s code obscurity is enhanced, as compared to the transmission of one code matrix (per user) for each data bit one in conventional “on-off keying” O-CDMA systems. Our performance analysis shows that there is a trade-off between the code performance and hardware complexity/speed related to the choice of $M$, for a given bit rate.

I. INTRODUCTION

Optical code-division multiple access (O-CDMA) recently receives renewed attention because of the advance of the wavelength-division multiple-access spreading (or simply wavelength-time) coding techniques [1]–[3]. On-off keying (OOK) is traditionally used, of which each user was assigned one distinct code matrix and only data bit ones were transmitted with the code matrix. Recently, the use of multicode keying in wavelength-time O-CDMA was studied [4], [5], in which each user was allocated with $M = 2^m$ code matrices to represent $m$ data bits per symbol. The advantages are two-folded: 1) the data rate is increased by a factor of $m$ of the “baud” and 2) user’s code obscurity is improved because data bit zeros are also transmitted in code matrices and eavesdroppers cannot determine the transmission of bit zeros or ones by simply detecting the absence or presence of energy at the downlink fiber, as opposed to the conventional OOK O-CDMA [6]. Multicode keying requires an $M$-fold increase in code matrices with good auto-correlation and cross-correlation properties. However, the study of wavelength-time codes was mostly focused on constructing code matrices with cross-correlation values of at most one (i.e., $\lambda_c = 1$) in order to minimize the amount of multiple-access interference (MAI). As a result, the code cardinality is rather restricted. On the other hand, it is known that a larger cardinality can be achieved by relaxing $\lambda_c$ at the expense of code performance [7], [8].

In this paper, we first construct a new family of carrier-hopping prime codes (CHPCs), so-called quadratic-congruence CHPC (QC-CHPC) [5], in Section II. To support multicode keying, the code has the cross-correlation function of at most two (i.e., $\lambda_c = 2$) and, thus, expanded code cardinality. The multicode-keying O-CDMA scheme [4], [5] does not need network synchronization because the code is designed with “aperiodic” cross-correlation properties. We only need the transmitter and the receiver that are communicating to synchronize, which is the same requirement as in the conventional OOK O-CDMA anyway. In Section III, the performance of the $\lambda_c = 2$ QC-CHPC in OOK and multicode-keying O-CDMA is analyzed. Our results show that there is a trade-off between the code performance and hardware complexity/speed related to the choice of $M$, for a given bit rate. To improve code performance and enhance user’s code obscurity, the numbers of decoders increases linearly with $M$. On the other hand, the required hardware speed can be reduced by a factor of $m$. For example, we can use 2.5-GHz hardware to support a bit rate of 10 Gbit/s if $M = 16$ is used, but then 16 decoders are required in each user. Multicode keying provides an option of trading hardware speed for hardware complexity. If code obscurity is not important, one should use OOK for hardware simplicity. If code performance is more important, one should use as large $M$ as possible.

II. QUADRATIC-CONGRUENCE CARRIER-HOPPING PRIME CODE

Here we define the $(L \times N, w, \lambda_\alpha, \lambda_c, \lambda_\tau)$ QC-CHPC, $\mathcal{C}$, as a collection of binary $(0,1)$ $L \times N$ matrices, each of Hamming weight $w$, such that

- **Autocorrelation.** For any matrix $x \in \mathcal{C}$ and integer $\tau \in [1, N-1]$, the binary discrete 2-D autocorrelation sidelobe of $x$ is no greater than a nonnegative integer $\lambda_a$, such that $\sum_{i=0}^{L-1} \sum_{j=0}^{N-1} x_{i,j} x_{i,j+\tau} \leq \lambda_a$, where $x_{i,j} \in \{0,1\}$ is an element of $x$ at the $i$th row and $j$th column, and “$\oplus$” denotes a modulo-$N$ addition.

- **Intersymbol cross correlation.** For any two distinct matrices $x \in \mathcal{C}$ and $y \in \mathcal{C}$ from two different code subsets and integer $\tau \in [0, N-1]$, the binary discrete 2-D cross-correlation function of $x$ and $y$ is no greater than a positive integer $\lambda_c$, such that $\sum_{i=0}^{L-1} \sum_{j=0}^{N-1} x_{i,j} y_{i,j+\tau} \leq \lambda_c$, where $y_{i,j} \in \{0,1\}$ is an element of $y$ at the $i$th row and $j$th column.
• **Intrasymbol cross correlation.** For any two distinct matrices $x \in C$ and $x' \in C$ from the same code subset, the binary discrete 2-D cross-correlation function of $x$ and $x'$ is no greater than a positive integer $\lambda'$, such that $\sum_{j=0}^{L-1} \sum_{i=0}^{N-1} x_{i,j} x'_{i,j} \leq \lambda'$, where $x'_{i,j} = \{0,1\}$ is an element of $x'$ at the $i$th row and $j$th column.

Given a positive integer $k$ and a set of prime numbers \{p_1, p_2, ..., p_k\}, such that $p_k \geq p_{k-1} \geq \cdots \geq p_3 \geq p_2 \geq p_1 \geq w$, matrices $x_{i_1,i_2,\ldots,i_k}$, with the ordered pairs

$$
[(0,0), (1,1) \oplus p_1, i_1 + (1 \odot p_2, i_2)p_1 + \cdots + (1 \odot p_k, i_k)p_1p_2 \cdots p_{k-1}], (2,2 \odot p_1, i_1)
$$

and

$$
[(0,0), (1,1) \odot p_1, i_1 + (1 \odot p_2, i_2)p_1 + \cdots + (1 \odot p_k, i_k)p_1p_2 \cdots p_{k-1}], \ldots, (w-1, (w-1) \odot p_1, i_1 + ((w-1) \odot p_2, i_2)p_1 + \cdots + ((w-1) \odot p_k, i_k)p_1p_2 \cdots p_{k-1})]
$$

$$
i_1 = \{0,1,\ldots,p_1-1\}, i_2 = \{0,1,\ldots,p_2-1\}, \ldots, i_k = \{0,1,\ldots,p_k-1\}, j = 0
$$

(1)

form the \((w \times N, w, 0, 2, 1)\) QC-CHPC with $p_1N$ matrices of length $N = p_1p_2 \cdots p_k$ and weight $w \leq p_1$, where $\odot p_l$ denotes a modulo-$p_l$ multiplication for $l = \{1, 2, 3, \ldots, k\}$. For ease of representation, every matrix in 2-D codes can equivalently be written as a set of $w$ ordered pairs (i.e., one ordered pair for every binary one), where an ordered pair $(\lambda_v, t_h)$ records the vertical ($v$) and horizontal ($h$) displacements of a binary one from the bottom-leftmost corner of a matrix. In other words, $\lambda_v$ represents the transmitting wavelength and $t_h$ shows the time position of a binary one in the matrix.

It is important to point out that this construction is different from that of [5] and, thus, requires a modification in the performance analysis in Section III.

These $p_1N$ code matrices can be separated into $p_1$ groups of $N$ matrices per group. The autocorrelation sidelobes of any matrices in the code set are always zero. Code matrices coming from different groups (i.e., different $j$ values) have the cross-correlation functions of at most two (i.e., $\lambda_c = 2$). However, code matrices coming from the same group (i.e., the same $j$ value) have the cross-correlation functions of at most one (i.e., $\lambda_c' = 1$).

This group property comes from the fact that the $j = 0$ group of matrices in (1) corresponds to the $N$ original matrices of our $\lambda_c = 1$ CHPC [3, Section 2.6], and that the $j = \{1, 2, \ldots, p_1\}$ groups of matrices in (2) are obtained by inserting the QC operator, $i^2 \cdot j$ (mod $p_1$), in every ordered pairs of (1), where $i \in GF(p_1)$. Since the linear equation in the CHPC is now replaced by the quadratic equation, the maximum cross-correlation function for any two distinct matrices, $x_{i_1,i_2,\ldots,i_k,j}$ and $x'_{i_1',i_2',\ldots,i_k',j'}$, in the \((w \times N, w, 0, 2, 1)\) QC-CHPC is at most two (i.e., $\lambda_c = 2$) if the index $j \neq j'$. For the matrices in the same $j$ group, the cross-correlation functions are at most one (i.e., $\lambda_c' = 1$) from the fact that the cross-correlation functions of the CHPC are at most one [3, Section 2.6]. To see that the autocorrelation sidelobes are always zero, we note that all of the binary ones in each code matrix are in different wavelengths.

Using $k = 1$, $p_1 = N = 5$, and $w = 4$ as an example, this \((4 \times 5, 4, 0, 2, 1)\) QC-CHPC has 5 groups of 5 matrices, $x_{i_1,i}$ (for $i_1 \in [0, 4]$ and $i \in [0, 4]$), as shown in Table I. Matrices with the same $j$ value have $\lambda_c' = 1$, but matrices with different $j$ values have $\lambda_c = 2$. For example, the matrices $x_{0,1} = x_{1,1}, x_{2,1}, x_{3,1}$, and $x_{4,1}$ in the $j = 1$ group, will have at most two hits (per time slot) with $x_{1,0}$, but at most one hit (per time slot) among themselves.

<table>
<thead>
<tr>
<th>Group</th>
<th>Matrices of the ((4 \times 5, 4, 0, 2, 1)) QC-CHPC.</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>{[(0,0), (1,0)], [(0,1), (2,0), (3,0)]}</td>
</tr>
<tr>
<td>1</td>
<td>{[(0,0), (1,1), (2,1), (3,2)], [(0,0), (1,2), (2,3), (3,3)]}</td>
</tr>
<tr>
<td>2</td>
<td>{[(0,0), (1,3), (2,0), (3,1)], [(0,0), (1,4), (2,2), (3,3)]}</td>
</tr>
<tr>
<td>3</td>
<td>{[(0,0), (1,1), (2,3), (3,2)], [(0,0), (1,2), (2,0), (3,3)]}</td>
</tr>
<tr>
<td>4</td>
<td>{[(0,0), (1,4), (2,3), (3,2)], [(0,0), (1,3), (2,0), (3,4)]}</td>
</tr>
</tbody>
</table>

### III. Performance Analysis of the QC-CHPC in Multicode Keying

In general, the code performance in OOK wavelength-time O-CDMA is determined by the cross-correlation functions, which are related to code weight, code length, and the number of available wavelengths [3]. With multicode keying in use, the code performance now depends on the intersymbol cross-correlation functions (i.e., $\lambda_c$) generated by the code matrices of interfering users and the intrasymbol cross-correlation functions (i.e., $\lambda_c'$) generated by self
interference of a user’s own code matrices (i.e., different symbols).

Instead of selecting the code matrices in a group in Section II for multicode keying, we use the following code
selection method for a better performance. Here, we assume
that each user is assigned a set of \( M \) \((\leq p_1)\) frequency-
or time-shifted code matrices obtained from the QC-CHPC
in accordance with the appendix, such that \( \lambda'_i = 1 \) for
minimizing the intrasymbol cross-correlation functions. Our
multicode keying scheme can support up to \( N \) sets (i.e.,
possible users) of \( M \) \((\leq p_1)\) code matrices (i.e., symbols).
\( M \) decoders per user are needed to detect these \( M \)
matri-
ces, corresponding to \( m = \lfloor \log_2 M \rfloor \) bit/symbol, where \( \lfloor . \rfloor \)
is a floor function.

The performance analysis of the QC-CHPC in multicode-
keying wavelength-time O-CDMA is very similar to our
work on wireless multilevel frequency-shift-keying
frequency-hopping CDMA [3]. The hit probabilities are given by

\[
q_{2,0} + q_{2,1} + q_{2,2} = 1 \quad (3)
\]

\[
q_{2,1} + 2q_{2,2} = \frac{w^2}{LN} = \frac{w}{N} \quad (4)
\]

\[
q_{2,2} = \left( \frac{p_1}{2} - (p_1 - w)w - \left( \frac{p_1 - w}{2} \right) \right) \left( \frac{p_1 - 1}{p_1 - 1} \right) \cdot \frac{1}{N} \quad (5)
\]

where \( q_{i,j} \) denotes the probability of getting \( j \) hits in a time
slot out of the maximum cross-correlation function of \( i \), \( w \) is
the code weight, \( L \) is the number of available wavelengths,
\( N = p_1 p_2 \cdots p_k \) is the code length, and \( L = w \) in our QC-
CHPC. Different from OOK, multicode keying does not need
the factor 1/2 on the right sides of both (4) and (5)
because of continuous symbol transmission.

For (5), \( \frac{p_1}{2} \) represents the number of possible delay
combinations among \( p_1 \) binary ones (i.e., pulses) in a code
matrix, \( p_1 - w \) represents the number of possible delay
combinations among \( w \) pulses after \( p_1 - w \) pulses have
been removed, \( \left( \frac{p_1 - w}{2} \right) \) represents the number of possible
delay combinations among the \( p_1 - w \) removed pulses, and
the denominator \( N \) represents the number of code matrices
in the same group. The term \( (p_1 - 1)/p_1 \) \( N/(p_1 - 1) \)
represents the probability of choosing code matrices from
different groups, out of a total of \( p_1 - 1 \) code matrices.
The last term \( 1/N \) represents the number of possible time
shifts in a code matrix of length \( N \).

Given that there are \( K - 1 \) interfering users and each of
them can generate at most two hits in a time slot over one
symbol period, the probability of having a cross-correlation
function of \( v \) appearing at any one of \( M - 1 \) wrong decoders
in the desired user is obtained by [3]

\[
P_r(v) = \binom{w}{v} \sum_{i=0}^{v} (-1)^i \binom{v}{i} q_{2,0} + \frac{q_{2,1}(v - i)}{w}
\]

\[
+ q_{2,2} \left( \frac{v - i(v - i - 1)}{w(w - 1)} \right)^{K-1}
\]

(6)

An decision error occurs if more than one decoders have
the output intensity of at least \( w \). Assume that there are \( t \)
of them. The probability that \( t \) decoders have the output
intensity of at least \( w \) and \( M - 1 - t \) decoders have the
output intensity less than \( w \) can be broken into two cases,
depending on the intrasymbol cross-correlation functions
of the code matrices in group \( j = 0 \) (which gives \( \lambda'_i = 0 \))
and group \( j = \{1, 2, 3, \ldots, p_1 - 1\} \) (which gives \( \lambda'_i = 1 \)).

According to our code-selection method in the appendix,
we need to separate the following analysis into the \( k = 1 \)
and \( k > 1 \) cases in order to minimize the intrasymbol cross-
correlation functions (i.e., \( \lambda'_c \)).

Here, we consider the \( k = 1 \) case. From the appendix, the
intrasymbol cross-correlation functions between any two of
the \( M = p_1 \) code matrices in group \( j = 0 \) are always zero
(i.e., \( \lambda'_c = 0 \)). Therefore, for users assigned code matrices
in group \( j = 0 \), the probability that \( t \) decoders have the
output intensity of at least \( w \) and \( M - 1 - t \) decoders have output intensity less than \( w \) is given by

\[
P_r(w, t) = \left( \frac{M - 1}{t} \right) \left[ P_r(w) \right]^t \sum_{z=0}^{w-1} P_r(z) \chi_{1-t}^{M-1-t} \quad (7)
\]

However, the intrasymbol cross-correlation functions be-
tween any two code matrices in group \( j = \{1, 2, \ldots, p_1 - 1\} \)
are at most one (i.e., \( \lambda'_c = 1 \)). Therefore, for users assigned
code matrices in group \( j = \{1, 2, \ldots, p_1 - 1\} \), the probability that \( t \) decoders have output intensity of at least \( w \) and \( M - 1 - t \) decoders have output intensity less than \( w \) is given by

\[
P'_r(w, t) = \left( \frac{M - 1}{t} \right) \left[ P'_r(w) \right]^t \sum_{z=0}^{w-1} P'_r(z) \chi_{1-t}^{M-1-t} \quad (8)
\]

The term \( P'_r(z) \) is used to account for the maximum in-
trasymbol cross-correlation function of one and is given by
\( (A.1) \) of the appendix.

Since the probability of correctly choosing the desired
decoder is \( 1/(t + 1) \) and there is only one correct symbol
out of \( M \) symbols, the bit error probability is given by [3]

\[
P_e(k=1) = \frac{M}{2(M-1)} \left[ 1 - \frac{p_1 - 1}{p_1} \frac{1}{t+1} \sum_{r=0}^{M-1} \frac{1}{t+1} P_r(w, t) \right]
\]

\[
- \frac{1}{p_1} \sum_{t=0}^{M-1} \frac{1}{t+1} P_r(w, t) \quad (9)
\]

The term \( (p_1 - 1)/p_1 \) accounts for the chances of choosing
the \( M \leq p_1 \) code matrices from group \( j = \{1, 2, \ldots, p_1 - 1\} \)
and the term \( 1/p_1 \) accounts for the chances of choosing the
\( M \leq p_1 \) code matrices from group \( j = 0 \).
Now, we consider the $k > 1$ case. The analysis is very similar to that of the $k = 1$ case, except that the intrasymbol cross-correlation functions all become zero (i.e., $\lambda'_c = 0$). The analysis follows (3)–(7), but the term $P_r(z)$ is now not needed because $\lambda'_c = 0$, as shown in the appendix. Since the probability of choosing the correct decoder is $1/(1 + t)$, the bit error probability is given by

$$P_e(k>1) = \frac{M}{2(M-1)} \left[ 1 - \sum_{t=0}^{M-1} \frac{1}{t+1} P_r(w,t) \right] \quad (10)$$

For comparison, the hard-limiting bit error probability of the $(w \times N, w, 0, 2, 1)$ QC-CHPC in the conventional OOK wavelength-time O-CDMA is given by [9, eq. (16)], such that

$$P_e\text{ OOK} = \frac{1}{2} \sum_{i=0}^{w} (-1)^i \frac{w!}{i!(w-i)!} \left[ q_{2,0} \frac{w}{w-i} + q_{2,1} \frac{(w-i)}{w} \right] + q_{2,2} \frac{(w-i)(w-i-1)}{w(w-1)} K^{-1} \quad (11)$$

In OOK, a factor of $1/2$ is needed on the right sides of both (4) and (5) because data bit ones and zeros are assumed with equal probability and bit zeros are not transmitted.

Figs. 1 and 2 compare the bit error probabilities of the $(w \times N, w, 0, 2, 1)$ QC-CHPC in OOK [i.e., (11)] and multicode-keying [i.e., (9)] wavelength-time O-CDMA, where $w = 7$, $k = 1$, and $M = \{2, 4, 8, 16\}$. Also in Fig. 1, we assume that $p_1 = N = 101 \times \lceil \log_2 M \rceil$ in order to keep the bit rate constant so that the relationship between bit error probability and $M$ can be investigated. We assume $p_1 = N = 317 \times \lceil \log_2 M \rceil$ in Fig. 2 so that the effect of code length to the bit error probability can also be studied when both figures are compared.

In general, the bit error probability improves when $M$ or code length $N$ increases. When $M$ increases, there are more data bits to be decided incorrectly if a symbol detection error occurs. However, the increase in code length (i.e., $N \propto \lceil \log_2 M \rceil$) provides a stronger compensation. The net effect is the improvement of bit error probability as $M$ increases when the data bit rate is kept constant. The bit error probability of the $M = 2$ case is the worst and even worse than that of the OOK case because the amount of MAI in the latter is reduced by half, in average, as data bit zeros are not transmitted. In these numerical examples, it is interest to see that we need to use $M = 8$ in order to catch up with the OOK case in terms of bit error probability.

In summary, our results show that there is a trade-off between the bit error probability and the choice of $M$, for a given data bit rate. To improve bit error probability and enhance user’s code obscurity, the numbers of decoders increases linearly with $M$. On the other hand, the required hardware speed can be reduced by a factor of $m$, as the number of the hardware increases with $M$. For example, we can use 2.5-GHz hardware to support a data bit rate of 10 Gbit/s when $M = 16$ is used, but then 16 decoders per user are needed. In other words, multicode keying provides an option of trading hardware speed for hardware complexity. If code obscurity is not important, one should use OOK for hardware simplicity. If bit error probability is more important, one should use as large $M$ as possible. In our numerical examples, the choice of $M = 8$ provides a good compromise among bit error probability, hardware
complexity/speed, and code obscurity, for a given data bit rate.

IV. Conclusions

In this paper, we studied a new family of the QC-CHPCs with expanded cardinality and the maximum cross-correlation value of two. The performance of the QC-CHPC in multicode-keying wavelength-time O-CDMA was analyzed. Our results showed that there was a trade-off between the code performance and hardware complexity/speed related to the choice of $M$. If code obscurity was not important, one should use OOK, according to our analyses. If code performance was more important, one should use as large $M$ as possible. Multicode-keying O-CDMA also provided an option of trading hardware speed for hardware complexity.

ACKNOWLEDGMENT

This work was supported in part by the U.S. Defense Advance Research Projects Agency under Grant MDA972-03-1-0006, in part by the National Science Council of the Republic of China under Grant NSC 95-2221-E-005-082, and in part by the presidential Research Award and Faculty Development and Research Grants of Hofstra University.

APPENDIX

I. Derivation of $P_r(z)$

As shown in the following, our multicode-keying scheme can support up to $N$ sets (i.e., possible users) of $M (\leq p_1)$ code matrices (i.e., symbols), and, at the same time, can minimize the intrasymbol cross-correlation functions. It is done by applying frequency- or time-shifts of the code matrices of the QC-CHPC in Section II.

First, we consider the $k = 1$ case. We assign code matrices for multicode keying depending on whether the code matrices come from group $j = 0$ or $j = \{1, 2, \ldots, p_1 - 1\}$. In group $j = 0$, the $p_1$ code matrices are basically the original CHPC. To minimize the intrasymbol cross-correlation function (i.e., $\lambda'_c$), any one of the $p_1 - 1$ code matrices (i.e., excluding the $i_1 = 0$ matrix) in group $j = 0$ can be frequency-shifted $p_1 - 1$ times for representing a total of $M = p_1$ symbols in multicode keying. Take $p_1 = N = 5$ in Table I as an example, if we assign code matrix $\{(0,0),(1,1),(2,2),(3,3),(4,4)\}$ (i.e., $j = 0$ and $i_1 = 1$) to a user, then its four frequency-shifted copies, $\{(0,4),(1,0),(2,1),(3,2),(4,3)\}$, $\{(0,3),(1,4),(2,0),(3,1),(4,2)\}$, $\{(0,2),(1,3),(2,4),(3,0),(4,1)\}$, and $\{(0,1),(1,2),(2,3),(3,4),(4,0)\}$ can be obtained. For $w = 4$, we can simply drop the last ordered pairs in the code matrices. These five code matrices are orthogonal to each other and, thus, do not create any intrasymbol interference (i.e., $\lambda'_c = 0$), supporting one user with multicode keying of $M \leq p_1$.

For group $j = \{1, 2, \ldots, p_1 - 1\}$, we minimize $\lambda'_c = 1$ by using time-shifted copies of code matrices. The amount of shifts applying to the original code matrices with indices $i_1 \in [0, p_1 - 1]$ depends on the time position of each pulse of the original code matrix with index $i_1 = 0$. Take group $j = 1$ in Table I as an example. The original code matrix with index $i_1 = 0$ is $\{(0,0),(1,1),(2,4),(3,4),(4,1)\}$ for a maximum code weight of $w = p_1 = 5$. By taking the corresponding right-time-shifts of the original code matrices with indices $i_1 \in [0, 4]$, we can obtain a total of five code matrices for multicode keying with $M = 5$. For $w = 4$, we can simply drop the last ordered pair in the code matrices, giving $\{(0,0),(1,1),(2,4),(3,4)\}$, $\{(0,1),(1,3),(2,2),(3,3)\}$, $\{(0,4),(1,2),(2,2),(3,4)\}$, $\{(0,4),(1,3),(2,4),(3,2)\}$, and $\{(0,1),(1,1),(2,3),(3,2)\}$. This method supports $p_1 - 1$ users with multicode keying of $M \leq p_1$.

In summary, the two rules for $k = 1$ supports a total of $N = p_1$ users with multicode keying of $M \leq p_1$. This code-assignment method is similar to that in [5]. Since there is no intrasymbol interference in group $j = 0$, the probability of having entries in an undesired decoder, caused by $\lambda'_c = 1$ in group $j = \{1, 2, \ldots, p_1 - 1\}$, can be obtained by correcting (14) of [5], such that

\[
P_r(z) = \begin{cases} 
1 - \frac{p_1 - 1}{p_1} \cdot \frac{z^{w+1}}{p_1} P_r(z) & \text{for } z = 0 \\
\frac{p_1 - 1}{p_1} \cdot \frac{z^w}{p_1} P_r(z-1) + \frac{1}{p_1} \cdot \frac{z^w}{p_1} P_r(z) & \text{for } z \in [1, w-1] \\
\frac{p_1 - 1}{p_1} \cdot \frac{z^w}{p_1} P_r(z-1) + P_r(z) & \text{for } z = w 
\end{cases}
\]

(A.1)

There are only $p_1 - 1$ positions (out of $p_1$ positions of desired code matrix) of having one hit from the other $p_1 - 1$ code matrices. Therefore, the factor $\frac{p_1 - 1}{p_1}$ is added to scale the conditional probability $z/p_1$, which accounts for the chances of increasing the number of entries in an undesired decoder from $z - 1$ to $z$, caused by the intrasymbol cross-correlation functions of at most one. Similarly, we also include the factor into the term $1 - \left(1 - \frac{(p_1 - 1)}{p_1}\right)\frac{z}{p_1} P_r(z)$, which considers the chances of increasing the number of entries in an undesired decoder from $z$ to $z + 1$ in order to scale the conditional probability $(z + 1)/p_1$.

Now, we consider the $k > 1$ case. For group $j = 0$, we choose one of the time-shifted copies of each original code matrix for multicode keying to minimize the intrasymbol cross-correlation functions. The rule to choose the code matrices depends on the index $i_1$ of the original code matrix to obtain the $i_1p_2p_3\cdots p_k$ right-time-shifted copy of the original code matrix. Take $k = 2$, $j = 0$, and $i_2 = 1$ as an example. The $p_1 = 5$ code matrices are $\{(0,0),(1,5),(2,10),(3,15),(4,20)\}$, $\{(0,0),(1,6),(2,12),(3,18),(4,24)\}$, $\{(0,0),(1,7),(2,14),(3,16),(4,23)\}$, $\{(0,0),(1,8),(2,11),(3,19),(4,22)\}$, and
Our rule right-shifts the corresponding code matrices by 0, 5, 10, 15, 20 time slots (i.e., right time-shifting by \( i_1 \cdot p_2 \) time slots, for \( i_1 \in [0, p_1 - 1] \), \( p_1 = p_2 = 5 \), respectively. Then, we can obtain \( p_1 = 5 \) new code matrices \( \{(0, 0), (1, 5), (2, 10), (3, 15), (4, 20)\} \), \( \{(0, 5), (1, 11), (2, 17), (3, 23), (4, 4)\} \), \( \{(0, 10), (1, 17), (2, 24), (3, 3), (4, 8)\} \), \( \{(0, 15), (1, 23), (2, 1), (3, 9), (4, 12)\} \), and \( \{(0, 20), (1, 4), (2, 8), (3, 12), (4, 16)\} \) to represent \( M = p_1 = 5 \) symbols for multicode keying. These new code matrices are orthogonal to each other. Therefore, the probability \( P'_r(z) \) is not needed for group \( j = 0 \) with the same indices \( (i_2, i_3, \ldots, i_k) \).

For group \( j = \{1, 2, \ldots, p_1 - 1\} \), we can also use the same rule (i.e., right shifting by \( i_1 \cdot p_2 \) time slots, for \( i_1 \in [0, p_1 - 1] \), \( p_1 = p_2 = 5 \)) to get new code matrices. The probability \( P'_r(z) \) is also not needed for group \( j = \{1, 2, \ldots, p_1 - 1\} \) with the same indices \( (i_2, i_3, \ldots, i_k) \) because these \( p_1 \) new codes are orthogonal to each other.

References