Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 7 (2012) pp. 252-258

Encryption Schemes from Williamson Matrices

Christos Koukouvinos[1] **and Dimitris E. Simos**[2]

[1]Department of Mathematics, National Technical University of Athens,
Zografou 15773, Athens, Greece
ckoukouv@math.ntua.gr

[2]Project-Team SECRET, INRIA Paris-Rocquencourt,
Le Chesnay Cedex 78153, Domaine de Voluceau - Rocquencourt B.P. 105, France
dimitrios.simos@inria.fr

Abstract: **In this paper, we propose an encryption scheme based on the famous Williamson construction for Hadamard matrices. The proposed cipher belongs to the class of symmetric cryptography. A cryptanalysis of the proposed scheme against some popular attacks, such as plaintext attacks and ciphertext attacks is explored and our study shows that these attacks does not compromise the security of the system. Furthermore, we make use of the Kronecker product to strengthen the proposed cipher while maintaining the private key size in reasonable lengths.**
Keywords: Cipher, Cryptography, Encryption, Williamson matrices, Hadamard matrices.

I. Introduction

In this paper, we propose a private symmetric key cipher based on constructions that have arisen using binary arrays of combinatorial designs. We were motivated to use the Williamson Hadamard matrices though they are part of a wider class, called combinatorial designs which are often hard to find and the algorithms for encryption and decryption are of reasonable length. By the term symmetric we mean that the same key is used both for encryption and decryption of a message. The respective cryptographic algorithms for the encryption and decryption process are called symmetric key block ciphers, and divide the original message which is going to be encrypted into blocks and encrypt each block separately. For encryption methods based on combinatorial designs we refer the interested reader to [20]. Applications of combinatorial designs to communications, cryptography and networking can be found in the survey paper, [5].

A. Specifications

The cipher has similarities to the Hill cipher, i.e. using the incidence matrix of a combinatorial design for encryption and decryption. For more details regarding the Hill encryption method, see [25, 19]. Moreover, we present a unified approach for iterated versions of these combinatorial design ciphers through the use of Kronecker product that approximate a k-round Feistel cipher or network ([19]). Widely known ciphers that use the block structure of a Feistel network are DES (Data Encryption Standard), Blowfish ([21]), FEAL ([24]) and the LOKI family of ciphers (LOKI89, LOKI91, [4]). A list of typical attacks and reference of the existing protocols can be found in ([8] and [3]), respectively. The design goals set for the combinatorial design ciphers include the following:

1. Require the key be shared only once
2. Use a relatively small key size
3. Computationally fast
4. Robust to most common cryptographic attacks

The ciphers we implement in this paper implement the first three goals. In addition, we demonstrate that the ciphers provide resistance to most common cryptographic attacks.
The encryption process can be described from the following procedure: consider a communications channel, we divide the channel into two subbands, one which will carry the message, and the other which will carry noise. The message, along with the noise is transmitted over the channel. The recipient then filters out the noise, leaving only the message. This procedure is carried out using Williamson Hadamard matrices.
This paper can be regarded as a continuation of the proposed schemes given in [12, 13, 14], and it is organized as follows. In Section II, we present the cryptographic algorithms used for the proposed encryption schemes. In Section III we design the encryption schemes using the Williamson Hadamard matrices, while in Section III-C we consider practical aspects of the proposed ciphers. Finally, in Section IV we study the security of the encryption schemes from Williamson matrices.

II. Cryptographic Algorithms

We assume that the message to be transmitted is a plaintext with n letters, which is represented by a vector of length n, whereas each coordinate of the vector is a numerical value of the corresponding letter of the plaintext (i.e. ASCII code). We note, that the design of cryptographic algorithms given here are a generalization of the ones given in [12] and similar to the ones proposed in [14], since in this paper we explore

the use of orthogonal matrices generated by combinatorial designs instead of orthogonal arrays.

If the message has more than n letters then the procedure which is given below, is being repeated as much times as needed. If it has less than n letters then we pad the plaintext with the letter "space" sufficient times. For the requirements of the proposed encryption method we will make use of a matrix A of order $n \times n$, of special structure, with entries $\{\pm 1\}$ where the matrix A satisfies $AA^T = kI_n$ for some constant $k \in IN$, where T stands for transposition and I_n is the identity matrix of order n. Design Theory is rich of such matrices of special structure having beautiful combinatorial properties, i.e. Hadamard matrices. For more details on the application of combinatorial designs in cryptography we refer the interested reader to [20, 5].

If the message we wish to transmit has been converted to a numerical vector $\bar{m}$, then the encrypted message which is going to be transmitted over a communication channel is

$$\bar{c} = \bar{m}A + d\bar{e}_n$$

where d is a suitable constant and $\bar{e}_n = (1, \ldots, 1)$ is a $1 \times n$ vector of ones. The receiver in order to decrypt the encrypt message has to make use of the transformation $\bar{m} = 1/k(\bar{c} - d\bar{e}_n)A^T$, where A^T is the transpose of the matrix A which has been used during the encryption. The encryption method described previously can be implemented with the following cryptographic algorithm given in [14].

Algorithm 1 Encryption Algorithm

function ENCRALG(msg)
Require: msg in ASCII code ▷ Encode a sample plaintext, msg
SELECT(A, d) ▷ Choose appropriate A and d
$k \leftarrow (A, d)$ ▷ Form private key k
TRANSMIT(k) ▷ Transmit securely the private key
$\bar{m} \leftarrow$ CONVERT(msg) ▷ Convert original msg
$\bar{c} \leftarrow \bar{m}A + d\bar{e}_n$ ▷ Encrypted msg is $\bar{c}$
return (TRANSMIT$(\bar{c})$)
end function

In order for the encryption method to be persistent with respect to the basic cryptographic principles, the encrypted message $\bar{c}$ has to be decrypted uniquely. This requirement is satisfied from the following theorem.

Theorem 1 (Koukouvinos and Simos [14]) *The encrypted message $\bar{c}$ which is transmitted with respect to the encryption algorithm is decrypted uniquely as $\bar{w} = 1/k(\bar{c} - d\bar{e}_n)A^T$ and $\bar{w} \equiv \bar{m}$.*

The decryption proccess uses the previous theorem as its cornerstone and is implemented with the following cryptographic algorithm, again given in [14].

III. Private-key Ciphers

In this Section, we provide several constructions for encryption schemes using one array of special structure. We give some necessary notations and definitions that we shall use throughout this paper. We note that all arrays that are used below can be considered as binary array bits with the aid of the following $\{1, -1\}$-bit notation taken from [16].

Algorithm 2 Decryption Algorithm

function DECRALG($\bar{c}$)
Require: given ciphertext $\bar{c}$ ▷ Decode a given ciphertext
RECEIVE(A, d) ▷ Receive the securely transmitted private key
$k \leftarrow (A, d)$ ▷ Set private key k
$\bar{m} \leftarrow 1/k(\bar{c} - d\bar{e}_n)A^T$ ▷ Decrypt ciphertext $\bar{c}$
$msg \leftarrow$ CONVERT$(\bar{m})$ ▷ Original plaintext is msg
return (msg)
end function

Definition 1 ($\{1, -1\}$-bit notation) *Sometimes, we find it convenient to view bits as being $\{1, -1\}$-valued instead of $\{0, 1\}$-valued. If $b \in \{0, 1\}$ then $\bar{b} \in \{1, -1\}$ is defined to be $\bar{b} = (-1)^b$. If $x \in \{0, 1\}^n$ then $\bar{x} \in \{1, -1\}^n$ is defined as the string where the i^{th} bit is $\bar{x}_i$.*

A cipher's strength is determined by the computational power needed to break it. The computational complexity of an algorithm is measured by two variables: T for time complexity which specifies how the running time depends on the size of the input, and S for space complexity or memory requirement. Both T and S are commonly expressed as functions of n, when n is the size of the input.

Generally, the computational complexity of an algorithm is expressed in what is called " big $\mathcal{O}$" notation; the order of magnitude of the computational complexity. We use $\mathcal{O}$-notation to give an upper bound on a function, to within a constant factor [6].

Definition 2 ($\mathcal{O}$-notation) *For a given function $g(n)$ we denote by $O(g(n))$ the set of functions $O(g(n)) = \{f(n) :$ there exist positive constants c and n_0 such that $0 \leq f(n) \leq cg(n)$ for all $n \geq n_0\}$.*

We give a necessary brief definition for an encryption scheme.

Definition 3 (Boyd and Mathuria [3]) *An encryption scheme consists of three sets: a key set K, a message set M, and a ciphertext set C together with the following three algorithms.*

1. *A key generation algorithm, which outputs a valid encryption key $k \in K$ and a valid decryption key $k^{-1} \in K$.*
2. *An encryption algorithm, which takes an element $m \in M$ and an encryption key $k \in K$ and outputs an element $c \in C$ defined as $c = E_k(m)$.*
3. *A decryption function, which takes an element $c \in C$ and a decryption key $k^{-1} \in K$ and outputs an element $m \in M$ defined as $m = D_k^{-1}(c)$. We require that $D_k^{-1}(E_k(m)) = m$.*

Remark 1 *We note that although we have used as a private key the pair (A, d), in terms of computational complexity henceforth we can refer to the private key using only the encryption matrix A since d is of size $\mathcal{O}(1)$.*

It is clear, that since we have an encryption algorithm and a decryption function we need a key generation algorithm in order to construct an encryption scheme. This key generation algorithm will be derived each time from a class of combinatorial designs, thus in the following sections we name the ciphers after the respective combinatorial structure used.

A. Williamson Ciphers

In this section, we use Williamson's construction for Hadamard matrices as the basis of our construction for a new private-key symmetric cryptosystem. We briefly describe the theory of Williamson's construction below.
Hadamard matrices are named after Jacques Hadamard, who found square matrices of orders 12 and 20, with entries ± 1, which had all their rows (and columns) orthogonal [10].

Definition 4 *A* Hadamard matrix *of order n is a square $n \times n$ matrix H whose elements are $+1$'s and -1's, with the property*

$$HH^T = nI_n$$

where T stands for transposition and I_n is the identity matrix of order n.
The Hadamard property entails that the rows (and columns) of a Hadamard matrix are pairwise orthogonal. It is well known that if n is the order of a Hadamard matrix then n is necessarily $1, 2$ or a multiple of 4. Hadamard matrices are used in Combinatorics, Statistics, Coding Theory, Telecommunications and other areas. More details on Hadamard matrices can be found in [7, 23].

Theorem 2 (Williamson [29]) *Suppose there exist four $(1, -1)$ matrices A, B, C, D of order n which satisfy*

$$XY^{\mathrm{T}} = YX^{\mathrm{T}}, X, Y \in \{A, B, C, D\}$$

Further, suppose

$$AA^{\mathrm{T}} + BB^{\mathrm{T}} + CC^{\mathrm{T}} + DD^{\mathrm{T}} = 4nI_n \tag{1}$$

Then

$$H = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix} \tag{2}$$

is an Hadamard matrix of order $4n$ constructed from a Williamson array.
We shall call such matrices, Williamson Hadamard matrices. Let the matrix T given below be called the shift matrix:

$$T = \begin{bmatrix} 0\,1\,0 & \cdots & 0 \\ 0\,0\,1 & \cdots & 0 \\ \cdots & \cdots & . \\ 0\,0\,0 & \cdots & 1 \\ 1\,0\,0 & \cdots & 0 \end{bmatrix} \tag{3}$$

and note

$$T^n = I,\ (T^i)^{\mathrm{T}} = T^{n-i} \tag{4}$$

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

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

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

Since A, B, C, D are symmetric, (1) becomes:

$$A^2 + B^2 + C^2 + D^2 = 4nI_n$$

and the relation $XY^{\mathrm{T}} = YX^{\mathrm{T}}$ becomes $XY = YX$ which is true for polynomials.

Definition 5 *Williamson matrices are $(1, -1)$ symmetric circulant matrices. As a consequence of being symmetric and circulant they commute in pairs.*
The scheme is constructed by using the Williamson Hadamard matrix $A = H_{4m}$ of order $n = 4m$ as an encryption matrix. However, in this case the circulant structure of symmetric matrices involved in the Williamson's construction gives us the opportunity to use a key of a significant less size than previously as follows.
In detail, for the encryption process is needed to construct the $(1, -1)$ circulant matrices:

$$\begin{array}{ll} A = [a_0, a_1, \ldots, a_{m-1}], & B = [b_0, b_1, \ldots, b_{m-1}], \\ C = [c_0, c_1, \ldots, c_{m-1}], & D = [d_0, d_1, \ldots, d_{m-1}], \end{array}$$

such that

$$A^2 + B^2 + C^2 + D^2 = 4mI_m. \tag{6}$$

The symmetry requirement gives $v_i = v_{m-i},\ i = 1, 2, \ldots, \frac{1}{2}(m-1),\ v_i \in \{a_i, b_i, c_i, d_i\}$.
The private key k for this scheme is the concatenation of the four vectors, A, B, C and D, denoted by $A_c \oplus B_c \oplus C_c \oplus D_c$ which consists of $m + m + m + m$ bits. Therefore, when a Williamson Hadamard matrix of order $n = 4m$ is used as an encryption matrix the key is of size $\mathcal{O}(n)$, since it consists of $n = 4m$ bits.

Proposition 1 *There exist a family of private-key ciphers using Williamson Hadamard matrices of order $n = 4m$, which will be called Williamson ciphers.*

Proof. The encryption scheme using a Williamson Hadamard matrix A of order $n = 4m$, will use a key $A_c \oplus B_c \oplus C_c \oplus D_c$ of size $\mathcal{O}(n)$, as described previously, and can be encrypted – decrypted using the algorithms of Section II since $AA^T = nI_n$.
An infinite family of Hadamard matrices of Williamson type has been proved to exist under certain conditions [28, 30]:

Theorem 3 *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 $C = D$, and A and 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.
Results for Hadamard matrices of Williamson type can be found on the web site of C. Koukouvinos ([11]) and in [9]. For example using the $\{1, -1\}$-bit notation and the four vectors $A = [1, -1, -1, -1, -1]$, $B = [1, -1, -1, -1, -1]$, $C = [1, 1, -1, -1, 1]$ and $D = [1, -1, 1, 1, -1]$ of length 5 from [11] we can construct a Williamson Hadamard matrix of order 20; which in the continuum will be used as an encryption matrix in Proposition 1 with a key $k = A \oplus B \oplus C \oplus D = 01111011110011001001$ of length equal to 20 bits to generate the corresponding Williamson cipher.

B. Kronecker Williamson Ciphers

Most block ciphers are constructed by repeatedly applying a simpler function. This approach is known as iterated block

cipher (or product cipher). Each iteration is termed a round, and the repeated function is termed the round function; anywhere between 4 to 32 rounds are typical. We present here a unified approach for all the combinatorial design block ciphers using Kronecker product. The product cipher will consist of a series of Kronecker products applied between the encryption matrices of the same type of the combinatorial design ciphers we have presented so far. Our goal is to achieve that the resulting cipher will be more secure than the individual components, thus making it resistant to cryptanalysis. We note that, this approach shares many similarities with the design of a k-round Feistel network of ciphers.

In particular, we apply the "blow-up" construction of encryption schemes first given in [12], which relies on the previous encryption schemes and the Kronecker product as its main characteristics. We first define the Kronecker product $A \otimes B$ between two matrices A and B, a crucial definition for the construction of this family of product ciphers.

Definition 6 ([15]) *Let* $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & & \ddots & \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$ *Then* $A \otimes B := \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ \vdots & & \ddots & \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{pmatrix}$

If A is an $m \times n$ and B is an $p \times q$ matrix, then $A \otimes B$ is an $mp \times nq$ matrix. We note that if A and B are orthogonal matrices, then $A \otimes B$ is also an orthogonal matrix. We specialise in the case of combinatorial designs, where the round function is one use of the Kronecker product.

Proposition 2 (Sylvester [27]) *Let H_1 and H_2 be Hadamard matrices of orders m and n, respectively. Then the Kronecker product $H_1 \otimes H_2$ is a Hadamard matrix of order mn.*

Remark 2 *We can repeat the previous construction using p Hadamard matrices $H_1, H_2, \dots, H_p$ of orders $n_1, n_2, \dots, n_p$. Thus the Kronecker product $\bigotimes_{i=1}^{p} H_i := H_1 \otimes H_2 \otimes \dots \otimes H_p$ is a Hadamard matrix of order $\prod_{i=1}^{p} n_i$.*

We illustrate the construction of a Kronecker Williamson cipher with the following example.

Example 1 *Let H_i, for $i = 1, \dots, k$ be Williamson Hadamard matrices of orders $n_i = 4m_i$, for $i = 1, \dots, k$ respectively. These matrices associated with their corresponding encryption keys $A_{c_i} \oplus B_{c_i} \oplus C_{c_i} \oplus D_{c_i} = [a_{1_i}, a_{2_i}, \dots, a_{m_i}] \oplus [b_{1_i}, b_{2_i}, \dots, b_{m_i}] \oplus [c_{1_i}, c_{2_i}, \dots, c_{m_i}] \oplus [d_{1_i}, d_{2_i}, \dots, d_{m_i}] = [a_{1_i}, a_{2_i}, \dots, a_{m_i}, b_{1_i}, b_{2_i}, \dots, b_{m_i}, c_{1_i}, c_{2_i}, \dots, c_{m_i}, d_{1_i}, d_{2_i}, \dots, d_{m_i}]$ for $i = 1, \dots, k$ where each private key $A_{c_i} \oplus B_{c_i} \oplus C_{c_i} \oplus D_{c_i}$ consists of $4m_i$ bits, form a k-family of encryption schemes or a k-round product cipher. If we consider the Kronecker product $\bigotimes_{i=1}^{k} H_i$ of these matrices, the generated matrix is a Hadamard matrix of order $\prod_{i=1}^{k} n_i$. Since a recipient can construct each individual Williamson Hadamard matrix H_i by assuming knowledge of the corresponding private key $A_{c_i} \oplus B_{c_i} \oplus C_{c_i} \oplus D_{c_i}$, the matrix generated by the Kronecker product can be used as an encryption matrix where its private key $\bigoplus_{i=1}^{k}(A_{c_i} \oplus B_{c_i} \oplus C_{c_i} \oplus D_{c_i})$ is the concatenation of the private keys $A_{c_i} \oplus B_{c_i} \oplus C_{c_i} \oplus D_{c_i}$, which consists of $\sum_{i=1}^{k} 4m_i = 4k \sum_{i=1}^{k} m_i$ bits. Let n denote the largest order of the Williamson Hadamard matrices we have used, i.e. $n = \max_i\{n_i\}$. In terms of computational complexity, since $\prod_{i=1}^{k} n_i \leq \prod_{i=1}^{k} n = n^k$, the size of the encryption matrix is of exponential growth $\mathcal{O}(n^k)$. However, the size of the private key grows linearly since $\sum_{i=1}^{k} 4m_i = \sum_{i=1}^{k} n_i \leq \sum_{i=1}^{k} n = nk$, therefore its growth is of size $\mathcal{O}(n)$.*

C. Encryption in Practice

We can now discuss in detail this weakness in the design of the Williamson ciphers which in some cases can be eliminated using their iterated versions of product ciphers, i.e. the Kronecker Williamson ciphers. As already noted, in cases the plaintext has more than n letters, we repeat the encryption process. This method, is also known as the *electronic codebook* mode, or ECB in the literature ([8, 17, 19, 26, 22]). A disadvantage of this method is that if two plaintext blocks are the same, then the corresponding ciphertext blocks will be identical, and that is visible to the attacker.

The "blow-up" construction can reduce the amount of information that can be retrieved from a potential attacker when using ECB mode by restricting the available choices for Williamson Hadamard matrices A_i, $i = 1, \dots, k$ to be $A_f \neq A_g$ for $i \leq f, g \leq k$ with $f \neq g$. In general, if we choose the A_i encryption matrices to have $\sum_{i=1}^{k} n_i = n$, where n is the size of the plaintext this weakness is eliminated since the encryption process does not have any repetition blocks.

IV. Cryptanalysis

The main cryptographic attacks can be classified in the following three categories:

- brute force attack.
- plaintext attack.
- ciphertext attack.

Modern cryptographic hardware breakers have the ability to perform a brute-force search for 2^{128} keys. This gives us an estimate of the security needed against brute force attacks. Clearly, the usage of any Williamson Hadamard matrix of order $n > 128$, which can easily be constructed from Theorem 2 for large orders in conjunction with the results for the circulant matrices given in [11] and [9], as an encryption matrix is recommended for protection against brute-force attacks.

In this section, we demonstrate that our ciphers are robust against ciphertext-only attacks, while considering some restrictions the corresponding encryption schemes are secure

under known-plaintext attacks, chosen-plaintext attacks and chosen-ciphertext attacks.

A. Cryptanalysis of Known-plaintext Attacks for Williamson Ciphers

Definition 7 (Known-plaintext Attack) *A known-plaintext attack is one where the adversary has a quantity of plaintext and corresponding ciphertext. This type of attack is typically only marginally more difficult to mount.*

Supposing a $n \times n$ matrix A is used for encryption, as described previously. In order to recover the matrix $A = H_n$ of a Williamson cipher without knowing the private key, we will need n $\overline{m}^i$'s, where with $\overline{m}^i = (m_1^i,\ m_2^i,\ \ldots,\ m_n^i),\ i = 1,\ \ldots,\ n$ we denote the vector consisting of n letters of the message that have been converted to its numerical values, and n $\overline{c}^i$'s, where each $\overline{c}^i = (c_1^i,\ c_2^i,\ \ldots,\ c_n^i)$ is the encryption of $\overline{m}^i$. The i-th column of A, $A(i) = (a_{1,i},\ a_{2,i},\ \ldots,\ a_{n,i})$, by solving the following n-linear systems, for $i = 1,\ \ldots,\ n$:

$$\begin{aligned} m_1^1 a_{1,i} + m_2^1 a_{2,i} + \ldots + m_n^1 a_{n,i} &= c_i^1 \\ m_1^2 a_{1,i} + m_2^2 a_{2,i} + \ldots + m_n^2 a_{n,i} &= c_i^2 \\ \vdots \qquad\qquad\qquad\qquad\quad &\ \ \vdots \\ m_1^n a_{1,i} + m_2^n a_{2,i} + \ldots + m_n^n a_{n,i} &= c_i^n \end{aligned}$$

or equivalently we denote the previous system

$$MA(i) = C(i)\ ,$$

where $C(i) = (c_i^1,\ c_i^2,\ \ldots,\ c_i^n)$.

Proposition 3 *Williamson ciphers are secure against known-plaintext attacks under the assumption that the adversary has knowledge of less than n messages of length n of the plaintext and the corresponding ciphertext.*

Proof. With the method described previously one can find the encryption matrix A, if the matrix M is not singular.

B. Cryptanalysis of Chosen-plaintext Attacks for Williamson Ciphers

Definition 8 (Chosen-plaintext Attack) *A chosen-plaintext attack is one where the adversary chooses plaintext and is then given corresponding ciphertext. Subsequently, the adversary uses any information deduced in order to recover plaintext corresponding to previously unseen ciphertext.*

In this type of attack the extra advantage of the adversary having knowledge of the encryption mechanism, does not reveal any further information with respect to a known-plaintext attack since the adversary in order to compromise the system still has to solve n linear systems,

$$MA(i) = C(i)$$

for $i = 1, \ldots, n$ as described in section IV-A.

Remark 3 *The adversary should take under account that the matrix M of the chosen plaintext must not be singular. This note restricts the choice of the available plaintexts for an adversary since $\overline{m}^i \neq \lambda \overline{m}^j$, in other words the vectors $\overline{m}^i$ must be linear independent.*

Proposition 4 *Williamson ciphers are secure against chosen-plaintext attacks, since the schemes are secure against known-plaintext attacks.*

C. Cryptanalysis of Chosen-ciphertext Attacks for Williamson Ciphers

Definition 9 (Chosen-ciphertext Attack) *A chosen-ciphertext attack is one where the adversary selects the ciphertext and is then given the corresponding plaintext. One way to mount such an attack is for the adversary to gain access to the equipment used for decryption (but not the decryption key, which may be securely embedded in the equipment). The objective is then to be able, without access to such equipment, to deduce the plaintext from (different) ciphertext.*

Similar, in this type of attack the extra advantage of the adversary having knowledge of the encryption mechanism, does not reveal any further information with respect to a known-plaintext attack since the adversary in order to compromise the system still has to solve n linear systems,

$$MA(i) = C(i)$$

for $i = 1, \ldots, n$ as described in section IV-A.

Proposition 5 *Williamson ciphers are secure against chosen – ciphertext attacks, since the schemes are secure against known – plaintext attacks.*

D. Cryptanalysis of Known-plainext, Chosen-plaintext and Ciphertext Attacks for Kronecker Williamson Ciphers

An intriguing question is if the security provided by the Williamson ciphers is enough for standard applications (i.e. banking transactions) in practice. Clearly, the security is a function of the value n of the plaintext's length. For example, with a plaintext of $n = 64$ bits an attacker which can deduce $64 = 2^6$ messages of the same length can break the ciphers and of course this is totally impractical!

The solution to this problem is to use the Kronecker Williamson ciphers. For example, using 16 rounds of encryption i.e. the Kronecker product of 16 Williamson Hadamard matrices of order 16 the size of the encryption matrix is $2^{4^{16}} = 2^{64}$, while the key size is $16 \cdot 16 = 256$ bits. Therefore, using a key of 256 bits we provide security for 2^{64} known and chosen-plaintexts and ciphertexts. We compare now this result with the security of a widely known modern block cipher, i.e. DES.

1. To break the full 16-rounds of DES, Bilham and Shamir showed that differential cryptanalysis requires 2^{47} chosen plaintexts (see [1, 2]).

2. Linear cryptanalysis discovered by Matsui needs 2^{43} known plaintexts to achieve similar results (see [18]).

E. Cryptanalysis of Ciphertext-only Attacks for Williamson Ciphers

Definition 10 (Ciphertext-only Attack) *A ciphertext-only attack is one where the adversary (or cryptanalyst) tries to deduce the decryption key or plaintext by only observing ciphertext. Any encryption scheme vulnerable to this type of attack is considered to be completely insecure.*

Two letters of the original message, m corresponds to different values of the ciphertext, $\overline{c}$. Analysing the worst-case scenario for this type of attack, we suppose that all letters of

the plaintext are the same. Then in the corresponding ciphertext all their numerical values are all different. Therefore an adversary cannot observe any further information regarding the encryption key or the plaintext, since any value of the encrypted message is a function of n values of the plaintext and one column of the encryption matrix A. Hence, two or more same values of the encrypted message does not represent the same letter in the plaintext. We note that, as n increases it is more difficult for an adversary to retrieve the encryption key or the plaintext by simple observation.

Proposition 6 *Williamson ciphers are secure against ciphertext-only attacks.*

Acknowledgments

The second author acknowledges that this work was carried out during the tenure of an ERCIM "Alain Bensoussan" Fellowship Programme. This Programme is supported by the Marie Curie Co-funding of Regional, National and International Programmes (COFUND) of the European Commission.

References

[1] E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In *Advances in Cryptology CRYPTO '90*, pp. 2-21, 1990.

[2] E. Biham and A. Shamir. Differential Cryptanalysis of the Full 16-Round DES. In *Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology - CRYPTO '92*, pp. 487-496, 1992.

[3] C. Boyd and A. Mathuria. *Protocols for Authentication and Key Establishment*, Information Security and Cryptography Series, Springer-Verlag, Heidelberg, 2003.

[4] L. Brown, J. Pieprzyk and J. Seberry. LOKI - A Cryptographic Primitive for Authentication and Secrecy Applications. In *Proceedings of the International Conference on Cryptology: Advances in Cryptology - AUSCRYPT '90*, pp. 229-236, 1990.

[5] C.J. Colbourn, J.H. Dinitz and D.R. Stinson. Applications of combinatorial designs to communications, cryptography, and networking, in *Surveys in Combinatorics*, J.D. Lamb and D.A. Preece (eds.), Cambridge University Press, Cambridge, pp. 37-100, 1999.

[6] T.H. Cormen, C.H. Leiserson, R.L. Rivest and C. Stein. *Introduction to Algorithms*, MIT Press, 2003.

[7] R. Craigen. Hadamard Matrices and Designs, in *The CRC Handbook of Combinatorial Designs*, C.J. Colbourn and J.H. Dinitz (eds.), CRC Press, Boca Raton, Fla., pp. 370-377, 1996.

[8] N. Ferguson and B. Schneier. *Practical Cryptography*, Wiley Publishing, Inc., 2003.

[9] S. Georgiou, C. Koukouvinos and J. Seberry. Hadamard matrices, orthogonal designs and construction algorithms, in *Designs 2002: Further Computational and Constructive Design Theory*, W.D. Wallis (eds.), Kluwer Academic Publishers, Norwell, Massachusetts, pp. 133-205, 2003.

[10] J. Hadamard. Resolution d'une question relative aux determinants, *Bull. des. Sci. Math.*, 17, pp. 240-246, 1893.

[11] C. Koukouvinos. Williamson matrices, [Online]. Available: http://www.math.ntua.gr/ ckoukouv/designs.htm

[12] C. Koukouvinos, E. Lappas and D.E. Simos. Encryption schemes using orthogonal arrays, *J. Discrete Math. Sci. Cryptogr.*, 12, pp. 615-628, 2009.

[13] C. Koukouvinos and D.E. Simos. Encryption schemes using plotkin arrays, *Appl. Math. & Inf. Sci.*, 5, pp. 500-510, 2011.

[14] C. Koukouvinos and D. E. Simos. Encryption schemes based on hadamard matrices with circulant cores. submitted for publication.

[15] J.H. van Lint and R.M. Wilson. *A Course in Combinatorics*, Cambridge University Press, Cambridge, 1992.

[16] M. Luby. *Pseudorandomness and Cryptographic Applications*, Princeton Academic Press, Princeton, 1996.

[17] W. Mao. *Modern Cryptography: Theory and Practice*, Prentice Hall, 2004.

[18] M. Matsui. Linear cryptanalysis method for DES cipher. In *Workshop on the theory and application of cryptographic techniques on Advances in cryptology - EUROCRYPT '93*, pp. 386-397, 1993.

[19] A. Menezes, P. van Oorschot and S. Vanstone. *Handbook of Applied Cryptography*, CRC Press, 1997.

[20] D.G. Sarvate and J. Seberry. Encryption methods based on combinatorial designs, *Ars Combinatoria*, 21-A, pp. 237-246, 1986.

[21] B. Schneier. Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish). In *Proceedings of Fast Software Encryption*, pp. 191-204, 1993.

[22] B. Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition, J. Wiley and Sons Inc., New York, 1996.

[23] J. Seberry and M. Yamada. Hadamard matrices, sequences and block designs, in *Contemporary Design Theory: A Collection of Surveys*, J.H. Dinitz and D.R. Stinson (eds.), J. Wiley & Sons, New York, pp. 431-560, 1992.

[24] A. Shimizu and S. Miyaguchi. Fast data encipherment algorithm FEAL. In *Proceedings of the 6th annual international conference on Theory and application of cryptographic techniques - EUROCRYPT '87*, pp. 267-280, 1988.

[25] W. Stallings. *Cryptography and Network Security: Principles and Practices*, 3rd Edition, Prentice Hall, 2003.

[26] D.R. Stinson. *Cryptography: Theory and Practice*, 3rd Edition, CRC Press, 2005.

[27] J.J. Sylvester. Thoughts on inverse orthogonal matrices, simultaneous sign-successions, and tessellated pavements in two or more colors, with applications to Newtons rule, ornamental tile-work, and the theory of numbers, *Phil. Mag.*, 34, pp. 461-475, 1867.

[28] R.J. Turyn. An infinite class of Williamson matrices, *J. Combin. Theory Ser. A*, 12, pp. 319-321, 1972.

[29] J. Williamson. Hadamard's determinant theorem and the sum of four squares, *Duke Math. J.*, 11, pp. 65-81, 1944.

[30] A.L. Whiteman. An infinite family of Hadamard matrices of Williamson type. *J. Combin. Theory Ser. A*, 14, pp. 334-340, 1973.

Author Biographies

Christos Koukouvinos is a Professor at the National Technical University of Athens, Department of Mathematics. He holds a Bachelor in Mathematics (1983) and a PhD (1988) in Statistics both obtained from the University of Thessaloniki. He is the author of numerous papers in the field of Combinatorics and Statistics and on the Editorial board of seven related journals. He was awarded the prestigious Hall Medal of the Institute of Combinatorics and its Applications (ICA) in 1996. He is a Fellow of the ICA and was member of Council of the ICA from 2000 to 2003. His research interests include combinatorial designs, statistical experimental and optimal designs and coding theory.

Dimitris E. Simos is an ERCIM/Marie Curie Fellow within Project-Team SECRET of INRIA Paris-Rocquencourt. He received his Bachelor in Mathematics (2006) from the University of Athens, and MSc in Applied Mathematical Sciences (2007) from the National Technical University of Athens. He holds a PhD in Discrete Mathematics and Combinatorics since 2011. He is the author of several papers in the field of Combinatorics and on the Ediorial board of three related journals. He is also a Fellow of the Institute of Combinatorics and its Applications (ICA). His research interests include combinatorial designs, coding theory, cryptography, symbolic computation and metaheuristics.