基于广义可验证秘密分享的分布式密钥生成

张福泰[1,2],王育民[2]
(1. 陕西师范大学计算机科学学院,陕西西安 710062;2. 西安电子科技大学 ISN 国家重点实验室,陕西西安 710071)

摘 要: 利用广义可验证秘密分享,提出了基于离散对数的公钥体制的密钥的分布式生成协议. 该协议适用于任意的接入结构,具有需要各参与者保存的秘密信息的数据量小,能保证所生成的私钥的随机性和均匀分布性等特点. 因而与通常的基于门限接入结构的分布式密钥生成协议相比能够更广泛的应用于群体密码学中的各种场合.

关键词: 可验证秘密分享; 分布式密钥生成; 离散对数; 接入结构
中图分类号: TN918.4 **文献标识码**: A **文章编号**: 0372-2112 (2003) 04-0580-05

Distributed Key Generation Based on Generalized Verifiable Secret Sharing

ZHANG Fu-tai[1,2], WANG Yu-min[2]
(1. *School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*;
2. *Key Lab. on ISN, Xidian University, Xi'an, Shannxi* 710071, *China*)

Abstract: A distributed key generation protocol for public key cryptosystem based on discrete-log is proposed using generalized verifiable secret sharing. The protocol is applicable to arbitrary access structures, and has the following properties: the amount of secret information needed to be stored by each participant is small, and it can guarantee the randomness and uniformity of the distribution of the generated secret key. Hence it can be more widely used in group oriented cryptosystems than those protocols based on threshold access structures.

Key words: verifiable secret sharing; distributed key generation; discrete logarithm; access structure

1 引言

分布式的密钥生成[1,2] (Distributed Key Generation,简称 DKG),是门限密码系统[3~6]及分布式密码计算的重要组成部分. 它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,如群体签字或群体解密. 对基于离散对数的密码系统,分布式的密钥生成相当于分享一个随机的来自均匀分布的秘密值 x,而使 $y = g^x \pmod p$ 公开(p, q 是大素数, $q \mid (p-1)$, g 是 $GF(p)$ 中的一个 q 阶元素). 安全的 DKG 协议还是其它许多分布式协议的重要组成部分,如基于离散对数的签字协议中随机数的生成协议[2]及 proactive 秘密分享[5]中秘密份额的更新协议等.

第一个 DKG 方案是由 Pedersen[3]于 1991 年提出的. 之后,该方案被多次修改并被多次用于门限密码学及其应用的研究中[2,5,6]. Pedersen 的 DKG 协议[3]是以可验证秘密分享[7~9]为基础的,其基本思想是并行执行 n 次 Feldman 的可验证秘密分享协议[7](Feldman-VSS 协议),其中每一参与者 P_i 作为分发者把他随机选择的秘密值 z_i 可验证的在所有参与者中分享,最终的秘密钥 x 是被正确分享的各 z_i 之和,最终的公钥 y 是被正确分享的各 z_i 所对应的公开值 $y_i = g^{z_i} \pmod p$ 之积.

文献[1]对基于离散对数的分布式密钥生成进行了深入研究. 该文献首先给出了安全的 DKG 协议的基本要求,紧接着指出了文[3]中的 DKG 协议的安全缺陷,并给出了一种攻击方法. 恶意的攻击者利用这种方法可操纵秘密钥 x 的输出分布使其与均匀分布大相径庭. 之后,作者又提出了一个可证明安全的 DKG 协议,在这一协议中,不仅使用了 Feldman-VSS,而且应用了 Pedersen-VSS[8]. 与文[3]中的 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.

到目前为止,对基于门限接入结构的分布式密钥生成的研究已有不少,但对基于一般接入结构的分布式密钥生成的研究在文献中几乎见不到. 而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,它需要所有参与者具有完全同等的安全性和可靠性的假设来支持. 而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广义 VSS 协议和密钥生成协议的研究具有重要的理论和现实意义. 本文将对这一问题进行探讨. 我们将提出一个信息论安全的,可适用于一般

收稿日期:2001-09-17;修回日期:2002-04-16
基金项目:国家自然科学基金(No. 60073052);陕西师大校级重点科研项目

接入结构的广义 VSS 协议,并以它为基础设计出一个安全实用的基于一般接入结构的分布式密钥生成协议.

2　安全的广义可验证秘密分享方案

2.1　一个适用于任意单调接入结构的秘密分享方案

我们给出一个适用于任意单调接入结构的秘密分享方案,它是下面将要给出的广义可验证秘密分享协议的基础.

设 $GF(q)$ 是含有 q 个元素的一个有限域,其中 q 是一个大素数. $S = GF(q)$ 是秘密空间,也是份额空间. 系统的参与者为分发者 D 及分享者的集合 $H = \{H_1, H_2, \cdots, H_n\}$,其中 D 持有从 $S = GF(q)$ 中随机选取的秘密 s, H 上有一个单调接入结构 Γ,它给出 H 的那些特定的子集可合作恢复出被分享的秘密. 以 $\Gamma_0 = \{A_1, A_2, \cdots, A_t\}$ 表示 Γ 的基,即在包含关系下, Γ 的极小元构成的集合.

假定以上信息在执行份额的分配算法之前就已经公开.

份额的分配算法　分发者 D 随机选择 $GF(q)$ 上的一个 $n-1$ 次多项式 $f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$,其中 n 是分享者的人数, $a_0 = s$ 是要在 $H_1, H_2, \cdots, H_n$ 中分享的秘密. 接下来,对每一最小合格子集 $A_i = \{H_{i_1}, H_{i_2}, \cdots, H_{i_k}\} \in \Gamma_0$, D 利用 $k+1$ 个点 $(i_1, f(i_1)), (i_2, f(i_2)), \cdots, (i_k, f(i_k))$ 及 $(0, s)$ 按照拉格朗日插值法找出一个次数不超过 k 次多项式 $f_i(x)$,并计算出 $f_i(n+1)$, $i = 1, 2, \cdots, t$. 最后, D 把 $f(j)$ 秘密地发送给 H_j 作为其持有的份额, $j = 1, 2, \cdots, n$,并向所有分享者公布 $f_1(n+1), f_2(n+1), \cdots, f_t(n+1)$.

秘密的恢复算法　设 A 是任一合格子集, $A_j = \{H_{j_1}, H_{j_2}, \cdots, H_{j_k}\}$ 是 A 所包含的一个最小合格子集. A_j 中的每一成员把其持有的份额向 A 中所有成员广播,收集到 A_j 中所有成员的份额后, A 中成员可由 $k+1$ 个点 $(j_1, f(j_1)), (j_2, f(j_2)), \cdots, (j_k, f(j_k))$ 和 $(n+1, f_j(n+1))$ 根据拉格朗日插值法恢复出秘密 s. 对任何非合格子集 B,由于无法收集到任何最小合格子集的全体成员的份额,因而无法恢复秘密 s.

注:对具体的接入结构 Γ,可根据实际情况适当降低 $F(x)$ 的次数. 例如当 $\Gamma_0 = \{A \subseteq H : |A| = k\}$,即 Γ 是 (k, n) 门限接入结构时, $F(x)$ 的次数可选为 $k-1$,而使所有的 $F_i(x) = F(x)$,这时计算 $F_i(x)$ 及 $F_i(n+1)$ 的过程可省略掉,在这种情况下,就得到了 Shamir 门限方案.

2.2　安全的广义可验证秘密分享方案

系统参数及参与者　系统参数及参与者与 Pedersen-VSS 方案中相同: 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,且任何人都不知道离散对数 $\log_g h$. 参与者为分发者 D 及分享者的集合 $H = \{H_1, H_2, \cdots, H_n\}$,其中 D 持有从 $S = GF(q)$ 中随机选取的秘密 s, H 上有一个单调接入结构 Γ,它给出 H 的那些特定的子集可合作恢复出被分享的秘密. 以 $\Gamma_0 = \{A_1, A_2, \cdots, A_t\}$ 表示 Γ 的基,即在包含关系下, Γ 的极小元构成的集合. 在协议开始之前,分发者 D 把 H 及 $A_1, A_2, \cdots, A_t$ 依次向所有分享者公布. 秘密空间 $S = Z_q$,份额空间 $= Z_q \times Z_q$.

2.2.1　份额的分配算法

(1) D 公布对要分享的秘密 $s \in Z_q$ 的一个承诺: $E_0 = E(s, e) = g^s h^e$,其中 e 是在 Z_q 中随机选取的一个秘密值.

(2) D 随机选取 $Z_q[X]$ 中的 $n-1$ 次多项式 $F(x) = s + F_1 x + \cdots + F_{n-1} x^{n-1}$,计算 $s_j = F(j)$, $j = 1, 2, \cdots, n$. 之后 D 随机选取 $G_1, G_2, \cdots, G_{n-1} \in Zq$,计算并广播对 F_j 的承诺 $E_j = E(F_j, G_j) = g^{F_j} h^{G_j}$, $j = 1, 2, \cdots, n-1$.

(3) 令 $G(x) = e + G_1 x + \cdots + G_{n-1} x^{n-1}$, $e_j = G(j)$, $j = 1, 2, \cdots, n$. 对每一个最小合格子集 $A_i = \{H_{i_1}, H_{i_2}, \cdots, H_{i_k}\}$, D 由 $(i_1, F(i_1)), (i_2, F(i_2)), \cdots, (i_k, F(i_k))$ 及 $(0, s)$ 共 $k+1$ 个点用拉格朗日插值公式确定出一个 k 次多项式 $F_i(x)$,由 $(i_1, G(i_1)), (i_2, G(i_2)), \cdots, (i_k, G(i_k))$ 及 $(0, e)$ 共 $k+1$ 个点用拉格朗日插值公式确定出另一 k 次多项式 $G_i(x)$,计算出 $F_i(n+1)$ 及 $G_i(n+1)$ 的值,并向所有参与者公布.

(4) D 把 (s_j, e_j) 秘密地发送给 H_j 作为其持有的秘密份额, $j = 1, 2, \cdots, n$.

(5) 收到自己的秘密份额后,每一 H_j 通过检验是否有 $E(s_j, e_j) = \prod_{j=0}^{n-1} E_i^{j^i}$ 来验证自己的份额是否有效. 对每一最小合格子集 $A_i = \{H_{i_1}, H_{i_2}, \cdots, H_{i_k}\}$,所有参与者都可通过检验是否有 $E(F_i(n+1), G_i(n+1)) = \prod_{m=0}^{k} E_m^{b_m}$ 来验证公开数据 $F_i(n+1)$ 及 $G_i(n+1)$ 的有效性,其中 $b_0 = \prod_{j=1}^{k} (n+1-i_j) \Big/ \prod_{j=1}^{k} (-i_j)$, $b_m = (n+1) \sum_{1 \le j \le k, j \ne m} (n+1-i_j) / i_m \sum_{1 \le j \le k, j \ne m} (i_m - i_j)$, $m = 1, 2, \cdots, k$.

2.2.2　恢复算法

对于最小合格子集 $A_i = \{H_{i_1}, H_{i_2}, \cdots, H_{i_k}\}$ 而言,其中的成员 $H_{i_1}, H_{i_2}, \cdots, H_{i_k}$ 持有的份额依次为 $(s_{i_1}, e_{s_1}), (s_{i_2}, e_{i_2}), \cdots, (s_{i_k}, e_{i_k})$,如果这些份额都被验证为有效,那么 $(i_1, s_{i_1}), (i_2, s_{i_2}), \cdots, (i_k, s_{i_k})$ 及 $(n+1, F_i(n+1))$ 是多项式 $F_i(x)$ 上的 $k+1$ 个点,而 $F_i(x)$ 的次数不超过 k,因此每一最小合格子集中的成员可利用他们的有效份额,按照拉格朗日插值法正确地恢复出秘密 $s = F_i(0)$. 份额的验证算法在恢复秘密时可用来检测提供假的份额的参与者.

2.2.3　协议的安全性

我们假定一个强可容许的(strong admissible)、静态(static)的攻击者[9]. 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被勾结. 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,我们称被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.

命题 1　对强可容许的静态攻击者而言,我们提出的广义 VSS 协议是强健的(robust,或鲁棒的). 即攻击者无法恢复秘密而且不能阻止由诚实的分享者构成的合格子集正确地恢

复秘密.

证明 设 $A_i=\{H_{i_1},H_{i_2},\cdots,H_{i_k}\}$ 是任一合格子集,由于攻击者无法得到 A_i 的全体成员的所有份额,他最多只能知道与 A_i 相应的 k 次多项式 $F_i(x)$ 上的 k 个点(其中包含了一个公开点 $(n+1,F_i(n+1))$),由这些点无法确定出 $F_i(x)$,也无法确定出 $F_i(x)$ 上的其它任何一个点.因此,攻击者无法恢复出秘密.攻击者勾结多个合格子集的部分成员(他们全体仅构成一个不合格子集),也无法求出其中各最小合格子集所对应的多项式 $F_i(x)$ 的所有交点,因此,也得不到关于被分享的秘密 s 的任何信息.另外,由于至少存在一个合格子集,其中的所有分享者都是诚实的,攻击者无法阻止这样的合格子集正确地恢复秘密.

命题 2 设在 $GF(p)$ 中计算以 g 为底的离散对数是不可行的,则强可容许的静态攻击者所获得的信息是独立于被分享的秘密 s.即广义 VSS 协议是信息论安全的(无条件安全的).

证明 首先,由于所使用的承诺方案的安全性质[8],以及攻击者不能计算离散对数 $\log_g h$,公开的承诺 $E_0,E_1,\cdots,E_n$ 不会泄露关于被分享的秘密 s 及各分享者的秘密份额 $(s_1,e_1),(s_2,e_2),\cdots,(s_n,e_n)$ 的任何信息;其次,从分发者分发秘密份额所使用的多项式 $F(x)$ 来说,由于 $F(x)$ 的次数为 $n-1$,而攻击者所能知道的 $F(x)$ 上的点的个数不超过 $n-1$,因此,攻击者不能获得关于秘密 s 的任何信息;再次,从对应于每一最小合格子集 $A_i=\{H_{i_1},H_{i_2},\cdots,H_{i_k}\}$ 的多项式 $F_i(x)$ 来说,$F_i(x)$ 的次数为 k,而攻击者最多只能知道 $F_i(x)$ 上的 k 个点.因此,他不能得到关于 $F_i(x)$ 的常数项 s 的任何信息.

综上可知,假设在 $GF(p)$ 中计算以 g 为底的离散对数是不可行的,则强可容许的静态攻击者所获得的信息是独立于被分享秘密 s 的.即我们的广义 VSS 协议是无条件安全的.

3 基于广义 VSS 的分布式密钥生成协议

设系统的参与者是由 n 个成员 $H_1,H_2,\cdots,H_n$ 所形成的群体,$H=\{H_1,H_2,\cdots,H_n\}$ 上有一个单调接入结构 Γ,以 $\Gamma_0=\{A_1,A_2,\cdots,A_t\}$ 表示 Γ 的基.参数 p,q,g,h 的意义与第 2 节中相同,它们由参与者的群体以某种公开的方式产生或者由一可信的第三方生成.以 $x\in Z_q$ 表示群体将要生成的私钥,$y=g^x \pmod p$ 表示对应的群体公钥.

3.1 私钥的生成协议

1) 群体 H 中的每一成员 H_j 在 Z_q 中按均匀分布随机地选一元素 x_j,并把 x_j 用 2.2 节中的广义 VSS 协议在全体成员中以 Γ 为接入结构分享.具体过程如下:

(a) H_j 公布对要分享的秘密 $x_j\in Z_q$ 的一个承诺:$E_{j0}=E(x_j,e_j)=g^{x_j}h^{e_j}$,其中 e_j 是在 Z_q 中随机选取的一个秘密值.

(b) H_j 随机选取 $Z_q[X]$ 中的 $n-1$ 次多项式 $F_j(x)=x_j+F_{j1}x+\cdots+F_{j,n-1}x^{n-1}$,计算 $x_{jk}=F_j(k)$,$k=1,2,\cdots,n$.之后 H_j 随机选取 $G_{j1},G_{j2},\cdots,G_{j,n-1}\in Z_q$,计算并广播对 F_{ji} 的承诺 $E_{ji}=E(F_{ji},G_{ji})=g^{F_{ji}}h^{G_{ji}}$,$j=1,2,\cdots,n-1$.

(c) 令 $G_j(x)=e_j+G_{j1}x+\cdots+G_{j,n-1}x^{n-1}$,$e_{jk}=G_j(k)$,$j=1,2,\cdots,n$.对每一个最小合格子集 $A_i=\{H_{i_1},H_{i_2},\cdots,H_{i_k}\}$,$H_j$ 由 $(i_1,F_j(i_1)),(i_2,F_j(i_2)),\cdots,(i_k,F_j(i_k))$ 及 $(0,x_j)$ 共 $k+1$ 个点,用拉格朗日插值公式确定出一个 k 次多项式 $F_{ji}(x)$,由 $(i_1,G_j(i_1)),(i_2,G_j(i_2)),\cdots,(i_k,G_j(i_k))$ 及 $(0,e_j)$ 共 $k+1$ 个点,用拉格朗日插值公式确定出另一 k 次多项式 $G_{ji}(x)$,计算并向所有参与者公布 $F_{ji}(n+1)$ 及 $G_{ji}(n+1)$ 的值,$i=1,2,\cdots,t$.

(d) H_j 把 (x_{jk},e_{jk}) 秘密地发送给 H_k 作为其持有的关于 x_j 的秘密份额,$j=1,2,\cdots,n$.

(e) 收到自己的秘密份额后,H_k 检验是否有 $E_{jk}=E(x_{jk},e_{jk})=\prod_{i=0}^{n-1}E_{ji}^{k^i}$ 以验证自己的份额是否有效.对每一最小合格子集 $A_i=\{H_{i_1},H_{i_2},\cdots,H_{i_k}\}$,所有参与者都可通过检验是否有 $E(F_{ji}(n+1),G_{ji}(n+1))=\prod_{m=0}^{k}E_{ji}^{b_m}$ 来验证公开数据 $F_{ji}(n+1)$ 及 $G_{ji}(n+1)$ 的有效性,其中 b_0,b_m 的取值与 2.2.1-(5) 中的相同.

2) 如果 H_k 验证失败(即 x_{jk},e_{jk} 无效),则广播 x_{jk},e_{jk} 及对 H_j 的一个抱怨.

3) 如果 H_j 受到 H_k 的抱怨,则 H_j 应广播他给 H_k 的有效份额.

4) 如果某一 H_j 受到了某一合格子集的全体成员的抱怨或者受到某些成员的抱怨而在步骤 3 中广播的份额仍然无效,则每一成员用 0 替换 H_j 给自己的份额,即记 $x_{jk}=0=e_{jk}$,同时把 H_j 所选的秘密值 x_j 也记为 0,而把 $F_j(x)$ 和 $G_j(x)$ 都作为零多项式对待.

5) 每一成员 H_k 计算自己关于群体私钥 x 的份额 $s_k=x_{1k}+x_{2k}+\cdots+x_{nk} \pmod q$,$u_k=e_{1k}+e_{2k}+\cdots+e_{nk} \pmod q$ 而私钥 $x=x_1+x_2+\cdots+x_n \pmod q$.

3.2 公钥的提取协议

在 3.1 节的 5 个步骤都完成后,全体成员可如下提取群体公钥 $y=g^x \pmod p$,过程如下:

1) 每一成员 H_k 广播 $A_{ki}=g^{F_{ki}} \pmod p$,$i=0,1,2,\cdots,n-1$.

2) 成员 H_j 验证 H_k 广播的数据 $A_{ki}=g^{F_{ki}}$,$i=1,2,\cdots,n-1$ 的有效性,即检验是否有 $g^{x_{kj}}=\prod_{i=1}^{n-1}A_{ki}^{j^i}$,$j=1,2,\cdots,n$.若验证失败 H_j 广播对 H_k 的一个抱怨,$j=1,2,\cdots,n$.

3) 对在上一步中受到抱怨的 H_k,所有成员协作按照 2.2 节中广义 VSS 协议的恢复算法计算出 $x_k,F_k(x)$.所有成员置 $y_j=A_{j0}=g^{F_{j0}} \pmod p$,$j=1,2,\cdots,n$.

4) 每一成员计算群体公钥 $y=\prod_{j=1}^{n}y_j \pmod p$.

4 分布式密钥生成协议的正确性与安全性

4.1 正确性

定理 1 私钥生成协议的运行结果,使得所有成员按照 2.2 节中的广义 VSS 协议,分享了一个以均匀分布从 Z_q 中随机选取的秘密值 x.

证明　首先,由于每一 x_j 都是按均匀分布从 Z_q 中随机选取的,因而 x(所有 x_j 之和)亦是以均匀分布从 Z_q 中选取的随机值.(保证 x 服从均匀分布,只需至少有一 x_j 服从均匀分布,而要保证 x_j 的安全性,x_j 必须是以均匀分布从 Z_q 中随机选取的).

其次,令 $F(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} = F_1(x) + F_2(x) + \cdots + F_n(x)$, $F_i(x) = F_{1i}(x) + F_{2i}(x) + \cdots + F_{ni}(x)$, $G(x) = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1} = G_1(x) + G_2(x) + \cdots + G_n(x)$, $G_i(x) = G_{1i}(x) + G_{2i}(x) + \cdots + G_{ni}(x)$,则有 $s_k = x_{1k} + x_{2k} + \cdots + x_{nk} (\mathrm{mod}\, q) = F(k)$, $u_k = e_{1k} + e_{2k} + \cdots + e_{nk} (\mathrm{mod}\, q) = G(k)$, $F(x)$ 的常数项 $a_0 = x_1 + x_2 + \cdots + x_n = x (\mathrm{mod}\, q)$, $G(x)$ 的常数项 $b_0 = e_1 + e_2 + \cdots + e_n = e$, $F_i(n+1) = F_{1i}(n+1) + F_{2i}(n+1) + \cdots + F_{ni}(n+1)$, $G_i(n+1) = G_{1i}(n+1) + G_{2i}(n+1) + \cdots + G_{ni}(n+1)$.

令 $E_0 = E(x, e) = g^x h^e$, $E_j = E(a_j, b_j) = g^{a_j} h^{b_j}$, $j = 1, 2, \cdots, n-1$,则

$$E_0 = \prod_{j=1}^{n} E_{j0},\ E(s_k, u_k) = g^{s_k} h^{u_k} = \prod_{j=0}^{n-1} E_j^{k^j} = \prod_{i=0}^{n-1} \prod_{j=0}^{n} E_{ji}^{k^i} = \prod_{j=1}^{n} \prod_{i=0}^{n-1} E_{ji}^{k^i} = \prod_{j=1}^{n} E_{ik}(x_{jk}, e_{jk}).$$

因此,若每一 H_j 用多项式 $F_j(x)$ 和 $G_j(x)$ $(j = 1, 2, \cdots, n)$ 成功地以 2.2 节中的广义 VSS 协议分享了自己选择的秘密值 x_j,则在私钥生成协议结束时,秘密值 x 就被全体成员用多项式 $F(x)$ 和 $G(x)$ 成功地以 2.2 节中的广义 VSS 协议分享.

这说明私钥的生成协议能够产生一个按均匀分布随机地取自 Z_q 的秘密值-私钥,因而私钥的生成协议是正确的.

4.2　安全性

由于我们的分布式密钥生成协议,主要采用了 2.2 节中的无条件安全的广义可验证秘密分享技术,与 2.2 节中一样,假定一个强可容许的静态攻击者[9]. 我们使用一个最基本的计算困难性假设,即在 $GF(p)$ 中计算以 g、h 为底的离散对数对任何人来说是不可行的.

定理 2　设在 $GF(p)$ 中计算以 g、h 为底的离散对数不可行的,则强可容许的静态攻击者在私钥的生成协议中无法获取关于私钥的任何信息.

证明　由于在私钥的生成协议中,每一成员 H_j 在全体成员中分享自己随机选择的秘密值 x_j 时,都采用了以 Γ 为接入结构的无条件安全的广义 VSS 协议,最终导致全体成员以 Γ 为接入结构,按照 2.2 节中的广义 VSS 协议分享了以均匀分布随机地选自 Z_q 的秘密值 x(定理 1). 对于强可容许的静态攻击者而言,因为他不能获取任何一个合格子集的所有成员关于私钥 x 的秘密份额,同时也由于在 $GF(p)$ 中计算以 g、h 为底的离散对数的不可行性,他也无法从公开信息中计算出任何诚实的成员的秘密份额,所以他无法获得关于被分享的秘密(私钥 x)的任何信息.

定理 3　公钥的提取协议是安全的,即公钥的提取协议不会泄露任何成员持有的关于私钥的份额.

证明　由于在公钥的提取协议中,每一成员只是公开对自己分发所选择的秘密的份额时所用的多项式的系数的承诺,在计算离散对数不可行的条件下,这些公开的承诺并不会泄露任何成员的私有信息. 虽然在协议的最后,分享私钥 x 所用的多项式的相关信息,即对其系数的承诺 $g^{a_j} (\mathrm{mod}\, p)$, $j = 1, 2, \cdots, n-1$ 被公开,但正如 Feldman-VSS 协议一样,基于在 $GF(p)$ 中计算离散对数的困难性,这些公开的承诺并不会泄露各成员持有的关于私钥 x 的任何秘密信息.

上述几个定理说明,我们提出的分布式密钥生成协议不仅是正确的,而且对强可容许的静态攻击者而言,是安全的.

4.3　分布式密钥生成协议的特点

® 能适用于任意的单调接入结构. 这一点可从 2.2 节中的广义 VSS 协议的特点看出.

® 具有简单的代数结构. 协议中采用的秘密分享方法类似于 Shamir 门限体制,以拉格朗日多项式插值法为基础,因而结构简单,便于应用.

® 需要各参与者保存的秘密信息的数据量小. 协议中所有可验证秘密分享均采用了 2.2 节中的广义 VSS 协议,在其中每一分享者只需保存两个秘密数据,而不用考虑各分享者所属的最小合格子集的个数,这一点在现有的其它广义 VSS 协议中都无法达到.

® 能保证所生成私钥的随机性和服从均匀分布的特性(定理 1). 这一特点在密钥的生成协议中具有非常重要的意义,协议之所以具有这样的特点,是由于我们在其中采用了类似于 Pedersen-VSS 方案的无条件安全的广义 VSS 协议. 正如文献[1]所指出的那样,若采用类似于 Feldman-VSS 方案的广义 VSS 协议,则攻击者就有可能左右协议所产生的私钥的分布.

® 通信代价较小. 如特点 2 所说,秘密信息的数据量小使得协议的通信代价大为减小.

® 协议的计算代价随着接入结构 Γ 的基 Γ_0 的基数的增大而增大. 在 Γ_0 的基数 $\leq n^2$ 的情况下,总体计算复杂度为 $O(n^4 \log n)$.

以上特点说明,我们提出的分布式密钥生成协议是安全有效的,且具有广泛的适用性.

5　结束语

分布式的密钥生成是群体密码学中一个重要的研究课题. 基于一般的单调接入结构的分布式解密、数字签字、签密及多方安全计算在许多场合是必不可少的,它们往往都要依赖于分布式的密钥生成. 因此,本文对具有一般接入结构的分布式密钥生成的研究在理论和实际两方面都有重要意义. 首先给出了一个可适用于任意接入结构的广义可验证秘密分享协议,该协议结构简捷,信息速率较高,且是无条件安全的. 其次,以文中提出的广义 VSS 协议为基础,设计了一个具有一般接入结构的分布式密钥生成协议. 从上分析可以看出本协议是安全的、有效的且具有广泛的适用性. 我们下一步的研究目标将是以本文提出的密钥生成协议为基础,设计出具有一般接入结构的安全实用的分布式数字签字及签密协议.

参考文献:

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

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

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

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

[5] Herzberg A, Jakobsson M, Jarecki S, Krawczyk H, Yung M. Proactive public key and signature systems [A]. In 1997 ACM Conference on Computers and Communication Security [C]. 1997. http://citeseer.nj.nec.com/39025.html.

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

[7] Feldman P. A Practical Scheme for non-interactive verifiable secret sharing [A], In Proceedings of 28th IEEE symposium on Foundations of Computer Science [C]. 1987. 427 - 437.

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

[9] Gennaro R. Theory and practice of verifiable secret sharing [D]. PhD thesis, Massachusetts Institute of Technology, May 1996.

作者简介:

张福泰 男,1965 年 8 月出生于陕西陇县,副教授,博士,主要研究兴趣为信息安全及电子商务. Email: Zhangfutai@263.net ffttzhang@hotmail.com

王育民 男,1936 年 2 月出生于北京市,教授,博士生导师,IEEE 高级会员,长期从事通信和信息安全方面的教学和研究工作,取得了大量研究成果.