基于离散对数的多重数字签名方案

谭凯军 诸鸿文
(上海交通大学电子工程系,上海 200030)

【摘 要】本文分析了近年来所提出的各种多重数字签名方案的特点及缺点,提出了一种基于离散对数的多重数字签名方案,它不但具有T.C.Wu方案的5个特点,而且不需要一个权力中心来为签名者产生私钥,签名者可以自己选择。它们的公、私钥并不固定,而是可以灵活地变换的。

【关键词】多重数字签名 签名者 按序签名方式 广播签名方式

1 前言

随着计算机网络的发展,信息技术的进步,在现代社会的各个领域都可能要利用通信网传送大量电子文件。在一些部门,如政府、商业、军事等部门,要确保电子文件的安全性、真实可靠性是非常重要的,并且要防止文件发送者或接收者事后否认曾发送或接收到某文件。这些都要用到数字签名。而在现实中,有可能需要多个签名者签署同一份文件。譬如在一个三方合作情况下,需要三方都签署同一份合同。于是,多重数字签名的概念被提出。

多重数字签名方案有两种形式:按序签名方式和广播签名方式。前者是签名者按照一定的顺序签名文件。后者则是文件提供者将文件广播给所有签名者,这些签名者各自独立地签名,然后传给签名收集者,由它产生多重数字签名。

在这些年来,好几种多重数字签名方案已相继提出[1~7]。文献[1]是首次提出的,它的缺点是签名的顺序在系统建立时就规定了。文献[3]改进了文献[1]的方案,签名顺序可以灵活规定,但是它需要通过交互的方式来验证签名。并且这两种方案中,多重数字签名的长度与签名者的数量成正比。在文献[2]方案中,签名长度是固定的,然而签名的顺序同文献[1]一样,是在系统建立时就已固定,并且签名和验证的计算时间与签名者的数量有关。在文献[4]的方案中,验证过程相当于验证普通的数字签名,但是它需要所有的用户通过两次交互过程来产生多重数字签名。在文献[5]的方案中,签名顺序可以灵活规定,签名与验证过程也简单,但是它只适于按序签名。而且上面所提的5种方案都只适于按序签名,要想实现广播签名,需要较大的改动。文献[6]方案适于广播签名,但是在签名的产生时需要两次交互式广播传送。在文献[7]中,T.C.Wu等人提出了一种基于ID的多重数字签名方案,它克服了原来方案的缺点而具有以下特点:①签名的长度固定,与签名者数量无关。②签名的产生与验证容易实现。③按序签名与广播签名的实现方法相似。④按序签名时,签名者的顺序可灵活规定。⑤每个签名者可以容易地验证所有前面签名者产生的部分签名,而且也能检测出是否前面的签名者没有签名或产生错误签名。但是方案必须依靠一个权力中心来为所有签名者产生私钥(对应的公

文稿收到日期:1998-07-20。

作者简介:谭凯军,女,1972年生。博士研究生。主要研究方向为信息与网络安全,密码学。

钥为 ID),一旦此中心不诚实,系统就很不安全。另外由于公钥 ID 固定,所以私钥也固定,两者不能灵活地改变。

本文我们提出了一种基于离散对数的多重数字签名方案,它不但具有以上 5 个特点,而且每个签名者都可以自己产生公、私钥,并不需要一个权力中心,安全性更高(当然公钥的可信度还涉及到公钥证书,本文我们不讨论这个问题,有关文献有[8,9]等),签名者的公、私钥都可以灵活地选择和改变。

2 本文所提出的方案

2.1 系统初始化

设 p 是一个大素数,α 是 $GF(P)$中的本原元。f 是一单向函数,$f(x)=\alpha^x \bmod p$,h 是一单向哈希函数,α, p, f, h 公开。让 U_I 代表文件发送者,U_V 代表文件接收者,U_C 代表广播签名过程中的签名收集者,$U_i(i=1,2,\cdots,n)$代表 n 个签名。D 表示被签名的文件。$U_i(i=1,2,\cdots,n)$随机选择一整数 $s_i \in GF(p)$作为其私钥,并计算其公钥 $P_i=f(s_i)=\alpha^{s_i} \bmod p$,$U_i$ 将 P_i 公布于众。

2.2 按序签名过程

(1)多重数字签名产生。

U_I 规定签名的顺序为$(U_1, U_2, \cdots, U_n)$,并将此顺序公布。然后将$\{D, SG_0=0\}$传给 U_1。

a. U_1 生成一随机数 $r_1 \in GF(p)$,计算 $f(r_1)=\alpha^{r_1} \bmod p$,并将 $f(r_1)$公布于众。然后计算 $SG_1=h(D)+r_1+s_1 \bmod p-1$,将$\{D, SG_1\}$传给 U_2。

b. 每个后序的签名者 $U_i(2 \leqslant i \leqslant n)$,通过公布的签名顺序,验证下式是否成立:

$$f(SG_{i-1}) \stackrel{?}{\equiv} f^{i-1}(h(D)) \prod_{j=1}^{i-1}(f(r_j)p_j) \bmod p$$

下面给出证明:

$$\begin{aligned} f(SG_{i-1}) &= \alpha^{((i-1)h(D)+\sum_{j=1}^{i-1}(r_j+s_j)) \bmod p-1} \bmod p \\ &= \alpha^{(i-1)h(D) \bmod p-1} \alpha^{\sum_{j=1}^{i-1}(r_j+s_j) \bmod p-1} \bmod p \\ &= f^{i-1}(h(D)) \prod_{j=1}^{i-1}(f(r_j)p_j) \bmod p \end{aligned}$$

如果验证得出是正确的部分签名,那么 U_i选取一随机数 $r_i \in GF(p)$,计算出 $f(r_i)=\alpha^{r_i} \bmod p$,并公布 $f(r_i)$,然后计算部分签名:

$$SG_i = SG_{i-1} + h(D) + r_i + s_i (\bmod p-1)$$

并将$\{D, SG_i\}$传给后序签名者(第 n 个签名者将$\{D, SG_n\}$传给 U_V)。

(2)多重数字签名验证。

U_V 得到 SG_n 后,验证下式的成立:

$$\begin{aligned} f(SG_n) &= \alpha^{nh(D)+\sum_{j=1}^{n}(r_j+s_j) \bmod p-1} \bmod p \\ &= \alpha^{nh(D) \bmod p-1} \alpha^{\sum_{j=1}^{i-1}(r_j+s_j) \bmod p-1} \bmod p \end{aligned}$$

$$= f^{r}(h(D))\prod_{j=1}^{n}(f(r_j)p_j) \bmod p$$

2.3 广播签名过程

(1)多重数字签名产生。

a. U_l 将 D 广播。

b. $U_i(i=1,2,\cdots,n)$生成随机数 $r_i \in GF(p)$,计算出 $f(r_i)=a^{r_i} \bmod p$。再计算 $M_i = h(D)+r_i+s_i \bmod p-1$,将$\{D,M_i,f(r_i)\}$传给 U_c。

c. U_c 验证下式的成立:$f(M_i)=a^{h(D)+r_i+s_i \bmod p-1}=a^{h(D)}f(r_i)P_i \bmod p$,就可以验证出每个 U_i 的签名是否正确。如果正确的话,U_c 产生多重数字签名:$SG=\sum_{i=1}^{n}M_i \bmod p(i=1,2,\cdots n)$,并将$\{D,SG\}$传给 U_V。

(2)多重数字签名验证。

与 2.2 节中的验证过程类似。

4 安全性及性能分析

(1)从签名者的公钥 P_i 中来得到其私钥 s_i 是很困难的,相当于解离散对数的难度。

(2)要想从 U_i 的某次签名 $M_i=h(D)+r_i+s_i \bmod p-1$ 来获得 s_i 也不可能,因为 s_i 与 r_i 均是秘密的。即使攻击者获得 U_i 某次签名时用到的$s_i+r_i(\bmod p-1)$,要想确定 s_i 和r_i,从理论上讲也很困难[10]。

(3)假设攻击者想伪装成 U_i 来对D 签名,它并不知道 s_i,于是随机选择一个 r_i^*,根据 SG_{i-1} ,来 生成 $SG_i^* = SG_{i-1}+h(D)+r_i^*+s_i(\bmod p-1)$,使 得 $f(SG_i^*) = f^{i}(h(D))\cdot\prod_{j=1}^{i-1}(f(r_j)p_j)\cdot f(r_i^*)\cdot p_i \bmod p$ 成立,要求 SG_i^* 是困难的,也相当于解离散对数的难度。

(4)验证者可以检测出是否有人没有签名。假设 U_i 没有签名,那么 U_{i+1}可以检测出来。U_{i+1}需要验证 $f(SG_i \overset{?}{=} f^{i}(h(D))\prod_{j=1}^{i}(f(r_j)p_j) \bmod p$,因为 U_i 没有签名,此时的 $SG_i = SG_{i-1}=(i-1)h(D)+\sum_{j=1}^{i-1}(r_j+s_j)(\bmod p-1)$, 所以 $f(SG_i)=f(SG_{i-1})=f^{i-1}(h(D))\cdot\prod_{j=1}^{i-1}(f(r_j)p_j) \bmod p$,验证不能成功。

(5)签名的长度范围是固定的,与签名者的数量无关。

(6)按序签名与广播签名都能实现,实现方法相似。

(7)按序签名时,签名者的顺序可以由 U_l 灵活地规定。

(8)签名者的公、私钥可以变换,并不是固定不变的,它们可以自己选择密钥,不需要一个权力中心为其分配,安全性比文献[7]中的方案高。

(9)签名的产生与验证过程的计算量分析如下:让 T_h, T_{exp}, T_{mul}分别代表一次模 N 的单向哈希函数h ,幂乘以及乘法运算时间,那么本方案签名中 U_i 验证部分签名时的计算量为 $(3i-4)T_{mul}+2T_{exp}+T_h$,如果预先计算好$\prod_{j=1}^{i-1}(f(r_j)p_j)$,那么计算量为$(i-1)T_{mul}+2T_{exp}+T_h$,生产新的部分签名的计算量为 T_{exp},如果每个 U_i 在签名前预先计算好 $f(r_i)$,那么签名时的即时计算量为 0。广播签名时, U_i产生签名的时间是: $T_{exp}+T_p$, 同样可以预先计算好 $f(r_i)$,所以时间为 T_h。而 U_c 需要的时间为$(3n-1)T_{mul}+(n+1)T_{exp}+T_h$,如果预先计算

好 $f(r_i)p_i$，那么需要的时间为$(2n-1)T_{mul}+(n+1)T_{exp}+T_h$，与 T.C.Wu 方案[7]中计算量相当。

5 结论

本文分析了近年来所提出的各种多重数字签名方案的特点及缺点，提出了一种基于离散对数的多重数字签名方案，它不但具有 T.C.Wu 方案[7]的 5 个特点，而且不需要一个权力中心来为签名者产生私钥，签名者可以自己选择。它们的公、私钥并不固定，而是可以灵活地变换的。

参考文献

1 Ltakura K, Nakamura K. A public key cryptosystem suitable for digital multisignatures. NEC Res and Develop, 1983,(71): 1～8

2 Harn L, Kielser T. New scheme for digital multisignatures. Electr Lett,1989, 25(15): 1002～1003

3 Okamoto T. A digital multisignature scheme using bijective public key cryptosystems. ACM Trans Computer System, 1988,6 (8): 432～441

4 Boyd C. Multisignature based on zero knowledge schemes, Electr Lett, 1991,27(22): 2002～2004

5 Hardjono T, Zheng Y. A pratical digital multisignature scheme based on discrete logarithms. Advances in Cryptology－AUSCRYPTO's 92, Spring－Verlag,1993: 16～21

6 Harn L. New digital signature scheme based on discrete logarithms. Electr Lett, 1994,30(5): 396～398

7 Wu T C, Chou S L. Two ID－based multisignature protocols for sequential and broadcasting architectures. Computer Communications, 1996,(19): 851～856

8 Horng G, Yang C S. Key authentication scheme for crypto systems based on discrete logarithms. Comp Comm, 1996,(19): 848～850

9 Laih S C, Chiou W H, Chang C C. Authentication and protection of public keys. Computers & Security, 1994,(13):581～585

10 Park C, Kurosawa K, Tsujii S. A key distribution protocol for mobile communication systems. IEICE Tran Fundamentals, January,1995, E78－A(1): 77～81

A Digital Multisignature Scheme Based on Discrete Logarithms

Tan Kaijun　　*Zhu Hongwen*

(Shanghai Jiaotong University ,Shanghai 200030)

【**Abstract**】 After analyzing several digital multisignature scheme's features and disadvantages of these years, a digital multisignature scheme based on discrete logarithms is proposed in this paper. Not only it has 5 features which T.C.Wu scheme claims it has, but also it doesn't need an Authority Center to assign private keys for the signatories who can choose their own private keys. Moreover, the signatorie's keys are not fixed and can be changed flexibly.

【**Key words**】 digital multisignature , signatories , sequential signing approach, broadcasting signing approach