两类强壮的门限密钥托管方案*

曹珍富+

(上海交通大学 计算机科学与技术系,上海 200030)

Two Classes of Robust Threshold Key Escrow Schemes

CAO Zhen-Fu+

(Department of Computer Science and Technology, Shanghai Jiaotong University, Shanghai 200030, China)

+Corresponding author: Phn: 86-21-62835602, Fax: 86-21-62932902, E-mail: zfcao@cs.sjtu.edu.cn

http://www.cs.sjtu.edu.cn

Received 2002-05-13; Accepted 2002-08-14

Cao ZF. Two classes of robust threshold key escrow schemes. *Journal of Software*, 2003,14(6):1164~1171.
http://www.jos.org.cn/1000-9825/14/1164.htm

Abstract: The definition of robust threshold key escrow scheme (RTKES) is proposed in this paper. Namely, in RTKES, malice escrow agency fail to obtain the system secret key or user's secret key, even if the number of malice escrow agency is more than or equal to the value of threshold. Clearly, the problem of "user's secret key completely depends on the trusted escrow agency" is solved if RTKES exists. In this paper, it is proved that the RTKES does exist, and some concrete designs of two classes of RTKES are given. In these schemes, the problem of "once monitor, monitor for ever" is solved effectively, every escrow agency can verify correctness of the secret shadow that he escrows during secret shadow distribution and monitor agency can exactly decide which escrow agency forges or tampers secret shadow during monitor procedure. Since the proposed RTKES is also threshold key escrow scheme, when an escrow agency or few agencies is not cooperating, monitor agency can easily reconstruct session key to monitor as long as there are other k effective escrow agencies. In addition, it also resists against LEAF feedback attack.

Key words: key escrow; threshold scheme; robustness; improved RSA cryptosystem; ElGamal cryptosystem; escrow agent; monitor

摘 要: 提出了门限密钥托管方案强壮性的概念,即对于一个强壮的门限密钥托管方案(robust threshold key escrow scheme,简称 RTKES),即使在恶意托管人数大于或等于门限值时仍然无法获取系统密钥或用户密钥.很明显,RTKES解决了"用户的密钥完全依赖于可信赖的托管机构"这一问题.证明了RTKES是存在的,并且还给出

* Supported by the National Natural Science Foundation of China under Grant No.60072018 (国家自然科学基金); the National Natural Science Foundation of China for Distinguished Young Scholars under Grant No.60225007 (国家杰出青年科学基金); the National Research Foundation for the Doctoral Program of Higher Education of China under Grant No.20020248024 (国家教育部高等学校博士点基金)

第一作者简介: **曹珍富**(1962－),男,江苏盐城人,博士,教授,博士生导师,主要研究领域为数论和现代密码学,信息安全理论与技术.

两类 RTKES 的具体设计.这些方案有效地解决了“一次监听,永久监听”的问题,每个托管人能够验证他所托管的子密钥的正确性,并且在监听阶段,监听机构能够确切地知道哪些托管人伪造或篡改了子密钥.由于提出的方案是门限密钥托管方案,所以在所有托管人中当有一个或几个托管人不愿合作或无法合作时,监听机构仍能够通过另外有效的 k 个托管人去重构会话密钥,从而实施监听.此外,RTKES 还具有抵抗 LEAF 反馈攻击的特性.

关键词: 密钥托管;门限方案;强壮性;改进的 RSA 体制;ElGamal 体制;托管代理,监听

中图法分类号: TP309 **文献标识码**: A

计算机密码学保证了人们利用公共网络能够获得可靠的保密消息,但同时也给犯罪分子进行犯罪活动提供了条件.如何在用户的隐私权与法律授权下政府机构的监听权之间寻找出一种折衷方法是近年来密码学界的热点课题之一.一方面,为了保护用户的隐私权,密码强度不应减弱;另一方面,为了打击犯罪分子的非法活动,法律授权下政府机构的监听权也应得到保证.1993 年 4 月,美国政府宣布的托管加密标准(escrowed encryption standard,简称 EES)[1]是最早的托管方案,它允许政府执法机构在得到诸如法庭传票这一类有效的授权后实施对用户的监听.密钥托管方案一经提出就受到了普遍的关注.但是关于如何平衡个人安全通信和执法机构监听这一问题仍存在很多争议.为了解决这一问题,国内外许多学者对密钥托管方案进行了深入的探讨.1995 年,Shamir[2]提出了部分密钥托管思想,A.K.Lenstra 等人[3]提出时间约束下的托管加密方案,Micali[4,5]提出了公正密钥托管方案和共享伪随机函数密钥托管方案.但这些工作都没有很好地解决有关的争议问题.

后来,文献[6~8]提出了门限密钥托管的概念.这是很自然的事情,利用门限方案可以在用户的隐私权与法律授权下政府机构的监听权之间找到一种折衷方法,即使用这种方案,当监听机构需要监听时,需要找到 k 个托管人才可实施监听.门限密码算法首先是 Y.Desmedt 和 Y.Frankel[9,10],A.D.Santis,Y.Desmedt,Y.Frankel 和 M.Yung[11] 以及 R.Gennaro,S.Jarecki,H.Krawczyk 和 T.Rabin[12]进行研究的,他们分别考虑了门限 ElGamal 密码算法和门限 RSA 密码算法.值得注意的是,简单地使用门限方案于密码算法是不正确的.例如,在门限 RSA 方案中,简单地将 RSA 的私钥 d 使用门限方案是不合适的.因为负责解密的机构(或签名机构)第一次使用 k 个人的子密钥恢复私钥后,今后解密(或签名)时就不需要再通过 k 个人来恢复消息(或签名)了.我们认为,真正的门限密码方案应该做到:每个人对密文(或消息)使用自己的子密钥“解密(或签名)”得到“子消息(或子签名)”,负责解密的机构(或签名机构)每次使用 k 个子消息(或子签名)可获得整个消息(或签名),而已知任何少于 k 个的子消息(或子签名)均不能获得整个消息(或签名)的任何信息.并且已知子消息(或子签名)不能获得密钥和子密钥的任何信息.正因为如此,我们发现,文献[6~8]提出的门限密钥托管方案都不是真正的门限方案,即这些方案中都是第一次需要 k 个人来恢复加密会话密钥的系统密钥,然后进行监听.这样,一旦监听机构监听了一个用户,它就可以监听所有用户以后的通信,即达到所谓的“一次监听,永久监听”的目的.

最近,我们分别利用改进的 RSA 和 ElGamal 体制提出了两种门限密钥托管方案[13,14],这是真正的(k,n)门限密钥托管方案,解决了“一次监听,永久监听”的问题.同时,也较好地解决了“用户的密钥完全依赖于可信赖的托管机构”这一问题.但是,由于没有考虑(k,n)门限密钥托管方案的强壮性,所以 k 个或 k 个以上托管人联合可以恢复用户的密钥.所谓门限密钥托管方案的强壮性是指,当恶意托管人数大于或等于门限值时仍然无法获取用户的密钥.很明显,一个强壮的门限密钥托管方案完全解决了“用户的密钥完全依赖于可信赖的托管机构”这一问题.有关门限密码算法的强壮性研究已成为现代密码学的重要课题之一[15~18].

本文提出了具有强壮性门限托管方案的两种模式,其中,第 1 种模式是监听机构与托管密钥、托管机构没有任何关联;第 2 种模式是监听机构与托管密钥、托管机构有某种固定的关联.按照这两种模式,本文提出了两类具有强壮性的门限密钥托管方案,它们是我们以往两个门限密钥托管方案的修改.这些方案不仅有效地解决了“用户的密钥完全依赖于可信赖的托管机构”问题,还与我们在文献[13,14]中提出的方案一样,解决了“一次监听,永久监听”的问题,而且简化了每个托管人验证他所托管的子密钥的正确性的过程,并且在监听阶段,监听机构能够确切地知道门限密钥托管方案中哪些托管人伪造或篡改了子密钥.我们提出的方案与已有的门限密钥托管方案一样,还具有其他一些优点,例如当在各托管人中有一个或几个不愿合作或无法合作时,监听机构仍能很容易地重构出会话密钥.此外,还具有抵抗 LEAF 反馈攻击的特性等.

1 具有强壮性门限托管方案的两种模式

1.1 模式1(监听机构与托管密钥、托管机构没有任何关联)

(A) 方案设计:在我们的门限密钥托管方案中,有一个密钥管理中心(key management center,简称 KMC),负责密钥的分发与管理;有一个密钥托管机构,负责用户密钥的托管;还有一个监听机构以及若干个用户等.使用 3 个密码算法:$E_1(x,k)$,$E_2(x,e)$,$S(x)$,其中 $E_1(x,k)$是一个标准的分组加密算法,用于用户间的秘密通话;$E_2(x,e)$是一个公钥加密算法;$S(x)$是一个签名算法,用于法律实施访问域(law enforcement access field,简称 LEAF).对 $E_2(x,e)$的私钥 d 使用"影子"变换得到 d',然后将影子 d'使用(k,n)门限方案得到 n 个"碎片"的集合$\{x_1,x_2,\ldots,x_n\}$.KMC 秘密地将"影子"变换的秘密(逆变换)发送给用户 A 作为他的秘密钥,而将 $x_1,x_2,\ldots,x_n$ 秘密地发送给托管机构的 n 个托管人.这里的(k,n)门限方案可以采用任意一个已有的门限方案[19],只要满足:对每个 x,设 $E_2'(x,e)$ 是用户 A 用他的秘密钥(即"影子"逆变换)对 $E_2(x,e)$的变换,那么只要任意知道 k 个 $x_{i_l}\in\{x_1,\ldots,x_n\}, l=1,2,\ldots,k$ 对 $E_2'(x,e)$ 的变换 $E_3(E_2'(x,e),x_{i_l}), l=1,2,\ldots,k$,监听机构即可恢复 x(注意:不是恢复 d'),而已知任意少于 k 个 $E_3(E_2'(x,e),x_{i_l})$ $l=1,2,\ldots,k-1$,均不能获得 x 的任何信息,其中 E_3 是一个单向加密函数.同时,KMC 公布一组参数使每个托管人 T_i 可以利用一个验证方程验证他所托管的内容是否有效.

(B) 用户间的通信.设用户 A 欲向用户 B 发送消息 M,$sk(<N)$是会话密钥(由用户事先协商).又设 H 是一公开的 hash 函数.

A 向 B 发送$\{E_1(M,sk),\text{LEAF}\}$,其中 LEAF=$\{E_2'(sk,e),S(H(M)),\text{A的证书}\}$.这里,$e$ 是 E_2 的公钥(加密密钥),由系统公开,$E_2'(sk,e)$ 是用户 A 用他的秘密钥对 $E_2(x,e)$的变换;A 的证书可取作由权威机构签署的 A 的签名公钥,用户 B 可由 A 的证书取出 A 的签名公钥. $S(H(M))$ 为 A 用其签名私钥对 $H(M)$ 的签名.

B 在恢复出消息 M 之后,再求 $H(M)$. 若求得的 $H(M)$ 满足签名方程,即与从 A 收到的 $S(H(M))$ 中的 $H(M)$ 一致,B 就可以确认所收到的 M 是有效的.

(C) 监听过程.监听机构首先获取法院许可监听用户 A,B 间通信的许可证书,并将证书分别出示给任意 k 个托管人 T_{i_j} $(1\le i_1<i_2<\ldots<i_k\le n)$,托管人 T_{i_j} 在验证了法院的证书之后,利用 $x_{i_l}(l=1,2,\ldots,k)$ 计算出 k 个子会话密钥 $sk_{i_l}=E_3(E_2'(sk,e),x_{i_l})(l=1,2,\ldots,k)$,并将其分别独立地交与监听机构.监听机构由 k 个子会话密钥求出会话密钥 sk.因而可解出消息 M,并且与用户 B 一样,可验证所监听到的消息的有效性.

1.2 模式2(监听机构与托管密钥、托管机构有某种固定的关联)

在模式 1 中,将"KMC 秘密地将'影子'变换的秘密(逆变换)发送给用户 A 作为他的秘密钥"修改为"KMC 秘密地将'影子'变换的秘密(逆变换)发送给监听机构",并且将所有 E_2' 仍换成 E_2.在监听时,监听机构只要任意知道 k 个 $x_{i_l}\in\{x_1,\ldots,x_n\}(l=1,2,\ldots,k)$ 对 $E_2(x,e)$的变换 $E_3(E_2(x,e),x_{i_l})(l=1,2,\ldots,k)$,即可利用自己掌握的"影子"变换的逆变换来恢复 x.

这种模式与文献[13,14]相比,增加了对 $E_2(x,e)$的私钥 d 使用"影子"变换得到 d',同时将"影子"变换的逆变换交给监听机构管理.

1.3 两种模式的特点

在我们设计的方案模式中,e 是 E_2 的公钥(加密密钥),由系统公开;E_2 的私钥 d 是系统密钥.我们的模式 1 是对 d 使用"影子"变换得到 d',KMC 秘密地将"影子"变换的秘密(逆变换)发送给用户 A 作为他的秘密钥;模式 2 是对 d 使用"影子"变换得到 d',KMC 秘密地将"影子"变换的秘密(逆变换)发送给监听机构,由监听机构在监听时使用.

在上述两种模式中,监听机构每次监听时都必须通过 k 个托管人恢复会话密钥,监听机构对公钥密码算法 E_2 的解密密钥(系统密钥)、用户密钥和每个托管人管理的数据一无所知.同时,k 个或大于 k 个托管人联合恢复 E_2 的解密密钥或用户密钥是不可能的,这是因为根据设计,k 个或大于 k 个的托管人联合只能恢复影子 d'的替代物.因此,这种模式具有强壮性.

与文献[13]相同,上述方案显然也能抵抗每个用户的"LEAF 反馈"(LEAF feedback)攻击.在下面两节里,我们将给出两类具有强壮性的门限密钥托管方案,它们分别是基于大整数问题和离散对数问题的,并且不失一般性,

我们的第 1 种方案用模式 1 实现,第 2 种方案用模式 2 实现.

2 具有强壮性的门限密钥托管方案 I——基于大整数的方案

在这一节中,我们利用改进的 RSA 公钥密码算法(其安全性等价于大整数分解)[13]给出具有强壮性门限密钥托管方案(模式 1)的一个具体实现.

2.1 改进的RSA体制介绍[13]

随机地选两个大素数 p,q, 满足 $p\equiv q\equiv 3(\mathrm{mod}\,4)$ (可以选 p,q 均为安全素数), 令 $N=pq$, 则 $\varphi(N)=(p-1)(q-1)$.选取 b 满足 Jacobi 符号: $\left(\frac{b}{N}\right)=-1$.再选取 $e\in\mathbb{Z}$ 满足 $\gcd(e,\frac{1}{2}\varphi(N))=1, 1<e<\frac{1}{2}\varphi(N)$,计算出 $d\in\mathbb{Z}$ 满足 $ed\equiv\frac{1}{2}(\frac{1}{4}\varphi(N)+1)(\mathrm{mod}\frac{1}{2}\varphi(N))$, $1<d<\frac{1}{2}\varphi(N)$.于是公开:b,e,N 作为加密密钥,而秘密钥为 d.

加密算法.

设明文 $x\in\mathbb{Z}_N$, 不妨设 $\gcd(x, N)=1$, 则可以很容易地计算

$$E(x)=\begin{cases}x^{2e}(\mathrm{mod}\,N), & \text{如果}\left(\frac{x}{N}\right)=1\\ (bx)^{2e}(\mathrm{mod}\,N), & \text{如果}\left(\frac{x}{N}\right)=-1\end{cases},\quad c_1=\begin{cases}0, & 2\mid x\\ 1, & 2\nmid x\end{cases},\quad c_2=\begin{cases}0, & \left(\frac{x}{N}\right)=1\\ 1, & \left(\frac{x}{N}\right)=-1\end{cases}.$$

密文为 $(E(x),c_1,c_2)$.

解密算法.

(A) 若 c_2=0,则有 $x^{2e}\equiv E(x)(\mathrm{mod}\,N)$,计算 $E(x)^d\equiv x^{2ed}\equiv x^{1+\frac{1}{4}\varphi(N)}\equiv\pm x(\mathrm{mod}\,N)$,再由标识位 c_1 可知 x 的奇偶性,即可确定明文 x.

(B) 若 c_2=1,则有 $(bx)^{2e}\equiv E(x)(\mathrm{mod}\,N)$,计算 $(E(x))^d\equiv(bx)^{2ed}\equiv(bx)^{1+\frac{1}{4}\varphi(N)}\equiv\pm bx(\mathrm{mod}\,N)$,即

$$x\equiv\pm b^{-1}(E(x))^d\,(\mathrm{mod}\,N),$$

再由标识位 c_1 可确定明文 x.

2.2 基于改进的RSA体制的强壮门限密钥托管方案

(A) 密钥分发阶段

KMC 利用第 2.1 节的方法计算改进的 RSA 公钥密码系统参数 p,q,N,b,e,d,这里, $p\equiv q\equiv 3(\mathrm{mod}\,4)$ (例如 p,q 均是安全素数),e,d 分别是系统的加密、解密密钥,N=pq.选取 d_1, $\gcd(d_1,\frac{1}{2}\varphi(N))=1$,使得 $d_1d\equiv d_2(\mathrm{mod}\frac{1}{2}\varphi(N))$, $1<d_1<\frac{1}{2}\varphi(N)$, $1<d_2<\frac{1}{4}\varphi(N)$,且 $d_1\neq d_2$ .d_2 称为系统密钥 d 的"影子".随机选取 k–1 次多项式 $f(x)\in\mathbb{Z}_{\varphi(N)/4}[x]$,使得 d_2=f(0),同时随机选取互异元素 $x_1,x_2,\ldots,x_n\in\mathbb{Z}_{\varphi(N)/4}$,使得

$$\gcd(x_i-x_j,\frac{1}{4}\varphi(N))=1(i\neq j).\tag{1}$$

当 p,q 取安全素数时,这是很容易做到的.记 $f(x)=d_2+c_1x+\ldots+c_{k-1}x^{k-1}$,在 $\mathbb{Z}_{\varphi(N)/4}$ 中计算 $y_i=f(x_i)$,i=1,2,…,n,其中任意知道 k 个 $y_{i_l}(l=1,2,\ldots,k)$, 利用插值公式可得[20]:

$$d_2\equiv f(0)\equiv\sum_{1\le l\le k}y_{i_l}\prod_{\substack{1\le w\le k\\ w\neq l}}(-x_{i_w})(x_{i_l}-x_{i_w})^{-1}(\mathrm{mod}\frac{1}{4}\varphi(N)).\tag{2}$$

由式(1)可知, $(x_{i_l}-x_{i_w})^{-1}(\mathrm{mod}\frac{1}{4}\varphi(N))$ 是存在的,即式(2)是可计算的.

KMC 在初始阶段为用户选择以下公开参数:$N,e,b,(i,x_i)$(i=1,2,…,n),同时计算

$$z_i \equiv y_i a^{-1} (\mathrm{mod} \frac{1}{4}\varphi(N)),\ i=1,2,\ldots,n, \tag{3}$$

这里, $a=\prod_{1\le j<i\le n}(x_i-x_j)$, a^{-1} 满足 $aa^{-1}\equiv 1(\mathrm{mod}\frac{1}{4}\varphi(N))$, $a^{-1}(\mathrm{mod}\frac{1}{4}\varphi(N))$ 的存在性由式(1)保证.KMC 将(i,z_i), i=1,2,…,n,通过安全信道秘密发送给托管机构的 n 个托管人 $T_i(i=1,2,\ldots,n)$,并将 $d_1^{-1}(\mathrm{mod}\frac{1}{2}\varphi(N))$ 秘密发送给需要托管的用户 A,作为 A 的秘密钥.

(B) 托管子密钥认证

为了让每个托管人都能验证自己掌管子密钥的有效性,KMC 选取 $g\in\mathbb{Z}_N$ 使得 g 是 mod N 阶为 $\frac{1}{4}\varphi(N)$ 的元.定义单向函数 $h(x)=g^x \bmod N$,计算 $h(d_2)$和 $h(c_i)(i=1,\ldots,k-1)$,并公开供托管人验证自己子密钥的有效性.

任一托管人 T_i 可用 KMC 公布的 $x_i(i=1,2,\ldots,n)$ 计算 $a=\prod_{1\le j<i\le n}(x_i-x_j)$,然后利用自己的子密钥$(i,z_i)$验证

$$h(d_2)\prod_{l=1}^{k-1}h(c_l)^{x_i^l}\equiv g^{az_i}\ (\mathrm{mod}\ N) \tag{4}$$

是否成立?若式(4)成立,则 T_i 认为他所托管的内容是有效的,这是因为由式(3)可知 $g^{az_i}\equiv g^{y_i}(\mathrm{mod}\ N)$,所以

$$h(d_2)\prod_{l=1}^{k-1}h(c_l)^{x_i^l}\equiv g^{d_2+\sum_{l=1}^{k-1}c_l x_i^l}\equiv g^{f(x_i)}\equiv g^{y_i}\equiv g^{az_i}(\mathrm{mod}\ N),$$

即式(4)成立.否则,T_i 认为他所托管的内容是无效的.

2.3 用户间的通信及监听

用户间的通信与文献[13]类似.设用户 A 欲向用户 B 发送消息 M,sk(<N)是会话密钥(由用户事先协商),又设 H 是一公开的 hash 函数.

A 向 B 发送$\{E_1(M,sk),\mathrm{LEAF}\}$,其中 LEAF=$\{(E_2(sk,e)^{d_1^{-1}} \bmod N, c_1, c_2), S(H(M)), \text{A 的证书}\}$,$E_1$ 是任一个标准的分组加密算法(比如 AES,IDEA),E_2 是改进的 RSA 加密算法,即

$$E_2(sk,e)=\begin{cases}(sk)^{2e}(\mathrm{mod}\ N), & \text{如果}\left(\frac{sk}{N}\right)=1\\ (b(sk))^{2e}(\mathrm{mod}\ N), & \text{如果}\left(\frac{sk}{N}\right)=-1\end{cases},\ c_1=\begin{cases}0, & 2\mid x\\ 1, & 2\nmid x\end{cases},\quad c_2=\begin{cases}0, & \left(\frac{sk}{N}\right)=1\\ 1, & \left(\frac{sk}{N}\right)=-1\end{cases}.$$

A 的证书可取作由权威机构签署的 A 的签名公钥,用户 B 可由 A 的证书取出 A 的签名公钥. $S(H(M))$ 为 A 用其签名私钥对 $H(M)$ 的签名.

B 在恢复出消息 M 之后,再求 $H(M)$. 若求得的 $H(M)$ 满足签名方程,即与从 A 收到的 $S(H(M))$ 中的 $H(M)$ 一致,B 就可以确认所收到的 M 是有效的.

监听过程.监听机构首先获取法院许可监听用户 A,B 间通信的许可证书,并将证书分别出示给托管机构的任意 k 个托管人 T_{i_j} $(1\le i_1<i_2<\ldots<i_k\le n)$,托管人 T_{i_j} 在验证了法院的证书之后,计算

$$E_3(E_2(sk,e)^{d_1^{-1}} \bmod N, z_{i_j})\equiv E_2(sk,e)^{d_1^{-1}z_{i_j}}\equiv E_2'(sk,e)^{2ed_1^{-1}z_{i_j}}(\mathrm{mod}\ N), \tag{5}$$

这里, $E_2'(sk,e)=sk$ (如果 c_2=0)或 $b(sk)$ (如果 c_2=0),并将 $E_3(E_2(sk,e)^{d_1^{-1}} \bmod N, z_{i_j})$ 交给监听机构.

监听机构用 KMC 公布的 x_{i_j} 和 N,计算出 a'' 和 $b_l(l=1,2,\ldots,k)$:

$$a'=\prod_{\substack{1\le l,w\le k\\ l>w}}(x_{i_l}-x_{i_w}),\quad a''=\frac{a}{a'},\quad b_l=\frac{a'}{\prod_{\substack{1\le w\le k\\ w\ne l}}(x_{i_l}-x_{i_w})}\prod_{\substack{1\le w\le k\\ w\ne l}}(-x_{i_w}). \tag{6}$$

因此,利用式(5)和式(6)可以计算出:

$$(\prod_{1\le l\le k}(E_3(E_2(sk,e)^{d_1^{-1}} \bmod N, z_{i_l}))^{b_l})^{a''} \equiv E_2'(sk,e)^{2ed_1^{-1}\sum_{1\le l\le k} a''b_l z_{i_l}} \equiv E_2'(sk,e)^{2ed_1^{-1}d_2}$$

$$\equiv E_2'(sk,e)^{2ed} \equiv E_2'(sk,e)^{1+\frac{1}{4}\varphi(N)} \equiv \pm E_2'(sk,e)(\bmod N),$$

由此,并由 c_1, c_2 的值即可求出 sk,即监听机构获得了 A 与 B 的会话密钥 sk,故由 sk 可解出消息 M.

2.4 本方案具有强壮性

本方案与文献[13]一样具有相应的安全性结论,这里从略.我们需要指出的是,本方案还具有强壮性.这样,用户的密钥就完全不依赖于托管机构了.

假设至少 k 个托管人联合起来攻击系统或用户密钥.直接攻击显然是徒劳的,即从式(2)和式(3)由恢复 $d_2(\bmod\frac{1}{4}\varphi(N))$ 来获得 d,因为 $\frac{1}{4}\varphi(N)$ 未知,所以无法获得 d.在已知 k 个托管人的子密钥 $z_{i_1},...,z_{i_k}$ 时,首先由式(6)可以算出 a'' 和 $b_l(l=1, 2,\ldots,k)$,然后 k 个托管人通过计算 $a''(b_1z_{i_1}+...+b_kz_{i_k})$ 就可以得出一个能够代替 $d_2(\bmod\frac{1}{4}\varphi(N))$ 的数,这是因为

$$a''(b_1z_{i_1}+...+b_kz_{i_k}) = a''\sum_{1\le l\le k} z_{i_l}\frac{a'}{\prod_{\substack{1\le w\le k\\ w\ne l}}(x_{i_l}-x_{i_w})}\prod_{\substack{1\le w\le k\\ w\ne l}}(-x_{i_w}) \equiv a^{-1}a'a''d_2 \equiv d_2(\bmod\frac{1}{4}\varphi(N)).$$

但在不知道 $\frac{1}{4}\varphi(N)$ 和 d_1 时,即使已知 d_2,也不能求出 d.因为从 $d_1d\equiv d_2(\bmod\frac{1}{2}\varphi(N))$ 和 $ed\equiv\frac{1}{2}(\frac{1}{4}\varphi(N)+1)(\bmod\frac{1}{2}\varphi(N))$ 我们只能得出 $d_1(\bmod\frac{1}{4}\varphi(N))$,由此无法得到 $d_1^{-1}(\bmod\frac{1}{2}\varphi(N))$(事实上,这等同于在 RSA 体制中,由 e 和 $ed\equiv 1(\bmod\varphi(N))$ 无法得到 $d(\bmod\varphi(N))$ 一样[21]).由此可以断言:大于或等于 k 个托管人联合起来攻击系统密钥或用户密钥是不可能的.

注 1:本方案与文献[13]提出的方案相比,用户间的通信模块基本是相同的,其他模块都增加了新的内容,特别是托管子密钥认证模块是全新的,这样修改主要是为了提高托管人在进行子密钥认证时的效率,并且使得我们的方案具有强壮性.

注 2:我们也可以这样来修改文献[13]中的方案:密钥管理中心将$(i,x_i)(i=1,2,\ldots,n)$秘密发送给监听机构(而不是公开出去).这样,只要修改原来的子密钥认证模块,使得在不知道$(i,x_i)(i=1,2,\ldots,n)$时同样可以认证子密钥的有效性,就可以获得一个新型的方案.

3 具有强壮性的门限密钥托管方案 II——基于离散对数的方案

本节我们给出一个基于 ElGamal 体制的强壮门限密钥托管方案(模式 2),这是我们最近一项工作[14]的进一步完善.

3.1 系统描述

在本节所讨论的密钥托管方案中,假设用户间采用标准的分组加密算法(比如 3DES,IDEA 等)来加密消息 M,且其中使用的会话密钥 sk 由用户 A,B 事先协商.$\mathrm{LEAF}=\{E_2(sk,y),\mathrm{Time},S(H(M,\mathrm{Time})),\text{A 的证书}\}$,$E_2$ 是 ElGamal 加密算法.托管系统中有一个密钥管理中心(KMC)负责颁发通信用户的公钥证书;有一个托管机构,其中有 n 个托管人 $\{T_1,...,T_n\}$,负责托管加密会话密钥的"影子";有一个监听机构负责实施用户通信的监听.在监听机构和托管人之间建有安全信道.

在描述本文的托管方案之前,先简单介绍一下 ElGamal 体制[22].

ElGamal 体制的安全性基于有限域上求解离散对数的困难性.设 p 是一个大素数,通常要求 $p-1$ 含有大素数因子,这样才能保证计算 $\mathbf{F}_p$ 上的离散对数的困难性,g 是有限域 $\mathbf{F}_p$ 上的一个本原元.用户 A 任选一随机数 $c\in\mathbf{F}_p$,并计算 $y\equiv g^c(\bmod p)$, 该用户以 c 作为他的秘密钥,以 (p,g,y) 作为他的公开钥.任一用户要加密信息 M 给用户 A,只需随机任意选取一整数 $t\in\mathbf{F}_p$,以适合 $\gcd(t,p-1)=1$,计算 $y_1\equiv g^t(\bmod p)$, $y_2\equiv M*y^t(\bmod p)$, 并将 (y_1,y_2)

传送给 A.用户 A 收到 (y_1, y_2) 后,由 $M \equiv y_2 * (y_1^c)^{-1} (\mathrm{mod}\ p)$ 还原出明文 M.

用户对一消息 M 的签名为 $S(M) = (a, b)$, 其中 $a \equiv g^t (\mathrm{mod}\ p)$,b 满足 $M \equiv ca + tb (\mathrm{mod}\ p-1)$. 接收者验证 $y^a y_1^b \equiv g^M (\mathrm{mod}\ p)$ 是否成立,若成立,则认为签名有效.

3.2 基于ElGamal体制的强壮门限密钥托管方案

(A) 密钥分发阶段

首先由 KMC 选取大素数 p,q 满足 $q|p-1$,选取 $\mathbf{F}_p$ 的一个 q 阶元 g,KMC 公开(p,q)作为系统参数.

设 d 为系统或用户的秘密钥,令 $d_1 d \equiv d_2 (\mathrm{mod}\ q)$,这里, $d_1 \in \mathbf{F}_q$, $\gcd(d_1, q) = 1$ .KMC 随机选取 $\mathbf{F}_q$ 上一个 $t-1$ 次多项式 $f(x) = \sum_{i=1}^{t-1} a_i x^i + d_2 \in \mathbf{F}_q[x]$,其中 $\gcd(a_{t-1}, q) = 1$ .KMC 随机选取互异元素 $x_1, ..., x_n \in \mathbf{F}_q$,计算 $b_i \equiv f(x_i) (\mathrm{mod}\ q)$, $y_i \equiv g^{b_i} \equiv g^{f(x_i)} (\mathrm{mod}\ p)$ $(i = 1, ..., n)$,公开 $(x_i, y_i)(i = 1, ..., n)$.

然后计算 $y \equiv g^{d_2} (\mathrm{mod}\ p)$,并公开 y 为 E_2 的加密密钥.把 b_i ,i=1,…,n 通过安全信道秘密地传送给托管人 T_i $(i = 1, ..., n)$ 严格保管.每个托管人验证 $y_i \equiv g^{b_i} (\mathrm{mod}\ p)$ 是否成立,若成立,则认为他托管的内容是有效的;否则,托管的内容无效.KMC 将 $d_1^{-1} (\mathrm{mod}\ q)$ 秘密发送给监听机构.

(B) 用户间的通信[14]

设用户 A 欲向用户 B 发送消息 M,sk 是本次通信的会话密钥,由 A,B 事先协商.Time 是时戳,H 是一公开的 hash 函数.A 向 B 发送 $\{E_1(M, sk), \mathrm{LEAF}\}$,其中 $\mathrm{LEAF} = \{E_2(sk, y), \mathrm{Time}, S(H(M, \mathrm{Time})), \text{A 的证书}\}$,$E_1$ 是一个标准的加密算法(比如 3DES,IDEA 等),E_2 是 ElGamal 加密算法,即 $E_2(sk, y) = (u, v) = (g^k, y^k * sk)$ (运算在 $\mathbf{F}_p$ 上), $k \in \mathbf{F}_q$ 满足 $\gcd(k, q) = 1$,是用户 A 产生的随机数,A 的证书由 KMC 颁发,用户 B 由 A 的证书取出 A 的签名公钥,$S(H(M,\mathrm{Time}))$为 A 用其签名私钥对 $H(M,\mathrm{Time})$的签名.

用户 B 接收到用户 A 发送的 $\{E_1(M, sk), \mathrm{LEAF}\}$ 后,由事先协商好的 sk 恢复出消息 M,然后求 $H(M,\mathrm{Time})$.若求得的 $H(M,\mathrm{Time})$满足签名方程,即与收到的 $S(H(M,\mathrm{Time}))$中的 $H(M,\mathrm{Time})$一致,B 就可以确认所收到的 M 是有效的.

(C) 监听过程

监听机构首先获取监听用户 A,B 间通信的许可证书,并将证书分别出示给任意 t 个托管人,不妨设为 T_i $(i = 1, ..., t)$. 托管人 T_i 验证了法院的许可证书之后,将 $Q_i \equiv u^{b_i} (\mathrm{mod}\ p)$ 通过安全信道交给监听机构,监听机构通过以下 3 步验证托管人 T_i $(i = 1, ..., t)$ 所托管的 b_i 及提交给监听机构的数据 Q_i $(i = 1, ..., t)$ 的有效性:

(1) 监听机构接收到托管人 T_i $(i = 1, ..., t)$ 发送的 Q_i $(i = 1, ..., t)$ 后,随机选取 $\lambda_i, \mu_i \in \mathbf{F}_q$,计算 $w_i \equiv Q_i^{\lambda_i} \cdot y_i^{\mu_i} (\mathrm{mod}\ p)$,并把 w_i 发送给托管人 T_i $(i = 1, ..., t)$.

(2) 托管人 T_i $(i = 1, ..., t)$ 计算 $R_i \equiv w_i^{b_i^{-1}} (\mathrm{mod}\ p)$,并把 R_i 发送给监听机构,其中 $b_i b_i^{-1} \equiv 1 (\mathrm{mod}\ p-1) (i = 1, ..., t)$.

(3) 监听机构验证等式 $R_i \equiv g^{k\lambda_i} \cdot g^{\mu_i} \equiv u^{\lambda_i} g^{\mu_i} (\mathrm{mod}\ p)$ 是否成立.若成立,监听机构则认为托管人 T_i 诚实地出示了 $Q_i \equiv u^{b_i} (\mathrm{mod}\ p)$;否则,托管人 T_i $(i = 1, ..., t)$ 具有欺诈行为或是冒充者,应给予重罚.

通过验证后,监听机构利用 $d_1^{-1} (\mathrm{mod}\ q)$ 计算 $sk \equiv v(\prod_{i=1}^{t} Q_i^{c_i})^{-d_1^{-1}} (\mathrm{mod}\ p)$,其中 $c_i \equiv \prod_{\substack{k=1 \\ k \neq i}}^{t} x_k (x_k - x_i)^{-1} (\mathrm{mod}\ q)$,由 sk 解密 $E_1(M, sk)$ 得到明文 M,计算 $H(M,\mathrm{Time})$并验证 $H(M,\mathrm{Time})$是否满足签名方程.若满足则说明 M 有效.

3.3 强壮性分析

显然,本方案保留了文献[14]中的全部优点和安全性.同时,本方案还具有强壮性.事实上,与(基于大整数的)方案 I 相似,任意 t 个托管人 T_i $(i = 1, ..., t)$ 合谋只能重构 d_2,而不是系统或用户的秘密钥 d.

注 3:与本方案一样,在(基于大整数的)方案 I 中,监听机构在实施监听时,也能够验证每个托管人提供给监听机构的数据和托管内容的有效性.

注 4:在托管子密钥验证阶段,本方案采用了简单的验证过程,即每个托管人 T_i 只需验证 $y_i \equiv g^{b_i} (\mathrm{mod}\ p)$ 是

否成立.当然,本方案也可以采用方案 I 的验证方法.同时,方案 I 也可以采用本方案的验证方法.

References:

[1] Denning DE, Smid M. Key escrowing today. IEEE Communications Magazine, 1994,32(9):58~68.

[2] Shamir A. Partial key escrow: A new approach to software key escrow. In: Proceedings of the Key Escrow Conference. Washington, 1995.

[3] Lenstra AK, Winkler P, Yacobi Y. A key escrow system with warrant bound. In: Coppersmith D, ed. Proceedings of the Crypto'95. LNCS 963, Berlin: Springer-Vrelag, 1995. 197~207.

[4] Micali S. Fair cryptosystems. Technique Report, MIT/LCS/TR-579.c, Cambridge: Massachusetts Institute of Technology, 1994.

[5] Micali S, Ney R. A simple method for generating and sharing pseudo-random functions with application to clipper-like key escrow system. In: Coppersmith D, ed. Proceedings of the Crypto'95. LNCS 963, Berlin: Springer-Vrelag, 1995. 184~196.

[6] Yang Bo, Ma WP, Wang, YM. A new secret sharing threshold scheme and key escrow system. Acta Electronica Sinica, 1998, 26(10):1~3 (in Chinese with English abstract).

[7] Nechvatal J. A public-key-based key escrow system. Journal of Systems Software, 1996,35(1):73~83.

[8] Denning DE. Description of key escrow system. 1997. http://www.cs.georgetown.edu/~denning/crypto/ Appendix.html/.

[9] Desmedt Y, Frankel Y. Threshold cryptosystems. In: Brassard G, ed. Proceedings of the Crypto'89. LNCS 435, Berlin: Springer-Verlag, 1990. 307~315.

[10] Desmedt Y, Frankel Y. Shared generation of authenticators and signatures. In: Feigenbaum J, ed. Proceedings of the Crypto'91. LNCS 576, Berlin: Springer-Verlag, 1992. 457~469.

[11] Santis AD, Desmedt Y, Frankel Y, Yung M. How to share a function securely. In: Proceedings of the 26th ACM Symp. on Theory of Computing. ACM Press, 1994. 522~533.

[12] Gennaro R, Jarecki S, Krawczyk H, Rabin T. Robust and efficient sharing of RSA functions. In: Koblitz N, ed. Proceedings of the Crypto'96. LNCS 1109, Berlin: Springer-Verlag, 1996. 157~172.

[13] Cao ZF. A threshold key escrow scheme based on public key cryptosystem. Science in China (Series E), 2001,44(4):441~448 (in Chinese with English abstract).

[14] Cao ZF, Li JG. A threshold key escrow scheme based on ElGamal cryptosystem. Chinese Journal of Computers, 2002,25(4): 346~350 (in Chinese with English abstract).

[15] Wang GL, Qing SH. Weaknesses of some threshold group signature schemes. Journal of Software, 2000,11(10):1326~1332 (in Chinese with English abstract).

[16] Cerecedo M, Matsumoto T, Imai H. Efficient and secure multiparty generation of digital signatures based on discrete logarithms. IEICE Transactions on Fundamentals, 1993,E76-A(4):532~545.

[17] Frankel Y, Gemmell P, Yung M. Witness-Based cryptographic program checking and robust function sharing. In: Proceedings of 28th the ACM Symposium on Theory of Computing. ACM Press, 1996. 499~508.

[18] Gennaro R, Jarecki S, Krawczyk H, Rabin T. Robust threshold DSS signatures. In: Maurer U, ed. Advances in Cryptology-Eurocrypt'96. LNCS 1070, Springer-Verlag, 1996. 354~371.

[19] Cao ZF. Public Key Cryptology. Harbin: Heilongjiang Education Press, 1993. 158~185 (in Chinese).

[20] Shamir A. How to share a secret. Communications of the ACM, 1979,22(11):612~613.

[21] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 1978,21(2):120~126.

[22] ElGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithm. IEEE Transactions on Informtion Theory, 1985,31(4):469~472.

附中文参考文献:

[6] 杨波,马文平,王育民.一种新的密钥分割门限方案及密钥托管体制.电子学报,1998,26(10):1~3.

[13] 曹珍富.基于公钥密码的门限密钥托管方案.中国科学(E 辑),2000,30(4):360~366.

[14] 曹珍富,李继国.基于 ElGamal 体制的门限密钥托管方案.计算机学报,2002,25(4):346~350.

[15] 王贵林,卿斯汉.几个门限群签名方案的弱点.软件学报,2000,11(10):1326~1332.

[19] 曹珍富.公钥密码学.哈尔滨:黑龙江教育出版社,1993.158~185.