Treatment of Weakness of partition in key computation phase

معالجة ضعف التقسيم في طور حساب المفتاح

المدرس الدكتور

صلاح عبد الهادي البيرماني

الكلية الاسلامية الجامعة

معالجة ضعف التقسيم في طور حساب المفتاح

المدرس الدكتور
صلاح عبد الهادي البيرماني
الكلية الاسلامية الجامعة

المستخلص :

تعتبر كفاءة توزيع المفتاح من المسائل المهمة لتأمين اتصالات مجموعة ، ففي هذه الورقة التي تعالج وتحسب طور حساب المفتاح ضمن حالة g من الأطراف الممتدة من حالة طرفيين ضمن مخطط توزيع المفتاح (KDS). اتفاقية التوزيع تنقسم إلى طورين، طور التوزيع، وطور حساب المفتاح، ففي طور حساب المفتاح توجد مجموعة جزئية من المستفيدين G في U (U مجموعة كل المستفيدين)،التي تمثل مؤتمر، يُحسب المفتاح المشترك للمؤتمر باستخدام معلومات سرية تصل من TA المخول الموثوق (الخادم المخول الموثوق) و الرسائل الموجودة على الشبكة خلال الطور. قبل تقسيم المستخدمين تبعاً إلى المعلومات الخاصة لا يعرف المؤتمر G الذي يكون المفتاح العام فيما بعد. في هذه الورقة استخدمنا مخطط قبل توزيع المفتاح العام للمستخدمين في المؤتمر وتطوير طريقة رياضية لحساب طور حساب المفتاح ضمن حالة g من الأطراف. الهدف من هذه الورقة هي تحسين توزيع المفتاح ومعالجة ضعف التقسيم في طور حساب المفتاح لبلوندو.

Abstract

Efficient key distribution is an important problem for secure group communications. In this paper, that is processing and computing key computation phase to g-party case which extends to 2-party case in key distribution scheme (KDS) . It is a

distribution protocol, divided into two phases : a distribution phase and a key computation phase . In the key computation phase some subset of users G in U, referred to as a conference, computes a common key using the secrete information received by the trusted authority TA and the messages 'seen' over the network during a phase. Before providing users with private information, does not know which conference G will recover a common key later. In this paper we use key pre-distribution scheme to generate common key of users in conference and development mathematical method to compute key computation phase for g-party case. The goal of this paper to improvement key distribution and treatment of the weakness of partition in key computation phase of Blundo.

Keywords

Key distribution, Broadcast encryption, Dynamic conference, Cryptography.

1.Introduction

Key distribution is a major problem in an environment where a large number of nodes communicate with each other[5]. The increase in bandwidth, size, usage, and applications of such systems is likely to pose new challenges on the required novel idea. A growing application area in networking is " conferencing" where a group of entities (or network locations)

collaborate privately in an interactive procedure (such as : board meeting, scientific discussion, a task-force, a classroom, or an interactive engineering design group). In this paper we consider the distribution for g-party communication (session-keys or common keys) is conference of size g. When a subset of users in network, referred to as a *conference*, or a group of users of a network, wishes to communicate privately, encryption algorithms can be used to provide security against eavesdropping. If conventional (private-key) cryptography is used, a common key must be shared by members of the conference.

A key distribution scheme (KDS) for dynamic conference is a method by which initially (off-line) trusted authority (TA) server distributes private individual pieces of information to a set of users [1], in such way that each group can compute a common key for secure communication. Usually, we have a distribution phase, in which a trusted authority (TA) distributes information in private way to each user and a key computation phase, where a conference computes a common key. If they have received the conference computed common key from certain majority of values received. Conference key (or common key) must be secure against attacks performed by a coalition of users, or servers [2].The user in a conference G in U must be able to compute the same conference key, after interacting with a subset

of good servers or users. The scheme is *unconditionally* secure if any disjoint coalition of adversaries does not gain information about the conference key, even through it has access to an infinite computational power. In this paper we restrict attention to unconditional secure KDS.

There are two methods for secure communication of users in broadcast networks used to solve all problems related to the confidentiality and authenticity of transmitted information. The first method is the *key pre-distribution scheme*. Secrete information is given to each user by the TA in the distribution phase. Later, in the key computation phase, every member of conference G can reconstruct the common key K_G from *his piece* and conference *identity*, while disjoint coalition F of adversaries does not gain any information about K_G.

The approach of distribution mechanism may still require that keys are unconditionally secure but only with respect to coalitions of limited size[3]. Blom [4] using MDS codes, an efficient scheme for conference G of size 2 and coalition F of size b. Other related schemes are presented in [5][6], subsequently, for conference G size g and coalitions of adversaries F of size b, in [1][3], using entropy.

A second approach allows interaction among the users in conference. In the key computation phase the members of

conference G, using the secret information received in the distribution phase, this approach, which is called the key agreement scheme (KAS), initiated in [1], was continued by Beimel and Chor [7][8]. It is aimed to reduce the size of information for each user must keep secret.

In [9] the authors presented a generalization of one-restricted scheme described by Beimel and Chor [7][8], using tools from design theory.

Fiat and Naor [10] introduced a new key distribution scheme referred to as the *broadcast encryption scheme*. The TA gives some predefined keys to each user in the distribution phase. More about broadcast encryption analysis is cited in [11,12,13,14,15,16,17]. Other key distribution schemes are known in the literatures. A survey of unconditional secure schemes can be found in [18], while general model for unconditional secure KDS can be found in [19].

The analysis of τ-restricted key agreement schemes can be found in [3].

In this paper, we process and compute key computation phase without using hyper graph on n points, but by using anther approach to find disjoint parallel classes.

2. A Key Predistribution Scheme

Key Predistribution refers to methods whereby a trusted authority (TA) will distributed secret information in such a way that specified privileged subsets of participants will be able to compute certain keys. In this section we describe the (g,b)-KPS given in [5][3]. Let $U=\{1, 2, \ldots, n\}$ be a set of n users and $G \subseteq U$ a conference of size g. Let p be a prime such that $p \geq n$ (the number of users). The TA chooses n distinct random numbers $s_i \in Z_p$ and gives s_i to user i ($1 \leq i \leq n$). These values s_i do not need to be secret and can be thought of as the 'identity' of user i Thus, for example, it is sufficient to take $s_i = i$ for $1 \leq i \leq n$. Next, the TA constructs a random symmetric polynomial in g variables with coefficients from Z_p, in which the degree of any variable is at most b:

$$f(x_1, \ldots, x_g)=\sum_{i_1=0}^{b} \ldots \sum_{i_g=0}^{b} a_{i_1,\ldots,i_g} x_1^{i_1} \ldots x_g^{i_g} .$$

The fact that f is symmetric is equivalent to $a_{i_1,\ldots,i_g} = a_{\pi(i_1),\ldots,\pi(i_g)}$ for all permutations π of $\{1, \ldots, g\}$.

Then, for $1 \leq i \leq n$, the TA computes a polynomial g_i in g-1 variables $x_2, \ldots, x_g$ by setting $x_1=s_i$, in $f(x_1, \ldots, x_g)$. The coefficients of g_i comprise the secret information which is given to user i. The key associated with the g-subset $G = \{i_1, \ldots, i_g\}$ is

$$K_G=f(s_{i_1},\ldots,s_{i_g}) \mod p$$

Each user $i_j \in G$ can compute

$$k_G = g_{i_j}(s_{i_1},...,s_{i_{j-1}},s_{i_{j+1}},...,s_{i_g}) \bmod p.$$

It can be shown that no subset of b users disjoint from G can compute any information about k_G (see [5]).

3. The proposed Model

The follwoing model is same as in [4]. It consists of a trusted authority (TA) and a set of users U={1, 2, . . ., n}, with the network is a *broadcast channel*, i.e., any information transmitted by the TA (or by a user in the network) will be received by every user. It is assumed to be insecure against passive attacks, i.e., the information that is broadcast can be observed by anyone. However, that the network is secure against active attacks. (In practice, we could obtain protection against active attacks by using an unconditionally secure authentication code to authenticate all information that is broadcasted.).

4. One or τ-Restricted key agreement scheme.

In this section present two protocols one and τ-restricted key agreement scheme that can be used by one or τ distinct conferences to set up a common key. For certain values of the parameters, the scheme proposed distributing less information than the trivial scheme obtained by considering τ independent copies of a one-restricted scheme or one copy. A design is a pair

(V, $\mathcal{B}$), where V is a set of n elements (called points) and $\mathcal{B}$ is a set of subsets of V of fixed size k, where $k \geq 2$ (called blocks). A parallel class of (V, $\mathcal{B}$) consists of n / k blocks from $\mathcal{B}$ which partition the set V. The design (V, $\mathcal{B}$) is said to be resolvable if the set of blocks, $\mathcal{B}$, can be partitioned into parallel classes. If $\mathcal{B}$ consists of all k-subsets of V, then (V, $\mathcal{B}$) is called the complete k-uniform hypergraph on V. By famous theorem of Baranyai, a proof of which can be found in [20, Theorem 36.1], by The complete k-uniform hypergraph on n points is resolvable if $n \equiv 0 \mod k$.

The resolutions of the designs in Baranyai theorem can be found efficiently.

In the scheme there is no effective interaction among the users. Every member i of a conference G independently chooses a random value $m^{(i)}$ and uses its secret information to compute an encrypted version of $m^{(i)}$ which is broadcast. Then, the key of $G=\{i_1, i_2, \ldots, i_g\}$ with with $i_1<\ldots<i_g$, will be $k_G = \left(m^{(i_1)},\ldots,m^{(i_g)}\right)$. Notice that in the following the sets elements are listed sequentially in increasing order. The protocol provided in [9], which is a one-time key agreement scheme, is a building block of this scheme.

5. A protocol for the one or τ-restricted key agreement scheme

Since U be a set of n users and $G_1, \ldots, G_\tau \subseteq U$ be τ distinct conferences where $|G_i| = g$, and $\ell \geq 1$ is an integer such that $g \equiv 1 \bmod (\ell - 1)$ and that $k \geq 1$ is integer.

5.1 One restricted key agreement scheme.

The set-up phase consists of the TA distributing secret information corresponding to an $(\ell, b+g-\ell)$-KPS, implemented over $(Z_{p^k})^\ell$, with *p* prime. For an ℓ-subset of users *A,* we denote the key associated with *A* by k_A . We think of k_A as being made up of ℓ independent keys over Z_{pk}, which we denote by $k_{A,1},\ldots, k_{A,\ell}$. Each user h of a conference G performs steps in [9].

5.2A τ-restricted key agreement scheme.

Distribution phase

- The TA distributes secret information corresponding to the KPS described in section 2 [3]. More precisely, the TA uses ℓ-1 copies of an $(\ell, b+g-\ell-1)$-KPS, say $\Delta_1,\ldots, \Delta_{\tau-1}$, implemented over $(Z_{p^{k_1}})^\ell,\ldots,(Z_{p^{k_{\tau-1}}})^\ell$, respectively and an $(\ell, b+g-\ell)$-KPS, say Δ_τ, implemented over $(Z_{p^{k_\tau}})^\ell$, with p prime and $k_i \leq k_1$, for $2 \leq i \leq \tau$.

Key computation phase

- When users in a conference G_1 want to compute a common key, they perform the steps from 1 to 5 of the protocol for the one-restricted key agreement scheme

  $\Delta 1$.. For $G_1 =\{i_1,i_2,\ldots,i_g\}$, $i_1<\ldots<i_g$, the final key k_{G_1}, will be $\left(m^{(i_1)},...,m^{(i_g)}\right)$.

- When users in a conference G_t, with $2 \le t \le \tau$ want to compute a common key they perform the steps from 1 to 5 of the protocol for the one-restricted key agreement scheme Δ_t. Since, for $2 \le t \le \tau$, we have that $G_t \backslash G_{t-1} \neq \varphi$, then let $h_1 \in G_t \backslash G_{t-1}$ be the user with 'minimum' identity. Using the scheme Δ_{t-1} implemented over $(Z_{p^{k_{t-1}}})^{\ell}$, user h_t performs steps in [3]:

broadcast.)

6.Weakness of partition in key computation phase of Blundo.

The protocol of one or τ-restricted key agreement scheme of Blundo for key computation phase is true only if g-1 is not prime number, but if we suppose that g=p+1, where p is prime number, and such that for any selected integer number $\ell \ge 2$, we can not find partition to the number g-1 into $\chi=(g-1)/(\ell-1)$ blocks. We suggest to solve the above problem by partition the prime number p into distinct size blocks greater than or equal to two users. The number of blocks is $\chi=\lfloor (g-1) / (\ell-1) \rfloor$ blocks and we have for any parallel class have χ-1 blocks of size ℓ-1 and one

block has size $(\ell-1)+rd$, this block called remainder block where

$$rd \equiv g-1 \bmod(\ell-1)$$

if $rd \equiv 0$, then we have to use the partition of Blundo.In the scheme, we propose there is no effective interaction among the users. Every member i of a conference G, independently chooses a random value $m^{(i)}$ and uses its secrete information to compute an encrypted version of $m^{(i)}$ which is broadcast. Then, the key of $G=\{i_1,i_2,\ldots,i_g\}$ with $i_1<\ldots<i_g$, will be $k_G = \left(m^{(i_1)},\ldots,m^{(i_g)}\right)$.

Suppose $G/\{h\} = \{u_1^h,\ldots,u_{g-1}^h\}$, where h is any user belong to G and partition the complete $(\ell-1)$ of $G/\{h\}$ into classes $C_1,C_2,\ldots,C_R$, where

$$R=r+\lfloor r/(\chi-rd-1)\rfloor$$

and

$$r = \begin{pmatrix} g-2-rd \\ \ell-2 \end{pmatrix}$$

The partition of the (g-1) users in G divided into two steps

- Partition the users $1,2,\ldots,g-rd-1$ into r parallel classes by using Baranyai's theorem with the remained users in last block of each class.
- Changing the remained users from last block for each of the above parallel classes into block one, two, . . , and so

on, respectively of blocks, the number of block enveloped with distinct blocks in class for each ℓ and g is $\lfloor r/(\chi\text{-}rd\text{-}1)\rfloor$.

From above two steps we can partition g-1 users into R classes, the TA can broadcast the message to the users.

The TA distributes secrete information corresponding to the KPS as described in section 2. More precisely the AT uses $(\ell,b+g-\ell)$-KPS for the blocks of size ℓ implementation over $(Z_{p^k})^{\ell}$ and $(\ell+rd,b+g-\ell-rd)$-KPS for the blocks of size $(\ell+rd)$ and over $(Z_{p^k})^{\ell+rd}$ with p prime number. When the users in a conference G want to compute common key, they perform the steps from 1 to 5 of the protocol for the one restricted key agreement scheme.The security of scheme is discussion in ref. [9].

7. Implementation

Suppose that g=8 and ℓ=3. Note that ,8≠1 mod 2 by using Blundo, since g-1=7 prime number, then $\chi=\lfloor 7/2\rfloor$ =3 blocks , rd=1. Suppose that privileged set or the set of users G={1,2,3,4,5,6,7,8}. The AT distributing secrete information corresponding to an (3,b+5)-KPA implement over $(Z_{p^k})^3$ and an (4,b+4)-KPA implement over $(Z_{p^k})^4$ For each user $i \in G$, we partition the 2-subset of G\{ i }with one set of size 3 into R=10

disjoint parallel classes. Below, we describe what is related to user i=5only.

$$C_1^5 = \{\{1,2\}\{3,4\}\{6,7,8\}\}, C_2^5 = \{\{1,3\}\{2,6\}\{4,7,8\}\}$$
$$C_3^5 = \{\{1,4\}\{2,7\}\{3,6,8\}\}, C_4^5 = \{\{1,6\}\{2,4\}\{3,7,8\}\}$$
$$C_5^5 = \{\{1,7\}\{2,3\}\{4,6,8\}\}, C_6^5 = \{\{2,8\}\{6,7\}\{1,3,4\}\}$$
$$C_7^5 = \{\{3,8\}\{4,7\}\{1,2,6\}\}, C_8^5 = \{\{4,8\}\{3,6\}\{1,2,7\}\}$$
$$C_9^5 = \{\{6,8\}\{3,7\}\{1,2,4\}\}, C_{10}^5 = \{\{7,8\}\{4,6\}\{1,2,3\}\}$$

Suppose the TA wants to broadcast the message

$$m^{(5)} = \{m_1^5, m_2^5, ..., m_{10}^5\} \in (Z_{P^k})^{10}$$

to the user in G\ { 5}. Next the user 5 computes the relevant α values . These are as follows:

$$\alpha_{1,1}^5 = 3,\ \alpha_{1,2}^5 = 3,\ \alpha_{1,3}^5 = 1,\ \alpha_{2,1}^5 = 3,\ \alpha_{2,2}^5 = 2$$
$$\alpha_{2,3}^5 = 2,\ \alpha_{3,1}^5 = 3,\ \alpha_{3,2}^5 = 2,\ \alpha_{3,3}^5 = 2,\ \alpha_{4,1}^5 = 2$$
$$\alpha_{4,2}^5 = 3,\ \alpha_{4,3}^5 = 2,\ \alpha_{5,1}^5 = 2,\ \alpha_{5,2}^5 = 3,\ \alpha_{5,3}^5 = 2$$
$$\alpha_{6,1}^5 = 2,\ \alpha_{6,2}^5 = 1,\ \alpha_{6,3}^5 = 4,\ \alpha_{7,1}^5 = 2,\ \alpha_{7,2}^5 = 2$$
$$\alpha_{7,3}^5 = 3,\ \alpha_{8,1}^5 = 2,\ \alpha_{8,2}^5 = 2,\ \alpha_{8,3}^5 = 3,\ \alpha_{9,1}^5 = 1$$
$$\alpha_{9,2}^5 = 2,\ \alpha_{9,3}^5 = 4,\ \alpha_{10,1}^5 = 1,\ \alpha_{10,2}^5 = 2,\ \alpha_{10,3}^5 = 4$$

The broadcast values is the concatenation of the following 30 values:

$$
\begin{aligned}
b^{(5)} = (&m_1^5 + k_{\{1,2,5\},3}, m_1^5 + k_{\{3,4,5\},3}, m_1^5 + k_{\{5,6,7,8\},1},\\
&m_2^5 + k_{\{1,3,5\},3}, m_2^5 + k_{\{2,5,6\},2}, m_2^5 + k_{\{4,5,7,8\},2},\\
&m_3^5 + k_{\{1,4,5\},3}, m_3^5 + k_{\{2,5,7\},2}, m_3^5 + k_{\{3,5,6,8\},2},\\
&m_4^5 + k_{\{1,5,6\},2}, m_4^5 + k_{\{2,4,5\},3}, m_4^5 + k_{\{3,5,7,8\}2,},\\
&m_5^5 + k_{\{1,5,7\},2}, m_5^5 + k_{\{2,3,5\},3}, m_5^5 + k_{\{4,5,6,8\},2},\\
&m_6^5 + k_{\{2,5,8\},2}, m_6^5 + k_{\{5,6,7\},1}, m_6^5 + k_{\{1,3,4,5\},4},\\
&m_7^5 + k_{\{3,5,8\},2}, m_7^5 + k_{\{4,5,7\},2}, m_7^5 + k_{\{1,2,5,6\},3},\\
&m_8^5 + k_{\{4,5,8\},2}, m_8^5 + k_{\{3,5,6\},2}, m_8^5 + k_{\{1,2,5,7\},3},\\
&m_9^5 + k_{\{5,6,8\},1}, m_9^5 + k_{\{3,5,7\},2}, m_9^5 + k_{\{1,2,4,5\},4},\\
&m_{10}^5 + k_{\{5,7,8\},1}, m_{10}^5 + k_{\{4,5,6\},2}, m_{10}^5 + k_{\{1,2,3,5\},4})
\end{aligned}
$$

we can calculate the $k_{B(i,j,h_t),\alpha_{i,j}^{h_t}}$ from KPS of size 3 and 4.

8. Conclusion

In this paper we have analyzed schemes that allow computation of one or τ common keys for one or τ distinct conferences for any integer number $\ell \geq 2$ as building blocks to realize a one or τ-restricted key agreement scheme. The analysis includes many facilities about creating random conference G in a set of users U, such that the users of G can establish the common key without any constraint about the number of conference define beforehand.

We used a mathematical approach to design R families called classes, each is partitioned of p elements where p is a prime number. The elements of class are called block, there are χ-1 blocks of size ℓ-1 and one block of size ℓ+rd-1, where χ is the

number of blocks for any class, i.e This partition of users in conference is mixed size of blocks. This approach can be used for one or τ-constricted key agreement scheme.

References :

[1] Blundo, C., De Santis A., and Herzberg A.,(1995) " Perfectly secure key distribution for dynamic conference", *Lecture Notes in Computer Science*, 740, 471-486.

[2] Nikov, V., Nikova S., Preneel B., and Vandewalle J., (2002) " On distributed key distribution centers and unconditionally secure proactive verifiable secrete sharing schemes based on general access structure", *NATO research action GOA_MEFISTO.*

[3] Blundo, C., D'Arco p., and Gaggia A., (1999) " A τ-restricted key agreement scheme".*The computer Jo*urnal, Vol. 42, No.1, 51-61.

[4] Blom, R.(1984)"An optimal class of symmetric key generation system.". *Lecture Notes in Computer Sc*ience, 209,335-338.

[5] Gong, L., and Wheeler, D.J., (1990)"A matrix key distribution scheme.". *J. Cryptology*, 2, 51-59.

[6] Matsumoto, T., and Imai, H.,(1987) " On the key predistribution system: a practical solution problem". *Lecture Notes in Computer Scien*ce, 239, 185-193.

[8] Beimel, A., and Chor, B.,(1994) " Interaction in key distribution schemes". *Lecture Notes in Computer Science*, 773,444-455.

[9] Beimel, A., and Chor, B.,(1994) "Communication in key distribution schemes". *IEEE Trans. Inform. Theory*, 42, 19-28.

[10] Blundo, C., Frota Mattos, L. A. and Stinson, D. R. (1998) "Generalized Beimel-Chor schemes for broadcast encryption and interactive key distribution". *Theor. Comput. Sci.*, 200, 313-334.

[11] Fait, A., and Naor, M.(1994) "Broadcast encryption". *Lecture Notes in Computer Science,*773,480-491.

[12] Berkovits, S.,(1992) "How to broadcast a secret". *Lecture Notes in Computer Science,* 547,536-541.

[13] Blundo, C., and Cresti, A., (1995) " Space requirement for broadcast encryption". *Lecture Notes in Computer Science*, 950,287-298.

[14] Blundo, C., and Cresti, A., (1996) "Broadcast encryption schemes with disenrollment cabability." *5th Italian Conf. Theoretical Computer Science*, PP.176-191. Word Scientific

[15] Blundo, C., Frota Mattos, L. A., and Stinson, D. R., (1996) " Multiple key distribution maintaining user anonymity via broadcast channels". *J.Comput. Security*, 3, 309-323.

[16] Blundo, C., Frota Mattos, L. A., and Stinson, D. R., (1996) "Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution". *Lecture Notes in Computer Science,* 1109, 387-400

[17] Chor, B., Fiat, A., and Naor, M., (1994) "Tracing traitors". *Lecture Notes in Computer Science,* 839, 257-270.

Just, M., Kranakis, E., Krizanc, D., and van Oorschot, P., (1994) "Key distribution via true broadcasting ". In Proc. 2nd ACM *Conf. on Computer and Communications Security,* PP. 81-88.

[18] Stinson, D. R. (1997) "On some methods for unconditionally secure key distribution and broadcast encryption". Designs, *Codes and Cryptography*, 12, 215-243.

[19] Blundo, C., and Cresti, A., (1998) "Lower bounds for unconditional secure key distribution scheme". Submitted for publication

[20] J. H. van Lint and R. M. Wilson,(1992) " A course in Combinatorics". Cambridge University Press.