Journal of mathematics and computer science 12 (2014), 316-319

Contents list available at JMCS

Journal of Mathematics and Computer Science

Journal Homepage: www.tjmcs.com

Improving the Key Agreement Protocol Security Based on Hadamard Matrices

Ali Zaghian, Mohammad Jafar Hashemi, Ahmad Majlessi

Department of mathematic and cryptography,Malek-e-Ashtar university of Technology, Isfahan, Iran

a_zaghian@mut-es.ac.ir

mjhashemi65@gmail.com, ahmad.majlessi @gmail.com

Article history:
Received July 2014
Accepted August 2014
Available online August 2014

Abstract

In this paper, the security of key agreement protocol based on Sylvester Hadamard matrices proposed by Chang-hui Choe and Moon Ho Lee has been improved. Applying new changes, the weakness of their protocol was introduced and its security was increased. In short, new symmetric key agreement protocol will be suitable for insecure communication when two users want to share a common secret key with the low computing power.

Keywords: Encryption, Security, Sylvester Hadamard Matrices, Key agreement.

1. Introduction

Key agreement is one of the fundamental cryptographic primitive after encryption and digital signature. Such protocols allow two or more parties to exchange information among themselves over an adversarially controlled insecure network and agree upon a common session key, which may be used for later secure communication among the parties. Thus, secure key agreement protocols serve as basic building block for constructing secure, complex, higher-level protocols [1,2,3]. Key agreement method using Sylvester Hadamard matrices has been proposed in [4]. Their proposal is lightweight and no exponential operation is needed to do that but the problem is that it is not secure. Increasing the security of this protocol, will make it very suitable for key agreement in constraint environment.

2. Sylvester Hadamard Matrices

A Hadamard matrix H of order n is an$n \times n$ matrix with elements ± 1 and $HH^T = nI$. Sylvester in 1867 noted that given a Hadamard matrix H of order n, Then the following matrix:

$$\begin{bmatrix} H & H \\ H & -H \end{bmatrix} \qquad (1)$$

is a Hadamard matrix of order $2n$. Matrices of the form (1) are called Sylvester Hadamard and are defined for all powers of 2. Below the Sylvester Hadamard matrix of order 2 is given:

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Starting with H_2, Sylvester Hadamard matrices of order 2^k can be formed by $\underbrace{H_2 \times \ldots . \times H_2}_{k-copies}$ the Kronecker product of k copies of H_2 and it is denoted by H_{2^k} . Also H_{2^k} can be represented as bellow [5]:

$$\forall a, b \in \{0,1,2, \ldots, 2^k - 1\}, \qquad H_{(a,b)} = (-1)^{<a,b>}$$

Where a and b are the row and column indices, respectively, of H_{2^k} starting from 0 (not from 1), $H_{(a,b)}$ is the entry of H_{2^k} located at the row a and column b, and $< a, b >$ is the inner product of a and b.
If G is a finite group and C is a finite abelian group, A cocycle is a mapping $\psi: G \times G \to C$ satisfying the cocycle equation:

$$\psi(g,h)\psi(g * h,k) = \psi(g,h * k)\psi(h,k), \qquad \forall g,h,k \in G$$

The group operation * with Sylvester Hadamard matrices is defined as bitwise XOR.
A cocycle is naturally displayed as a cocyclic matrix that is a square matrix whose rows and columns are indexed by the elements of G under some fixed ordering, and whose entry in position (g,h) is $\psi(g,h)$.(Elsewhere this is termed a pure cocyclic matrix) We write:

$$M_{\psi} = [\psi(g,h)]_{g,h \in G}$$

Theorem1: Sylvester Hadamard matrices are co-cyclic[6].

3. Key Agreement Protocol Using Silvester Hadamard Matrices and weakness

In this section, the key agreement protocol proposed by Chang-hui Choe and Moon Ho Lee has been described. The secret key, generated by two user and one Trusted Authority (TA) using the same Sylvester Hadamard matrices. Fig. 1 shows the key agreement process:

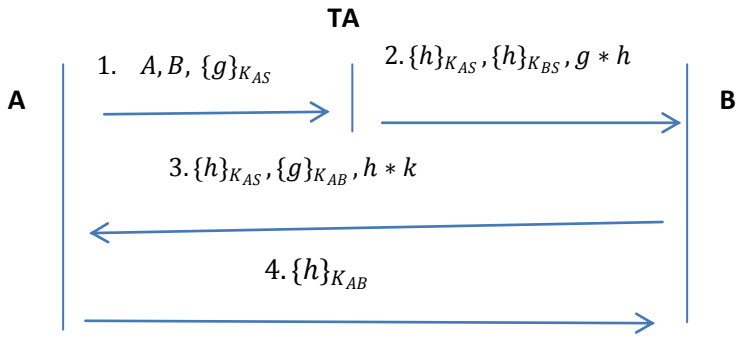

Fig. 1. Proposed key agreement protocol in [4]

Unfortunately, the proposed key agreement protocol is not secure because of the following reasons:

1. $g * h$ and $h * k$ have not been encrypted and the enemy can simply find the g with brute force attack. It can receive the $\{g\}_{K_{AS}}$ and will find the session key K_{AS} via interception between A and TA.
2. In this protocol (step 2),B can calculate the K_{AS} as follows:
   a) B decrypts the $\{h\}_{K_{BS}}$ and finds the h.
   b) Since B has the $\{h\}_{K_{AS}}$ it can find the K_{AS} with calculate $\{h\}_{K_{AS}} \oplus h$.

   Therefore,it is not suitable and the secrecy of the session key K_{AS}, is vulnerable.

Hence, a new and more secure protocol has been proposed in the next session.

3. Security increase of the key agreement protocol based on Hadamard matrices.

A trusted authority (TA) share secret key K_{AS}, K_{BS} and n bit number h. After key agreement, A and B share a secret common key K_{AB}. Users can share a m bit session key K_{AB} with a $2^n \times 2^n$ Sylvester Hadamard matrix and N bit number g and k that can be divided into m numbers of n bit such as $k = (k_0, k_1, \dots, k_{m-1})$, where $N = mn$. The new key agreement process, is shown in Fig. 2 as follows:

1. A randomly generates g, encrypts it with K_{AS}, and sends cipher text to the TA.
2. The TA encrypts $g * h$ with K_{BS} and sends it to B.
3. B decrypts the $\{g * h\}_{K_{BS}}$ and obtains g from $\{g * h\} \oplus h$. B randomly generates k and calculates the secret common key as follows:

$$K_{AB} = K_{AB_0} \| \dots \left\| K_{AB_{m-1}} = \psi(h_0, k_0)\psi(g_0, h_0 * k_0) \right\| \dots \psi(h_{m-1}, k_{m-1})\psi(g_{m-1}, h_{m-1} * k_{m-1})$$

After generating K_{AB}, B encrypts k with K_{BS} and sends encrypted message to TA. Also B encrypts g with K_{AB} and sends it to A.

TA obtains k and encrypts it with K_{AS} and sends it to A.

4. A decrypts the message received from TA and obtain sk. Therefor, A can calculate K_{AB} and the same step3. For key confirmation, A decrypts $\{g\}_{AB}$, encrypts k with K_{AB} and sends it to B. B decrypts $\{k\}_{AB}$ for confirmation.

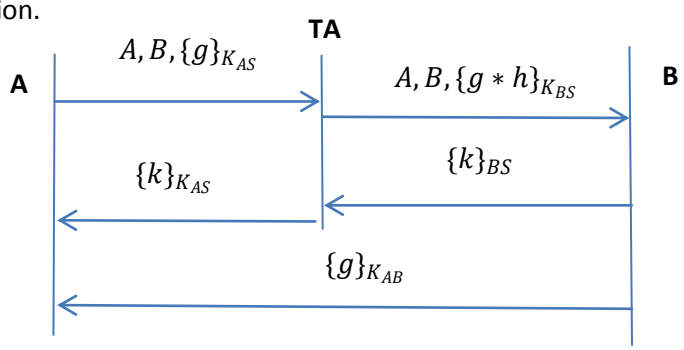

Fig. 2.new proposed key agreement protocol

5. Security Analysis

The authors of [4] have proved that the probability of every possible m bit session key in proposed protocol is always $1/2^m$. Key freshness and key confirmation are provided in this protocol [4], But the key agreement protocol proposed in [4] contains weakness which have been introduced in section 3. After encryption of $g * h$ and changing the protocol, A new secure protocol will be acquired.

6. Conclusion

Successful key management is critical to the security of a cryptosystem. In practice it is arguably the most difficult aspect of cryptography because it involves system policy, user training, organizational and departmental interactions, and coordination between all of these elements. The key agreement protocol based on public key cryptography is expensive and it is not suitable for low computing power environments. Instead, the proposed symmetric key agreement protocol is sufficiently secure and lightweight.

References

[1] W. Stallings, Cryptography and Network Security principels and practice, 5th ed., 2011.
[2] W. Diffie and M. Hellman, New directions in cryptography, IEEE Trans.Inf. Theory, vol. 22,(1976) no. 6, 644–654.
[3] Behrouz A. Forouzan, Cryptography and Network Security · 2nd Edition, McGraw-Hill Education Pvt. Ltd., 2010
[4] C. -h. Choe, M.H. Lee, Key agreement protocol using Sylvester Hadamard matrices, Journal of Communication and networks, Vol. 13, No. 3,(2011) 1435–1443.
[5] K.J. Horadam, Hadamard Matrices, Princeton university Press 2007.
[6] K. J. Horadam, P. Udaya, Cocyclic Hadamard codes, IEEE Trans.Inf. Theory, vol. 46, no. 4, (2000) 545–1550.