University of Wollongong

Research Online

Faculty of Informatics - Papers (Archive)

Faculty of Engineering and Information Sciences

2003

Williamson-Hadamard Spreading Sequences for DS-CDMA Applications

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Beata J. Wysocki
bjw@uow.edu.au

Tadeusz A. Wysocki
wysocki@uow.edu.au

Follow this and additional works at: https://ro.uow.edu.au/infopapers

Part of the Physical Sciences and Mathematics Commons

Recommended Citation

Seberry, Jennifer; Wysocki, Beata J.; and Wysocki, Tadeusz A.: Williamson-Hadamard Spreading Sequences for DS-CDMA Applications 2003.
https://ro.uow.edu.au/infopapers/1188

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

Williamson-Hadamard Spreading Sequences for DS-CDMA Applications

Abstract

Orthogonal bipolar spreading sequences are used in direct sequence code division multiple acces (DS-CDMA) systems for both spectrum spreading and channel separation. The most commonly used sequences are Walsh-Hadamard sequences of lenghts being an integer power of 2. A construction based on Williamson's arrays leading to sequences of lengths $N \equiv 4 (\mathrm{mod}\ 8)$ is presented in the paper. Aperiodic correlation characteristics, for example sequence sets of lengths 12-252 are presented. The correlation properties of the sequence sets are later improved using a diagonal modification technique.

Disciplines

Physical Sciences and Mathematics

Publication Details

Jennifer Seberry, Beata J. Wysocki and Tadeusz A. Wysocki Williamson-Hadamard Spreading Sequences for DS-CDMA Applications, Special Issue on "Coding and Its Applications in CDMA Wireless Systems", Journal of Wireless Communications and Mobile Computing. 3 (2003), 597-607.

This journal article is available at Research Online: https://ro.uow.edu.au/infopapers/1188

WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. 2003; **3**:597–607 (DOI: 10.1002/wcm.143)

Williamson–Hadamard spreading sequences for DS-CDMA applications

Jennifer Seberry, Beata J. Wysocki and Tadeusz A. Wysocki*,†
University of Wollongong, NSW2522, Australia

Summary

Orthogonal bipolar spreading sequences are used in direct sequence code division multiple access (DS-CDMA) systems for both spectrum spreading and channel separation. The most commonly used sequences are Walsh–Hadamard sequences of lengths being an integer power of 2. A construction based on Williamson's arrays leading to sequences of lengths $N \equiv 4 \pmod 8$ is presented in the paper. Aperiodic correlation characteristics, for example sequence sets of lengths 12–252 are presented. The correlation properties of the sequence sets are later improved using a diagonal modification technique. Copyright © 2003 John Wiley & Sons, Ltd.

KEY WORDS: Williamson's arrays; spreading sequences; code division multiple access; correlation functions

1. Introduction

Orthogonal bipolar sequences are of a great practical interest for the current and future direct sequence (DS) code division multiple access (CDMA) systems where the orthogonality principle can be used for channels separation, e.g. Reference [1]. The most commonly used sets of bipolar sequences are Walsh–Hadamard sequences [2], as they are easy to generate and simple to implement. However, they exist only for sequence lengths being an integer power of 2, which can be a limiting factor in some applications. In the paper, we describe a technique to generate sets of bipolar sequences of order $N \equiv 4 \pmod 8$ based on a Williamson's construction [3]. The resultant Williamson–Hadamard sequences possess very good autocorrelation properties that make them amenable to synchronization requirements.

It is well known, e.g. Reference [4–6], that if the sequences have good aperiodic cross-correlation properties, the transmission performance can be improved for those CDMA systems where different propagation delays exist. Wysocki and Wysocki in Reference [7] proposed a technique to modify bipolar Walsh–Hadamard sequences to achieve changes in their correlation characteristics without compromising orthogonality. In this paper, we apply the same technique to improve cross-correlation properties of Williamson–Hadamard sequences. As it is always the case, the improvement is achieved at the expense of slightly worsening the autocorrelation properties. However, the overall autocorrelation properties of the modified sequence sets are still significantly better than those of Walsh–Hadamard sequences of comparable lengths.

The paper is organized as follows. In Section 2, we introduce principles of constructing Hadamard matrices using Williamson's arrays and provide a list of some possible seed sequences of lengths 3–63 to construct Williamson–Hadamard matrices of orders 12–252. Section 3 introduces some correlation measures that can be used to compare different sets of

*Correspondence to: Tadeusz A. Wysocki, University of Wollongong, NSW2522, Australia.
†E-mail: wysocki@uow.edu.au

Copyright © 2003 John Wiley & Sons, Ltd.

spreading and show the values of those parameters for the sequence sets derived utilizing the seed sequences listed in Section 2. In Section 4, we briefly describe the method used to modify correlation characteristics of sequence sets and show the results when applied to Williamson–Hadamard sequences. Section 5 concludes the paper.

2. Williamson–Hadamard Construction

A Hadamard matrix $\mathbf{H}$ of order n has elements ± 1 and satisfies $\mathbf{H}\mathbf{H}^T = n\mathbf{I}_n$. The order of a Hadamard matrix is 1, 2 or $n \equiv (0 \bmod 4)$ and the first unsolved case is order 428. We briefly describe the theory of Williamson's construction below. Previous computer searches for Hadamard matrices using Williamson's condition are described in Section 2.1.

Theorem 1 (Williamson [8])**:** *Suppose there exist four symmetric* (1, −1) *matrices* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{D}$ *of order n which satisfy*

$$\mathbf{X}\mathbf{Y}^T = \mathbf{Y}\mathbf{X}^T, \qquad \mathbf{X}, \mathbf{Y} \in \{\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}\}.$$

Further, suppose

$$\mathbf{A}\mathbf{A}^T + \mathbf{B}\mathbf{B}^T + \mathbf{C}\mathbf{C}^T + \mathbf{D}\mathbf{D}^T = 4n\mathbf{I}_n. \qquad (1)$$

Then

$$\mathbf{H} = \begin{bmatrix} \mathbf{A} & \mathbf{B} & \mathbf{C} & \mathbf{D} \\ -\mathbf{B} & \mathbf{A} & -\mathbf{D} & \mathbf{C} \\ -\mathbf{C} & \mathbf{D} & \mathbf{A} & -\mathbf{B} \\ -\mathbf{D} & -\mathbf{C} & \mathbf{B} & \mathbf{A} \end{bmatrix} \qquad (2)$$

is a Hadamard matrix of order 4n constructed from a Williamson array.

Let the matrix $\mathbf{T}$ given below be called the shift matrix:

$$\mathbf{T} = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{bmatrix} \qquad (3)$$

and note that

$$\mathbf{T}^n = \mathbf{I}, \qquad \left(\mathbf{T}^i\right)^T = \mathbf{T}^{n-i}. \qquad (4)$$

If n is odd, $\mathbf{T}$ is the matrix representation of the nth root of unity ω, $\omega^n = 1$.

Let

$$\begin{cases} \mathbf{A} = \sum_{i=0}^{n-1} a_i \mathbf{T}^i, & a_i = \pm 1, \quad a_{n-i} = a_i \\ \mathbf{B} = \sum_{i=0}^{n-1} b_i \mathbf{T}^i, & b_i = \pm 1, \quad b_{n-i} = b_i \\ \mathbf{C} = \sum_{i=0}^{n-1} c_i \mathbf{T}^i, & c_i = \pm 1, \quad c_{n-i} = c_i \\ \mathbf{D} = \sum_{i=0}^{n-1} d_i \mathbf{T}^i, & d_i = \pm 1, \quad d_{n-i} = d_i. \end{cases} \qquad (5)$$

Then matrices $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{D}$ may be represented as polynomials. The requirement that $x_{n-i} = x_i, x \in \{a, b, c, d\}$, forces the matrices $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{D}$ to be symmetric. Hereafter, we will refer to the sequences a, b, c, d, as the seed sequences.

Since $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{D}$ are symmetric, Equation (1) becomes

$$\mathbf{A}^2 + \mathbf{B}^2 + \mathbf{C}^2 + \mathbf{D}^2 = 4n\mathbf{I}_n,$$

and the relation $\mathbf{X}\mathbf{Y}^T = \mathbf{Y}\mathbf{X}^T$ becomes $\mathbf{X}\mathbf{Y} = \mathbf{Y}\mathbf{X}$ which is true for polynomials.

Definition 1: *Williamson matrices are* (1, −1) *symmetric circulant matrices.*

As a consequence of being symmetric and circulant, they commute in pairs.

The following theorem of Williamson has been used as the motivator for search algorithm:

Theorem 2 (Williamson [8]): *If there exist solutions to the equations*

$$\mu_i = 1 + 2\sum_{j=1}^{s} t_{ij}\left(\omega^j + \omega^{n-j}\right), \qquad i = 1, 2, 3, 4, \qquad (6)$$

where $s = \frac{1}{2}(n-1)$, ω *is a nth root of unity, exactly one of* $t_{1j}, t_{2j}, t_{3j}, t_{4j}$, *is nonzero and equals* ± 1 *for each* $1 \le j \le s$, *and*

$$\mu_1^2 + \mu_2^2 + \mu_3^2 + \mu_4^2 = 4n,$$

then there exist solutions to the equations:

$$\begin{cases} \mathbf{A} = \sum_{i=0}^{n-1} a_i \mathbf{T}^i, & a_0 = 1, \quad a_i = a_{n-i} = \pm 1 \\ \mathbf{B} = \sum_{i=0}^{n-1} b_i \mathbf{T}^i, & b_0 = 1, \quad b_i = b_{n-i} = \pm 1 \\ \mathbf{C} = \sum_{i=0}^{n-1} c_i \mathbf{T}^i, & c_0 = 1, \quad c_i = c_{n-i} = \pm 1 \\ \mathbf{D} = \sum_{i=0}^{n-1} d_i \mathbf{T}^i, & d_0 = 1, \quad d_i = d_{n-i} = \pm 1. \end{cases} \qquad (7)$$

That is, there exists a Hadamard matrix of order 4n.

In matrix form, $\omega^j + \omega^{n-j}$ is represented as $\mathbf{T}^j + \mathbf{T}^{n-j}$. Since these are symmetric, we write

$$\omega = \omega^j + \omega^{n-j}.$$

Copyright © 2003 John Wiley & Sons, Ltd.

Remark 1: The solutions for Equation (6) are independent of the particular root ω, so if n as defined by Equation (1) is prime, ω can be chosen so that the first μ having any ω_j assigned has ω_1. Since the equations are true for all roots of unity ω, they are also true for $\omega = 1$.

2.1. Results From Previous Searches

In many cases, complete searches have been conducted for Hadamard matrices of Williamson type. Searches have also been conducted for special classes of Williamson type Hadamard matrices. Furthermore, an infinite class of such matrices is known and will also be discussed briefly.

- Williamson [8] used algebraic and number theoretic results to simplify his first searches by hand in 1944.
- Baumert and Hall [9] report results of a complete search for orders $4t$, t odd and $3 \le t \le 23$. Some incomplete results for higher orders are also given.
- Sawade [10] reports results of a complete search for orders $4t$, $t = 25$, 27. The results for $t = 25$ were later demonstrated to be incomplete by Djokovic [11].
- Djokovic [12] reports results of a complete search for orders $4t$, $t = 29$, 31. Only a single non-equivalent solution was found for $t = 29$ and is equivalent to an earlier result of Baumert [13].
- Koukouvinos and Kounias [14, 15] report results of a complete search for order $4t$, $t = 33$ and 39. These results were complete search for order $4t$, $t = 33$ and 39. These results were later demonstrated to be incomplete by Djokovic [16].
- Djokovic [16] reports results of a complete search for orders $4t$, $t = 33$, 35, 39.
- Djokovic [11] reports results of a complete search for orders $4t$, $t = 25$, 37. This extends results obtained by Sawade [10] for $t = 25$ and, for $t = 37$, by Williamson [9] and later Yamada [17] for a special class of matrices.
- Horton *et al.* [18] report results of a complete search for orders $4t$, t odd and 25 t 37. No new results were found, confirming existence results.

An infinite family of Hadamard matrices of Williamson type has been proved to exist under certain conditions [19, 20]:

Theorem 3 (Williamson [9])**:** *If q is a prime power, $q \equiv 1 \pmod 4$, $q + 1 = 2t$, then there exists a Williamson matrix of order $4t$; we have $\mathbf{C} = \mathbf{D}$, and $\mathbf{A}$ and $\mathbf{B}$ differ only on the main diagonal.*

This theorem gives examples of Hadamard matrices of Williamson type for orders $4t$, $t = 31, 37, 41, 45, 49, 51, 55, \ldots$, for example.

Yamada [17] has searched for Hadamard matrices of Williamson type, with certain restrictions. These matrices are referred to as Williamson type j matrices. The Williamson equation for such matrices, of order $4n$ is:

$$\begin{aligned} 4n = {} & \left(1 - 2\sum_{s\in A} c_s\omega_s\right)^2 + \left(1 - 2\sum_{s\in A} c_s\omega_{sj}\right)^2 \\ & + \left(1 - 2\sum_{s\in B} c_s\omega_s\right)^2 + \left(1 - 2\sum_{s\in B} c_s\omega_{sj}\right)^2, \end{aligned} \tag{8}$$

where $c_s, d_s = \pm 1$, $\omega_s = \omega^s + \omega^{-s}$, $\omega^n = 1$, $j^2 \equiv -1 \pmod n$, $\mathbf{A}$, $\mathbf{B}$, $j\mathbf{A}$, $j\mathbf{B}$ is a partition of $\{1, 2, \ldots, (n-1)/2\}$. Such a j exists, if and only if, all prime divisors of n are $\equiv 1 \pmod 4$. This led to some new results for $n = 29$, 37, 41. A summary of the presently known results can be found in Horton *et al.* [18].

In Table 1, we list some of the seed sequences that can be used to construct Walsh–Hadamard sequence sets for DS-CDMA applications. This list includes just a single quadruple of sequences for a given length.

3. Correlation Measures

It is well known (e.g. References [4, 5]) that the level of multi-access interference and synchronization amenability depend on the cross-correlations between the sequences and the autocorrelation functions of the sequences respectively. In this section, we introduce some of the quantitative measures based on the aperiodic correlation functions that can be used to compare the sequence sets from the viewpoint of their usefulness in DS-CDMA systems. Then, we present the computed values of these measures for the Williamson–Hadamard sequences created using formula (2) from the seed sequences listed in Table I.

For general polyphase sequences $\{s_n^{(i)}\}$ and $\{s_n^{(l)}\}$ of length N, the discrete aperiodic correlation function is defined as [5,22]:

$$c_{i,l}(\tau) = \begin{cases} \frac{1}{N}\sum_{n=0}^{N-1-\tau} s_n^{(i)}[s_{n+\tau}^{(l)}]^*, & 0 \le \tau \le N-1 \\ \frac{1}{N}\sum_{n=0}^{N-1+\tau} s_{n-\tau}^{(i)}[s_n^{(l)}]^*, & 1-N \le \tau < 0 \\ 0, & |\tau| \ge N, \end{cases} \tag{9}$$

Copyright © 2003 John Wiley & Sons, Ltd.

Table I. List of the seed sequences for Williamson–Hadamard sequences of length 12–252.

N		Seed sequences
12	A	+++
	B	+−−
	C	+−−
	D	+−−
20	A	+−−−−
	B	+−−−−
	C	++−−+
	D	+−++−
28	A	+−−−−−−
	B	++−−−−+
	C	+−+−−+−
	D	+−−++−−
36	A	++−−−−−−+
	B	+−+−−−−+−
	C	+−−+−−+−−
	D	+−−−++−−−
44	A	++−−−−−−−−+
	B	++−++−−++−+
	C	++−+−++−+−+
	D	+−++−−−−++−
52	A	+++−++−−++−++
	B	++−+−++++−+−+
	C	++−−+−++−+−−+
	D	+−−−++++++−−−
60	A	+−+−−−−++−−−−+−
	B	+−+−−−−++−−−−+−
	C	+−−++−++++−++−−
	D	+++−−+−−−−+−−++
68	A	+−−+−+−−−−−−+−+−−
	B	+−+−−−++−−++−−−+−
	C	+−−−−−++++++−−−−−
	D	++−−+−++−−++−+−−+
76	A	++−−++−++++++−++−−+
	B	+−++−−+−−−−−−+−−++−
	C	+++−−−+−+−−+−+−−−++
	D	+++−−−+−+−−+−+−−−++
84	A	+++++−−++−−−−++−−++++
	B	+++−+−−+−++++−+−−+−++
	C	+++−−+−+++−−+++−+−−++
	D	+−−−+−+−++−−++−+−+−−−
92	A	+−++−++−−++++++−−++−++−
	B	++−−−+−−−+−++−+−−−+−−−+
	C	+++−−−++−+−++−+−++−−−++
	D	+++−+++−+−−−−−−+−+++−++
100	A	+−−−+−+−++−−−−−−++−+−+−−−
	B	+−−+−−+−+−−−++−−−+−+−−+−−
	C	++−++−+++−−−−−−−−+++−++−+
	D	+−++++−−−−++−−++−−−−++++−
108	A	+−+−++−+++−−++++−−+++−++−+−
	B	++−+−+−++−++−++−++−++−+−+−+
	C	++++−++−−−−−++++−−−−−++−+++
	D	++++−−−++−−−+−−+−−−++−−−+++
116	A	++++−++−+−−−++++++−−−+−++−+++
	B	++−−+−−+−+++−++++−+++−+−−+−−+
	C	+++−−−++−−+−+−−−−+−+−−++−−−++
	D	+−+−−−++−−+−++++++−+−−++−−−+−
124	A	++−+−−−+++++−+−++−+−+++++−−−+−+
	B	+++++−−+++−+−−+−−+−−+−+++−−++++
	C	++−++−−+−−−−++−−−−++−−−−+−−++−+
	D	+−−−+++−++−+−+−−−−+−+−++−+++−−−
132	A	+−−+++−−+−−++++++++++++−−+−−+++−−
	B	++++++−−−−++−+−−++−−+−++−−−−+++++
	C	++−+−+−+−−+++−+−++−+−+++−−+−+−+−+
	D	++−−+−+−−++−+++−−−−+++−++−−+−+−−+

Continues

Copyright © 2003 John Wiley & Sons, Ltd.

Table I. Continued

148	A	+−−+−++++−−−−−+−+−−−−+−+−−−−−++++−+−−
	B	++−−−+−+−−++−−−+−−++−−+−−−++−−+−+−−−+
	C	+++−−++++−+++−+−−−−−−−−+−+++−+++++−++
	D	++−−+−+−++++−++−−+−−+−−++−++++−+−+−−+
156	A	+++−−+−+−−−−−+−−++−−−−++−−+−−−−−+−+−−++
	B	+++−−++−+−−−+−+−−+−−−−+−−+−+−−−+−++−−++
	C	++++−−−+−−++−−−−+−+−−+−+−−−−++−−+−−−+++
	D	+−−−++−+−+−−−−−+++−++−+++−−−−−+−+−++−−−
164	A	+−+−−−+++−++−+−−++++++++++−−+−++−+++−−−+−
	B	+−+−−−+++−++−+−−++++++++++−−+−++−+++−−−+−
	C	++−−−−+−+++−++−++−−−++−−−++−++−+++−+−−−−+
	D	+−++++−+−−−+−−+−−+++−−+++−−+−−+−−−+−++++−
172	A	+−−−++−−++++−+−+++−++−−++−+++−+−++++−−++−−−
	B	++−++++++−−−−+−+−−++−++−++−−+−+−−−−++++++−+
	C	+++−+−++−−+−+−++++−+−−−−+−++++−+−+−−++−+−++
	D	++−−−++++−+−−+−−++−−−−−−−−++−−+−−+−++++−−−+
180	A	+++−−+++−++−+−+++++−−−−−−−−+++++−+−++−+++−−++
	B	+−−++−−−+−−+−+−−−−−++++++++−−−−−+−+−−+−−−++−−
	C	++−−++++−+−+−+++−−+−−+−−+−−+−−+++−+−+−++++−−+
	D	++−−++++−+−+−+++−−+−−+−−+−−+−−+++−+−+−++++−−+
196	A	++++−++−+−−−++−+++−−−++−++−++−−−+++−++−−−+−++−+++
	B	++++−++−+−−−++−+++−−−++−++−++−−−+++−++−−−+−++−+++
	C	+−−−−+−++++−−+−+++−+−+++−−+++−+−+++−+−−++++−+−−−−
	D	+++++−+−−−−++−+−−−+−+−−−++−−−+−+−−−+−++−−−−+−++++
220	A	+−+−−+−+−++−−+−+++++−+++−−++++−−+++−+++++−+−−++−+−+−−+−
	B	++−++−+−+−−++−+−−−−−+−−−++−−−−++−−−+−−−−−+−++−−+−+−++−+
	C	+++−−−−++−++−−++−−−−+−+−++++++++−+−+−−−−++−−++−++−−−−++
	D	+++−−−−++−++−−++−−−−+−+−++++++++−+−+−−−−++−−++−++−−−−++
228	A	+−−−++−+−−++++−+++−++−−−+−++++++−+−−−++−+++−++++−−+−++−−−
	B	++++−−+−++−−−−+−−−+−−+++−+−−−−−−+−+++−−+−−−+−−−−++−+−−+++
	C	++−+−+−−−++−++−+−−+++−−−−−+−−−−+−−−−−+++−−+−++−++−−−+−+−+
	D	++−+−+−−−++−++−+−−+++−−−−−+−−−−+−−−−−+++−−+−++−++−−−+−+−+
244	A	++−−+−−++−−+−+−++++−−+−−−−−+−−−−−−+−−−−−+−−++++−+−+−−++−−+−−+
	B	++−−+−−++−−+−+−++++−−+−−−−−+−−−−−−+−−−−−+−−++++−+−+−−++−−+−−+
	C	+−−−+−+−++++−−−++−−+−++−+−−−++++++−−−+−++−+−−++−−−++++−+−+−−−
	D	++++−+−+−−−−+++−−++−+−−+−+++−−−−−−+++−+−−+−++−−+++−−−−+−+−+++
252	A	++++−++−+−++++−+−−−+−−−+++−−−++++++−−−+++−−−+−−−+−++++−+−++−+++
	B	++++−++−+−++++−+−−−+−−−+++−−−++++++−−−+++−−−+−−−+−++++−+−++−+++
	C	++−+++−−++−++−−+−−+−++−+−+++−−−−−−−−+++−+−++−+−−+−−++−++−−+++−+
	D	+−+−−−++−−+−−++−++−+−−+−+−−−++++++++−−−+−+−−+−++−++−−+−−++−−−+−

where $[\bullet]^*$ denotes a complex conjugate operation. When $\{s_n^{(i)}\} = \{s_n^{(l)}\}$, Equation (9) defines the discrete aperiodic autocorrelation function.

In order to evaluate the performance of a whole set of M spreading sequences, the average mean-square value of cross-correlation for all sequences in the set, denoted by R_{CC}, was introduced by Oppermann and Vucetic [5] as a measure of the set cross-correlation performance:

$$R_{CC} = \frac{1}{M(M-1)} \sum_{i=1}^{M} \sum_{\substack{k=1 \\ k \neq i}}^{M} \sum_{\tau=1-N}^{N-1} |c_{i,k}(\tau)|^2. \qquad (10)$$

A similar measure, denoted by R_{AC}, was introduced in Reference [5] for comparing the autocorrelation performance:

$$R_{AC} = \frac{1}{M} \sum_{i=1}^{M} \sum_{\substack{\tau=1-N \\ \tau \neq 0}}^{N-1} |c_{i,i}(\tau)|^2. \qquad (11)$$

The measure defined by Equation (11) allows for comparison of the autocorrelation properties of the set of spreading sequences on the same basis as the cross-correlation properties.

The measures defined by Equations (10) and (11) are very useful for large sets of sequences and large number of active users, when the constellation of interferers (i.e. relative delays among the active users and the spreading sequences used) changes randomly for every transmitted information symbol. However, for a more static situation, when the constellation of interferers stays constant for the duration of many information symbols, it is also important to consider the worst-case scenarios. This can be accounted for by analyzing the maximum value of peaks in the aperiodic cross-correlation functions over the whole set of sequences and in the aperiodic autocorrelation function for $\tau \neq 0$. Hence, we introduce here two

Copyright © 2003 John Wiley & Sons, Ltd.

Table II. Correlation parameters of the Williamson–Hadamard sequences of length $N = 12$–252 obtained from the seed sequences listed in Table I.

N	R_{CC}	R_{AC}	C_{max}	A_{max}
12	0.9082	1.00930	0.9167	0.6667
20	0.9675	0.61800	0.9500	0.4000
28	0.9813	0.50510	0.9643	0.2857
36	0.9818	0.63820	0.9722	0.3333
44	0.9874	0.54040	0.9773	0.2727
52	0.9854	0.74700	0.9808	0.3077
60	0.9894	0.62730	0.9833	0.4000
68	0.9898	0.68330	0.9853	0.2941
76	0.9916	0.62770	0.9868	0.3158
84	0.99355	0.53507	0.9881	0.26190
92	0.99246	0.68655	0.98913	0.27174
100	0.99300	0.69333	0.9900	0.26000
108	0.99379	0.66439	0.99074	0.22222
116	0.99461	0.62025	0.99138	0.23276
124	0.99323	0.83231	0.99194	0.23387
132	0.99530	0.61556	0.99242	0.21970
148	1.01010	0.64471	0.99324	0.22297
156	0.99516	0.74966	0.99359	0.19231
164	0.99656	0.56130	0.99390	0.23780
172	0.99641	0.61407	0.99419	0.19186
180	0.99668	0.59480	0.99444	0.21667
196	0.99714	0.55864	0.99490	0.24490
220	0.99736	0.57722	0.99545	0.20909
228	0.99760	0.54495	0.99561	0.27632
244	0.99769	0.56104	0.9959	0.19262
252	0.99762	0.5984	0.99603	0.21825

additional measures to compare the spreading sequence sets:

- Maximum value of the aperiodic cross-correlation functions C_{max}

$$c_{max}(\tau) = \max_{\substack{i=1,\ldots,M \\ k=1,\ldots,M \\ i\neq k}} |c_{i,k}(\tau)|;$$
$$\tau = (-N+1), \ldots, (N-1)$$
$$C_{max} = \max_{\tau}\{c_{max}(\tau)\}. \tag{12}$$

- Maximum value of the off-peak aperiodic autocorrelation functions

$$a_{max}(\tau) = \max_{k=1,\ldots,M} \left|c_{k,k}(\tau)\right|;$$
$$A_{max} = \max_{\tau\neq 0}\{a_{max}(\tau)\}. \tag{13}$$

In Table II, we list the correlation parameters R_{CC}, R_{AC}, C_{max} and A_{max}, computed for the Williamson–Hadamard sequences of lengths 12–252 created using the seed sequences listed in Table I. In Figures 1 and 2, we show the typical behavior of the peaks in the aperiodic cross-correlation functions $c_{max}(\tau)$ and peaks in the aperiodic autocorrelation functions $a_{max}(\tau)$ respectively.

4. Modification Method

Further improvement to the values of correlation parameters of the sequence sets based on Williamson–Hadamard matrices can be obtained using the method introduced in Reference [7] for Walsh–Hadamard sequences. That method is based on the fact that for a matrix $\mathbf{H}$ to be orthogonal, it must fulfill the condition $\mathbf{HH}^T = N\mathbf{I}$, where $\mathbf{H}^T$ is the transposed Hadamard matrix of order N and $\mathbf{I}$ is the $N \times N$ unity matrix. In the case of Williamson–Hadamard matrices, we have $N = 4n$. The modification is achieved by taking another orthogonal $N \times N$ matrix $\mathbf{D}_N$, and the new set of sequences is based on a matrix $\mathbf{W}_N$, given by:

$$\mathbf{W}_N = \mathbf{HD}_N. \tag{14}$$

Of course, the matrix $\mathbf{W}_N$ is also orthogonal [7].

In Reference [7], it has been shown that the correlation properties of the sequences defined by $\mathbf{W}_N$ can be

Copyright © 2003 John Wiley & Sons, Ltd.

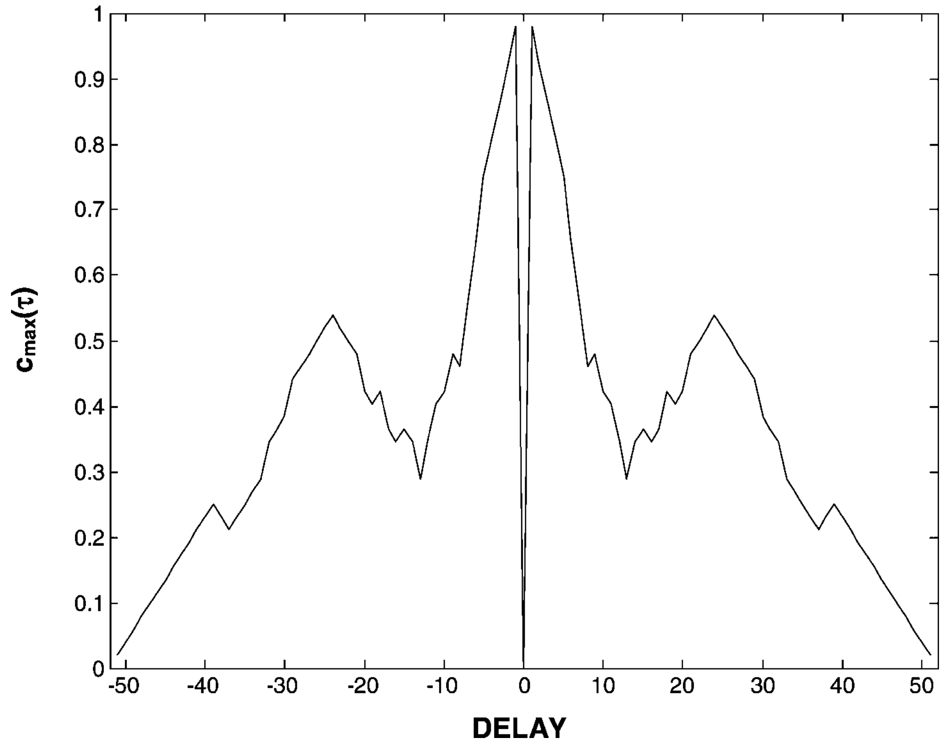

Fig. 1. Plot of the peaks in cross-correlation functions for the Williamson–Hadamard sequence set of order $N = 52$.

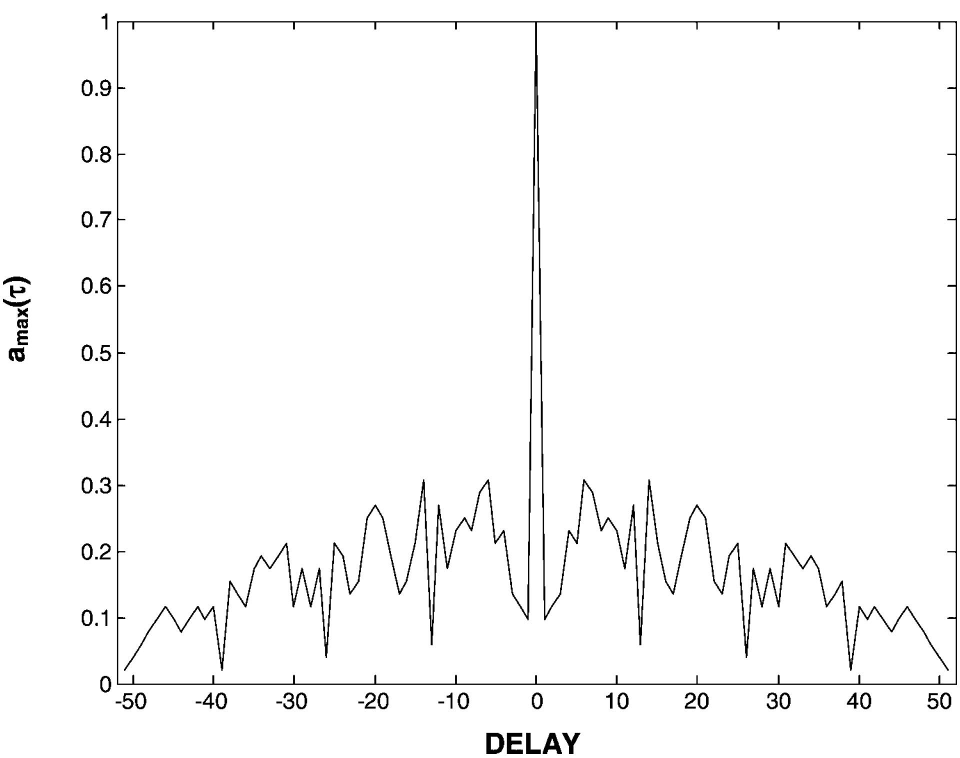

Fig. 2. Plot of the peaks in autocorrelation functions for the Williamson–Hadamard sequence set of order $N = 52$.

Copyright © 2003 John Wiley & Sons, Ltd.

significantly different than those of the original sequences.

A simple class of orthogonal matrices of any order are diagonal matrices with their elements $d_{i,j}$ fulfilling the condition:

$$|d_{l,m}| = \begin{cases} 0 & \text{for} \quad l \neq m \\ k & \text{for} \quad l = m \end{cases}; \qquad l, m = 1, \ldots, N. \quad (15)$$

To preserve the normalization of the sequences, the elements of $\mathbf{D}_N$, being in general complex numbers, must be of the form:

$$d_{l,m} = \begin{cases} 0 & \text{for} \quad l \neq m \\ \exp(j\phi_l) & \text{for} \quad l = m \end{cases}; \quad l, m = 1, \ldots, N. \qquad (16)$$

From the implementation point of view, the best class of sequences are binary sequences.

To find the best possible modifying diagonal matrix $\mathbf{D}_N$, we can do an exhaustive search of all possible bipolar sequences of length N and choose the one which leads to the best performance of the modified set of sequences. However, this approach is very computationally intensive, and even for a modest value of N, e.g. $N = 28$, it is rather impractical. Hence, other search methods, like a random search, must be considered.

By applying a Monte Carlo algorithm [23,24] to $N \geq 20$ and looking for a minimum value of the peaks in the aperiodic cross-correlation functions $C_{\max}$ in 5000 random draws, we have found the sequences listed in Table III for lengths 20–100, and in Table IV, we present the corresponding correlation parameters of the modified sequence sets. In Figures 3 and 4, we present examples of the plots of the peaks in the aperiodic cross-correlation functions $c_{\max}(\tau)$ and peaks in the aperiodic autocorrelation functions $a_{\max}(\tau)$ respectively for the modified sequence sets. There, it is clearly visible that the peaks in the cross-correlation functions are significantly reduced compared to the original sequence sets, shown in the figures by the dotted line. However, this is done on the expense of lifting the peaks in the off-peak autocorrelation functions.

Because of the nonlinear character of the cost function, it is difficult to assess how far the obtained result is from the global minimum without performing the exhaustive search. Calculating the theoretical

Table III. Modifying diagonal sequences for the sequence lengths $N = 20$–100 for the Williamson–Hadamard sequences obtained from the seed sequences listed in Table I.

N	D_N
20	−+−−+−+−−+++−−−+−+++
28	−+++−−++−−+−+++−−+−−−++−+++−
36	−++−−++−−+−+++−−−+−−−+−++−++−−+++−−+
44	+−−+−−−−+−++−++−−+−−++−−+−−−−−−−−−−++−++−+++
52b	++−++−+++++++++−+++++++−−−−+−+++−−−−−−−+−−−−−+++−+−++
60	−−+−+++−+−−++−+−++−−−−+−−−−−−++−+−+−+−−+++−++−+++−−−++−+++−−
68	+−++−++++−+−+−−−−−+−+−−−+−+−+−+−++−++++−−−+−+−+−−−−−−−+−−−+−++++−−++
76	−−−+−++−+++++++−−−−++++−−−+++−+−+−+++++−−++−+−+−++++−−+−+−+−−−+−−−++−++−−−+
84	−−+−++−−+−−−−+−−−+−++−+−++−+−++−+−+−+−++−+++−+++−−++++++−+−−−+−−++−−−−+−−−−−−−−−+−++
92	−+++−+−−+++++−−−−−−+−−+−+−−−−+−++−++−++−−−−+−−+−++++++−−+++−+−++−+−−+−+−++++−−−++++−−+−+−−+−
100	−−+−−−−+−++−−−−−−+−+++++−−−−+++−+++−++++−++−+−−++−−+−++−+−+−−−+++++−−++−−−−−−++++−−−+−−+−++−++−−−+++

Table IV. Correlation parameters of the Williamson–Hadamard sequences of length N modified using a diagonal method to find minimum of $AC_{\max}$.

N	R_{CC}	R_{AC}	$C_{\max}$	$A_{\max}$	B_W	B_L
20	0.9321	1.2900	0.5500	0.6500	0.1562	0.1759
28	0.9664	0.9074	0.5357	0.4643	0.1325	0.1503
36	0.9764	0.8248	0.5000	0.4444	0.1170	0.1333
44	0.9777	0.9604	0.4773	0.5227	0.1060	0.1210
52	0.9804	0.9987	0.4615	0.3654	0.0976	0.1116
60	0.9838	0.9539	0.4500	0.3833	0.0909	0.1041
68	0.9854	0.9795	0.4265	0.4412	0.0854	0.0979
76	0.9877	0.9210	0.4079	0.3026	0.0808	0.0927
84	0.9879	1.0008	0.3929	0.4048	0.0769	0.0883
92	0.9885	1.0451	0.3913	0.3261	0.0735	0.0844
100	0.9902	0.9660	0.3800	0.3400	0.0705	0.0810

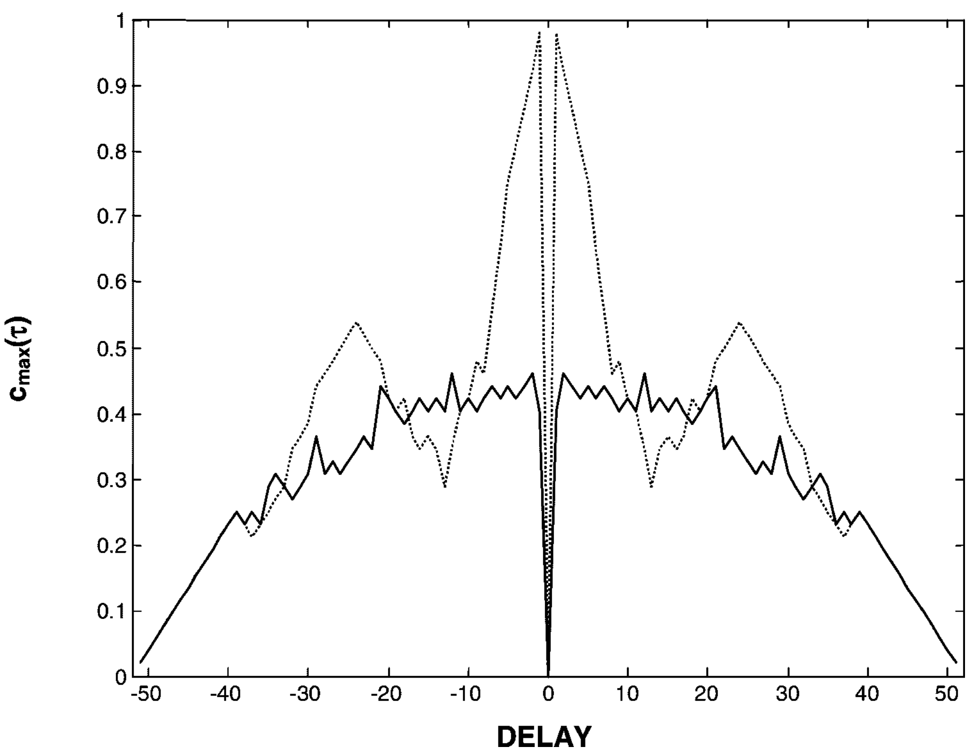

Fig. 3. Plot of the peaks in cross-correlation functions for the modified Williamson–Hadamard sequence set of order $N=52$; the dotted line represents the values for the original sequence set.

lower bound for the aperiodic cross-correlation and aperiodic out-of-phase autocorrelation magnitudes can give some insight into this. The best-known bound is given by Welch [25] and states that for any set of M bipolar sequences of length N

$$\max\{C_{\max}, A_{\max}\} \geq \sqrt{\frac{M-1,}{2NM-M-1}} = B_W. \quad (17)$$

A more tighter bound was given by Levenshtein [26] and is expressed by:

$$\max\{C_{\max}, A_{\max}\} \geq \sqrt{\frac{(2N^2+1)M-3N^2}{3N^2(MN-1)}} = B_L. \quad (18)$$

The values of both B_W and B_L calculated for the considered values of N are also listed in Table IV.

It must be noted here that both Welch and Levenshtein bounds are derived for sets of bipolar sequences where the condition of orthogonality for perfect

Copyright © 2003 John Wiley & Sons, Ltd.

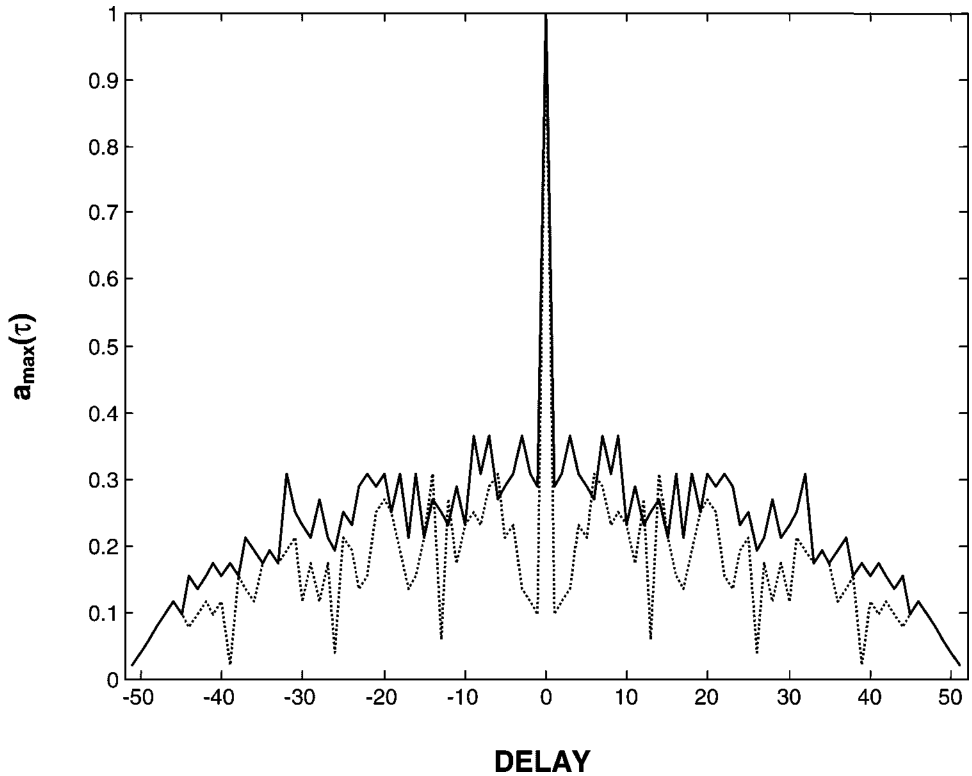

Fig. 4. Plot of the peaks in autocorrelation functions for the modified Williamson–Hadamard sequence set of order $N = 52$; the dotted line represents the values for the original sequence set.

synchronization is not imposed. Hence, one can expect that by introducing the orthogonality condition, the lower bound for the aperiodic cross-correlation and aperiodic out-of-phase autocorrelation magnitudes must be significantly lifted.

5. Conclusions

In this paper, we presented a family of bipolar orthogonal spreading sequences of order $N \equiv 4 \pmod 8$ based on a Williamson's construction. These sequences possess very good autocorrelation properties that make them amenable to synchronization requirements. Later, we applied a modification technique to improve cross-correlation properties of Williamson–Hadamard sequences without compromising their orthogonality. The improvement was achieved at the expense of slightly worsening the autocorrelation properties. However, the overall autocorrelation properties of the modified sequence sets are still significantly better than those of Walsh–Hadamard sequences of comparable lengths. The proposed family of bipolar spreading sequences can be very useful in those DS-CDMA systems that require spreading different than by a factor being an integer power of 2.

References

1. Steele R. Introduction to digital cellular radio. In *Mobile Radio Communications* (2nd edn), Steele R, Hanzo L (eds). IEEE Press: New York, 1999.
2. Harmuth HF. *Transmission of Information by Orthogonal Functions*. Springer–Verlag: Berlin, 1970.
3. Williamson J. Hadamard's determinant theorem and the sum of four squares. *Duke Mathematical Journal* 1944; **11**: 65–81.
4. Pursley MB. Performance evaluation for phase-coded spread-spectrum multiple-access communication—Part I: system analysis. *IEEE Transactions on Communications* 1977; **COM-25**: 795–799.
5. Oppermann I, Vucetic BS. Complex spreading sequences with a wide range of correlation properties. *IEEE Transactions on Communications* 1997; **COM-45**: 365–375.
6. Oppermann I. Orthogonal complex-valued spreading sequences with a wide range of correlation properties. *IEEE Transactions on Communications* 1997; **COM-45**: 1379–1380.
7. Wysocki BJ, Wysocki T. Modified Walsh–Hadamard sequences for DS-CDMA wireless systems. *International Journal of Adapt. Control and Signal Processing* 2002; **16**: 589–602.
8. Williamson J. Hadamard's determinant theorem and the sum of four squares. *Duke Mathematical Journal* 1944; **11**: 65–81.
9. Baumert LD, Hall M, Jr. Hadamard matrices of the Williamson type. *Mathematics of Computation* 1965; **19**: 442–447.
10. Sawade. Hadamard matrices of order 100 and 108. *Bulletin of Nagoya Institute of Technology* 1977; **29**: 147–153.
11. Djokovic DZ. Note on Williamson matrices of orders 25 and 37. *Journal of Combinatorial Mathematics and Combinatorial Computing* 1995; **18**: 171–175.

Copyright © 2003 John Wiley & Sons, Ltd.

12. Djokovic DZ. Williamson matrices of orders 4×29 and 4×31. *Journal of Combinational Theory Series A* 1992; **59**: 442–447.
13. Baumert LD. Hadamard matrices of orders 116 and 232. *Bulletin of the American Mathematical Society* 1966; **72**: 237.
14. Koukouvinos C, Kounias S. Hadamard matrices of the Williamson type of order 4 m, m = pq: an exhaustive search for m = 33. *Discrete Mathematics* 1988; **68**: 45–47.
15. Koukouvinos C, Kounias S. There are no circulant symmetric Williamson matrices of order 39. *Journal of Combinatorial Mathematics and Combinatorial Computing* 1990; **7**: 161–169.
16. Djokovic DZ. Williamson matrices of orders 4n for n = 33,35,39. *Discrete Mathematics* 1993; **115**: 267–271.
17. Yamada M. On the Williamson type j matrices of orders 4×29, 4×41 and 4×37. *Journal of Combinational Theory Series A* 1979; **27**: 378–381.
18. Horton J, Koukouvinos C, Seberry J. A search for Hadamard matrices constructed from Williamson matrices. *Bulletin of the Institute of Combinatorics and its Applications* 2002; **35**: 75–88.
19. Turyn RJ. An infinite class of Williamson matrices. *Journal of Combinational Theory Series A* 1972; **12**: 319–321.
20. Whiteman AL. An infinite family of Hadamard matrices of Williamson type. *Journal of Combinational Theory Series A* 1973; **14**: 334–340.
21. http://www.uow.edu.au/~jennie/
22. Fan P, Darnell M. *Sequence Design for Communications Applications*. John Wiley & Sons: New York, 1996.
23. Fishman G. *Monte Carlo: Concepts, Algorithms, and Applications* (3rd edn). Springer Series in Operations Research, Springer–Verlag: NY, 1999.
24. Nocedal J, Wright SJ. *Numerical Optimization*. Springer Series in Operations Research, Springer–Verlag: NY, 1999.
25. Welch LR. Lower bounds on the maximum cross-correlation of signals. *IEEE Transactions on Information Theory* 1974; **IT-20**: 397–399.
26. Levenshtein VI. A new lower bound on aperiodic crosscorrelation of binary codes. 4th International Symposium On Communication Theory and Applications, ISCTA'97. Ambleside, UK, 13–18 July 1997; 147–149.

Authors' Biographies

Dr Seberry was awarded Ph.D. in Computation Mathematics from La Trobe University in 1971. She has subsequently held positions at the Australian National University, The University of Sydney and ADFA, The University of New South Wales. She has published extensively in Discrete Mathematics and is world renowned for her new discoveries on Hadamard Matrices and Statistical Designs. She started Teaching in Cryptology and Computer Security in 1980. She is especially interested in authentication and privacy. In 1987 at University College, ADFA, she founded the Centre for Computer and Communications Security Research to be a reservoir of expertise for the Australian community. Her studies of the application of discrete mathematics and combinatorial computing via bent functions, S-box design, have led to the design of secure crypto-algorithms and strong hashing algorithms for secure and reliable information transfer in networks and telecommunications. Her studies of Hadamard matrices and orthogonal designs are applied in CDMA technologies. In 1990, she founded the AUSCRYPT/ASIACRYPT series of International Cryptologic Conferences in the Asia/Oceania area. She is presently Professor of Computer Science at the University of Wollongong. She has over 300 publications and has successfully supervised 22 Ph.D. theses.

Beata Joanna Wysocki graduated from Warsaw University of Technology receiving her M.E. (Electrical Engineering) in 1991. In 1994, she started the Ph.D. in the Australian Telecommunications Research Institute at Curtin University of Technology. In March 2000, she was awarded Ph.D. for the thesis: *Signal Formats for Code Division Multiple Access Wireless Networks*. During the Ph.D., she was involved in a research project Wireless ATM Hub at the Cooperative Research Centre for Broadband Telecommunications and Networking, and worked as a research assistant at Edith Cowan University within the ARC funded CDMA with enhanced protection against frequency selective fading and Reliable high rate data transmission over microwave local area networks. Since October 1999, she has been with the Telecommunications & Information Technology Research Institute at the University Wollongong as a research fellow. Her research interests include sequence design for direct sequence (DS) code division, multiple access (CDMA) data networks and error control strategies for broadband wireless access (BWA) systems.

Tadeusz Antoni Wysocki received the M.Sc.Eng. degree with distinction in telecommunications from the Academy of Technology and Agriculture, Bydgoszcz, Poland, in 1981. In 1984, he was awarded Ph.D. and in 1990, was awarded a D.Sc. (habilitation) in telecommunications from the Warsaw University of Technology. In 1992, Dr. Wysocki moved to Perth, Western Australia to work at Edith Cowan University. He spent the whole of the year 1993 at the University of Hagen, Germany, within the framework of Alexander von Humboldt Research Fellowship. After returning to Australia, he was appointed as a Program Leader, Wireless Systems, within Cooperative Research Centre for Broadband Telecommunications and Networking. Since December 1998, he has been working as an Associate Professor at the University of Wollongong, NSW, within the School of Electrical, Computer and Telecommunications Engineering. The main areas of Dr. Wysocki's research interests include: indoor propagation of microwaves, code division multiple access (CDMA), digital modulation and coding schemes, as well as mobile data protocols including those for ad hoc networks. He is the author or co-author of four books, over 100 research publications and nine patents. He is a Senior Member of IEEE.

Copyright © 2003 John Wiley & Sons, Ltd.