基于属性的广义签密方案

韩益亮[1,2] 白寅城[1] 房鼎益[2] 杨晓元[1]

[1]武警工程大学电子技术系，西安 710086
[2]西北大学信息科学与技术学院，西安 710127
yilianghan@hotmail.com

Attribute-based Generalized Signcryption Scheme

Han Yiliang, Bai Yincheng, Fang Dingyi, Yang Xiaoyuan

[1] (Department of Electronic Technology, Engineering University of Armed Police Force, Xi'an 710086)

[2] (School of Information Science and Technology, Northwest University, Xi'an 710127)

Abstract The existed signcryption schemes has the shortages of failing to send the data to the recipients with fuzzy identities and failing to dealing the precise access control. By employing the attribute set, the data could be distributed according to the user's attribute. By identify the users' key, it could provide the separate or combined confidentiality and authenticity adaptively. It shows that the scheme is undistinguished under chosen cipher text attack under DBDH assumption, and it is unforgeable under chosen message attack under CDH assumption. Compared with similar schemes, the length of the cipher text and key are not increased linearly when the attributes is increasing.

Key words identity-based; signcryption; standard model; public verification; provably secure

摘要 现有签密方案存在不能向模糊身份的接收方发送数据、且对数据的共享访问控制不够精细，而基于属性的签密也无法自适应地实现机密性、认证性以及机密且认证等不同的安全需求。本文在离散对数和随机预言机模型下提出了一种基于属性的广义签密方案。通过引入属性集，使数据可以凭用户的属性为依据进行分发；通过区分通信双方所持有的密钥，可以提供单独的机密性、认证性和复合的机密性和认证性功能。在 DBDH 假设下的安全性分析表明方案证明了方案在选择密文攻击下达到了不可区分性，在 CDH 假设下的安全性分析表明方案在选择消息攻击下达到了不可伪造性。与其它类似方案相比，本方案的在属性个数增加时，密文长度和密钥长度不会线性增长，效率更高。

关键词 基于身份；签密；标准模型；公开验证；可证安全

中图法分类号 TP309

保密性和认证性是通信过程中重要的两个安全性特征。1997 年 Zheng[1]等人提出签密的概念，能够在一个逻辑步骤内实现加密和签名操作，实现了保密和认证的功能。然而其成本开销远低于先签名后加密操作的开销总和，但是仍然不能够符合某些特殊的应用需求。在有些只需要加密或者签名的操作中签密方案便失去了优势，在加密、签名和签密之间的频繁转换也必定消耗大量的资源。2006 年韩益亮[2]等人提出的广义签密概念，能够在一个模块内灵活地选择加密、签名或者签密操作，能够应用到更广泛的环境中。

身份基密码体制[3]简化了传统公钥密码体制中的证书管理问题，其能够将某些用户的信息（例如年

收稿日期：2014-10-05
基金项目：国家自然科学基金（61103231, 61272492），中国博士后科学基金资助项目（2014M562445），

龄、身高等）作为公钥。2001 年 Boneh 等人[4] 利用双线性对提出了第一个身份基加密方案。Sahai 和 Waters[5]考虑到用户隐私方面的问题，提出基于模糊身份加密方案，其中用户身份用多个用户的属性来代替，这也是基于属性密码方案的雏形。Goyal[6]在 2006 年将基于属性的加密方案分为基于密钥策略的(Key Policy ABE,KP-ABE）和基于密文策略的(Ciphertext Policy ABE,CP-ABE) 属性基加密方案。随后 Hemanta[7]在 2008 年提出了基于属性的签名方案。Gagne[8]等人在 2010 年首次提出基于属性的签密（Attribute Based Signcryption,ABSC）方案。但是由于方案性能单一并且效率不高，2012 年张国印[9]等人提出了具有动态门限的属性基签密方案，并且在密文长度上做了较大改进。2013 年刘佳[10]等人在矢量空间上提出了基于属性的签密方案。由于签名属性隐私等问题没有很好地解决，相继提出的 ABSC 方案[11]不断地进行完善。

本文结合广义签密和基于属性的密码体制的特点，根据 2010 年 Li[12]的属性基签名方案的思想提出了基于属性的广义签密方案，同时具有多接收者和用户属性的隐私安全性特点。相比 2013 年提出的功能相似的方案[13]而言，本方案在模块选择上更具灵活性。本方案实现了消息保密性，并且具有广义功能。进一步拓宽了应用场景，并且在随机预言机模型下证明本方案具有适应性选择密文攻击不可区分性和适应性选择明文攻击不可伪造性。

1. 基础理论

1.1 双线性对

设 g 是阶为素数 p 的循环群 G 和 G_1 的生成元，映射 $e:G\times G\to G_1$ 称为双线性对，需要满足以下三条性质：

1)双线性性。存在任意 $g_1,g_2\in G,x,y\in {}_RZ_q^*$，$e(g_1^x,g_2^y)=e(g_1,g_2)^{xy}$ 成立。

2)非退化性。存在对任意的 $g_1,g_2\in G$ 使得 $e(g_1,g_2)\neq 1$。

3)可计算性。存在对任意的 $g_1,g_2\in G$，有一个有效算法能够计算 $e(g_1,g_2)\in G_1$。

可以通过超椭圆曲线或者椭圆曲线的 Tate 对、Weil 对变形来得到双线性对[4]。

1.2 困难性假设

1）DBDH 困难性假设

定义 1 若没有攻击者能够至少以 ε 优势在下面的游戏中获胜，则 $\varepsilon-$DBDH 假设成立：

挑战者 B 随机选取参数 $a,b,c,z\in Z_p$ 和 $\eta\in\{0,1\}$，若 $\eta=1$ 则 B 输出参数 $(g,g^a,g^b,g^c,e(g,g)^{abc})$；若 $\eta=0$ 则输出 $(g,g^a,g^b,g^c,e(g,g)^z)$。攻击者 A 对 η 的猜测为 η'。

若

$$|\Pr[A(g,g^a,g^b,g^c,e(g,g)^{abc})=1]-\Pr[A(g,g^a,g^b,g^c,e(g,g)^z)=1]|\geq\varepsilon$$

则 A 至少有 ε 的优势能够解决 DBDH 问题。

2）CDH 困难性假设

定义 2 若没有攻击者能够至少以 ε 优势在下面的游戏中获胜，则 $\varepsilon-$CDH 假设成立：

挑战者 B 随机选取参数 $a,b\in Z_p$，输出参数值 (g,g^a,g^b)。攻击者则尝试得到结果 $g^{ab}\in G$。

若 $\Pr[A(g,g^a,g^b)=g^{ab}]\geq\varepsilon$，则 A 至少有 ε 的优势能够解决 CDH 问题。

1.3 基于属性的广义签密方案安全性定义

定义 3 若攻击者 A 能够在多项式时间里以可以忽略的概率攻破如下游戏，则基于属性的广义签密方案具有选择属性集下的安全性。

1）系统初始化算法。攻击者 A 的挑战属性集为 γ^*，且不能对其密钥生成询问；挑战者 B 选择安全参数 s，输出系统公钥 PK 以及主密钥 MK。

2）查询算法。攻击者 A 对属性 Ω 进行密钥生成查询，挑战者 B 返回密钥 d_Ω。

3）挑战算法。挑战者 B 收到来自 A 的等长度明文消息 m_0，m_1，签名属性集合 S^*，加密属性集合 γ^*

及其符合的访问结构，并且 A 没有进行过 γ^* 的密钥生成询问。B 随机选取 $b\in\{0,1\}$ 并对签名属性集进行密钥生成查询，最后发送给 A 签密文 σ^*

4）猜测。A 继续进行询问，但不能对 γ^* 进行询问。最终挑战者选择 b' 作为 b 的猜测。若 $b'=b$ 则攻击者在游戏中获胜。获胜的优势为 $Adv_A^{IND-CPA}=|2\Pr[b=b']-1|$。

定义 4 若攻击者 A 能够在多项式时间里以可以忽略的概率攻破如下游戏，则基于属性的广义签密方案具有选择属性集下的选择明文攻击不可伪造性。

系统初始化算法同定义 3。

查询算法中攻击者 A 进行如下查询：

1)签密和密钥生成查询统定义 3。

2)解签密查询中 A 对用户属性、解签密访问结构和签密文 σ 进行查询，B 输出消息 m，否则输出 $\perp$。

伪造。若 A 没有对签名属性集进行过密钥生成查询，A 生成签密文 σ^*（不是之前签密询问时返回的结果），并且 σ^* 为有效签密文。则攻击者 A 获胜的优势为 $Succ_A^{EUF-CMA}=\Pr[Awins]$。

2 基于属性的广义签密方案

1）参数生成。PKG 随机选择 $s,r\in Z_q^*$。假设由 r-1 个属性组成缺省属性集 $M=\{M_1,M_2,\cdots,M_{r-1}\}$，$M_i\in Z_q^*$，$1\le i\le r-1$。选择双线性对 $e:G\times G\to G_1$，随机选择 $g,g_2\in G,k\in Z_q^*$ 并计算 $g_1=g^k$，$E=e(g_1,g_2)$。拉格朗日系数设定为 $\Theta_{x,Z}(y)=\prod_{z\in Z,z\ne x}\frac{y-z}{x-z}$，随机选择属性集 $\Omega\in Z_q^*$。哈希函数分别为 $H:\{0,1\}^*\to G$，$H_1:\{0,1\}^*\times\{G\}^*\to G$。加解密算法分别为 $E_\theta(\cdot),D_\theta(\cdot)$。系统主密钥为 k，系统公开参数为 $params=(s,r,q,G,G_1,e,g,g_1,g_2,E,H,H_1,E_\theta(\cdot),D_\theta(\cdot))$。

2）密钥生成。私钥生成中心随机选取 r-1 次满足 $l(0)=a$ 的多项式 l(n)。用户 ID 的属性集为 $\gamma_{ID}\in\Omega$，并生成属性集 $\gamma_{ID}'=\gamma_{ID}\cup M$。随机选取 $t_n\in Z_q^*$，$n\in\gamma_{ID}'$。计算用户私钥 $R_n=(r_{no},r_{n1})=(g_2^{l(n)}H(i)^{t_n},g^{t_n})$。

3）签密。此方案中支持的断言为 $T_{\theta,\gamma^*}(\cdot)$，其中 γ^* 为属性集，θ 为门限值，$1\le\theta\le r$。若属性集 γ' 至少包括属性集 γ^* 里 θ 个元素则 γ' 满足断言 $T_{\theta,\gamma^*}(\cdot)$。即：$T_{\theta,\gamma^*}(\gamma')=\begin{cases}1,|\gamma'\cap\gamma^*|\ge k\\0,\text{其他}\end{cases}$。

方案中的加密断言 $T_{\theta',\gamma_2^*}(\cdot)$，签名断言 $T_{\theta,\gamma_1^*}(\cdot)$，其中的 $|\gamma_1^*|=v_1$，$|\gamma_2^*|=v_2$。发送方 A 属性集合为 $\gamma_A=\{n_1,n_2,\cdots,n_{vA}\}$，并满足 $T_{\theta,\gamma_1^*}(\gamma_A)=1$。A 的属性子集为 $\gamma_A'\subseteq\gamma_1^*\cap\gamma_A$。$M$ 中的 $r-\theta$ 个缺省属性组成缺省属性集合 $M_1'=\{n_{\theta+1},n_{\theta+2},\cdots,n_r\}\subset M$，$M$ 中的 $r-\theta'$ 个缺省属性构成缺省属性集合 $M_2'=\{n_{\theta'+1},n_{\theta'+2},\cdots,n_r\}\subset M$。随机选择 $\eta\in Z_q^*$，计算 $\sigma_0=g^\eta$，$\{\sigma_n=H(n)^\eta\}_{n\in\gamma_2^*\cup M_2'}$。随机选择 $v_1+r-\theta$ 个随机数 $t_n'\in Z_q^*$，计算 $\sigma_0'=[\prod_{n\in\gamma_A'\cup M_1'}r_{n,0}^{\Theta_{n,\eta}(0)}][\prod_{n\in\gamma_1^*\cup M_1'}H(n)^{t_n'}]\cdot H_1(m,\{\sigma_n\}_{n\in\gamma_2^*\cup M_2'})^\eta$，$\theta=E^\eta$，$c=E_\theta(m)\oplus g^{\sigma_0'}$。若为加密操作，输出密文 $\sigma=\{\sigma_0,\ \sigma_0',\{\sigma_n\}_{n\in\gamma_2^*\cup M_2'},0,c\}$。否则计算 $\{\sigma_n'=r_{n,1}^{\Theta_{n,\eta}(0)}g^{t_n'}\}_{n\in\gamma_A'\cup M_1'}$，$\{\sigma_n'=g^{t_n'}\}_{n\in\gamma_1^*\cup M_1'}$。输出

密文 $\sigma=\{\sigma_0,\ \sigma_0',\{\sigma_n\}_{n\in\gamma_2*\cup M_2'},\{\sigma_n'\}_{n\in\gamma_A*\cup M_1'},c\}$。若以上签密过程为单独的签名过程，则发送方私钥为空集，因此 $c=E_\theta(m)\oplus g^{\sigma_0'}=E_0(m)\oplus g^0=m$。

4）解签密。a)签密：接收方 B 属性集合为 $\gamma_B=\{n_1,n_2,\cdots,n_{vB}\}$，并满足 $T_{\theta,\gamma_2*}(\gamma_B)=1$。若密文的签名者满足断言 $T_{\theta,\gamma_1*}(\cdot)$ 则继续，否则终止操作。计算 $H_1(m,\{\sigma_n\}_{n\in\gamma_2*\cup M_2'})$，若等式

$$E=\frac{e(g,\sigma_0')}{[\prod_{n\in\gamma_1*\cup M_1'}e(H(n),\sigma_n')]e(H_1(m,\{\sigma_n\}_{n\in\gamma_2*\cup M_2'}),\sigma_0)} \quad (1)$$

成立则继续，否则终止操作。B 选择属性集 $\gamma_B'\subseteq\gamma_2*\cap\gamma_B$。计算 $\{r_{n0}'=r_{n0}\}_{n\in\gamma_B'\cup M_2'}$，$\{r_{n0}'=H(n)\}_{n\in\gamma_2*/\gamma_B'}$，$\{r_{n1}'=r_{n1}\}_{n\in\gamma_B'\cup M_2'}$，$\{r_{n1}'=g\}_{n\in\gamma_2*/\gamma_B'}$ 计算 $\theta=\prod_{n\in\gamma_2*\cup M_2'}(\frac{e(r_{n0}',\sigma_0)}{e(\sigma_n,r_{n1}')})^{\Delta_{n\eta}(0)}$，$m=D_\theta(c)\oplus g^{\sigma_0'}$。

b) 签名：若接收方私钥为空集，则 $c=E_\theta(m)\oplus g^{\sigma_0'}=E_0(m)\oplus g^0=m$，则加密过程被屏蔽。

c)加密：若 $\{\sigma_n'\}_{n\in\gamma_A*\cup M_1'}=0$ 则为加密操作，计算 $\{r_{n0}'=r_{n0}\}_{n\in\gamma_B'\cup M_2'}$，$\{r_{n0}'=H(n)\}_{n\in\gamma_2*/\gamma_B'}$，$\{r_{n1}'=r_{n1}\}_{n\in\gamma_B'\cup M_2'}$，$\{r_{n1}'=g\}_{n\in\gamma_2*/\gamma_B'}$，计算 $\theta=\prod_{n\in\gamma_2*\cup M_2'}(\frac{e(r_{n0}',\sigma_0)}{e(\sigma_n,r_{n1}')})^{\Delta_{n\eta}(0)}$，$m=D_\theta(c)\oplus g^{\sigma_0'}$。

3 安全性分析

3.1 正确性分析

$$\frac{e(g,\sigma_0')}{[\prod_{n\in\gamma_1*\cup M_1'}e(H(n),\sigma_n')]e(H_1(m,\{\sigma_n\}_{n\in\gamma_2*\cup M_2'}),\sigma_0)}$$
$$=\frac{e(g,[\prod_{n\in\gamma_A'\cup M_1'}(g_2^{l(n)}H(n)^{t_n})^{\Theta_{n,\eta}(0)}][\prod_{n\in\gamma_1*\cup M_1'}H(n)^{t_n'}]\cdot H_1(m,\{\sigma_n\}_{n\in\gamma_2*\cup M_2'})^\eta)}{[\prod_{n\in\gamma_1*\cup M_1'}e(H(n),g^{t_n\Theta_{n,\eta}(0)}g^{t_n'})\prod_{n\in\gamma_1*/M_A'}e(H(n),g^{t_n'})](H_1(m,\{\sigma_n\}_{n\in\gamma_2*\cup M_2'}),g^\eta)} \quad (2)$$
$$=\prod_{n\in\gamma_A'\cup M_1'}(g,g_2^{l(n)})^{\Theta_{n,\eta}(0)}=E$$

$$\theta=\prod_{n\in\gamma_2*\cup M_2'}(\frac{e(r_{n0}',\sigma_0)}{e(\sigma_n,r_{n1}')})^{\Delta_{n\eta}(0)}$$
$$=\prod_{n\in\gamma_2*\cup M_2'}(\frac{e(g_2^{l(n)}H(n)^{t_n},g^\eta)}{e(H(n)^\eta,g^{t_n})})^{\Delta_{n\eta}(0)}\prod_{n\in\gamma_2*/M_2'}(\frac{e(H(n),g^\eta)}{e(H(n)^\eta,g)})^{\Delta_{n\eta}(0)} \quad (3)$$
$$=\prod_{n\in\gamma_2*\cup M_2'}(g_2^{l(n)},g^\eta)^{\Delta_{n\eta}(0)}=E^\eta$$

3.2 安全性证明

定理 1 若 DBDH 困难问题在群 G 上成立，那么攻击者不能够以不可忽略的优势攻击本方案，即本方案具有选择属性集下的安全性。

证明：若攻击者 A 最多进行 q_{H_n} 次 H_n 询问，n=1,2,q_{SC} 次密钥生成询问，q_η 次签密询问和 q_{US} 次解签密询问的条件下，用多项式时间以 ε 的优势攻击定义 3 中的游戏。

系统设置：算法 F 构造 $g_1=g^a,g_2=g^b$。缺省属性集合为 $M=\{M_1,M_2,\cdots,M_{r-1}\}$，其中随机选取系统参数 $s,r\in Z_q*$。挑战者 A 用于挑战的签名属性集合 γ_1* 以及门限为 $1\le\theta\le r$，加密属性集合 γ_2* 以及门限为 $1\le\theta'\le r$。随机选择的缺省属性集合为 $M_1'*\subseteq M$，$|M_1'*|=r-\theta$，$M_2'*\subseteq M$，$|M_2'*|=r-\theta'$。各自的签密和加密断言分别为 $T_{\theta,\gamma_1*}(\cdot)$ 和 $T_{\theta',\gamma_2*}(\cdot)$。

随机预言查询：

H_1 预言机：查询 n，若 n 在保存 H_1 的列表 K_1 里，返回相应结果。否则若 $n\in\gamma_2*\cup M_2'*$，则随机选择 $x_n\in Z_q*$ 并记录到序列 K_1 中 $H_1(n)=g_1^{x_n}$，否则随机

选择 $x_n, y_n \in Z_q^*$ 并记录到序列 K_1 中 $H_1(n) = g_1^{-x_n} g^{y_n}$。

H_2 预言机：随机选择 $h_1, h_2 \in [1, q_{H_2}]$。查询 n，若 n 在保存 H_2 的列表 K_2 里，返回相应结果。否则若 $n \neq h_1, h_2$，随机选择 $x_n, z_n \in Z_q^*$ 并记录到保存 H_1 的列表 K_2 中 $H_2(u_n, \{\sigma_m\}_{m\in\Omega}) = g_1^{z_n} g^{x_n}$。若 $n = h_1$ 则随机选择 $x_{h_1} \in Z_q^*$ 并记录到列表 K_2 中 $H_2(u_n, \{\sigma_m\}_{m\in\Omega}) = g^{x_{h_1}}$，若 $n = h_2$ 则随机选择 $x_{h_2} \in Z_q^*$ 并记录到列表 K_2 中 $H_2(u_n, \{\sigma_m\}_{m\in\Omega}) = g^{x_{h_2}}$。

密钥查询：定义集合 O, O', P，使得 $P = O' \cup \{0\}$，$|O'| = r-1$，$O \subseteq O' \subseteq P$，$O = (\gamma_A \cap \gamma_2^*)M_n'$。若 γ_n 满足 $|\gamma_A \cap \gamma_2^*| < \theta'$ 则首先令 $N_n = (g_1^{a_n} H_1(n)^{b_n}, g^{b_n})$，其中 $n \in O', a_n, b_n \in Z_q^*$，即满足 $l(i)=a_n$，$l(0)=a$ 的 r-1 次多项式 $l(i)$。对 $n \in O'$，令 $b_n = \frac{\Theta_{0,Z}(n)}{y_n} b + b_n'$，

$$l(n) = \sum_{m\in O'} \Theta_{m,Z}(n) l(m) + \Theta_{0,Z}(n) l(0) \quad ,$$

$$N_n = (g_2^{\frac{\Theta_{0,Z}(n)x_n}{y_n} + \sum_{m\in O'} \Theta_{m,Z}(n) l(m)} (g_1^{-y_n} g^{x_n})^{t_n'}, g_2^{\frac{\Theta_{0,Z}(n)}{y_n}} g^{t_n})_{n\in\gamma_n}$$

。否则查询失败。

签密查询：若 $|\gamma_A \cap \gamma_2^*| < \theta'$ 则根据 γ_A 产生的私钥 $R_{An} = (r_{no}, r_{n1})$ 生成密文发送给 A。否则 M 中的 $r-\theta$ 个缺省属性组成集合 M_1'，M 中的 $r-\theta'$ 个缺省属性构成缺省属性集合 M_2'。假设 $\gamma_A \cup M_1' = \{n_1, n_2, \cdots, n_r\}$，随机选择 $t_n, \eta' \in Z_q^*$，假设 $\eta = \frac{-1}{Z_{n_r}} b + \eta'$ 计算

$$\sigma_0 = g^{\eta} = g_2^{\frac{-1}{Z_{n_r}}} g^{\eta'} \quad , \quad H_2(m, \{\sigma_n\}_{n\in\gamma_2^*\cup M_2'}) = g_1^{z_{n_r}} g^{y_n} \quad ,$$

$$\sigma_0' = g_2^{a} \prod_{n\in\gamma_1'\cup M_1'} H_1(n)^{t_n} H_2(m, \{\sigma_n\}_{n\in\gamma_2^*\cup M_2'})^{\eta}$$

$$= (g_1^{z_{n_r}} g^{y_n})^{\eta'} \prod_{n\in\gamma_1'\cup M_1'} H_1(n)^{t_n} g_2^{\frac{-y_n}{Z_{n_r}}} \quad ,$$

$\{\sigma_n' = g^{t_n'}\}_{n\in\gamma_1^*\cup M_1'}$，$\{\sigma_n = g^{y_n\eta} = g_2^{\frac{-y_n}{Z_{n_r}}} g^{y_n\eta'}\}_{n\in\gamma_2^*\cup M_2'}$，$c_n = E_\theta(m_n) \oplus g^{\sigma_0'}$，其中 θ 为随机选择。输出密文 $\sigma = \{\sigma_0, \sigma_0', \{\sigma_n\}_{n\in\gamma_2^*\cup M_2'}, \{\sigma_n'\}_{n\in\gamma_A^*\cup M_1'}, c_n\}$。

解签密查询：若 $|\gamma_A \cap \gamma_2^*| < \theta'$，$|\gamma_B \cap \gamma_2^*| < \theta'$ 则生成私钥，解密返回明文 m_n 或 $\perp$。否则返回无效的签名。若攻击者已经进行了签密查询，则终止。最后 A 选择等长明文 m_0 和 m_1 以及 γ_1^*, γ_2^* 的缺省属性集合 $M_1'^*, M_2'^*$，但是没有进行密钥查询。否则终止查询。

挑战：属性集合 $\gamma_A'^* \in \gamma_1'^*$ 由 θ 个属性组成。查询得到 $\gamma_A'^*$ 的密钥 $r_{n,0}$，$r_{n,1}$。计算 $\sigma_0^* = g^{c\eta^*}$，

$$\{\sigma_n^* = H_1(n)^{c\eta^*} = g^{cy_n\eta^*}\}_{n\in\gamma_2^*\cup M_2'^*} \quad ,$$

$$\sigma_0'^* = [\prod_{n\in\gamma_A'^*\cup M_1'^*} r_{n,0}^{\Theta_{n,\eta}(0)}][\prod_{n\in\gamma_1^*\cup M_1'^*} H_1(n)^{t_n'}]$$

$$H_2(m, \{\sigma_n^*\}_{n\in\gamma_2^*\cup M_2'^*})^{c\eta^*} \quad ,$$

$$= [\prod_{n\in\gamma_A'^*\cup M_1'^*} r_{n,0}^{\Theta_{n,\eta}(0)}][\prod_{n\in\gamma_1^*\cup M_1'^*} (g_1^{-y_n} g^{x_n})^{t_n'}] g^{cy_{h_y}\eta^*} \quad ,$$

$\theta = C^{\eta^*}$ ，$c^* = E_\theta(m) \oplus g^{\sigma_0'^*}$ ，

$\{\sigma_n'^* = r_{n,1}^{\Theta_{n,\eta}(0)} g^{t_n'}\}_{n\in\gamma_A'^*\cup M_1'^*}$，$\{\sigma_n'^* = g^{t_n'}\}_{n\in\gamma_1^*/M_A'^*}$，输出 $\sigma^* = \{\sigma_0^*, \sigma_0'^*, \{\sigma_n^*\}_{n\in\gamma_2^*\cup M_2'^*}, \{\sigma_n'^*\}_{n\in\gamma_A^*/M_A'^*}, c^*\}$。若 $H_2(m, \{\sigma_n^*\}_{n\in\gamma_2^*\cup M_2'^*}) \neq g^{y_{h_y}}$ 游戏结束，该过程可以查询 σ^* 是否合法但不能进行 σ^* 的解签密查询和 γ_2^* 的密钥查询。

猜测：若 A 输出的 $b'=b$，则 $C = e(g,g)^{abc}$ 即在游戏中胜利。其优势分析为：A 没有对 γ_2^* 查询的概率至少为 $1/q_{H_1}$，拒绝有效密文概率最多为 $q_{US}/2^s$，挑

战 γ_1^*,γ_2^* 的概率至少 $1/\binom{2}{q_{H_1}}$，选择 $M_1'^*,M_2'^*$ 的概率至少 $1/\binom{r-\theta}{r-1}$。$H_2(m,\{\sigma_n^*\}_{n\in\gamma_2^*\cup M_2'^*})=g^{y_{h_y}}$，$b\in\{0,1\}$ 的概率至少 $1/q_{H_2}^2$。则优势可计算为：

$$\varepsilon'=\frac{((\varepsilon+1)/2-1/1)(1-q_{US}/2^S)}{q_{H_1}q_{H_2}^2\binom{2}{q_{H_1}}\binom{r-\theta}{r-1}\binom{r-\theta'}{r-1}}。$$

定理 2 若 CDH 困难问题在群 G 上成立，那么攻击者不能够以不可忽略的优势攻击本方案，即本方案具有选择属性集下的选择明文攻击不可伪造性。

证明：算法 B 收到 CDH 问题实例，它的目的是根据 (g^a,g^b) 计算 g^{ab}。该过程跟定理 1 类似。F 设置相应的系统参数，B 对攻击者 A 进行随机预言查询、密钥查询、签密查询、解签密查询的回答。若 A 不选择 γ_1^*,γ_2^*、$M_1'^*,M_2'^*$ 或 $H_2(m,\{\sigma_n^*\}_{n\in\gamma_2^*\cup M_2'})\neq g^{y_h}$ 则游戏结束。则

$$\frac{e(g,\sigma_0'^*)}{[\prod_{n\in\gamma_1^*\cup M_1'}e(H_1(n),\sigma_n'^*)]e(H_2(m,\{\sigma_n^*\}_{n\in\gamma_2^*\cup M_2'}),\sigma_0^*)}$$
$$=e(g,\sigma_0'^*/\prod_{n\in\gamma_1^*\cup M_1'}\sigma_n'^{*x_n}\sigma_0^{*y_h})=e(g,g^{ab})$$

。

因此在游戏中获胜的优势为

$$\varepsilon'=\frac{\varepsilon(1-q_{US}/2^S)}{q_{H_1}q_{H_2}\binom{2}{q_{H_1}}\binom{r-\theta}{r-1}\binom{r-\theta'}{r-1}}。$$
$$>\frac{(r-\theta)(r-\theta')(2\varepsilon-q_{US}/2^{S-1})}{q_{H_2}q_{H_1}^3(r-1)^{2r-\theta-\theta'}}$$

4 效率分析

1) 计算效率分析

通信代价和计算代价是方案分析中需要考虑的两个重要因素，分别由密文长度和签密、解签密操作的计算代价决定。本节利用表 1 分别将本方案与功能相似的具有代表性的同类基于属性的签密方案[14]在计算量和密文长度签密时的密文长度和计算量进行比较。其中 e、p 分别表示指数运算和双线性对运算，$|G|$，$|G_1|$分别表示群的模，l 表示属性数量，n_m 表示消息长度。

表 1 运算量和密文长度比较

方案	签密	解签密	密文长度
方案[14]	e+8p	(6+2l)e	(5+2l)$\|G_1\|$+n_m
本方案	e+6p	2le	4$\|G_1\|$+n_m
	e+8p	(l+2)e	
	e+9p	(3l+2)e	

分析结果表明本方案在选择签密模块时具有与其相当的效率，但是由于方案[14]只能实现单一的签密功能，在选择加密或签名模块时无论在计算量还是存储代价方面本方案都有较大提高。并且方案与方案[14]相比密文长度不随属性的数量而线性增长。其中两个方案的密文长度与属性数量的关系可以通过图 1 更清晰地反映出来，假设消息长度 n_m=64 bits，群 G_1 的模为 128 bits。

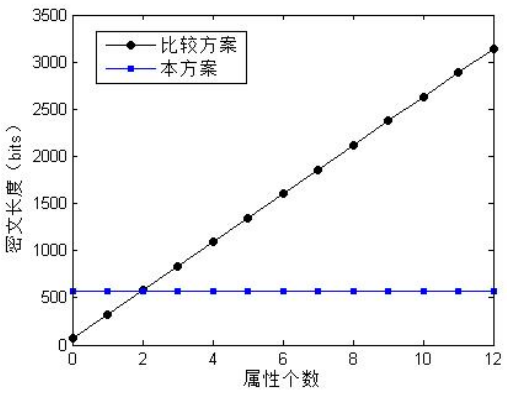

图 1 密文长度比较

2) 存储效率分析

另一方面，系统公钥和用户私钥的长度也是消息传输中需要考虑的重要因素。在此本文将利用表 2 与 2013 年方案[13]对密钥长度和密文长度进行比较。

表 2 存储代价比较

方案	系统公钥	用户私钥	密文长度
方案[13]	(n+4)$\|G\|$	2n(n+1)$\|G\|$	5$\|G_1\|$+n_m
本方案	4$\|G\|$+3$\|G_1\|$	$\|G\|^{n+1}$+$\|G\|$	4$\|G\|$+n_m

存储代价的三个主要影响因素主要体现在密钥长度和密文长度两方面。通过表 2 可以看出本文与方案[13]比较而言用户私钥较长，但是在系统公钥和密文长度方面本方案具有较大优势，并且方案[13]的系统公钥长度与用户属性的最大个数存在线性关系。利用

下面图 2 将两个方案的系统公钥长度与属性个数的关系更清晰地表示出来，其中假设群 G 的模为 64 bits，群 G_1 的模为 128 bits。

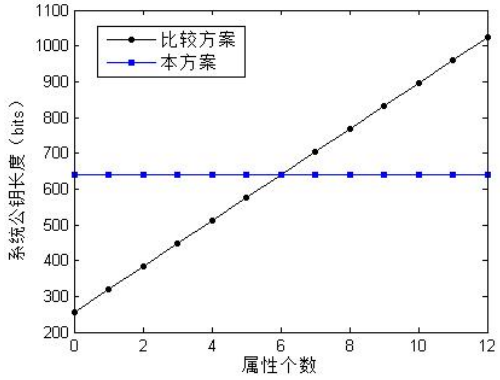

图 2 系统公钥长度比较

通过图表分析可以得出，在不影响功能选择的情况下该方案能够适应较为复杂的网络结构。尤其是在对系统的计算效率要求较高、用户数量庞大、属性数目较多的网络环境中本方案具有较大优势。

5 结论

结合广义签密和基于属性的密码体制的优点，本文提出了基于属性的广义签密方案，并在随机预言机模型下证明方案是安全的。本方案能够自适应地在一个密码模块内选择目前数据通信中所需要的保密性或认证性或者二者兼备的签密操作，并能够在只需要某一种功能时能够自动屏蔽另一种操作，兼顾考虑到了功能的灵活选择和效率的提高，适用范围更广。

参 考 文 献

[1] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption)<< cost(signature)+cost(encryption) [C]. Advances in Cryptology-CRYPTO'97, LNCS 1294, Springer-Verlag, 1997:165-179

[2] Han Y, Yang X. New ECDSA-Verifable generalized signcryption [J]. Chinese Journal of Computers, 2006, 11: 2003-2012

[3] Shamir A. Identity-based cryptosystems and signature schemes[C] //Advances in cryptology. Springer Berlin Heidelberg, 1985: 47-53

[4] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]//Advances in Cryptology—CRYPTO 2001. Springer Berlin Heidelberg, 2001: 213-229

[5] Sahai A, Waters B. Fuzzy identity-based encryption [C]. In Eurocrypt 2005, LNCS 3494: 457-473

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute Based Encryption for Fine-Grained Access Conrol of Encrypted Data[A]. In: Proceedings of the 13th ACM conference on Computer and communications security2006[C]. Alexandria, Virginia, USA, 2006: 89-98

[7] Ma J, Prabhakaran M, Rosulek M. Attribute-based signatures: achieving attribute-privacy and collusion-resistance [R/OL]. Cryptology ePrint Archive, Report 2008/328. http://eprint. iacr. org / 2008/328

[8] Gagne´ M, Narayan S, Safavi-Naini R. Threshold attribute-based signcryption [C]. In SCN 2010, LNCS 6280, 2010: 154–171

[9] 张国印, 付小晶, 马春光. 一个动态门限的基于属性签密方案[J]. 电子与信息学报, 2012, 34(11): 2680-2686

[10] 刘佳, 王建东, 庄毅. 基于矢量空间的属性基签密方案[J]. 电子学报, 2013, 41(4): 776-780

[11] Meng X Y, Chen Z, Meng X Y. Privacy-Preserving Decentralized Key-Policy Attribute-Based Signcryption in Cloud Computing Environments[J]. Applied Mechanics and Materials, 2014, 475: 1144-1149

[12] Li J, Au M H, Susilo W, et al. Attribute-based signature and its applications[C]//Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ACM, 2010: 60-69

[13] 韩益亮，卢万谊，武光明，杨晓元，适用于网络大数据的属性基广义签密方案[J].计算机研究与发展，2013，50(Suppl.II):23-29

[14] 陈少真, 王海斌. 高效的基于属性的签密方案[J]. 信息工程大学学报, 2011, 12(5): 526-531

韩益亮，男，1977 年生，副教授，博士，博导，研究方向：密码学与信息安全。

白寅城，男，1991 年生，硕士研究生，研究方向：密码学与信息安全

房鼎益，男，1959 年生，博士，教授，博导，研究方向：物联网与信息安全。

杨晓元，男，1959 年生，教授，博导，研究方向：密码学与信息安全。