Weaknesses in Hadamard Based Symmetric Key Encryption Schemes

Gajraj Kuldeep, Devendra Kumar Yadav, A. K. Sharma
SAG DRDO

In this paper security aspects of the existing symmetric key encryption schemes based on Hadamard matrices are examined. Hadamard matrices itself have symmetries like one circulant core or two circulant core. Here, we are exploiting the inherent symmetries of Hadamard matrices and are able to perform attacks on these encryption schemes. It is found that entire key can be obtained by observing the ciphertext.

1 Introduction

Hadamard matrices [4] are square matrix with entries are +1 and -1. These matrices are having a special property that the rows/columns of a Hadamard matrix are pairwise orthogonal. Let H be a Hadamard matrix then $HH' = NI_n$ where $'$ for transposition and I_n is the identity matrix of order N.

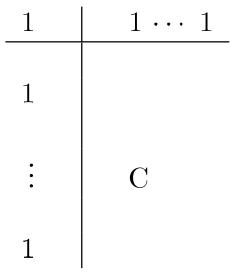
There are several operations on Hadamard matrices which preserve the Hadamard property:

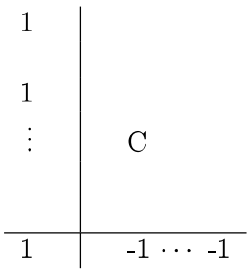
(a) permuting rows, and changing the sign of some rows;

(b) permuting columns, and changing the sign of some columns;

(c) transposition.

We call two Hadamard matrices $H1$ and $H2$ equivalent if one can be obtained from the other by operations of types (a) and (b); that is, if $H2 = P^{-1}H1Q$, where P and Q are matrices (having just one non-zero element in each row or column) with non-zero entries +1 and -1. Hadamard matrices having one circulant core can take one of the forms described below.





For the following case a Hadamard matrix of order $N+1$ with one circulant core can be constructed if

- $N \cong 3 \mod 4$ is a prime [4];
- $N = q(q+2)$ where q and $q+2$ are both primes [6, 7];
- $N = 2^w - 1$ where w is a positive integer [5];
- $N = 4w^2 + 27$ where N is a prime and w a positive integer [1].

Hadamard matrices based encryption schemes were discussed by Christos and Dimitris [2]. They proposed symmetric key cipher based on several constructions of Hadamard matrices. Here, encryption and decryption algorithm given by Christos and Dimitris are discussed.

Encryption Algorithm

$k \leftarrow (H, d)$ key
$m \leftarrow message$
$c \leftarrow mH + de_n$
H is Hadamard matrix, d is a constant, c is cipher, e_n is $1 \times N$ vector of ones.

Decryption Algorithm

Receive c
$s \leftarrow c - de_n$
$m \leftarrow sH'/N$ recovered message

In section 2, various attacks on the symmetric key encryption scheme based on Hadamard matrices are discussed.

2 Attacks on the Scheme

Authors [2] claimed that above discussed schemes are secure against brute force attacks, ciphertext-only attacks, known-plaintext attacks and chosen-plaintext attacks. By using the symmetries in the Hadamard matrices these attacks are possible.

2.1 Ciphertext only Attack

This attack can be launched by observing the value of cipher text only. By analysing the cipher text if one can get a part of a key or part of plain text then the method is susceptible to this attack.

2.1.1 Finding d part of the Key

By observing the cipher vectors one can obtain d. When all values of cipher vector are equal, which is possible when input is all zeros then the cipher $c \leftarrow de_n$ itself contains the value of d.

When input is not equal to zero then also it is possible to find the value of d as described

Theorem 2.1 *Let m be the message vector of size $1 \times N$,H be the Hadamard matrix of size $N \times N$, c be a constant, e_n is $1 \times N$ vector of ones. Then $mH = ce_n$ is possible if and only if $m = (c\ 0 \cdots\ 0)$*

Proof 2.1 *Let $m = (c\ 0 \cdots\ 0)$ then $mH = ce_n$ which is trivial to observe.*
Now consider the other part where

$$mH = ce_n \tag{1}$$

Then multiplying both sides by H' we get

$$mHH' = ce_nH' \tag{2}$$

Since $HH' = NI_n$ and sum of all but first columns of Hadamard matrix is zero. Therefore above equation becomes

$$\begin{array}{rcl} mNI_n & = & c(N0\cdots0) \\ & = & (cN0\cdots0) \end{array} \tag{3}$$

which gives the desired m.

Lemma 2.2 *If message m is of the form $(0\ 0\ c \cdots\ 0)$ then $mH = cf_n$, where f_n has entries $\pm$ 1.*

Since cipher c is given by

$$c_i = m_i H + de_n \tag{4}$$

where each c_i corresponds to m_i. Let m_i has the form $(k_i\ 0 \cdots 0)$. Using Theorem 2.1 cipher $c_i = d_i e_n$ where d_i corresponds to $k_i + d$. Therefore all c_i's will have the form $(k_i + d \cdots k_i + d)$. Let us assume that we have collection of N c_i's. There are two methods to find d from the captured c_i's.

First Method

Authors[2] have designed this algorithm for ASCII input which cannot take negative values. Hence k_i's can taken positive values. With high probability d can be find out by $min(d_1, d_2 \cdots, d_n)$. As N increases probability of getting correct value of d also increases.

Second Method

Since d_i's are of the form $k_i + d$ where k_i are ASCII values. So by applying frequency test on d_i's we can get highest frequency d_i corresponding to english alphabet 'e' (This alphabet has the highest frequency among English Alphabets). By subtracting ASCII value of 'e' from d_i we can obtain the value of d as shown in the figure below.

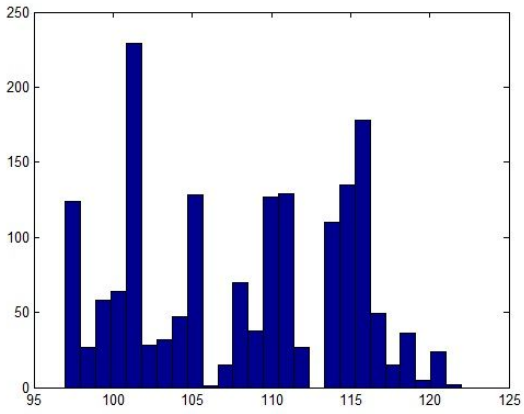


Figure 1: Frequency plot of $k_i + d$

2.1.2 Finding d part of Key(Message Independent)

In section 2.1.1 we observe that we can find d if messages take particular form. In this section our aim is to deduce d independent from messages structure. Hadamard matrices possess Hadamard property which leads them to orthogonal matrices. Let H be the Hadamard matrix and e_n be a column vector of ones then

$$He_n = (N, 0, 0, ..., 0)'$$

cipher can be written

$$c = mH + de'_n \tag{5}$$

multiplying equation 5 by e_n we get

$$ce_n = mHe_n + de'_n e_n$$

$$\sum_{i=1}^{N} c_i = [m_1 \cdots m_N] \begin{bmatrix} N \\ 0 \\ \vdots \\ 0 \end{bmatrix} + dN$$

$$m_1 + d = \frac{1}{N} \sum_{i=1}^{N} c_i$$

By using second method as explained in section 2.1.1 we can obtain value of d. This method is independent from the structure of message.

2.1.3 Finding part of Plaintext

As we know that the Hadamard matrix with one circulant core has structure as given in section 1 above where C is a circulant matrix. As in section 2.1.1 we have suggested methods to find out d which is a part of key. Now we can define

$$\tilde{c} = c' - de_n \tag{6}$$

C is a circulant matrix which is part of Hadamard matrix. So to fulfil the Hadamard property, each columns/rows of C should have $N/2$ numbers of $-1's$. As we can see that $\tilde{c} = mH$. This can be expressed as

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & a_1 & a_2 & \cdots & a_{N-1} \\ 1 & a_2 & a_3 & \cdots & a_1 \\ \vdots & \vdots & \vdots & & \\ 1 & a_{N-1} & a_1 & \cdots & a_{N-2} \end{pmatrix} \begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ \vdots \\ m_{N-1} \end{pmatrix} = \begin{pmatrix} \tilde{c}_0 \\ \tilde{c}_1 \\ \tilde{c}_2 \\ \vdots \\ \tilde{c}_{N-1} \end{pmatrix}$$

where $a'_k s = \pm 1$

$$m_0 + \sum_{i=1}^{N-1} m_i = \tilde{c_0} \tag{7}$$

$$m_0 + \sum_{i=1}^{N-1} a_{i+k-1} m_i = \tilde{c_k}, k = 1, 2 \cdots N-1 \tag{8}$$

So, here we have $N-1$ equations. By adding all of these,we get

$$(N-1)m_0 - \sum_{i=1}^{N-1} m_i = \sum_{k=1}^{N-1} \tilde{c_k} \tag{9}$$

By adding equation 7 and 9, we get

$$m_0 = \frac{1}{N} \sum_{k=0}^{N-1} \tilde{c_k} \tag{10}$$

Here we have applied cipher text only attack and we are able to get part of plain text m_0. Therefore this scheme is vulnerable to such type of attacks. Ciphertext also reveals about plaintext. When all the values of ciphertext are equal then also from theorem 2.1 we get that atleast $N-1$ values of plaintext are zero.

2.2 Known Plaintext Attack

In known plaintext attack we are given with pair of plaintext and its corresponding cipher text. Authors [2] have claimed that *if the adversary has knowledge of less than n messages of length n of the plaintext and the corresponding ciphertext then all encryptoin schemes using Hadamard matrices with circulant cores are secure against known-plaintext attacks.* As we can see from equation 8 only one pair of message and its corresponding cipher text is sufficient to find the entries of circulant core of Hadamard matrices.

2.3 Chosen Plaintext Attack

In this attack we can choose the plain text and obtain the corresponding cipher text. By choosing a particular form of message similar to the one shown in Lemma 2.2 we can deduce row of a Hadamard matrix. Since Hadamard matrices have one circulant core, therefore one row is sufficient to reconstruct the entire Hadamard matrix. Therefore by choosing a particular form of message, complete Hadamard matrix can be reconstructed. Hence entire key can be obtained by launching this attack.

3 Concluding Remarks

In this paper we have examined the security aspects of Hadamard based symmetric key encryption scheme. It was found that this scheme is vulnerable to two type of attacks: ciphertext only attack and known plaintext attack. Cipher text only attack is more difficult to mount but we applied this attack and were able to retrieve the part of the key and part of plaintext.In chosen plaintext attack we were able to retrieve the entire key by choosing only one message.

Acknowledgement

We would like to acknowledge Dr Dhananjoy Dey for listening to the ideas and supportive guidance.We are also thankful to the Director, SAG for permitting us to carry out this work.

References

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

[2] C. Koukouvinos & D. E. Simos, *Encryption schemes based on Hadamard matrices with circulant cores*, Journal of Applied Mathematics & Bioinformatics, 2013,17-41.

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

[4] J. Seberry and M. Yamada, *Hadamard matrices, sequences and block designs*, in Contemporary Design Theory, J. Wiley and Sons NewYork,(1992), 431-560

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

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

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