Key Agreement Protocol Using Sylvester Hadamard Matrices

Chang-hui Choe and Moon Ho Lee

Abstract: **In this paper, we propose a key agreement protocol using Sylvester Hadamard matrices. Users obtain their common key by using a matrix shared in advance. Matrix construction is very simple, and the computation is quite fast. The proposal will be useful for communication between two users, especially for those having low computing power.**

Index Terms: **Co-cycle, Hadamard matrix, key agreement.**

I. INTRODUCTION

When two users U_1 and U_2 want to share a common key, U_1 can make and send a secret key to U_2 that is encrypted by U_2's public key, and U_2 can receive and decrypt the key. They now share the same key. In this case, the common key is generated by U_1 only, and they should use an expensive public key cryptographic method.

Key agreement methods using a certain pattern of a Jacket matrix, which is co-cyclic, have been proposed [1], [2]. In this paper, we propose a key agreement scheme using Sylvester Hadamard matrices, which is simpler than those in [1], [2]. We will show that Sylvester Hadamard matrices are co-cyclic and propose our protocol. Then, we will present the steps of the key agreement and a brief security analysis.

II. SYLVESTER HADAMARD MATRICES AND CO-CYCLES

$2^n \times 2^n$ Sylvester Hadamard matrix H_{2^n} can be defined as follows.

$$\begin{aligned} H_{2^n} &= H_{2^{n-1}} \otimes H_2, \quad \text{for } n \geq 2, \\ H_2 &= \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \end{aligned} \tag{1}$$

where $A \otimes B$ is the Kronecker product of A and B, defined as follows for a $p \times q$ matrix A.

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1q}B \\ \vdots & \ddots & \vdots \\ a_{p1}B & \cdots & a_{pq}B \end{bmatrix}. \tag{2}$$

Manuscript received February 5, 2010; approved for publication by Emanuele Viterbo, Division I Editor, October 5, 2010.

This work was supported by the World Class University (WCU) program (R32-2008-000-20014-0) and the Fundamental Research (FR) program (2010-0020942) through the National Research Foundation of Korea.

M. H. Lee is the corresponding author.

The authors are with the Department of Electronic Engineering, Chonbuk National University, Jeonju, 561-756, Republic of Korea, email: {nblue95, moonho}@jbnu.ac.kr.

Also H_{2^n} can be represented as [3]

$$\forall a, b \in \{0, 1, 2, \cdots, 2^n - 1\}, \quad H_{(a,b)} = (-1)^{\langle a,b \rangle} \tag{3}$$

where a and b are the row and column indices, respectively, of H_{2^n} starting from 0 (not from 1), $H_{(a,b)}$ is the entry of H_{2^n} located in row a and column b, and $\langle a, b \rangle$ is the inner product of a and b, i.e.,

$$\begin{aligned} a &= (a_{n-1}, a_{n-2}, \cdots, a_0), \\ b &= (b_{n-1}, b_{n-2}, \cdots, b_0), \\ \langle a, b \rangle &= \sum_{m=0}^{n-1} a_m b_m. \end{aligned} \tag{4}$$

With (3), we can directly obtain an element of a Sylvester Hadamard matrix without generating or storing the entire matrix. For example, the entry located in the second row ($a = 1$) and the third column ($b = 2$) is

$$H_{(1,2)} = (-1)^{\langle 1,2 \rangle} = 1. \tag{5}$$

Moreover, we do not need to perform any exponential operation to calculate (3), since the base is -1. If $\langle a, b \rangle$ is odd, (3) is -1, otherwise it is 1.

Let G be a finite group of order v and C be a finite abelian group of order w. A co-cycle is a mapping $\varphi : G \times G \to C$ with some operation $\circ$, satisfying the co-cyclic equation.

$$\begin{aligned} &\varphi(g, h)\varphi(g \circ h, k) = \varphi(g, h \circ k)\varphi(h, k), \quad \forall g, h, k \in G, \\ &\varphi(g, 0)\varphi(0, h) = 1, \quad \forall g, h \in G. \end{aligned} \tag{6}$$

Then, the co-cycle φ over G is naturally presented as a co-cyclic matrix M_φ. It is a $v \times v$ matrix whose rows and columns are indexed by the elements of G, such that the entry in row g and column h is $\varphi(g, h)$.

If $\varphi(g, h) = \varphi(h, g)$, then M_φ is symmetric and for a co-cyclic function $\varphi()$,

$$\begin{aligned} \varphi(g, h)\varphi(g \circ h, k) &= \varphi(h, k)\varphi(h \circ k, g) \\ &= \varphi(k, g)\varphi(k \circ g, h). \end{aligned} \tag{7}$$

In this paper, we define the operation $\circ$ with Sylvester Hadamard matrices as bitwise XOR.

Theorem 1: Sylvester Hadamard matrices are co-cyclic.

Proof: From (3) and (6),

$$\varphi(g, h)\varphi(g \circ h, k) = (-1)^{\langle g,h \rangle + \langle g \circ h, k \rangle}, \tag{8}$$

$$\varphi(h, k)\varphi(h \circ k, g) = (-1)^{\langle h,k \rangle + \langle g, h \circ k \rangle}. \tag{9}$$

We show that (8) and (9) are the same to prove the theorem.

In (8) and (9), the bases are -1, and the result of calculation does note change if all additions ("+") are changed into mod 2

1229-2370/11/$10.00 © 2011 KICS

additions ("⊕"), i.e., bitwise XOR is realized. From (4), the exponents of (8) and (9) can be expressed as follows, respectively.

$$\begin{aligned}&\langle g,h\rangle\oplus\langle g\circ h,k\rangle\\&\quad=(g_0h_0\oplus\cdots\oplus g_{n-1}h_{n-1})\\&\qquad\oplus((g_0\oplus h_0)\,k_0\oplus\cdots\oplus(g_{n-1}\oplus h_{n-1})\,k_{n-1})\\&\quad=(g_0h_0\oplus h_0k_0\oplus k_0g_0)\\&\qquad\oplus\cdots\oplus(g_{n-1}h_{n-1}\oplus h_{n-1}k_{n-1}\oplus k_{n-1}g_{n-1})\\&\quad=\sum_{i=0}^{n-1}(g_ih_i\oplus h_ik_i\oplus k_ig_i)\,.\end{aligned}\tag{10}$$

$$\begin{aligned}&\langle h,k\rangle\oplus\langle g,h\circ k\rangle\\&\quad=(h_0k_0\oplus\cdots\oplus h_{n-1}k_{n-1})\\&\qquad\oplus(g_0\,(h_0\oplus k_0)\oplus\cdots\oplus g_{n-1}\,(h_{n-1}\oplus k_{n-1}))\\&\quad=(h_0k_0\oplus k_0g_0\oplus g_0h_0)\\&\qquad\oplus\cdots\oplus(h_{n-1}k_{n-1}\oplus k_{n-1}g_{n-1}\oplus g_{n-1}h_{n-1})\\&\quad=\sum_{i=0}^{n-1}(g_ih_i\oplus h_ik_i\oplus k_ig_i)\,.\end{aligned}\tag{11}$$

From (10) and (11), (8) and (9) are the same, and Theorem 1 has been proven. □

III. KEY AGREEMENT PROTOCOL USING SYLVESTER HADAMARD MATRICES

Two users A and B want to share a common key for secure communication on public channels. A trusted authority (TA) shares secret keys K_{AS} and K_{BS} with A and B, respectively. After key agreement, A and B share a session key K_{AB}. A, B, and the TA share n; i.e., they agree in advance to use the same matrix for this key agreement. Users can share a m bit session key with a $2^n\times 2^n$ Sylvester Hadamard matrix and N bit numbers g, h, and k that can be divided into m numbers of n bits such as $g=(g_0,g_1,\cdots,g_{m-1})$, where $N=mn$. The key agreement process, shown in Fig. 1, is as follows.

1) A randomly generates g, encrypts it with K_{AS}, and sends the encrypted message to the TA.
2) The TA randomly generates h, encrypts it with K_{AS} and K_{BS}, and sends the encrypted messages to B with $g\circ h$.
3) B randomly generates k and obtains g from $g\circ h$ and h. Then, from (6), B can calculate

$$\begin{aligned}K_{\mathrm{AB}}&=K_{\mathrm{AB}_0}||\cdots||K_{\mathrm{AB}_{m-1}}\\&=\varphi(h_0,k_0)\,\varphi(g_0,h_0\circ k_0)\,||\cdots||\\&\quad\varphi(h_{m-1},k_{m-1})\,\varphi(g_{m-1},h_{m-1}\circ k_{m-1})\,.\end{aligned}\tag{12}$$

Thereafter B encrypts g with K_{AB}, and sends it and the message from the TA that is encrypted by K_{AS} to A with $h\circ k$.

4) A obtains k from $h\circ k$ and k. Then, from (6), A can calculate

$$\begin{aligned}K_{\mathrm{AB}}&=K_{\mathrm{AB}_0}||\cdots||K_{\mathrm{AB}_{m-1}}\\&=\varphi(h_0,k_0)\,\varphi(g_0,h_0\circ k_0)\,||\cdots||\\&\quad\varphi(h_{m-1},k_{m-1})\,\varphi(g_{m-1},h_{m-1}\circ k_{m-1})\,.\end{aligned}\tag{13}$$

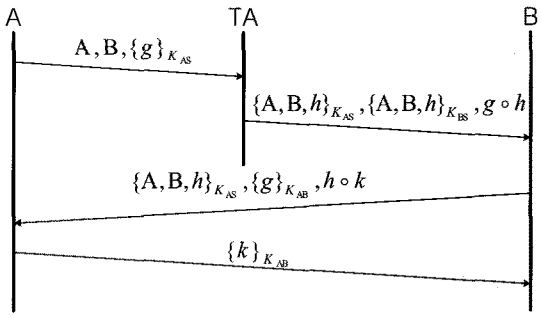

Fig. 1. Proposed key agreement protocol.

Thereafter A decrypts g with K_{AB} for confirmation, encrypts k with K_{AB} and sends it to B. B decrypts k with K_{AB} for confirmation.

From (6), (12) and (13) are guaranteed to be the same.

IV. SECURITY ANALYSIS

In the proposed protocol, key authentication for A and B is provided, since the protocol is based on symmetric ciphers. Also, since A and B randomly generate g and k, respectively, and they can confirm each other's session keys in steps 3) and 4) of the key agreement, key freshness and key confirmation are provided.

During the key agreement, only $g\circ h$ and $h\circ k$ are not encrypted. Thus, nobody other than the TA, A, and B can obtain one of g, h, or k without revealing K_{AS} or K_{BS}. We present the simplest example: Let $N=m=n=1$. If $g\circ h=1$ and $h\circ k=0$, then there are two cases of g, h, and k such that $(g,h,k)=(1,0,0)$ or $(g,h,k)=(0,1,1)$, and g, h, and k cannot be determined without additional information.

Theorem 2: The probability of every possible m bit session key in the proposed protocol is always $1/2^m$; i.e., the probability that any segment of an agreed key is 1 (or -1) is 1/2.

Proof: From (3) and (7), $\forall i\in\{0,1,\cdots,m-1\}$,

$$\begin{aligned}K_{\mathrm{AB}_i}&=\varphi(g_i,h_i)\,\varphi(g_i\circ h_i,k_i)\\&=(-1)^{\langle g_i,h_i\rangle}(-1)^{\langle g_i\circ h_i,g_i\rangle}\\&=(-1)^{\langle g_i,h_i\rangle+\langle g_i\circ h_i,g_i\rangle}.\end{aligned}\tag{14}$$

In (14), the base is -1, and the result of calculation is the same if all additions ("+") are changed into mod 2 additions ("⊕"), i.e., bitwise XOR is realized. Hereafter, we use g, h, and k instead of g_i, h_i, and k_i, respectively, and consider their binary expression, such as $g=(g_0,g_1,\cdots,g_{n-1})$ where $\forall l\in\{0,1,\cdots,n-1\}, g_l\in\{0,1\}$.

Then, from the proof of Theorem 1, the exponent of (14) becomes the following.

$$\langle g,h\rangle\oplus\langle g\circ h,k\rangle=\sum_{l=0}^{n-1}(g_lh_l\oplus h_lk_l\oplus k_lg_l)\,.\tag{15}$$

For each l, let $X_l=g_lh_l\oplus h_lk_l\oplus k_lg_l$. There are four possible cases. If all of g_l, h_l and k_l are 1, $X_l=1$. In contrast, if all of them are 0 (i.e., none of them are 1), $X_l=0$. Each of these two cases has one possibility. If two of them are 1, $X_l=1$.

In contrast, if exactly two of them are 0 (i.e., only one of them is 1), $X_l = 0$. Each of these two cases has three possibilities. Therefore, the probability of $X_l = 1$ is 1/2. Also, the same is true of $X_l = 0$. Thus, each X_l has the same probabilities of 0 and 1, and (15) does as well. Then, for each i, the probability that (14) is 1 is 1/2, and Theorem 2 has been proven. □

From Theorem 2, we can find that each K_{AB_i} has the same probability of 1 and -1, even though the number of 1's and that of 0's in a Sylvester Hadamard matrix are different (for example, select a 4×4 (i.e., $n = 2$) Sylvester Hadamard matrix to share a 1 bit session key. Then, the number of 1's in H_{2^2} is 10, the number of 0's is 6, and there are a total of 64 cases of $[g, h, k]$. Accordingly, there are 64 cases of the session key, and in 32 [half] of them, the key is 1). This property means that every possible key in the proposed protocol has the same probability, and the generated session keys are probabilistically secure.

V. CONCLUSION

In this paper, we proposed a key agreement protocol using Sylvester Hadamard matrices. This protocol allows users to share a common session key without using conventional public key ciphers. To do this, no exponential operation is needed; only bitwise addition, multiplication and XOR. Furthermore, users do not need to compute and keep all of the matrix entries because they can directly obtain each entry they need by using (3). Moreover, the risk of leakage of secret information is minimized, since only incomplete information used for key generation is shared.

The computation time of this key agreement is proportional to $N = mn$ where m is the length of the common key that the users agree to use, and n is the factor that determines the size of the Sylvester Hadamard matrix that they share in advance. It is difficult for an eavesdropper to guess promising keys, since the probabilities of all possible keys are the same.

REFERENCES

[1] C.-h. Choe, G. Y. Hwang, S. H. Kim, H. S. Yoo, and M. H. Lee, "Key agreement protocols based on the center weighted jacket matrix as a symmetric co-cyclic matrix," *Lecture Notes in Computer Science* 4105, pp. 121–127, Sept. 2006.

[2] C.-h. Choe, J. Hou, S. J. Choi, S. Y. Kim, and M. H. Lee, "Co-cyclic jacket matrices for secure communication," in *Proc. IWSDA*, Shimonoseki, Japan, Oct. 2005, pp. 103–105.

[3] K. J. Horadam, *Hadamard Matrices*, Princeton University Press, 2007.

[4] K. J. Horadam and P. Udaya, "Cocyclic Hadamard codes," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1545–1550, July 2000.

[5] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

Chang-hui Choe received the B.S. degree in computer science from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Republic of Korea, in 1999, and the M.S. and Ph.D. degrees in Information Security Engineering from the Chonbuk National University, Jeonju, Republic of Korea, in 2006 and 2010, respectively. He is a Lecturer at the Chonbuk National University. His major interests are cryptography, information security, cyber security, and mobile communications.

Moon Ho Lee received both his B.S. and M.S. degrees in Electrical Engineering from Chonbuk National University, Jeonju, Republic of Korea, in 1967 and 1976, respectively, and his Ph.D. degrees in Electronics Engineering from Chonnam National University, Gwangju, Republic of Korea, in 1984 and from the University of Tokyo, Japan, in 1990. From 1970 to 1980, he was a chief engineer with Namyang Moonhwa Broadcasting Corporation. Since 1980, he has been a Professor in the department of electronic engineering at Chonbuk National University. From 1985 to 1986, he was also with the University of Minnesota, as a postdoctoral fellow. He held Visiting Positions at the University of Hanover, Germany, 1990; the University of Aachen, Germany 1992 and 1996; and the University of Munich, Germany, 1998. He has authored 34 books, including Digital Communication (Youngil, 1999, Korea), Information and Coding (Bokdu, 1998, Korea), Digital Image Processing (Daeyoung, 1994, Korea), and Digital Filter Design (Daeyoung, 1995, Korea). His current research interests include multi-dimensional source and channel coding, mobile communications, image processing, information security, signal processing, digital communications, and polar codes. He is a Registered Telecommunication Professional Engineer and a member of the National Academy of Engineering in Korea. He was the recipient of the paper prize award from the Korean Institute of Communication Science in 1986 as well as in 1997, the Institute of Electronics Engineers of Korea in 1987, and Chonbuk Province in 1992, and the commendation of the Prime Minister in 2002 for inventing the Jacket matrix. In addition, he won the Best Paper Awards from ICSEA, France, in 2006; ICSNC, France, in 2006; and EITC, Korea, in 2006. Furthermore, he won the National Order of Merit, the Doyak Medal, from the Korean government in 2007; the Haedong Information and Communications Best Prize from the Korea Information and Communications Society in 2007; the Award for Scientist and Engineer of the Month from the Ministry of Science and Technology and the Korea Science and Engineering Foundation in January, 2008; the Best Paper Awards from CEIC 2009 and CEIC 2010, sponsored by IEEE's Korea Daejeon Section; and the Grand Alumni Award from the Chonbuk National University's alumni association in 2009. Moreover, he has been a principal of the World Class University project since 2008 and an honor professor of Central South University, China, since 2009.