doi:10.3969/j.issn.1000-436x.2013.z1.002

高效的模糊属性基签密方案

杨晓元[1,2]，林志强[1]，韩益亮[1,2]
（1. 武警工程大学 电子技术系 武警部队密码与信息安全保密重点实验室，陕西 西安 710086；
2. 武警工程大学 电子技术系 网络与信息安全研究所，陕西 西安 710086）

摘 要：多用户通信是当今信息交互的主要模式，提高通信安全性与解决通信效率问题是当前研究的重点。属性基签密保证了多用户在通信中消息的机密性与完整性，并通过一步操作实现对多用户的消息发送，提高了签密的效率。利用密钥共享模型及双线性对，提出一种高效的模糊属性基签密方案，基于 DMBDH 与 CDH 问题证明了机密性与不可伪造性，同时还满足可公开验证性与短密文性。分析对比表明，签密与解签密的运算量仅为$(n+3)e$和$ne+(n+4)p$，远小于同类方案的运算量，实现了算法的高效性。

关键词：模糊属性；密钥共享；短密文；可公开验证
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2013)Z1-0008-06

Efficient fuzzy attribute-based signcryption scheme

YANG Xiao-yuan[1,2], LIN Zhi-qiang[1], HAN Yi-liang[1,2]
(1. Key Laboratory of the Chinese Armed Police Force for Cryptology and Information Security, Department of Electronic Technology, Engineering University of the Chinese Armed Police Force, Xi'an 710086,China；2. Institute of Network and Information Security Under the Chinese Armed Police Force, Department of Electronic Technology, Engineering University of the Chinese Armed Police Force, Xi'an 710086,China)

Abstract: Multi-user communication is the major model of present information exchange and to improve communication security and to solve the problem of communication efficiency is the key of present research. Attributed-based signcryption ensures the confidentiality and integrity of the information during communication and realizes the sending of information through one-step operation, thus improving the efficiency of signcryption. By using secret sharing model and bilinear pairs, an efficient fuzzy attribute-based signcryption scheme was presented, and based on DMBDH and CDH problem, the confidentiality and unforgeability of the scheme were proved. Meanwhile, it meets public verifiability and short ciphertext. Compared with other analysis, the amount of computation of signcryption and designcryption is only $(n+3)e$ and $ne+(n+4)p$, far less than those of other similar schemes and this realizes the efficiency of computation.

Key words: fuzzy attribute; secret sharing; short ciphertext; public verifiability

1 引言

在网络通信中，为了保证通信消息的机密性与完整性，发送方需要对消息进行签密，接收方则需对消息进行解密并验证。在传统的“一对一”通信模式中，通信双方的信息交互则需指定具体的接收方与发送方，对于庞大而繁忙的网络环境，这种单一的模式不仅效率低、开销大，而且暴露用户的相关信息，显然不能满足实际通信的需求。

模糊属性基的签密系统面向多用户环境，任何用户只需根据自身属性满足指定的访问控制结构就能够解密消息，不仅实现多用户通信，提高了算法的应用广度，而且隐藏接收方的个人信息，保护了用户的隐私。同时，签密过程使发送方在一个逻辑步骤内同时完成消息的加密与签名，可以显著降低通信的开销。

1984 年，SHAMIR[1]首次提出基于身份的密码学概念，用户以他们的身份信息，如名字、身份证

收稿日期：2013-06-28
基金项目：国家自然科学基金资助项目（61272492, 61103231, 61103230）；陕西省自然科学基础研究计划基金资助项目(2011JM8012)
Foundation Items: The National Natural Science Foundation of China (61272492, 61103231, 61103230); The Natural Science Research Project of Shanxi Province (2011JM8012)

号、地址及邮箱地址作为公钥，解决了传统公钥基础设施中公钥证书的复杂性管理问题。之后，基于身份的密码研究得到快速发展[2~4]。而在基于身份的密码体制中，通信模式通常为一对一模式，加密者需要知道解密者身份信息，验证者也需要知道签名者的身份信息，造成了身份信息的泄露，因此，基于属性的密码系统成为发展的需要[5]。2005 年，SAHAI 等人[6]首次提出基于模糊身份的加密(Fuzzy IBE)概念，它以用户的生物信息作为身份，该身份为一个描述属性的集合，它则是基于属性密码系统的雏形。在 Fuzzy IBE 提出之后，模糊身份的密码系统得到了进一步的发展[7~9]。2006 年，文献[10]首次提出了基于属性加密的密码学概念，它具备 2 个特性，即多用户性和隐藏身份性，确保了隐私信息在通信中的安全性。

虽然属性基加密可以解决访问权限问题，但为了避免用户收到无关的消息以及能够对消息的来源进行认证，则引入了签密。签密最初由 ZHENG 等人[11]于 1997 年提出，它能够在一个逻辑步骤内同时实现对消息的加密和签名，其计算量远小于对签名和加密的简单组合，且安全性更高。2010 年，ZHANG 等人[12]将签密与属性基结合，首次提出基于模糊生物特征的签密方案，以较小的计算开销同时实现数字签名与加密，但该方案的密文长度较大，通信负荷较高。2012 年，HU 等人[13]将基于模糊属性的签密用于体域网中，实现体域网访问控制的安全性，但其方案在签密与解签密阶段的计算开销较大。由于属性基性能的优越性以及多用户通信模型的安全需求，对属性基签密的研究得到进一步发展，形式更为广泛[14]。对短密文长度方案的研究可以减少通信量，降低通信负荷，文献[15]提出了一种具有短密文长度性质的签密方案，利用对字符串的压缩表示，既减小运算长度，又降低通信负荷，但它是基于身份的，并且为一对一通信的签密方案，在实际网络通信中的实用性不高。

本文结合各方案的优点，提出一种高效的模糊属性基签密方案，实现了以下 4 点特性：一是构造访问控制结构，任何用户的属性只要满足指定的属性门限值均可对消息进行解密；二是可公开验证性，任何用户不需要暴露私人信息即可验证消息来源的有效性；三是短密文长度，有效降低了通信负荷；四是算法高效性，在签密与解签密阶段的运算量在同类方案中为最小，可以大幅度减少计算开销。

2　相关知识

2.1　双线性对

令 G 和 G_T 是阶为素数 p 的循环群，g 为 G 的生成元。定义双线性对 $e: G_1 \times G_1 \to G_2$ 满足以下 3 个特性。

1) 双线性：对于任意的 $a,b \in Z_p$ 和 $g_1,g_2 \in G$，有 $e(ag_1,bg_2)=e(g_1,g_2)^{ab}$。

2) 非退化性：存在 $g_1,g_2 \in G$，使 $e(g_1, g_2) \neq 1$。

3) 可计算性：对于所有的 $g_1,g_2 \in G$，$e(g_1,g_2)$ 必须存在有效的计算算法。

2.2　困难问题假设

定义 1　Decisional bilinear Diffie-Hellman (DBDH) assumption:随机选择 a,b,c 且 $a,b,c,z \in Z_P$，$g \in G$，则假设不存在多项式时间敌手以大于不可忽略的优势从 $(A=g^a,B=g^b,C=g^c,\ Z=e(g,g)^z)$ 中区分出 $(A=g^a,B=g^b,C=g^c,Z=e(g,g)^{abc})$。

定义 2　DMBDH(decisional modified bilinea Diffie-Hellman) assumption：随机选择 a,b,c 且 $a,b,c,z \in Z_p, g \in G$，则假设不存在多项式时间敌手以大于不可忽略的优势从 $(A=g^a,B=g^b,\ C=g^c,\ Z=e(g,g)^z)$ 中区分出 $(A=g^a,B=g^b,\ C=g^c,\ Z=e(g,g)^{\frac{ab}{c}})$。

定义 3　CDH(computational diffie-hellman) assumption：假设随机选择 a,b 且 $a,b \in Z_p$，$g \in G$，已知 (g,g^a,g^b)，计算 g^{ab}。

2.3　选定模糊属性的安全模型

本小节为基于模糊属性的密码方案定义如下选定属性的安全模型。

Init：敌手宣布所要挑战的身份为 γ，敌手向目标身份询问密钥时，所询问的属性个数不能超过 d 个。

Setup：挑战者运行该算法，并告诉敌手系统公共参数。

Queries：敌手可以向许多属性 κ_i 的私钥进行询问，其中，对于所有的 i 满足 $|\kappa_i \cap \gamma| < d$。

Challenge: 敌手提交 2 个等长度的消息 M_0, M_1。挑战者随机选择 $\Omega \in \{0,1\}$，用 γ 对 M_Ω 加

密，并将密文发给敌手。

Guess：敌手输出一个 Ω 的猜测值 Ω'。

其中，敌手在游戏中的优势为 $Pr[\Omega'=\Omega]-\frac{1}{2}$。

定义 4 选定模糊属性安全(fuzzy selective- attribute secure):如果敌手在多项式时间内的优势小于以上游戏中的不可忽略优势，那么方案在选定模糊属性的安全模型下是安全的。

2.4 密钥共享模型

密钥共享方案最早是由 SHARMIR[16]提出，它利用插值多项式实现密钥共享。其过程是将密钥分成 n 个部分，将其分发给 n 个用户，每个用户拥有自己唯一的部分，只有满足一定数量 $(d\leqslant n)$ 的用户才能共同恢复出密钥。

令 $GF(q)$ 为 $q>n$ 的定义域，同时令 $s\in GF(q)$ 为被共享密钥。随机选取 $d-1$ 阶的多项式 $f(x)$，构造 $f(x)=s+\sum_{i=1}^{d-1}a_i x^i$。协议者标记每个用户 μ_i 拥有唯一元素 ϑ_i，协议者发送其共享密钥 $s_i=f(\vartheta_i)$，若用户子集 $N\subset P$，其中 $|N|>>t$，则他们可通过 $f(x)=\sum_{\mu_i\in N}\Delta_{\vartheta_i,N(x)f(\vartheta_i)}=\sum_{\mu_i\in N}\Delta_{\vartheta_i,N(x)s_i}$，其中 $\Delta_{\vartheta_i,N(x)}=\prod_{\mu_i\in P,j\neq i}\frac{x-\vartheta_j}{\vartheta_j-\vartheta_i}$，从而共同恢复密钥 $s=f(0)$。

3 模糊属性基签密的框架模型

模糊属性基签密方案一般由以下 4 个算法组成。

Setup:给定一个安全系数 r 与长度为 n、门限为 d 的属性字符串，PKG 生成系统主密钥 msk 与系统参数 $Params$。

KeyExtract: 输入主密钥 msk，给定一个属性字符串 $i\in\{0,1\}^n$，PKG运行该算法生成相应的密钥 D_i。

Signcrypt: 发送方用具有 n 个元素的属性集 ω 生成相应密钥 $(D_i)_{i\in\omega}$，输入消息 M，并运行该算法，得到签密文 σ。

Unsigncrypt: 当发送方发出签密文后，若接收方的属性集 ω' 满足 $|\omega\cap\omega'|\geqslant d$，则运行该算法实现对消息 M 的解密。

4 模糊属性基签密方案

4.1 访问控制结构

本文主要设计一种基于模糊属性的签密方案，方案中的用户身份是由多个属性组成的属性集，假设一个身份由 n 个属性组成，每一个属性可视为相应的字符串，例如身份可表示为 $Id=\{Name,age,title,hometown\}$，用户的访问权限则由用户自身的属性集所决定。本文对用户的访问结构定义为：如果用户符合指定 n 个属性中的至少 d 个属性，则用户有权限访问相关数据，即用户能够对签密文进行解签密。

4.2 方案描述

本文设计的签密方案主要包括 4 个算法，其具体过程如下。

Setup:

1) 随机选择 $y\in Z_p$，$g_2\in G$，计算 $g_1=g^y$，$X=e(g_1,g_2)$；

2) 随机选择 $a',b'\in G$，以及长度分别为 $n_{a'}$、$n_{b'}$ 的向量 $\vec{A}=(a_i)$、$\vec{B}=(b_j)$，其中 $a_i,b_j\in G$；

3) 定义拉格朗日系数 $\Delta_{i,S(x)}=\prod_{j\in S,j\neq i}\frac{x-j}{i-j}$，其中 $i\in Z_q$，S 为属性集，表示为 $S=\{1,2,\cdots,n+1\}$；

4) 随机选择 $r=\{r_1,r_2,\cdots,r_{n+1}\}\in Z_p$，计算 $R=\{R_i=g_2^{t_i}\}_{i\in S}$；

5) 选择一个抗碰撞散列函数 $H:\{0,1\}^*\rightarrow\{0,1\}^{n_{b'}}$；

6) 公开系统参数 $params=(e,G,G_T,g,g_1,g_2,X,H,a',b',\vec{A},\vec{B},R)$，保密系统主密钥 $msk=(r,y)$。

KeyExtract:

1) 随机选一个 $d-1$ 次多项式 q，满足 $q(0)=y$；

2) eExtract:输入属性集 $\omega\subseteq S$ 生成加密密钥 $(D_i)_{i\in\omega}$，对于每一个 $i\in\omega$，都有 $D_i=g^{q(i)/t_i}$；

sExtract:输入一个发送者特有身份 θ 生成签名密钥 D_s，令 $P\subset\{1,2,\cdots,n_{a'}\}$ 满足 $\theta[i]=1$，其中 $\theta[i]$ 表示字符串 θ 中第 i 位的值。随机选择 $k\in Z_p$，计算 $D_s=(D_{s1},D_{s2})=(g_2^y\cdot(a'\prod_{i\in P}a_i)^k,g^k)$。

Signcrypt:属性集 ω' 作为公共密钥集，消息 $M\in G_T$，签密过程如下：

1) 随机选择 $s\in Z_p$，计算 $C_1=M\cdot X^s$；

2) 计算 $C_2=g^s$；

3) 计算 $C_3=D_{s2}$；

4) 计算 $J:\{J_i=R_i^s\}_{i\in\omega'}$；

5) 计算 $\lambda = H(C_1, C_2, C_3, \theta)$，令 $Q \subset \{1,2,\cdots,n_{b'}\}$ 满足 $\lambda[i]=1$，其中 $\lambda[i]$ 表示字符串 λ 中第 i 位的值；

6) 计算 $V = D_{s1}(b'\prod_{i\in Q} b_i)^s$；

7) 发布签密文 $\sigma = (C_1, C_2, C_3, J, V)$。

Unsigncrypt: 接收方收到签密文 $\sigma = (C_1, C_2, C_3, J, V)$ 后，将自身的属性集 ω 与公共属性集 ω' 做对照，若 $|\omega \cap \omega'| \geqslant d$，则随机选择元素个数为 d 的子集 S，解签密过程如下：

1) 计算 $\lambda' = H(C_1, C_2, C_3, \theta)$，令 $Q \subset \{1,2,\cdots,n_{b'}\}$ 满足 $\lambda'[j]=1$，其中 $\lambda'[j]$ 表示字符串 λ' 中第 j 位的值；

2) 验证 $e(V,g) \stackrel{?}{=} e(g_1,g_2)e(a'\prod_{i\in P} a_i, C_3)e(b'\prod_{i\in Q} b_i, C_2)$，若等式成立，则有 $M = C_1 \Big/ \prod_{i\in S} (e(D_i, J_i))^{\Delta_{i,S(0)}}$；否则输出 $\perp$。

5　方案分析

5.1　正确性分析

定理 1　在 Unsigncrypt 阶段可以通过判定 $e(V,g) \stackrel{?}{=} e(g_1,g_2)e(a'\prod_{i\in P} a_i, C_3)e(b'\prod_{i\in Q} b_i, C_2)$ 验证所接收密文是否被伪造或篡改。

证明　如果消息没有被伪造或篡改，则有

$$\begin{aligned} e(V,g) &= e(g_2^y (a'\prod_{i\in P} a_i)^k \cdot (b'\prod_{i\in Q} b_i)^s, g) \\ &= e(g_2^y, g)e((a'\prod_{i\in P} a_i)^k, g)e((b'\prod_{i\in Q} b_i)^s, g) \\ &= e(g_2, g^y)e(a'\prod_{i\in P} a_i, g^k)e(b'\prod_{i\in Q} b_i, g^s) \\ &= e(g_1,g_2)e(a'\prod_{i\in P} a_i, C_3)e(b'\prod_{i\in Q} b_i, C_2) \end{aligned}$$

定理 2　在 Unsigncrypt 阶段，若接收方满足 $|\omega \cap \omega'| \geqslant d$，则可对密文进行解密。

证明　接收方利用其属性集 ω 生成相应解密密钥 $(D_i)_{i\in\omega} = g^{q(i)/t_i}$，则有

$$\begin{aligned} M &= C_1 \Big/ \prod_{i\in S} (e(D_i, J_i))^{\Delta_{i,S(0)}} \\ &= MX^s \Big/ \prod_{i\in S} (e(g^{q(i)/t_i}, R_i^s))^{\Delta_{i,S(0)}} \\ &= Me(g_1,g_2)^s \Big/ \prod_{i\in S} (e(g^{q(i)/t_i}, g_2^{s\cdot t_i}))^{\Delta_{i,S(0)}} \\ &= Me(g_1,g_2)^s \Big/ \prod_{i\in S} (e(g,g_2)^{sq(i)})^{\Delta_{i,S(0)}} \\ &= Me(g_1,g_2)^s \Big/ e(g,g_2)^{s\sum_{i\in S} q(i)\Delta_{i,S(0)}} \\ &= Me(g_1,g_2)^s / e(g,g_2)^{sy} = M \end{aligned}$$

其中，$y = \sum_{i\in S} (q(i)\Delta_{i,S(0)})$。

5.2　安全性证明

5.2.1　机密性

定理 3　在随机预言模型中，如果 DMBDH 在群 G 上是困难问题，那么本方案在任何概率多项式时间内，对 Fuzzy Selective-attribute 敌手 α 的自适应选择密文攻击是安全的。

证明　该证明过程基于文献[6]中的证明方法。在 Fuzzy Selective-attribute 游戏中，假设多项式时间敌手 α 知道系统参数，并以 ε 的优势执行 q_1 次密钥询问、q_2 次签密询问、q_3 次解签密询问成功攻击本方案，则说明存在一个以不可忽略的优势 ε' 解决 DMBDH 问题的算法 $A\lg$，其中 $\varepsilon' = \frac{\varepsilon}{2}$。

令 G 和 G_T 分别为加法群和乘法群，e 为双线性对，g 为生成元。挑战者随机选择 $\tau \in \{0,1\}$，若 $\tau = 0$，令 $(A,B,C,Z) = (g^a, g^b, g^c, e(g,g)^{abc})$；否则令 $(A,B,C,Z) = (g^a, g^b, g^c, e(g,g)^z)$，其中 a,b,c,z 为随机数。假设全局属性为 $\mathcal{N}$，随机选择一个属性集 $\gamma \in Z_p$，该属性集包括 n 个元素，且 $|\gamma| < d$，其中 d 为合法用户成功解签密时所需的最小属性个数值。

Setup: 令系统参数为 $Y = e(g,A) = e(g,g)^a$，对于所有的 $i \in \gamma$，随机选择 $\psi_i \in Z_p$，令 $T_i = C^{\psi_i} = g^{c\psi_i}$；对于所有的 $i \in \mathcal{N} - \gamma$，随机选择 $\zeta_i \in Z_p$，令 $T_i = g^{\zeta_i}$。将系统参数发送给 α。

Queries: Private key queries，敌手 α 向模拟器请求询问私钥，在 γ 中所询问的元素个数不能超过 d 个。

假设 α 请求询问身份为 Id 的私钥，且 $|Id \cap \gamma| < d$。首先定义 3 组集合 L_1, L_2, L_3 如下：$L_1 = Id \cap \gamma$，L_2 满足 $L_1 \subset L_2 \subset Id$ 且 $|L_2| = d-1$，$L_3 = L_2 \cup \{0\}$。然后定义加密密钥 D_i $(i \in L_2)$ 如下：如果 $i \in L_1$，则随机选择 $h_i \in Z_p$，使 $D_i = g^{h_i}$；如果 $i \in L_2 - L_1$，则随机选择 $v_i \in Z_p$ 使 $D_i = g^{\frac{v_i}{\zeta_i}}$。

随机选择 $d-1$ 个元素值构成 $d-1$ 阶多项式 $q(x)$，使得 $q(0) = a$。对于 $i \in L_1$，$q(i) = c\psi_i h_i$；对于 $i \in L_2 - L_1$，$q(i) = v_i$。

对于所有的 $i \in \gamma$，当已知离散函数 T_i 的值时，

模拟器可以计算其他密钥值 $D_i,(i \notin L_2)$。并且有：若 $i \notin L_2$， $D_i = (\prod_{j \in L} C^{\frac{\psi_j h_j \Delta_{j,S(i)}}{\zeta_i}})(\prod_{j \in L_2 - L_1} g^{\frac{v_j \Delta_{j,S(i)}}{\zeta_i}}) Y^{\frac{\Delta_{0,S(i)}}{\zeta_i}}$。模拟器利用插值可以计算 $D_i = g^{q(i)/t_i},(i \notin L_2)$，其中 $q(x)$ 由随机安排的 $d-1$ 个变量 $D_i \in L_2$ 与变量 Y 所定义。

因此，模拟器能够构造属性 γ 的私钥，并且与原方案的私钥分布是相同的。

Signcryption queries：在任何时间下，敌手可以对明文请求签密询问，同时模拟器运行 *Signcrypt* 算法回答敌手的询问。

Unsigncryption queries：在任何时间下，敌手可以对密文请求解签密询问，同时模拟器运行 *Unsigncrypt* 算法回答敌手的询问。

Challenge：敌手 α 向模拟器 β 提交 2 个相同长度的挑战消息 M_1 和 M_0，β 随机选择 $\Omega \in \{0,1\}$，然后返回 M_Ω 的加密值。密文为：$\sigma = (\gamma, C_1 = M_\Omega Z, \{J_i = B^{\psi_i}\}_{i \in \gamma})$，如果 $\tau = 0$，则 $Z = e(g,g)^{\frac{ab}{c}}$，令 $r' = \frac{b}{c}$，则 $C_1 = M_\Omega Z = M_\Omega e(g, g)^{\frac{ab}{c}} = M_\Omega e(g,g)^{a \cdot r'} = M_\Omega Y^{r'}$，$J_i = B^{\psi_i} = g^{b\psi_i} = g^{\frac{b}{c} \cdot c \cdot \psi_i} = g^{r' c \psi_i} = (T_i)^{r'}$，由此表明在属性集 γ 下，消息 M_Ω 的密文是有效的；如果 $\tau = 1$，则 $Z = e(g,g)^z$，$C_1 = M_\Omega Z = M_\Omega e(g, g)^z$。由于 z 是随机选取的，对于敌手 α 而言，C_1 为 G_T 的一个随机元素，所以得到的消息不包含关于 M_Ω 的任何信息。

Guess：敌手 α 提交猜测值 Ω'。如果 $\Omega' = \Omega$，则表明模拟器接受一个 DMBDH 元组，输出 $\tau' = 0$；否则表明接受一个随机的四元组，输出 $\tau' = 1$。

当 $\tau = 1$ 时，敌手将得不到关于 Ω 的信息，有 $Pr[\Omega \neq \Omega' | \tau = 1] = \frac{1}{2}$。若模拟器猜测 $\tau' = 1$，且 $\Omega \neq \Omega'$，有 $Pr[\tau \neq \tau' | \tau = 1] = \frac{1}{2}$；当 $\tau = 0$ 时，敌手将获得消息 M_Ω 的签密文，其优势则为 ε，则 $Pr[\Omega = \Omega' | \tau = 0] = \frac{1}{2} + \varepsilon$。若模拟器猜测 $\tau' = 0$，且 $\Omega = \Omega'$，有 $Pr[\tau = \tau' | \tau = 0] = \frac{1}{2} + \varepsilon$。

所以敌手解决 DMBDH 问题的优势为 $Pr_{A\lg}[\alpha] = \frac{1}{2} Pr[\tau = \tau' | \tau = 0] + \frac{1}{2} \Pr[\tau = \tau' | \tau = 1] - \frac{1}{2} = \frac{1}{2} \times (\frac{1}{2} + \varepsilon) + \frac{1}{2} \times \frac{1}{2} - \frac{1}{2} = \frac{\varepsilon}{2}$。因为 DMBDH 在群 G 上是困难问题，所以本方案对自适应选择密文攻击是安全的。

5.2.2 不可伪造性

定理 4 在随机预言模型中，如果 CDH 在群 G 上是困难问题，那么本方案在任何概率多项式时间内，对 EUF-IBBSC-CMA2 敌手 α 的自适应选择消息攻击是安全的。

证明 在 EUF-IBBSC-CMA2 游戏中，挑战者收到一个随机的 CDH 实例：给定 (g, g^a, g^b)，挑战者的目标为计算 g^{ab}。假设存在一个 EUF-IBBSC-CMA2 敌手 α 想要伪造密文，则必须拥有签密方密钥。然而，敌手不能推断密钥 $D_s = (D_{s1}, D_{s2}) = (g_2^y \cdot (a' \prod_{i \in P} a_i)^k, g^k)$，因为 y 为系统主密钥、k 为随机选择。若敌手能够伪造出密钥，说明敌手攻破了本方案，即解决了 CDH 困难问题。另外，敌手 α 无法通过用户的密文生成一个新的有效密文，尽管敌手可以改变消息的密文，但接收方依然可以通过 *Unsigncrypt* 算法验证密文的合法性。因此，本方案在选择消息攻击下是不可伪造的。

5.3 性能及效率分析

5.3.1 可公开验证性

在签密方发布签密文后，任意的第三方均可验证

$$e(V, g) = e(g_1, g_2) e(a' \prod_{i \in P} a_i, C_3) e(b' \prod_{i \in Q} b_i, C_2)$$

该过程不需要接收方密钥等信息的参与，防止接收方隐私信息的泄露，因此本方案提供可公开验证。

5.3.2 运算量分析

影响方案效率的主要因素为方案的运算量。将本方案与现有的模糊属性基签密方案进行分析比较，得到如表 1 所示的数据，其中 e 表示指数运算，p 表示双线性对运算，且 $e < p$，n 表示签密属性的个数。

如表 1 所示，在签密阶段，ZHANG[12]方案需要进行 $(2n+2)$ 次指数运算，HU[13]方案则要 $(4n+4)$ 次，而本方案在签密过程仅需要 $(n+3)$ 次。显然，本方案的运算量远小于其他方案，其签密效率最高；在解签密阶段，ZHANG[12]方案要进行 n 次指数运算与 $5n$ 次对运算，HU[13]方案则有 $3n$ 次指数运算与 $4n+1$ 次对运算，而本方案在解签密阶段只需完成 n 次指数运算和 $n+4$ 次对运算，因此，本方案在同类方案中其运算量为最小。

表 1　FABSC 方案间的运算量比较

方案	签密过程	解签密过程
ZHANG[12]	$(2n+2)e$	$ne+5np$
HU[13]	$(4n+4)e$	$3ne+(4n+1)p$
本文方案	$(n+3)e$	$ne+(n+4)p$

5.3.3　密文长度分析

影响方案效率的另一个重要因素为通信量，主要体现在方案的密文长度。用$|G|$，$|G_T|$和$|Z_p|$表示密文元素分别在G，G_T和Z_p中的长度，如表 2 所示，由于本方案的签密文长度为$(n+2)|G|+2|G_T|$，均小于$(2n+2)|G|+|G_T|$与$(n+2)|G|+2|G_T|+|Z_p|$，与其他同类方案对比则具有密文长度短的特点。

表 2　FABSC 方案间的性能比较

方案	签密文长度	可公开验证性
ZHANG[12]	$(2n+2)\|G\|+\|G_T\|$	NO
HU[13]	$(n+2)\|G\|+2\|G_T\|+\|Z_p\|$	NO
本文方案	$(n+2)\|G\|+2\|G_T\|$	YES

对于方案通信量的分析，设$|Z_p|=192$ bit，$|G|=384$ bit，$|G_T|=384$ bit，同类方案间的通信量对比如表 3 所示，本方案的通信量明显小于同类方案，尤其对比方案[12]，随着签密属性个数增加，本方案的性能优势则体现得更加明显。

表 3　FABSC 方案间的通信量（bit）比较

属性个数	1	3	5	7
ZHANG[12]	2 304	2 688	4 992	6 528
HU[13]	2 112	2 496	3 648	4 416
本文方案	1 920	2 304	3 456	4 224

综上对比分析，本方案在签密与解签密阶段的运算量均远小于其他同类方案，具有较高运算效率。在具备短密文长度特点的同时，本方案还提供可公开验证性。因此，本方案在效率上比其他同类方案更为高效，在性能上则更具优越性、实用性。

6　结束语

针对网络通信安全的发展需求，本文利用密钥共享模型与双线性对构造一种模糊属性基的签密方案，通过设定属性门限值构造访问控制策略，并基于 DMBDH 和 CDH 困难问题证明了方案的机密性与不可伪造性，方案最终解决了多用户信息交互中的隐私泄漏及通信开销大等问题，在实际的网络通信环境中具有更高的安全保障及实用价值。

参考文献：

[1] SHAMIR A. Identity-based cryptosystems and signature schemes[A]. CRYPTO 1984 LNCS 196[C]. Springer, Heidelberg, 1985. 47-53.

[2] CANETTI R, HALEVI S, KATZ J. Chosen ciphertext security from identity based encryption[A]. Advances in Cryptology-Eurocrypt 2004, LNCS 3027[C]. Springer-Verlag, 2004. 207-222.

[3] WATERS B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions[A]. Advances in Cryptology-Crypto 2009, LNCS 5677[C]. Springer-Verlag, 2009. 619-636.

[4] LEWKO A, WATERS B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts[A]. Proceeding of TCC 2010, LNCS 5978[C]. Springer-Verlag, 2010. 455-479.

[5] LIANG X H. Research on Attribute Based Cryptosystem[D]. Shanghai: Shanghai Jiao Tong University, 2009.

[6] SAHAI A, WATERS B. Fuzzy identity-based encryption[A]. EUROCRYPT 2005 LNCS 3494[C]. Springer, Heidelberg, 2005. 457-473.

[7] YANG P Y, CAO Z F, DONG X L. Fuzzy identity based signature with applications to biometric authentication[J]. Computers & Electrical Engineering, 2011,37(4): 532-540.

[8] LI F G, KHAN M K. A biometric identity-based signcryption scheme[J]. Future Generation Computer Systems, 2012,28(1):306-310.

[9] WANG M W, REN Z Y, CAI J. A biometric signcryption scheme without bilinear pairing[A]. International Conference on Graphic and Image Processing (ICGIP 2012)[C]. Singapore, 2013.

[10] GOYAL V, PANDEY O, SAHAI A. Attribute-based encryption for fine-grained access control of encrypted data[A]. Proceedings of the 13th ACM Conference on Computer and Communications Security[C]. Alexandria, VA, USA, 2006. 221-238.

[11] ZHENG Y L. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)[A]. Cryptology-CRYPTO'97, LNCS 1294[C]. Berlin, New York, Tokyo, 1997. 165-179.

[12] ZHANG M W, YANG B. Fuzzy biometric signcryption scheme with bilinear pairings in the standard model[A]. Proceeding of PAISI 2010, LNCS 6122[C]. Springer-Verlag Berlin Heidelberg, 2010. 77-87.

[13] HU C Q, ZHANG N, LI H. Body area network security: a fuzzy attribute-based signcryption scheme[EB/OL]. http://www.seas.gwu.edu/~cheng/Publications/2012/BANSecurity-JSAC-2012.pdf, 2012-09-15/2013-05-06.

（下转第 20 页）

计算机应用, 2003, 23(5):45-47.
WU H S, FAN X L, WU W M, *et al*. An efficient one-time password authentication[J]. Journal of Computer Applications, 2003, 23(5):45-47.
[6] OpenID authentication 2.0-final[EB/OL]. http://openid.net/specs/openid-authentication-2_0.html.
[7] 江伟玉, 高能, 刘泽艺等. 一种云计算中的多重身份认证与授权方案[J]. 信息网络安全, 2012, (8):7-10.
JIANG W Y, GAO N, LIU Z Y, *et al*. A multi-identities authentication and authorization schema[J]. Netinfo Security, 2012, (8):7-10.
[8] OASIS standard SAML V2.0[EB/OL]. http://docs.oasis-open.org/secu-rity/saml/v2.0/.
[9] LI Z, GARCIA-LUNA-ACEVES J J. New non-interactive key agreement and progression (NIKAP) schemes and their applications to security in ad hoc network[A]. The 2005 International Workshop on Wireless and Sensor Networks Security(WSNS 2005)[C]. Washington DC, USA, 2005. 6.
[10] JUANG W S, CHIU J Y, CHANG H Y. A secure and efficient delegation-based authentication scheme in public clouds[A]. The 1st Cross-Straits Conference On Information Security[C]. Hangzhou, China, 2011. 96-102.
[11] 杜瑞忠，田俊峰，张焕国. 基于信任和个性偏好的云服务选择模型[J]. 浙江大学学报(工学版), 2013, (1):53-61.
DU R Z，TIAN J F，ZHANG H G. Cloud service selection model based on trust and personality preference[J]. Journal of Zhejiang University(Engineering Science), 2013, (1):53-61.

作者简介：

何文才（1956-），男，黑龙江鹤岗人，北京电子科技学院教授，主要研究方向为编码理论及其应用、信息安全及保密。

杜敏（1987-），女，陕西西安人，西安电子科技大学硕士生，主要研究方向为网络通信安全。

陈志伟（1989-），男，河南周口人，西安电子科技大学硕士生，主要研究方向为密码学与信息安全。

刘培鹤（1972-），男，黑龙江鹤岗人，北京电子科技学院教师，主要研究方向为信息安全。

韩妍妍（1982-），女，黑龙江哈尔滨人，北京电子科技学院助理研究员，主要研究方向为可视密码、密码学。

（上接第 13 页）

[14] GUO Z Z, LI M C, FAN X X. Attribute-based ring signcryption scheme[J]. Security and Communication Networks, 2013, 6(6):790-796.
[15] LI X X, QIAN H F, WENG J. Fully secure identity-based signcryption scheme with shorter signcryptext in the standard model[J]. Mathematical and Computer Modelling, 2013, 57(3-4):503-511.
[16] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11):612-613.

林志强（1988-），男，福建漳州人，武警工程大学硕士生，主要研究方向为密码学。

作者简介：

杨晓元（1959-），男，湖南湘潭人，武警工程大学教授，主要研究方向为信息安全与密码学。

韩益亮（1977-），男，甘肃会宁人，博士，武警工程大学副教授，主要研究方向为密码学。