MULTIPARTY KEY AGREEMENT PROTOCOL BASED ON SYMMETRIC TECHNIQUES

HYANG - SOOK LEE, YOUNG-RAN LEE, JU-HEE LEE

Department of Mathematics
Ewha Womans University
11-1, Daehyun-dong, Seodaemun-gu, Seoul, 120-750, Korea
hsl@mm.ewha.ac.kr, sens1990@yahoo.co.kr, 00cookie@hanmail.net

ABSTRACT. In this paper, we propose a multiparty key agreement protocol by generalizing the Blom's scheme based on 2 variable polynomials. Especially we develop three party and four party key agreement schemes with security. The advantage of the new schemes is to have small demands on storage space.

0. INTRODUCTION

We assume the network has N-users and every message transmitted in the network by encryption should be protected. For the encryption, we usually use a public key cryptosystem or conventional cipher. In the second case we distribute keys by key distribution center or by pubilc key distribution algorithm. In either case many protocols are developed for sharing the common key between two participants. The problem of setting a common key between more than two participants has already been addressed by using pubilc key distribution algorithm. The example is the protocol of conference key system [7]. Recentely, tripartite new scheme was developed by using Weil pairing based on Diffie-Hellman [10]. This system needs only a single round communication. In this paper, we propose a multipart-key ageement scheme with a parameter k, where k is the largest size of the coalition against security of the scheme. In our setting, we assume a key

2000 Mathematics Subject Classification: 94A60, 11T71, 11T06.
Key words and phrases: key agreement protocol, Blom's scheme, symmetric technique.
[1]The authors were supported by the MOST through National R & D Program M10022040004-01G050900310 for Women's Universities.

distribution center (KDC) and the secret data used to generate keys are sent from the KDC to the user in a secret way. The advantage of this system is to reduce the number of round communication and to have small demands on storage space.

This paper is organized as follows.

We begin in section 2 by reviewing Blom's basic scheme. Section 3 presents the multi-party key distribution scheme. First we give the special case of the scheme sharing the keys among three users with the security $k = 1$. Furthermore, we also deal with the case of four users with $k = 1$ and $k = 2$. Section 4 proves the security of the schemes suggested in the previous section. Section 5 shows the advantages of our multiparty key schemes and summarizes our results with the future work.

1. PRELIMINARIES

Many key distribution systems are used in the field of protocol algorithm. In this section, we introduce Blom's scheme which gives the motivation of our scheme.

In this scheme we assume that there exists a key distribution center and that user keys or secret data used to generate keys are sent from the center to the users in a secure way.

BLOM'S BASIC SCHEME : We introduce the scheme using two variable polynomials with $k = 1$.

STEP 1. A prime number p is public. For each user U, an element $r_U \in Z_p$ is chosen to be public and the elements r_U must be distinct.

STEP 2. The KDC chooses three random elements $a, b, c \in Z_p$ which is not necessarily distinct, and forms the polynomial

$$f(x, y) = a + b(x + y) + cxy \pmod{p}$$

STEP 3. For each user U, the KDC computes the polynomial

$$g_U(x) = f(x, r_U) \pmod{p}$$

and transmits $g_U(x)$ to U over a secure channel. Note that $g_U(x)$ is a linear polynomial in x, so it can be written as

$$g_U(x) = a_U + b_U x \pmod{p}$$

where $a_U = a + br_U$ and $b_U = b + cr_U$.

STEP 4. If U and V want to communicate, then they use the common key

$$K_{U,V} = K_{V,U} = f(r_U, r_V) = a + b(r_U + r_V) + c(r_U r_V) \pmod{p},$$

where U and V obatin $K_{U,V}$ by computing $g_U(r_V)$ and $g_V(r_U)$ respectively.

The security of the Blom's scheme is proved where the number of the coalition is one. Hence no user can determine any information about the common key of two other participants.

THEOREM 1.1 [1] The Blom's scheme is unconditionally secure against any individual user. □

However the coalition of k users, $k \geq 2$, will be able to determine any key they wish.

2. MULTI-PARTY KEY DISTRIBUTION SYSTEM

In this section we propose three party key agreement protocol with $k = 1$ and four party protocol with $k = 1$ and $k = 2$.

2.1. THREE PARTY CASE

STEP 1. A prime number p is public. For each user U, an element $r_U \in Z_p$ is chosen to be public and the element r_U must be distinct.

STEP 2. The KDC chooses four random elements $a, b, c, d \in Z_p$ which is not necessarily distinct and forms the polynomial

$$f(x, y, z) = a + b(x + y + z) + c(xy + yz + zx) + d(xyz) \pmod{p}.$$

STEP 3. For each user U, the KDC computes the polynomial

$$g_U(x, y) = f(x, y, r_U) \pmod{p}$$

and transmits $g_U(x, y)$ to U over a secure channel. Note that $g_U(x, y)$ can be written as

$$g_U(x, y) = a_U + b_U(x + y) + c_U(xy)$$

where $a_U = a + br_U, b_U = b + cr_U$ and $c_U = c + dr_U \pmod{p}$.

STEP 4. If U, V and W want to communicate, then they use the common key

$$\begin{aligned} K_{U,V,W} &= f(r_U, r_V, r_W) \\ &= a + b(r_U + r_V + r_W) + c(r_U r_V + r_V r_W + r_W r_U) + dr_U r_V r_W \pmod{p} \end{aligned}$$

where $[\, i, j, k, \ell]$ is the class of indices i, j, k and l which appears ignoring the order and we denote $a_{[i,j,k,\ell]}$ by a_* if $i+j+k+\ell = *$.

STEP 3. For each user U, the KDC computes the polynomial

$$\begin{aligned} g_U &= f(x,y,z,r_U) \\ &= a_U + b_U(x+y+z) + c_U(x^2+y^2+z^2) + d_U(xy+yz+zx) + \\ &\quad e_U(xy^2+yz^2+zx^2+yx^2+zy^2+xz^2) + f_U(x^2y^2+y^2z^2z^2x^2) + \\ &\quad g_U(xyz) + h_U(xyz^2+yzx^2+xzy^2) + k_U(xy^2z^2+yz^2x^2+zx^2y^2) + \\ &\quad \ell_U(x^2y^2z^2) \pmod p \end{aligned}$$

where

$$\begin{aligned} a_U &= a + br_U + cr_U{}^2, & b_U &= b + dr_U + er_U{}^2, \\ c_U &= c + er_U + fr_U{}^2, & d_U &= d + gr_U + hr_U{}^2, \\ e_U &= e + hr_U + kr_U{}^2, & f_U &= f + kr_U + \ell r_U{}^2, \\ g_U &= g + mr_U + nr_U{}^2, & h_U &= h + nr_U + or_U{}^2, \\ k_U &= k + or_U + pr_U{}^2, & \ell_U &= \ell + pr_U + qr_U{}^2, \end{aligned}$$

and

$$\begin{aligned} a &= a_{[0,0,0,0]}, & b &= a_{[0,0,0,1]} \\ c &= a_{[0,0,0,2]}, & d &= a_{[0,0,1,1]} \\ e &= a_{[0,0,1,2]}, & f &= a_{[0,0,2,2]} \\ g &= a_{[0,1,1,1]}, & h &= a_{[0,1,1,2]} \\ k &= a_{[0,1,2,2]}, & \ell &= a_{[0,2,2,2]} \\ m &= a_{[1,1,1,1]}, & n &= a_{[1,1,1,2]} \\ o &= a_{[1,1,2,2]}, & p &= a_{[1,2,2,2]} \\ q &= a_{[2,2,2,2]}, \end{aligned}$$

STEP 4. If U, V, W and R want to communicate, then they use the common key

$$K_{U,V,W,R} = f(r_U, r_V, r_W, r_R)$$

where U, V and W obtainsthe common key $K_{U,V,W}$ by computing $g_U(r_V, r_W), g_V(r_U, r_W)$ and $g_W(r_V, r_U)$.

2.2. FOUR PARTY CASE WITH $k = 1$

STEP 1. This is the same as the first step in 2.1.

STEP 2. The KDC chooses five random elements $a, b, c, d, e \in Z_p$ which is not necessarily distinct and forms the polynomial

$$\begin{aligned} f(x,y,z,w) &= a + b(x+y+z+w) + c(xy+yz+zw+wx+xz+yw) \\ &\quad + d(xyz+xzw+yzw+xyw) + e(xyzw) \pmod p. \end{aligned}$$

STEP 3. For each user U, the KDC computes the polynomial

$$\begin{aligned} g_U(x,y,z) &= f(x,y,z,r_U) \\ &= a_U + b_U(x+y+z) + c_U(xy+yz+zx) + d_U(xyz) \pmod p \end{aligned}$$

where $a_U = a + br_U, b_U = b + cr_U, c_U = c + dr_U$ and $d_U = d + er_U \pmod p$.

STEP 4. If U, V, W and R want to communicate, then they use the common key

$$\begin{aligned} K_{U,V,W,R} &= f(r_U, r_V, r_W, r_R) \\ &= a + b(r_U + r_V + r_W + r_R) + c(r_U r_V + r_U r_W + r_U r_R + r_V r_W \\ &\quad + r_V r_R + r_W r_R) + d(r_U r_V r_W + r_U r_W r_R + r_U r_R r_V + r_V r_W r_R) \\ &\quad + e(r_U r_V r_W r_R) \pmod p \end{aligned}$$

where U computes $K_{U,V,W,R}$ as $f(r_U, r_V, r_W, r_R) = g_U(r_V, r_W, r_R)$ and similarly for V, W and R.

2. 3. FOUR PARTY CASE WITH $k = 2$

In this case, we choose the different type of the polynomial in step 2.

STEP 1. This is the same as the first step in 2.1.

STEP 2. The KDC chooses the random elements $a_{i,j,k,\ell} \in Z_p, 0 \le i, j, k, \ell \le 2$ which is not necessarily distinct and forms the polynomial

$$f(x,y,z,w) = \sum_{i=0}^{2}\sum_{j=0}^{2}\sum_{k=0}^{2}\sum_{\ell=0}^{2} a_{[ijk\ell]}\, x^i y^j z^k w^\ell \pmod p$$

It is possible to generalize our scheme for general n users using the different polynomials in step 2. Next we show the security of our scheme against the coalition of the other users.

3. Proof of the Security

In this section we show the security of our schemes which we proposed in Section 2. Recall k is the largest size of the coalition. In the three party case, the scheme is safe for $k = 1$. In the four party case, the scheme is safe for $1 \leq k \leq 2$.

3.1. SECURITY OF THE SCHEME 2.1. Suppose that X wants to try to compute the common key of three participants U, V and W,

$$K_{U,V,W} = a + b(r_U + r_V + r_W) + c(r_U r_V + r_V r_W + r_W r_U) + d(r_U r_V r_W) \pmod{p}$$

where the value r_U, r_V and r_W is public, but a, b, c and d are unknown. Now the adversary X can obtain the values, $a_X = a + br_X, b_X = b + cr_X$ and $c_X = c + dr_X \pmod{p}$ from KDC. First X guesses the common key $K_{U,V,W}$ by l. With the information of X and l, the following matrix equation is induced over Z_p.

$$\begin{pmatrix} 1 & r_U + r_V + r_W & r_U r_V + r_V r_W + r_W r_U & r_U r_V r_W \\ 1 & r_X & 0 & 0 \\ 0 & 1 & r_X & 0 \\ 0 & 0 & 1 & r_X \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} l \\ a_X \\ b_X \\ c_X \end{pmatrix}.$$

Let the above matrix equation be $\mathcal{CX} = \mathcal{B}$. Then,

$$det(\mathcal{C}) = (r_X - r_U)(r_X - r_V)(r_X - r_W).$$

Since r_U, r_V, r_W and r_X are all distinct, $det(\mathcal{C})$ is nonzero. Hence the matrix equation has unique solution for a, b, c and d. However this implies the possible values of a, b, c and d depend only on the information of X itself. Therefore it is impossible for X to derive the exact values of a, b, c and d from his own information. If we have a network of three users then the largest size k of the coalition against the security is only one. If $k > 1$, then the scheme is not secure. We show the case of $k = 2$. Let X and Y be adversaries to derive the common key $K_{U,V,W}$ and assume $\{X, Y\} \bigcap \{U, V, W\} = \emptyset$. Then X and Y combine their information $a_X = a + br_X, a_Y = a + br_Y, b_X = b + cr_X, b_Y = b + cr_Y, c_X = c + dr_X$ and $c_Y = c + dr_Y$. Thus they have six-equations in four unknowns and they can easily compute the unique solution for a, b, c and d. Therefore they can form the polynomial $f(x, y, z)$ and compute any key they wish.

3.2. SECURITY OF THE SCHEME 2.2. We suppose that we have four participants sharing the key, say U, V, W and R. Assume that the adversary X wants to try to compute the common key

$$\begin{aligned} K_{U,V,W,R} &= a + b(r_U + r_V + r_W + r_R) + c(r_U r_V + r_U r_W + r_U r_R + r_V r_W + \\ &\quad r_V r_R + r_W r_R) + d(r_U r_V r_W + r_V r_W r_R + r_U r_V r_R + r_U r_W r_R) \\ &\quad + e(r_U r_V r_W r_R) \pmod{p}. \end{aligned}$$

The values r_U, r_V, r_W and r_R are public, but a, b, c, d and e are unknown. Because X has the polynomial $g_X(x, y, z)$ that was transmitted by KDC, he knows the values $a_X = a + br_X, b_X = b + cr_X, c_X = c + dr_X$ and $d_X = d + er_X \pmod{p}$.

The adversary X guesses the common key l and he wants to conclude $l = K_{U,V,W}$ by using the known information. He induces the following matrix equation over Z_p.

$$\begin{pmatrix} 1 & r_U + \cdots + r_R & r_U r_V + \cdots + r_W r_R & r_U r_V r_W + \cdots + r_U r_V r_R & r_U r_V r_W r_R \\ 1 & r_X & 0 & 0 & 0 \\ 0 & 1 & r_X & 0 & 0 \\ 0 & 0 & 1 & r_X & 0 \\ 0 & 0 & 0 & 1 & r_X \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix} = \begin{pmatrix} \ell \\ a_X \\ b_X \\ c_X \\ d_X \end{pmatrix}$$

For convenience, let the above matrix equation be $\mathcal{CX} = \mathcal{B}$. Since r_U, r_V, r_W, r_R and r_X are all distinct,

$$det(\mathcal{C}) = (r_X - r_U)(r_X - r_V)(r_X - r_W)(r_X - r_R) = 0.$$

Thus $\mathcal{C}$ has the unique solution for a, b, c, d and e, but those values always depend on l and the information of X.

3.3. SECURITY OF THE SCHEME 2.3. We suppose that the coalition of two users, say X and Y, wants to try to compute the key

$$\begin{aligned} K_{U,V,W,R} &= f(x, y, z, w) \\ &= \sum_{i=0}^{2}\sum_{j=0}^{2}\sum_{k=0}^{2}\sum_{\ell=0}^{2} a_{[ijk\ell]}\, x^i y^j z^k w^\ell \pmod{p} \end{aligned}$$

where$[i, j, k, \ell]$ is the class of indices i, j, k and l which appear ignoring the order. We denote $a_{i,j,k,\ell}$ by a_* if $i+j+k+\ell = *$. The value r_U, r_V, r_W and r_R are public,

but $a_{i,j,k,\ell}$ are unknown. Now X and Y combine their informatin from KDC,

$$\begin{aligned}
a_X &= a + br_X + cr_X{}^2 & a_Y &= a + br_Y + cr_Y{}^2 \\
b_X &= b + dr_X + er_X{}^2 & b_Y &= b + dr_Y + er_Y{}^2 \\
c_X &= c + er_X + fr_X{}^2 & c_Y &= c + er_Y + fr_Y{}^2 \\
d_X &= d + gr_X + hr_X{}^2 & d_Y &= d + gr_Y + hr_Y{}^2 \\
e_X &= e + hr_X + kr_X{}^2 & e_Y &= e + hr_Y + kr_Y{}^2 \\
f_X &= f + kr_X + \ell r_X{}^2 & f_Y &= f + kr_Y + \ell r_Y{}^2 \\
g_X &= g + mr_X + nr_X{}^2 & g_Y &= g + mr_Y + nr_Y{}^2 \\
h_X &= h + nr_X + or_X{}^2 & h_Y &= h + nr_Y + or_Y{}^2 \\
k_X &= k + or_X + pr_X{}^2 & k_Y &= k + or_Y + pr_Y{}^2 \\
\ell_X &= \ell + pr_X + qr_X{}^2, & \ell_Y &= \ell + pr_Y + qr_Y{}^2.
\end{aligned}$$

Thus they have 20 equations with 15 unknowns. From the above equations, they can obtain the following equations.

$$\begin{aligned}
a_X - a_Y &= (r_X - r_Y)[b + cr_X + cr_Y{}^2], \\
b_X - b_Y &= (r_X - r_Y)[d + er_X + cr_Y{}^2], \\
c_X - c_Y &= (r_X - r_Y)[e + fr_X + cr_Y{}^2], \\
d_X - d_Y &= (r_X - r_Y)[g + hr_X + cr_Y{}^2], \\
e_X - e_Y &= (r_X - r_Y)[h + kr_X + cr_Y{}^2], \\
f_X - f_Y &= (r_X - r_Y)[k + \ell r_X + cr_Y{}^2], \\
g_X - g_Y &= (r_X - r_Y)[m + nr_X + cr_Y{}^2], \\
h_X - h_Y &= (r_X - r_Y)[n + or_X + cr_Y{}^2], \\
k_X - k_Y &= (r_X - r_Y)[o + pr_X + cr_Y{}^2], \\
\ell_X - \ell_Y &= (r_X - r_Y)[p + qr_X + cr_Y{}^2],
\end{aligned}$$

Using $r_X = r_Y$, X and Y have the following matrix equation over Z_p.

$$\left[\frac{1}{r_X - r_Y}\right] \begin{bmatrix} a_X - a_Y \\ b_X - b_Y \\ c_X - c_Y \\ d_X - d_Y \\ e_X - e_Y \\ f_X - f_Y \\ g_X - g_Y \\ h_X - h_Y \\ k_X - k_Y \\ \ell_X - \ell_Y \end{bmatrix} = \begin{pmatrix} 0 & 1 & * & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & * & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & * & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \\ e \\ f \\ g \\ h \\ k \\ \ell \\ m \\ n \\ o \\ p \\ q \end{pmatrix}$$

where $* = r_X + r_Y$. Simply say $\mathcal{CX} = \mathcal{B}$. A linear system $\mathcal{CX} = \mathcal{B}$ is an underdetermined linear system, since the number of unknowns is 15 and the number of the equations is 10. Then the column vectors of $\mathcal{C}$ cannot be linearly independent. Moreover, by the dimension theorem for the matrices, our system has infinitely many solutions. Hence, the coalition of two user X and Y cannot determine the exact value of $(a, b, c, d, e, f, g, h, k, l, m, n, o, p, q)$. In other words, they cannot rule out only values for $K_{U,V,W,R}$.

4. Advantages and Remarks

4.1. Advantages of Our Scheme Our scheme is originated from Blom's scheme but it has more advantages than Blom's scheme. There are two advantages from our scheme. The first advantage is the following. In the process of generating common key, it has lots of computational process since the Blom's scheme gives unique key for each pair of users. If one is changed between user's pair, both of them have to change their common key. However, our scheme generate a common key only one time for all users. If n users want to generate a common key for each user then the Blom's scheme must generate $\binom{n}{2}$ key, but our scheme must generate only one time. The second advantage is to reduce the size of key storage space. We assume that the network has n users and they want to have a common key for every users, then the Blom's scheme requires $\binom{n}{2} nlogp$-bits or $n^2 logp$-bits since the required number of secure channels has been reduced from $\binom{n}{2}$ to n. But our scheme requires $nlogp$-bits since the number of computation is only one-time.

4.2. CONCLUSION AND FUTURE WORKS We have described a multiparty key agreement protocol for which each party compute the common key by using other party's public data and the transmitted polynomial. The presented protocol is established non-interactively. So we can reduce the number of generating step of common key, and also the size of key storage. Although our scheme contribute to one-time common key setup in multiparty communication, our scheme is not so much practical. The presented protocol ignores the very real problem of how to distribute secret data. For the security, this protocol relies on the absolute trusted third party, key distributed center. So, if the adversary pretend to be KDC, this scheme suffers a fatal blow. In that point of view, we want to develop the dynamic keying conference based on public-key technique. One of examples is a tripartite generalization of the Diffie-Hellman protocol using Weil and Tate pairings by Antoine Joux [10]. We desire the efficient scheme satisfying the principle of security.

REFERENCES

[1] R.Blom, *Non-public key distribution*, Advances in cryptology-Proceedings of Crypto82, pp. 231-236,1983..

[2] R.Blom, *An optimal class of symmetric key generation systems*, Advances in cryptology-proceedings of EUROCRYPT 84 LNCS vol. 209 , pp.335-338, 1985.

[3] C. Blundo, A. De santis, A. Herzberg, S. Kutten, U.Vaccaro, and M. Yung, *Perfectly-secure key distribution for dynamic conferences*, Advances in cryptology-CRYPTO'92, LNCS vol. 740, pp. 471-486,1993.

[4] Matsumoto,T. and Imai,H. , *On the key predistribution system: a practical solution to the key distribution problem*, Advanced in Cryptology-CRYPTO'87 LNCS vol. 293, pp.185-193, 1988.

[5] Waterloo Maple. **http:// www.maplesoft.com/products/Maple6.**

[6] F. J. MacWilliams and N.J.A. Sloane, chapter 11 in : *The Theory of error correcting codes*, North Holland, Amsterdam (Third Pressing 1981).

[7] M. Stein, G. Tsudik, M. Waidner, *Diffie Hellman Key Distribution Extended to Group Communication*, ACM conference on computer and communication security, 1996.

[8] D. R. Stinson, *Cryptography Theory and Practice*, CRC press.

[9] A.J.Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of applied cryptography*, CRC press.

[10] Antoine Joux, *A one round protocol for tripartite Diffie-Hellman*, ANTS 2000.