Journal of Applied Mathematics & Bioinformatics, vol.3, no.1, 2013, 17-41
ISSN: 1792-6602 (print), 1792-6939 (online)
Scienpress Ltd, 2013

Encryption Schemes based on Hadamard Matrices with Circulant Cores

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

Abstract

In this paper, we propose two encryption schemes based on Hadamard matrices with one and two circulant cores, which are classes of combinatorial designs. A cryptanalysis of the proposed schemes against some popular attacks, brute force, 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 our encryption schemes while maintaining the private key size in reasonable lengths.

Mathematics Subject Classification: 94A60, 68P25, 05B15, 05B20
Keywords: Cipher, Encryption, Cryptography, Hadamard matrices

[1] Department of Mathematics, National Technical University of Athens, Zografou 15773, Athens, Greece, e-mail: ckoukouv@math.ntua.gr
[2] Project-Team SECRET, INRIA Paris-Rocquencourt, 78153 Le Chesnay Cedex, Domaine de Voluceau - Rocquencourt B.P. 105, France, e-mail: dimitrios.simos@inria.fr

Article Info: *Received* : November 1, 2012. *Revised* : January 30, 2013
Published online : March 30, 2013

1 Introduction

In this paper, we propose private symmetric key cipher based on several constructions that have arisen using binary arrays of combinatorial designs. We were motivated to use 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. For encryption methods based on combinatorial designs we refer the interested reader to [23]. Applications of combinatorial designs to communications, cryptography and networking can be found in the survey paper, [2]. 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 [30]. A list of typical attacks and reference of the existing protocols can be found in ([5] and [1]), respectively. Our design goals include the following:

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

This paper can be regarded as a continuation of the proposed schemes given in [15], and it is organized as follows. In Section 2, we present the concept of our encryption schemes. In Section 3 we design the encryption schemes using Hadamard matrices with circulant cores, while in Section 4 we study the security of the proposed schemes. Finally in Section 5 we enhance the strength of our cryptographic schemes using the Kronecker product.

2 Design of 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 [15], since in this paper we explore the use of orthogonal matrices 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 $k \in \mathbb{N}$, 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 [23, 2].

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.

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 2.1. *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 $\bar{w} \equiv \bar{m}$.*

Proof. $\bar{c} = \bar{m}A + d\bar{e}_n \Rightarrow \bar{c} - d\bar{e}_n = \bar{m}A \Rightarrow 1/k(\bar{c} - d\bar{e}_n)A^T = 1/k(\bar{m}AA^T) \Rightarrow 1/k(\bar{c} - d\bar{e}_n)A^T = \bar{m}I_q \Rightarrow \bar{m} = 1/k(\bar{c} - d\bar{e}_n)A^T$. □

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$(\bar{m})$	Encrypted msg is $\bar{c}$

Return(msg)

End Function

3 Encryption Schemes using Hadamard Matrices

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 [17].

$\{1,-1\}$-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 [3].

$\mathcal{O}$-notation For a given function $g(n)$ we denote by $\mathcal{O}(g(n))$ the set of functions $\mathcal{O}(g(n)) = \{f(n) :$ 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 3.1 ([1]). *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 3.2. *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 $\mathcal{O}(1)$.*

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 [11].

Definition 3.3. *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 [4, 27].

As an encryption matrix for this scheme we will use a Hadamard matrix of order n. In the case of Hadamard matrices it is obvious that the use of two different Hadamard matrices of the same order will result in two different ciphertexts, due to the presence of the H-equivalence property described below.

Two Hadamard matrices are called equivalent (or Hadamard equivalent, or H-equivalent) if one can be obtained from the other by a sequence of row negations, row permutations, column negations and column permutations. More specifically, two Hadamard matrices are equivalent if one can be obtained by the other by a sequence of the following transformations:

- Multiply rows and/or columns by -1;
- Interchange rows and/or columns.

Two Hadamard matrices are called inequivalent, if they are not equivalent. Therefore, the choice of inequivalent Hadamard matrices as encryption matrices ensures that two inequivalent Hadamard matrices will result in two different ciphertexts. Otherwise one could transform the one encryption matrix to another, following the transformations mentioned above.

It is vital for our application to have large databases of inequivalent matrices to our disposal. As of release 2.13, Magma contains a database of inequivalent Hadamard matrices. There exist several thousands (even millions) of inequivalent Hadamard matrices for some orders. As an example for order 32 which is a reasonable length for the encryption process there are more than $3,578,006$ inequivalent Hadamard matrices [20].

The private key k used in the encryption process, will be the Hadamard matrix of order n, $A = H_n$, which consists of $n \times n$ bits. In terms of computational complexity, the size of the key is $\mathcal{O}(n^2)$.

Proposition 3.4. *There exist an ecryption scheme using Hadamard matrices of order n.*

Proof. The encryption scheme using a Hadamard matrix A of order n, will use a key k of size $\mathcal{O}(n^2)$, as described previously, and can be encrypted – decrypted using the algorithms of section 2 since $AA^T = nI_n$. □

There are some special constructions of Hadamard matrices which enable us to reduce the size complexity of the private key.

3.1 Schemes based on Hadamard matrices with one circulant core

A Hadamard matrix of order $p + 1$ which can be written in one of the two equivalent forms

$$\begin{array}{c|c} 1 & 1\cdots 1 \\ \hline 1 & \\ \vdots & C \\ 1 & \end{array} \qquad \text{or} \qquad \begin{array}{c|c} 1 & \\ \vdots & C \\ 1 & \\ \hline 1 & -1\cdots -1 \end{array}$$

where $C = (c_{ij})$ is a circulant matrix of order p i.e. $c_{ij} = c_{1,j-i+1(\text{mod p})}$, is said to have a circulant core. The following matrices are examples for order 12.

1	1	1	1	1	1	1	1	1	1	1	1
1	-	1	-	1	1	1	-	-	-	1	-
1	-	-	1	-	1	1	1	-	-	-	1
1	1	-	-	1	-	1	1	1	-	-	-
1	-	1	-	-	1	-	1	1	1	-	-
1	-	-	1	-	-	1	-	1	1	1	-
1	-	-	-	1	-	-	1	-	1	1	1
1	1	-	-	-	1	-	-	1	-	1	1
1	1	1	-	-	-	1	-	-	1	-	1
1	1	1	1	-	-	-	1	-	-	1	-
1	-	1	1	1	-	-	-	1	-	-	1
1	1	-	1	1	1	-	-	-	1	-	-

1	1	-	1	-	-	-	1	1	1	-	1
1	1	1	-	1	-	-	-	1	1	1	-
1	-	1	1	-	1	-	-	-	1	1	1
1	1	-	1	1	-	1	-	-	-	1	1
1	1	1	-	1	1	-	1	-	-	-	1
1	1	1	1	-	1	1	-	1	-	-	-
1	-	1	1	1	-	1	1	-	1	-	-
1	-	-	1	1	1	-	1	1	-	1	-
1	-	-	-	1	1	1	-	1	1	-	1
1	1	-	-	-	1	1	1	-	1	1	-
1	-	1	-	-	-	1	1	1	-	1	1
1	-	-	-	-	-	-	-	-	-	-	-

Where $-$ stands for -1 to conform with the customary notation for Hadamard matrices. The two forms are equivalent as described earlier.

The scheme is constructed by using the previous Hadamard matrix $A = H_n$ of order $n = 4m = p + 1$ as an encryption matrix. However, in this case the

circulant structure of the Hadamard matrix gives us the opportunity to use a key of a significant less size than previously as follows.

Let $A_c = [a_1, a_2, \ldots, a_p]$ denote the first row of the circulant matrix, C used in the one circulant core construction previously. The private key k for this scheme is the binary vector, A_c which consists of p bits. Therefore, when a Hadamard matrix of order $n = p + 1$ is used as an encryption matrix the key is of size $O(n)$, since it consists of $p = n - 1$ bits.

Proposition 3.5. *There exist an ecryption scheme using Hadamard matrices with one circulant core of order $n = p + 1$.*

Proof. The encryption scheme using a Hadamard matrix A with one circulant core of order $n = p + 1$, will use a key k of size $\mathcal{O}(n)$, as described previously, and can be encrypted – decrypted using the algorithms of section 2 since $AA^T = nI_n$. □

Four families of these kinds of Hadamard matrices have been found by Paley [21], Stanton, Sprott and Whiteman [29, 33], Singer [28] and Marshall Hall Jr. [12], which can be used in the previous proposition and give rise to infinite families of encryption schemes based on Hadamard matrices with one circulant core. The following theorem was given in [13].

Theorem 3.6 (Circulant Core Hadamard Construction Theorem). *A Hadamard matrix of order $p + 1$ with circulant core can be constructed if*

1. $p \equiv 3 (\mathrm{mod}\ 4)$ *is a prime [21];*
2. $p = q(q + 2)$ *where q and $q + 2$ are both primes [29, 33];*
3. $p = 2^t - 1$ *where t is a positive integer [28];*
4. $p = 4x^2 + 27$ *where p is a prime and x a positive integer [12].*

3.2 Schemes based on Hadamard matrices with two circulant cores

A Hadamard matrix of order $2\ell + 2$ (for ℓ odd) which can be written in one

of the two equivalent forms ($-$ stands for -1 and $+$ stands for $+1$)

$$\left[\begin{array}{cc|ccc|ccc} - & - & + & \cdots & + & + & \cdots & + \\ - & + & + & \cdots & + & - & \cdots & - \\ \hline + & + & & & & & & \\ \vdots & \vdots & & A & & & B & \\ + & + & & & & & & \\ \hline + & - & & & & & & \\ \vdots & \vdots & & B^T & & & -A^T & \\ + & - & & & & & & \end{array}\right] \quad \text{or} \quad \left[\begin{array}{cc|ccc} + & + & & & \\ \vdots & & & A & & B \\ + & + & & & \\ \hline + & - & & & \\ \vdots & & & B^T & & -A^T \\ + & - & & & \\ \hline - & - & + & \cdots & + \quad + & \cdots & + \\ - & + & + & \cdots & + \quad - & \cdots & - \end{array}\right]$$

where $A = (a_{ij})$, $B = (b_{ij})$ are two circulant matrices (with ± 1 elements) of order ℓ i.e. $a_{ij} = a_{1,j-i+1(\text{mod } \ell)}$, $b_{ij} = b_{1,j-i+1(\text{mod } \ell)}$, is said to have two circulant cores.

As before the scheme is constructed by using the previous Hadamard matrix $A = H_n$ of order $n = 2\ell + 2$ as an encryption matrix. However, in this case the circulant structure of the Hadamard matrix gives us the opportunity to use a key of a significant less size than previously as follows.

Let $A_c = [a_1, a_2, \ldots, a_\ell]$ and $B_c = [b_1, b_2, \ldots, b_\ell]$ denote the first row of the circulant matrices, A and B used in the two circulant core construction respectively. The private key k for this scheme is the concatenation of the two vectors, A_c and B_c, denoted by $A_c \oplus B_c$ which consists of $\ell + \ell$ bits. Therefore, when a Hadamard matrix of order $n = 2\ell + 2$ is used as an encryption matrix the key is of size $\mathcal{O}(n)$, since it consists of $2\ell = n - 2$ bits.

Proposition 3.7. *There exist an ecryption scheme using Hadamard matrices with two circulant cores of order $n = 2\ell + 2$.*

Proof. The encryption scheme using a Hadamard matrix A with with two circulant cores of order $n = 2\ell + 2$, will use a key $k = A_c \oplus B_c$ of size $\mathcal{O}(n)$, as described previously, and can be encrypted – decrypted using the algorithms of section 2 since $AA^T = nI_n$. □

Since $2\ell + 2$ must be equal to a multiple of 4 we have that ℓ must be an odd integer for this construction to yield a Hadamard matrix.

Georgiou, Koukouvinos and Seberry [8] point out that GL-pairs, which can be used to construct Hadamard matrices of order $2\ell+2$ with two circulant cores,

exist for many cases. These matrices can be used in the previous proposition and give rise to infinite families of encryption schemes based on Hadamard matrices with two circulant cores. The following theorem was given in [14].

Theorem 3.8. (Two Circulant Cores Hadamard Construction Theorem)
An Hadamard matrix of order $2\ell + 2$ with with two circulant cores can be constructed if

1. *ℓ is a prime (see for example [6]);*
2. *$2\ell + 1$ is a prime power (these arise from Szekeres difference sets, see for example [6] or [9]);*
3. *$\ell = 2^k - 1$, $k \geq 2$ (two Galois sequences are a GL-pair, see for example [25]);*
4. *$\ell = p(p + 2)$ where p and $p + 2$ are both primes (two such sequences are a GL-pair,see for example, [29, 33]);*
5. *$\ell = 49, 57$ (these have been found by a non-exhaustive computer search that uses generalized cyclotomy and master-switch techniques, see [9, 10]);*
6. *$\ell = 3, 5, \ldots, 45$ (these have been found and classified by exhaustive computer searches, see [6]);*
7. *$\ell = 47, 49, 51, 53$ and 55 (these have been found and classified by partial computer searches, see [6]);*
8. *$\ell = 143$ (also verified the results for $\ell = 3$, 5, 7, 11, 13, 15, 17, 19, 23, 25, 31, 35, 37, 41, 43, 53, 59, 61, 63 see [7]).*

4 Security of the Method: Cryptanalytic Approaches

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

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

In this section we demonstrate that our ciphers are robust against brute force attacks and ciphertext-only attacks, whilst considering some restrictions the corresponding encryption schemes are secure under known-plaintext attacks, chosen-plaintext attacks and chosen-ciphertext attacks.

4.1 Cryptanalysis of brute force attacks

Definition 4.1 (Brute force attack). *A brute force attack is a method of defeating a cryptographic scheme by trying a large number of possibilities. For most ciphers, a brute force attack typically means a brute-force search of the key space; that is, testing all possible keys in order to recover the plaintext used to produce a particular ciphertext.*

One way for an adversary to break any of the proposed systems using brute force attack, is to generate all possible matrices with elements ± 1, that is 2^{n^2} matrices, having in mind that Hadamard matrices of order n are represented by n^2 bits. However due to the structure of these matrices there exists a more sophisticated method that would be developed next.

4.1.1 Cryptanalysis of brute force attacks for schemes based on Hadamard matrices with one circulant core

In order for an adversary to break this system using a brute force attack, he would have to deduce the encryption key $k = A_c$, which is the binary vector $A_c = [a_1, a_2, \ldots, a_p]$ of length p by trying a large number of possibilities.

In our case, an adversary would have to simulate a brute force search of the key space. Assuming the adversary has knowledge of the encryption protocol he would have to search on p binary variables. Since, the encryption key consists of binary variables using enumerative combinatorics, the size of the

key space, $K(\mathcal{H}_p)$, is $\mid K(\mathcal{H}_p) \mid = 2^p$ therefore its computational complexity is of exponential growth $\mathcal{O}(2^n)$ as $n = p + 1$ increases. Furthermore, the possibility a solution obtained from a brute-force search of the key space to be an encryption key is given by the total number of Hadamard matrices with one circulant core that exist in a specific order divisible by the size of the key space in that order.

For example, if we consider schemes that are using the Hadamard matrices of order $24 = 23 + 1$, the key space consists of 23 binary variables while the total number of Hadamard matrices that exist in that order are 46, therefore we have 46 possible encryption keys. As can be seen in the following table, the probability of breaking the system via a brute force attack for this case is $P = \frac{46}{2^{23}} \approx 0.00002$, only. It is worthwhile to note that using a key of length only 23 bits we almost provide total security against brute force attacks for this scheme.

We summarize in the following table the available Hadamard matrices with one circulan core, denoted by $\mid V(\mathcal{H}_p) \mid$, for orders $n = p + 1$ whereas $\ell = 3, 7, 11, 15, 19, 23$ using the results obtained via exhaustive searches in [13], the cardinality of the key space $\mid K(\mathcal{H}_p) \mid$, and the probability P_{BA} of breaking the cipher via a brute force attack for each order.

Table 1: Probabilities of breaking the cipher for different key sizes

p	matrix order	$\mid V(\mathcal{H}_p) \mid$	$\mid K(\mathcal{H}_p) \mid = 2^p$	$P_{BA} = \frac{\lvert V(\mathcal{H}_p)\rvert}{\lvert K(\mathcal{H}_p)\rvert}$
3	4	3	2^3	$P = \frac{3}{2^3} \approx 0.375$
7	8	14	2^7	$P = \frac{14}{2^7} \approx 0.1$
11	12	22	2^{11}	$P = \frac{22}{2^{11}} \approx 0.01$
15	16	30	2^{15}	$P = \frac{30}{2^{15}} \approx 0.0009$
19	20	38	2^{19}	$P = \frac{38}{2^{19}} \approx 0.00007$
23	24	46	2^{23}	$P = \frac{46}{2^{23}} \approx 0.00002$

As it can be seen from the previous table the sequence of probabilities P_{BA} is strictly decreasing. Based on these computational results we deduce the following remark, when the order n is large enough.

Remark 4.2. *The encryption scheme based on Hadamard matrices with one circulant core is secure against brute force attacks.*

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 Hadamard matrix of order $n > 128$, which can easily be constructed from theorem 3.6 for large orders, as an encryption matrix justifies our previous claim.

4.1.2 Cryptanalysis of brute force attacks for schemes based on Hadamard matrices with two circulant cores

In order for an adversary to break this system using a brute force attack, he would have to deduce the encryption key $k = A_c \oplus B_c$, which is the concatenation of the binary vectors $A_c = [a_1, a_2, \ldots, a_\ell]$ and $B_c = [b_1, b_2, \ldots, b_\ell]$, of total length 2ℓ by trying a large number of possibilities.

In our case, an adversary would have to simulate a brute force search of the key space. Assuming the adversary has knowledge of the encryption protocol he would have to search on 2ℓ binary variables. Since, the encryption key consists of binary variables using enumerative combinatorics, the size of the key space, $K(\mathcal{H}_\ell)$, is $\mid K(\mathcal{H}_\ell) \mid = 2^{2\ell}$ therefore its computational complexity is of exponential growth $\mathcal{O}(2^n)$ as $n = 2\ell + 2$ increases. Furthermore, the possibility a solution obtained from a brute-force search of the key space to be an encryption key is given by the total number of Hadamard matrices with two circulant cores that exist in a specific order divisible by the size of the key space in that order.

For example, if we consider schemes that are using the Hadamard matrices of order $28 = 2 \cdot 13 + 2$, the key space consists of 26 binary variables while the total number of Hadamard matrices that exist in that order are $7,098$, therefore we have $7,098$ possible encryption keys. As can be seen in the following table, the probability of breaking the system via a brute force attack for this case is $P = \frac{42 \times 13^2}{2^{26}} \approx 0.0001$, only. It is worthwhile to note that using a key of length only 26 bits we almost provide total security against brute force attacks for this scheme.

We summarize in the following table the available Hadamard matrices with two circulan cores, denoted by $\mid V(\mathcal{H}_\ell) \mid$, for orders $n = 2\ell + 2$ whereas $\ell = 3, \ldots, 25$ using the results obtained via exhaustive searches in [6, 14], the cardinality of the key space $\mid K(\mathcal{H}_\ell) \mid$, and the probability P_{BA} of breaking

the cipher via a brute force attack for each order.

Table 2: Probabilities of breaking the cipher for different key sizes

ℓ	matrix order	$\mid V(\mathcal{H}_\ell) \mid$	$\mid K(\mathcal{H}_\ell) \mid = 2^{2\ell}$	$P_{BA} = \frac{\lvert V(\mathcal{H}_\ell)\rvert}{\lvert K(\mathcal{H}_\ell)\rvert}$
3	8	$9 = 1 \times 3^2$	2^6	$P = \frac{1\times 3^2}{2^6} \approx 14 \cdot 10^{-2}$
5	12	$50 = 2 \times 5^2$	2^{10}	$P = \frac{2\times 5^2}{2^{10}} \approx 4 \cdot 10^{-2}$
7	16	$196 = 4 \times 7^2$	2^{14}	$P = \frac{4\times 7^2}{2^{14}} \approx 10 \cdot 10^{-3}$
9	20	$972 = 12 \times 9^2$	2^{18}	$P = \frac{12\times 9^2}{2^{18}} \approx 4 \cdot 10^{-3}$
11	24	$2,904 = 24 \times 11^2$	2^{22}	$P = \frac{24\times 11^2}{2^{22}} \approx 7 \cdot 10^{-4}$
13	28	$7,098 = 42 \times 13^2$	2^{26}	$P = \frac{42\times 13^2}{2^{26}} \approx 10 \cdot 10^{-5}$
15	32	$38,700 = 172 \times 15^2$	2^{30}	$P = \frac{172\times 15^2}{2^{30}} \approx 3 \cdot 10^{-5}$
17	36	$93,058 = 322 \times 17^2$	2^{34}	$P = \frac{322\times 17^2}{2^{34}} \approx 5 \cdot 10^{-6}$
19	40	$161,728 = 448 \times 19^2$	2^{38}	$P = \frac{488\times 19^2}{2^{38}} \approx 5 \cdot 10^{-7}$
21	44	$433,944 = 984 \times 21^2$	2^{42}	$P = \frac{984\times 21^2}{2^{42}} \approx 10 \cdot 10^{-8}$
23	48	$1,235,744 = 2336 \times 23^2$	2^{46}	$P = \frac{2336\times 23^2}{2^{46}} \approx 2 \cdot 10^{-8}$
25	52	$2,075,000 = 3320 \times 25^2$	2^{50}	$P = \frac{3320\times 25^2}{2^{50}} \approx 2 \cdot 10^{-9}$

As it can be seen from the previous table the sequence of probabilities P_{BA} is strictly decreasing and using (cf. [14, Property 1.]) is upper bounded from 1. In addition, asserting the truth of [14, Conjecture 1.], that for every odd $\ell = 3, \ldots$ there exists a Hadamard matrix of order $2\ell + 2$ with two circulant cores, and that the sequence of $\mid V(\mathcal{H}_\ell) \mid$ will continue to increase we can conclude that the limit of the sequence of probabilities $\lim_{\ell\to\infty} P_{BA} = \lim_{\ell\to\infty} \frac{\mid V(\mathcal{H}_\ell) \mid}{\mid K(\mathcal{H}_\ell) \mid}$ converges to zero. Note that Conjecture 1 of [14], would settle the general Hadamard conjecture. In particular, we deduce the following lemma.

Lemma 4.3. *Assume the following two conditions hold,*

(i) There exists a Hadamard matrix of order $2\ell + 2$ with two circulant cores for every odd $\ell = 3, \ldots$

(ii) The sequence of $\mid V(\mathcal{H}_\ell) \mid$ is increasing for every odd $\ell = 3, \ldots$

Then, the encryption scheme based on Hadamard matrices with two circulant cores is secure against brute force attacks.

Proof. Since, $\lim_{\ell\to\infty} P_{BA} = \lim_{\ell\to\infty} \frac{\mid V(\mathcal{H}_\ell) \mid}{\mid K(\mathcal{H}_\ell) \mid} \to 0$ as $n = 2\ell + 2$ increases, it is computationally infeasible a brute force attack of the key space to result on an encryption key. □

4.2 Cryptanalysis of known-plaintext attacks

Definition 4.4. *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 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 $i = 1,\ \ldots,\ n$:

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

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 4.5. *All encryption schemes using Hadamard matrices with circulant cores 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. □

4.3 Cryptanalysis of chosen-plaintext attacks

Definition 4.6. *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 4.2.

Remark 4.7. *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 4.8. *All encryption schemes using Hadamard matrices with circulant cores are secure against chosen-plaintext attacks, since the schemes are secure against known-plaintext attacks.*

4.4 Cryptanalysis of ciphertext-only attacks

Definition 4.9. *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 4.10. *All encryption schemes using Hadamard matrices with circulant cores are secure against ciphertext-only attacks.*

4.5 Cryptanalysis of chosen-ciphertext attacks

Definition 4.11. *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 4.2.

Proposition 4.12. *All encryption schemes using Hadamard matrices with circulant cores are secure against chosen – ciphertext attacks, since the schemes are secure against known – plaintext attacks.*

We note that any attack on an encryption scheme is only valid if it violates some property that the scheme was intended to achieve. In other words all

attacks must be considered relative to the design goals that the encryption scheme is meant to achieve.

5 A "Blow-up" Construction of Encryption Schemes using Kronecker Product

In this section we apply the "blow-up" construction of encryption schemes given in [15], 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 scheme.

Definition 5.1 ([16]). *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 Hadamard matrices.

Proposition 5.2 ([32]). *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 5.3. *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 $\prod_{i=1}^{p} n_i$.*

Our aim is to improve the schemes presented in the previous section in order to be completely secure against known-plaintext attacks, chosen-plaintext

attacks and chosen-ciphertext attacks by enhancing the use of Kronecker product. We illustrate our method by giving detailed examples in the case of encryption schemes based on Hadamard matrices with one and two circulant cores below.

Example 5.4. *Let H_i, for $i = 1, \ldots, k$ be Hadamard matrices with one circulant core of orders $n_i = p_i+1$, for $i = 1, \ldots, k$ respectively. These matrices associated with their corresponding encryption keys $A_{c_i} = [a_{1_i}, a_{2_i}, \ldots, a_{p_i}]$ for $i = 1, \ldots, k$ where each private key A_{c_i} consists of p_i bits, form a k-family of encryption schemes. 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 Hadamard matrix H_i by assuming knowledge of the corresponding private key A_{c_i}, the matrix generated by the Kronecker product can be used as an encryption matrix where its private key $\bigoplus_{i=1}^{k} A_{c_i}$ is the concatenation of the private keys A_{c_i}, which consists of $\sum_{i=1}^{k} p_i$ bits. Let n denote the largest order of the 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 $\sum_{i=1}^{k} p_i = \sum_{i=1}^{k}(n_i - 1) = \sum_{i=1}^{k}(n_i) - k \leq \sum_{i=1}^{k}(n) - k = kn - k = k(n-1)$, therefore its growth is of size $\mathcal{O}(n)$.*

Example 5.5. *Let H_i, for $i = 1, \ldots, k$ be Hadamard matrices with two circulant cores of orders $n_i = 2\ell_i+2$, for $i = 1, \ldots, k$ respectively. These matrices associated with their corresponding encryption keys $A_{c_i} \oplus B_{c_i} = [a_{1_i}, a_{2_i}, \ldots, a_{\ell_i}] \oplus [b_{1_i}, b_{2_i}, \ldots, b_{\ell_i}] = [a_{1_i}, a_{2_i}, \ldots, a_{\ell_i}, b_{1_i}, b_{2_i}, \ldots, b_{\ell_i}]$ for $i = 1, \ldots, k$ where each private key $A_{c_i} \oplus B_{\ell_i}$ consists of $2\ell_i$ bits, form a k-family of encryption schemes.*

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 Hadamard matrix* H_i *by assuming knowledge of the corresponding private key* $A_{c_i} \oplus B_{c_i}$*, the matrix generated by the Kronecker product can be used as an encryption matrix where its private key* $\bigoplus_{i=1}^{k}(A_{c_i} \oplus B_{c_i})$ *is the concatenation of the private keys* $A_{c_i} \oplus B_{c_i}$*, which consists of* $\sum_{i=1}^{k} 2\ell_i = 2k\sum_{i=1}^{k} \ell_i$ *bits. Let* n *denote the largest order of the 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* $\sum_{i=1}^{k} 2\ell_i = \sum_{i=1}^{k}(n_i - 2) = \sum_{i=1}^{k}(n_i) - 2k \leq \sum_{i=1}^{k}(n) - 2k = nk - 2k = k(n-2)$*, therefore its growth is of size* $\mathcal{O}(n)$*.*

In each case, with this "blow-up" construction we have achieved an "explosion" to the size of the encryption matrix while maintaining the key size in reasonable lengths. One of our goals was to make a linear analysis of the encryption schemes computationally infeasible. Since this is achieved by solving a linear system, thus making use of Gaussian elimination, in order for an adversary to perform successfully known-plaintext attacks, chosen-plaintext attacks and chosen-ciphertext attacks, based on the cryptanalysis we presented in the previous section.

Proposition 5.6. *The encryption schemes constructed via the "blow-up" construction using Kronecker product is completely secure known-plaintext attacks, chosen-plaintext attacks and chosen-ciphertext attacks, since a linear cryptanalysis is computationally infeasible.*

We can now discuss, a weakness in the design of the encryption scheme proposed in Section 2 which in some cases can be eliminated using the previous

"blow-up" construction. 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 ([5, 18, 19, 31]). 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 orthogonal arrays A_i, $i = 1, \ldots, k$ 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.

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

[2] 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, (1999), 37–100.

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

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

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

[6] R.J. Fletcher, M. Gysin and J. Seberry, Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices, *Australas. J. Combin.*, **23**, (2001), 75–86.

[7] S. Georgiou and C. Koukouvinos, On generalized Legendre pairs and multipliers of the corresponding supplementary difference sets, *Utilitas Math.*, **61**, (2002), 47–63.

[8] S. Georgiou, C. Koukouvinos and J. Seberry, Hadamard matrices, orthogonal designs and construction algorithms, Chapter 7, in *Designs 2002: Further Computational and Constructive Design Theory*, ed. W.D. Wallis, Kluwer Academic Publishers, Norwell, Massachusetts, 2003, 133–205.

[9] A.V. Geramita and J. Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Dekker, New York-Basel, 1979.

[10] M. Gysin and J. Seberry, An experimental search and new combinatorial designs via a generalization of cyclotomy, *J. Combin. Math. Combin. Comput.*, **27**, (1998), 143–160.

[11] J. Hadamard, Resolution d'une question relative aux determinants, *Bull. des. Sci. Math.*, **17**, (1893), 240–246.

[12] M. Hall Jr, A survey of difference sets, *Proc. Amer. Math. Soc.*, **7**, (1956), 975–986.

[13] I.S. Kotsireas, C. Koukouvinos and J. Seberry, Hadamard ideals and Hadamard matrices with circulant core, *J. Combin. Math. Combin. Comput.*, **57**, (2006), 47–63.

[14] I.S. Kotsireas, C. Koukouvinos and J. Seberry Hadamard ideals and Hadamard matrices with two circulant cores, *European J. Combin.*, **27**, (2006), 658–668.

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

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

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

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

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

[20] W. Orrick, Switching operations for Hadamard matrices, *SIAM J. Discr. Math.*, **22**, (2008), 31–50.

[21] R.E.A.C. Paley, On orthogonal matrices, *J. Math. Phys.*, **12** (1933), 311–320.

[22] M. Plotkin, Decomposition of Hadamard matrices, *J. Combin. Theory, Ser. A*, **13**, (1972), 127–130.

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

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

[25] M.R. Schroeder, *Number Theory in Science and Communication*, Springer–Verlag, New York, 1984.

[26] J. Seberry and R. Craigen, Orthogonal designs, in *CRC Handbook of Combinatorial Designs*, C.J. Colbourn and J.H. Dinitz (Eds.), CRC Press, Boca Raton, (1996), 400–406.

[27] 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 and Sons, New York, (1992), 431–560.

[28] J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.*, **43**, (1938) 377–385.

[29] R.G. Stanton and D.A. Sprott, A family of difference sets, *Can. J. Math.*, **10** (1958), 73–77.

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

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

[32] 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**, (1867), 461–475.

[33] A.L. Whiteman, A family of difference sets, *Illinois J. Math.*, **6**, (1962), 107–121.