文章编号:1001 - 9081(2007)10 - 2450 - 03

有门限可认证的多重秘密密钥协商方案

张艳硕[1,2],刘卓军[2]
(1. 北京电子科技学院 基础部,北京 100070;
2. 中国科学院 数学机械化重点实验室,北京 100080)
(zhangyanshuo@amss.ac.cn)

摘 要:密钥管理是信息安全中的一个重要领域,密钥协商是密钥管理中的一个重要方面。基于线性码理论给出了一个计算安全的有门限可认证的多重秘密密钥协商方案。该方案使得参与者可以协商秘密密钥,而不用基于离散对数假设。参与秘密密钥协商的参与者组成的集合必须满足门限要求才能进行秘密密钥协商;同时协商的秘密密钥具有多重性,即进行一次秘密协商,可产生出多个秘密密钥。该方案基于线性码理论,可以进行验证,具有认证功能,能够防止第三方攻击。

关键词:线性码;第三方攻击;密钥协商;门限;多重秘密;认证
中图分类号: TP309 **文献标志码**:A

Multi-secret key agreement scheme with threshold and authority

ZHANG Yan-shuo[1,2], LIU Zhuo-jun[2]
(1. *Department of Basic Sciences, Beijing Electronic Science and Technology Institute, Beijing* 100070, *China*;
2. *Key Laboratory of Mathematics Mechanization, Chinese Academy of Sciences, Beijing* 100080, *China*)

Abstract: Key management is an important field in information security. Key agreement is one of the core problems in the key management. A new computationally secure threshold multi-secret key agreement scheme with authority based on the theory of linear codes was introduced. The scheme makes the users share the secret key, and does not need to be based on discrete logarithm. The set of participants to perform key agreement should satisfy threshold. In the scheme, multi - secret key can be initiated in one key agreement session. The scheme based on linear codes has the property of authority by checking the equality to prevent the third party attack.

Key words: linear codes; third party attack; key agreement; threshold; multi-secret; authority

0 引言

在信息安全系统中,密钥是合法访问系统的唯一凭证。密钥一旦丢失或泄漏,安全系统整个将被破坏。因此,可靠的密钥管理方案对通信系统的安全十分重要。

1949 年,Shannon 提出了著名的 Shannon 保密理论[1],指出一次一密的系统的安全性和经常更换密钥的重要性。过去经常更换密钥在实际操作中因为过于繁琐而不可行。

密钥协商方案[2]是一种能够让通信系统中的两个或多个用户在一个公开的、不必保证安全性的信道上通过协商共同建立密钥的通信机制。

Whitfield Diffie 和 Martin Hellman 在 1976 年公布了一种密钥生成算法(协议)。Diffie-Hellman 密钥交换协议是一种交互建立秘密密钥的方法,所产生的秘密密钥可用于加密和进一步的密钥管理。该协议允许两个用户在不必保证安全的媒介上交换信息从而形成秘密密钥,其有效性依赖于计算离散对数的难度,即这样一个事实:虽然计算以一个素数为模的指数相对容易,但计算离散对数却很困难,人们通常自然地接受这样的假设,即对于大的素数,计算出离散对数几乎是不可能的。而 Diffie-Hellman 密钥交换协议的关键之处就是承认了这个假设。

同时,Diffie-Hellman 密钥交换协议容易被第三方攻击。Diffie-Hellman 密钥交换协议之所以有这个弱点,是因为在密钥交换时并不对其用户进行认证。可能的解决办法是使用数字签名进行认证,或使用其他的协议变种。

1992 年文献[3]开发了认证的 Diffie-Hellman 密钥交换协议,或称为 Station-to-Station (STS)协议。其目的在于防止对 Diffie-Hellman 协议的第三方攻击。新协议能有此功效,原因来自两方面,一个是使用数字签名来相互认证,另一个是使用公钥认证。因此,这个增强的协议能够抵挡第三方攻击。

考虑到秘密密钥协商方案的可操作性和实用性,即参与秘密密钥协商的参与者有一定的门限,同时协商的秘密密钥具有多重性,即一次秘密协商,可产生多个秘密密钥。此外,考虑到协商的秘密密钥对于参与者来说可以验证,本文基于线性码理论,给出计算安全的多重秘密密钥协商方案。我们给出的多重秘密密钥协商方案基于线性码的所具有的校验特性,起到认证作用,可以防止第三方攻击。同时,该秘密密钥协商方案具有门限性和秘密密钥的多重性。

1 线性码的相关知识[4-6]

相关运算都在有限域 $GF(q)$ 上的进行,其中 q 为某一素数的幂次。令 $[n,k;q]$ 为 $GF(q)$ 上的一个 k 维线性子空间,该

收稿日期:2007 - 05 - 22;**修回日期**:2007 - 07 - 13。
基金项目:国家 973 计划项目(G2004CB318000);北京电子科技学院信息安全与保密重点实验室基金项目(YZDJ0712)。
作者简介:张艳硕(1979 -),男,陕西宝鸡人,讲师,博士研究生,主要研究方向:密码学、编码学、信息安全; 刘卓军(1958 -),男,山东即墨人,研究员,博士生导师,主要研究方向:密码学、编码学、符号计算。

线性子空间上的每一个向量称为一个码字。一个$[n,k;q]$线性码C的生成矩阵是一个$GF(q)$上的$k\times n$阶矩阵,其中每一行是码C的一个基向量。

如果$\boldsymbol{G}$是线性码C的生成矩阵,那么$C=\{aG/a\in GF(q)^k\}$。如果$\boldsymbol{G}=(I_k,P)$,其中$\boldsymbol{I}_k$是$k\times k$单位矩阵,就称$\boldsymbol{G}$是标准型的。若$\boldsymbol{G}$是标准型的,那么一个码字的前k个符号称为信息符号,可以随意选取,但一经选定,其余$n-k$个符号(称为奇偶校验符号)便随之而确定。

若$\boldsymbol{G}=(I_k,P)$是线性码C的生成矩阵,那么矩阵$\boldsymbol{H}=(-P^T,I_{n-k})$,有$CH^T=0$,这意味着每个码字$aG$与$H$的每行之内积为0。换言之,有$x\in G\Leftrightarrow xH^T=0$,$\boldsymbol{H}$被称为$C$的校验矩阵。

2　基于线性码的一些重要结果

这一节给出有门限可认证的多重秘密密钥协商方案用到的有关线性码的重要结果[7-9]。选择$[n+1,k;q]$线性码C,其生成矩阵为$\boldsymbol{G}$,若假设$s'\in GF(q)$表示秘密,令$g_0=(g_{10},g_{20},\cdots,g_{k0})^T$表示生成矩阵$\boldsymbol{G}$的第一列。选择线性子空间$GF(q)$上向量$\boldsymbol{s}=(s_1,s_2,\cdots,s_k)$为信息向量使得:$s'=sg_0=\sum_{i=1}^{k}s_ig_{i0}$,相应于这一信息向量$\boldsymbol{s}$的码字为:$K=(K_0,K_1,K_2,\cdots,K_n)=\boldsymbol{sG}$。

其中码字K的第一个分量K_0就是原始秘密$s'=sg_0=k_0$。由于码C是线性码,不难证明在线性码$[n+1,k;q]$中,其生成矩阵$\boldsymbol{G}=(g_0,g_1,\cdots,g_n)$满足$g_0$是其他$n$列中$\{g_1,g_2,\cdots,g_n\}$某些列的线性组合[7,8]。原始秘密$K_0$被子秘密$\{K_{i_1},K_{i_2},\cdots,K_{i_t}\}$所确定当且仅当$g_0$是向量$\{g_{i_1},g_{i_2},\cdots,g_{i_t}\}$的线性组合,且$1\leqslant i_1<i_2<\cdots<i_t\leqslant n$。

如果假设原始秘密k_0就是要协商的秘密,即要计算原始秘密k_0,首先解线性方程组:$g_0=\sum_{j=1}^{t}x_jg_{i_j}$求得$x_j;j=1,2,\cdots,t$,然后通过计算获得经过协商的秘密密钥:

$$k_0=sg_0=s\sum_{j=1}^{t}x_jg_{i_j}=\sum_{j=1}^{t}x_jsg_{i_j}=\sum_{j=1}^{t}x_jK_{i_j};\ t\text{为门限值}$$

下面介绍有门限可认证的多重秘密密钥协商方案。

3　有门限可认证的多重秘密密钥协商方案

整个方案在n个参与者$P_i;i=1,2,\cdots,n$之间进行,其中t个或t个以上参与者可以进行秘密密钥协商,每个参与者P_i已知同一个$[n+1,k;q]$线性码C,$\boldsymbol{G}$为该线性码的生成矩阵,g_0为$\boldsymbol{G}$的第一列,记$g_0=(g_{10},g_{20},\cdots,g_{k0})^T$。线性码$C$对应生成矩阵$\boldsymbol{G}$的校验矩阵记为$\boldsymbol{H}$,即有等式$\boldsymbol{GH}^T=0$成立。这里假设有且仅有$t$个参与者进行秘密密钥协商。

1)协商步骤如下:

每个参与秘密密钥协商的参与者$P_{i_j};j=1,2,\cdots,t$随机选择一个$d^{ij}\in GF(q)$,同时选择信息向量$\boldsymbol{s}^{ij}=(s_1^{ij},s_2^{ij},\cdots,s_k^{ij})$为信息向量使得:$d^{ij}=s^{ij}g_0=\sum_{i=1}^{k}s_i^{ij}g_{i0}=K_0^{ij}$,相应于这一信息向量$\boldsymbol{s}^{ij}$的码字为:$K^{ij}=(K_0^{ij},K_1^{ij},K_2^{ij},\cdots,K_n^{ij})=s^{ij}\boldsymbol{G}$。

参与者进行一次协商就可以产生r个秘密,所有参与者共同拥有一个多项式$a_1x+a_2x^2+a_3x^3+\cdots+a_{r-1}x^{r-1}$(如果共享的$r$个秘密分别为$k_1,k_2,\cdots,k_r$,那么对$r$个点对$(i,k_i)$进行拉格朗日插值,就可得到一个唯一的次数小于$r$的多项式$f(x)$,定义$f(x)$为$f(x)=a_0+a_1x+a_2x^2+a_3x^3+\cdots+a_{r-1}x^{r-1}$,$a_0$是由参与者协商所得)。

每个参与秘密密钥协商的参与者$P_{i_j};j=1,2,\cdots,t$将$(K_1^{ij},K_2^{ij},\cdots,K_n^{ij})$秘密地分发给其他$t-1$个参与者。于是每个参与者$P_{i_j};j=1,2,\cdots,t$获得的数据:$(K_1^{ij},K_2^{ij},\cdots,K_n^{ij});j=1,2,\cdots,t$。每个参与者$P_{i_j}$分别计算$T_i:T_k=\sum_{j=1}^{t}K_k^{ij};k=1,2,\cdots,n$。

参与者协商的秘密密钥即是:$D=\sum_{j=1}^{t}d^{ij}=\sum_{j=1}^{t}K_0^{ij}$。为计算$D$,首先解线性方程组:$g_0=\sum_{j=1}^{t}x_jg_{i_j}$求得$x_j;j=1,2,\cdots,t$,然后通过计算获得:

$$D=\sum_{i=1}^{t}d^{ij}=\sum_{i=1}^{t}s^{ij}g_0=\sum_{i=1}^{t}s^{ij}\sum_{j=1}^{t}x_jg_{i_j}=\sum_{j=1}^{t}x_j\sum_{i=1}^{t}s^{ij}g_{i_j}=\sum_{j=1}^{t}x_j\sum_{i=1}^{t}K_{i_j}^{ij}=\sum_{j=1}^{t}x_jT_{i_j}$$

显然参与者通过协商可以得到共享的r个秘密密钥,秘密密钥分别为$k_1,k_2,\cdots,k_r$。以知所有参与者共同拥有多项式$a_1x+a_2x^2+a_3x^3+\cdots+a_{r-1}x^{r-1}$,以及协商获得的秘密密钥$a_0=D=\sum_{j=1}^{t}d^{ij}=\sum_{j=1}^{t}K_0^{ij}$,即可以得到多项式$a_0+a_1x+a_2x^2+a_3x^3+\cdots+a_{r-1}x^{r-1}$,于是有多项式$f(x)=a_0+a_1x+a_2x^2+a_3x^3+\cdots+a_{r-1}x^{r-1}$。即有$k_i=f(i);i=1,2,\cdots,r$,即得到协商的$r$个秘密密钥分别为$k_1,k_2,\cdots,k_r$。

2)密钥验证过程如下:

由上可以得到$T_0=\sum_{j=1}^{t}K_0^{ij}=D$,即得$(T_0 \bmod q,T_1 \bmod q,T_2 \bmod q,\cdots,T_n \bmod q)$。显然由线性码的定义,$(T_0 \bmod q,T_1 \bmod q,T_2 \bmod q,\cdots,T_n \bmod q)$应该是一个码字。每个参与秘密密钥协商的参与者验证以下等式是否成立:

$$(T_0 \bmod q,T_1 \bmod q,T_2 \bmod q,\cdots,T_n \bmod q)H^T=0$$

如果成立,则认为r个秘密$k_1,k_2,\cdots,k_r$就是协商的秘密密钥,如果等式不成立,不考虑参与者的计算错误和信道噪声情况下,即认为有第三方攻击,那么参与协商的参与者按照上述多重秘密密钥协商方案的步骤重新进行秘密密钥协商。这一步骤就是该秘密密钥协商方案的认证功能所在,通过上述验证,完成对秘密密钥的认证。

3)方案特性如下:

a)整个方案基于线性码的特性,即对于线性码$[n+1,k;q]$来说,其生成矩阵$\boldsymbol{G}=(g_0,g_1,\cdots,g_n)$满足$g_0$是其他$n$列中$\{g_1,g_2,\cdots,g_n\}$某些列的线性组合。原始秘密$k_0$被子秘密$\{k_{i_1},k_{i_2},\cdots,k_{i_t}\}$所确定当且仅当$g_0$是向量$\{g_{i_1},g_{i_2},\cdots,g_{i_t}\}$的线性组合且$1\leqslant i_1<i_2<\cdots<i_t\leqslant$。这保证了上述方案的门限性。

b)本方案将基于线性码的特性实施的,即任何少于门限个数要求的参与者集合不能获得任何有关协商的秘密密钥的任何信息,而任何不少于门限要求的参与者的集合都能进行秘密密钥协商,这是本方案的门限性所在。

c)该方案通过一次秘密密钥协商就可以产生多个秘密密钥。这是该秘密密钥协商方案秘密密钥多重性的体现。秘密密钥更新时,无需更新参与者的子秘密,参与者重新选取自己的参数$d^{ij}\in GF(q)$即可。如果增加或删除某个参与者,相应的参数重新选取即可。该方案容易实现,且具有实际意义。

d) 该方案中,秘密密钥是经过满足门限的参与者集合经过协商产生,不只依赖于其中一个人,和整个参与者集合的每一个人都有关,即我们给出的是秘密密钥协商方案。

4 多重秘密密钥协商方案安全性分析

上述基于线性码理论构造的秘密密钥协商方案,要求协商各方拥有不对外公开的线性码和一个多项式。该方案简单易行,容易操作和实现。对于安全性讨论如下:

1) 方案能够防止第三方攻击。如果有一个第三方截获了参与者 P_{i_j} 发送给其他参与者的子秘密($K_1^{i_j},K_2^{i_j},\cdots,K_n^{i_j}$),他需要向其他参与者发送一个自己的子秘密,该子秘密和其他子秘密模加后应是一个码字,相当于攻击者要在线性空间 $GF(q)^n$ 中找到一个码字。由于攻击者不知道线性码的生成矩阵,那么其成功的概率是 $\frac{q^k}{q^{n+1}}=\frac{1}{q^{n+1-k}}$。显然攻击者成功的可能性非常小。

2) 通过线性码校验矩阵的计算实现了多个参与者之间的相互认证。经过成功认证,满足门限个数的参与者集合就有了协商的秘密密钥。

3) 上述方案中,满足门限个数的参与者协商的秘密密钥是通过求解线性方程组:$g_0=\sum_{j=1}^{t}x_jg_{i_j}$ 求得 $x_j;j=1,2,\cdots,t$,然后通过计算 $D=\sum_{i=1}^{t}d^{i_j}=\sum_{i=1}^{t}s^{i_j}g_0=\sum_{j=1}^{t}x_jT_{i_j}$ 获得的。生成矩阵是参与者私有的,攻击者也不知晓。攻击者对求解线性方程组:$g_0=\sum_{j=1}^{t}x_jg_{i_j}$ 一无所知,所以攻击者就是知道 $T_k=\sum_{j=1}^{t}K_k^{i_j};k=1,2,\cdots,n$ 也不能计算出 $D=\sum_{i=1}^{t}d^{i_j}=\sum_{j=1}^{t}x_jT_{i_j}$。故想获得真正的秘密密钥 $k_1,k_2,\cdots,k_r$ 的概率是非常低的。

4) 线性码 C 的生成矩阵若以 $\boldsymbol{G}=(I_k,P),H=(-P^T,I_{n-k})$ 为例。容易看出,整个线性空间 $GF(q)^n$ 中有 $q^{k(n+1-k)}$ 个相互不等价的标准型生成矩阵,即有 $q^{k(n+1-k)}$ 个相互不等价的线性码$[n+1,k;q]$。所以攻击者找到正确的生成矩阵 $\boldsymbol{G}$ 的概率是 $\frac{1}{q^{(n+1-k)}}$,当然,攻击者找到正确的校验矩阵 $\boldsymbol{H}$ 的概率也是 $\frac{1}{q^{(n+1-k)}}$。

5 方案的优点

上述方案同其他类似方案比较具有如下优势:

1)不论是 Diffie-Hellman 密钥交换协议还是后来的 STS 协议都要基于离散对数假设,而这样的假设至少到目前为止是没有理论保证的。本文方案不需要这样的假设,只是基于线性码理论的特性而需要协商各方能够共同选取一个线性码。这样做带来的好处是秘密密钥协商各方如果认为有必要就可以经常更换协商的秘密密钥,而且可以防止第三方攻击。

2)方案中用到的就是矩阵的相乘和加减运算,这些计算的计算量很小,且计算方便,容易操作。在计算复杂性上明显优于其他方案。

3)方案有认证功能。每个参与者可以通过方案中的验证步骤对协商的秘密密钥的正确性作出判断。如果验证步骤中等式不成立,则说明有第三方攻击。

4)上述方案具有门限性,即大于等于门限个数的参与者组成的集合才可以进行秘密密钥协商,这使得秘密密钥协商更具可操作性和广泛性。同时,该秘密密钥协商过程中,一次秘密密钥协商,可以产生多个秘密密钥。

6 结语

本文给出了一个有门限可认证的多重秘密密钥协商方案,该方案可以防止第三方攻击,也是计算安全的。该方案只有参与者集合满足门限的情况下可以进行秘密密钥协商,方案本身基于线性码理论,具有认证功能;同时,运用该方案,满足门限的参与者集合一次协商,可以产生多个通过协商的秘密密钥。

参考文献:

[1] SHANNON C E. A mathematical theory of communication[J]. Bell System Technical Journal, 1948,27:379-423;623-656.

[2] DIFFIE-HELLMAN R. RFC2631, Key Agreement Method[S]. 1999.

[3] DIFFIE W, VAN OORSCHOT P C, WIENER M J. Authentication and authenticated key exchanges[J]. Designs, Codes and Cryptography, Kluwer Academic Publishers, 1992,(2):107-125.

[4] 冯登国,裴定一. 密码学导引[M]. 北京:科学出版社,1999:223-244.

[5] VAN LINT J H. 编码理论导引[M]. 余敏安,陈冬生,译. 北京:科学出版社,1988:37-40.

[6] 王新梅,马文平,武传坤. 纠错密码理论[M]. 北京:人民邮电出版社,2001:48-52.

[7] MASSEY J L. Minimal codewords and secret sharing[C]// Proceedings of the 6th Joint Swedish-Russian Workshop on Information Theory. Sweden: Molle, 1993:22-27.

[8] MASSEY J L. Some applications of coding theory in cryptography[C]// Codes and Ciphers: Cryptography and Coding IV(ED. PG Farrel1). England: IMA, 1995:33-47.

[9] 谭晓青. 无信任分配中心的动态秘密分享方案[J]. 湘潭大学自然科学学报,2005,27(4):42-45.

(上接第 2442 页)

参考文献:

[1] FORREST S, PERRELASON A S. Self-nonself Discrimination in a Computer[C]// Proceedings of the 1994 IEEE Synposium on Research in Security and Privacy. California: IEEE Computer Society, 1997:202-212.

[2] GHOSH A K, MICHAEL C, SCHATZ M. A Real-Time Intrusion Detection System Based on Learning Program Behavior[C]// Recent Advances in Intrusion Detection (RAID). Toulouse: Spinger-Verlag, 2000:120-132.

[3] LEE W, STOLFO S J, MOK K W. A Data Mining Framework for Building Intrusion Detection Models[C]// Proceedings of the 1999 IEEE Symposium on Security and Privacy. Oakland: IEEE Press, 1999:120-132.

[4] VAPNIK V N. The Nature of Statistical Learning Theory[M]. New York: Spring-Verlag, 1995.

[5] 饶鲜,董春曦,杨绍全. 基于支持向量机的入侵检测系统[J]. 软件学报,2003,14(4): 798-803.

[6] Lincoln Labs. KDD-cup data set[DB/OL]. [2004-12-02]. http://kdd.ics.uci.edu/databases/kddcup99.html.