基于向量空间接入结构的分布式密钥生成

张福泰
(南京师范大学数学与计算机科学学院,江苏南京 210097)

摘 要: 密钥生成是密码系统的一个重要组成部分,其安全性对整个密码系统的安全性起着至关重要的作用. 在群体保密通信、电子商务和面向群体的密码学中,往往需要采用分布式的密钥生成方式. 本文对基于向量空间接入结构的分布式密钥生成进行了研究. 以向量空间接入结构上信息论安全的一个可验证秘密分享方案为基础,提出了适应于这类接入结构的一个安全高效的分布式密钥生成协议. 该协议比常见的基于门限接入结构的分布式密钥生成协议具有更广泛的适用性.

关键词: 密钥生成; 分布式密钥生成; 群体密码学; 可验证秘密分享; 向量空间接入结构
中图分类号: TN918.4 **文献标识码**: A **文章编号**: 0372-2112 (2005) 05-0816-04

Distributed Key Generation Based on Vector Space Access Structures

ZHANG Fu-tai
(School of Mathematics, Nanjing Normal University, Nanjing, Jiangsu 210097, China)

Abstract: Key generation plays an important role in a cryptosystem. Its security is significant for the security of the whole cryptosystem. In situations such as group oriented cryptography, group secret communication and electronic commerce, distributed key generation are needed. The problem of distributed key generation based on vector space access structures is studied. On the foundation of an information theoretic secure verifiable secret sharing scheme over vector space access structures, a secure and efficient distributed key generation protocol over this kind of access structures is presented. Compared to the existing distributed key generation protocols based on threshold access structures, the new protocol has a wider range of applications.

Key words: key generation; distributed key generation; group oriented cryptography; verifiable secret sharing; vector space access structure

1 引言

密钥生成是密码系统的一个重要组成部分,其安全性对整个密码系统的安全性起着至关重要的作用. 分布式的密钥生成[1,2] (Distributed Key Generation) 简称 DKG,主要用于面向群体的密码系统[3~6]及分布式密码计算,它在信息与网络安全的多个方面发挥着极其重要的作用. DKG 协议允许多个参与者共同合作以生成一个密码系统的公钥和私钥,使得公钥以公开形式输出,而私钥被参与者按照某一秘密分享方案所分享. 这一被分享的私钥以后可以用于面向群体的密码系统,如群体签名或群体解密等.

Pedersen[1]于 1991 年提出了第一个 DKG 协议. Gennaro 等人在文献[2]中指出了 Pedersen 的 DKG 协议所存在的安全缺陷,并提出了一个新的可证明安全的分布式密钥生成协议. 与 Pedersen 的 DKG 协议相比,不仅提高了安全性,而且保持了原协议的高效性. DKG 协议都是以可验证秘密分享[7~9]为基础的. 在基于离散对数的分布式密钥生成协议中,运用最多的是计算安全的 Feldman 可验证秘密分享 (VSS) 协议[7] (Feldman-VSS 协议) 和信息论安全的 Pedersen 可验证秘密分享协议 (Pedersen-VSS 协议).

目前已有的 DKG 协议,主要都是基于门限接入结构的,其中运用的都是门限 VSS 方案. 对基于一般接入结构的,即使用非门限 VSS 方案的分布式密钥生成的研究在文献中却不多见. 类似于秘密分享,基于门限接入结构的分布式密钥生成仅是分布式密钥生成的一种特殊情况,它需要所有参与者都具有完全同等的地位、权利、安全性和可靠性的假设来支持. 但在实际中往往由于各参与者所处的地位以及所拥有的权利等的差异,他们的安全性、可靠性以及在协议中所起的作用并不是完全对等的,因而对基于一般接入结构的密钥生成协议的研究具有重要的理论和现实意义. 在非门限接入结构中,向量空间接入结构占有重要的地位,它不仅有好的代数结构,而且包含了所有的门限接入结构,同时,其上的秘密分享方案还具

收稿日期:2003-09-05;修回日期:2005-02-20
基金项目:江苏省高校自然科学研究计划重点项目(No. 03KJA520066);计算机网络与信息安全教育部重点实验室(西安电子科技大学)开放课题;国家"211"工程重点学科建设项目

有类似于门限秘密分享方案的简捷、高效等特点.因此,如何把向量空间接入结构的特点应用到分布式的密钥生成中,以扩大分布式密钥生成的适用范围,是值得研究的.本文将对这一问题进行探讨.我们将以向量空间接入结构上的一个信息论安全的广义 VSS 方案为基础,设计出一个安全实用的基于向量空间接入结构[9,10]的分布式密钥生成协议.

2　向量空间接入结构上的一个信息论安全的广义 VSS 方案

2.1　向量空间接入结构上的秘密分享

设 $H=\{H_1,H_2,\cdots,H_n\}$ 是 n 个分享者的集合,分发者 $D\notin H$, $K=GF(q)$ 是一个有限域, $E=K^t$ 是 K 上的 t 维向量空间. Γ 是 H 上的一个单调接入结构,且 t 不小于所有最小合格子集的最大基数,说 Γ 是一个向量空间接入结构,如果存在一个映射

$$\Psi: H\cup\{D\}\to E$$

使得 H 的一个子集 $A\in\Gamma$ 当且仅当向量 $\Psi(D)$ 可以由 $\{\Psi(P)\mid P\in A\}$ 中的向量线性表示.把接入结构 Γ 中的元素称为 H 的合格(授权)子集,按集合的包含关系而论,把 Γ 中的极小元称为最小合格子集.如果 Γ 是一个向量空间接入结构,那么我们可以构造 Γ 上的一个使得秘密空间和每一个份额空间都为 K 的理想的秘密分享方案,具体的构造方法如下[9,10]:

份额的分配算法:首先 D 向全体参与者公布映射 Ψ 及接入结构 Γ.对要分享的秘密 $s\in K$, D 随机地选取 E 中的一个向量 v,使得 $\mathrm{v}\cdot\Psi(\mathrm{D})=\sum_{j=1}^{t}v_ja_j=s$,其中 $\mathrm{v}=(v_1,v_2,\cdots,v_t)$, $\Psi(\mathrm{D})=(a_1,a_2,\cdots,a_t)$.记 $\Psi(\mathrm{H}_j)=(a_{1j},a_{2j},\cdots,a_{tj})$, $j=1,2,\cdots,n$,则 D 发给 H_j 的秘密份额为 $s_j=\mathrm{v}\cdot\Psi(\mathrm{H}_j)$,这里"·"表示向量的数量积(内积).

恢复算法:当 H 的一个合格子集 $A\in\Gamma$ 恢复秘密时, A 中成员先求出 E 中的一个(列)向量 X,使得 $\Psi(\mathrm{A})^T\mathrm{X}=\Psi(\mathrm{D})^T$.然后计算 $s=\mathrm{X}\cdot S_A$,其中 $S_A=\mathrm{v}\Psi(\mathrm{A})^T$ 是 A 中成员持有的份额所构成的向量, $\Psi(\mathrm{A})$ 是由所有的 $\Psi(\mathrm{P})$, $\mathrm{P}\in\mathrm{A}$,为行向量构成的矩阵.

由上述方法构造的向量空间秘密分享方案是完备的,同时也是理想的.向量空间接入结构包含了所有的门限接入结构,因而内容相当丰富. Shamir 门限秘密分享体制和矩阵法门限体制都是向量空间秘密分享体制的特例.

2.2　向量空间接入结构上信息论安全的广义 VSS 方案

系统参数: p, q 是大素数,其中 $q\mid(p-1)$, G_q 是 Z_p^* 的惟一的 q 阶子群. g, h 是 G_q 的生成元,假定在 Z_p^* 中计算以 g, h 为底的离散对数是不可行的,且任何人都不知道离散对数 $\log_g h$.

设 $H=\{H_1,H_2,\cdots,H_n\}$ 是 n 个分享者的集合,分发者 $D\notin H$, $K=GF(q)$, $E=K^{n-1}$ 是 K 上的 $n-1$ 维向量空间. Γ 是 H 上的一个向量空间接入结构,其中至少含有两个不相交的最小合格子集.(这一条件可以保证,不存在 $P\in H$,使得对每一 $A\in\Gamma$,均有 $P\in A$.)

份额的分配算法:与 2.1 节中类似,首先 D 向全体参与者公布映射 Ψ.对要分享的秘密 $s\in K$, D 随机选取 $E=K^{n-1}$ 中的向量 v, β,使得 $\mathrm{v}\cdot\Psi(\mathrm{D})=s$,即 $v_1a_1+v_2a_2+\cdots+v_{n-1}a_{n-1}=s$.记 $r=\beta\cdot\Psi(\mathrm{D})=b_1a_1+b_2a_2+\cdots+b_{n-1}a_{n-1}$,其中 $\mathrm{v}=(v_1,v_2,\cdots,v_{n-1})$, $\beta=(b_1,b_2,\cdots,b_{n-1})$, $\Psi(\mathrm{D})=(a_1,a_2,\cdots,a_{n-1})$.记 $\Psi(\mathrm{H}_j)=(a_{1j},a_{2j},\cdots,a_{n-1,j})$, $j=1,2,\cdots,n$. D 计算并广播对秘密 s 的承诺

$$E_0=E(s,r)=g^sh^r\pmod p$$

及对向量 $\mathrm{v}=(v_1,v_2,\cdots,v_{n-1})$ 的承诺

$$E_j=E(v_j,b_j)=g^{v_j}h^{b_j}\pmod p,\ j=1,2,\cdots,n-1.$$

之后 D 计算给每一成员 H_j 的份额 $s_j=\mathrm{v}\cdot\Psi(\mathrm{H}_j)=\mathrm{v}\Psi(\mathrm{H}_j)^T=v_1a_{1j}+v_2a_{2j}+\cdots+v_{n-1}a_{n-1,j}$, $r_j=\beta\cdot\Psi(\mathrm{H}_j)=\beta\Psi(\mathrm{H}_j)^T=b_1a_{1j}+b_2a_{2j}+\cdots+b_{n-1}a_{n-1,j}$,并把 (s_j,r_j) 秘密地发送给 H_j, $j=1,2,\cdots,n$.

份额的验证算法:为验证自己收到的份额的有效性,每一 H_j 检验以下两个等式是否成立:

$$E_0=\prod_{i=1}^{n-1}E_i^{a_{ij}}\pmod p,\quad E(s_j,r_j)=g^{s_j}h^{r_j}=\prod_{k=1}^{n-1}E_k^{a_{kj}}\pmod p$$

若第一个等式不成立,则说明 D 有欺骗行为,协议终止.在第一个等式成立的情况下,若某一 H_j 检验第二个等式不成立,则 H_j 广播对 D 的一个抱怨,同时也广播 D 发送给自己的份额 (s_j,r_j),并要求 D 广播应发给自己的有效份额.如果 D 受到了某一合格子集的全体成员的抱怨,则协议终止.

恢复算法:在恢复秘密时,合作者可根据验证算法中的第二类等式来检验各成员提交的份额的有效性.在收集到一个合格子集中所有成员的有效份额后,即可按 2.1 节中的恢复算法计算出被分享的秘密.

该方案是文献[8]中的门限可验证秘密分享方案到向量空间接入结构上的推广.

3　基于向量空间接入结构的分布式密钥生成协议

3.1　基于离散对数的公钥系统的密钥的分布式生成及其安全性

设有基于离散对数的一个公钥系统,其参数为 p, q, g,其中 p, q 为大素数, $q\mid p-1$, g 是 Z_p^* 中的一个 q 阶元,在 Z_p^* 中计算以 g 为底的离散对数是不可行的.对这样的密码系统,密钥的分布式生成(DKG)协议是指,由一组参与者 H_1, H_2, $\cdots$, H_n 协作来生成系统的私钥 $x\in Z_q$ 和公钥 $y=g^x\pmod p$,使得 x 被 H_1, H_2, $\cdots$, H_n 按某一接入结构 Γ 所分享,即每一 H_k 都拥有关于 x 的一个秘密份额,而 $y=g^x\pmod p$ 是公共输出.

一个安全的 DKG 协议必须具备以下四条性质[2]:

(C1)如果一个合格子集中的所有成员都是诚实的,则由该合格子集中成员所提供的份额,就可惟一确定私钥 x.

(C2)所有诚实的参与者都得到相同的公钥 $y=g^x\pmod p$,其中 x 是由(C1)所保证的惟一的私钥.

(C3) x 在 Z_q 中是均匀分布的,从而 $y=g^x\pmod p$ 在 Z_p^* 的由 g 所生成的子群中是均匀分布的.

(C4)除了公开信息 $y=g^x\pmod p$ 外,攻击者不能获得私钥 x 的任何信息.

3.2 密钥的生成协议

系统参数与 2.2 节相同. 符号 p, q, g, h, K, E 的含义也与 2.2 节相同,即 p, q 是大素数,其中 $q|(p-1)$, g, h 是 Z_p^* 中的 q 阶元,在 Z_p^* 中计算以 g, h 为底的离散对数是不可行的,且任何人都不知道离散对数 $\log_g h$. $K = Z_q^*$, $E = K^{n-1}$. 参数选取的可行性参见文献[2,8]. 设参与者 $H_1, H_2, \cdots, H_n$ 构成集合 H. 在初始阶段, H 中全体成员以某种方式协商确定 H 上的一个向量空间接入结构 Γ,即确定出映射

$$\Psi: H \cup \{D\} \to E$$

H 的一个子集 $A \in \Gamma$ 当且仅当向量 $\Psi(D)$ 可以由向量组 $\{\Psi(P) | P \in A\}$ 线性表示,且对每一 $P \in H$,存在 $B \in \Gamma$ 使得 $P \notin B$,每一合格子集至少有两个成员. 记 $\Psi(D) = \alpha = (a_1, a_2, \cdots, a_{n-1})$, $\Psi(H_j) = (a_{1j}, a_{2j}, \cdots, a_{n-1,j})$, $j = 1, 2, \cdots, n$.

对于攻击者模型,我们假定一个强可容许的(strong admissible)、静态(static)的攻击者[11]. 这里的强可容许指的是攻击者可以勾结任何分享者,但每一个合格子集中至少有一名成员不能被勾结,同时至少有一个合格子集,其中的所有成员都不会与攻击者勾结. 静态指的是攻击者在协议开始之前就已经确定好了要与那些分享者勾结. 为方便起见,我们称与攻击者勾结的分享者是不诚实的. 攻击者可以得到不诚实的分享者所拥有的任何秘密信息.

私钥的生成

(1) H 中每一成员 H_j 在 $K = Z_q$ 上按均匀分布随机选择一个元素 x_j, H_j 作为分发者把自己的秘密 x_j 按 2.2 节中的可验证秘密分享方案在 H 的全体成员(包括自己)中,以 Γ 为接入结构进行分享. 他发给 H_k 的秘密份额为 (s_{jk}, r_{jk}). 之后,他向 H 的全体成员广播 $g^{x_j} \pmod p$. 具体过程如下: H_j 随机地选取 $E = K^{n-1}$ 中的向量 v_j, β_j,使得 $v_j \cdot \Psi(D) = s_j$,即 $v_{j1} a_1 + v_{j2} a_2 + \cdots + v_{j,n-1} a_{n-1} = s_j$. 记 $r_j = \beta_j \cdot \Psi(D) = b_{j1} a_1 + b_{j2} a_2 + \cdots + b_{j,n-1} a_{n-1}$,其中 $v_j = (v_{j1}, v_{j2}, \cdots, v_{j,n-1})$, $\beta_j = (b_{j1}, b_{j2}, \cdots, b_{j,n-1})$, D 计算并广播对秘密 s_j 的承诺

$$E_{j0} = E(s_j, r_j) = g^{s_j} h^{r_j} \pmod p$$

及对向量 $v_j = (v_{j1}, v_{j2}, \cdots, v_{j,n-1})$ 的承诺

$$E_{jk} = E(v_{jk}, b_{jk}) = g^{v_{jk}} h^{b_{jk}} \pmod p, \quad j = 1, 2, \cdots, n-1.$$

之后 H_j 计算给每一成员 H_k 的份额

$$s_{jK} = v_j \cdot \Psi(H_k) = v_{j1} a_{1k} + v_{j2} a_{2k} + \cdots + v_{j,n-1} a_{n-1,k},$$

$$r_{jk} = \beta_j \cdot \Psi(H_k) = b_{j1} a_{1k} + b_{j2} a_{2k} + \cdots + b_{j,n-1} a_{n-1,k}$$

并把 (s_{jk}, r_{jk}) 秘密地发送给 H_k, $k = 1, 2, \cdots, n$.

(2) 每一 H_k 验证 H_j 发给自己的份额的有效性,即每一 H_k 检验以下两个等式是否成立:

$$E_{j0} = \prod_{i=1}^{n-1} E_{ji}^{a_i} \pmod p, \quad E(s_{jk}, r_{jk}) = g^{s_{jk}} h^{r_{jk}} = \prod_{i=1}^{n-1} E_{ji}^{a_{ik}} \pmod p$$

若第一个等式不成立,则说明 H_j 对其秘密 s_j 及向量 $v_j = (v_{j1}, v_{j2}, \cdots, v_{j,n-1})$ 的承诺不相容,所有 H_k 记 $s_{jK} = r_{jk} = 0$, $k = 1, 2, \cdots, n$. ,从而 s_j 被默认为 0;若第二个等式不成立,则说明 H_j 发给自己的份额 (s_{jk}, r_{jk}) 无效, H_k 广播 (s_{jk}, r_{jk}) 及对 H_j 的一个抱怨;若 H_j 受到某一合格子集中全体成员的抱怨,则所有 H_k 记 $s_{jK} = r_{jk} = 0$, $k = 1, 2, \cdots, n$,从而 s_j 被默认为 0. 当 s_j 被默认为 0 时, H 中全体成员记 $v_j = \beta_j = 0 = (0, 0, \cdots, 0)$.

(3) H 中每一成员 H_k 计算 $x_k = s_{1k} + s_{2k} + \cdots + s_{nk}$, $t_k = r_{1k} + r_{2k} + \cdots + r_{nk}$, $k = 1, 2, \cdots, n$,并向全体成员广播"ok",以表示已经收到了所有成员发送的份额 (s_{jk}, r_{jk}), $j = 1, 2, \cdots, n$.

(4) 分布式生成的私钥为 $x = s_1 + s_2 + \cdots + s_n$. H 中每一成员 H_k 持有的关于私钥 x 的份额为 (x_k, t_k).

公钥的提取

(5) 在步骤 2 中正确地分享了其所选的秘密数 s_j 的每一 H_j (步骤 2 中的两个等式都成立, s_j 未被全体成员默认为 0) 向全体成员广播 $A_{j0} = g^{s_j} \pmod p$, $A_{jk} = g^{v_{jk}} \pmod p$, $k = 1, 2, \cdots, n-1$.

(6) 每一 H_k 验证各 H_j 在步骤 5 中广播的数据的有效性,即检验是否有

$$A_{j0} = \prod_{k=1}^{n-1} (g^{v_{jk}})^{a_k} \pmod p, \quad g^{s_{jk}} = \prod_{i=1}^{n-1} (g^{v_{ji}})^{a_{ik}} \pmod p$$

若对某一 H_j 上述等式不成立, H_k 广播对 H_j 的一个抱怨以及相应的 (s_{jk}, r_{jk}).

(7) 若某一 H_j 在步骤 6 中受到至少一个成员 H_k 的有效抱怨,即 $E_{j0} = \prod_{i=1}^{n-1} E_{ji}^{a_i} \pmod p$, $E(s_{jk}, r_{jk}) = g^{s_{jk}} h^{r_{jk}} = \prod_{i=1}^{n-1} E_{ji}^{a_{ik}} \pmod p$,而 $A_{j0} = \prod_{k=1}^{n-1} (g^{v_{jk}})^{a_k} \pmod p$, $g^{s_{jk}} \neq \prod_{i=1}^{n-1} (g^{v_{ji}})^{ik} \pmod p$,除 H_j 外的其他成员运行 2.2 节中的恢复算法,计算出 s_j 及 $A_{j0} = g^{s_j} \pmod p$.

(8) 所有成员置 $y_j = \begin{cases} A_{j0}, & s_j \text{ 未被默认为 } 0 \\ 1, & s_j \text{ 被默认为 } 0 \end{cases}$,

并计算 $y = \prod_{k=1}^{n} y_k \pmod p$ 作为与所生成的私钥 x 对应的公钥.

执行完公钥提取协议后,每一 H_j 安全保存自己的秘密份额 (x_j, t_j),并及时销毁自己在密钥生成过程中所选取的秘密值 s_j 及秘密向量 v_j, β_j.

3.3 密钥生成协议分析

定理 1 密钥生成协议的运行结果使得 H 中的全体成员以向量空间接入结构 Γ 可验证地分享了一个按均匀分布从 Z_q 中随机选取的秘密值 $x = s_1 + s_2 + \cdots + s_n$.

证明 由攻击者模型知,至少有一个合格子集,其中的所有成员都是诚实的,因而他们能自始至终正确地执行协议. 这保证了 $s_1, s_2, \cdots, s_n$ 中至少有一个是按均匀分布从 Z_q 中随机选取的秘密值,从而 $x = s_1 + s_2 + \cdots + s_n$ 也是按均匀分布从 Z_q 中随机选取的秘密值.

令 $t = r_1 + r_2 + \cdots + r_n$, $v = v_1 + v_2 + \cdots + v_n = (v_1, v_2, \cdots, v_{n-1})$, $\beta = \beta_1 + \beta_2 + \cdots + \beta_n = (b_1, b_2, \cdots, b_{n-1})$,由私钥的生成算法,我们有

$$\begin{aligned} x &= s_1 + s_2 + \cdots + s_n = v_1 \Psi(D)^{\mathrm{T}} + v_2 \Psi(D)^{\mathrm{T}} + \cdots + v_n \Psi(D)^{\mathrm{T}} \\ &= (v_1 + v_2 + \cdots + v_n) \Psi(D)^{\mathrm{T}} = v \Psi(D)^{\mathrm{T}} \\ t &= r_1 + r_2 + \cdots + r_n = \beta_1 \Psi(D)^{\mathrm{T}} + \beta_2 \Psi(D)^{\mathrm{T}} + \cdots + \beta_n \Psi(D)^{\mathrm{T}} \\ &= (\beta_1 + \beta_2 + \cdots + \beta_n) \Psi(D)^{\mathrm{T}} = \beta \Psi(D)^{\mathrm{T}} \end{aligned}$$

对 $k = 1, 2, \cdots, n$, H 中成员 H_k 持有的关于私钥 x 的份额

$x_k = s_{1k} + s_{2k} + \cdots + s_{nk} = v_1 \Psi(H_k)^T + v_2 \Psi(H_k)^T + \cdots + v_n \Psi(H_k)^T = (v_1 + v_2 + \cdots + v_n) \Psi(H_k)^T = v\Psi(H_k)^T$,

$t_k = r_{1k} + r_{2k} + \cdots + r_{nk} = \beta_1 \Psi(H_k)^T + \beta_2 \Psi(H_k)^T + \cdots + \beta_n \Psi(H_k)^T = (\beta_1 + \beta_2 + \cdots + \beta_n) \Psi(H_k)^T = \beta \Psi(H_k)^T$,

令 $E_0 = \prod_{j=1}^{n} E_{j0} \pmod p$, $E_k = \prod_{j=1}^{n} E_{jk} \pmod p$, 则有

$$E_0 = \prod_{j=1}^{n} g^{s_j} h^{r_j} \pmod p = g^{\sum_{j=1}^{n} s_j} h^{\sum_{j=1}^{n} r_j} \pmod p$$

$$= g^x h^t \pmod p = \prod_{i=1}^{n-1} E_i^{a_i},$$

$$E_k = \prod_{j=1}^{n} g^{v_{jk}} h^{b_{jk}} \pmod p = g^{\sum_{j=1}^{n} v_{jk}} h^{\sum_{j=1}^{n} b_{jk}} \pmod p = g^{v_k} h^{b_k} \pmod p$$

$$E(x_j, t_j) = g^{x_j} h^{t_j} \pmod p = g^{\sum_{i=1}^{n-1} v_i a_{ij}} h^{\sum_{i=1}^{n-1} b_i a_{ij}} \pmod p$$

$$= \prod_{k=0}^{n-1} E_k^{a_{kj}} \pmod p$$

$v_1, v_2, \cdots, v_n, \beta_1, \beta_2, \cdots, \beta_n$ 的随机性决定了 $v = v_1 + v_2 + \cdots + v_n$ 和 $\beta = \beta_1 + \beta_2 + \cdots + \beta_n$ 的随机性,因此密钥生成协议中的私钥生成算法,使 H 中的全体成员以向量空间接入结构 Γ 按 2.2 节中的可验证秘密分享方案分享了一个按均匀分布从 Z_q 中随机选取的秘密值 $x = s_1 + s_2 + \cdots + s_n$.

定理 2　公钥的提取算法能够保证 $y = g^x \pmod p$.

证明　由公钥的提取算法可知

$$y = \prod_{k=1}^{n} y_k \pmod p = \prod_{j=1}^{n} A_{j0} \pmod p = \prod_{j=1}^{n} g^{s_j} \pmod p$$
$$= g^{\sum_{j=1}^{n} s_j} \pmod p = g^x \pmod p.$$

定理 3　假定在 Z_p^* 中计算以 g, h 为底的离散对数是不可行的,且任何人都不知道离散对数 $\log_g h$,则公钥的提取协议不会泄露私钥 x 及任何成员 H_k 持有的关于私钥 x 的份额 (x_k, t_k) 的信息.

证明　从公钥的提取协议中,攻击者可以得知 $y = g^x = \prod_{i=1}^{n} g^{s_i} = \prod_{j=1}^{n} A_{j0} \pmod p$,以及 $h^t = E_0 y^{-1} \pmod p$. 由在 Z_p^* 中计算以 g, h 为底的离散对数及计算 $\log_g h$ 的不可行性,攻击者无法获得私钥 x 及任何成员 H_k 持有的关于私钥 x 的份额 (x_k, t_k) 的信息.

类似的,$A_{j0} = g^{s_j} \pmod p$ 及 $A_{jk} = g^{v_{jk}} \pmod p$, $k = 1, 2, \cdots, n-1$,也不会泄露 s_j 及 v_j 的任何信息.

由上面的几个结果可以看出,我们提出的分布式密钥生成协议满足 3.1 节中关于安全 DKG 协议的三条基本要求,因而我们有

定理 4　3.2 节中所给出的分布式密钥生成协议满足安全的 DKG 协议必须具备的四条性质 $C1 \sim C4$.

在计算复杂性方面,本文提出的分布式密钥生成协议大约需要 $7n^2$ 次 Z_p^* 中的模指数运算和 $2n^3 + 4n(n-2)$ 次 Z_p 和 Z_q 中的乘法运算.

4　小结

分布式的密钥生成是面向群体的密码系统的一个重要组成部分. 现实世界中,有许多场合需要基于一般接入结构的群体密码系统. 在这样的密码系统中,密钥生成也应采用基于一般接入结构的分布式密钥生成协议. 向量空间接入结构是一类重要的接入结构,它具有良好的代数结构,且内容丰富,包含了所有的门限接入结构. 因而,对基于向量空间接入结构的分布式密钥生成协议的研究不仅在群体密码学的研究中有重要的理论意义,而且在分布式的数字签名、适应性秘密分享等方面有着重要的应用价值. 本文提出了向量空间接入结构上的一个分布式密钥生成协议. 分析表明,该协议具有良好的安全性,而且计算复杂度小,因此有一定的实用价值. 我们将在此协议的基础上进一步研究一些数字签名方案(如 DSS)的基于向量空间接入结构的群体实现问题.

参考文献:

[1] Pedersen T. A threshold cryptosystem without a trusted party[A]. EUROCRYPT '91[C]. Berlin: Springer-Verlag, 1991. 522 - 626.

[2] Gennaro R, Jarecki S, Krawczyk H, Rabin T. Secure distributed key generation for discrete-log based cryptosystems[A]. EUROCRYPT '99[C]. J Stern (Ed.), Berlin: Springer-Verlag, 1999. 295 - 310.

[3] Gennaro R, Jarecki S, Krawczyk H, Rabin T. Robust threshold DSS signatures[J]. Information and Computation, 2001, 164: 54 - 84.

[4] Shoup V. Practical threshold signaturs[A]. EUROCRYPT '2000[C]. Berlin: Springer-Verlag, 2000. 207 - 220.

[5] Herzberg A, Jakobsson M, Jarecki S, Krawczyk H, Yung M. Proactive public key and signature systems[A]. Proc. of the ACM Conference on Computers and Communication Security[C]. New York, ACM Press, 1997. 100 - 110.

[6] Shoup V, Gennaro R. Securing threshold cryptosystems against chosen ciphertext attack[A]. EUROCRYPT '98[C]. Berlin: Springer-Verlag, 1998. 1 - 16.

[7] Feldman P. A practical scheme for non-interactive verifiable secret sharing[A]. Proceedings of 28th IEEE symposium on Foundations of Computer Science[C]. New York: IEEE Press, 1987. 427 - 437.

[8] Pedersen T. Non-interactive and information-theoretic secure verifiable secret sharing[A]. Advances in Cryptology-Crypto '91[C]. Berlin, Springer Verlag, 1991. 129 - 140.

[9] Padró C, Sáez G, Villar J L. Detection of cheaters in vector space secret sharing schemes[J]. Designs, Codes and cryptography, 1999, 16(1): 75 - 85.

[10] Padró C. Robust vector space secret sharing schemes[J]. Information Processing Letters, 1998, 68: 107 - 111.

[11] Gennaro R. Theory and practice of verifiable secret sharing[D]. Massachusetts Institute of Technology (MIT), May, 1996.

作者简介:

张福泰　男,教授、博士,1965 年出生于陕西省陇县,主要研究兴趣为密码学与信息安全. E-mail: ffttzhang@sina.com.