一个改进的动态门限基于属性签名方案

付小晶[1,2] 张国印[1] 马春光[1,2]
(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)[1]
(电子科技大学网络与数据安全四川省重点实验室 成都 611731)[2]

摘 要 分析了一个基于属性签名方案的安全缺陷,并改进了Li等人的基于属性签名方案,从而减少了签名计算代价和签名长度。在随机预言机模型下,利用CDH问题的困难性,证明了改进方案满足在适应性选择消息和断言下的不可伪造性。改进方案还满足签名者属性隐私安全。仿真实验结果表明,改进方案可以较好地应用于移动对等网络数据分发,以实现消息认证。

关键词 基于属性签名,动态门限,签名者属性隐私,随机预言机模型
中图法分类号 TP309 **文献标识码** A

Dynamic Threshold Attributes-based Signature Scheme

FU Xiao-jing[1,2] ZHANG Guo-yin[1] MA Chun-guang[1,2]
(College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)[1]
(Network and Data Security Key Laboratory of Sichuan Province, University of Electronic Science and Technology of China, Chengdu 611731, China)[2]

Abstract Security flaw of an attribute-based signature was pointed out and analyzed firstly, and on the basis of Li's attribute-based signature (ABS), a new efficient ABS was proposed, in which signing cost and signature size are decreased. The proposed ABS is proved secure in the random oracle machine and satisfies existential unforgeability against adaptive chosen message and predicate attack based on the standard computational Diffie-Hellman assumption. Furthermore, it provides attribute-signer privacy. Result of simulation shows that the proposed ABS can be well applied to data dissemination in mobile peer-to-peer network to achieve message authentication.

Keywords Attributes-based signature, Dynamic threshold, Attribute signer-privacy, Random oracle model

1 引言

1984年Shamir等[1]首次提出基于身份密码学(Identity-based Cryptography, IBC)概念,2001年Boneh等[2]利用双线性对提出第一个实用的基于身份加密(Identity-based Encryption, IBE)方案。IBC解决了传统公钥基础设施中公钥证书的复杂性管理问题。2005年,Sahai和Waters[2]基于秘密共享理论,提出了基于模糊身份的加密(Fuzzy IBE)概念。在Fuzzy IBE中,用户的生物信息充当身份,被看作是一个描述属性的集合。Goyal等[4]首次提出了基于属性加密(Attribute-based Encryption, ABE)的概念,并将ABE分成了密钥策略基于属性加密(Key-Policy ABE)和密文策略基于属性加密(Ciphertext-Policy ABE)两种类型。ABE可以看作是一种新型的IBE,不用暴漏用户的身份,任何用户只要它的属性满足指定的访问策略就能够解密消息,可以较好地实现数据细粒度的访问控制。基于属性签名(Attribute-based Signature, ABS)可以验证消息的签名者是否满足所指定的访问策略,保证消息的完整性和来源的真实性。在Fuzzy IBE基础上,出现了一些模糊身份签名方案[5,6],但这些方案都不考虑签名者匿名问题。Khader等[7]提出基于属性群签名方案,签名者保持匿名,并且可由群管理者撤销匿名。Maji等[8,9]提出了支持任何访问结构的ABS方案,其能够保护签名者的属性隐私,但只在一般群模型下证明其安全性。Li和Kim[10]提出第一个标准CDH问题假设下可证安全的(n,n)门限ABS方案,实现了签名者匿名性和属性隐私安全性,但是门限是固定的。之后出现了改进方案[11,12],其支持(k,n)动态门限,并提高了效率。Chen等[13]对Li-Kim方案[10]进行了改进,提出了一个高效的ABS方案,但我们发现Chen方案[13]不能满足不可伪造性,攻击者只要获得一个消息的有效签名就能伪造其他消息的签名。Herranz等[14]提出一个基于属性短签名方案,其支持门限访问结构,但是属性私钥数量和计算代价较大。基于此,本文首先指出Chen方案[13]的缺陷,并且对Li方案[12]进行改进,进一步降低了签名代价和签名长度,并在随机预言机模型下证明其安全性。

到稿日期:2012-09-19 返修日期:2013-02-27 本文受国家自然科学基金(61073042,61170241),中央高校基本科研业务费专项资金(HEUCF100606),2012年黑龙江省教育厅科学技术研究项目资金(12523049),网络与数据安全四川省重点实验室开放课题资金(201107)资助。
付小晶(1980—),女,博士生,主要研究方向为网络与信息安全、密码学,E-mail:fuxiaojing@hrbeu.edu.cn;张国印(1962—),男,博士,教授,主要研究方向为网络与信息安全、嵌入式系统;马春光(1974—),男,博士,教授,主要研究方向为密码学与信息安全、Ad hoc与传感网络安全。

2 预备知识

2.1 双线性对和困难问题假设

定义 1(双线性对) G_1、G_2 是阶为素数 q 的循环群，g 是 G_1 的生成元。双线性对 $\hat{e}: G_1 \times G_1 \to G_2$ 满足以下条件：

(1)双线性(bilinearity)：对于任意 $g_1, g_2 \in G_1$，$a, b \in {}_R Z_q^*$，$\hat{e}(g_1^a, g_2^b) = \hat{e}(g_1, g_2)^{ab}$ 都成立；

(2)非退化性(nondegeneracy)：对于任意 $g_1, g_2 \in G_1$，存在 $\hat{e}(g_1, g_2) \neq 1_{G_2}$，$1_{G_2}$ 是 G_2 的单位元；

(3)可计算性(computable)：对于任意 $g_1, g_2 \in G_1$，存在一种有效的算法计算 $\hat{e}(g_1, g_2) \in G_2$。

定义 2(计算 Diffie-Hellman 问题，CDHP) 对于 $x, y \in {}_R Z_q^*$，已知 $g, g^x, g^y \in G_1$，计算 g^{xy}。

2.2 算法定义

动态门限基于属性签名方案由初始化、私钥生成、签名和验证 4 个算法构成，设属性集为 $U \subset {}_R Z_q^*$，断言 Υ 为 U 上的单调布尔函数，如果属性集 $\omega \subset U$，则 $\Upsilon(\omega) = 1$。

(1)初始化 $Setup(1^\lambda)$

输入安全参数 1^λ，密钥生成中心(PKG)输出参数 $params$ 和系统主密钥 x。公开 $params$，保密 x。

(2)私钥生成 $Extract(\omega)$

给定用户属性集 $\omega \subset U$，PKG 计算用户私钥 sk_ω，返回给用户。

(3)签名 $Sign(\Upsilon, \omega, m)$

利用断言 Υ 和属性集 $\omega' \subset \omega$，$\Upsilon(\omega') = 1$ 的私钥 $sk_{\omega'}$ 对消息 m 签名，返回签名 σ。

(4)验证 $Verify(\Upsilon, param, \sigma)$

利用 $params$ 和断言 Υ 验证消息 m 的签名 σ 是否合法，返回 true 或者 false。如果 $\Upsilon(\omega') = 1$，则 σ 是一个有效的签名，说明签名者的属性集满足断言 Υ。

2.3 形式化安全模型

定义 3(EF-ABS-ACMA 安全) 在概率多项式时间内，如果攻击者 $\mathcal{A}$ 没有以不可忽略的优势在如下游戏中获胜，则称基于属性签名方案在适应性选择消息和断言攻击下具有存在不可伪造性(existential unforgeablility of attribute-based signature against adaptive chosen message and selective-predicate attack，EF-ABS-ACMA)：

初始化：挑战者 $\mathcal{C}$ 运行初始化算法，利用系统安全参数产生公共参数 $params$ 和系统密钥 x。将 $params$ 发布给攻击者 $\mathcal{A}$，x 保密。$\mathcal{A}$ 输出预挑战的断言 Υ。

询问阶段：$\mathcal{A}$ 向 $\mathcal{C}$ 执行以下询问：

(1)Hash 询问：$\mathcal{A}$ 可以询问任意输入的 Hash 值；

(2)私钥生成询问：$\mathcal{A}$ 选择一个属性集 ω_i，$\mathcal{C}$ 根据系统参数 $params$ 和主密钥 x，计算用户私钥 sk_{ω_i}，并将用户私钥 sk_{ω_i} 发送给 $\mathcal{A}$；

(3)签名询问：$\mathcal{A}$ 询问在属性集 ω 和断言 Υ 下的消息 m 的签名，$\mathcal{C}$ 计算 $\sigma = Sign(\Upsilon, \omega, m)$，将签名 σ 发送给 $\mathcal{A}$。

(4)验证询问：$\mathcal{A}$ 请求验证断言 Υ 下的 m 的签名 σ，$\mathcal{C}$ 计算 $Verify(\Upsilon, params, \sigma)$，返回 true 或者 false。

伪造阶段：游戏最后，$\mathcal{A}$ 输出一个新的二元组 (Υ^*, σ^*)，并且 $\omega \subseteq \omega^*$，$\Upsilon^*(\omega) = 1$，在询问阶段没有被执行过私钥生成询问。如果 $Unsigncrypt(\Upsilon^*, params, \sigma^*)$ 没有返回 false，则 $\mathcal{A}$ 在游戏中获胜。定义攻击者 $\mathcal{A}$ 在游戏中获胜的优势为 $Adv(\mathcal{A}) = \Pr[\text{Win}]$。

定义 4(签名者属性隐私安全) 如果给定消息 m，签名属性集合 ω_1, ω_2 和签名断言 Υ 上的签名 σ，且 $\Upsilon(\omega_1) = \Upsilon(\omega_2) = 1$，攻击者 $\mathcal{A}$ 无法区分 ω_1 和 ω_2 中哪个集合用于产生 σ，则称基于属性签名方案满足签名者属性隐私(attribute-signer privacy)安全性。

3 Chen 方案安全性分析

3.1 Chen 方案简述

(1)初始化

设置拉格朗日插值系数 $\Delta_{j,S}(i) = \prod_{k \in S, k \neq j} \frac{i-k}{j-k}$，属性集 $U \subset {}_R Z_q^*$，缺省属性集 $\Omega = \{\Omega_1, \Omega_2, \cdots, \Omega_{d-1}\}$。PKG 选择双线性对 $\hat{e}: G_1 \times G_1 \to G_2$，随机选取 $g, g_2 \in G_1$，$x \in {}_R Z_q^*$，计算 $g_1 = g^x$，$Z = \hat{e}(g_1, g_2)$。选择哈希函数 $H_1, H_2: \{0,1\}^* \to G_1$。公开参数 $params = (g, g_1, g_2, Z, H_1, H_2)$。保密系统主密钥 x。

(2)私钥生成

给定属性集 $\omega \subset U$，令 $\hat{\omega} = \omega \cup \Omega$。PKG 随机选择 $d-1$ 次多项式 $q(y)$，满足 $q(0) = x$。随机选择 $r_i \in {}_R Z_q^*$，计算 $d_{i0} = g_2^{q(i)} H_1(i)^{r_i}$，$d_{i1} = g^{r_i}$。输出私钥为 $D_i = (d_{i0}, d_{i1})$，$i \in \hat{\omega}$。

(3)签名

用属性集 $\omega' = \{i_1, i_2, \cdots, i_k\} \subseteq \omega$，$1 \leqslant k = |\omega'| \leqslant d$ 对消息 m 进行签名。从属性集 Ω 选取 $d-k$ 个缺省属性构成缺省属性集 $\Omega' = \{i_{k+1}, i_{k+2}, \cdots, i_d\} \subseteq \Omega$，随机选择 $r_1', r_2', \cdots, r_d' \in {}_R Z_q^*$ 和 $d-1$ 次多项式 $q'(y)$，满足 $q'(0) = 0$。令 $L = \omega' \cup \Omega'$，计算 $m = H_2(L, M)$，$\sigma_{v1} = d_{i_v 0}^m H_1(i_v)^{r_v'} g_2^{q'(i_v)}$，$\sigma_{v2} = d_{i_v 1}^m g^{r_v'}$，签名为 $\sigma = \{\sigma_{v1}, \sigma_{v2}\}_{1 \leqslant v \leqslant d}$。

(4)验证

输入签名 $\sigma = \{\sigma_{v1}, \sigma_{v2}\}_{1 \leqslant v \leqslant d}$，$\omega' = \{i_1, i_2, \cdots, i_k\} \subseteq \omega$，缺省属性集 $\Omega' = \{i_{k+1}, i_{k+2}, \cdots, i_d\} \subseteq \Omega$，$L = \omega' \cup \Omega'$。计算 $m = H_2(L, M)$，判断等式 $\prod_{k=1}^{v} \left(\frac{\hat{e}(\sigma_{v1}, g)}{\hat{e}(H_1(i_v), \sigma_{v2})}\right)^{\Delta_{i_v, S}(0)} = Z^m$ 是否成立。如果成立，接受签名，否则拒绝签名。

3.2 伪造签名攻击

Chen 方案[13]对 Li-Kim 方案[10]进行了改进，提高了签名效率，但是经分析发现，Chen 方案不满足不可伪造性。在 Chen 方案中，如果攻击者获得消息 M 的一个合法签名 $\sigma = \{\sigma_{v1}, \sigma_{v2}\}_{1 \leqslant v \leqslant d}$，攻击者可以按照下面方法伪造消息 M^* 的签名 σ^*。

计算 $m = H_2(L, M)$，$m^* = H_2(L, M^*)$，随机选择 $s \in {}_R Z_q^*$，计算 $\sigma_{v1}^* = \sigma_{v1}^{m^*/m}$，$\sigma_{v2}^* = \sigma_{v2}^s$，则 $\sigma^* = \{\sigma_{v1}^*, \sigma_{v2}^*\}_{1 \leqslant v \leqslant d}$ 是消息 M^* 的合法签名。因此，Chen 方案不满足不可伪造性。

正确性证明：

$$\prod_{k=1}^{v}\left(\frac{\hat{e}(\sigma_{v1}^{*},g)}{\hat{e}(H_1(i_v),\sigma_{v2}^{*})}\right)^{\Delta_{i_v},S^{(0)}}=\prod_{k=1}^{v}\left(\frac{\hat{e}(\sigma_{v1}^{m^{*}/m},g)}{\hat{e}(H_1(i_v),\sigma_{v2}^{\prime})}\right)^{\Delta_{i_v},S^{(0)}}$$

$$=\prod_{k=1}^{v}\left(\frac{\hat{e}(\sigma_{v1},g)}{\hat{e}(H_1(i_v),\sigma_{v2})}\right)^{\Delta_{i_v},S^{(0)}m^{*}/m}=(Z^{m})^{m^{*}/m}=Z^{m^{*}}$$

4 改进的基于属性签名方案

Li 等在文献[12]中对 Li-Kim 方案[10]进行了改进，减少了签名代价和签名长度。本文将进一步提高签名效率，降低代价。所提 ABS 方案支持包含门限的断言 $\Upsilon_{k,\omega^{*}}()$，$\omega^{*}$ 是用于签名的属性集，k，$1\leqslant k\leqslant d$ 为门限值。$\Upsilon_{k,\omega^{*}}(\omega')=\begin{cases}1, & |\omega'\cap\omega^{*}|\geqslant k\\ 0, & \text{otherwise}\end{cases}$，即当属性集 ω' 包含属性集 ω^{*} 中至少 k 个元素时，称 ω' 满足断言 $\Upsilon_{k,\omega^{*}}()$。签名方案设计如下：

(1)初始化 $Setup(d)$

PKG 选择系统安全参数 $d\in_R Z_q^{*}$，设拉格朗日插值系数 $\Delta_{j,S}(i)=\prod_{k\in S,k\neq j}\frac{i-k}{j-k}$，属性集 $U\subset_R Z_q^{*}$，U 中的元素为属性映射的整数(mod q)。设由 $d-1$ 个属性构成的缺省属性集为 $\Omega=\{\Omega_1,\Omega_2,\cdots,\Omega_{d-1}\}$，$\Omega_i\in_R Z_q^{*}$，$1\leqslant i\leqslant d-1$。选择一个双线性对 $\hat{e}:G_1\times G_1\to G_2$，随机选取 $g,g_2\in G_1$，$x\in_R Z_q^{*}$，计算 $g_1=g^{x}$，$Z=\hat{e}(g_1,g_2)$。选择哈希函数 $H_1,H_2\{0,1\}^{*}\to G_1$。公开参数 $params=(d,q,G_1,G_2,\hat{e},g,g_1,g_2,Z,H_1,H_2)$。保密系统主密钥为 x。

(2)私钥生成 $Extract(\omega_{ID})$

给定用户 ID，其属性集为 $\omega_{ID}\subset U$。PKG 随机选择 $d-1$ 次多项式 $q(y)$，满足 $q(0)=x$。产生一个新的属性集 $\hat{\omega}_{ID}=\omega_{ID}\cup\Omega$，对于任一 $i\in\hat{\omega}_{ID}$，随机选择 $r_i\in_R Z_q^{*}$，计算 $d_{i0}=g_2^{q(i)}H_1(i)^{r_i}$，$d_{i1}=g^{r_i}$。用户的私钥为 $D_i=(d_{i0},d_{i1})$，$i\in\hat{\omega}_{ID}$。

(3)签名 $Sign(\Upsilon_{k,\omega^{*}}(),\omega,m)$

签名者的属性集为 $\omega=\{i_1,i_2,\cdots,i_N\}$，断言为 $\Upsilon_{k,\omega^{*}}()$，$|\omega^{*}|=n$，且 $\gamma_{k,\omega^{*}}(\omega)=1$。选择属性子集 $\omega'\subseteq\omega^{*}\cap\omega$，从属性集 Ω 选取 $d-k$ 个缺省属性构成缺省属性集 $\Omega'=\{i_{k+1},i_{k+2},\cdots,i_d\}\subseteq\Omega$，对于 $r_i\in\omega^{*}\cup\Omega'$，选择 $n+d-k$ 个随机数 $r_i'\in_R Z_q^{*}$。计算 $\sigma_0=[\prod_{i\in\omega'\cup\Omega'}d_{i,0}^{\Delta_{i,s}(0)}][\prod_{i\in\omega^{*}\cup\Omega'}H_1(i)^{r_i'}]H_2(m)^{r_{i_d}'}$，$\{\sigma_i=d_{i1}^{\Delta_{i,s}(0)}g^{r_i'}\}_{i\in\omega'\cup\Omega'}$，$\{\sigma_i=g^{r_i'}\}_{i\in\omega^{*}/\omega'}$，签名为 $\sigma=\{\sigma_0,\{\sigma_i\}_{i\in\omega^{*}\cup\Omega'}\}$。

(4)验证 $Verify(\Upsilon_{k,\omega^{*}}(),param,\sigma)$

验证消息 m 的签名 $\sigma=\{\sigma_0,\{\sigma_i\}_{i\in\omega_1^{*}\cup\Omega_1'}\}$ 的签名者是否满足签名断言 $\Upsilon_{k,\omega_1^{*}}()$。判断

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

是否成立，如果成立则接受消息 m，否则拒绝。

正确性证明：

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

$$\frac{\hat{e}(g,[\prod_{i\in\omega'\cup\Omega'}(g_2^{q(i)}H_1(i)^{r_i})^{\Delta_{i,s}(0)}][\prod_{i\in\omega^{*}\cup\Omega'}H_1(i)^{r_i'}]H_2(m)^{r_{i_d}'})}{[\prod_{i\in\omega'\cup\Omega'}\hat{e}(H_1(i),g^{r_i\Delta_{i,s}(0)}g^{r_i'})\prod_{i\in\omega^{*}/\omega'}\hat{e}(H_1(i),g^{r_i'})](H_2(m),g^{r_{i_d}'})}$$

$$=\frac{\hat{e}(g,[\prod_{i\in\omega'\cup\Omega'}(g_2^{q(i)}H_1(i)^{r_i})^{\Delta_{i,s}(0)}][\prod_{i\in\omega'\cup\Omega'}H_1(i)^{r_i'}])}{[\prod_{i\in\omega'\cup\Omega'}\hat{e}(H_1(i),g^{r_i\Delta_{i,s}(0)}g^{r_i'})]}=$$

$$\prod_{i\in\omega'\cup\Omega'}(g,g_2^{q(i)})^{\Delta_{i,s}(0)}=Z$$

5 方案分析

5.1 安全性证明

定理 1 假定 G_1 上的 CDH 困难问题成立，则本文所提签名方案满足 EF-ABS-ACMA 安全，即不存在一个 EF-ABS-ACMA 攻击者以不可忽略的优势攻破所提方案。

证明：假设攻击者 $\mathcal{A}$ 能够在概率多项式时间内以 ε 的优势在定义 3 中的游戏中获胜，并且攻击者 $\mathcal{A}$ 最多进行 q_{H_i} 次 H_i 询问($i=1,2$)、q_K 次私钥生成询问、q_S 次签名询问。构造算法 $\mathcal{C}$，利用 $\mathcal{C}$ 解决 CDH 问题，即给定 (g,g^{x},g^{y})，计算 g^{xy}。设置系统参数 $d\in_R Z_q^{*}$，缺省属性集 $\Omega=\{\Omega_1,\Omega_2,\cdots,\Omega_{d-1}\}$，$\mathcal{A}$ 输出预挑战的断言 $\Upsilon_{k,\omega^{*}}()$，$1\leqslant k\leqslant d$，$\mathcal{C}$ 随机选择缺省属性集 $\Omega^{*}\subseteq\Omega$，$|\Omega^{*}|=d-k$。$C$ 仿真如下：

(1)初始化：$\mathcal{C}$ 设置 $g_1=g^{x}$，$g_2=g^{y}$。

(2)随机预言机：$\mathcal{A}$ 保存列表 $\mathcal{L}_1$ 和 $\mathcal{L}_2$ 来存储 H_1-预言机和 H_2-预言机的答案。C 选择 1 个随机数 $\delta\in[1,q_{H_2}]$。

H_1-预言机：如果对 i 进行 H_1-预言机询问，$\mathcal{C}$ 检查 $\mathcal{L}_1$，仿真如下：

①如果能在 $\mathcal{L}_1$ 中找到 i，返回其对应的值；

②否则，如果 $i\in\omega^{*}\cup\Omega^{*}$，选择随机数 $\beta_i\in_R Z_q^{*}$，返回 $H_1(i)=g^{\beta_i}$，并记录于 $\mathcal{L}_1$；

③否则，如果 $i\notin\omega^{*}\cup\Omega^{*}$，选择随机数 $\beta_i,\gamma_i\in_R Z_q^{*}$，返回 $H_1(i)=g^{-\beta_{i_1}}g^{\gamma_i}$，并记录于 $\mathcal{L}_1$。

H_2-预言机：如果对 m_i 进行 H_2-预言机询问。$\mathcal{C}$ 检查列表 $\mathcal{L}_2$，仿真如下：

①如果能在 $\mathcal{L}_1$ 中找到 i，返回其对应的值；

②否则，如果 $i\neq\delta$，选择随机数 $\alpha_i,\beta_i'\in_R Z_q^{*}$，返回 $H_2(m_i)=g_1^{\alpha_i}g^{\beta_i'}$，并记录于 $\mathcal{L}_2$；

③如果 $i=\delta$，选择随机数 $\beta_\delta\in_R Z_q^{*}$，返回 $H_2(m_i)=g^{\beta_\delta}$，并记录于 $\mathcal{L}_2$。

(3)私钥生成预言机：

①如果对属性集 ω_i(且满足 $|\omega_i\cap\omega^{*}|<k$)进行私钥生成询问。定义 3 个集合 Γ,Γ',S，满足：$\Gamma=(\omega_i\cap\omega^{*})\cup\Omega_i'$，$\Gamma\subseteq\Gamma'\subseteq S$，$|\Gamma'|=d-1$，$S=\Gamma'\cup\{0\}$。$\mathcal{C}$ 仿真如下：

对于 $i\in\Gamma'$，令 $D_i=(g_2^{t_i}H_1(i)^{r_i},g^{r_i})$，其中 $t_i,r_i\in_R Z_q^{*}$。相当于隐式选择了一个 $d-1$ 次多项式 $q(x)$，且 $q(i)=t_i$，并且 $q(0)=x$。

对于 $i\notin\Gamma'$，设 $r_i=\frac{\Delta_{0,S}(i)}{\beta_i}y+r_i'$，$q(i)=\sum_{j\in\Gamma}\Delta_{j,S}(i)q(j)+\Delta_{0,S}(i)q(0)$，$D_i=(g_2^{\frac{\Delta_{0,S}(i)\gamma_i}{\beta_i}+\sum_{j\in\Gamma}\Delta_{j,S}(i)q(j)}(g_1^{-\beta_i}g^{\gamma_i})^{r_i'},g_2^{\frac{\Delta_{0,S}(i)}{\beta_i}}g^{r_i'})_{i\in\omega_i}$。因为

$$g_2^{q(i)} H_1(i)^{r_i} = g_2^{\sum_{j\in\Gamma'}\Delta_{j,S^{(i)}q(j)}+\Delta_{0,S^{(i)}q(0)}} (g_1^{-\beta_i} g^{\gamma_i})^{\frac{\Delta_{0,S^{(i)}}}{\beta_i}y+r_i'}$$

$$= g_2^{\frac{\Delta_{0,S^{(i)}}\gamma_i}{\beta_i}+\sum_{j\in\Gamma'}\Delta_{j,S^{(i)}q(j)}} (g_1^{-\beta_i} g^{\gamma_i})^{r_i'}$$

$$g^{r_i} = g^{\frac{\Delta_{0,S^{(i)}}}{\beta_i}y+r'} = g_2^{\frac{\Delta_{0,S^{(i)}}\gamma_i}{\beta_i}} g^{r_i'}$$

所以，$D_i = (g_2^{\frac{\Delta_{0,S^{(i)}}\gamma_i}{\beta_i}+\sum_{j\in\Gamma'}\Delta_{j,S^{(i)}q(j)}} (g_1^{-\beta_i} g^{\gamma_i})^{r_i'}, g_2^{\frac{\Delta_{0,S^{(i)}}}{\beta_i}} g^{r_i'})_{i\in\omega_i}$ 是一个合法的私钥。

②如果$|\omega_i \cap \omega^*| \geqslant k$，则$\mathscr{C}$仿真失败。

(4)签名预言机：$\mathscr{A}$请求在属性集ω和断言Υ_{k,ω_1^*}()下的消息m_i的签名询问。$\mathscr{C}$仿真如下：

①如果$|\omega \cap \omega^*| < k$，则$\mathscr{C}$利用私钥生成预言机产生$\omega_A$的私钥$D_{Ai} = (d_{i0}, d_{i1})$，并且按照正常的签名算法产生签名并返回给$\mathscr{A}$。

②否则，$\mathscr{C}$从缺省属性集Ω随机选择由$d-|\omega|$个元素构成的子集Ω'。假设$\omega \cup \Omega' = \{i_1, i_2, \cdots, i_d\}$，$\mathscr{C}$随机选择$r_i, s' \in_R Z_q^*$，$1 \leqslant i \leqslant d-1$，设$r_d = \frac{-1}{\alpha_{i_d}}y + s'$，设置$\sigma_0 = g_2^x \prod_{i\in\omega^* \cup \Omega'/(i_d)}$

$H_1(i)^{r_i} H_1(i_d)^{r_d} H_2(m_i)^{r_d} = (g_1^{\alpha_{i_d}} g^{\beta_i})^{s'} \prod_{i\in\omega^* \cup \Omega'/(i_d)} g^{\beta_i r_i}$

$g_2^{\frac{-\beta_{i_d}}{\alpha_{i_d}}} g^{\beta_{i_d} s_i'} g_2^{\frac{-\beta_i}{\alpha_{i_d}}}$，$\{\sigma_i = g^{r_i'}\}_{i\in\omega^* \cup \Omega'}$，其中，$H_2(i) = g^{\beta_i}$，$H_2(m_i) = g_1^{\alpha_{i_d}} g^{\beta_i}$。返回签名$\sigma = \{\sigma_0, \{\sigma_i\}_{i\in\omega^* \cup \Omega'}\}$。$\sigma$是一个有效的签名。

(5)伪造签名：$\mathscr{A}$选择挑战的属性集ω^*和缺省属性集Ω^*，输出一个消息m_δ的签名$\sigma^* = \{\sigma_0^*, \{\sigma_i^*\}_{i\in\omega^* \cup \Omega'}\}$。如果$\mathscr{A}$没有选择$\omega^*$和$\Omega^*$或者$H_2(m_\delta) \neq g^{\beta_\delta}$，则$\mathscr{C}$仿真失败。

如果σ^*合法，则满足

$$\frac{\hat{e}(g, \sigma_0^*)}{[\prod_{i\in\omega^* \cup \Omega'} \hat{e}(H_1(i), \sigma_i^*)] \hat{e}(H_2(m_\delta), \sigma_{i_d}^*)} = Z$$，那么$\mathscr{A}$赢得游戏。由于$H_1(i) = g^{\gamma_i}$，$H_2(m_\delta) = g^{\beta_\delta}$，则

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

$$\frac{\hat{e}(g, \sigma_0^*)}{[\prod_{i\in\omega^* \cup \Omega'} \hat{e}(g^{\gamma_i}, \sigma_i^*)] \hat{e}(g^{\beta_\delta}, \sigma_{i_d}^*)} = \hat{e}(g, \sigma_0^* / \prod_{i\in\omega^* \cup \Omega'} \sigma_i^{*\gamma_i} \sigma_{i_d}^{*\beta_\delta}) =$$

$\hat{e}(g, g^{xy})$，所以$g^{xy} = \sigma_0^* / \prod_{i\in\omega^* \cup \Omega'} \sigma_i^{*\gamma_i} \sigma_{i_d}^{*\beta_\delta}$，$\mathscr{C}$解决了CDH问题。

$\mathscr{A}$不对ω^*进行私钥生成询问的概率至少为$1/q_{H_1}$，$\mathscr{A}$选择挑战ω^*的概率至少为$1/q_{H_1}$，$\mathscr{A}$选择缺省属性Ω^*的概率至少为$1/\binom{d-k}{d-1}$，$H_2(m_\delta) = g^{\beta_\delta}$的概率至少为$1/q_{H_2}$，可得$\mathscr{C}$解决CDH问题的优势为：

$$\varepsilon' = \frac{\varepsilon}{q_{H_1}^2 q_{H_2} \binom{d-k}{d-1}} > \frac{(d-k)\varepsilon}{q_{H_2} q_{H_1}^2 (d-1)^{d-k}}$$

定理2 本文所提签名方案满足签名者属性隐私安全。

证明：$\mathscr{C}$设置主密钥为$x \in_R Z_q^*$和系统参数$param$，攻击者$\mathscr{A}$输出2个属性集ω_1^*，ω_2^*，$\bar{\omega}^* = \omega_1^* \cap \omega_2^*$。选择缺省属性集$\Omega$。设置$\hat{\omega}_b^* = \omega_b^* \cup \Omega, b \in \{0,1\}$。$\mathscr{C}$产生属性私钥$sk_{\omega_1^*}^{\wedge} =$ $(d_{i0}^1, d_{i1}^1)_{i\in\hat{\omega}_1^*}$，$sk_{\omega_2^*}^{\wedge} = (d_{i0}^2, d_{i1}^2)_{i\in\hat{\omega}_2^*}$，设置$\{d_{i0}^\theta = g_2^{q_\theta(i)} \mathscr{H}(i)^{r_i^\theta}, g^{r_i^\theta}\}_{i\in\hat{\omega}_\theta^*}$，$\theta \in \{0,1\}$，$r_i^\theta \in_R Z_q^*$，$q_\theta(i)$为$d-1$次多项式，$q_\theta(0) = x$。$\mathscr{A}$输出一个消息$m^*$和属性子集$\omega^* = \{i_1, \cdots, i_k\} \subseteq \hat{\omega}^*$，$|\omega^*| \leqslant d$，请求$\mathscr{C}$利用$sk_{\omega_1^*}^{\wedge}$或$sk_{\omega_2^*}^{\wedge}$，在$\omega^*$下对消息$m^*$进行签名。$\mathscr{C}$随机选择$b \in \{0,1\}$，选择$d-k$个元素构成的缺省属性集$\Omega' = \{i_{k+1}, i_{k+2}, \cdots, i_d\} \subseteq \Omega$，运行签名算法，输出签名$\sigma_0 = g_2^x \prod_{i\in\omega^* \cup \Omega'} H_1(i)^{r_i} H_2(m)^{r_{i_d}}$，$\{\sigma_i = g^{r_i'}\}_{i\in\omega^* \cup \Omega'}$。由拉格朗日插值定理可知，该签名可由$sk_{\omega_1^*}^{\wedge}$或$sk_{\omega_2^*}^{\wedge}$产生。因此攻击者$\mathscr{A}$无法区分$\hat{\omega}_1^*$和$\hat{\omega}_2^*$中哪个集合用于产生$\sigma$。因此，定理2成立。

5.2 性能分析

表1中给出了本文方案与Li方案[12]的比较，分别列出了签名阶段和验证阶段的计算代价、签名长度和私钥存储代价。S表示G_1上的幂运算，P表示双线性对运算。从表1中可以看出，本文方案在签名代价和签名长度方面有所改进。

表1 本文方案与其他方案性能比较

	计算代价	签名长度	存储代价
Li方案[12]	(2n+4d−2k+2)S (n+d−k)P	(n+d−k+2)|G_1|	2(|ω_{ID}|+d−1)|G_1|
本文方案	(2n+4d−2k+1)S (n+d−k)P	(n+d−k+1)|G_1|	2(|ω_{ID}|+d−1)|G_1|

5.3 仿真实验

本文将所提签名方案应用于移动对等网络的数据分发，完成消息的认证，并进行了仿真实验。图1、图2给出了基于ABS的移动对等网络数据分发代价，分别给出了消息发送者和接收者的时间消耗。由图1和图2可以看出，当门限d和签名属性增加时，消息接收者运行的时间增长较快，这是由于签名的验证过程包含双线性对运算，耗时较多。而消息发送者受门限和签名属性集的影响不大。随着门限k的增加，签名方案变成(d,n)门限，签名和验证的代价降低，所以消息发送者和接收者的消耗降低。由仿真实验可知，当属性小于250，d小于150时，消息接收者的代价可以接受，因此本文提出的签名方案可以满足大多数移动对等网络数据分发应用需求。

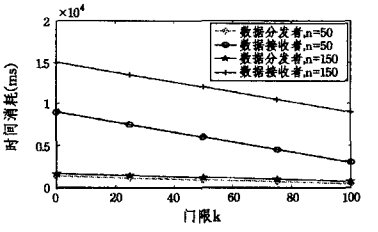

图1 基于ABS的移动对等网络数据分发代价(d=100)

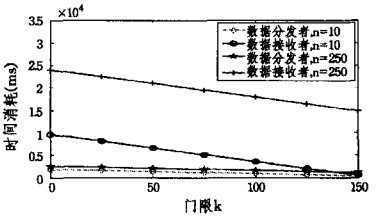

图2 基于ABS的移动对等网络数据分发代价(d=150)

结束语 本文指出了Chen等人的基于属性签名方案[13]

不能满足不可伪造性，攻击者可以根据一个合法的签名伪造其他消息的签名；并改进了 Li 基于属性签名方案[12]，提出了一个高效的支持动态门限的基于属性签名方案，降低了签名代价和签名长度，并且利用 CDH 问题的困难性，在随机预言机模型下证明了所提方案满足在适应性选择消息和断言下的不可伪造性。仿真实验结果表明，所提签名方案可以较好地应用于移动对等网数据分发，以实现消息认证。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signatures schemes [C]// Proceedings of CRYPTO 84 on Advances in Cryptology. 1985:47-53

[2] Boneh D, Franklin M. Identity based encryption from the weil Pairing[C]// Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology. California, USA, August 19-23, 2001:213-229

[3] Sahai A, Waters B. Fuzzy Identity-Based Encryption[C]// Proceedings of EUROCRYPT. Aarhus, Denmark, May 2005: 457-473

[4] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]// Proceedings of ACM Conference on Computer and Communications Security. New York, USA, 2006:221-238

[5] Yang P, Cao Z, Dong X. Fuzzy identity based signature[R]. Report 2008/002. IACR Cryptology ePrint Archive, 2008

[6] Guo S, Zeng Y. Attribute-based signature scheme [C]// Proceedings of the 2nd International Conference on Information Security and Assurance. Busan, Korea, April 2008:509-511

[7] Khader D. Attribute based group signatures[R]. Report 2007/159. IACR Cryptology ePrint Archive, 2007

[8] Maji H K, Prabhakaren M, Rosulek M. Attribute-based signatures: achieving attribute-privacy and collusion-resistance[R]. Report 2008/328. IACR Cryptology ePrint Archive, 2008

[9] Maji H K, Prabhakaren M, Rosulek M. Attribute-based signatures[R]. Report 2010/595. Cryptology ePrint Archive, 2010

[10] Li J, Kim K. Attribute-based ring signatures[R]. Report 2008/394. IACR Cryptology ePrint Archive, 2008

[11] Shahandashti S F, Safavi-Naini R. Threshold attribute-based signatures and their application to anonymous credential systems [C]// Proceedings of the 2nd International Conference on Cryptology in Africa. Gammarth, Tunisia, June 2009:198-216

[12] Li J, LMan H A. Attribute-based signature and its applications [C]// Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. Beijing, China, Apr. 2010:60-69

[13] 陈少真，王文强，彭书娟. 高效的基于属性环签名方案[J]. 计算机研究与发展，2010，47(12)：2075-2082

[14] Herranz J, Laguillaumie F, Libert B, et al. Short attribute-based signatures for threshold predicates[C]// Proceedings of the 12th International conference on Topics in Cryptology. San Francisco, CA, USA, 2012, LNCS 7178:51-67

(上接第 70 页)

感器网络中的多跳路由。RBMC 协议簇头选举协议过于简单，和 LEACH 协议相同，并未考虑其他因素，极易造成簇头分布不均衡，使分环的效果降低。MCBMC 路由协议对 RBMC 作了多处改进，包括簇头自举的方法，以及根据预测环剩余能量使每环多轮成簇等。通过对协议 MCBMC 进行仿真并分析仿真结果，验证了 MCBMC 协议网络生存时间比 RBMC 协议更长，节点的平均能耗速率更小，节点成簇开销更少，能量消耗更少，提高了网络能效。

参 考 文 献

[1] 孙利民，李建中，陈渝，等. 无线传感器网络[M]. 北京：清华大学出版社，2005:3-4

[2] Ahmed A, Mohamed Y. A survey on clustering algorithms for wireless sensor networks[J]. Comput Communication, 2007, 30 (14/15):2826-2841

[3] Mhatre V, Rosenberg C. Design guidelines for wireless sensor networks: communication, clustering and aggregation [J]. Ad Hoc networks, 2004, 2(1):45-63

[4] 侯西梅，万润泽. 无线传感器网络的多跳分簇路由协议建模与实现[J]. 江西师范大学学报，2008，32(2)：215-218

[5] Heinzelman W R, Chandrakasan A, Balakrishnan H. Energy—eficient communication protocol for wireless microsensor networks[C]// Proceedings of the 33rd Annual Hawaii International Conference on System Sciences. Hawaii, 2000:10-15

[6] Manjeshwar A, Agrawal D P. TEEN: A protocol for enhanced efficiency in wireless sensor networks[C]// Int'l Proc. of the 15th Parallel and Distributed Processing Symp. San Francisco: IEEE Computer Society, 2001:2009-2015

[7] Lindsey S, Raghavendra C S. PEGASIS: Power-efficient gathering in sensor information systems[C]// Proc. of the IEEE Aerospace Conf. Montana: IEEE Aerospace and Electronic Systems Society, 2002:1125-1130

[8] Younis O, Fahmy S. HEED: A hybrid, energy-eficient, distributed clustering approach for Ad hoe sensor networks[J]. IEEE n8ns. on Mobile Computing, 2004, 3(4):366-379

[9] Ye Mao, Li Cheng-fa, Chen Gui-hai, et al. EECS: an energy efficient clustering scheme in wireless sensor network[C]// Performance, Computing, and Communications IPCCC 2005 24th IEEE International Conference. April 2005:535-540

[10] Li Cheng-fa, Chen Gui-hai. An Uneven Cluster-Based Routing Protocol for Wireless Sensor Networks[C]// Chinese Journal of Computers, 2007:27-35

[11] 刘志，裘正定. 基于分环多跳的无线传感网分簇路由协议[J]. 通信学报，2008，29(3)：104-113

[12] 卿利，朱清新，王明文. 异构传感器网络的分布式能量有效成簇算法[J]. 软件学报，2006，17(3)：481-489