一种新的基于离散对数的签名方案

贾晓芸[1,3]，罗守山[2,3]，袁超伟[1]

(1. 北京邮电大学 通信网络综合技术研究所，北京 100876；2. 北京邮电大学 软件学院，北京 100876；3. 西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071)

摘要：针对传统签名方案中验证者的验证权限是相同的缺点，提出了一种新的基于离散对数的链式验证签名方案.利用有序秘密分享方法将验证参与者分为签名验证者和链式验证授权者，签名验证者只有在经过链式验证授权组中每一个成员的依次授权时，才可以验证签名的有效性，而且链式验证授权组中的任何成员(即使所有成员合谋)都不能验证签名的有效性.此外，该方案可以方便地增删链式验证授权组中的成员和维护链式验证授权者和签名验证者的私钥.

关键词：离散对数；数字签名；链式验证签名

中图分类号：TN918.1 **文献标识码**：A **文章编号**：1001-2400(2008)02-0351-05

New digital signature scheme based on the discrete logarithm

JIA Xiao-yun[1,3], *LUO Shou-shan*[2,3], *YUAN Chao-wei*[1]

(1. Inst. of Communication Networks Integrated Technique, Beijing Univ. of Posts and Telecommunications, Beijing 100876, China; 2. School of Software Eng., Beijing Univ. of Posts and Telecommunications, Bejing 100876, China; 3. State Key Lab. of Integrated Service Networks, Xidian Univ., Xi′an 710071, China)

Abstract: A new chain verification digital signature scheme based on the discrete logarithm is proposed, which can avoid the equal verifying right of the verifiers which normally accompany the conventional schemes. In this scheme, by means of the sequence secret sharing scheme, the verification participators can divide the signature verifier from the chain grantors, the signature verifier cannot verify the validity of the signature until he is authorized by all chain grantors in turn, and any chain grantor(even all chain grantors are collusive)cannot verify the validity of the signature. What's more, the signature scheme can conveniently add or delete the chain grantor and defend the secret key of the chain grantors and signature verifier.

Key Words: discrete logarithm; digital signature; chain verification digital signature

数字签名是现代密码学的一项重要发明，它是现代通信中实现消息认证和身份认证的一种重要手段.使用普通的数字签名时，无论是产生签名还是验证签名，都只有一个用户参与.随着网络应用的蓬勃发展，普通的数字签名技术已经不能满足许多应用的要求.近十年来，众多研究者提出了许多特殊的数字签名，例如，群签名[1~4]、门限群签名[5,6]、前向安全的群签名[7]、代理签名[8]、盲签名和多方签名等.

在诸多实际应用中，作为签名的一方并不希望任何一个个体都能对其签名进行有效性验证，原因是：第一，签名可能携带了签名方的重要信息；第二，签名有效性的验证者可能正是潜在的攻击者.为防止验证签名有效性的任意传播，1993 年 L. Harn[9] 提出了门限共享验证签名方案，即 (t, n) 门限共享验证签名方案，该签名的有效性只有在 t 个成员的合作下才能得以验证，少于 t 个成员的合作，签名是无法得以验证的.此方案的主要目的是为了分散验证者的权利，以防签名滥用. Lee 和 Chang[10] 指出 Harn 的方案易受伪造攻击.此后，陆续有很多学者提出了安全的门限共享验证签名方案[11~14].但在这种门限共享验证签名方案中，各个签

收稿日期：2007-05-18

基金项目：国家自然科学基金资助(60642008)；西安电子科技大学综合业务网理论及关键技术国家重点实验室开放课题(ISN7-01)

作者简介：贾晓芸(1980-)，女，北京邮电大学博士研究生，E-mail：purping@gmail.com.

名验证者在验证签名时的权力是相等的.在实际应用中,往往需要具有不同权利的签名验证者的签名方案,比如存在这样一种情况,一个秘密情报部门主管 A 对某文件签名后,他要求下级部门 P_n 在验证签名前要先通过 P_n 的上级主管 $P_1,P_2,\cdots,P_{n-1}$ 的依次同意,然后才可以验证其签名的有效性,基于这种实际应用,参考有序多重数字签名协议[15,16]的思想和协议设计方法,提出了一种新的签名方案——链式验证签名.

首先,给出了链式验证签名的形式化定义,接着,基于离散对数和有序秘密分享方案提出了一种链式验证签名方案,此方案中,合法验证者 P_n 在验证 A 的签名之前,必须要经过 $P_1,P_2,\cdots,P_{n-1}$ 依次地同意才可以验证签名的有效性,$P_1,P_2,\cdots,P_{n-1}$ 称为链式验证授权者.此外,分析了该方案的性能,该方案可以方便地增删链式验证授权者的成员和维护链式验证授权者和签名验证者的私钥.最后,分析了此方案的安全性和效率.

1 方案的模型

定义(链式验证签名方案) 设一个链式验证签名方案由 3 个参与实体和 5 个算法组成.这 3 个参与实体是系统,也称为可信中心,记为 TA,签名人 A 和签名验证参与者,这里签名验证参与者可分为签名验证者 P_n 和链式验证授权组 $P=\{P_1,P_2,\cdots,P_{n-1}\}$. 5 个算法是{InitS, GenK, Sig, AutV, Ver},各个算法的详细定义如下:

(1) InitS(系统的初始化过程,Initiation of System) 确定产生链式验证签名方案的基本参数、符号和有关算法.

(2) GenK(密钥的产生,Generation of Key) 由密钥产生算法 GenK 产生签名的公私钥以及链式验证授权者的密钥.

(3) Sig(签名算法,Signature Algorithms) 当签名者 A 想对消息 M 进行签名时,他只需利用自己的签名私钥就可以完成对消息 M 的签名.

(4) AutV(签名验证的授权,Authorization of Verifier) 通过一定的算法设计,使得依次经过链式验证授权组中的成员 $P_1,P_2,\cdots,P_{n-1}$ 的一一授权,签名验证者 P_n 才可以获得签名验证公钥,由此则可以有效地验证签名的合法性.在这一过程中,要保证即使所有的链式验证授权者合谋攻击都没有权利验证签名的有效性.

(5) Ver(签名验证算法,Verification Algorithms) 签名验证者根据恢复的签名验证公钥,验证签名的有效性.

2 方案的实现

笔者基于离散对数设计了一种链式验证签名方案,此方案只有经过链式验证授权组中的成员 $P_1,P_2,\cdots,P_{n-1}$ 的一一授权之后,签名验证者 P_n 才可以验证签名的有效性.按照上一节的模型,实现步骤如下:

[InitS] 可信中心 TA 选取 p:$p=2q+1$,其中 p,q 都为大素数,g 为有限域 Z_p 上的一个 q 阶元,在 Z_p 中计算以 g 为底的离散对数是不可行的.

[GenK] TA 随机选 n 个相异元素 $d_1,d_2,\cdots,d_n\in Z_q^*$,计算 $e_i=g^{d_i+h(d_i)}\pmod p$,将有序数组 $(e_1,e_2,\cdots,e_n)$ 公开,把 d_i 通过安全的秘密信道发送给 P_i 作为他的私钥($1\leqslant i\leqslant n$). 签名人 A 任选一元素 x,计算 $y=g^x\pmod p$.这时签名人 A 的签名私钥是 x,验证公钥是 y.

[Sig] 签名者 A 若想对消息 M 进行签名,首先 A 任意选取 $k\in Z_p$,且 $\gcd(k,p-1)=1$,然后计算 $r=g^k\pmod q$,$s=[x(h(M)+r)-k]\pmod q$,则消息 M 的签名是 (r,s).

[AutV] TA 随机选两个相异元素 $a_1,a_2\in Z_q^*$,令 $a_0=a_1+a_2(a_0\neq q)$,计算 $u=a_0+d_1+d_2+\cdots+d_n\pmod q$,$v=a_2-h(d_1)-h(d_2)-\cdots-h(d_n)\pmod q$,$T=u+y$,$e_0=g^{a_1}\pmod p$,然后公布 $T,v,e_0,h(y)$,再将 a_1 送给链式验证授权组中的成员 P_1.

成员 P_1 收到 a_1 后,先计算 $g^{a_1}\pmod p=e_0$ 是否成立,若成立则计算 $u_1=a_1+d_1+h(d_1)\pmod q$,然

后将 u_1 传给 P_2,否则停止传送并向 TA 抱怨,要求重新发送 a_1. P_2 收到 u_1 后先检验 u_1 的有效性,即检验 $g^{u_1}=e_0e_1 \pmod p$ 是否成立,如果不成立则说明 P_1 有欺诈,公布他的欺诈行为,并要求重新传送 u_1;否则计算 $u_2=u_1+d_2+h(d_2) \pmod q$,将 u_2 传给 P_3. 依次类推,一直到 P_n,P_n 先检验 u_{n-1} 的有效性,即检验 $g^{u_{n-1}}=e_0e_1\cdots e_{n-1} \pmod p$ 是否成立,若成立则计算 $u_n=u_{n-1}+d_n+h(d_n) \pmod q$,然后计算 $u^*=u_n+v$,则 $y=T-u^*$. 从而 P_n 可以得到签名验证公钥 y.

[Ver] 合法的验证者 P_n 通过上面的步骤可以得到签名验证公钥 y,于是可以通过验证等式 $y^{h(M)+r}=rg^s \pmod p$ 是否成立来确定签名的有效性,若等式成立,则签名者 A 的签名是有效的,否则签名无效.

下面简要地分析此方案的正确性.

首先,证明签名验证者按照上述过程恢复出的公钥是正确的. 从上述描述中可以看出,每一个签名验证授权者 P_i $(i=1,2,\cdots,n-1)$ 根据之前的信息可以计算 $u_i=u_{i-1}+d_i+h(d_i) \pmod q$(这里 $u_0=a_1$),则签名验证者 P_n 根据 P_{n-1} 的信息计算 $u_n=u_{n-1}+d_n+h(d_n)=a_1+d_1+h(d_1)+\cdots+d_n+h(d_n) \pmod q$,再根据可信中心 TA 计算出的 $v=a_2-h(d_1)-h(d_2)-\cdots-h(d_n) \pmod q$,可得 $u^*=u_n+v=a_1+a_2+d_1+\cdots+d_n \pmod q$.

又根据 $T=u+y$,$u=a_0+d_1+d_2+\cdots+d_n \pmod q$ 和 $a_0=a_1+a_2$ 可以得到

$$T-u^*=u+y-u^*=a_0+y-a_1-a_2=y \pmod q \quad .$$

从上面的分析,可以看出签名验证者可以恢复出正确的签名验证公钥 y.

下面,分析签名的正确性. 由 $r=g^k \pmod p$,$s=[x(h(M)+r)-k] \pmod{p-1}$ 及 $y=g^x \pmod p$,可得 $rg^s=g^kg^{x(h(M)+r)-k}=g^{x(h(M)+r)}=y^{h(M)+r} \pmod p$. 故通过此签名算法可以验证签名的有效性.

由以上的分析,可以看出此签名协议是正确的.

3　安全性及性能分析

3.1　安全性分析

首先分析任何一个个体伪造合法签名的可能性,若攻击者 Eve 要伪造签名,可以有两种途径:

(1) 根据签名者的验证公钥和单个或多个有效的签名获得签名私钥 x. 从签名者的验证公钥获得签名私钥相当于求解离散对数问题. 从单个有效的签名获得签名私钥相当于根据给出的信息和签名求解 x,即求解方程 $s=[x(h(M)+r)-k] \pmod q$,而此方程中有两个未知参数 x 和 k,故无法求解此方程. 如果 Eve 收集多个有效签名 $(r_1,s_1),(r_2,s_2),\cdots,(r_t,s_t)$,他将求解同余方程组,但是由于 r_i 所对应的 k_i 是随机选择的,所以方程组每增加一个方程将同时增加一个未知数,故也没有办法在多项式时间内解出 x. 从以上的分析可以看出攻击者 Eve 根据签名者的验证公钥和单个或多个有效的签名是无法获得签名私钥 x,所以通过这种方法 Eve 不能得到有效的签名.

(2) 直接伪造出签名中的 s,从而构造出一个伪造签名. 即攻击者 Eve 根据方程 $y^{h(M)+r}=rg^s \pmod p$ 来伪造签名 (r,s),首先 Eve 任选一整数 r',然后基于上述的方程来计算相应的 s',而这相当于求解离散对数问题. 此外,Eve 任选一整数 s',然后基于上述的方程来计算相应的 r',这也是一个求解离散对数问题. 所以 Eve 不能伪造有效的签名.

总之,要伪造签名者的有效签名等价于求解离散对数,也就是说只有解决了离散对数问题才能攻破这个方案,所以该方案中签名者的签名是不可伪造的.

下面分析链式验证签名的特殊性质. 链式验证签名要求,只有签名验证者 P_n 可以验证签名的有效性,而链式验证授权组 $P=\{P_1\cdots,P_{n-1}\}$ 中的任何个体都不能验证签名的有效性,而且要依次经过 $P_1,P_2,\cdots,P_{n-1}$ 的一一授权,签名验证者 P_n 才可以验证签名的有效性.

首先,分析链式验证授权组中成员 $P_i(1\leqslant i<n)$ 是否可以验证签名的有效性. 要想正确验证签名的有效性,就必须要获得签名验证公钥 y,通过此签名协议的过程,可以知道 P_i $(1\leqslant i<n)$ 从协议中知道的值是 $T,v,e_0,h(y),u_i,P_i$ $(1\leqslant i<n)$,要想从这些值求出 y 就必须知道他后面的链式验证授权者的私钥,而从这

些值中计算后面的链式验证授权者的私钥等同于求解离散对数问题.即使所有的链式验证授权者合作,由于他们不知道合法验证者 P_n 的私钥,故而也没有能力验证签名的有效性.

其次,分析合法验证者 P_n 在获得签名验证公钥时,是否需要依次经过 $P_1,P_2,\cdots,P_{n-1}$ 的一一授权.从上面的协议过程可以看出合法验证者 P_n 要想获得签名验证公钥 y 就必须要获得 u_{n-1},而 u_{n-1} 是通过每一个链式验证授权者的私钥计算出来的,所以必须要经过所有的链式验证授权者的授权才可以,此外,每一个链式验证授权者 P_i $(1\leqslant i<n)$ 在计算自己的 u_i 时,要验证他前面的链式验证授权者是否给出正确的 u_{i-1},而此验证不仅可以防止链式验证授权者的欺诈行为,还可以保证链式验证授权者必须按照 $P_1,P_2,\cdots,P_{n-1}$ 依次授权,P_n 才可以验证签名的合法性.

3.2 性能分析

此方案除了有链式验证签名的特性外,还有两个优点:

(1) 链式验证授权者可方便地增删成员　在实际应用中,经常会碰到因为部门调整遇到的链式验证授权者增加或删除成员的情况,利用此方案可以方便地实现增加或删除成员,如果加入新成员 P_{t+1} 时,TA 随机选一个 $d_{t+1}\in Z_q^*$(与之前所选数不同)给 P_{t+1},计算 $e_{t+1}=g^{d_{t+1}+h(d_{t+1})}\pmod p$,添加 e_{t+1} 到有序组 $(e_1,e_2,\cdots,e_n)$ 中,在 u 和 v 的计算中分别加入 d_{t+1} 和 $-h(d_{t+1})$,相应改变 T 即可.当要删除一个成员时,设删除 P_i,TA 公布此消息与所有的链式验证授权者,并把 $(e_1,e_2,\cdots,e_n)$ 中的 e_i 去掉,在计算 u 和 v 时去掉 d_i 和 $-h(d_i)$,相应改变 T 即可.

(2) 链式验证授权者和签名验证者子秘密的维护　若某个链式验证授权者 $P_i(1\leqslant i\leqslant n-1)$ 或签名验证者 P_n 的子秘密 d_i 泄漏,TA 只需给他重新分配子秘密 d'_i,将 $g^{d'_i+h(d'_i)}\pmod p$ 公开,在计算 u 和 v 时分别换为 d'_i 和 $-h(d'_i)$,相应改变 T 即可,而不必更改其他成员的子秘密.

3.3 效率分析

最后分析此方案的效率.很明显,此方案中最耗时的操作是模指数运算,方案效率的提高主要取决于如何有效地进行模指数运算.许多文献已经对这个问题分别进行了研究,并取得了许多成果.在文献[17,18]中给出了若干快速模指数运算的方法.目前,若底数和指数均为1 024位,进行模指数运算所需的时间是5 166.613 ms;若底数和指数均为2 048位,进行模指数运算所需的时间是10 634.236 ms.从上面的方案实现过程,可以看到签名者 A 需要做 1 次模指数运算,可信中心 TA 需要做 $n+1$ 次模指数运算,每个链式验证授权者为了验证前面的链式验证授权者是否诚实,需要做一次模指数运算,签名验证者 P_n 为了得到签名验证密钥,需要进行一次模指数运算,为了验证签名的有效性需要进行 2 次模指数运算.这里假设 TD 表示模指数运算的复杂度,则文中提出的环式验证签名方案的复杂度为 $(2n+4)$TD.效率的提高使得此方案有很大的应用价值.

4 结　论

实际应用中,签名人要求下级部门在验证签名前要先通过他的上级主管的依次授权,然后才可以验证 A 签名的有效性.针对需求,提出了一种新的签名方案——链式验证签名方案.并参考有序多重数字签名协议的思想,及协议设计方法,提出了一种基于离散对数的链式验证签名方案.此方案的优势在于签名验证者只有经过链式验证授权组中每一个成员的依次授权,才可以验证签名的有效性,而且链式验证授权组中的任何一个成员(即使所有成员共谋)都没有权利验证签名的有效性,此外,此方案可以方便地增加或删除链式验证授权者,并在链式验证授权者或签名验证者泄漏子秘密时,可以进行及时地维护.此方案的效率主要体现在模指数运算,而这种运算已有很多成熟的快速运算,故而使得此方案的效率相当高,应用前景广阔.

参考文献:

[1] Jun Z, Dake H. ACJT Group Blind Signature Scheme[C]//First International Conference on Commnicaitons and Networking. ChinaCom'06. Beijing: Springer-Verlag, 2006: 1-6.

[2] Wang G, Bao F, Azhou J, et al. Security Remarks on a Group Signature Scheme with Member Deletion[C]//Proceeding

of Information and Communications Security (ICICS'3):LNCS 2836. Berlin: Spring-Verlag, 2003: 252-265.

[3] 吕继强，王新梅. 两个基于身份的数字签名方案的安全性改进[J]. 通信学报，2003，24(9)：128-131.
Lü Jiqiang, Wang Xinmei. Improvement of Two ID-based Digital Signature Schemes[J]. Journal of China Institite of Communications, 2003, 24(9):128-131.

[4] 王凤和，胡予濮，王春晓. 一种基于中国剩余定理的群签名方案的攻击及其改进方案[J]. 电子与信息学报，2007，29(1)：182-184.
Wang Fenghe, Hu Yupu, Wang Chunxiao. An Attack and Improve of a Group Signature Scheme Based on Chinese Remainder Theorem[J]. Journal of Electronics & Informations Technology, 2007, 29(1): 182-182.

[5] Chen T S, Hsiao T, Chen T L. An Efficient Threshold Group Signature Scheme[C]//TENCON 2004, 2004 IEEE Region 10 Conference: 2. Thailand: Springer-Verlag, 2004: 13-16.

[6] 刘颖，胡予濮，王飞，等. 一个高效的基于身份的门限签名方案[J]. 西安电子科技大学学报，2006，33(2)：311-315.
Liu Ying, Hu Yupu, Wang Fei, et al. An Efficient ID-based Threshold Signature[J]. Journal of Xidian Unviersity, 2006, 33(2): 311-315.

[7] Johan V, Dawoud S, Stephen M. A Fully Distributed Proactively Secure Threshold-Mulisignature Scheme[J]. IEEE Trans on Parallel and Distributed Systems, 2007, 18(4): 562-575.

[8] Mehta M, Harn L. Efficient One-time Proxy Signatures[J]. Communications IEE Proceedings, 2005, 152(2): 129-133.

[9] Harn L. Digital Signature with (t,n) Shared Verification Based on Discrete Logarithms[J]. Electron Lett, 1993, 29(24): 2094-2095.

[10] Lee W B, Chang C C. Comment: Digital Signature with (t,n) Shared Verification Based on Discrete Logarithmes[J]. Electron Lett, 1995, 31 (3): 176-177.

[11] Wang M, Zhu Q, Qing L. Shared Verification Signature for Generalized Subsets of Receiving Group [J]. Communications and Information, 2005, 2 (10): 1318-1321.

[12] Jia X Y, Luo S S, Yuan C W. A New Signature Scheme with Shared Verification[J]. The Journal of China Universities of Posts and Telecommunications, 2006, 13(2): 66-69.

[13] 许春香，牛志华，肖国镇. 没有可信机构的矢量空间秘密共享-多重签名方案[J]. 西安电子科技大学学报，2005，32(2)：225-228.
Xu Chunxiang, Niu Zhihua, Xiao Guozhen. A Vector Space Secret Sharing-multisignature Scheme without a Trusted Share Distribution Center [J]. Journal of Xidian Unviersity, 2005, 32(2): 225-228.

[14] Shi R. A (t,n) Threshold Shared Verification Signature Scheme Based on Discrete Logarithms[J]. Journal of Computer Research & Development, 2000, 37(3): 319-323.

[15] Harn L, Lin C Y, Wu T C. Structured Multisignature Algorithms[J]. Computers and Digital Techniques, 2004, 151 (3): 231-234.

[16] Wang Y L, Wang L H. A New Type of Digital Multisignature[J]. Computer Supported Cooperative Work in Design, 2005, 2(2): 750-754.

[17] Aho A, Hopcroft J, Ullman J. The Design and Analysis of Computer Algorithms[M]. MA: Addison-Wesley, Reading, 1974.

[18] Chang C C, Horug H J, Buechrer D J. A Cascade Exponentiation Evaluation Scheme Based on the Lempel-Ziv-Welch Compression Algorithm[J]. Journal of Information Science and Engineering, 1995,11(3): 417-431.

(编辑：高西全)