一种基于秘密分享的认证中心私钥保护方案①

张子振，毕殿杰

(安徽财经大学 信息工程学院，蚌埠 233041)

摘 要： 针对 CA 私钥的高安全性需求，提出一种新的(t,n)秘密分享机制保护 CA 私钥。首先，使用 RSA 算法产生 CA 私钥，保证了私钥的不可伪造性；然后基于新的(t,n)秘密共享机制将 CA 私钥进行分存，使用其身份作为私钥份额的标识，并使用私钥作为秘密份额。在使用 CA 私钥进行签名时，使用 Lagrange 插值多项式进行重构，并提供了简单高效的合作者欺骗验证方法；秘密重构中无需真正的秘密份额，因此，无需维护安全通道，提高了效率。理论分析和实验结果表明方案的有效性。

关键词： 秘密分享；认证中心；私钥；安全

Protection for CA Private Key Based on Secret Sharing Scheme

ZHANG Zi-Zhen, BI Dian-Jie

(College of Information Engineering, Anhui University of Finance & Economics, Bengbu 233041, China)

Abstract: For the high-security needs of CA private key, a new (t,n) secret sharing mechanism is proposed. First, the CA private key is generated using the RSA algorithm to ensure its un-Forged; then CA private key is shared based on the new (t,n) secret sharing mechanism. It uses its identification as a share of the private key and the private key as a secret share. It also provides a simple and efficient method to detect partner deceive, there is no real secret share is needed when secret is reconstructed, and without the need to maintain security channel too, so it enhances the efficiency. Applied to CA private key protection, it improves its security.

Keywords: secret sharing; certificate authority; private key; security

目前，数字证书正在电子商务、电子政务等应用中发挥着越来越重要的作用。数字证书是由 CA (Certificate Authority:认证中心)颁发的。从本质讲，数字证书是将公开密钥和身份信息结合在一起，用 CA 的私钥签名后得到的数据。由此可见，数字证书的可信任性取决于 CA 私钥的正确性。如果 CA 的私钥一旦被窃取或者恶意破坏,由该 CA 发的所有证书就只能全部作废。因此，如何保护 CA 私钥的安全性，进而保证所签发证书的有效性一直是一个重要的研究问题。(t,n)秘密分享机制将秘密分成 n 份，分别由 n 个参与者保存，t 个或 t 个以上的参与者使用其拥有的秘密份额可以恢复出秘密，而少于 t 个参与者不能得到有关秘密的任何信息。由于(t,n)共享机制本身提供的安全性，在 CA 私钥保护中得到了广泛应用。在已有的基于(t,n)秘密分享机制的 CA 私钥保护方案中，主要存在以下问题：各参与者的私钥份额值由私钥分发者产生，由于私钥分发者需要保存大量的信息，因而具有单点失效的安全隐患[1,2]；在私钥分发者和各参与者之间需要一条安全的通信信道进行私钥份额的分发，提高了系统的代价和复杂性[3,4]；没有提供参与私钥保护的合作者进行欺骗的解决方案[5]；私钥分发者需要专门的验证算法来验证是否有合作者欺骗，从而增加了系统的复杂度，并影响效率[6]。基于此，本文提出了一个新的(t, n)门限秘密分享算法来保护 CA 私

① 基金项目:安徽省高校自然科学研究基金(KJ2009060Z);安徽财经大学校级科研项目(ACKYQ0947ZC)
收稿时间:2010-05-11;收到修改稿时间:2010-06-02

钥。算法使用参与者的身份作为其私钥份额对应的公开信息，使用私钥作为秘密份额；私钥分发者和各参与者之间无须进行任何信息交换；算法同时提供了简单的合作者欺骗验证方法；在私钥重构过程中，每个合作的参与者只需提交一个由私钥份额计算的伪份额，无需其真实的私钥份额值，有效提高了 CA 私钥的安全性。

1 CA私钥保护方案的具体实现过程

本文提出的 CA 私钥保护方案包括私钥的产生过程、用户密钥产生过程、私钥分发算法、私钥重构算法四个步骤。私钥的产生基于 RSA 生成，过程如下：

1.1 私钥的产生过程

(1) 取两个大素数 p,q ,计算 $N=pq$；

(2) 计算 $\phi(N)=(p-1)(q-1)$；

(3) 找一个与 $\phi(N)$ 互素的指数 e；

(4) 根据 $ed\equiv 1(\phi(N))$ 计算出秘密指数 d

(5) 找一个具有最大乘法阶的公开元素 $g\in z^*$，分别计算模 p 和模 q 的生成元 g_p 和 g_q， g 的计算通过中国剩余定理[7]得出。

(6) CA 公开系统参数 (N,e,g)，并秘密保存 d。

本文中，把 d 作为 CA 的私钥。基于 RSA 的安全性，在已知 N,e,g 的情况下无法求得 d，保证了 CA 私钥的安全性和不可伪造性。

用户(私钥的分发者和持有者)密钥产生过程如下：

1.2 用户密钥数据产生过程

CA 私钥的分发者和私钥份额的持有者(也是后期参与数字签名者)密钥的生成过程如下：

假设参与者 A 要建立自己的密钥系统，则执行以下过程：

(1) A 随机选择一个长度为 128 比特的整数 s_A 作为私钥，计算 $v\leftarrow g^{-s_A}\pmod N$，并把 v 发送给 CA。

(2) A 运用任意一个零知识证明协议[7]向 CA 证明自己知道 s_A 但不会泄漏 s_A，同时向 CA 发送自己的身份 I_A。

(3) CA 创建 A 的公钥 P_A：$P_A\leftarrow(v-I_A)^t\pmod N$

(4) A 的密钥数据记为 (s_A,P_A,I_A)。s_A 为其私钥，P_A 为其公钥签名，I_A 为其身份。

当私钥产生后，对私钥的分发按照以下算法完成：

1.3 CA 私钥分发算法

通过(t,n)秘密共享方案将 CA 私钥进行共享。CA 私钥分发系统包括可信的私钥 CA 分发者 D 和 n 个参与者 P_1，P_2，…，P_n。假设 CA 私钥分发者的密钥数据记为 (s_d,P_d,I_d)，各参与者 P_i 的密钥数据为 (s_i,P_i,I_i)；令 E_k,D_k 分别表示高安全的对称密码算法的加、解密算法(本文采用 3DES 算法)，其中 k 为对称密钥。

算法中，把 CA 私钥记作 d，$d\in z_q$ (q 是一个随机选取的且大于 N 的素数)。CA 私钥分发者执行如下算法：

(1) 从[N1/2, N-1]中随机选取一个整数 r；

(2) 对于每一个参与者 P_i（i=1，2，…，n），私钥分发者执行以下过程：

1) 计算 $K_{d,i}=(P_i^e+I_i)^{s_d}=g^{-s_d s_i}(\bmod N)$；

2) 利用自己计算的 $K_{d,i}$ 作为对称加密密钥对 r 进行加密，即计算 $E_{K_{d,i}}(r)$；

3) 计算 $H_{d,i}=h(E_{K_{d,i}}(r))$。其中，$h(\cdot)$ 是一个单向 hash 函数。

(3) 利用 (n + 1) 个点 $(0,d),(x_1,E_{K_{d,1}}(r)),(x_2,E_{K_{d,2}}(r))....,(x_r,E_{K_{d,n}}(r))$ 和拉格朗日插值方法构造 n 阶多项式 $f(x)$:

$$f(x)=d\times\prod_{k=1}^{n}(x-x_k)/(-x_k)+\sum_{l=1}^{n}$$

$[E_{K_{d,l}}(r)\times(x/x_l)\times\prod_{k=1,k\neq l}^{n}(x-x_k)/(x_l-x_k)]\bmod q$，分别计算 $f(1),f(2),...,f(n-t+1)$；

(4) 将 $H_{d,i}$、$f(i)$ 分发给 p_i.

在使用 CA 私钥之前，需要先进行重构，重构过程如下：

1.4 CA 私钥重构算法

为了重构 CA 密钥，需要至少 t 个参与者合作。考虑一般性，假设 t 个参与者为 P_1，P_2，…，P_t。重构算

法如下：

(1) 每个参与者 Pi 利用自己的私钥计算 $K_{i,d}=(P_d^e+I_d)^{s_i}=g^{-s_d s_i}(\bmod N)$

(2) 每个参与者 Pi 利用自己计算的作为对称加密密钥对 r 进行加密，即计算 $E_{K_{i,d}}(r)$。

(3) 由 $K_{i,d}=K_{d,i}$，有 $E_{K_{i,d}}(r)=E_{K_{d,i}}(r)$。这样就可以得到 t 个点 $(x_1,E_{K_{1,d}}(r))$，$(x_2,E_{K_{1,d}}(r))\cdots$，$(x_t,E_{K_{1,d}}(r))$，同时，得到另外的(n－t＋1)个点 $(1,f(1)),(2,f(2))....(n-t+1,f(n-t+1))$。通过这 (n+1)个点，采用 Lagrange 插值多项式即可重构多项式 f(x)。本文用 $(x_i,y_i)(i=1,2,...,n+1)$ 来表示所得到的(n+1)对数据，使用如下方法重构多项式:

$$f(x)=\sum_{i=1}^{n+1}Y_i\prod_{j=1,j\neq i}^{n+1}\frac{x-X_j}{X_i-X_j}\bmod q$$

(4) 要恢复的分享的 CA 私钥 $d=f(0)$。

2 算法安全性分析与讨论

本算法安全性分析如下：

(1) 本算法符合门限秘密分享机制的门限规则,具有容侵特性。

在本算法中，要恢复出所分享的 CA 私钥,就必须首先重新构造出 n 次 Lagrange 插值多项式 f(x). 由 Lagrange 内插多项式的性质可知，只有 t 个或 t 个以上的参与者合作才可以重构多项式 f(x)，从而恢复私钥 d；而少于(t－1)个的合作者获得私钥 d 的任何信息。在这种情况下,要计算出分享的私钥等价于攻破 Shamir 的门限机制[8],这显然是不可行的。

(2) 本算法能够防止各个参与者之间的相互欺骗。

如果某个参与者 P_i 想进行欺骗，有可能在秘密恢复过程，计算 $E_{K_{i,d}}(r)$ 时进行欺骗。但是，因为信息 $H_{d,i}$ 是公开的，任何参与者均可以通过验证等式 $H_{d,i}=h(E_{K_{i,d}}(r))$ 是否成立来验证其提交的份额 $E_{K_{i,d}}(r)$ 是否有效，从而发现这种欺骗，进而防止了内部参与者之间的相互欺骗。

(3) 本算法能够防止外部攻击者的主动攻击。

系统外的攻击者可以通过设法推导出秘密分发者计算的密钥 $K_{d,i}$，或各参与者 P_i 计算的密钥 $K_{i,d}$ 来进行攻击。如果想攻击成功，攻击者必须能够获取私钥份额分发者或各参与者的私钥。而此问题是是一个离散对数难题[9]，因此，在理论上是不可能实现的。

3 相关算法性能分析

与已有的秘密分享机制相比：(1)本算法可以提供参与者身份验证;(2)使用了改进的签密技术。由于签名时候无需私钥份额本身，所以不需要安全信道。(3)本算法使用参与者的私钥作为私钥份额，可以在秘密分发的同时进行秘密份额的分发,事先无须进行任何处理，效率更高。(4)本算法通过验证 $H_{d,i}=h(E_{K_{i,d}}(r))$ 提供了更简单的合作者欺骗检测机制。相比较而言,本文算法应用到 CA 私钥保护中，提供了更强的 CA 私钥安全保护能力。

4 仿真实验及其结果分析

为了验证算法的有效性，在 windows 平台下，基于 C++开发环境，借助利用 Miracle 库提供的类函数来进行仿真实现[10]。Miracle 是一个功能强大的类库，提供了执行密码协议中所需的大部分基本操作：RSA 公钥密码，Diffie－Hellman 密钥交换等。为了方便计算，算法中参数设置：RSA 参数的设置，p=43,q=59,e=13,故 n=2539,d=937。实际使用时，建议选择 p 和 q 都是 100 位的十进制素数，d 就相当于 1024 位 2 进制数，满足 CA 私钥的实际需求。摘要函数采用 MD5 算法。为了得到较为可信的结果，重复进行 100 次实验，取平均值作为最后的结果。测试对象为单个证书请求的时间。实验结果如表 1 所示和图 1 所示。

表 1　签名请求时间(ms)与(t,n)的关系

性能	t=3	t=(n-1)/2
n=7	398.2	398.2
n=9	400.5	460.3
n=11	397.1	590.5
n=13	395.6	670.4
n=15	398.9	720.3

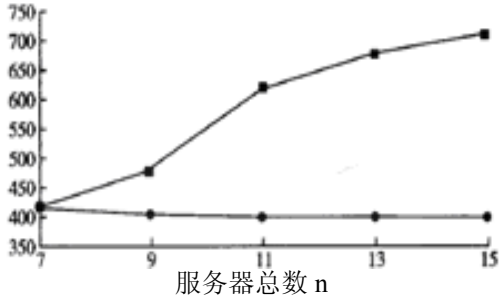

图 1 证书请求时间与(t,n)关系示意图

从表 1 可以看出，(t,n)门限秘密不同的取值对结果有一定的影响。当 t 给定时，n 对证书请求的时间影响不大；当 n 给定，随着 t 的增加，系统请求的时间明显增加。图 1 验证了这一点。因此，必须根据实际需要选择合适的门限密码值。本文从安全性和效率方面考虑，对(t,n) 取 t=3,n=7，得到满意结果。

5 结论

本文提出了一个基于身份的(t, n)门限秘密分享机制，并将其应用到 CA 私钥的保护中。提出的新方法中，参与者的私钥份额不是由私钥分发者决定，而是使用他们的私钥作为秘密份额；由于私钥分发者和各参与者间不需要进行任何交互，因此无需维护一条安全信道，提高了效率；私钥重构过程中，任何参与者可以立即检验每个合作的参与者是否进行了欺骗。理论分析和实验结果表明了本算法的有效性。

参考文献

1 张仕斌.应用密码学.西安:西安电子科技大学出版社,2009. 15－20.

2 蔡永泉,杜秋玲.一种 CA 私钥安全管理方案.电子学报, 2005,33(8):1407－1410.

3 费如纯,王丽娜.基于RSA和单向函数防欺诈的秘密共享体制.软件学报,2003,14(1):146－150.

4 Li HX, Pang LJ, Cai WD. An efficient threshold multi -group-secret sharing scheme. Advances in Soft Computing, ICFIE'07, Springer-Verlag. ASC 40, 2007. 911－918.

5 Pang LJ, Wang YM. A new (t,n) multi-secret sharing scheme based on Shamir's secret sharing. Applied Mathematics and Computation, 2005,167(2):840－848.

6 白浩,张浩军.一种 CA 私钥容侵保护机制.计算机应用, 2008,28(4):910－913.

7 Hwang RJ, Lai CH, Su FF. An efficient signcryption scheme with forward secrecy based on elliptic curve. Applied Mathematics and Computation, 2005,167(1):870－881.

8 Pang LJ, Wang YM. A New (t,n) Multi-secret Sharing Scheme based on Shamir's Secret Sharing. Applied Mathematics and Computation, 2005,167(2):840－848.

9 于小佳,郝蓉.先动的可公开验证服务器辅助秘密 CA 私钥. 北京邮电大学学报, 2008,26(10):325－328.

10 甘仁驹,谢仕义.对安全有效的(t,n)多秘密 CA 私钥认证方案的改进.电子与信息学报,2009,26(12):31－35.