适用于移动网络的属性基在线/离线签密方案

姜 頔 韩益亮

(武警工程大学电子技术系 西安 710086) (武警部队网络与信息安全重点实验室 西安 710086)

摘 要 签密能够同时实现加密和签名的功能,并且代价小于传统方法。在线/离线技术能够有效提高签名与加密效率,适用于计算能力严格受限的移动网络终端设备。针对现有的属性签密方案实用性不强、效率低下的现状,提出了一个基于属性的在线/离线签密方案,在随机预言机模型下,利用判定双线性Diffie-Hellman倒转(l-DBDHI)问题和计算Diffie-Hellman(CDH)问题的困难性,证明了该方案满足在适应性选择密文攻击下的不可区分性以及适应性选择消息下的不可伪造性。基于属性的在线/离线签密方案虽然在密文长度方面有所增加,但该方案既可以支持保密性和认证性,又更加贴近于实际环境。

关键词 签密,在线/离线技术,基于属性的密码体制,可证明安全

中图法分类号 TP391 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.11.043

Attribute-based Online/Offline Signcryption for Mobile Network

JIANG Di HAN Yi-liang

(Department of Electronic, Engineering University of CAPF, Xi'an 710086, China)

(Key Laboratory of Network and Information Security of the Chinese Armed Police Force, Xi'an 710086, China)

Abstract Signcryption combines the functionalities of signature and encryption and costs less than the traditional approach. Online/Offline techniques can improve the efficiency of the signature and encryption, and one motivating application for this technology is mobile network devices. The previous attribute-based signcryption scheme is not practical and efficient, on the basis of Li's attribute-based signature, an efficient attribute-based online/offline signcryption scheme was proposed in this paper. This scheme is provable secure in the random oracle model and it satisfies indistinguishability against adaptive chosen ciphertext attack based on l-th decisional bilinear Diffie-Hellman inversion (l-DBDHI) assumption and satisfies existential unforgeability against adaptive chosen message attack based on the standard computational Diffie-Hellman(CDH) assumption. Although the size of ciphertext increases, the new scheme achieves confindentiality and authentication, which is more suitable for the practical applications.

Keywords Signcryption, Online/Offline techniques, Attribute-based cryptography, Provable security

Zheng[1]提出了"签密"的概念。签密可以在一个合理的逻辑步骤内同时完成签名和加密两项功能,代价要远远低于传统的"先签名后加密",是实现既保密又认证传输消息的理想方法。

在线/离线的思想最先由Even等[2]在数字签名中引入,是能够有效提高签名与加密效率的加密技术。在线/离线签名方案尤其适用于无线传感网络、智能卡应用系统以及计算能力高度受限的终端设备,计算量较大的离线阶段可以在无线传感网络的基站(或者智能卡应用系统的智能卡)上运行,在线阶段可以在一个计算能力较弱的处理器上运行(无限传感网络的结点)。在ASIA CCS 2011会议上Chow等[3]改进了IBOOE方案,提高了在线加密算法的效率,缩短了密文的长度。与此同时,Chow等也提出了新的问题,即能否构建可证明安全的基于属性的在线/离线加密机制。

文献[4]首次提出了基于属性加密(Attribute-Based Encryption, ABE)的概念,不用暴露用户的身份,任何用户只要其属性满足指定的访问策略就能够解密消息。基于属性的密码学具有天然的"多用户"和"隐藏身份"特性,为隐私保护提供了可行的途径。Maji等人[5,6]提出了支持任何访问结构的基于属性的签名(ABS)方案,该方案能够保护签名者的属性隐私,但他们只在一般群模型下证明其安全性。2014年Hohenberger和Waters[7]提出了基于属性的在线/离线加密方案(ABOOE),目前仍缺乏有效的基于属性的签密(ABSC)方案。Gagne等人[8]提出1个标准模型下可证安全的(n,n)门限ABSC方案,签密者和加密者的门限是固定的。Emura等人[9]提出一个密文策略ABSC方案,其支持复杂访问结构和

到稿日期:2015-12-25 返修日期:2016-05-22 本文受国家自然科学基金(61272492,61572521),陕西省自然科学基础研究计划项目(2015JM6353),武警工程大学基础理论研究项目(WJY201521)资助。

姜 頔(1991—),男,硕士,主要研究领域为应用密码学,E-mail:jd9110@163.com;韩益亮(1977—),男,副教授,博士生导师,CCF高级会员,主要研究领域为应用密码学。

动态属性，但是需要明确知道签密者具体拥有的属性。现有的 ABSC 方案在门限、属性隐私保护等方面存在不足，而且效率低下，实用性不高。

针对此问题，本文结合基于属性的签密、在线/离线技术的优点，在文献[10]的基础上提出了适用于移动网络设备的基于属性的在线/离线签密方案，本方案更具实用性，具有较高的通信效率，并且在随机预言机模型下利用判定双线性 Diffie-Hellman 倒转（l-DBDHI）问题和计算 Diffie-Hellman（CDH）问题的困难性可以得出本方案是可证安全的。

1 预备知识

定义 1（双线性对） 令 G_1 和 G_2 为 q 阶乘法循环群，随机选择 g 作为 G_1 的生成元，定义一个双线性映射 $e: G_1 \times G_1 \rightarrow G_2$，满足如下性质：

1）双线性：对任意的 $u, v \in G_1$ 和 $a, b \in Z_q$，则 $e(u^a, v^b) = e(u, v)^{ab}$；

2）非退化性：$e(g, g) \neq 1$；

3）可计算性：对任意的 $u, v \in G_1$，存在有效多项式算法计算 $e(u, v)$。

定义 2（判定双线性 Diffie-Hellman 倒转假设，l-th Decisional Bilinear Diffie-Hellman Inversion Assumption，l-DBDHI[3]） l-DBDHI 问题在 (G, G_T) 上的定义为：随机选择 $\partial \in Z_p^*$，g 是 G 的生成元，给定一个 $(l+2)$ 元组 $(g, g^{\partial}, g^{\partial^2}, \cdots, g^{\partial^l}, T) \in G^{l+1} \times G_T$，判定 T 的值是否为 $e(g, g)^{\frac{1}{\partial}}$。如果对于任意概率多项式时间（$PPT$）算法 A 在 (G, G_T) 上解决 l-$DBDHI$ 问题的优势均是可忽略的，则称 l-$DBDHI$ 假设在 (G, G_T) 上是成立的。

定义 3（计算 Diffie-Hellman 问题，CDH） 对于 $x, y \in_R Z_q^*$，已知 $g, g^x, g^y \in G_1$，计算 g^{xy}。

定义 4（拉格朗日插值定理） 令 q 是一个素数，$f(x)$ 是一个次数为 n 的多项式，给定多项式 $f(x)$ 上的 $n+1$ 个不同的点 $(x_i, f(x_i))$，其中 $x_i \in Z_q, i \in [1, n+1]$，则可以将多项式 $f(x)$ 唯一确定为：

$$f(x) = \sum_{i=1}^{n} \left(f(x_i) \prod_{\substack{1 \leqslant m \leqslant n \\ m \neq i}} \frac{x - x_m}{x_i - x_m} \right)$$

其中拉格朗日系数为：

$$\Delta_{i,s}(x) = \prod_{j \in s, j \neq i} \frac{x - j}{i - j}, i \in Z_q, s \subset Z_q$$

定义 5 本文所提基于属性的在线/离线签密方案支持包含门限的断言 $\gamma_{k,\omega^*}(\cdot)$，$\omega^*$ 是用于加密或者签名的属性集，$k(1 \leqslant k \leqslant d)$ 为门限值。$\gamma_{k,\omega^*}(\omega') = \begin{cases} 1, & |\omega' \cap \omega^*| \geqslant k \\ 0, & \text{otherwise} \end{cases}$，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 $\gamma_{k,\omega^*}(\cdot)$。

2 基于属性的在线/离线签密算法的定义

2.1 基于属性的在线/离线签密算法

基于属性的在线/离线签密由 5 个算法组成：系统初始化算法（Setup）、密钥提取算法（Extract）、离线签密算法（Offline-signcryption）、在线签密算法（Online-signcryption）和解签密算法（Unsigncryption）。

初始化：该算法输入安全参数 λ，d 和属性域 $U \in_R Z_q^*$，该属性域定义了系统中所有的允许属性，输出并公开公共参数 $params$，保密主密钥 x。

密钥提取：该算法输入主密钥 x、用户 ID 和公共参数 $params$，输出用户的私钥 SK。

离线签密：该算法输入公共参数 $params$、随机属性 x_j 和 x_p，输出离线签密文 σ_{off}。

在线签密：该算法输入公共参数 $params$、离线签密文 σ_{off}、确认属性集 r_i'，输出在线签密文 σ_m。

解签密：该算法输入密文 σ、解密者属性集，输出明文消息 m 或者解签密失败符号 $\perp$。

2.2 基于属性的在线/离线签密算法安全模型

定义 6 如果没有任何多项式有界时间的敌手以不可忽略的优势赢得以下游戏，则称一个基于属性的在线/离线签密方案在随机预言机模型下的选择密文攻击不可区分（IND-CCA），该模型可以通过攻击者 A 与挑战者 C 之间的游戏来进行定义。

初始化：攻击者 A 公布挑战属性集 ω_B^*，不能对属性集 ω_B^* 进行密钥生成询问。

系统建立：挑战者 C 运行算法，利用系统安全参数 λ 和 d 产生公共参数 $params$ 和系统密钥 t。将 $params$ 发布给攻击者 A，保密 t。

询问阶段 1：A 向 C 执行以下询问：

（1）Hash 询问：A 可以询问任意输入的 Hash 值。

（2）私钥生成询问：A 选择一个属性集 ω_i，根据系统参数 $params$ 和主密钥 t，C 计算用户私钥 S_{ω_i}，并且将其发送给 A。

（3）签密询问：A 选择属性集 ω_i 和 ω_j 以及明文 m 和 ω_i 用于签名，ω_j 用于加密。C 对 ω_i 进行私钥生成询问，C 计算 $\sigma = Signcrypt(\omega_i, \omega_j, S_{\omega_i}, m)$，将签密文 σ 发送给 A。

（4）验证解密询问：A 选择属性集 ω_i 和 ω_j 和签密文 σ 和 ω_i 用于签名，ω_j 用于加密。C 对 ω_j 进行私钥生成询问，计算 $m = Unsigncrypt(\omega_i, \omega_j, S_{\omega_i}, \sigma)$，返回明文 m 或者终止符号 $\perp$。

在询问阶段 1，A 可以根据以前的询问结果进行自适应询问。最后，A 选择两个等长的明文 m_0 和 m_1 以及两个挑战的属性集 ω_A^* 和 ω_B^*，ω_A^* 用于签名，ω_B^* 用于加密，且 ω_B^* 没有被执行过私钥生成询问。

挑战阶段：C 随机选择 $b \in \{0, 1\}$，计算 $\sigma_b^* = Signcrypt(\omega_A^*, \omega_B^*, S_{\omega_A}^*, m_b^*)$。返回签密文 σ_b^* 给 A。

询问阶段 2：A 执行与阶段 1 相同的询问，但有一定的限制：不允许对 ω_B^* 进行私钥生成询问，不允许询问 $\omega_A^*, \omega_B^*, \sigma_b^*$ 的明文。

猜测阶段：游戏最后，A 输出 $b' \in \{0, 1\}$，如果 $b' = b$，则 A 在游戏中获胜。定义攻击者 A 在游戏中获胜的优势为 $Adv_A^{IND\text{-}CCA} = |2\Pr(b' = b) - 1|$。

定义 7 如果多项式时间内敌手赢得以下游戏的概率可以忽略，则称基于属性的在线/离线签密方案具有在随机预言机模型下对选择明文攻击的不可伪造性。

初始化、系统建立：同定义 6；

询问阶段：同定义 6 中的“询问阶段 1”；

伪造阶段：游戏最后，A 输出一个新的三元组 $(\omega_A^*, \omega_B^*, \sigma^*)$，且 ω_A^* 在询问阶段没有被执行过私钥生成询问。如果 $Unsigncrypt(\omega_A^*, \omega_B^*, S_{\omega_B^*}^*, \sigma^*)$ 没有返回终止符号 $\perp$，则 A 在游戏中获胜，A 获胜的优势定义为 $Succ_A^{EUF\text{-}CMA}=\Pr[Awins]$。

3 方案描述

方案描述具体如下：

(1)初始化阶段：密钥生成中心选择系统安全参数 λ，$d\in_R Z_q^*$，属性域 $U\subset_R Z_q^*$，设有 $(d-1)$ 个属性构成默认属性集为 $\Omega=\{\Omega_1,\cdots,\Omega_{d-1}\}$，$\Omega_i\in_R Z_q^*$，$1\leqslant i\leqslant d-1$。选择一个双线性对 $e:G_1\times G_1\rightarrow G_2$，随机选取 $g,g_2\in G_1$，$x\in_R Z_q^*$，计算 $g_1=g^x$，$Z=e(g_1,g_2)$。选择一个对称密码算法的加、解密算法 $E_k(\cdot)$ 和 $D_k(\cdot)$。选择哈希函数 $H_1:\{0,1\}^*\rightarrow G_1$，$H_2:\{0,1\}^*\times\{G_1\}^*\rightarrow G_1$。保密系统主密钥 x，公开公共参数 $params=(\lambda,d,q,G_1,G_2,e,g,g_1,g_2,Z,H_1,H_2,E_k(\cdot),D_k(\cdot))$。

(2)密钥提取阶段：为生成用户的私钥，首先给定该用户的 ID，其对应的属性集 $\omega_{ID}\subset U$，密钥生成中心随机选择 $d-1$ 次多项式 $q(y)$，满足 $q(0)=x$。随机选择 $r_i\in_R Z_q^*$，计算 $d_{i0}=g_2^{q(i)}H_1(i)^{r_i}$，$d_{i1}=g^{r_i}$，因此该用户的私钥为 $D_i=(d_{i0},d_{i1})$。

(3)离线签密阶段：设签名断言为 $\gamma_{k,\omega_1^*}(\cdot)$，$|\omega_1^*|=n_1$，加密断言为 $\gamma_{k,\omega_2^*}(\cdot)$，$|\omega_2^*|=n_2$。从默认属性集 Ω 选取 $(d-k)$ 和 $(d-k')$ 个默认属性分别构成默认属性集 $\Omega_1'=\{i_{k+1},\cdots,i_d\}\subseteq\Omega$，$\Omega_2'=\{i_{k'+1},\cdots,i_d\}\subseteq\Omega$，选择随机数 $s\in_R Z_q^*$，随机属性 $x_j,x_p\in\Omega$，计算 $\sigma_0=g^s$，$k_e=Z^s$，$\{\sigma_{off}'=g^{r_j}d_{i1}^{\Delta i,s(0)}\}$，$\{\sigma_{off}''=g^{r_p}\}$，而后输出离线签密文 $\sigma_{off}=\{\sigma_0,k_e,\sigma_{off}',\sigma_{off}''\}$。

(4)在线签密阶段：此阶段，签密者得到要发送的明文消息 m，签密者属性集 $\omega_A=\{i_1,\cdots,i_{n_A}\}$，且 $\gamma_{k,\omega_1^*}(\omega_A)=1$，$A$ 用属性集 ω_A 在断言 $\gamma_{k,\omega_1^*}(\cdot)$ 和 $\gamma_{k,\omega_2^*}(\cdot)$ 下对消息 m 签密，用户 A 选择属性子集 $\omega_A'\subseteq\omega_1^*\cap\omega_A$，离线签密文 σ_{off}，得到 $r_i'\in\omega_A$。计算：

$$\{\sigma_i=H_1(i)^s\}_{i\in\omega_2^*\cup\Omega_2'},c=E_{k_e}(m),\sigma_0'=\Big[\prod_{i\in\omega_A'\cup\Omega_1'}d_{i0}^{\Delta i,s(0)}\Big]\cdot\Big[\prod_{i\in\omega_1^*\cup\Omega_1'}H_1(i)^{r_i'}\Big]\cdot H_2(c,\{\sigma_i\})^s,\sigma_2=g^{r_i'-x_j},\sigma_3=g^{r_i'-x_p}$$

而后输出最终签密文 $\sigma_{on}=(\sigma_0,\{\sigma_i\},\sigma_0',\{\sigma_{off}\},c,\sigma_2,\sigma_3)$。

(5)解签密阶段：接收方用户 B 的属性集 $\omega_B=\{i_1,\cdots,i_{n_B}\}$，且在满足 $\gamma_{k,\omega_2^*}(\omega_B)=1$ 时，可以验证消息 m 的签密文 $\sigma_{on}=(\sigma_0,\{\sigma_i\},\sigma_0',\{\sigma_{off}\},c,\sigma_2,\sigma_3)$ 的签名者是否满足签名断言 $\gamma_{k,\omega_1^*}(\cdot)$，并解密获得明文消息 m，B 计算 $H_2(c,\{\sigma_i\})$，进而判断式(1)是否成立，如果成立则接受密文 σ_{on}，否则拒绝。B 选择属性集 $\omega_B'\subseteq\omega_2^*\cap\omega_B$，并令

$$\{d_{i0}'=d_{i0}\}_{i\in\omega_B'\cup\Omega_2'},\{d_{i0}'=H(i)\}_{i\in\omega_2^*/\omega_B'}$$

$$\{d_{i1}'=d_{i1}\}_{i\in\omega_B'\cup\Omega_2'},\{d_{i1}'=g\}_{i\in\omega_2^*/\omega_B'}$$

$$\frac{e(g,\sigma_0')}{\Big[\prod_{i\in\omega_1^*\cup\Omega_1'}e(H_1(i),\sigma_{off}\cdot\sigma_{2,3})\Big]e(H_2(c,\{\sigma_i\}),\sigma_0)}=Z \quad (1)$$

计算：$k_e=\prod_{i\in\omega_2^*\cup\Omega_2'}\Big(\frac{e(d_{i0}',\sigma_0)}{e(\sigma_i,d_{i1}')}\Big)^{\Delta i,s(0)}$，$m=D_{k_e}(c)$。

4 方案分析

4.1 正确性分析

等式(1)的证明如下：

$$\frac{e(g,\sigma_0')}{\Big[\prod_{i\in\omega_1^*\cup\Omega_1'}e(H_1(i),\sigma_{off}\cdot\sigma_{2,3})\Big]e(H_2(c,\{\sigma_i\}),\sigma_0)}$$

$$=\frac{e\Big(g,\Big[\prod_{i\in\omega_A'\cup\Omega_1'}(g_2^{q(i)}H_1(i)^{r_i})^{\Delta i,s(0)}\Big]\Big[\prod_{i\in\omega_1^*\cup\Omega_1'}H_1(i)^{r_i'}\Big]H_2(c,\{\sigma_i\})^s\Big)}{\Big[\prod_{i\in\omega_A'\cup\Omega_1'}e(H_1(i),g^{r_j}d_{i1}^{\Delta i,s(0)}\cdot g^{r_i'-x_j})\prod_{i\in\omega_1^*/\omega_A'}e(H_1(i),g^{r_p}\cdot g^{r_i'-x_p})\Big]e(H_2(c,\{\sigma_i\}),g^s)}$$

$$=\frac{e\Big(g,g_2^s\Big[\prod_{i\in\omega_A'\cup\Omega_1'}(H_1(i)^{r_i})^{\Delta i,s(0)}\Big]\Big[\prod_{i\in\omega_1^*\cup\Omega_1'}H_1(i)^{r_i'}\Big]H_2(c,\{\sigma_i\})^s\Big)}{\Big[\prod_{i\in\omega_A'\cup\Omega_1'}e(H_1(i),g^{\Delta i,s(0)r_i+r_i'})e\Big(H_1(i),\prod_{i\in\omega_1^*/\omega_A'}g^{r_i'}\Big)\Big]e(H_2(c,\{\sigma_i\})^s,g)}$$

$$=Z\frac{e\Big(g,\prod_{i\in\omega_A'\cup\Omega_1'}H_1(i)^{\Delta i,s(0)r_i+r'}\Big)e(g,H_2(c,\{\sigma_i\})^s)e\Big(g,\prod_{i\in\omega_1^*\cup\Omega_1'}H_1(i)^{r_i}\Big)}{\Big[\prod_{i\in\omega_A'\cup\Omega_1'}e(H_1(i),g^{\Delta i,s(0)r_i+r_i'})e\Big(H_1(i),\prod_{i\in\omega_1^*/\omega_A'}g^{r_i'}\Big)\Big]e(H_2(c,\{\sigma_i\})^s,g)}$$

$$=Z$$

$$k_e=\prod_{i\in\omega_2^*\cup\Omega_2'}\Big(\frac{e(d_{i0}',\sigma_0)}{e(\sigma_i,d_{i1}')}\Big)^{\Delta i,s(0)}$$

$$=\prod_{i\in\omega_B'\cup\Omega_2'}\Big(\frac{e(g_2^{q(i)}H_1(i)^{r_i},g^s)}{e(H_1(i)^s,g^{r_i})}\Big)^{\Delta i,s(0)}\prod_{i\in\omega_2^*/\omega_B'}\Big(\frac{e(H_1(i),g^s)}{e(H_1(i)^s,g)}\Big)^{\Delta i,s(0)}$$

$$=\prod_{i\in\omega_B'\cup\Omega_2'}(g_2^{q(i)},g^s)^{\Delta i,s(0)}$$

$$=Z^s$$

4.2 安全性证明

第 2.2 节定义的安全模型是在随机预言模型下建立的，因此在下面的证明中假设方案中用到的 Hash 函数是理想的随机预言机。为了便于描述，机密性证明时只对加密部分进行分析，不可伪造性证明时只对签名部分进行分析。

4.2.1 机密性

定理 1 如果 l-DBDHI 假设成立，则本文所提的签密方案满足 ND-CCA 安全，即不存在一个 IND-CCA 攻击者以不可忽略的优势攻破所提方案。

证明：假设存在一个 PPT 攻击者 A 能够在概率多项式时间内以 ε 的优势攻破方案的安全性，则可以构造一个仿真器 β 攻破 $n(l+1)$-DBDHI 假设；并且 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 次签密询问和 q_U 次验证解签密询问。构造仿真器 β，利用 A 解决 l-DBDHI 问题，β 仿真如下。

首先挑战者 C 生成系统公钥参数，并给出一个 $n(l+1)$-

DBDHI 元组$(g,g^{a},g^{a^2},\cdots,g^{a^{n(l+1)}},T)$，其中 $T=e(g,g)^{\frac{1}{a}}$ 或 T 为 G_T 中的一个随机元素。当 $T=e(g,g)^{\frac{1}{a}}$，仿真器 β 输出 1，否则输出 0。

初始化：攻击者 A 公布挑战属性集 ω_B^*，不能对属性集 ω_B^* 进行密钥生成询问，A 输出预挑战的用于签名的属性集 ω_1^* 和门限 $k(1\leqslant k\leqslant d)$，用于加密的属性集 ω_2^* 和门限 $k'(1\leqslant k'\leqslant d)$，设签名断言为 $\gamma_{k,\omega_1^*}(\cdot)$，加密断言为 $\gamma_{k',\omega_2^*}(\cdot)$，$\beta$ 选择默认属性集 $\Omega_1'^*\subseteq\Omega$，$|\Omega_1'^*|=d-k$，$\Omega_2'^*\subseteq\Omega$，$|\Omega_2'^*|=d-k$。令 $g_1=g^r$，$g_2=g^y$。

随机预言机：A 保存列表 L_1 和 L_2 来存储 H_1 预言机和 H_2 预言机的答案。β 选择 2 个随机数 $\delta_0,\delta_1\in[1,q_{H_2}]$。$H_1$ 预言机：如果对于 i 进行 H_1 预言机询问，β 检查 L_1，具体如下：

(1)如果能在 L_1 中找到 i，返回对应值；

(2)在 L_1 中找不到 i，且 $i\in\omega_2^*\cup\Omega_2'^*$，选择随机数 $\eta_i\in_R Z_q^*$，返回 $H_1(i)=g^{\eta_i}$，并记录在表 L_1 中；

(3)在 L_1 中找不到 i，且 $i\notin\omega_2^*\cup\Omega_2'^*$，选择随机数 η_i，$\gamma_i\in_R Z_q^*$，返回 $H_1(i)=g_1^{-\eta_i}g^{\gamma_i}$，并记录在表 L_1 中。

H_2 预言机：如果对 $\{\sigma_j\}_{j\in U}$，$c_i\in G_1$ 进行 H_2 预言机询问，同 H_1 预言机，过程如下：

(1)如果能在 L_2 中找到 i，返回对应值；

(2)在 L_2 中找不到 i，且 $i\neq\delta_0$，$i\neq\delta_i$，选择随机数 α_i，$\eta_i\in_R Z_q^*$，返回 $H_2(c_i,\{\sigma_j\}_{j\in U})=g_1^{\alpha_i}g^{\eta_i}$，并记录在表 L_2 中；

(3)在 L_2 中找不到 i，且 $i=\delta_0$，选择随机数 $\eta_{\delta_0}\in_R Z_q^*$，返回 $H_2(c_i,\{\sigma_j\}_{j\in U})=g^{\eta_{\delta_0}}$，并记录在表 L_2 中；

(4)在 L_2 中找不到 i，且 $i=\delta_1$，选择随机数 $\eta_{\delta_1}\in_R Z_q^*$，返回 $H_2(c_i,\{\sigma_j\}_{j\in U})=g^{\eta_{\delta_1}}$，并记录在表 L_2 中。

密钥生成预言机：1)如果对于属性集 ω_i，其满足 $|\omega_i\cap\omega_2^*|<k'$，进行密钥生成询问。首先定义 3 个集合 Γ,Γ',S，满足：$\Gamma=(\omega_i\cap\omega_2^*)\cup\Omega_i'$，$\Gamma\subseteq\Gamma'\subseteq S$，$|\Gamma'|=d-1$，$S=\Gamma'\cup\{0\}$。$\beta$ 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，$r_i\in_R Z_q^*$。式中隐藏着一个 $d-1$ 次多项式 $q(x)$，而且 $q(i)=t_i$，$q(0)=x$。当对于 $i\notin\Gamma'$，令 $r_i=\frac{\Delta_{0,S}(i)}{\eta_i}y+r_i'$，$q(i)=\sum_{j\in\Gamma'}\Delta_{j,S}(i)q(j)+\Delta_{0,S}(i)q(0)$，那么 $D_i=(g_2^{\frac{\Delta_{0,S}(i)r_i}{\eta_i}+\sum_{j\in\Gamma'}\Delta_{j,S(i)q(j)}}(g_1^{-\eta_i}g^{r_i})^{r_i'},g_2^{\frac{\Delta_{0,S}(i)}{\eta_i}}g^{r_i'})$，因此，对于攻击者 A 来说，D_i 是个合法的密钥。2)如果 $|\omega_i\cap\omega_2^*|\geqslant k'$，则 β 仿真失败。

签密预言机：A 请求在属性集 ω_A 和断言 $\gamma_{k,\omega_1^*}(\cdot)$、$\gamma_{k,\omega_2^*}(\cdot)$ 下的消息 m 的签密询问。β 仿真如下：1)如果 $|\omega_A\cap\omega_2^*|<k'$，则 β 利用密钥生成预言机产生 ω_A 的私钥 $D_{A_i}=(d_{i0},d_{i1})$，并且按照正常的签密算法产生签密文并返回给 A；2)否则，β 从默认属性集 Ω 中随机选择 $d-k$ 个元素构成属性子集 Ω_1'，从默认属性集 Ω 中随机选择 $d-k'$ 个元素构成属性子集 Ω_2'，设 $\omega_A\cup\Omega_1'=\{i_1,i_2,\cdots,i_d\}$，$\beta$ 随机选择 k_e，计算 $c_i=E_{k_e}(m_i)$。随机选择 $r_i,s'\in_R Z_q^*$。设 $s=\frac{1}{\partial_{id}}y+s'$。令 $\sigma_0=g^s=g_2^{\frac{-1}{\partial_{id}}}g^{s'}$，$\{\sigma_i=g^{\beta_i s}=g_2^{\frac{-\beta_i}{\partial_{id}}}g^{\beta_i s'}\}_{i\in\omega_2^*\cup\Omega_2'}$，$H_2(c_i,\{\sigma_i\}_{i\in\omega_2^*\cup\Omega_2'})=g_1^{\partial_{id}}g^{\beta_i}$，$\sigma_0'=g_2^{r_i}\prod_{i\in\omega_1^*\cup\Omega_1'}H_1(i)^{r_i}H_2(c_i,\{\sigma_i\}_{i\in\omega_2^*\cup\Omega_2'})^s=(g_1^{\partial_{id}}g^{\beta_i})^{s'}\prod_{i\in\omega_1^*\cup\Omega_1'}H_1(i)^{r_i}g_2^{\frac{-\beta_i}{\partial_{id}}}$，$\{\sigma'_i=g^{r_i'}\}_{i\in\omega_1^*\cup\Omega_1'}$。因为 A 不能对 ω_B，$|\omega_B\cap\omega_2^*|\geqslant k'$ 进行私钥生成询问，不能计算 k_e，进而无法判断随机数 k_e 是否合法，所以从攻击者 A 的角度看签密文是一个合法的密文。

验证解签密预言机：A 请求密文 σ 的解密询问。β 仿真如下：1)如果 $|\omega_A\cap\omega_2^*|<k'$，$|\omega_B\cap\omega_2^*|<k'$，则 β 利用密钥生成预言机产生 ω_A 和 ω_B 的私钥，并且按照正常的解签密算法，验证并解密得到明文 m 或者返回终止符号 $\perp$；2)否则，β 返回无效的签名。

挑战阶段：β 随机选择 $b\in\{0,1\}$，β 仿真如下：选取 k 个属性构成的属性集 $\omega_A^*{}'\subseteq\omega_1^*$，$\beta$ 询问密钥生成预言机，在获得 $\omega_A^*{}'$ 的私钥 d_{i0},d_{i1} 后，按照正常的算法计算得 $k_e^*=h^{s^*}$，$c_b^*=E_{k_e}(m_b)$，$\sigma_0^*=g^{\alpha s^*}$，$\{\sigma_i^*=g^{\alpha\beta_i s^*}\}_{i\in\omega_2^*\cup\Omega_2^*{}'}$，$\sigma_0^*{}'=[\prod_{i\in\omega_A^*{}'\cup\Omega_1^*{}'}d_{i0}^{\Delta i,s(0)}][\prod_{i\in\omega_1^*\cup\Omega_1^*{}'}H_1(i)^{r_i'}]$

$$H_2(c_b^*,\{\sigma_i^*\}_{i\in\omega_2^*\cup\Omega_2^*{}'})^{\alpha s^*}=[\prod_{i\in\omega_A^*{}'\cup\Omega_1^*{}'}d_{i0}^{\Delta i,s(0)}]\cdot[\prod_{i\in\omega_1^*\cup\Omega_1^*{}'}(g_1^{-\beta_i}g^{r_i})^{r_i'}]g^{\alpha\beta_b s^*}$$

$\{\sigma_1^*{}'=d_{i1}^{\Delta i,s(0)}\cdot g_i^{r'}\}_{i\in\omega_A^*{}'\cup\Omega_1^*{}'}$，$\{\sigma_i^*{}'=g_i^{r'}\}_{i\in\omega_1^*/\omega_A^*{}'}$

β 输出以上结果作为挑战结果给 A，如果 $H_2(c_b^*,\{\sigma_i^*\}_{i\in\omega_2^*\cup\Omega_2^*{}'})\neq g^{\alpha\beta_b}$，则仿真失败；而如果 $h=e(g,g)^{\frac{1}{a}}$，从攻击者 A 的角度来看输出结果是一个合法的签密文。

挑战阶段以后，A 执行上述询问，但不允许其对 ω_B^* 进行密钥生成询问，不允许其询问 σ^* 的明文，但允许其询问 σ^* 是否合法，即判断式(1)是否成立。

猜测阶段：如果攻击者 A 输出 b'，而且 $b'=b$，β 输出 1，攻击者 A 赢得游戏，则 β 可以判断 $h=e(g,g)^{\frac{1}{a}}$，进而解决 l-DBDHI 问题；否则 $b'\neq b$，β 输出 0，表示 h 是个随机元素。

如果以下事件发生，那么游戏模拟将会终止，β 将会失败。

$E1$：攻击者 A 对 ω_B^* 进行私钥生成询问；$E2$：攻击者 A 拒绝一个正确的签密文；$E3$：攻击者 A 选择挑战属性集 ω_1^*，ω_2^*；$E4$：攻击者 A 选择默认属性集 $\Omega_1^*{}'$，$\Omega_2^*{}'$；$E5$：判断失败 $H_2(c_b^*,\{\sigma_i^*\}_{i\in\omega_2^*\cup\Omega_2^*{}'})\neq g^{\beta\delta_b}$，综合上述 5 个事件，最终攻击者能够解决 l-DBDHI 问题的概率至少为：

$$\frac{1}{q_{H_1}}\cdot(1-\frac{q_U}{2^\lambda})\cdot\frac{1}{\binom{2}{q_{H_1}}}\cdot\frac{1}{\binom{d-k}{d-1}}\cdot\frac{1}{\binom{d-k'}{d-1}}\cdot\frac{1}{q_{H_2}^2}\varepsilon$$

4.2.2 不可伪造性

定理 2 假定 G_1 上的 CDH 困难问题成立，则本文所提的签密方案满足 EF-CMA 安全，即不存在一个 EF-CMA 攻击者以不可忽略的优势攻破所提方案。

证明：设存在一个 PPT 攻击者 A 能够在概率多项式时间内以 ε 的优势攻破方案的安全性，则可以构造一个仿真器 β 攻破 CDH 假设；并且 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 次签密询问和 q_U 次验证解签密询问。构造仿真器 β，利用 β 解决 CDH 问题，即给定 (g,g^r,g^y)，计算 g^{ry}。

对不可伪造性的证明与机密性的证明比较类似，这里仅做简要分析。

攻击者 A 选择挑战的属性集 ω_1^*，ω_2^* 和默认属性集 $\Omega_1^{*\prime}$，$\Omega_2^{*\prime}$，输出一个明文 m_δ 的密文 $\sigma^* = \{\sigma_0^*, \{\sigma_i^*\}_{i\in\omega_2^*\cup\Omega_2'}, \sigma_0^{*\prime}, \{\sigma_i^{*\prime}\}_{i\in\omega_1^*\cup\Omega_1'}, c_\delta^*\}$。如果 A 没有选择 ω_1^*，ω_2^* 和 $\Omega_1^{*\prime}$，$\Omega_2^{*\prime}$ 或者 $H_2(c_b^*, \{\sigma_i^*\}_{i\in\omega_2^*\cup\Omega_2^{*\prime}}) \neq g^{\beta_\delta}$，则仿真失败。如果签密文合法，则满足式(1)，那么 A 赢得游戏，由于 $H_1(i) = g^{r_i}$，$H_2(c_b, \{\sigma_i^*\}_{i\in\omega_2^*\cup\Omega_2'}) = g^{\beta_\delta}$，可以得到：

$$\frac{e(g,\sigma_0^{*\prime})}{[\prod_{i\in\omega_1^*\cup\Omega_1'} e(H_1(i),\sigma_i^{*\prime})]e(H_2(c_\delta,\{\sigma_i^*\}_{i\in\omega_2^*\cup\Omega_2'}),\sigma_0^*)}$$

$$= e(g, \frac{\sigma_0^{*\prime}}{\prod_{i\in\omega_1^*\cup\Omega_1'} \sigma_i^{*r_i'}\sigma_0^{*\beta_\delta}})$$

$$= e(g, g^{xy})$$

所以 $g^{xy} = \frac{\sigma_0^{*\prime}}{\prod_{i\in\omega_1^*\cup\Omega_A'} \sigma_i^{*r_i'}\sigma_0^{*\beta_\delta}}$，由此可知 β 解决了 CDH 问题。即若存在一个攻击者能以一个不可忽略的概率伪造出一个合法签密文，则他能以一个不可忽略的概率解决 CDH 问题。

如果以下事件发生，那么游戏模拟将会终止，β 将会失败。

$E1$：攻击者 A 对 ω_B^* 进行私钥生成询问；$E2$：攻击者 A 拒绝一个正确的签密文；$E3$：攻击者 A 选择挑战属性集 ω_1^*，ω_2^*；$E4$：攻击者 A 选择默认属性集 $\Omega_1^{*\prime}$，$\Omega_2^{*\prime}$；$E5$：判断失败 $H_2(c_b, \{\sigma_i^*\}_{i\in\omega_2^*\cup\Omega_2'}) = g^{\beta_\delta}$，综合上述 5 个事件，最终攻击者能够解决 CDH 问题的概率至少为：

$$\frac{1}{q_{H_1}} \cdot (1-\frac{q_U}{2^\lambda}) \cdot \frac{1}{\binom{2}{q_{H_1}}} \cdot \frac{1}{\binom{d-k}{d-1}} \cdot \frac{1}{\binom{d-k'}{d-1}} \cdot \frac{1}{q_{H_2}} \varepsilon$$

5 性能分析

系统效率主要从通讯效率和计算效率两个方面来考虑。通讯效率主要由密文长度决定，而计算效率主要由加解密算法产生的计算开销决定。从这两个主要方面进行分析，其中 p 表示双线性对运算，e 表示指数运算，S 表示 G_1 上的幂运算，E 表示 G_2 上的幂运算，n 为属性集的最大属性个数，N_1 表示签名属性集包含的属性个数，N_2 表示加密属性集包含的属性个数，n_m 为明文消息长度，d 为门限值，$|G_1|$，$|G_2|$，$|Z_q^*|$ 分别表示相应群中元素的长度，在这里均表示为 $|G|$。与文献[8,11]的性能对比如表 1 所列。

表 1 本方案与文献[8,11]方案的比较

方案	运算量	密文长度
文献[8]	$(n_m/2+2d+n+6)e+(3d+2)p+(n_m/2+2d+1)e$	$(2n+3)\|G\|+n_m$
文献[11]	$S(3(N_1+d-k)+d+2+(N_2+d-k'))+E[(N_1+d-k)+2(N_2+d+k')]p+(N_2+d-k')E$	$(N_1+d-k+N_2+d-k'+3)\|G\|$
本文方案	$S(2(N_1+d-k)+d+3+(N_2+d-k'))+E[(N_1+d-k)+2(N_2+d+k')]p$	$(N_1+d-k+N_2+d-k'+5)\|G\|$

本文方案将基于属性的签密分解成为离线签密与在线签密，在离线阶段不需要知道明文和属性集合，先完成大量的预操作，这对于计算能力受限的轻量级设备是至关重要的。通过表 1 的对比可以发现，通过在线/离线技术，本文方案的运算量有所降低，虽然密文长度有所增加，但是现有的移动网络终端设备是能够满足这些开销的，因此该方案适合于移动网络终端设备收集敏感信息。本文方案在随机预言机模型下是可证明安全的，从理论上讲，随机预言机模型下的密码方案的安全性不如标准模型下的密码方案的安全性高，但此类方案的安全性仍然可以接受，尤其是在效率要求严格的场景中，随机预言机模型下的高效签密方案是一个不错选择。

结束语 本文提出了一个基于属性的离线/在线签密方案，将离线/在线技术引入到方案中，可以更加贴近实际情况；并证明了其在随机预言机模型下的安全性，将基于属性的签密和离线/在线技术相结合，适合于移动网络终端设备的敏感信息存取。下一步将继续研究如何进一步提高方案的效率，同时对访问结构的优化做进一步的研究。

参 考 文 献

[1] Zheng Y. Digital signcryption or How to Achieve Cost (Signature Encryption)<=Cost(Signature)+Cost(Signature)+Cost(Encryption)[C]// Proceeding of CRYPTO'97, LNCS 1294. Berlin: Springer-Verlag, 1997: 165-179

[2] Even S, Goldreich O, Micali S. Online/Offline digital signatures [C]// Proc. CRYPTO 89, LNCS 2442, 1989: 263-277

[3] Chow S S M, Liu J K, Zhou J Y. Identity-based online/offline key encapsulation and encryption[C]// Proc of ASIACCS'11. HongKong, China, 2011: 52-60

[4] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]// Proceedings of the 13th ACM Conference on Computer and Communications Security. Alexandria, VA, USA, 2006: 221-238

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

[6] Maji H K, Prabhakaren M, Rosulek M. Attribute-based signatures[J]. Lecture Notes in Computer Science, 2011, 6588: 376-392

[7] Hohenberger S, Waters B. Online/Offline attribute-based Encryption[M]// Public Key Cryptography. Buenos Aires: Springer, 2014: 293-310

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

[9] Emura K, Atsuko M, Mohammad S. Dynamic attribute based signcryption without random oracles [J]. International Journal of Applied Cryptography, 2012, 2(3): 199-211

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

[11] Zhang Guo-ying, Fu Xiao-jing, Ma Chun-guang. A Dynamic Threshold Attributes-based Signcryption Scheme[J]. Journal of Electronics & Information Technology, 2012, 34(11): 2680-2686(in Chinese)
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