可证明安全的无中心授权的多授权属性签名

孙昌霞[1,2]，马文平[1]，陈和风[1]

(1. 西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071; 2. 河南农业大学信息与管理科学学院 郑州 450002)

【摘要】设计了无需中心授权机构的多授权签名方案，将用户的多个属性由不同的授权机构分别管理。与往常的多授权机构密码体制不同，不需要一个可信的中心授权机构来管理和约束多个授权机构，而是可信授权机构的数量达到一定值就能保证整个系统的安全性，提高了系统的实用性。采用归约的可安全证明方法证明该方案的安全性归约为计算Diffie-Hellman难题、分布式密钥生成协议(DKG)和联合的零秘密共享协议(JZSS)的安全性，从而说明该方案有存在性、不可伪造和抗合谋攻击的安全特性。

关 键 词 基于属性; CDH难题; 中心授权机构; 合谋攻击; 多授权机构

中图分类号 TP309 **文献标识码** A doi:10.3969/j.issn.1001-0548.2012.04.014

Provable Secure Multi-Authority Attribute-Based Signature without a Central Authority

SUN Chang-xia[1,2], MA Wen-ping[1], and CHEN He-feng[1]

(1. Key Laboratory of Network and Information of Education, Xidian University Xi'an 710071;

2. College of Information and Management Science, Henan Agricultural University Zhengzhou 450002)

Abstract In attribute-based cryptosystem, many attributes of a user were monitored by a single authority, which would inevitably increase its workload and reduce its efficiency. In this paper, a multi-authority signature scheme without a central authority is proposed. In this scheme, many attributes of a user are monitored by many different authorities respectively, in stead of a trusted central authority. The scheme increases the system's applicability. The security of this scheme is proved equal to computational Diffie-Hellman (CDH) problem. So the scheme has two characteristics of existential unforgeability and security preventing collusion attack.

Key words attribute-based; CDH/problem; central authority; collusion attack; multi-authority

基于属性的数字签名(ABS)由基于模糊身份加密体制[1]的概念发展而来，签名者可以声称签名对应于一组特定的属性或某种特定访问结构[2]，验证者可以检验签名是否由相应的属性或访问结构拥有者签的名，基于属性的数字签名机制直观且灵活，能细粒度地划分身份特征，从而引起了广大学者的关注，相继出现了很多的签名方案[3-8]。但这些方案都是属于单个授权机构的基于属性的签名方案，用户的多个属性需向单个授权机构获得签名私钥，单个授权机构需要管理大量属性，会大大增加其工作负担，降低其工作效率，在现实生活中也不现实。事实上，如驾驶执照号码由授权机构机动车辆管理局统一发放管理，身份证号码由公安局身份证办理机构管理等。文献[9]提出了多授权机构的概念，并给出了一个多授权机构的基于属性的加密方案(MA-ABE)，用户的多个属性由不同的授权机构监管，分别对其中的每个属性产生加密私钥。但该方案中的多个授权机构需要一个诚实可信的中心授权机构来统一管理与监督，一旦诚实可信的中心授权机构被攻破，整个系统就会被攻破，大大限制了整个系统的安全性和实用性。文献[10]利用分布式密钥生成技术(DKG)[11]和联合的零秘密共享技术(JZSS)[12]成功地将中心授权机构移除，使多授权机构体制的安全性不再只依赖一个诚实可信的中心授权机构，从而提高了系统安全性和实用性。

文献[5]提出了多授权机构的属性签名(MA-ABS)的概念，并对MA-ABS的过程进行了定义，但没有提出具体的构造方案。文献[13]只是简单地提出方案构造，没有提供完整的可证明安全的过程。文献[14]提出了一个多授权机构的基于属性的签名方

收稿日期：2011 – 06 – 03; 修回日期：2011 – 11 – 30
基金项目：国家自然科学基金(61072140)；高等学校创新引智计划(B08038)
作者简介：孙昌霞(1977 –)，女，博士生，主要从事数字签名和可证明安全理论方面的研究.

案，进行了有关正确性和安全性的分析，但缺乏完整的可证明安全的过程。该文献利用文献[10]使用的DKG技术和JZSS技术，构造了一个无需中心授权机构的多授权签名方案，并给出了完整的可证明安全的过程，即用规约法证明此方案是安全的，能抵抗适应性选择明文的存在性伪造攻击；同时该方案仍具有抗合谋攻击的特性。

1　预备知识

1.1　双线性对

定义 1　设G_1、G_2是阶为素数p的循环群，g是群G_1的生成元，映射$e:G_1\times G_1\to G_2$为一个双线性对，当且仅当e满足以下性质：

1) 双线性。对于任意的$g_1,g_2\in G_1$和$a,b\in Z$，都有$e(g_1^{\,a},g_2^{\,b})=e(g_1,g_2)^{ab}$；

2) 非退化性。对于生成元g，有$e(g,g)\neq 1$，1是G_2中的单位元；

3) 可计算性。存在一个有效的算法，对任意的$g_1,g_2\in G_1$，可以计算$e(g_1,g_2)$的值。

1.2　计算Diffie-Hellman问题

定义 2　计算Diffie-Hellman(CDH)问题：设G_1是阶为素数p的循环群，g是群G_1的生成元，对任意的$a,b\in Z_p^{\,*}$，已知$g,g^a,g^b\in G_1$，计算g^{ab}。

如果没有能在运算时间t内以不可忽略的概率ε解决群G_1上CDH问题的算法，则称CDH问题在群G_1中是困难的。

2　签名方案的构造

设方案有n个授权机构，利用DKG协议和JZSS协议将可信的中心授权机构移除，但要求必须至少有$t+1$个授权机构是可信的，其中要求$t\leqslant n/2$。文献[10-12]介绍了有关DKG和JZSS的详细知识，在此本文只简单介绍两个协议及其在本文方案中所起的作用。在DKG中，有随机值δ的一个(t,n)秘密共享方案，多个参与者$P_k(k=1,2,\cdots,n)$获得相应的私钥块δ_k，即$(\delta_1,\delta_2,\cdots,\delta_n)\xrightarrow{(t,n)}\delta$，若$g^{\delta}$已知，则只有$t+1$可信的参与者合作才能重建密钥$\delta$。JZSS与DKG相似，是值为0的一个$(t,n)$秘密共享方案，同样至少有$t+1$可信的参与者合作才能重建0值。本文方案中，系统私钥a_0由执行一次DKG协议产生，任何授权机构$\mathrm{AA}_k(k=1,2,\cdots,n)$都不知道$a_0$，每个授权机构拥有$a_0$相应的私钥块$a_{k,0}$，为生成多项式$a_{k,0}+a_{k,1}x+\cdots+a_{k,m}x^m$的其他系数$a_{k,j}$，$k=1,2,\cdots,n$，$j=1,2,\cdots,m$，需要执行$m$次JZSS来确定，并且能保证$(a_{1,j},a_{2,j},\cdots,a_{n,j})_{j=1,2,\cdots,m}$是0的$m$个$(t,n)$秘密共享方案所对应的随机多项式的各个系数，再执行一次DKG协议产生系统私钥b_0，使下式成立：

$$a_0=\sum_{l=1}^{l=t+1}a_{k_l,0}\gamma_{k_l}\qquad b_0=\sum_{l=1}^{l=t+1}b_{k_l,m+1}\gamma_{k_l}$$

$$0=\sum_{l=1}^{l=t+1}a_{k_l,j}\gamma_{k_l}\qquad j=1,2,\cdots,m$$

同样，3个式子都表明如果要重建a_0、b_0和0，都至少需要$t+1$个可信的授权机构的合作才能完成。

本文提出的全域[1]属性范围内的签名方案的构造过程如下：

1) 系统建立算法。阶为素数的群G_1,G_2，线性映射$e:G_1\times G_1\to G_2$，生成元$g\in G_1$，多个授权机构AA_k分别管理各自的n_k+1个属性，$N=\{1,2,\cdots,n_k+1\}$。AA_k随机选择$t_{k,1},t_{k,2},\cdots,t_{k,n_k+1}\in G_1$，且公开。定义$T_k(x)=g_2^{\,x^{n_k}}\prod_{i=1}^{n_k+1}t_{k,n_k+1}^{\Delta_{i,(1,2,\cdots,n_k+1)}(x)}$，哈希函数$H$:$\{0,1\}^*\to G_1$。

执行2次DKG和m次JZSS，产生系统私钥a_0和b_0，且公开g_1和g_2，其中$g_1=g^{a_0},g_2=g^{b_0}$，设$z=e(g_1,g_2)$。对于每个授权机构AA_k的私钥SK_k为$\langle a_{k,0},a_{k,1},a_{k,2},\cdots,a_{k,m},b_{k,m+1}\rangle$，所有授权机构产生的私钥为$\mathrm{SK}=\langle\mathrm{SK}_1,\mathrm{SK}_2,\cdots,\mathrm{SK}_n\rangle$，公共参数$\mathrm{PK}=\langle g,g_1,g_2,\{t_{k,1},t_{k,2},\cdots,t_{k,n_k+1}\}_{k=1,2,\cdots,n}\rangle$。

2) 密钥生成算法。用户u为自己随机选择全局身份标识GID，作用是防止合谋攻击，要求不同的用户的GID是不同的。每个授权机构随机选择多项式q_k，使其满足$q_k(0)=a_{k,0}+a_{k,1}\mathrm{GID}+\cdots+a_{k,m}\mathrm{GID}^m$，用户$u$的属性集合$\omega_u^{\,k}$中的每个属性对应的私钥为$D_u=\langle\{g_2^{\,q_k(i)}T_k(j)^{r_i}\}_{i\in\omega_u^{\,k}},\{g^{r_i}\}_{i\in\omega_u^{\,k}}\rangle_{k=1,2,\cdots,n}$，其中随机选择$r_i\in z_p$。

3) 签名算法。用户u选择签名属性集合$S_k\subseteq\omega_k$，$|S_k|=d_k$，d_k是事先设定的各个授权机构的门限值。设$\Delta_{i,s_k}(0)$是签名属性集合S_k中$\{1,2,\cdots,d_k\}$拉格朗日插值多项式的系数，$\Delta_{k,S}(0)$是集合$\{1,2,\cdots,t+1\}$拉格朗日插值多项式的系数，用户u对消息M产生的签名为：

$$\sigma=\langle S_k,\prod_{k=1}^{k=t+1}\Big(\prod_{i\in S_k}g_2^{\,q_k(i)}T_k(i)^{r_i}\Big)^{\Delta_{i,s_k}(0)}\Big)^{\Delta_{k,S}(0)}H(M)^s,$$

$$((g^{r_i})^{\Delta_{i,s_k}(0)})^{\Delta_{k,S}(0)},g^s\rangle_{i\in S_k}$$

其中，随机选择$s\in z_p$。

4) 验证算法。由签名结果可以设：

$$\sigma_1=\prod_{k=1}^{k=t+1}(\prod_{i\in S_k}(g_2^{q_k(i)}T_k(i)^{r_i})^{\Delta_{i,S_k}(0)})^{\Delta_{k,S}(0)}H(M)^s$$

$$\sigma_2=((g^{r_i})^{\Delta_{i,S_k}(0)})^{\Delta_{k,S}(0)}$$

$$\sigma_3=g^s \qquad i\in S_k$$

已知消息 M 及签名属性集合 S_k，验证等式 $e(g,\sigma_1)=z\prod_{k=1}^{k=t+1}(\prod_{i\in S_k}(e(T_k(i),\sigma_2))e(H(M),\sigma_3)$ 是否成立。如果成立则接受；否则拒绝。

3 安全性与性能

3.1 正确性

验证算法中等式成立的条件是签名者的签名属性集合 S_k 中已知足够多的 d_k 个点 $q_k(i)$，从而最终递归地恢复出 $q_k(0)=y_{k,u}$，同时对于多个授权机构，至少需要 $t+1$ 个可信的授权机构参与，利用DKG和JZSS才能恢复出 a_0。由拉格朗日插值多项式的性质可得：

$$q_k(0)=\sum_{i\in s_k}q_k(i)\Delta_{i,s_k}(0)$$

其中

$$\Delta_{i,s_k}(0)=\prod_{j\in s_k,j\neq i}\frac{j}{j-i}$$

具体推导过程如下：

$$\frac{e(g,\sigma_1)}{\prod_{k=1}^{k=t+1}(\prod_{i\in S_k}(e(T_k(i),\sigma_2))e(H(m),\sigma_3)}=$$

$$e(g,\prod_{k=1}^{k=t+1}(g_2^{a_{k,0}+a_{k,1}\mathrm{GID}+\cdots+a_{k,m}\mathrm{GID}^m})^{\Delta_{k,S}(0)})=$$

$$e(g,g_2^{\sum_{k=1}^{k=t+1}(a_{k,0}+a_{k,1}\mathrm{GID}+\cdots+a_{k,m}\mathrm{GID}^m)\Delta_{k,S}(0)})=e(g,g_2^{a_0})$$

上式最后一步通过利用执行DKG和JZSS生成的等式 $a_0=\sum_{l=1}^{l=t+1}a_{k_l,0}\gamma_{k_l}$ 和 $0=\sum_{l=1}^{l=t+1}a_{k_l,j}\gamma_{k_l}$ 可得。

3.2 方案安全性

1) 存在性不可伪造。对于一个签名，如果用户不满足各属性授权机构声明的属性结构，无法伪造出存在的签名。在本文的方案中，如果敌方以不可忽略的概率 ε 伪造签名，说明敌方能以不可忽略的概率来解决CDH难题，这是矛盾的，从而该方案具有抗存在性伪造的安全性。

定理 1 如果CDH问题是困难的，DKG协议和JZSS协议是安全的，即使任意 $t-1$ 个授权机构被敌方恶意破坏，本文的方案在自适应选择消息和指定访问结构攻击下存在性不可伪造。

证明：利用规约法证明，假设敌方能以不可忽略的概率优势 ε 伪造签名，表明敌方能解决CDH问题，从而导致矛盾。给定一个CDH问题的实例 $a=a_0,b=b_0,A=g_1=g^{a_0},B=g_2=g^{b_0}$，$z=(g_1,g_2)$，已知 (g,g^a,g^b)，敌方为了计算 g^{ab}，其模拟挑战者达到伪造签名的过程如下：

① 系统建立的模拟。挑战的属性集合是 ω_k^*。已知 A,B 作为公钥参数。考虑最坏的情况，假设敌方已控制 $t-1$ 个授权机构，已被攻破授权机构的集合是 $\phi=\{\mathrm{AA}_1,\mathrm{AA}_2,\cdots,\mathrm{AA}_{t-1}\}$,，可信授权机构的集合是 $\varphi=\{\mathrm{AA}_t,\cdots,\mathrm{AA}_n\}$。

② 随机预言机的模拟。挑战者可以最多询问 q_H 次随机预言机 H，并保存随机预言机 H 的询问结果列表 L，随机选择整数 $\lambda\in[1,q_H]$，M_v 是要询问随机预言机 H 的消息，挑战者检查列表 L，并执行下面操作：如果询问的消息 M_v 能在列表 L 中找到，挑战者则将消息对应的相同的回答返回给敌方。否则，挑战者会进行两种选择：若 $v\neq\lambda$，挑战者随机选择 α_v，$\beta_v\in Z_p$，$H(M_v)=g_1^{\alpha_v}g^{\beta_v}$；若 $v=\lambda$，挑战者随机选择 $\beta_v\in Z_p$，$H(M_v)=g^{\beta_v}$。

③ 密钥生成算法的模拟。敌方进行私钥询问的多个属性集合是 ξ_k，前提条件是 $|\xi_k\cap\omega_k^*|<d_k$。对于 $\mathrm{AA}_k\in\phi$，即授权机构 AA_k 已被攻破，敌方通过模拟DKG和JZSS协议，获得 $a_{k,0},a_{k,1},a_{k,2},\cdots,a_{k,m}$，$b_{k,m+1},k\in\{1,2,\cdots,t-1\}$，表明敌方能模拟 $t-1$ 个已攻破的授权机构的私钥。由于 $y_{k,u}=q_k(0)=a_{k,0}+a_{k,1}\mathrm{GID}+\cdots+a_{k,m}\mathrm{GID}^m$，则用户的签名私钥为 $D_u^k=\langle g_2^{q_k(i)}T_k(j)^{r_i},g^{r_i}\rangle$；而对于 $\mathrm{AA}_k\in\varphi$，且 $|\xi_k\cap\omega_k^*|<d_k$。由于至少有t+1个可信授权机构能保证签名的顺利完成，允许敌方能获得 φ 中的一个授权机构 $\mathrm{AA}_{\bar{k}}$ 的私钥：随机选择 $y_{\bar{k},u}\in Z_p$ 使 $q_{\bar{k}}(0)=y_{\bar{k},u}$。随机多项式 $q_{\bar{k}}$ 并满足 $q_{\bar{k}}(0)=y_{\bar{k},u}$，则用户的签名私钥是 $D_u^{\bar{k}}=\langle g_2^{q_{\bar{k}}(i)}T_{\bar{k}}(j)^{r_i},g^{r_i}\rangle$。对于 φ 中其他的授权机构，$\mathrm{AA}_{\hat{k}}$ 的签名私钥可以从等式 $a_0=\sum_{l=1}^{l=t+1}a_{k_l,0}\gamma_{k_l}$ 获得：

$$q_{\hat{k}}(0)=\frac{a-\sum_{k\in\{1,2,\cdots,k,\bar{k}\}}(y_{k,u}\gamma_k)}{\gamma_{\hat{k}}}=$$

$$\frac{a-\sum_{k\in\{1,2,\cdots,k,\bar{k}\}}(y_{k,u}\gamma_k)}{\gamma_{\hat{k}}}$$

式中，$\gamma_{\hat{k}}$是集合$\{1,2,\cdots,\hat{k},\bar{k}\}$的拉格朗日多项式的系数。设置3个集合$\Gamma_{\hat{k}}$、$\Gamma'_{\hat{k}}$、$S_{\hat{k}}$，且满足$\Gamma_{\hat{k}}=\xi_{\hat{k}}\cap\omega^*_{\hat{k}},\Gamma^*_{\hat{k}}\subseteq\Gamma'_{\hat{k}}\subseteq\omega_{\hat{k}},\left|\Gamma'_{\hat{k}}\right|=d_{\hat{k}}-1,S_{\hat{k}}=\Gamma'_k\cup\{0\}$。若$i\in\omega^*_{\hat{k}}\setminus\Gamma'_{\hat{k}}$，随机选择$d_{\hat{k}}-1$个点$v_i$，设置$q_{\hat{k}}(i)=v_i$，则用户的签名私钥是$D_u^{\hat{k}}=\langle g_2^{q_k(i)}T_{\hat{k}}(i)^{r_i},g^{r_i}\rangle$，其中随机选择$r_i\in Z_p$。若$i\in\omega^*_{\hat{k}}\setminus\Gamma'_{\hat{k}}$，$q_{\hat{k}}(i)=\Delta_0(i)(q_{\hat{k}}(0)+\sum\Delta_j(i)v_j)$，$\Delta_j(i)$是$q_{\hat{k}}(j)$的拉格朗日系数。用户的签名私钥为：

$$D_u^{\hat{k}}=\langle g_2^{q_k(i)}T_{\hat{k}}(j)^{r_i},g^{r_i}\rangle=$$

$$\langle g_2^{\Delta_0(i)\frac{a-\sum_{k\in\{1,2,\cdots,\hat{k},\bar{k}\}}(y_{k,u}\gamma_k)}{\gamma_{\hat{k}}}+\sum\Delta_j(i)v_j}T_{\hat{k}}(j)^{r_i},g^{r_i}\rangle$$

由此可见，不管用户的属性是属于集合ϕ还是集合φ都能获得签名私钥，且形式都相同，说明敌方能模拟方案中的私钥生成算法。

④ 签名算法的模拟。敌方通过挑战者对多个属性集合ξ_k进行签名询问，前提条件是$\left|\xi_k\cap\omega_k^*\right|<d_k$或者$H(M_v)=g^{\beta_v}$，即消息的随机预言机询问在$[1,q_H]$之中。挑战者对消息的签名模拟为：如果$\left|\xi_k\cap\omega_k^*\right|<d_k$或$H(M_v)=g^{\beta_v}$，可以按照上述签名算法正常签名，有：

$$\sigma=\langle S_k,\prod_{k=1}^{k=t+1}(\prod_{i\in S_k}(g_2^{q_k(i)}T_k(i)^{r_i})^{\Delta_{i,s_k}(0)})^{\Delta_{k,S}(0)}H(M)^s,$$

$$((g^{r_i})^{\Delta_{i,s_k}(0)})^{\Delta_{k,S}(0)},g^s\rangle_{i\in S_k}$$

否则，根据哈希函数的设置，$H(M_v)=g_1^{\alpha_v}g^{\beta_v}$，挑战者的签名主要是为了模拟签名算法两部分$\langle g_2^a\prod_{k=1}^{k=t+1}(\prod_{i\in S_k}(T_k(i)^{r_i})^{\Delta_{i,s_k}(0)})^{\Delta_{k,S}(0)}H(M)^s,g^s\rangle$，随机选择$s'\in Z_p$，使$s=-\frac{1}{\alpha_i}b+s'$，这两部分变成$\langle g_2^{\frac{-\alpha_v}{\beta_v}}\prod_{k=1}^{k=t+1}(\prod_{i\in S_k}(T_k(i)^{r_i})^{\Delta_{i,s_k}(0)})^{\Delta_{k,S}(0)}(g_1^{\alpha_v}g^{\beta_v})^{s'},g_2^{\frac{-1}{\alpha_v}}g^{s'}\rangle$，说明挑战者在两种情况下都能够获得签名，且形式也相同，所以敌方能模拟方案中的签名算法。

⑤签名伪造。敌方输出消息M^*在属性集合ω^*上伪造的签名σ^*。如果满足$\left|\xi_k\cap\omega_k^*\right|>d_k$或者$H(M^*)\neq g^{\beta_\lambda}$就退出；否则，利用上面得到的私钥代入签名算法得到签名$\sigma^*=\langle\sigma_1^*,\sigma_2^*,\sigma_3^*\rangle$，并将其代入验证算法的等式中，即$e(g,\sigma_1^*)=z\prod_{k=1}^{k=t+1}(\prod_{i\in S_k}(e(T_k(i),\sigma_2^*))e(H(M),\sigma_3^*)$，由文献[1]可设$T_k(i)=g^{f_k(i)}$。另外，$H(M^*)=g^{\beta_\lambda}$，则$e(g,\sigma_1^*)=z\prod_{k=1}^{k=t+1}(\prod_{i\in S_k}(e(g,\sigma_2^{*f_k(i)}))e(g,\sigma_3^{*\beta_\lambda})$，进一步得到：

$$g^{ab}=\prod_{k=1}^{k=t+1}(\prod_{i\in S_k}(\frac{\sigma_1^*}{\sigma_2^{*f_k(i)}\sigma_3^{*\beta_\lambda}}))$$

上式表明CDH难题是可以求解的，或者敌方能违反DKG协议和JZSS的私密性，所以该方案是存在性不可伪造安全的。

2) 抗合谋攻击。不同签名者即使合谋也不能伪造出一个其独自不能生成的签名。具有抵抗合谋攻击的安全性是基于属性加密体制的一般要求。该方案采用了与文献[9]相同的方法，不同的签名者通过随机选择GID来实现抗合谋攻击。

3.3　与其他方案的性能比较

与文献[9]方案相比，两者都能容忍$t-1$个授权机构被敌方恶意破坏，但本文的方案无需可信的中心授权机构，需要多个授权机构中可信的授权机构个数达到$t+1(t\leqslant n/2)$，便可保证整个系统的安全性能，所以减少了有关中心授权和各个授权机构的大量通信工作，从而提高系统的工作效率。

与其他基于属性的签名方案[1,4]相比，本文方案有3个优点：1) 签名者只需公开部分属性集合，即$S_k\subseteq\omega_k,|S_k|=d_k$，验证者只知道签名者满足声称的属性门限值$d_k$及签名属性集合，并不确定签名者所拥有的全部属性特征，更获得不了签名者的身份u，较好地保护了签名者的隐私。2) 该算法的签名效率高，签名过程只是群上的指数运算、加法和乘法运算，不需要任何的双线性对的运算。3) 验证算法的效率也有所提高，文献[1,4]是对属性集合中的每个属性进行签名，验证算法进行各个双线性对的连乘运算；而本文的方案是在签名算法中进行连乘运算，在验证算法中大大减少了双线性对的运算次数，从而提高了验证的效率。

4　结　论

本文提出了更实用的多授权机构的签名方案，用户的多个属性由不同的授权机构发放管理，大大缓解了单个授权机构的工作负担，并提高了工作效率，事实证明在现实生活中是可行的。本文设计的方案进一步改进了过去的多授权机构的基于属性的签名方案，不再需要一个可信的中心授权机构，只需一定数量$(t+1,t\leqslant n/2)$授权机构是诚实可信的，同样也能建立安全的多授权机构的签名系统，具有

现实意义；并用规约的研究方法证明了其正确性和安全性，签名和验证效率也有所提高。下一步的研究工作重点在于考虑能否完全保护签名者身份属性的多授权机构的签名方案。

参 考 文 献

[1] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//Advances in Cryptology-EUROCRYPT, 2005. Aarhus: Springer-Verlag, 2005.

[2] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//Proc of CCS. New York, USA: ACM Press, 2006.

[3] GUO S, ZENG Y. Attribute-based signature scheme[C]// Conference of Information Security and Assurance (ISA2008). Xi'an: Xidian University Press, 2008.

[4] SHAHANDASHTI S F, SAFAVI-NAINI R. Threshold attribute-based signatures and their application to anonymous credential systems[C]//AFRICACRPT'2009. Berlin: Springer-Verlag, 2009.

[5] MAJI H, PRABHAKARAN M, ROSULEK M. Attribute-based signatures: Achieving attribute-privacy and collusion-resistance[R/OL]. [2008-05-11]. Cryptology ePrint Archive, Report 2008/328. http://eprint.iacr.org/2008/328 .

[6] KHADER D. Attribute based group signatures[R/OL]. [2007-10-20]. Cryptology ePrint Archive, Report 2007/159. http://eprint.iacr.org/2007/159.

[7] LI J, KIM K. Attribute-based ring signatures[R/OL]. [2008-03-26]. Cryptology ePrint Archive, Report 2008/394. http://eprint.iacr.org/2008/394.

[8] YANG P, CAO Z, DONG X. Fuzzy identity based signature. [R/OL]. [2008-03-26]. Cryptology ePrint Archive, Report 2008/002. http://eprint.iacr.org/2008/002.

[9] CHASE M. Multi-authority attribute based encryption[C]// Lecture Notes in Computer Science of TCC. [S.l.]: Springer-Verlag, 2007.

[10] LIN H, CAO Z, LIANG X, et al. Secure threshold multi authority attribute based encryption without a central authority[J]. Information Sciences, 2010, 180: 2618-2632.

[11] GENNARO R, JARECKI S, KRAWCZYK H, et al. Robust threshold dss signatures[J]. Inform Comput, 2001, 164(1): 54-84.

[12] GENNARO R, JARECKI S, KRAWCZYK H, et al. Secure distributed key generation for discrete-log based cryptosystems[J]. Cryptol, 2007, 20(1): 51-83.

[13] LI J, AU M H. Attribute-based signatures and its applications[C]//ASIACC'10 2010. Beijing, China: ACM, 2010.

[14] 孙昌霞, 马文平, 陈和凤. 多授权中心的基于属性的签名[J]. 四川大学学报(工程科学版), 2011, 43(1): 83-86.
SUN Chang-xia, MA Wen-ping, CHEN He-feng. Multiauthority attribute-based signature[J]. Journal of Sichuan University(Engineering Science Edition), 2011, 43(1): 83-86.

编 辑 黄 莘