属性基门限签名方案及其安全性研究

马春光[1,2],石 岚[1],周长利[1],汪 定[1]
(1.哈尔滨工程大学计算机科学与技术学院,黑龙江哈尔滨 150001;2.网络与数据安全四川省重点实验室,四川成都 611731)

摘 要: 属性基门限签名方案要求用户的身份用一系列的属性来描述,签名者的权力由其所拥有的属性集合决定.验证者通过验证该签名,只能确定该签名者属性集与验签属性集合相同的属性数目超过门限值个,具有保护属性隐私的作用.本文分析了Li等人的灵活门限签名方案,发现其存在签名伪造的安全问题.针对该方案安全性方面的不足,本文设计了一个安全可证的属性基门限签名方案,并基于CDH困难假设,在标准模型下证明了该签名算法的安全性.

关键词: 属性基门限签名方案; 安全性; 标准模型
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2013)05-1012-04
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.05.029

Threshold Attribute-Based Signature and Its Security

MA Chun-guang[1,2], SHI Lan[1], ZHOU Chang-Li[1], WANG Ding[1]
(1. *College of Computer Science and Technology, Harbin Engineering University, Harbin, Heilongjiang* 150001, *China*;
2. *Network and Data Security Key Laboratory of Sichuan Province, Chengdu, Sichuan* 611731, *China*)

Abstract: A threshold attribute-based signature (t-ABS) scheme defines each signer with a set of attributes, which determine signature ability for each signer. In a t-ABS, signature holder prove possession of signatures by revealing only a threshold number of attributes in common with the verification attribute set, hence providing signer-attribute privacy for the signers. In this paper, we analyze a flexiblethreshold ABS proposed by Li et al and demonstrate its vulnerability to forgeable attacks. Finally, we introduce a t-ABS scheme, which is proved to be secure in the standard model based on CDH problem.

Key words: threshold attribute-based signature; security; standard model

1 引言

Sahai[1]等人在2005年欧密会上提出了一个模糊身份加密体制(Identity-Based Encryption, IBE),并给出了基于属性的门限加密体制,该体制可以看作是第一个属性基密码系统的雏形.属性基加密方案(Attribute-Based Encryption, ABE)是IBE方案的一个扩展,在这种体制中用户的身份信息用一系列的属性来表示而不是用单个的身份串来描述.在ABE方案中,密钥和密文分别对应于一个访问结构和一个属性集合,解密者当且仅当能够满足访问结构时才能获得明文.

受ABE体制的启发,Maji[2]等人第一次提出属性基签名(Attribute-Based Signature, ABS)的概念.最初的ABS方案[3,4]是一类模糊身份基签名方案,并没有考虑到用户的属性隐私性[5].现在的ABS体制要求用户从属性中心获得一组属性私钥,然后用这组属性私钥进行签名.签名者的权力由其所拥有的属性集合决定.验证者通过验证该签名,只能确定该签名满足某个访问结构,但是不知道签名者是如何满足这个访问结构的,更不知道签名者的身份,所以其为签名者提供了一定的隐私保护性.ABS与群签名[6]、环签名[7]密码原型结合分别形成了属性基群签名[8],属性基环签名[5].最近,Shahandashti[9]等人提出属性基门限签名(Threshold Attribute-Based Signature, t-ABS)概念,在t-ABS中签名者属性集合与验签属性集合相同的属性至少为门限值个才能生成正确的签名.此后t-ABS方案相继被提出[10,11].本文对文献[10]中灵活门限ABS方案的安全性问题进行研究,指出该方案在安全性方面的不足,并设计了一个安全可证的t-ABS方案.基于CDH困难假设,在标准模型下证明了该签名算法的安全性.

收稿日期:2012-05-14;修回日期:2012-10-12
基金项目:国家自然科学基金(No.61170241);黑龙江省自然科学面上项目(No.F201229);网络与数据安全四川省重点实验室开放课题基金;哈尔滨市科技创新人才研究专项资金(No.2012RFXXG086)

2 Li 等人的签名方案安全性弱点分析

2.1 Li 等人签名方案介绍

首先,简要介绍 Li 的签名方案.

Setup 选择默认属性集合 $\Omega=\{\Omega_1,\Omega_2,\cdots,\Omega_{d-1}\}$.选择 $g\in G_1, x\in Z_p^*$ 并使 $g_1=g^x$.设置 $Z=e(g_1,g_2)$,其中 $g_2\in G_1$.随机选两个哈希函数 $H_1,H_2:\{0,1\}^*\rightarrow G_1$.系统公钥为 $PK=(g,g_1,g_2,Z,d,H_1,H_2)$,主密钥 $MK=x$.

Extract 生成属性集合 ω 的私钥.随机选择一个 $(d-1)$次多项式 $q(y)$,令 $q(0)=x$.设集合 $\hat{\omega}=\omega\cup\Omega$.对于每个 $i\in\hat{\omega}$,随机选择 $r_i\in Z_p$.用户私钥 SK 为 $\{D_i=(d_{i0},d_{i1})\}_{\forall i\in\hat{\omega}}$,其中 $d_{i0}=g_2^{q(i)}\cdot H_1(i)^{r_i}, d_{i1}=g^{r_i}$.

Sign 假设属性集合 ω 满足签名断言 $\Upsilon_{k,\omega^*}(\cdot)$,即集合 ω 和集合 ω^* 至少有 k 个相同的元素,对消息 m 进行签名.选择 k 元集合 $\omega'\subseteq\omega\cap\omega^*$ 和默认属性集合的一个子集 $\Omega'\subseteq\Omega$,使 $|\Omega'|=d-k$.对于每个 $i\in\omega^*\cup\Omega'$,随机选择 $n+d-k$ 个 $r_i'\in\mathbb{Z}_p$.生成签名为 $\sigma=(\sigma_0,\{\sigma_i\}_{i\in\omega^*\cup\Omega'},\sigma_0')$,其中 $\sigma_0=[\prod_{i\in\omega'\cup\Omega'}d_{i0}^{\Delta_{i,S}(0)}][\prod_{i\in\omega^*\cup\Omega'}H_1(i)^{r_i'}]H_2(m)^s$,当 $i\in\omega'\cup\Omega'$ 时,$\{\sigma_i=d_{i1}^{\Delta_{i,S}(0)}g^{r_i'}\}_{i\in\omega'\cup\Omega'}$,当 $i\in\omega^*/\omega'$ 时,$\{\sigma_i=g^{r_i'}\}_{\omega^*/\omega'}$,$\sigma_0'=g^s$.

Verify 验证下面等式是否成立.

$$\frac{e(g,\sigma_0)}{[\prod_{i\in\omega^*\cup\Omega'}e(H_1(i),\sigma_i)]e(H_2(m),\sigma_0')}=Z \quad (1)$$

如果成立,则认证成功,否则失败.

2.2 对 Li 等人的签名方案的安全性分析

假设存在用户属性集合为 ω,存在断言为 $\Upsilon_{k,\omega^*}(\cdot)$的消息 m,并满足有 $|\omega\cap\omega^*|=\varnothing$,下来将论证用户能伪造一个有效的签名.首先执行 Setup 算法,系统输出公钥为 $PK=(g,g_1,g_2,Z,d,H_1,H_2)$,$Z=e(g_1,g_2)$系统保留主密钥为 $MK=x$.然后系统执行 Extract 算法,(1)选择 $d-1$ 阶多项式 $q(y)$,并使 $q(0)=x$.(2)假设 $\hat{\omega}=\omega\cup\Omega=\{A,B,C,D,\cdots\}$则生成私钥为 $D_A=\{d_{A0}=g_2^{q(A)}\cdot H_A^{r_A}, d_{A1}=g^{r_A}\}$, $D_B=\{d_{B0}=g_2^{q(B)}\cdot H_B^{r_B}, d_{B1}=g^{r_B}\}$, $D_C=\{d_{C0}=g_2^{q(C)}\cdot H_C^{r_C}, d_{C1}=g^{r_C}\}$, $D_D=\{d_{D0}=g_2^{q(D)}\cdot H_D^{r_D}, d_{D1}=g^{r_D}\}$等.注意用户只拥有自己的私钥,而不知道主密钥.

接着选择集合:$S_1=\{A,B,\cdots\}$, $S_2=\{A,C,\cdots\}$, $S_3=\{A,D,\cdots\}$, $S_4=\{B,C,\cdots\}$, $S_5=\{B,D,\cdots\}$,在这些集合中省略的元素都相同.对每个集合计算 $\prod_{i\in S}d_{i0}^{\Delta_{i,S}(0)}$,则得到结果:

$$\begin{aligned}
X_1&=\prod_{i\in S_1}d_{i0}^{\Delta_{i,S_1}(0)}=g_2^xH_A^{r_A\Delta_{AS_1}}H_B^{r_B\Delta_{BS_1}}\cdots\\
X_2&=\prod_{i\in S_2}d_{i0}^{\Delta_{i,S_2}(0)}=g_2^xH_A^{r_A\Delta_{AS_2}}H_C^{r_C\Delta_{CS_2}}\cdots\\
X_3&=\prod_{i\in S_3}d_{i0}^{\Delta_{i,S_3}(0)}=g_2^xH_A^{r_A\Delta_{AS_3}}H_D^{r_D\Delta_{DS_3}}\cdots\\
X_4&=\prod_{i\in S_4}d_{i0}^{\Delta_{i,S_4}(0)}=g_2^xH_B^{r_B\Delta_{BS_4}}H_C^{r_C\Delta_{CS_4}}\cdots\\
X_5&=\prod_{i\in S_5}d_{i0}^{\Delta_{i,S_5}(0)}=g_2^xH_B^{r_B\Delta_{BS_5}}H_D^{r_D\Delta_{DS_5}}\cdots
\end{aligned} \quad (2)$$

对上述结果进行运算,可得到如下值.

$$\begin{aligned}
Y_1&=X_1/X_2=H_A^{r_A\Delta_{AS_{12}}}H_B^{r_B\Delta_{BS_1}}H_C^{-r_C\Delta_{CS_2}}\cdots\\
Y_2&=X_1/X_3=H_A^{r_A\Delta_{AS_{13}}}H_B^{r_B\Delta_{BS_1}}H_D^{-r_D\Delta_{DS_3}}\cdots\\
Y_3&=X_1/X_4=H_A^{r_A\Delta_{AS_1}}H_B^{r_B\Delta_{BS_{14}}}H_C^{-r_C\Delta_{CS_4}}\cdots\\
Y_4&=X_1/X_5=H_A^{r_A\Delta_{AS_1}}H_B^{r_B\Delta_{BS_{15}}}H_D^{-r_D\Delta_{DS_5}}\cdots
\end{aligned} \quad (3)$$

为了证明过程清晰,我们设置符号 $\Delta_1=\Delta_{AS_{12}}\cdot\Delta_{CS_4}-\Delta_{AS_1}\cdot\Delta_{CS_2}$, $\Delta_2=\Delta_{BS_1}\cdot\Delta_{CS_4}-\Delta_{BS_{14}}\cdot\Delta_{CS_2}$, $\Delta_3=\Delta_{AS_{13}}\cdot\Delta_{DS_5}-\Delta_{AS_1}\cdot\Delta_{DS_3}$, $\Delta_4=\Delta_{BS_1}\cdot\Delta_{DS_5}-\Delta_{BS_{15}}\cdot\Delta_{DS_3}$, $\Delta_5=\Delta_1\cdot\Delta_4-\Delta_2\cdot\Delta_3$.

最后我们可以计算得出:

$$\begin{aligned}
Z_1&=\frac{Y_1^{\Delta_{CS_4}}}{Y_3^{\Delta_{CS_2}}}=\frac{(H_A^{r_A\Delta_{AS_{12}}}H_B^{r_B\Delta_{BS_1}}H_C^{-r_C\Delta_{CS_2}}\cdots)^{\Delta_{CS_4}}}{(H_A^{r_A\Delta_{AS_1}}H_B^{r_B\Delta_{BS_{14}}}H_C^{-r_C\Delta_{CS_4}}\cdots)^{\Delta_{CS_2}}}\\
&=H_A^{r_A\Delta_1}H_B^{r_B\Delta_2}\cdots\\
Z_2&=\frac{Y_2^{\Delta_{DS_5}}}{Y_4^{\Delta_{DS_3}}}=\frac{H_A^{r_A\Delta_{AS_{13}}}H_B^{r_B\Delta_{BS_1}}H_D^{-r_D\Delta_{DS_3}}\cdots)^{\Delta_{DS_5}}}{(H_A^{r_A\Delta_{AS_1}}H_B^{r_B\Delta_{BS_{15}}}H_D^{-r_D\Delta_{DS_5}}\cdots)^{\Delta_{DS_3}}}\\
&=H_A^{r_A\Delta_3}H_B^{r_B\Delta_4}\cdots\\
Z_3&=\frac{Z_1^{\Delta_4}}{Z_2^{\Delta_2}}=\frac{(H_A^{r_A\Delta_1}H_B^{r_B\Delta_2}\cdots)^{\Delta_4}}{(H_A^{r_A\Delta_3}H_B^{r_B\Delta_4}\cdots)^{\Delta_2}}\\
&=H_A^{r_A(\Delta_1\cdot\Delta_4-\Delta_2\cdot\Delta_3)}\cdots=H_A^{r_A\cdot\Delta_5}\cdots
\end{aligned} \quad (4)$$

由于 $\sigma_A=Z_3^{(\Delta_5)^{-1}}=(H_A^{r_A\cdot\Delta_5}\cdots)^{(\Delta_5)^{-1}}=H_A^{r_A}\cdots$, $\sigma_B=(Z_1/\delta_{A^1}^{\Delta_1})^{(\Delta_2)^{-1}}=H_B^{r_B}\cdots$,可以计算出 $\beta=X_1/\prod_{i\in S_1}(H_i^{r_i})^{\Delta_{iS_1}}=g_2^x$,则该签名者可以构造签名 $\sigma=\{\sigma_0,\{\sigma_i\}_{i\in\omega^*\cup\Omega'},\sigma_0'\}$,其中,对于每个 $i\in\omega^*\cup\Omega'$ 随机 $r_i'\in Z_p$, $\sigma_0=g_2^x\prod_{i\in\omega^*\cup\Omega'}H_i^{r_i'}H_2(m)^s$, $\sigma_i=g^{r_i'}$, $\sigma_0'=g^s$.

签名的正确性很容易验证,有

$$\begin{aligned}
&\frac{e(g,\sigma_0)}{[\prod_{i\in\omega^*\cup\Omega'}e(H_2(i),\sigma_i)]e(H_4(m),\sigma_0')}\\
=&\frac{e(g,g_2^x)\prod_{i\in\omega^*\cup\Omega'}e(g,H_i^{r_i'})e(g,H_4(m)^s)}{\prod_{i\in\omega^*\cup\Omega'}e(H_i,g^{r_i'})e(H_4(m),g^s)}=e(g,g_2^x)=Z
\end{aligned} \quad (5)$$

从上述的认证过程可以看出,即使签名者不满足消息断言也能伪造出一个有效的签名,所以该签名算法是不安全的.

3 新 t-ABS 方案描述

上述中我们可以看出文献[10]中的方案是不安全的.本节我们提出了一个安全的 t-ABE 方案,并在标准模型下证明了其安全性.

3.1 方案构造

Setup 定义 $N=\{1,2,\cdots,n+1\}$ 是默认属性集合. G_1 是循环群,其生成元为 g,阶为素数 p 并在其上定义一个双线性映射 $e: G_1\times G_1\rightarrow G_2$. 定义一个抗碰撞的哈希函数 $H:\{0,1\}^*\rightarrow G_1$. 在 Z_p 中随机选择 $y,t_1,t_2,\cdots t_{n+1}$,并令 $g_1=g^y$, $T_i=g^{t_i}$ 其中 $i\in N$. 从 G_1 随机选择 g_2,h,输出系统公钥为 $mpk=(g,g_1,g_2,T_1,T_2,\cdots,T_{n+1},h,H(\cdot))$,主密钥为 $msk=(y,t_1,t_2,\cdots,t_{n+1})$.

Extract(A, msk) 为属性集合 A 生成私钥. 随机选择一个 $(d-1)$ 次多项式 $q(x)$,令 $q(0)=y$. 对每个 $i\in A$ 在 Z_p 中随机选择 r_i,输出用户私钥 $ssk=(\{g_2^{q(i)/t_i}\cdot H(i)^{r_i/t_i}, g^{r_i}\}_{i\in A})$.

Sign(ssk, m) 对消息 m 进行签名,对于每个 $i\in A$ 在 Z_p 中随机选择 s_i,输出签名为 $\sigma=(A,\{ssk_{1i}, ssk_{2i}(g_1^m\cdot h)^{s_i},(g_1^m\cdot h)^{s_i}\}_{i\in A})$.

Verify(mpk, m, σ, B) 验证对消息 m 的签名,选择集合 $S\subseteq A\cap B$ 使满足 $|S|=d$,并验证下面等式是否成立.

$$\prod_{i\in S}\left(\frac{e(\delta_{1i},T_i)e(H(i),\sigma_{3i})}{e(H(i),\sigma_{2i})}\right)^{\Delta_{i,S}(0)}=e(g_1,g_2) \quad (6)$$

如果成立,则表明认证成功.否则认证失败.

3.2 安全性分析

我们可以很容易的验证该方案的正确性和隐私保护性.接下来证明该方案的不可伪造性.

定义 1 假设 CHD 问题是难解的,该方案在适应性选择消息和身份攻击下是不可伪造的.证明:如果存在敌手 A 能伪造出一个有效的签名,我们可以构造一个算法 B 解决 CDH 难题. B 拥有数组 (g,g^a,g^b),它能通过运行 A 而计算出 g^{ab}.攻击过程如下.

当 B 运行 A 时, A 输出认证属性集合 β 和消息 m. B 设置 $g_1=g^a$ 和 $g_2=g^b$.然后选择一个 n 阶的多项式 $f(x)$和另外一个 n 阶的多项式 $u(x)$,使得对于任何的 $x\in\beta$ 有 $u(x)=-x^n$. 当 $i=1,\cdots,n+1$ 设置 $t_i=u(i)+f(i)$ 和 $T_i=g^{u(i)+f(i)}$. 注意我们有 $H(x)=g_2^{x^n}\cdot g^{u(x)+f(x)}$.实行 Setup 算法后, B 输出公钥 $\mathrm{mpk}=(g,g_1,g_2,T_1,T_2,\cdots,T_{n+1},H(\cdot))$给 A.接下来 A 进行私钥的询问查询.

敌手 A 询问属性集合 α 的私钥,并保证 $|\alpha\cap\beta|<d$. B 定义 $\Gamma=\beta\cap\alpha$ 并选择集合 Γ' 使 $\Gamma\subseteq\Gamma'\subseteq\alpha$ 和 $|\Gamma'|=d-1$.接着 B 设 $S=\Gamma'\cup\{0\}$,并进行如下计算:

对于 $i\in\Gamma'$,在集合 Z_p 中随机选择 r_i 和 λ_i,输出私钥为:

$$ssk_i=(g_2^{\lambda_i/(u(i)+f(i))}H(i)^{r_i/(u(i)+f(i))},g^{r_i}) \quad (7)$$

对于 $i\in\alpha/\Gamma'$,在集合 Z_p 中随机选择 r_i',输出私钥为:

$$\begin{aligned}ssk_{1i}&=(g_1^{\frac{-f(i)}{i^n}}(g_2^{i^n}g^{f(i)+u(i)})^{r_i'})^{\frac{\Delta_{0,S}(i)}{u(i)+f(i)}}\prod_{j\in\Gamma'}g_2^{\frac{\lambda\Delta_{i,S}(i)}{u(i)+f(i)}}\\ ssk_{2i}&=(g_1^{\frac{-1}{i^n}}g^{r_i'})^{\frac{\Delta_{0,S}(i)}{u(i)+f(i)}}\end{aligned} \quad (8)$$

对于 $i\in\Gamma'$,上面输出私钥显然是正确的.接下我们将证明 $i\in\alpha/\Gamma'$,输出的私钥也是正确的.其实通过上面对私钥的模拟,我们已经选择了 $d-1$ 阶的多项式 $q(x)$,使 $i\in\Gamma'$有 $q(i)=\lambda_i$ 并 $q(0)=a$.然后设 $r_i=(r_i'-\frac{a}{i^n})\frac{\Delta_{0,S}(i)}{u(i)+f(i)}$,有如下计算.

$$\begin{aligned}ssk_{1i}&=(g_1^{\frac{-f(i)}{i^n}}(g_2^{i^n}g^{f(i)+u(i)})^{r_i'})^{\frac{\Delta_{0,S}(i)}{u(i)+f(i)}}\prod_{j\in\Gamma'}g_2^{\frac{\lambda\Delta_{j,S}(i)}{u(i)+f(i)}}\\ &=(g_2^{\frac{-af(i)}{i^n}}(g_2^{i^n}g^{f(i)+u(i)})^{r_i'})^{\frac{\Delta_{0,S}(i)}{u(i)+f(i)}}\prod_{j\in\Gamma'}g_2^{\frac{\lambda\Delta_{j,S}(i)}{u(i)+f(i)}}\\ &=(g_2^a(g_2^{i^n}g^{f(i)+u(i)})^{\frac{-a}{i^n}}(g_2^{i^n}g^{f(i)+u(i)})^{r_i'})^{\frac{\Delta_{0,S}(i)}{u(i)+f(i)}}\prod_{j\in\Gamma'}g_2^{\frac{\lambda\Delta_{j,S}(i)}{u(i)+f(i)}}\\ &=(g_2^a(g_2^{i^n}g^{f(i)+u(i)})^{r_i'-\frac{a}{i^n}})^{\frac{\Delta_{0,S}(i)}{u(i)+f(i)}}\prod_{j\in\Gamma'}g_2^{\frac{\lambda\Delta_{j,S}(i)}{u(i)+f(i)}}\\ &=g_2^{\frac{a\Delta_{0,S}(i)}{u(i)+f(i)}}H(i)^{\frac{r_i}{u(i)+f(i)}}\prod_{j\in\Gamma'}g_2^{\frac{\lambda\Delta_{j,S}(i)}{u(i)+f(i)}}\\ &=g_2^{\frac{q(0)\Delta_{0,S}(i)+\sum_{j\in\Gamma'}q(j)\Delta_{j,S}(i)}{u(i)+f(i)}}H(i)^{\frac{r_i}{u(i)+f(i)}}=g_2^{\frac{q(i)}{u(i)+f(i)}}H(i)^{\frac{r_i}{u(i)+f(i)}}\\ ssk_{2i}&=(g_1^{\frac{-1}{i^n}}g^{r_i'})^{\frac{\Delta_{0,S}(i)}{u(i)+f(i)}}=(g^{\frac{-a}{i^n}}g^{r_i'})^{\frac{\Delta_{0,S}(i)}{u(i)+f(i)}}\\ &=g^{(r_i'-\frac{a}{i^n})\frac{\Delta_{0,S}(i)}{u(i)+f(i)}}=g^{r_i}\end{aligned} \quad (9)$$

敌手 A 对消息 $\tilde{m}$ 进行签名的询问,保证 $m\neq\tilde{m}$.

当 $|\alpha\cap\beta|<d$ 时,输出签名 $\sigma=(\{ssk_{1i}, ssk_{2i}(g_1^m\cdot h)^{s_i},(g_1^m\cdot h)^{s_i}\}_{i\in\alpha})$.否则 B 随机选择 $d-1$ 度多项式 $q'(x)$,并使 $q'(0)=\frac{1}{m-\tilde{m}}$.对于所有元素 $i\in\alpha$,在集合 Z_p 中随机选择 s_i' 和 r_i,并生成签名 $\sigma=(\{g_2^{\frac{q(i)}{u(i)+f(i)}}H(i)^{\frac{r_i}{u(i)+f(i)}},g^{r_i}(g_1^m\cdot h)^{s_i'-\frac{1}{m-\tilde{m}}},g^{\frac{-1}{m-\tilde{m}}}g^{s_i'}\}_{i\in\alpha})$.

对于前一种情况, B 生成的签名显然是正确的.我们将证明对于后一种情况生成的签名也是正确的.由于 $m\neq\tilde{m}$,我们定义 $s_i=s_i'-\frac{1}{m-\tilde{m}}$,则上述的签名就可

以表示成 $\sigma = (\{g_2^{\frac{q(i)}{u(i)+f(i)}} H(i)^{\frac{r_i}{u(i)+f(i)}}, g^{r_i}(g_1^m \cdot h)^{s_i}, g^{s_i}\}_{i\in a})$.

最后,敌手 A 生成一个有效的伪造签名 $\tilde{\delta}$,由于签名是有效的,则如下公式成立.

$$\prod_{i\in B}\left(\frac{e(\sigma_{1i}, T_i)e(H(i), \sigma_{3i})}{e(H(i), \sigma_{2i})}\right)^{\Delta_{i,B}(0)} = e(g_1, g_2) \quad (10)$$

上面的公式又可以写成

$$\prod\left(\frac{e(\sigma_{1i}, g^{u(i)+f(i)})e(g^{(b-1)i^n+f(i)}, \sigma_{3i})}{e(g^{(b-1)i^n+f(i)}, \sigma_{2i})}\right) = e(g^{ab}, g) \quad (11)$$

则 B 可以通过下面的计算求出 g^{ab},解决 CDH 难题.

$$\prod\left(\frac{\sigma_{1i}^{u(i)+f(i)} \cdot \sigma_{3i}^{(b-1)i^n+f(i)}}{\sigma_{2i}^{(b-1)i^n+f(i)}}\right)^{\Delta_{i,B}(0)} = g^{ab} \quad (12)$$

3.3 效率分析

签名消息进行的指数运算的次数与用户属性集合的大小成线性关系.认证所需的代价主要是进行 d 次线性对运算.公钥中元素的增长随系统默认的属性数目成线性的增长.用户私钥的长度和签名长度都和用户的属性集合的大小成正比.最后,认证阶段参与的运算的元素个数与门限值 d 成正比.

4 结束语

ABS 是近几年密码学研究的热点,本文首先分析了现存的 ABS 方案的安全性方面的不足.针对其安全方面的不足,本文设计了一个安全的 t-ABS 方案,并基于 CDH 困难假设,在标准模型下证明了该签名算法的安全性.在上述的 t-ABS 方案中签名长度与用户的属性集合大小成正比,接下来可以对固定长度的 ABS 方案进行研究.

参考文献

[1] Sahai A, Waters B. Fuzzy identity-based encryption[A]. Advances in Cryptology-EUROCRYPT 2005[C]. Berlin: Springer, 2005. 557 – 557.

[2] Maji H, Prabhakaran M, Rosulek M. Attribute-based signatures: Achieving attribute-privacy and collusion-resistance[DB/OL]. http://www.iacr.org/cryptodb/data/paper.php, 2008 – 03 – 28.

[3] Shaniqng G, Yingpei Z. Attribute-based signature scheme[A]. International Conference on Information Security and Assurance, ISA 2008[C]. USA: IEEE, 2008. 509 – 511.

[4] Yang P, Cao Z, Dong X. Fuzzy identity based signature[DB/OL]. http://eprint.iacr.org/2008/002.pdf, 2008 – 01 – 01.

[5] Li J, Kim K. Attribute-based ring signatures[DB/OL]. http://eprint.iacr.org/2008/394.html, 2011 – 12 – 20.

[6] Chaum D, Van Heyst E. Group signatures[A]. Advances in Cryptology-EUROCRYPT'91[C]. Berlin: Springer, 1991. 257 – 265.

[7] Rivest R, Shamir A, Tauman Y. How to leak a secret[A]. Advances in Cryptology-ASIACRYPT 2001[C]. Berlin: Springer, 2001. 552 – 565.

[8] Khader D. Attribute based group signature with revocation[DB/OL]. http://eprint.iaer.org/2007/241.html, 2009 – 03 – 12.

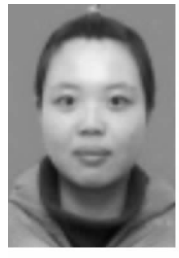
[9] Shahandashti S, Safavi-Naini R. Threshold attribute-based signatures and their application to anonymous credential systems [A]. Progress in Cryptology-AFRICACRYPT 2009 [C]. Berlin: Springer, 2009. 198 – 216.

[10] Li J, Au M H, Susilo W, Xie D, Ren K. Attribute-based signature and its applications[A]. ASIACCS'10 Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security[C]. New York: ACM, 2010. 60 – 69.

[11] 庞辽军,焦李成.无可信中心的可变门限签名方案[J].电子学报,2008,36(8):1559 – 1563.
Pang Liaojun, Jiao Licheng. Changeablethreshold signature scheme without a trusted cente[J]. Acta Electronica Sinica, 2008, 36(8): 1559 – 1563. (in chinese)

作者简介

马春光(通信作者) 男,博士,1974 年生于黑龙江省双鸭山市.哈尔滨工程大学计算机科学与技术学院教授、博士生导师.中国密码学会理事,CCF 高级会员.研究方向为密码学、信息安全、传感网与物联网、网络编码等.
E-mail: machunguang@hrbeu.edu.cn



石　岚 女,1990 年生于湖南省新邵县.哈尔滨工程大学计算机科学与技术学院硕士研究生,研究方向为密码学、信息安全.
E-mail: shilan@hrbeu.edu.cn.