具有空间、时间双重分布性的随机会话密钥分发系统

逯海军,苏云学,祝跃飞
(信息工程大学信息工程学院网络工程系,河南郑州 450002)

摘 要: 本文首先提出了分布式密码协议的空间分布性和时间分布性的观点,并从双重分布性的角度研究分布式密码协议.作为一个例子,在 V. Daza 的密钥分发系统中一个只具有空间分布性的分布式密钥分发系统的基础上,引入了前置安全(proactive security)体制,得到了一个具有空间和时间双重分布性,可以抵抗动态攻击者的分布式密钥分发协议.拓展了分布式密码协议的研究空间.同时,文中在建立概率空间的基础上,证明了分布式密钥分发系统的安全性.

关键词: 分布式密码; 秘密共享; 随机会话密钥; 动态攻击者; 概率空间
中图分类号: TN918, TP309 **文献标识码**: A **文章编号**: 0372-2112 (2005) 01-0096-05

A Distributed Random Key Distribution System with Distributed Characteristics of Space and Time

LU Hai-jun, SU Yun-xue, ZHU Yue-fei
(Department of Network Engineering, Information Engineering College, Information Engineering University, Zhengzhou, Henan 450002, China)

Abstract: This paper first gives the notion about distributed cryptographic protocol with distributed characteristics of space and time. Then research distributed cryptographic protocol based on the notion. For an instance, we use proactive security in an distributed key distribution system only with distributed characteristic of space and give a distributed protocol against mobile adversary. This paper enlarges research field of distributed cryptographic protocol. At last, this paper proves the security of distributed random key distribution protocol based on the probability space.

Key words: distributed cryptographic; sharing secret; random session key; mobile adversary; probability space

1 引言

近年来,分布式密码是一个特别活跃的研究领域,它涉及到具有一般结构的分布式密码系统、新的公钥密码体制、秘密共享、多方计算和密钥分发、管理等等[1]研究领域.但这些领域都是在多个主体参与的分布式应用环境中研究的.

目前人们研究的分布式应用环境是指空间的分布性.空间分布性是指涉及多个主体参与的,实现密码算法或密码协议的硬件分布和其所用数据分布的环境.硬件的分布是指分布式的应用环境中包含多台计算机,每个计算机都拥有自己的处理机和存储器.数据的分布性包含两方面的含义,一是指数据的分割,即数据分割成多个部分;一是指数据重复,即同一数据有多个拷贝,每个拷贝存放在不同的计算机上.这些计算机可以看作分布式密码中涉及的主体.

本文中则把时间的分布性作为分布式应用环境必不可少的组成部分.时间的分布性是指时间的延续和延迟.比如,信息在网络中传输延迟就是一种时间分布性.计算网络就是一个典型的,最常见的分布式应用环境.

针对在分布式的网络环境中出现的新的安全需求,分布式密码协议的设计和应用面临着更为复杂的情形,这种复杂不仅表现在参与密码协议运行的主体的大数量性、动态性及协议运行的并发性,而且表现在分布式网络环境的复杂性,包括攻击者的复杂性.一方面,分布式密码可以包含多个密码运算或者是多个密码协议的协同综合.另一方面,其攻击者由一个转为多个,甚至是多个攻击者协同攻击的攻击系统.参与分布式密码协议的主体也变为多个,甚至是动态变化的.

分布式环境中的这种攻击者称为动态攻击者(mobile adversary).这种攻击者可以在整个系统的运行时间内,控制所有的系统参与者,但不能在较短的时间中控制足够多的参与者而达到攻击目的.Ostrovsky 和 Yung 最先在文[2]中考虑了这种攻击者,他们要求参与者经常交换消息并刷新内存,从而达到抵抗这种攻击者的目的.事实上,前置安全就是指可抵抗一个动态攻击者的密码体制.文献[3]中利用可证实的秘密共享系统提出了一个多项式秘密共享的前置安全系统.后来,文献[4]进

收稿日期:2003-06-12;修回日期:2004-10-22
基金项目:国家 973 项目(No. G1999035804);国家自然科学基金(No. 90204015,19931010);河南省杰出青年基金(No. 0212001400)

一步讨论了前置安全的秘密共享系统,给出了一个详细的实用系统.在这个系统中,系统的运行时间被分成时间段.在每个时间段的开始,秘密共享者参与一个交互式的更新协议.在时间段的结束,秘密共享者得到一个新的共享份额文[5,6]也讨论了这方面的问题.之后文[7]在文[2,4]的基础上,提出了一个无条件安全的前置安全秘密共享系统.这个系统主要是利用一个对称多项式达到了共享秘密的更新.

如上,尽管人们已研究了抵抗动态攻击者的方法,但在分布式的密钥分发体制中,目前较多地考虑了只有部分参与者被控制的情形,如文献[7]给出了一个分布式的,计算上安全的密钥分发系统.是在修改了文献[9]的系统的基础上完成的.利用服务器之间的秘密共享,给出了一个由一组服务器为一群用户分发会话密钥的安全系统.该系统利用了 EL Gamal 加密的特性,并将文[9]中由用户完成的大量计算交由服务器完成.是一个很好的密钥分发系统.但是,该系统中将攻击者的能力局限于只控制一组服务器中一定数量的服务器.事实上,一个动态攻击者在足够的时间中完全可以控制更多的,甚至是全部服务器.因此在该系统中引入前置安全机制是必要的.

本文的主要工作是在分布式密码协议的空间分布性和时间分布性观点的指导下,利用向量空间秘密共享的更新方法,在文献[8]中提出的 DKDS(distributed key distribution scheme)密钥分发协议中,通过共享秘密及时更新的方法来抵抗动态攻击者对该协议的攻击.另外,我们还在建立概率空间的基础上,证明了分布式密钥分发系统的安全性.

2　预备知识

这部分我们描述一些后文要用到的密码体制和协议.

2.1　EL Gamal 公钥加密体制.

文献[10]中,EL Gamal 提出了一个公钥加密体制.系统的公开参数是两个大素数 p, q.且 $q \mid p-1$. g 是一个阶为 q 的 Z_p^* 的乘法子集的生成元.每一个用户 U 如下生成公钥和私钥.

随机选取 $x \in Z_q^*$,计算 $y = g^x \bmod p$, U 的公钥是 (p, q, g, y),私钥是 x.如果一个用户加密一个消息 $m \in Z_p$,则随机选取 $\beta \in Z_q^*$,计算 $r = g^\beta \bmod p$, $s = my^\beta \bmod p$,传输给 V 的密文为 $c = (r, s)$, V 计算的明文为 $m = sr^{-x} \bmod p$,该加密体制的安全性等价于 Diffie-Hellman 假设[11].这个体制的一个最有用的特性是密文的同态性.即,如果 $c_i = (r_i, s_i)$ 是 m_i 的密文,则 $c_i = (r_1 r_2, s_1 s_2)$ 是 $m = m_1 m_2$ 的密文.这种特性将用在 DKDS 系统中.要特别注意的是,在分布式密码的研究中,寻找具有类似特性的公钥加密体制是一个重要的研究任务.

2.2　离散对数的知识证明

零知识证明,是 VSS 和 PVSS 不可缺少的环节.零知识证明有交互式和非交互式两种.考虑到通信代价的因素,我们这里只考虑非交互式的零知识证明.再考虑到对分布式密码协议的适用性,我们这里只考虑离散对数的知识证明.本文中,我们使用了文[16]中的非交互式的离散对数的知识证明协议,用

$$PK\{(\alpha,\beta): A = g_1^\alpha g_2^\beta \wedge B = g_3^\alpha\}$$

表示使 $A = g_1^\alpha g_2^\beta$, $B = g_3^\alpha$ 的 α, β 值的零知证据.$(\alpha, \beta, \cdots)$ 表示当被校验者知道 (A, B, g_1, g_2, g_3) 时被证明的知识的数量.

2.3　秘密共享体制

Shamir[12]和 Blakley[13]最早提出了秘密共享概念,在秘密共享体制中,有多个主体 $P = \{P_1, \cdots, P_n\}$ 共享一个秘密,只有得到授权的一组主体能够恢复秘密,这种可以恢复秘密的主体子集的集合称为秘密共享体制的访问结构(access structure),记为 Γ,它为一个单增集合,即任何一个包含一个授权子集的集合也是一个授权集.同时,因为要考虑有部分服务器被攻击者控制的情况,引入了攻击结构(adversary structure) $A \subset 2^s$,它是由安全系统可容忍的,被攻击者控制的服务器的子集组成的集合.它也是一个单增集合.

本文中,考虑下面的向量空间秘密共享体制.

文献[14]中的向量空间中的秘密共享体制,体制的访问结构 Γ,由定义在 Z_q 上的体制实现.具体如下.

对素数 q,取一个正数 r 和一个函数

$\Psi: P \cup \{D\} \to (Z_p)^r$,使

$W \in \Gamma$,当且仅当, $\Psi(D) \in (\Psi(p_i))_{p_i \in W}$(线性空间).

其中, D 是一个不属于 $P = \{P_1, \cdots, P_n\}$ 的特殊主体,即 Dealer.

若 D 要使一个秘密 $x \in Z_q$ 在 $P = \{P_1, \cdots, P_n\}$ 中共享,则 D 随机选择 $v \in (Z_q)^r$,使

$$v \cdot \Psi(D) = x.$$

则 D 发送给一个参与共享的主体 $p_i \in P$ 的共享份额是

$$x_i = v \cdot \Psi(p_i) \in Z_q$$

令 W 是一个授权子集,即 $W \in \Gamma$,则存在, $\lambda_i^W \in Z_q$,使

$$\Psi(D) = \sum_{p_i \in W} \lambda_i^W \Psi(p_i)$$

为恢复秘密, W 计算

$$\sum_{p_i \in W} \lambda_i^W x_i = \sum_{p_i \in W} \lambda_i^W x_i v \cdot \Psi(p_i) = v \cdot \sum_{p_i \in W} \lambda_i^W \Psi(P_i) = x \bmod q$$

2.4　DKDS(distributed key distribution scheme)分布式密钥分发系统

文献[8]中提出的 DKDS 密钥分发协议如下.

设 $S = \{S_1, \cdots, S_n\}$ 为一个服务器集合, $U = \{U_1, \cdots, U_n\}$ 为一个用户集,令 $C \subset 2^u$ 是由需要安全通信的用户集组成的集合,称为会议集,集合中每一个元素 c 称为一个会议,每个会议都有一个会话密钥.在这里,秘密共享体制的访问结构 $\Gamma \subset 2^s$,攻击结构 $A \subset 2^s$.

协议的目的是服务器集 S 中的服务器子集利用各自的共享秘密为用户集提供会话密钥.

需要说明的是,在很多有关秘密共享的协议中,都有一个知道所有共享份额的管理者(Dealer),一旦这个 Dealer 被攻击者所控制,后果不堪设想.为解决这一安全隐患,在随机秘密的产生时,使用了没有这种 Dealer 的分布式的秘密产生方式.

对和前文同样的访问结构 Γ 和攻击者结构 A,若对所有的 $B \in A$,有 $R - B \in \Gamma$,则称这样的子集 R 为协议的 Robust

子集,记所有子集 R 组成的集合为 $\Omega=(\Gamma,A)$,协议由服务器的 Robust 子集 $R\in\Omega$ 如下实现.

首先,每一个 $s_i\in R$ 随机选择 $k_i\in Z_q$,用文[15]中的可认证的向量空间秘密共享体制分发给 S 中的服务器. 具体如下.

p,q 是大素数,使,是 $q/p-1$,g 是阶为 q 的 Z_p^* 的一个乘法子群的生成元. $s_i\in R$ 选择一个随机向量 $v_i=(v_i^{(1)},\cdots,v_i^{(r)})\in(Z_q)^r$,使 $v_i\Psi(D)=k_i$. 对任一得到授权的服务器子集 $W\in\Gamma$,存在,$\lambda_i^W\in Z_q$,使 $\Psi(D)=\sum_{p_i\in W}\lambda_i^W\Psi(p_i)$.

然后,$s_i\in R$ 给每个 $s_j\in R$ 发送它的对 $k_i\in Z_q$ 的共享份额 $k_{ij}=v_i\Psi(S_j)$,并公布 $v_{il}=g^{v_i^{(l)}}$,$1\le l\le r$.

接着,每个 $s_j\in R$ 通过下面的等式验证自己共享份额的正确性,$g^{k_{ij}}=g^{v_i\Psi(S_j)}=\prod_{l=1}^{r}g^{v_i^{(l)}\Psi(s_j)^{(l)}}=\prod_{l=1}^{r}(v_{il})^{\Psi(s_j)^{(l)}}$

如果失败,$s_j\in R$ 公开发出一个对该 s_i 的谴责.

若 $s_i\in R$ 接到的谴责自己的服务器组成的集合不属于攻击者结构 A,则这个集合被拒绝. 相反的话,$s_i\in R$ 向谴责自己的 $s_j\in S$ 公布相应其 k_{ij},其后,若任一被公布的共享不满足以前的认证等式,则 s_i 也被拒绝. 通过这种方法,得到了一个通过认证的服务器集合.

记 $Qual\subset R$ 为通过认证的服务器集合,根据 Ω 的定义,可知 $Qual\in\Gamma$,因此,可以从 $Qual\in\Gamma$(记 $Qual\in\Gamma$ 为 W)中每个服务器的共享份额中计算出共享秘密 x

$$\begin{aligned}\sum_{j\in W}\lambda_j^W\alpha_j&=\sum_{j\in W}\lambda_j^W\sum_{i\in S}k_{ij}=\sum_{j\in W}\sum_{i\in S}\lambda_j^W v_i\Psi(p_j)\\&=\sum_{i\in S}v_i\sum_{j\in W}\lambda_j^W\Psi(p_j)=\sum_{i\in S}v_i\Psi(D)\\&=\sum_{i\in S}k_i=\alpha\end{aligned}$$

我们记这种秘密共享方式为

$$(\alpha_1,\cdots,\alpha_n)\xleftarrow{(S,\Gamma,A)}(\alpha,g,\{D_i\}_{1\le i\le n})$$

注 1:由于 $Qual\in\Gamma$,故 $Qual\notin A$,因此攻击结构 A 的任一子集都不可以从它们最初的共享份额 k_i 中的得到共享秘密 α,每个 $s_j\in S$ 如下计算自己对 α 的共享份额,$\alpha_j=\sum_{i\in Qual}k_{ij}$

注 2:任何一个服务器都可以如下计算用来进行离散对数知识证明的 $D_j=g^{\alpha_j}$ 的值(此值作为后面验证时的证据),

$$D_j=g_i\sum_{i\in Qual}k_{ij}=\prod_{i\in Qual}g^{k_{ij}}=\prod_{i\in Qual}\prod_{l=1}^{r}(v_{il})^{\Psi(p_j)^{(l)}}$$

DKDS(分布式密钥分发系统)分下面三阶段:

初始化阶段 利用上面的秘密共享方式,在建立访问结构 Γ 的基础上,每一个服务器得到一个随机秘密 α 的共享份额 $\{\alpha_i\}_{i\in S}$.

会话密钥要求和计算阶段 一个会议 $c\in C$ 的用户 u_j 联系服务器的子集 $R\in\Omega$ 索要会议 $c\in C$ 的会话密钥 k_c,每一个服务器 $s_i\in R$ 验证 u_j 是不是 $c\in C$ 中成员,若通过验证,服务器 $s_i\in R$ 用其共享份额 $\{\alpha_i\}_{i\in S}$ 和一个与会议相关的值计算对会议 $c\in C$ 的会话密钥 k_c,$c\in C$ 的共享份额. 然后 $s_i\in R$ 用 EL Gamal 公钥加密体制,利用 u_j 的公钥加密这个共享份额. $s_i\in R$ 中通过认证的服务器集合用自己的共享份额,并利用 EL Gamal 公钥加密体制的同态性,计算出会议的会话密钥 k_c 的利用 u_j 的公钥加密的密文.

密钥传递阶段 $s_i\in R$ 中的所有服务器根据攻击者的主动性和被动性,通过一个鉴别信道将计算结果发送给 u_j,用户可以利用自己的私钥解密并得到会话密钥 k_c.

3 抗动态攻击者的分布式会话密钥分发协议

系统设置 在给出会话密钥分发协议之前,我们先给出系统的基本设置.

$S=\{S_1,\cdots,S_n\}$ 为一个服务器集合,$U=\{U_1,\cdots,U_n\}$ 为一个用户集,$c\in C\subset 2^u$ 称为一个会议,每个会议都有固定的 HUSH 值 h_c. 秘密共享体制的访问结构 $\Gamma\subset 2^S$,攻击结构 $A\subset 2^S$,同前,且 $\Gamma\cap A=\phi$.

初始化阶段 要求一个服务器的 Robust 子集 $R\in\Omega=\Gamma$ 执行该协议,它们共同用可验证的共享份额产生一个随机共享密钥,并可察觉被攻击者控制的服务器. 用前文的秘密共享方案. $(\alpha_1,\cdots,\alpha_n)\xleftarrow{(S,\Gamma,A)}(\alpha,g,\{D_1\}_{1\le i\le n})$

这里,g 是一个阶为 q 的 Z_p^* 的乘法子集的生成元,$D_j=g^{\alpha_j}$ 是公开发送的. 需要注意的是,尽管攻击者控制了 Robust 子集 $R\in\Omega=\Gamma$ 中一部分可容忍的服务器,但这些被控制的服务器可以被发现,剩下的服务器(记为 W)则属于 Γ,它们可以正确完成协议.

由于是利用向量空间秘密共享体制,因此,对 $W\subset R\in\Omega=\Gamma$,存在一组 Z_p 中的值 $\{\lambda_i^W\}_W$,使

$$\Psi(D)=\sum_{j\in W}\lambda_j^W\Psi_{(p_j)}$$

因此,可以从 $W\in\Gamma$ 中每个服务器的共享份额中计算出共享秘密 α

$$\begin{aligned}\sum_{j\in W}\lambda_j^W\alpha_j&=\sum_{j\in W}\lambda_j^W\sum_{i\in S}k_{ij}=\sum_{j\in W}\sum_{i\in S}\lambda_j^W v_i\Psi(p_j)\\&=\sum_{i\in S}v_i\sum_{j\in W}\lambda_j^W\Psi(p_j)=\sum_{i\in S}v_i\Psi(D)\\&=\sum_{i\in S}k_i=\alpha\end{aligned}$$

密钥要求和计算阶段 一个用户 u_j 向一个服务器的 Robust 子集 $R\in\Omega=\Gamma$ 要求会议会话密钥 k_c,每一个服务器 $s_i\in R$ 验证 u_j 是不是 $c\in C$ 中成员,若通过验证,服务器 $s_i\in R$ 输入会议 $c\in C$,求 HUSH 值,输出为 $h_c\in Z_p^*$ 中的一个元素,然后每个 $s_i\in R$ 用 u_j 的公钥 EL Gamal 公钥 (p,q,g,y_j) 加密 $h_c^{\alpha_i}$(注:会议密钥为 h_c^{α})具体加密过程是,服务器 $s_i\in R$ 选择一个随机元 $\beta_i\in Z_p^*$,再计算 $r_i=g^{\beta_i}\bmod p$,$\delta_i=h_c^{\alpha_i}y^{\beta_i}\bmod p$,则密文为 $c_i=(r_i,\delta_i)$. 然后 $s_i\in R$ 广播密文. 之后,每个服务器 $s_i\in R$ 广播 $h_c^{\alpha_i}$ 的密文 $c_i=(r_i,\delta_i)$.

下面,系统处理被控制的服务器联合抵制系统的情况. 即被控制的服务器发送和 $h_c^{\alpha_i}$ 不相配的密文 $\overline{c_i}=(\overline{r_i},\delta_i)$. 这里,我们使用前面提到的离散对数知识证明的概念.

具体在本协议中,零知识的证据为

$$PK\{\alpha_i,\beta_i\}:D_i=g^{\alpha_i}\wedge r_i=g^{\beta_i}\wedge\delta_i=(h_c)^{\alpha_i}(y_j)^{\beta_i}$$

也即,广播后 $c_i=(r_i,\delta_i)$,服务器必需证明它知道 α_i,β_i,

使　　$D_i = g^{\alpha_i}, r_i = g^{\beta_i}, \delta_i = (h_c)^{\alpha_i}(y_i)^{\beta_i}$

关于证明的过程,在文献[8]中有详细的叙述,主要是每个服务器公布证据,其他服务器来验证证据. 这里不再说明.

这样,每一个服务器 $s_i \in R$ 验证其他服务器公布的证据,直到它从一个授权子集中得到正确的共享份额的密文. 然后,$s_i \in R$ 可以用 EL Gamal 公钥加密体制的特性,如下得到会话密钥 $k_c = h_c^{\alpha}$ 的密文 $c = (r, \delta)$.

$$R = \prod_{s_i \in R} r_i^{\lambda_i^R} = (g)^{\sum_{s_i}\lambda_i^R\beta_i \bmod p}$$

$$\delta = \prod_{s_i \in R} \delta_i^{\lambda_i^R} = (h_c)^{\sum_{s_i}\lambda_i^R\alpha_i}(y_i)^{\sum\lambda_i^R\beta_i \bmod p}$$

$$= h_c^{\alpha}(y_i)^{\sum\lambda_i^R\beta_i \bmod p}$$

在每一个服务器 $s_i \in R$ 验证其他服务器公布的证据的过程中,在网络中广播公布不正确证据的服务器. 则要求会话密钥的用户和每个服务器都可以得到一个公布不正确证据的服务器的列表 L.

密钥发送阶段　服务器 $s_i \in R$ 发送密文 $c = (r, \delta)$ 给用户 u_j,它接到后,从所有值中选择一个不属于攻击者结构的服务器的子集所发的值并解密得到所要求的会话密钥.

Proactive 阶段　首先将系统运行时间划分为等长的时间段. 在下列情况下,系统进入 Proactive 阶段.

一是在每个时间段的开始,在这时,由于我们生成的密钥都是在服务器接到用户请求后随机产生的,故只要在时间段的开始对系统重新启动即可达到 Proactive 安全的目的.

二是在用户 u_j 接到会议的会话密钥并解密进行会话后,根据所收到的密文异常的情况和公布不正确证据的服务器的列表情况来确定是否更新会话密钥(比如说,用户发现有一个不属于访问结构的服务器子集发来相同的会话密钥的密文). 当要更新时,用户 u_j 向不属于 L 的服务器的子集发出更改会话密钥的要求. 不属于 L,也即未被攻击者控制的服务器实施更新工作.

秘密更新阶段分更新秘密的产生,被控制服务器的重新启动两个阶段.

(1) 更新秘密产生阶段. 接到用户的请求后,未被攻击者控制的服务器根据前面会话密钥的生成方式(和前面有一点区别是,由于这些服务器未被攻击者控制,故生成密钥的过程不需要验证部分,这使更新密钥的产生比较快捷)得到同一个会议 $c \in C$ 的另一个随机会话密钥的密文,$c' = (r', \delta')$,则用户 u_j 得到新的会话密钥的加密密文为 $c = (rr', \delta\delta')$

(2) 系统重新启动被控制服务器. 在这里,更新的秘密产生的会话密钥只在用户 u_j 要求的一次会话中使用.

4　协议的安全性证明

首先我们分析会话密钥的生成,以便从中抽象出其数学模型,也即会话密钥的生成函数. 由于一个会议的会话密钥为会话密钥 $k_c = h_c^{\alpha}$,而 $\alpha = \sum_{i \in S} k_i$,且 k_i 是从 Z_q^* 中随机选取的故这里可将会话密钥的生成函数看为,$g^{x_1} \cdots\cdots g^{x_n}$

有了会话密钥的生成函数,我们在承认秘密共享方案的安全性的基础上,来讨论分布式密钥分发协议的安全性. 为证明方便,我们建立如下的概率空间.

记 $\Omega = Z_q^* = \{1, 2, \cdots, q-1\}$, $F = \{A : A \subset \Omega\}$,对 $A \subset \Omega$,定义　　$P(A) = \frac{|A|}{q-1}$

则 (Ω, F, p) 为一概率空间.

定义 1[18]　设 (Ω, F, p) 为一概率空间,X 为 F 到 Ω 上的一个变换,则对任意的 $a \in Z_q^*$,都有 $\{w : w \in \Omega, X(w) = a\} \in F$,则称 X 为 Ω 上取值于 Z_q^* 上的随机变量,若对任意的,都有 $P\{X = a\} = 1/(q-1)$,则称 X 服从均匀分布.

由以上定义,显然有,

$$P\{\{k\}\} = 1/(q-1), k \in \Omega = Z_q^*$$

则对 $X(k) = k, k \in \Omega = Z_q^*$,有

$$P\{X = k\} = 1/(q-1), k \in \Omega = Z_q^*$$

定理 1　p, q 是一个大素数,且 $q \mid p-1$. 指数函数 $f(x) = g^x \bmod p, x \in Z_q^*$, g 是乘法子群 Z_q^* 的一个生成元,则 $P\{f(X) = i \bmod p\} = 1/(q-1), i = 1, 2, \cdots, q-1$.

证明　由于 g 是乘法子群 Z_q^* 的一个生成元,故对 $f(x) = g^x = k \bmod p, k \in Z_q^*$,存在 $j \in Z_q^*, x = j$,使 $g^j = k \bmod p, i, k \in Z_q^*$,

故 $P\{f(X) = k\} = P\{X = i\} = 1/(q-1), i, k \in \Omega = Z_q^*$

定理得证.

定理 2　p, q 是一个大素数,且 $q \mid p-1$. 指数函数 $f(x_j) = g^{x_j} \bmod p, x_j \in Z_q^*, j = 1, \cdots, n$, g 是乘法子群 Z_q^* 的一个生成元,则

$$P\{f(X_1), \cdots, f(X_n) = k \bmod p\} = \frac{1}{q-1}, k = 1, 2, \cdots, q-1$$

证明　为了证明的简洁,这里只证明 $n = 2$ 的情况,则用数学归纳法,定理可证.

当 $n = 2$ 时,即证明

$$P\{f(X_1) \cdot f(X_2) = k \bmod p\} = \frac{1}{q-1}, k = 1, 2, \cdots, q-1$$

由于,$P\{f(X_1) \cdot f(X_2) = k \bmod p\} = P\{g^{X_1} g^{X_2} = k \bmod p\}$

$$= P\{g^{X_1 + X_2} = k \bmod p\}$$

而 g 是乘法子群 Z_q^* 的一个生成元,显然,存在 $i \in Z_q^*$ 使 $g^i = k \bmod p$,再利用定理 1 有

$$\text{上式} = P\{X_1 + X_2 = i \bmod p\}, i \in Z_q^*$$

$$= \sum_{j=1}^{q-1} P\{X_1 = j \bmod p\} P\{X_2 + j = i \bmod p\}, i, j \in Z_q^*$$

$$= \sum_{j=1}^{q-1} \frac{1}{(q-1)^2} = \frac{1}{q-1}$$

定理得证.

定理 3　p, q 是一个大素数,且 $q \mid p-1$. 指数函数 $f(x_j) = g^{x_j} \bmod p, x_j \in Z_q^*, j = 1, \cdots, n$, g 是乘法子群 Z_q^* 的一个生成元,则

$$P\{f(X_1), \cdots, f(X_n) = k \bmod p \mid f(X_1) = k_1, \cdots, f(X_b) = k_b\}$$

$$= \frac{1}{q-1}, k_1, \cdots, k_b, k = 1, 2, \cdots, q-1,$$

$$b < n, x \in Z_q^*.$$

证明

$$\begin{aligned} P\{f(X_1), \cdots, f(X_n) = k \bmod p \mid f(X_1) = k_1, \cdots, f(X_b) = k_b\} \\ = P\{k_1 \cdots k_b \cdot f(X_{b+1}), \cdots, f(X_n) \\ = k \bmod p\} = P\{f(X_{b+1}), \cdots, f(X_n) \\ = k_b^{-1}, \cdots, k_1^{-1} k \bmod p\} \end{aligned}$$

由定理 2,上式 = $1/q - 1$.

定理得证.

注:本定理说明,当攻击者知道 b 个服务器对会议 C 的会话密钥的分密钥 $h(c)^{\alpha_1}, \cdots, h(c)^{\alpha_{b1}}$,时,会话密钥的生成函数 $f(x_1) \cdots f(x_n) = k \bmod p = h(c)^{x_1}, \cdots, h(c)^{x_n}$ 还是均匀的.

定理 4 本文的分布式密钥分发系统是安全地抗动态攻击者的随机密钥生成系统,也即动态攻击者 A 不能以大于 $1/q - 1$ 的概率猜出共享秘密 α.

证明 利用前面的结论,证明如下.

首先,由于分布式密钥分发系统具有 Proactive 阶段,因此,保证了被动态攻击者控制的服务器总不属于被授权子集,因此,攻击者无法通过秘密共享本身的方式恢复共享秘密.

其次,当被攻击者控制的服务器(b 个)总不属于被授权子集时,设授权子集包含的最小服务器的个数为 t,则有被攻击者控制的服务器的个数 $b < t < n$,此时,攻击者知道 b 个服务器对会议 C 的会话密钥的分密钥 $h(c)^{\alpha_1}, \cdots, h(c)^{\alpha_{b1}}$,在这种情况下,由定理 3,动态攻击者 A 不能以大于 $1/q - 1$ 的概率猜出共享秘密 x.

5 结束语

在本文的研究中,得到了一个安全地抗动态攻击者的随机密钥分发系统. 特别是抽象出了系统所利用的数学模型,在建立概率空间的基础上,证明了动态攻击者 A 不能以大于 $1/q - 1$ 的概率猜出共享秘密 x. 但更重要的是,我们首次从空间和时间的双重角度来理解分布式密码的分布性,在此基础上,我们将进一步研究通常实现空间分布性的算法和实现时间分布性的算法以及它们之间的相互转换. 这对分布式密码的研究有很重要的理论意义. 另外,分析本文所得的随机密钥分发系统,还有一些工作可做. 比如,若攻击者掌握了任何一个用户的私钥,这个系统就无安全可言,因此,对用户的私钥加入 Proactive 等体制是必要的. 也可以用其他的秘密共享体制来代替文中的向量空间秘密共享体制. 还可以研究是否可用其他公钥体制来代替 ECLME 体制.

参考文献:

[1] Paz Morillo ect. Some Trends for Future Research in Distributed Cryptography[DB/OL]. http://www-mat.upc.es/grup_de_cripto/.

[2] R Ostrovsky, M Yung. How to withstand mobile virus attacks[J]. ACM Symposium on Principles of Distributed Computing, 1991. 51 - 59.

[3] T Rabin, M Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority[A]. Proc 21st Annual Sympo. On the Theory of Computing[C]. ACM, 1989. 73 - 85.

[4] A Herzberg, S Jarecki, H Krawczyk, M Yung. Proactive secret sharing or: how to copy with perpetual leakage[A]. Crypto '95[C]. 1995, 339 - 352.

[5] Y Frankel, P Gemmel, P D MacKenzie, M Yung. Proactive RSA[A]. Crypto '97[C], LNCS 1294. 440 - 452.

[6] T Rabin. A simplified approach to threshold and proactive RSA[A]. Crypto '98[C]. LNCS 1462, 1998. 89 - 104.

[7] D R Stinson, R Wei. Unconditionally Secure Proactive Secret Sharing Scheme with Combinatorial Structures[DB/OL]. http://citeseer.nj.nec.com/198663.html(1999).

[8] Vanesa Daza, Javier Herranz, Carles Padro, German Saez. A Distributed and Computationally Secure Key Distribution Scheme[DB/OL]. http://citeseer.nj.nec.com/daza02distributed.html(2002).

[9] M Naor, B Pinkas, O Reingold. Distributed pseudo-radom functions and KDCs[A]. Advances in Cryptology. Eurocrypt '99[C]. LNCS 1592, Springer-Verlag, 1999. 327 - 346.

[10] T EL Gamal. A public key cryptosystem and a signature scheme based on discrete logariyhems[J]. IEEE Transactions on Information Theory 31. 1985. 469 - 472.

[11] W Diffie, M E Hellman. New directions in cryptography[J]. IEEE Trans. Inform. Theory, IT - 22, 1976. 644 - 654.

[12] A Shamir. How to share secret[J]. Communications of ACM No. 1979, 22: 612 - 613.

[13] Blakley G R. Safeguarding Cryptographic Keys[A]. In: Proceedings of the National Computer Conference[C]. AFIPS, 1997, 48(): 313 - 317.

[14] E F Brickell. Some ideal secret sharing schemes[J]. J Combin Math. And Combin. Comput. 9p. 1989. 105 - 113.

[15] P Feldman. A practical scheme for non-interactive verifiable secret sharing[A]. Proceedings of the 28th IEEE Symposium on the Foundations of Computer Science[C]. IEEE Press, 1987. 427-437.

[16] 李世取,曾本胜,廉玉忠等. 密码学中的逻辑函数[M]. 北京:中软电子出版社,2003. 1.

作者简介:

逯海军 男,1968 年 11 月 28 日出生于甘肃天水,解放军信息工程大学博士研究生,研究方向为密码理论及信息安全技术应用. Email: lhjisme@163.com.