doi:10.3969/j.issn.1000-436x.2014.07.013

高效可证明安全的基于属性的在线/离线加密机制

马海英[1,2]，曾国荪[1]，王占君[3]，王伟[1]

(1. 同济大学 计算机科学与技术系，上海 201804；
2. 南通大学 计算机科学与技术学院，江苏 南通 226019；3. 南通大学 理学院，江苏 南通 226007)

摘 要：为了提高加密的效率，将在线/离线密码技术引入到 ABE 中，提出了基于属性的在线/离线加密(ABOOE)机制。ABOOE 将加密过程非平凡地分解成离线和在线 2 个阶段，离线阶段在不知明文和所需属性集合的前提下，对复杂计算进行预处理；在线阶段获知消息和属性集合后，仅需少量简单计算即可生成密文。首先构建出一个 CPA 安全的 ABOOE 方案。为了提高 ABOOE 的安全性，提出基于属性的在线/离线密钥封装机制(ABOOKEM)和一个相应方案，并构造出一种将单向性 ABOOKEM 转化成 CCA 安全 ABOOE 的通用性方法。该方法在不增加计算量的前提下有效提高了 ABOOE 的安全性。与知名 ABE 方案相比，所提出的 ABOOE 极大地提高了 ABE 中加密的效率，特别适用于计算能力高度受限的终端设备。

关键词：基于属性加密；在线/离线；密钥封装；轻量级设备；可证明安全

中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)07-0104-09

Efficient and provably secure attribute-based online/offline encryption schemes

MA Hai-ying[1,2], ZENG Guo-sun[1], WANG Zhan-jun[3], WANG Wei[1]

(1. Department of Computer Science and Technology, Tongji University, Shanghai 201804, China;.
2. College of Computer Science and Technology, Nantong University, Nantong 226019, China;
3. School of Science, Nantong University, Nantong 226007, China)

Abstract: To improve the encryption efficiency, the online/offline cryptography was extended to ABE and the primitive of attribute-based online/offline encryption (ABOOE) was proposed. The ABOOE non-trivially splited the encryption process into two phases: the offline phase first executed most of heavy computations prior to knowing the message and the attributes' set; and then the online phase only performed light computations to produce the ciphertext once the attributes' set and the message get available. An ABOOE scheme was first constructed with the CPA security. To enhance its security, the primitive of attribute-based online/offline KEM (ABOOKEM) was also introduced and a concrete ABOOKEM scheme was given, and then a generic transformation was proposed to get security against chosen-ciphertext attack (CCA) for ABOOE from any ABOOKEM with one-wayness. This transformation greatly improved the security for ABOOE without increasing the amount of computation. Compared with the famous ABE schemes, the proposed schemes improved the encryption efficiency and get suitable for power-constrained devices.

Key words: attribute-based encryption; online/offline; key encapsulation; lightweight devices; provable security

---

收稿日期：2013-03-18；**修回日期**：2013-10-04

基金项目：国家高技术研究发展计划(“863”计划)基金资助项目(2009AA012201)；国家自然科学基金资助项目(61272107, 61202173, 61103068, 61272424, 11371207, 61202006, 61300167)；NSFC-微软亚洲研究院联合基金资助项目(60970155)；上海市优秀学科带头人计划基金资助项目(10XD1404400)；国家教育部博士点基金资助项目(20090072110035)；教育部网络时代科技论文快速共享专项研究课题基金资助项目(20110740001)；上海自然科学基金资助项目(13ZR1443100)；南通市科技计划基金资助项目(BK2013050, BK2012026, BK2011070)；江苏省高校自然科学研究基金资助项目(12KJB520015, 12KJB520013)

Foundation Items: The National High Technology Research and Development Program of China(863 Program)(2009AA012201); The National Natural Science Foundation of China (61272107, 61202173, 61103068, 61272424, 11371207, 61202006, 61300167); The Joint of NSFC and Microsoft Asia Research(60970155); The Program of Shanghai Subject Chief Scientist (10XD1404400); The Ph.D. Programs Foundation of Ministry of Education of China(20090072110035); The Special Fund for Fast Sharing of Science Paper in Net Era by CSTD (20110740001); Shanghai Natural Science Foundation Program (13ZR1443100); The Science and Technology Project of Nantong (BK2013050, BK2012026, BK2011070); The Natural Science Foundation of the Jiangsu Higher Education Institutions of China (12KJB520015, 12KJB520013)

1　引言

2005 年，由 Sahai 和 Waters[1]在欧密会上首先提出了基于属性的加密 (ABE)机制。在该 ABE 中，用属性标识用户的特征信息(例如学生具有院系、专业、学生类别等属性)，授权中心根据用户具有的属性为其颁发私钥，加密者使用一组属性公钥以预定门限值进行加密，用户能够解密密文当且仅当该用户的属性集与密文属性集的交集不小于系统设定的门限参数。该 ABE[1]仅能实现门限访问控制策略。为了支持更加灵活的访问控制策略，2006 年，Goyal 等[2]在 ACM CCS 上提出密钥策略的 ABE 方案(KP-ABE)，实现了对密文的细粒度访问控制。在 KP-ABE 中，授权中心根据用户的访问策略为其颁发私钥，密文与一组属性相关，只有密文的属性满足用户私钥的访问策略时，才能解密密文。2007 年，Bethencourt 等[3]提出密文策略的 ABE 方案(CP-ABE)。在 CP-ABE 中，用户密钥与属性集相关，密文与访问结构相关。Attrapadung 等[4]提出双策略的基于属性加密方案。此外，学者们对 ABE 中的访问结构的设计[3~6]、属性撤销[7]、用户密钥撤销[8,9]、密钥滥用[9~12]、密钥托管[13]、多授权中心[14~16]等难点问题进行了深入研究，并提出了许多好的研究成果。因此，ABE 机制已成为近年来国内外密码学和安全协议领域的研究热点。

由于 ABE 能够在密文中灵活地表示访问控制策略，从而极大地降低了数据共享细粒度访问控制带来的网络带宽和加密节点的计算开销。因此，ABE 在无线传感网、云存储等细粒度访问控制领域得到广泛应用[17~20]。特别地，在分布式无线传感网中，传感器收集敏感数据并将其传送给基站，为了确保将敏感数据安全地传送给所有授权用户，Hur[19]和 Yu 等[17]利用 KP-ABE 构造了适用于分布式无线传感网的数据共享细粒度访问控制方案。然而，上述方案的加密过程仍然需要执行幂乘等复杂计算。由于轻量级设备(例如无线传感器和智能卡等)计算能力非常有限，在短时间内完成加密请求的复杂计算几乎是不可能的。因此，为了提高加密的效率，在得知消息和属性集合之前，对加密所需复杂计算进行预处理是非常有必要的，一旦获知消息和属性集合，真实的加密过程将可以快速完成。

在线/离线密码机制是一种有效地提高签名或加密效率的密码学技术。1989 年 Even 等[21]首次提出了在线/离线签名机制。但直到 2008 年 Guo 等[22]才首次提出了基于身份的在线/离线加密机制(IBOOE)，与在线/离线签名相类似，该方案巧妙地将加密过程划分成离线和在线 2 个阶段：离线阶段无需得知消息和接收者身份，对加密所需的复杂计算进行预处理；然后，在线阶段获知明文和接收者身份信息后，仅需执行少量简单计算，即可生成密文。因此，在线/离线密码技术尤其适合于计算能力有限的传感器和智能卡等终端设备。在 ASIA CCS 2011 会议上，Chow 等[23]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。

借鉴在线/离线密码技术，本文提出基于属性的在线/离线加密 (ABOOE)机制。在该机制中，将加密过程划分成离线和在线 2 个阶段：离线加密在不知道消息和所需属性的前提下，对所有属性进行预处理，即执行加密所需的幂乘或双线性对等复杂计算，保存计算结果为离线密文；轻量级设备执行在线加密算法，即在获知消息和属性集合后，利用离线密文仅需少量简单计算(整数加法/乘法或散列运算)即可生成密文。但是，现有的 ABE 系统中，由于采用布尔属性描述用户，属性个数较多，如果对每个属性都进行预处理，则生成的离线密文长度过大，轻量级设备很难承受。针对这个问题，本文采用非布尔属性描述用户，根据用户具有的特征信息将所有属性划分成少量的 n 类，每类属性拥有一个共同的属性公钥。离线阶段对每类属性进行预处理，生成相应的离线子密文，离线密文由这 n 个子密文构成。当得知消息和属性集合后，在线阶段利用离线密文快速生成相应的密文。本文利用 Sakai 等提出基于身份的加密方案[24]，构造出一个具体的 CPA 安全的 ABOOE 方案。为了进一步提高 ABOOE 的安全性，本文提出基于属性的在线/离线密钥封装机制(ABOOKEM)和一个相应的具体方案，并构造出一种将单向性的 ABOOKEM 转化成 CCA 安全 ABOOE 的通用性方法，该方法有效地提高了 ABOOE 的安全性。与知名 ABE 方案在性能方面对比分析可得，本文的 ABOOE 方案极大地提高了 ABE 中加密的效率，特别适用于计算能力高度受限的终端设备。

2 预备知识

2.1 对称双线性对和困难性假设

定义 1 (对称双线性对[23]) 令 $\boldsymbol{G}$ 和 $\boldsymbol{G}_T$ 是阶为大素数 p 的乘法循环群，g 是 $\boldsymbol{G}$ 的生成元，若存在一个映射 e: $\boldsymbol{G}\times\boldsymbol{G}\rightarrow\boldsymbol{G}_T$，满足如下条件：1) 双线性，对于$\forall u, v\in\boldsymbol{G}$, $\forall a, b\in Z_p$, $e(u^a, v^b) = e(u, v)^{ab}$; 2) 非退化性，$e(g, g)\neq 1$; 3) 可计算性，$\forall u, v\in\boldsymbol{G}$，存在有效的算法在多项式时间内计算 $e(u, v)$；那么称上述映射 e 为一个对称的双线性对。

定义 2 (l-DBDHI 假设[23]) l-DBDHI 问题在$(\boldsymbol{G}, \boldsymbol{G}_T)$上定义为：随机选择 $\alpha\in Z_p^*$，g 是 $\boldsymbol{G}$ 的生成元，给定一个 $(l+2)$ 元组 $(g, g^{\alpha}, g^{\alpha^2},\cdots,g^{\alpha^l}, T)\in\boldsymbol{G}^{l+1}\times\boldsymbol{G}_T$，判定 T 的值是否为 $e(g,g)^{1/\alpha}$。如果对于任意概率多项式时间(PPT)算法 A 在$(\boldsymbol{G}, \boldsymbol{G}_T)$上解决 l-DBDHI 问题的优势均是可忽略的，则称 l-DBDHI 假设在$(\boldsymbol{G}, \boldsymbol{G}_T)$上是成立的。

定义 3 (l-BDHI 假设[23]) l-BDHI 问题在$(\boldsymbol{G}, \boldsymbol{G}_T)$上定义为：随机选择 $\alpha\in Z_p^*$，g 是 $\boldsymbol{G}$ 的生成元，给定一个$(l+1)$元组$(g, g^{\alpha}, g^{\alpha^2},\cdots,g^{\alpha^l})\in\boldsymbol{G}^{l+1}$，计算 $e(g,g)^{1/\alpha}$。如果对于任意 PPT 算法 A 在$(\boldsymbol{G}, \boldsymbol{G}_T)$上解决 l-BDHI 问题的优势均是可忽略的，则称 l-BDHI 假设在$(\boldsymbol{G}, \boldsymbol{G}_T)$上是成立的。

2.2 访问结构和线性秘密共享方案(LSSS)

定义 4 (访问结构[9]) 设 $P=\{P_1, P_2, \cdots, P_n\}$ 是 n 个属性的集合，集族 $A\subseteq 2^P$，如果对任意集合 B, C，都有：若 $B\in A$ 且 $B\subseteq C$，则 $C\in A$，则称 A 是单调的。访问结构是 P 的某些非空子集构成的集族 A，即 $A\subseteq 2^P\backslash\phi$，访问结构 A 中的集合称为授权集。否则，称为非授权集。若集族 A 是单调的，则称 A 是单调访问结构。

定义 5 (LSSS[9]) 属性集合 $P=\{P_1, P_2, \cdots, P_n\}$ 上的秘密共享方案 Π 是线性的，如果 Π 满足如下条件：1) 参与者的秘密分享值构成 Z_p 上的一个向量；2) 对于 Π，存在一个秘密份额生成矩阵 $\boldsymbol{M}_{d\times h}$ 和行标号函数 ρ:$\{1,\cdots, d\}\rightarrow P$。设 $s\in Z_p$ 是待共享的秘密值，随机选择 $r_2, \cdots, r_h\in Z_p$，构成向量 $\boldsymbol{v} = (s, r_2, \cdots, r_h)$，令 $\boldsymbol{v}'$为 $\boldsymbol{v}$ 的转置，则 $\boldsymbol{Mv}'$是 d 个秘密份额构成的向量，根据标号函数将秘密份额 $\lambda_i=(\boldsymbol{Mv}')_i(1\leqslant i\leqslant d)$分配给属性 $\rho(i)$。

LSSS 满足线性重构性质：若 Π 是访问结构 A 的线性秘密共享方案，令 $S\in A$ 是授权集，定义 $I=\{i: \rho(i)\in S\}\subseteq\{1,\cdots, d\}$，则存在 PPT 算法计算$\{c_i\in Z_p\}_{i\in I}$，使得对于秘密共享值 s 的任意有效份额 $\{\lambda_i\}, i\in\{1,\cdots, d\}$，均满足 $\Sigma_{i\in I}c_i\lambda_i = s$。

3 ABOOE 和 ABOOKEM 的定义和安全模型

3.1 ABOOE 的定义

一个 ABOOE 方案由 5 个 PPT 算法组成：初始化(Setup)、密钥生成(KeyGen)、离线加密(Enc^{Off})、在线加密(Enc^{On})、解密(Dec)。

Setup(λ, n) → (Pub, Msk) 初始化算法输入系统安全参数 λ 和属性类型个数 n，生成系统公钥 Pub 和主密钥 Msk。

KeyGen(Msk, $A(\boldsymbol{M}, \rho)$) → Pvk_A 密钥生成算法输入主密钥 Msk 和用户的访问结构 $A(\boldsymbol{M}, \rho)$，输出用户私钥 Pvk_A。

Enc^{off}(Pub) → Δ: 离线加密算法输入系统公钥 Pub，生成离线密文 Δ。

Enc^{on}(m, ω, Δ)→CT: 在线加密算法输入消息 m、属性集 ω 和离线密文 Δ，生成密文 CT。

Dec(Pvk_A, CT) → m/⊥ 解密算法输入用户私钥 Pvk_A 和密文 CT，如果 CT 中的属性集 ω 满足用户私钥中的访问策略 $A(\boldsymbol{M}, \rho)$，输出消息 m；否则，输出解密失败符号⊥。

3.2 ABOOE 的选择性安全模型

定义 6 (选择模型下选择密文攻击 IND-SS-CCA 安全性游戏) ABOOE 的选择安全模型可以通过敌手 A 和挑战者 C 之间的游戏来进行如下定义。

Init 敌手 A 宣布一个挑战属性集合 γ。

Setup 挑战者 C 运行 ABOOE 的 Setup 算法，将公钥参数 Pub 发送给 A，并保存 Msk。

Phase 1 A 可以向 C 多次询问下面 2 类预言机。1) 密钥生成预言机 OKeyGen(·)：A 提交访问结构 $A(\boldsymbol{M}, \rho)$给 C，C 运行 KeyGen(Msk, $A(\boldsymbol{M}, \rho)$)，输出计算结果 Pvk_A，且要求 γ 不能满足 $A(\boldsymbol{M}, \rho)$; 2) 解密预言机 ODec(·)：A 提交密文 CT 给解密预言机，如果解密成功，返回消息 m 给 A，否则返回⊥，表示拒绝解密。

Challenge 敌手 A 将 2 个等长的消息 m_0 和 m_1 提交给 C。C 随机选择 $b\in\{0,1\}$，用 γ 加密消息 m_b，计算密文 $CT^*=\text{Enc}^{\text{on}}(m_b, \gamma, \text{Enc}^{\text{off}}(Pub))$，并将 CT^*发送给 A。

Phase 2 敌手 A 可以继续执行 Phase 1 中的密钥生成询问和解密询问，但询问密文不能为 CT^*。

Guess　敌手 A 给出一个猜测值 b'。当 $b'=b$ 时，敌手 A 赢得这个游戏，A 在该游戏中的优势定义为 $|Pr[b'=b]-1/2|$。

定义 7　(IND-SS-CCA 安全性)如果任意 PPT 敌手 A 赢得 IND-SS-CCA 安全性游戏的优势都是可忽略的，则称该 ABOOE 方案在适应性选择密文攻击下是选择安全的。

定义 8　(选择模型下选择明文攻击（IND-SS-CPA）安全性)如果任意 PPT 敌手 A 在上述 IND-SS-CCA 安全性游戏中不允许询问解密预言机，且赢得该游戏的优势均是可忽略的，则称该 ABOOE 方案在适应性选择明文攻击下是选择安全的。

3.3　ABOOKEM 的定义和单向性安全模型

一个 ABOOKEM 方案由 5 个 PPT 算法组成：初始化(Setup)，密钥生成(KeyGen)，离线密钥封装(KEM^{Off})，在线密钥封装(KEM^{On})，解封装(KDM)。

Setup 和 KeyGen　与 ABOOE 的初始化算法和私钥生成算法相同。

$KEM^{Off}(Pub, r) \rightarrow (\Gamma, K)$　离线密钥封装算法是确定性算法，输入系统公钥参数 Pub 和随机数 r，生成离线数据 Γ 和会话密钥 K。注意：当随机数 r 相同时，输出的二元组(Γ, K)必须相同。

$KEM^{On}(\Gamma, \omega) \rightarrow CT$　在线密钥封装算法输入属性集 ω 和离线密文 Γ，生成密文 CT。

KDM(CT, Pvk_A): $\rightarrow$ (K/⊥)　解封装算法输入密文 CT 和用户私钥 Pvk_A，如果 CT 中的属性集 ω 满足用户私钥中的访问策略 $A(\boldsymbol{M}, \rho)$，输出会话密钥 K；否则，输出解封装失败符号⊥。

ABOOKEM 单向性选择安全游戏可以通过敌手 A 和挑战者 C 之间的游戏来进行如下定义。

Init　敌手 A 宣布一个挑战属性集合 γ。

Setup　挑战者 C 运行 ABOOKEM 的 Setup 算法，将公钥参数 Pub 发送给 A，并保留 Msk。

Phase 1　A 提交访问结构 $A(\boldsymbol{M}, \rho)$给 C，C 运行 KeyGen(Msk, $A(\boldsymbol{M}, \rho)$)，输出计算结果 Pvk_A，且要求 γ 不能满足 $A(\boldsymbol{M}, \rho)$。

Challenge　C 选择随机数 r，计算密文 CT^*= $KEM^{on}(Pub, \gamma, KEM^{off}(Pub, r))$，并将 CT^*发给 A。

Phase 2　敌手 A 可以继续执行 Phase 1 中的密钥询问。

Output calculation　敌手 A 依据密文 CT^*计算出会话密钥 K。

当 A 输出的 K 等于 CT^*中加密的会话密钥 K' 时，称敌手 A 赢得上述单向性选择安全游戏。A 赢得上述游戏的优势定义为 $Pr[K'=K]$。

定义 9　(单向选择 OW-SS 安全性)　如果任意 PPT 敌手 A 赢得 OW-SS 安全性游戏的优势都是可忽略的，则称该 ABOOKEM 是单向性选择安全。

4　具有 CPA 安全的 ABOOE 方案

在 ABOOE 系统中，将全部属性划分成少量的 n 类，每类属性拥有一个共同的属性公钥，且每个属性对应 Z_p 中的一个元素。首先，离线加密为每类属性选择一个随机数，计算该随机属性的离线子密文，并存储一些辅助信息。然后，在线加密在得知消息和属性集合后，利用离线密文计算 Z_p 中的若干个整数(实现了从随机属性到指定属性的有效转化)，即可快速生成给定消息和属性集合下的密文。

4.1　ABOOE 方案

Setup(λ, n)　初始化算法输入系统安全参数 λ 和属性类型个数 n。首先，生成双线性映射 $e: \boldsymbol{G} \times \boldsymbol{G} \rightarrow \boldsymbol{G}_T$ 和群 $\boldsymbol{G}$ 的生成元 g，令 $v = e(g, g)$; 构造 n 个独立的 SK-IBE[24]子系统，$Msk_i = (a_i)$, $Pub_i = \{g, g^{a_i}, v, H_i: \{0,1\}^* \rightarrow Z_p\}$。输出该系统公钥 $Pub=(g, v, g^{a_1}, \cdots, g^{a_n}, H_1, \cdots, H_n)$和主密钥 $Msk= (a_1, \cdots, a_n)$。

KeyGen(Msk, $A(\boldsymbol{M}, \boldsymbol{\rho})$)　密钥生成算法输入主私钥 Msk、访问结构 $A(\boldsymbol{M}, \rho)$，其中，$\boldsymbol{M}$ 是 $d \times h$ 矩阵，进行如下计算：1) 选择随机数 $u_2, \cdots, u_h \in Z_p^*$，令 $\boldsymbol{u} = (1, u_2, \cdots, u_h)$; 2) 对矩阵 $\boldsymbol{M}$ 的任一行 $\boldsymbol{M_x}$ ($x = 1, 2, \cdots, d$)，有属性 $I_{\rho(x)}$($I_{\rho(x)}$为第 $\rho(x)$类属性)与之相对应，计算该属性私钥为

$$D_{\rho(x)} = g^{\frac{\boldsymbol{M_x u}}{a_{\rho(x)}+I_{\rho(x)}}}$$

输出用户私钥

$$Pvk_A = \left(g^{\frac{\boldsymbol{M}_1 \boldsymbol{u}}{a_{\rho(1)}+I_{\rho(1)}}}, \cdots, g^{\frac{\boldsymbol{M}_d \boldsymbol{u}}{a_{\rho(d)}+I_{\rho(d)}}} \right)$$

$Enc^{off}(Pub)$　离线加密算法对 i =1, 2,⋯, n，随机选择 r，β_i，$\gamma_i \in Z_p^*$，计算：$R = v^r$，$T_{1,i} = (g^{a_i} g^{\beta_i})^r$，$T_{2,i} = g^{\gamma_i \cdot r}$，$c_i' = H_i(R, T_{2,i})$。输出离线密文 $\Delta= (T_{1,i}, T_{2,i}, c_i', \beta_i, \gamma_i)$,$i$=1, 2, ⋯,$n$。

$Enc^{on}(m, \omega, \Delta)$　在线加密算法输入消息 m、属性集 $\omega=(I_{i1}, I_{i2}, \cdots, I_{it})$和离线密文 Δ，计算：$t_{ij}' = \gamma_{ij}^{-1}(I_{ij} - \beta_{ij}) \bmod p$, $c=c_{i1}' \oplus \cdots \oplus c_{it}' \oplus m$。输出在线密文 CT = $(c, (T_{1,ij}, T_{2,ij}, t_{ij}'), j=1, 2, \cdots, t)$。

Dec(Pvk_A, CT)　解密算法输入用户私钥 Pvk_A 和密文 CT，记 $I = \{x \mid I_{\rho(x)} \in \omega\}$。当 CT 中的属性满

足 Pvk_A 中的策略 $A(\boldsymbol{M}, \rho)$时，首先计算系数 $\theta_x \in Z_p$，使

$$\sum_{x\in I}\theta_x \boldsymbol{M}_x = (1, 0, \cdots, 0)$$

然后计算

$$e(T_{1,\rho(x)}T_{2,\rho(x)}^{t'_{\rho(x)}}, g^{\frac{\boldsymbol{M}_x\boldsymbol{u}}{a_{\rho(x)}+I_{\rho(x)}}}) = e(g,g)^{r\boldsymbol{M}_x\boldsymbol{u}}$$

$$\prod_{x\in I} e(g,g)^{r\theta_x\boldsymbol{M}_x\boldsymbol{u}} = v^r = R$$

$$c'_{ij} = H_{ij}(R, T_{2,ij})，\ m = c \oplus c'_{i1} \oplus c'_{i2} \oplus \cdots \oplus c'_{it}$$

否则，解密失败。

4.2 IND-SS-CPA 安全性证明

定理 1 如果 $n(l+1)$-DBDHI 假设成立，则 ABOOE 方案满足选择模型下的 IND-SS-CPA 安全性。

证明 假设存在一个 PPT 敌手 A 以 ε 的优势攻破 ABOOE 方案在选择属性集模型下的 CPA 安全性，则可以构造一个仿真器 B 以 $\varepsilon/2$ 优势攻破 $n(l+1)$-DBDHI 假设。

挑战者 C 给出一个 $n(l+1)$-DBDHI 元组$(g, g^{\alpha}, \cdots, g^{\alpha^{n(l+1)}}, T)$，其中 $T=e(g,g)^{1/\alpha}$ 或 T 为 $\boldsymbol{G}_T$ 中一个随机元素。当 $T=e(g,g)^{1/\alpha}$，仿真器 B 输出 1；否则，B 输出 0。

Init A 宣布挑战属性集 $\gamma = \{I_{i1}, I_{i2}, \cdots, I_{it}\}$，并将其发给 B。

Setup 当 $i = i_1, \cdots, i_t$ 时，B 随机选择 $\pi_i \in \{1, 2, \cdots, l\}$, $I_{\pi i} \in Z_p^*$, $w_{i1}, \cdots, w_{i\pi_i-1}, w_{i\pi_i+1}, \cdots, w_{il} \in Z_p^*$，对 $i_j \in \{1, 2, \cdots, l\}\backslash\{\pi_i\}$，计算 $I_{ij} = I_{\pi i} - w_{ij}$，构造 $t(l-1)$ 次多项式

$$f(z) = \prod_{i=i_1}^{i_t}\prod_{j=1, j\neq\pi_i}^{l}(z + w_{ij})$$

得到系数 $c_0, c_1, \cdots, c_{t(l-1)} \in Z_p^*$，即 $f(z) = \sum_{i=0}^{t(l-1)} c_i z^i$。然后，$B$ 设置生成元 $G = \prod_{i=0}^{t(l-1)}(g^{\alpha^i})^{c_i} = g^{f(\alpha)}$。

当 $ij \in \{1, \cdots, l\}\backslash\{\pi_i\}$，$B$ 计算

$$f_{ij}(z) = \frac{f(z)}{z + w_{ij}} = \sum_{k=0}^{t(l-1)-1} d_{ij,k} z^k$$

系数为 $d_{ij,0}, \cdots, d_{ij,t(l-1)-1} \in Z_p^*$，计算

$$\widetilde{H_{ij}} = \prod_{k=0}^{t(l-1)-1}(g^{\alpha^k})^{d_{ij,k}} = g^{f_{ij}(\alpha)} = G^{\frac{1}{\alpha+w_{ij}}}$$

$$\widetilde{H_{ij}}^{\alpha} = \prod_{k=0}^{t(l-1)-1}(g^{\alpha^{k+1}})^{d_{ij,k}} = G^{\frac{\alpha}{\alpha+w_{ij}}}$$

B 计算 $Pub_i = G^{-\alpha}G^{-I_{\pi i}}$，其中，$G^{-\alpha} = \prod_{i=0}^{t(l-1)}(g^{\alpha^{i+1}})^{c_i}$，使得第 i 类属性的未知主密钥 $Msk_i = -\alpha - I_{\pi i}$。

当 $i \neq i_1, \cdots, i_t$，B 随机选择 $a_i \in Z_p^*$，计算 $Pub_i = G^{a_i}$，即 $msk_i = a_i$。

最后，B 设置公钥参数 $Pub = \{G, v = e(G, G), Pub_1, \cdots, Pub_n, H_1, \cdots, H_n\}$, $Msk = \{Msk_1, \cdots, Msk_n\}$。

Phase 1 A 询问访问结构 $A(\boldsymbol{M}, \rho)$的私钥，使得 γ 不满足(M, ρ)，记为 $\gamma \nvDash (M, \rho)$。令 $\boldsymbol{M}_\gamma = \{\boldsymbol{M}_x \mid I_{\rho(x)} \in \gamma\}$，因为 $\gamma \nvDash (\boldsymbol{M}, \rho)$，所以$(1, 0, \cdots, 0) \notin$ Span M_γ。因此，存在向量 $\boldsymbol{w} = (w_1, \cdots, w_h)$，使得 $\boldsymbol{w}$ 垂直 $\boldsymbol{M}_\gamma$，即 $\boldsymbol{w}\boldsymbol{M}_\gamma = 0$，但 $\boldsymbol{w}$ 不垂直 $\boldsymbol{I} = (1, 0, \cdots, 0)$。为了生成 Pvk_A，B 随机选择 $\lambda_1, \cdots, \lambda_h \in Z_p^*$，隐式的设置

$$\boldsymbol{v} = (\lambda_1\alpha, \cdots, \lambda_h\alpha),\ \psi = \frac{1-\lambda_1\alpha}{w_1},\ \boldsymbol{u} = \boldsymbol{v} + \psi\boldsymbol{w}$$

，注意，$\boldsymbol{I}\boldsymbol{u} = \boldsymbol{I}\boldsymbol{v} + \boldsymbol{I}(\psi\boldsymbol{w}) = \lambda_1\alpha + \frac{1-\lambda_1\alpha}{w_1}w_1 = 1$。

令 $\boldsymbol{M}_x = (m_{x,1}, \cdots, m_{x,h})$

1) 当 $I_{\rho(x)} \in \gamma$ 时，B 计算 $\phi_1 = -\sum_{j=1}^{h} m_{x,j}\lambda_j$，令 $D_{\rho(x)} = G^{\phi_1}$，由于 ϕ_1 是已知的，且

$$\frac{\boldsymbol{M}_x\boldsymbol{u}}{a_{\rho(x)}+I_{\rho(x)}} = \frac{\boldsymbol{M}_x(\boldsymbol{v}+\psi\boldsymbol{w})}{a_{\rho(x)}+I_{\rho(x)}}$$

$$= \frac{\alpha\sum_{j=1}^{h} m_{x,j}\lambda_j}{-\alpha} = -\sum_{j=1}^{h} m_{x,j}\lambda_j$$

所以 $D_{\rho(x)}$是一个正确生成的私钥。

2) 当 $I_{\rho(x)} \notin \gamma$ 且 $I_{\rho(x)}$是 $i_1, \cdots, i_t$ 类的属性时，记 $I_{\rho(x)} = I_{ij}$，其中 $\rho(x) = i_1, \cdots, i_t$，且 $j \neq \pi_i$, B 令 $D_{\rho(x)} = D_{ij} = (H_{ij}^{\alpha})^{\phi_2}$，其中

$$\phi_2 = -\sum_{j=1}^{h} m_{x,j}\lambda_j$$

注意：H_{ij}^{α} 和 ϕ_2 是已知的，且

$$\frac{\boldsymbol{M}_x\boldsymbol{u}}{a_{\rho(x)}+I_{\rho(x)}} = \frac{\boldsymbol{M}_x\boldsymbol{v}}{a_{\rho(x)}+I_{\rho(x)}} =$$

$$\frac{\alpha\sum_{j=1}^{h} m_{x,j}\lambda_j}{-\alpha-w_{ij}} = \frac{\alpha}{\alpha+w_{ij}}(-\sum_{j=1}^{h} m_{x,j}\lambda_j)$$

3) 当 $I_{\rho(x)} \notin \gamma$ 且 $I_{\rho(x)}$不是 $i_1, i_2, \cdots, i_t$ 类的属性时，即 $\rho(x) \neq i_1, \cdots, i_t$, B 计算 $D_{\rho(x)} = (G^{\alpha})^{\phi_2} G^{\phi_3}$，其中

$$\phi_2 = \frac{\sum_{j=1}^{h} m_{x,j}\lambda_j}{a_{\rho(x)} + I_{\rho(x)}}, \quad \phi_3 = \frac{\psi\sum_{j=1}^{h} m_{x,j} w_j}{a_{\rho(x)} + I_{\rho(x)}}$$

由于

$$\frac{\boldsymbol{M}_x \boldsymbol{u}}{a_{\rho(x)} + I_{\rho(x)}} = \frac{\alpha\sum_{j=1}^{h} m_{x,j}\lambda_j}{a_{\rho(x)} + I_{\rho(x)}} + \frac{\psi\sum_{j=1}^{h} m_{x,j} w_j}{a_{\rho(x)} + I_{\rho(x)}} = \alpha\phi_2 + \phi_3$$

且 G^{α}、ϕ_2 和 ϕ_3 是已知的，因此，$D_{\rho(x)}$是正确生成的属性私钥。

综上所述，当 γ 不满足 $A(\boldsymbol{M}, \rho)$时，B 可以为访问结构 $A(\boldsymbol{M}, \rho)$生成相应的属性私钥。

Challenge　A 输出消息 m_0, m_1。B 随机选择一个比特 $b \in \{0,1\}$，并利用 γ 对消息 m_b 进行如下加密。对 $i = i_1, \cdots, i_t$，B 随机选择 $\xi, t_{0,i}, s_i \in Z_p^*$，隐式地设置 $\lambda_i = I_{\pi_i} + (t_{0,i} + 1)\alpha$，$\beta_i = -s_i(t_{0,i} + 1)\alpha$，计算

$$T_{1,i} = \xi t_{0,i} G = \frac{\xi}{\alpha}(\lambda_i G + Pub_i), \; T_{2,i} = \frac{\xi\beta G}{\alpha}$$

$$t_i^{'} = \beta_i^{-1}(I_i - \lambda_i) = 1/s_i, \quad T_h = T^{c_0^2} T_0$$

其中

$$T_0 = e(g^{\sum_{i=1}^{n(l-1)} c_i \alpha^{i-1}}, g^{f(\alpha)}) e(g^{\sum_{i=1}^{n(l-1)} c_i \alpha^{i-1}}, g^{c_0}) = e(g,g)^{\frac{f(\alpha)^2 - c_0^2}{\alpha}}$$

计算 $c_i' = H_i(T_h, T_{2,i})$, $c = c_{i1}' \oplus \cdots \oplus c_{it}' \oplus m_b$，输出挑战密文 $CT^* = (c, (T_{1,j}, T_{2,j}, t_{1,j}) j = i_1, i_2, \cdots i_t)$。

Phase 2　重复 Phase 1。

Guess　最后，A 输出对 b 的猜测值 b'。若 $b' = b$，B 输出 1，表示 $T = e(g,g)^{\frac{1}{\alpha}}$；否则，若 $b' \neq b$，B 输出 0，表示 T 是一个随机元素。

Probability Analysis　当 $T = e(g,g)^{\frac{1}{\alpha}}$ 时，$T_h = T^{c_0^2} T_0 = e(g,g)^{\frac{f(\alpha)^2}{\alpha}} = e(G,G)^{\frac{1}{\alpha}}$, CT^*是正确的密文，A 猜对的概率为 $\frac{1}{2}+\varepsilon$。当 T 是随机元素时，T_h 也是 G_T 的随机元素，CT^*将是随机消息的密文，A 猜对概率为 $\frac{1}{2}$。总之，A 猜对概率为 $\frac{1}{2}+\varepsilon$，B 猜对 $n(l+1)$-DBDHI 元组的优势是 $\varepsilon/2$。

5　CCA 安全 ABOOE 的通用性构造方法

为了提高 ABOOE 的安全性，本节首先给出一个高效的 ABOOKEM 方案，并对其单向性进行证明。然后，提出一种将单向性 ABOOKEM 转化成 CCA 安全 ABOOE 的通用性方法，并证明该 ABOOE 方案满足 IND-SS-CCA 安全性。

5.1　单向性 ABOOKEM 方案

1) ABOOKEM 方案

Setup(λ, n)　除了删除 n 个散列函数外，与 ABOOE 的初始化算法相同。

KeyGen(Msk, $A(\boldsymbol{M}, \rho)$)　与 ABOOE 的私钥生成算法相同。

KEM^{off}(Pub, r)　离线密钥封装算法输入 $r \in Z_p^*$，计算会话密钥 $K = e(g,g)^r$。然后，对 i =1, 2, …, n，随机选择 β_i, $\gamma_i \in Z_p^*$，计算 $T_{1,i} = (g^{a_i} g^{\beta_i})^r$，$T_{2,i} = g^{\gamma_i \cdot r}$，输出会话密钥 K 和离线数据 Γ= ($T_{1,i}$, $T_{2,i}$, β_i, γ_i)i=1, 2, …,n。

KEM^{on}(ω, Γ)　在线密钥封装算法输入属性集 ω=(I_{i1}, I_{i2}, …, I_{it})和离线数据 Γ，计算：$t_{ij}' = \gamma_{ij}^{-1} \cdot (I_{ij} - \beta_{ij}) \bmod p$，输出密文 CT=($T_{1,ij}$, $T_{2,ij}$, t_{ij}') j=1, 2, …,t。

KDM(Pvk_A, CT)　解封装算法输入用户私钥 Pvk_A 和密文 CT，记 $I = \{x \mid I_{\rho(x)} \in \omega\}$。当 CT 中的属性满足 Pvk_A 中的策略 $A(\boldsymbol{M}, \rho)$时，首先计算系数 $\theta_x \in Z_p$，使得 $\Sigma x \in I \theta_x \boldsymbol{M}_x$= (1,0,…,0)，然后计算

$$e(T_{1,\rho(x)} T_{2,\rho(x)}^{t_{\rho(x)}'}, g^{\frac{\boldsymbol{M}_x \boldsymbol{u}}{a_{\rho(x)} + I_{\rho(x)}}}) = e(g,g)^{r\boldsymbol{M}_x \boldsymbol{u}}$$

$$\prod_{x \in I} e(g,g)^{r\theta_x \boldsymbol{M}_x \boldsymbol{u}} = v^r = K$$

得到会话密钥 K；否则，解封装失败。

2) 单向性证明

定理 2　如果 $n(l+1)$-BDHI 假设成立，则 ABOOKEM 方案满足选择模型下的单向性。

证明　假设存在一个 PPT 敌手 A 以 ε 的优势攻破 ABOOKEM 方案的单向性，则可以构造一个仿真器 B 以 ε 优势攻破 $n(l+1)$-BDHI 假设。

首先挑战者 C 生成系统公钥参数，并给出一个 $n(l+1)$-BDHI 元组$(g, g^{\alpha}, g^{\alpha^2}, \cdots, g^{\alpha^{n(l+1)}})$。仿真器 B 运行 A，输出 $e(g,g)^{\frac{1}{\alpha}}$。

Init　A 宣布挑战属性集 $\gamma = \{I_{i1}, I_{i2}, \cdots, I_{it}\}$，并将其发给 B。

Setup 和 Phase 1 与 ABOOE 的 Setup 阶段和 Phase 1 阶段相同。

Challenge A 提交挑战属性集 $\gamma=\{I_{i1}, I_{i2}, \cdots, I_{it}\}$给 B。对 $i=i_1, i_2, \cdots, i_t$，B 随机选择 $\xi, t_{0,i}, s_i \in Z_p^*$，隐式地设置

$$\lambda_i = I_{\pi_i} + (t_{0,i}+1)\alpha\,,\ \beta_i = -s_i(t_{0,i}+1)\alpha$$

计算

$$T_{1,i} = \xi t_{0,i} G = \frac{\xi}{\alpha}(\lambda_i G + Pub_i)\,,$$

$$T_{2,i} = \xi(-s_i)(t_{0,i}+1)G = \frac{\xi\beta G}{\alpha},$$

$$t_i' = \beta_i^{-1}(I_i - \lambda_i) = 1/s_i,\ (T_{1,i}, T_{2,i}, t_i')_{i=i_1,i_2,\cdots i_t}$$

为正确生成的密文。

Phase 2 重复 Phase 1。

Output Calculation A 以 ε 的优势输出 K，即 $K=e(g,g)^{\frac{\xi\cdot f(\alpha)^2}{\alpha}}$，其中，$f(z)=\sum_{i=0}^{t(l-1)} c_i z^i$，则 $n(l+1)$-BDHI 假设的解为

$$\left(\frac{K^{1/\xi}}{e(\prod_{i=0}^{t(l-1)-1}(g^{\alpha^i})^{c_{i+1}}, g^{c_0})\cdot e(\prod_{i=0}^{t(l-1)-1}(g^{\alpha^i})^{c_{i+1}}, G)}\right)^{1/c_0^2}$$

$$=\left(\frac{e(g,g)^{\frac{f(\alpha)^2}{\alpha}}}{e(g,g)^{\frac{f(\alpha)^2-c_0^2}{\alpha}}}\right)^{1/c_0^2} = e(g,g)^{\frac{1}{\alpha}}$$

总之，A 解决 $n(l+1)$-BDHI 假设的优势为 ε。

5.2 构造 CCA 安全 ABOOE 的通用性方法

1) 单向性 ABOOKEM 转化成 CCA 安全 ABOOE 的通用性方法

Setup(λ, n) 与 ABOOKEM 相同，此外，需增加 2 个散列函数 H、H'，它们将任意字符串映射到合适的域上。

KeyGen(Msk, $A(M, \rho)$) 与 ABOOKEM 相同。

Enc^{off}(Pub) 离线加密算法随机选择 r，计算$(\Gamma, K)\leftarrow \mathrm{KEM}^{off}(Pub, r)$，输出离线密文 $\Delta=(\Gamma, K, r)$。注意：该算法是确定性算法，即当随机数 r 相同时，输出的二元组(Γ, K)必须相同。

Enc^{on}(m, ω, Δ) 在线加密算法输入消息 m、属性集$\omega=(I_{i1}, I_{i2}, \cdots, I_{it})$和离线密文$\Delta$，计算 $C_1=\mathrm{KEM}^{on}(\Delta, \omega)$, $C_2=H(K, C_1, m)\oplus r$, $C_3=H'(K, C_1)\oplus m$, 输出密文 $CT=(C_1, C_2, C_3)$。

Dec(Pvk_A,CT) 解密算法输入用户私钥 Pvk_A 和密文 CT，记 $I=\{x \mid I_{\rho(x)}\in\omega\}$，当 CT 中的属性满足 Pvk_A 中的策略 $A(\boldsymbol{M}, \rho)$时，计算：$K\leftarrow \mathrm{KDM}(Pvk_A, C_1)$；否则，输出⊥，表示解密失败。然后，计算：$m=H'(K, C_1)\oplus C_3$，$K'=\mathrm{KEM}^{off}(H(K, C_1, m)\oplus C_2)$，若 $K'=K$，输出 m，否则解密失败。

2) IND-SS-CCA 安全性证明

定理 3 如果 ABOOKEM 具有选择模型下的单向性，则该 ABOOE 在选择模型下是 CCA 安全的。

证明 如果存在一个 PPT 敌手 A 可以攻破 ABOOE 的 CCA 安全性，则可以构造仿真器 B 攻破 ABOOKEM 的单向性。挑战者 C 仿真 ABOOKEM 的单向性如下。

Init A 宣布挑战属性集 $\gamma=\{I_{i1}, I_{i2}, \cdots, I_{it}\}$，并将 γ 发给 B。B 将 γ 发送给 C。

Setup C 生成 ABOOKEM 的主密钥 Msk 和公钥参数 Pub，并将 Pub 发给 B。B 将 Pub 发给 A，并仿真散列函数 H 和 H'。

Phase 1 A 提交访问结构 $A(\boldsymbol{M}, \rho)$给 B，B 将 $A(\boldsymbol{M}, \rho)$提交给 C，C 生成相应的私钥 Pvk_A，并将其发送给 A。由 ABOOKEM 到 ABOOE 的转化方法可知，ABOOE 与 ABOOKEM 私钥相同，可确保生成的密钥是正确的。

Decryption Oracle 输入密文 $CT=(C_1, C_2, C_3)$，B 执行如下操作：1) 检索散列函数 H 的输入和输出列表$\{h_i\}$，使得 $h_i=H(K_i, C_1, m_i)$，m_i =

表 1 本文 ABOOE 方案与知名 ABE 方案的性能比较

方案	加密或在线加密	解密	密文长度	安全性
Fuzzy IBE[1]	$(\|\omega\|+1)E+M$	$\mathrm{d}E+\mathrm{d}M+\mathrm{d}P$	$\|\omega\|\|G\|+\|G_T\|$	标准模型 IND-SS-CPA
KP-ABE[2]	$(\|\omega\|+1)E+M$	$\|\omega\|P+2\|S\|E+(\|S\|+1)M$	$\|\omega\|\|G\|+\|G_T\|$	标准模型 IND-SS-CPA
ABOOE-Ⅰ	$\|\omega\|m_c$	$(2\|S\|-1)M+\|S\|P+\|S\|E$	$\|Z_p\|+\|\omega\|(2\|G\|+\|Z_p\|)$	随机模型 IND-SS-CPA
ABOOE-Ⅱ	$\|\omega\|m_c$	$(2\|S\|-1)M+\|S\|P+\|S\|E$	$2\|Z_p\|+\|\omega\|(2\|G\|+\|Z_p\|)$	随机模型 IND-SS-CCA

$C_3 \oplus H'(K_i, C_1)$，注意：散列函数 H，H' 中的 K_i 必须相同；2) 对输入输出列表的$\{h_i\}$，检测 K_i 与 $\mathrm{KEM}^{\mathrm{off}}(C_2 \oplus h_i)$是否相等。若对所有的 K_i，$K_i \neq \mathrm{KEM}^{\mathrm{off}}(C_2 \oplus h_i)$，输出失败信息⊥；否则，输出 $m_i = C_3 \oplus H'(K_i, C_1)$。

Challenge　A 将消息 m_0, m_1 提交给 B。C 利用 γ 执行 ABOOKEM 的密钥封装算法，生成密文 C'，B 随机选择 C_2^*, C_3^*，将 $CT=(C', C_2^*, C_3^*)$发送给 A。类似于参考文献[23]，如果 A 能以不可忽略的优势赢得上述游戏，则它在输出猜测值 b' 之前一定询问过 $H(K^*, C', m^*)$或 $H'(K^*, C')$。B 选择一个随机预言机询问，并输出第一个变量的值，作为 ABOOKEM 单向性游戏的输出值。

Probability Analysis　如果 A 没有询问过 K^*，其成功的概率为 0；如果 A 询问过 K^*，其成功的概率为 $1/q_H$。总之，B 成功的概率为 ε/q_H，q_H 是询问随机预言机的次数。

5.3　性能对比

表 1 将本文的 2 个 ABOOE 方案和知名 ABE 方案在效率和安全模型方面进行详细比较，其中，E 表示群 $\boldsymbol{G}$ 或 $\boldsymbol{G}_T$ 的幂乘运算量，M 表示群 $\boldsymbol{G}$ 或 $\boldsymbol{G}_T$ 的乘法运算量，P 表示双线性对运算量，m_c 表示域 Z_p 中的模运算量，$|\omega|$表示集合 ω 中属性的个数，$|\boldsymbol{G}|$表示群 $\boldsymbol{G}$ 中元素的长度，$|\boldsymbol{G}_T|$表示群 $\boldsymbol{G}_T$ 中元素的长度，d 是基本 ABE[1]的门限值。$|S|$表示满足树状访问结构的最小中间节点个数，或 LSSS 中访问结构的最小属性个数。ABOOE-Ⅰ和 ABOOE-Ⅱ分别表示本文提出的第一个和第二个 ABOOE 方案。

本文的 ABOOE 方案成功地将 KP-ABE 的加密过程分解成离线加密和在线加密，使得在线加密只需少量的 Z_p 中模运算即可生成密文。由于 Z_p 中的模运算比群 $\boldsymbol{G}$ 或 $\boldsymbol{G}_T$ 中的幂乘运算快很多倍，这对于计算能力受限的轻量级设备是至关重要的。此外，解密过程的运算量没有过多额外的增加。虽然本文的 ABOOE 方案需要预存一定量的离线密文，而且密文长度也有所增加，但现有轻量级设备的存储能力足以满足这种需求，因此，ABOOE 方案特别适合于轻量级设备收集敏感数据。本文 ABOOE 方案是在随机预言机模型下可证明安全的，理论上讲，随机模型下的加密方案不如标准模型下加密方案的安全性高，但此类方案的安全性仍然是可以接受的。特别在效率要求严格的场景中，随机模型下高效的加密方案将是一个更好的选择。

6　结束语

本文首先提出 ABOOE 机制，设计出一个 CPA 安全的具体方案。然后给出 ABOOKEM 机制，提出一种将单向性 ABOOKEM 转化成 CCA 安全 ABOOE 的通用性方法。该方法在不增加计算量的情况下有效地提高了 ABOOE 的安全性。本文 CCA 安全的 ABOOE 方案就是该构造方法的一个具体实例。文中 2 个 ABOOE 方案的优势在于：1）在线加密阶段效率极高；2）离线加密阶段可在不知道消息和属性集合的前提下执行。ABOOE 方案特别适用于轻量级计算设备。此外，ABOOKEM 可以用来设计安全的通信协议，可能具有独立的应用价值。

参考文献：

[1] SAHAI A, WATERS B. Fuzzy identity based encryption[A]. Proc of the EUROCRYPT[C]. Aarhus, Denmark, 2005. 457-473.

[2] GOYAL V, PANDEY O, SAHAI A, *et al*. Attribute-based encryption for fine-grained access control of encrypted data[A]. Proc of the 13th ACM Conference on Computer and Communication Security[C]. Alexandria, Virginia, USA, 2006. 89-98.

[3] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[A]. Proc of the 2007 IEEE Symposium on Security and Privacy[C]. Oakland, California, USA, 2007. 321-334.

[4] ATTRAPADUNG N, IMAI H. Dual-Policy attribute based encryption[A]. Applied Cryptography and Network Security[C]. Paris, France, 2009. 168-185.

[5] CHEUNG L, NEWPORT C. Provably secure ciphertext policy ABE[A]. Computer and Communications Security[C]. New York, USA, 2007. 456-465.

[6] OKAMOTO T, SAHAI A, WATERS B. Attribute-based encryption with non-monotonic access structures[A]. Proc of the 14th ACM Conference on Computer and Communication Security[C]. New York, USA, 2007. 195-203.

[7] 王鹏翩, 冯登国, 张立武. 一种支持完全细粒度属性撤销的 CP-ABE 方案[J]. 软件学报, 2012,23(10): 2805-2816.
WANG P P, FENG D G, ZHANG L W. CP-ABE scheme supporting fully fine-grained attribute revocation[J]. Chinese Journal of Software, 2012, 23(10): 2805-2816.

[8] ATTRAPADUNG N, IMAI H, Conjunctive broadcast and attribute-based encryption[A]. Proc of the Pairing-Based Cyptography-Pairing 2009[C]. Palo Alto, USA, 2009.248-265.

[9] 马海英, 曾国荪. 可追踪并撤销叛徒的属性基加密方案[J]. 计算机学报, 2012, 35(9):1845-1855.
MA H Y, ZENG G S. An attribute-based encryption scheme for traitor tracing and revocation together[J]. Chinese Journal of Computers, 2012, 35(9):1845-1855.

[10] WANG Y T, CHEN K F, CHEN J H. Attribute-based traitor tracing[J]. Journal of Information Science and Engineering, 2011, 27(1):181-195.

[11] YU S C, REN K, LOU W J, LI J. Defending against key abuse attacks in KP-ABE enabled broadcast system[A]. Pro of the Security and Privacy in Communication Networks[C]. Athens, Greece, 2009. 311-329.

[12] LI J, REN K, ZHU B, *et al*. Privacy-aware attribute-based encryption with user accountability[J]. Information Security, 2009, 5735:347-362.

[13] WANG Y T, CHEN K F, LONG Y. Toward accountable authority attribute-based encryption[J]. High Technology Letters, 2013, 19(1): 82-87.

[14] BOZOVIC V, SOCEK D, STEINWANDT R, *et al*. Multi-authority attribute based encryption with honest-but-curious central authority[J]. International Journal of Computer mathematics, 2012, 89(1/3):268-283.

[15] LEWKO A, WATERS B. Decentralizing attribute-based encryption[EB/OL]. http://eprint.iacr.org/2010 /351, 2010.

[16] LIN H, CAO Z F, LIANG X H, *et al*. Secure threshold multi-authority attribute based encryption without a central authority[J]. Progress in Cryptology INDOCRYPT, 2008, 5365: 426-436.

[17] YU S S, REN K, LOU W J. FDAC: toward fine-grained distributed data access control in wireless sensor networks[A]. IEEE INFOCOM 2009[C]. Rio de Janeiro, Brazil, 2009.963-971.

[18] 洪澄，张敏，冯登国. 面向云存储的高效动态密文访问控制方法[J]. 通信学报, 2011, 32(7): 125-132.
HONG C, ZHANG M, FENG D G. Achieving efficient dynamic cryptographic access control in cloud storage[J]. Chinese Journal of Communications, 2011, 32(7): 125-132.

[19] HUR J. Fine-grained data access control for distributed sensor networks[J]. Wireless Network, 2011, 17(4): 1235-1249.

[20] 祁正华，杨庚，任勋益，王卉. 基于 ABE-IBS 的无线传感网签名加密一体化方法[J]. 通信学报, 2010, 31(4):37-44.
QI Z H, YANG G, REN X Y, *et al.* ABE-IBS based signature- encryption method for WSN[J]. Journal on Communications, 2010, 31(4): 37-44.

[21] EVEN S, GOLDREICH O, MACALI S. Online/offline digital signatures[A]. Proc of Advances in Cryptology[C]. Santa Barbara, California, USA, 1989. 263-275.

[22] GUO F C , MU Y ,CHEN Z D. Identity-based online/offline encryption[A]. Proc of Financial Cryptography and Data Security 2008[C]. Cozumel, Mexico, 2008. 247-261.

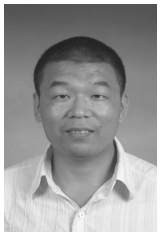
[23] CHOW S SM, LIU J K, ZHOU J Y. Identity-based online/offline key encapsulation and encryption[A]. Proc of ASIACCS'11[C]. Hong Kong, China, 2011. 52-60.

[24] SAKAI R, KASAHARA M. ID based cryptosystems with pairing on elliptic curve[EB/OL]. http://eprint.iacr.org/2003/54, 2003.

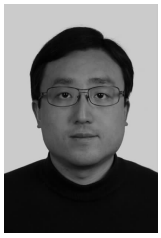
作者简介：

马海英（1977-），女，河南卫辉人，同济大学博士生，南通大学讲师，主要研究方向为公钥密码学和网络安全。

曾国荪（1964-），男，江西吉安人，博士，同济大学教授、博士生导师，主要研究方向为网格计算、可信软件。



王占君（1978-），男，河南鹤壁人，硕士，南通大学讲师，主要研究方向为公钥密码学和 Hopf 代数。



王伟（1979-），男，湖北武汉人，博士，同济大学副教授，主要研究方向为可信计算和信息安全。