防欺诈的动态(*t*,*n*)认证加密方案

甘元驹，彭银桥，梅其祥

(广东海洋大学信息学院 广东 湛江 524088)

【摘要】针对已有的共享认证加密方案不能有效抵制成员欺骗，不能动态调整验证成员的门限值，以及增加或删除验证者时，系统需重新给所有验证者分配新的密钥等安全缺陷，提出了一种基于动态秘密共享和认证加密算法的具有动态调整验证者门限值的共享认证加密方案。该方案可高效检测验证者的欺诈行为；用户自己选择秘密份额，系统中心不需向用户传送任何秘密信息；当有用户加入或退出系统时，其他用户不必更改自己的密钥。此外，签名者可根据消息的重要性，动态确定验证组中参与验证的门限值。

关 键 词 认证加密； 密码学； 离散对数； 拉格朗日插值公式

中图分类号 TP309 **文献标识码** A doi:10.3969/j.issn.1001-0548.2011.02.008

Dynamic (*t*, *n*) Authenticated Encryption Scheme for Cheat-Proof

GAN Yuan-ju, PENG Yin-qiao, and MEI Qi-xiang

(School of Information, Guangdong Ocean University Zhanjiang Guangdong 524088)

Abstract Most authenticated encryption schemes with shared verification have some security flaws. In this study, an efficient authenticated encryption scheme is designed with dynamically adjusting the threshold of the verifier group based on dynamic secret sharing and authenticated encryption algorithm. The proposed scheme has the following properties: cheating of any verifier can be detected efficiently; each participant select his secret key by himself, the system center (SC) needn't send any secret information to any participant; and the secret key of other participants would not change when the system accepts a new participant or fires an old participant. Moreover, a signer could adjust the threshold value of the verifier group, depending on the secure level of a message.

Key words authenticated encryption; cryptography; discrete logarithm; Lagrange interpolation formula

文献[1]提出了具有消息恢复的新型数字签名方案，该方案结合了数据加密与数字签名密码技术。文献[2-4]在文献[1]的基础上设计出具有低通信代价的认证加密方案。由于认证加密只有指定的接收者才能恢复消息并进行签名认证，与直接对消息进行先加密和后签名方法相比，认证加密不仅可以同时实现消息的机密性、完整性与认证性，而且还具有更小的通信量与计算量，然而这些方案都只有一个指定的接收者可验证签名的有效性。文献[5]结合共享验证和认证加密技术，提出(*t*,*n*)共享认证加密方案，将单个验证者扩展到群体验证者，即*n*个验证者中的*t*个合作者可验证消息认证加密的有效性。文献[6]指出了文献[5]要求*t*个验证者都是诚实的假设在实际中很难满足的缺陷，并给出了两种攻击方法。但存在的不足是：1) 验证组的门限值*t*是固定的，但签名者可根据消息的机密性设置不同的门限值；2) 在不修改其他验证者密钥的前提下，无法有效增加新成员或删除旧成员。基于对以上问题的研究，本文结合动态门限秘密共享技术[7-9]和认证加密技术[4,10]，提出了一种动态(*t*,*n*)认证加密方案。

1 方案描述

方案由系统参数初始化、用户的注册、签名加密过程和消息的恢复与认证4个阶段组成。系统有各方均可访问的用于存放公开参数或数据，且只有系统中心SC才能修改或更新权限的公告栏NB。

1.1 参数初始化

系统中心SC选择如下参数：

1) 选择p和q两个大素数，且$q|p-1$；

2) g是Z_p^*中的一个q阶生成元；

3) 一个无碰撞的单向Hash函数$H(\ )$，并将$\{p,q,g,H(\ )\}$4个参数存放于公告栏NB。

收稿日期：2009－09－18； 修回日期：2010－09－16
基金项目：广东省科技基金(2006B501018)
作者简介：甘元驹(1974－)，男，副教授，主要从事密码协议分析与信息安全方面的研究.

1.2 用户的注册

设$G=\{U_0,U_1,U_2,\cdots,U_n\}$是所有用户组成的集合，在系统中心SC公布$\{p,q,g,H(\ )\}$后，用户$U_i\in G$随机选择自己的密钥$x_i(\sqrt{q}<x_i<q-1)$和身份标识$\mathrm{ID}_i(p>\mathrm{ID}_i>n)$，并计算公钥$y_i=g^{x_i} \bmod p$。用户$U_i\in G$将$x_i$保密，并把$y_i$和$\mathrm{ID}_i$发给系统中心SC。若有用户的$y_i$和$\mathrm{ID}_i$相同，则系统中心SC要求相关用户重新选择参数，直到所有用户参数互异。最后系统中心SC将用户$U_i\in G$的信息$\{\mathrm{ID}_i,y_i\}$写入公告栏。

1.3 签名加密过程

系统的任一用户$U_i\in G$都可为消息的签名者，不妨设U_0是消息的签名者，向$G'=\{U_1,U_2,\cdots,U_n\}$中的用户发送消息$M$认证加密信息，在恢复消息和认证时，要求$G'$中的$n$个用户至少有$t$个参加。其步骤如下：

1) U_0根据加密信息M的安全性要求，选择一个合适的整数t，$1<t\leqslant n$。

2) U_0随机选择$r\in Z_p^*$，计算$L=g^r \bmod p$，并利用n个数对$(\mathrm{ID}_i,y_i^r \bmod p)$ $(i=1,2,\cdots,n)$共n个点用拉格朗日插值公式构造一个$n-1$次多项式:

$$f(x)=\sum_{i=1}^{n} y_i^r \prod_{j=1,j\neq i}^{n}((x-\mathrm{ID}_i)(\mathrm{ID}_i-\mathrm{ID}_j)^{-1}) \bmod p \quad (1)$$

同时计算出$\{f(1),f(2),\cdots,f(n-t)\}$共$n-t$个点的值。

3) U_0随机选择一整数$k\in Z_p^*$，计算$v=L^{f(0)} \bmod p$，再计算$\{C_1,C_2,S,C_3\}$，其中：

$$C_1=M\oplus H(v^k \bmod p) \quad (2)$$

$$C_2=H(M\|C_1\|g^k \bmod p) \bmod q \quad (3)$$

$$S=rk-x_0C_2 \bmod q \quad (4)$$

$$C_3=H(L\|C_1\|C_2\|S\|f(1)\|f(2)\|\cdots\|f(n-t)\|g^{rk} \bmod p) \quad (5)$$

式中，“$\oplus$”为异或运算；“$\|$”为连接运算，将$\{L,C_1,C_2,S,C_3,f(1),f(2),\cdots,f(n-t)\}$组播给$G'=\{U_1,U_2,\cdots,U_n\}$的$n$个用户。

1.4 消息的恢复与认证

不失一般性，假设G'中的t个用户$w=\{U_1,U_2,\cdots,U_t\}$$(t\leqslant n)$相互合作恢复消息$M$。每个$U_j\in w(j=1,2,\cdots,t)$接收到$\{L,C_1,C_2,S,C_3,f(1),f(2),\cdots,f(n-t)\}$后，进行如下计算：

1) 每个$U_j\in w(j=1,2,\cdots,t)$在系统公告栏中查出消息的签名者U_0的公钥，验证等式：

$$C_3=H(L\|C_1\|C_2\|S\|f(1)\|f(2)\|\cdots\|f(n-t)\|g^S y_0^{C_2} \bmod p) \quad (6)$$

若式(6)不成立，则所收到数据已被攻击或有用户假冒U_0发送数据，终止计算；若式(6)成立，表示收到的信息为U_0所发，进入下一步。

2) 每个$U_j\in w(j=1,2,\cdots,t)$，计算：

$$A_j=L^{X_j} \bmod p \quad (7)$$

并随机选择一整数$k_j\in Z_p^*$计算：

$$B_j=H(A_j,g^{k_j} \bmod p,L^{k_j} \bmod p) \quad (8)$$

$$D_j=k_j-x_jB_j \pmod p \quad (9)$$

将$\{A_j,B_j,D_j\}$安全地发给w中的其他成员。

3) 收到其他成员$U_j(U_j\in w)$的$\{A_j,B_j,D_j\}$后，w中的每一成员可验证等式$B_j=H(A_j,g^{D_j}y_j^{B_j} \bmod p,L^{D_j}A_j^{B_j} \bmod p)$的正确性。若不正确表示$U_j$提供的$\{A_j,B_j,D_j\}$无效。

4) 当所有的$\{A_j,B_j,D_j\}$都验证正确后，$U_j(U_j\in w)$由点(ID_j,A_j)(其中$j\in w$，t个点)以及点$\{1,f(1)\},\{2,f(2)\},\cdots,\{n-t,f(n-t)\}$(共$n-t$数对)，用拉格朗日插值公式可重构$n-1$阶多项式：

$$f'(x)=\sum_{i=1}^{n} Y_i \prod_{j=1,j\neq i}^{n}((x-X_j)(X_i-X_j)^{-1}) \bmod p \quad (10)$$

式中，$(X_i,Y_i)(i=1,2,\cdots,n)$表示$n$个数值对。

计算$Z=g^S y_0^{C_2} \bmod p$，于是消息M可恢复为：

$$M=C_1\oplus H(Z^{f'(0)} \bmod p) \quad (11)$$

并验证等式$C_2=H(M\|C_1\|Z)$是否成立，判断恢复的消息M是否正确。

2 方案特性分析

2.1 正确性证明

定理 1 方程$f(x)$与方程$f'(x)$等价。

证明 $A_j=L^{X_j} \bmod p=(g^r)^{X_j} \bmod p=(g^{X_j})^r \bmod p=y_j^r \bmod p$，从式(1)可知，方程$f(x)$是由$n$个数对$(\mathrm{ID}_i,y_i^r \bmod p)(i=1,2,\cdots,n)$用拉格朗日插值公式构造而成，因此有$f(\mathrm{ID}_i)=y_i^r \bmod p$，即$y_i^r \bmod p$是方程$f(x)$对应点$\mathrm{ID}_i$的根，并且有$p>\mathrm{ID}_i>n$。此外值$f(1)$、$f(2)$、$\cdots$、$f(n-t)$是从方程$f(x)$中利用从点1、2、$\cdots$、$n-t$，共$n-t$个点计算出的值。因此$\{f(1)$、$f(2)$、$\cdots$、$f(n-t)$、$f(\mathrm{ID}_1)$、$f(\mathrm{ID}_2)$、$\cdots$、$f(\mathrm{ID}_n)\}$是$n-1$次方程$f(x)$的$n-t+n$个不同点的根。从式(10)和拉格朗日插公式可得，式(1)与式(10)是等价的，即$f(0)=f'(0)$。证毕。

定理 2 消息M一定可由式(11)恢复。

证明：

$$C_1\oplus H(Z^{f'(0)} \bmod p)=C_1\oplus H((g^S y_0^{C_2})^{f'(0)} \bmod p)=C_1\oplus H((g^{rk-x_0C_2}y_0^{C_2})^{f'(0)} \bmod p=M\oplus H((L^{f(0)})^k \bmod p)\oplus H((L^k)^{f'(0)}=M$$

证毕。

2.2 欺骗者的识别

定理 3 假设在消息的恢复与认证过程步骤2中，合作的用户$U_j(U_j\in w)$给出的$\{A_j,B_j,D_j\}$满足$B_j=H(A_j,g^{D_j}y_j^{B_j},L^{D_j}A_j^{B_j})$，则$\{A_j,B_j,D_j\}$是正确的，

否则$\{A_j,B_j,D_j\}$是错误的，用户$U_j(U_j\in w)$可能是骗子。

证明：

$$H(A_j,g^{D_j}y_j^{B_j}\bmod p,L^{D_j}A_j^{B_j}\bmod p)=$$
$$H(A_j,g^{k_j-x_jB_j}y_j^{B_j}\bmod p,L^{k_j-x_jB_j}A_j^{B_j}\bmod p)=$$
$$H(A_j,g^{k_j}g^{-x_jB_j}y_j^{B_j}\bmod p,L^{k_j}L^{-x_jB_j}A_j^{B_j}\bmod p)=$$
$$H(A_j,g^{k_j}y_j^{-B_j}y_j^{B_j}\bmod p,L^{k_j}A_j^{-B_j}A_j^{B_j}\bmod p)=$$
$$H(A_j,g^{k_j}\bmod p,L^{k_j}\bmod p)=B_j$$

证毕。

2.3　讨论与分析

1) 系统中心SC与用户之间的通信不需安全信道。从方案的工作过程中可知，系统中心SC与用户之间没有任何秘密信息且SC并不需知道用户的秘密，因此用户$U_i\in G$只需随机选取密钥x_i，并可将公钥y_i和ID_i通过公开信道发送给系统中心SC。

2) 本文系统与文献[9]一样可高效地增加或删除用户，其他用户不需更改自己的密钥。

2.4　安全性分析

攻击 1　攻击者试图求出签名者的私钥x_0。

若要求出签名者的私钥x_0有两种方法：一种是从$y_0=g^{x_0}\bmod p$求出x_0，该方法将求解离散对数难题；另一种是利用式(4)求出x_0，但式中有3个未知变量，且求出变量r与k，将同时求解离散对数与单向Hash函数求逆难题。

攻击 2　本文方案中用户的密钥x_j可以多次使用，并且系统中心SC和其他用户若从$A_j=L^{x_j}\bmod p=g^{rx_j}\bmod p$或从$D_j=k_j-x_jB_j(\bmod p)$求出$x_j$，即需求解离散对数问题和方程多解问题。若$U_j$在下一次恢复中选用相同的随机数$k_j$，攻击者可通过同余方程组$D_j=k_j-x_jB_j(\bmod p)$和$D_j'=k_j-x_jB_j'(\bmod p)$求出$x_j$，但由于$k_j$是$Z_p^*$均匀随机选择的，在有限次数内出现相同的概率可以忽略不计。

攻击 3　对于任一要恢复的消息M，$G'=\{U_1,U_2,\cdots,U_n\}$中小于$t$个用户联合不可能恢复消息$M$。

恢复消息M有两种途径：一种是用拉格朗日插值公式重构多项式$f(x)$，然后用式(11)恢复消M，然而从文献[9]中可知攻击是不可能成功的；另一种是设法求出$H(v^k\bmod p)$的值，然后利用式(2)恢复消息M，若要求出$H(v^k\bmod p)$的值，攻击者必须知道v与k的值，然而攻击者不可能从式(3)或(4)求出k值，也不可能从$v=L^{f(0)}\bmod p$求出，因少于t 个合作者不可能重构多项式$f(x)$。

3　结　论

本文设计的动态共享认证加密方案，优点在于用户的密钥由自己选择，系统中心不需向用户传送任何秘密信息；当有用户加入或删除时，其他用户不需更改自己的密钥；签名者可根据签名消息的重要性，动态确定验证组中参与验证的门限t值。

参　考　文　献

[1] NYBERG K, RUEPPEL R A . A new signature scheme based on the DSA giving message recovery: Proceeding of the First ACM Conf on computer and communications security[R]. New York: ACM, 1993.

[2] TSAI J L. Convertible multi-authenticated encryption scheme with one-way hash function[J]. Computer Communications, 2009, 32(5), 783-786.

[3] LEE W B, CHANG C C, YANG W P. Authenticated encryption schemes without using a one way function[J]. Electron Letter, 1995, 31(19): 1656-1657.

[4] WU T S, HSU C L, TSAI K Y, et al. Convertible multi-authenticated encryption scheme[J]. Information Sciences, 2008, 178(1), 256-263.

[5] HSU C L, WU, T C . Authenticated encryption schemes with (t,n) shared verification[J]. IEE Proceeding Computer Digital Technique, 1998, 145(2): 117-120.

[6] HWANG S J, LIAO H C. Security of HSU-WU's authenticated encryption scheme with (*t*,*n*) shared veification[J]. Applied Mathematics and Computation, 2005, 167(8): 281-285.

[7] 黄东平, 王华勇, 黄连生, 等.动态门限秘密共享方案[J]. 清华大学学报(自然科学版), 2006, 46(1): 102-105.
HUANG Dong-ping, WANG Huan-yong, HUANG Lian-shen, et al. Dynamic threshold secret sharing scheme[J]. Journal of Tsinghua University (Science and Technology), 2006, 46(1): 102-105.

[8] 甘元驹, 谢仕义, 付东洋, 等. 防欺诈的广义多秘密分享方案[J]. 电子科技大学学报, 2008, 37(1): 68-69.
GAN Yuan-ju, XIE Shi-yi, FU Dong-yang, et al. A general multi-secret sharing scheme for cheat-proof[J]. Journal of University of Electronic Science and Technology of China, 2008, 37(1): 68-69.

[9] 甘元驹, 谢仕义,付东洋. 防欺诈的动态(*t*,*n*)门限多秘密共享方案[J]. 四川大学学报(工程科学版), 2006, 38(6), 131-134.
GAN Yuan-ju, XIE Shi-yi, FU Dong-yang. A cheat proof dynamic (*t*,*n*) threshold multisecret sharing scheme[J]. Journal of Sichuan University (Engineering Science Edition), 2006, 38(6), 131-134.

[10] 甘元驹, 彭银桥, 施荣华. 具有消息链接的可转换的认证加密方案[J].浙江大学学报(理学版), 2004, 31(5): 535-537.
GAN Yuan-ju, PENG Yin-qiao, SHI Rong-hua. Convertible authenticated encryption scheme with message linkages[J]. Journal of Zhejiang University (Sciences Edition), 2004, 31(5): 535-537.

编　辑　张　俊