# 双重系统加密研究：获得完全安全的IBE及其扩展*

罗 颂[1,2]，陈 宇[1,3]，陈 钟[1]

（1. 北京大学 信息科学技术学院，北京 100871；
2. 重庆理工大学 计算机科学与工程学院，重庆 400054；
3. 中国科学院 信息工程所，北京 100190）

**摘 要**：双重系统加密技术首先由Waters提出，是用于构造完全安全的基于身份的加密（IBE）及其扩展方案的有力方法。针对完全安全方案的构造，研究了双重系统加密技术并提出了一个完全安全方案的通用构造方法，即将一个利用双重系统加密的IBE方案与一个普通的方案相结合，得到一个新的可以利用双重系统加密证明安全的方案。在通用构造的基础上提出了一个实例，该实例是一个基于层级身份的加密（HIBE）方案，具有常密文长度。该方案比Waters提出的双重系统加密HIBE方案更高效，并且在判定BDH假设和判定线性假设下证明是完全安全的。

**关键词**：双重系统加密；基于身份的加密；完全安全

**中图分类号**：TP309 **文献标志码**：A **文章编号**：1001-2486(2012)02-0006-04

# Dual system encryption revisited: attaining fully secure identity-based encryption and its extensions

*LUO Song*[1,2], *CHEN Yu*[1,3], *CHEN Zhong*[1]

（1. School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China;
2. College of Computer Science and Engineering, Chongqing University of Technology, Chongqing 400054, China;
3. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100190, China）

**Abstract**: Dual system encryption was first proposed by Waters as a powerful method to prove full security for identity-based encryption (IBE) schemes and its extensions. To construct fully secure schemes, the application of dual system encryption is considered and a generic construction of fully secure schemes is presented. The construction combines a dual system encryption IBE scheme with a normal secure scheme and produces a new scheme which can be proven secure by dual system encryption. Based on the proposed generic construction, an instantiation, which is a hierarchical identity-based encryption (HIBE) scheme with constant ciphertext size, is presented. This scheme is more efficient than Waters' original dual system encryption HIBE scheme, and it is proven fully secure under the Decision BDH and Decision Linear assumptions.

**Key words**: dual system encryption; identity-based encryption; full security

基于身份的加密（Identity-Based Encryption，IBE）是由Shamir[1]于1984年提出的一种公钥加密系统，其目的在于简化公钥管理设施。在IBE中，用户的公钥可以由任意字符串计算得到，如用户的IP地址、电子邮件等，从而避免了管理公钥证书带来的开销。第一个实用的IBE方案由Boneh和Franklin[2]在具有可有效计算的双线性对的群上构造，另一个基于二次剩余的IBE方案由Cocks[3]提出，但该方案在效率上不如前者。

双重系统加密（Dual System Encryption）是由Waters[4]提出的一种方法，可以用来构造完全安全（或称自适应安全）的IBE方案及其扩展方案，如基于层级身份的加密（Hierarchical Identity-Based Encryption，HIBE）或基于属性的加密（Attribute-Based Encryption，ABE）等。通过双重系统加密，可以在安全性证明中为所有的密钥查询生成密钥，这种内在的特性非常适合用于证明IBE或者HIBE方案的完全安全性。特别地，当前所有利用双重系统加密构造的IBE或HIBE方案都在标准模型上基于简单静态假设证明了完全安全性[4-7]。最近，双重系统加密还用于构造抗泄露攻击的密码系统[8]。

目前对双重系统加密有两个显著的改进。一个改进由Lewko和Waters[5]提出，他们给出了一

* **收稿日期**：2011-07-28
**基金项目**：国家自然科学基金项目（61073156，61170263）
**作者简介**：罗颂（1979—），男，福建上杭人，讲师，博士，E-mail：luosong@infosec.pku.edu.cn；
陈钟（通信作者），男，教授，博士，博士生导师，E-mail：chen@infosec.pku.edu.cn

个近乎完美的 IBE 方案,该方案具有自然的表现形式,同时移除了 Waters 的原始方案中可忽略的解密错误,即半功能密钥无法解密对应的半功能密文的问题。为了达到这一点,他们引入了半功能密钥的一种变体,称为象征性半功能密钥。它具有半功能密钥的表现形式,但能够解密特定的半功能密文。Lewko 和 Waters 提出的新方案在合数阶群上构造,利用了一些不同阶子群之间元素的消去性。这种方法同样可用于基于属性的加密和功能加密来证明安全性。

另外一个改进由 Okamoto 和 Takashima[10] 提出。他们将双重系统加密和双重配对向量空间(Dual Pairing Vector Space, DPVS)相结合,后一概念也是由他们提出的[11]。DPVS 是比本原群更高层次的概念,Okamoto 和 Takashima 利用层级的方式,在顶层假设中将 DPVS 和判定线性假设联系起来,同时构造了若干层级的假设。

本文继续研究双重系统加密的应用。基于双重系统加密,我们提出了一种完全安全方案的通用构造方法。通过将一个利用双重系统加密构造的方案和一个普通的方案相结合,我们得到一个新的方案。新方案与原方案类似,但能够在简单假设下证明自适应安全性。

在通用构造的基础上,我们给出了一个实例。该实例为 HIBE 方案,具有常密文长度,与 Waters 基于双重系统加密的 HIBE 方案相比,更为高效。同时,该 HIBE 方案在标准模型上基于判定 BDH 假设和判定线性假设证明是完全安全的。

## 1　背景

**定义 1**　令$\mathbb{G}$,$\mathbb{G}_1$为 $p$ 阶的乘法循环群,$p$ 是素数。$g$ 是$\mathbb{G}$的一个生成元,$e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_1$是一个双线性映射,具有如下性质:

(1)双线性性:对于任意的 $u$, $v\in\mathbb{G}$ 和 $a$, $b\in\mathbb{Z}$,有 $e(u^a, v^b)=e(u, v)^{ab}$。

(2)非退化性:$e(g, g)\neq 1$。注意到$\mathbb{G}_1$是素数阶群,这意味着 $e(g, g)$是$\mathbb{G}_1$的生成元。

如果$\mathbb{G}$中的运算及双线性映射 $e$ 都是多项式时间可计算的,我们称$\mathbb{G}$是一个双线性群,$e$ 是一个双线性对。

我们假定有一个有效的算法$\mathcal{G}$来生成双线性群。该算法以安全参数 $\lambda$ 为输入,输出一个四元组 $G=[p, \mathbb{G}, \mathbb{G}_1, g\in\mathbb{G}, e]$,其中 $g$ 是$\mathbb{G}$的一个生成元,$\log_2 p=\Theta(\lambda)$。

**定义 2**　令 $c_1$, $c_2$, $c_3\in\mathbb{Z}_p^*$ 是随机选择的整数,$g$ 是$\mathbb{G}$的一个生成元。判定 BDH 假设指没有概率性的多项式时间算法能够以不可忽略的优势分辨元组$[g, g^{c_1}, g^{c_2}, g^{c_3}, e(g, g)^{c_1c_2c_3}]$和元组$[g, g^{c_1}, g^{c_2}, g^{c_3}, T]$,这里 $T$ 是$\mathbb{G}_1$中的一个随机元素。

**定义 3**　令 $c_1$, $c_2\in\mathbb{Z}_p^*$ 是随机选择的整数,$g, f, v$ 是$\mathbb{G}$中的随机元素。判定线性假设指没有概率性的多项式时间算法能够以不可忽略的优势分辨元组$[g, f, v, g^{c_1}, f^{c_2}, v^{c_1+c_2}]$和元组$[g, f, v, g^{c_1}, f^{c_2}, T]$,这里 $T$ 是$\mathbb{G}$中的一个随机元素。

使用双重系统加密构造的 HIBE 方案(或称为双重系统加密 HIBE 方案)包括 5 个常规算法 Setup、KeyGen、Derive、Encrypt 和 Decrypt,以及两个额外算法 KeyGenSF 和 EncryptSF 用于生成半功能密钥和半功能密文。由于篇幅限制,这里略去这些算法的正式定义,它们都可以在文献[12]中找到。

双重系统加密 HIBE 方案使用混合争论(hybrid argument)的方法,通过一系列游戏的两两不可区分性来证明系统的安全性。这些游戏简述如下,正式的定义可以在文献[12]中找到。

**Game**$_{Real}$:此游戏为普通的 IND-ID-CPA 游戏,所有的密钥查询返回的都是正常密钥,挑战密文为正常密文。

**Game**$_i$:此游戏与 **Game**$_{Real}$相似,区别在于挑战密文为半功能密文,而前 $i$ 次密钥查询返回的是半功能密钥,剩下的查询返回正常密文。

**Game**$_{Final}$:此游戏中所有的密钥都是半功能的,挑战密文则是对一个随机消息加密得到的一个半功能密文。

## 2　通用构造

令 $e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_1$为双线性对,消息 $M$ 是$\mathbb{G}_1$中的元素。我们来给出完全安全的 IBE 及其扩展方案如 HIBE 的通用构造。构造的主要思路是将一个使用双重系统加密的完全安全的 IBE 方案($\varepsilon_1$)和一个普通的(完全安全或者选择安全)IBE、HIBE 或其他方案($\varepsilon_2$)结合起来。为表述清楚,我们先给出 $\varepsilon_1$ 和 $\varepsilon_2$ 的简要描述。

假设 $\varepsilon_1$ 构造如下:

**Setup.** 该算法输出公钥 $PK_1$ 和主密钥 $MK_1$。

**KeyGen**($PK$, $MK$, $ID$). 给定身份 $ID$,该算法输出对应的密钥 $SK_{ID}=(d_1, d_2, \cdots, d_k)\in\mathbb{G}^k$。

**KeyGenSF**($PK$, $MK$, $ID$). 给定身份 $ID$,该算法输出对应的半功能密钥$\widetilde{SK}_{ID}=(d'_1, d'_2, \cdots, d'_k)\in\mathbb{G}^k$。

**Encrypt**($PK$, $M$, $ID$). 给定要加密的消息 $M$ 和身份 $ID$, 该算法输出对应的密文 $CT=(C, C_1, C_2, \cdots, C_k)\in\mathbb{G}_1\times\mathbb{G}^k$。

**EncryptSF**($PK$, $M$, $ID$). 给定要加密的消息 $M$ 和身份 $ID$, 该算法输出对应的半功能密文 $\widehat{CT}=(C', C'_1, C'_2, \cdots, C'_k)\in\mathbb{G}_1\times\mathbb{G}^k$。

**Decrypt**($CT$, $SK_{ID}$).

$M=C\cdot e(d_1,C_1)\cdot e(d_2,C_2)\cdots e(d_k,C_k)$。

假设 $\varepsilon_2$ 构造如下,注意我们并不知道方案 $\varepsilon_2$ 的类型(IBE、HIBE 或其他), 因此忽略了 $\varepsilon_2$ 每个算法的具体参数。此外, 我们还假定消息 $M$ 被随机化为 $M\cdot Y$, 这里 $Y\in\mathbb{G}_1$是会话密钥。

**Setup.** 该算法输出公钥 $PK_2$ 和主密钥 $MK_2$。

**KeyGen.** 该算法输出对应的密钥 $SK=(E_1, E_2, \cdots, E_m)\in\mathbb{G}^m$。

**Encrypt.** 给定要加密的消息 $M$, 该算法输出对应的密文 $CT=(\tilde{C}=M\cdot Y, F_1, F_2, \cdots, F_m)\in\mathbb{G}_1\times\mathbb{G}^m$。

**Decrypt.**

$M=\tilde{C}\cdot e(E_1,F_1)\cdot e(E_2,F_2)\cdots e(E_m,F_m)$。

根据双重系统加密的性质, 我们可以将方案 $\varepsilon_1$输出的一个正常密钥转换为半功能密钥。如果其中某个元素, 不妨设为 $d_k$, 在转换前后都保持不变, 我们就可以构造一个新的方案 $\varepsilon$, 它与方案 $\varepsilon_2$ 相似, 但具有完全安全性。此外,$\varepsilon$ 可以和 $\varepsilon_1$ 在相同的假设下得到证明。注意到在方案 $\varepsilon_2$ 中, 我们假定消息 $M$ 被随机化为 $M\cdot Y$, 设 $Y=e(d_k,Y_2)$, 这里 $Y_2\in\mathbb{G}$ 是随机元素。结合 $\varepsilon_1$ 和 $\varepsilon_2$ 后得到的新方案 $\varepsilon$ 构造如下:

**Setup.** 该算法输出公钥 $PK_1\cup PK_2$ 和主密钥 $MK_1\cup MK_2$。

**KeyGen.** 该算法输出对应的密钥 $SK=(d_1, d_2, \cdots, d_k, E_1, E_2, \cdots, E_m)$。

**KeyGenSF.** 该算法输出对应的半功能密钥 $\widehat{SK}=(d'_1, d'_2, \cdots, d'_k, E_1, E_2, \cdots, E_m)$。

**Encrypt.** 给定要加密的消息 $M$, 该算法输出对应的密文 $CT=(C, C_1, C_2, \cdots, C_k\cdot Y_2, F_1, F_2, \cdots, F_m)$。

**EncryptSF.** 给定要加密的消息 $M$, 该算法输出对应的半功能密文$\widehat{CT}=(C', C'_1, C'_2, \cdots, C'_k\cdot Y_2, F_1, F_2, \cdots, F_m)$。

**Decrypt.**

$$M=C\cdot e(d_1,C_1)\cdot e(d_2,C_2)\cdots e(d_k,C_k)\cdot e(E_1,F_1)\cdot e(E_2,F_2)\cdots e(E_m,F_m)。$$

很容易验证新方案的正确性。实际上, 我们给出的通用构造对 IBE 方案来说具有冗余, 但我们可以修正构造的方案得到一个更有效的方案。在下节中将给出具体实例——一个比 Waters[4] 构造的双重系统加密 HIBE 方案更高效的 HIBE 方案。

## 3　基于层级身份的加密

令 $\varepsilon_1$ 为 Waters[4] 的双重系统加密 IBE 方案, $\varepsilon_2$ 为 Boneh 等[13] 的 HIBE 方案(又称 BBG-HIBE 方案)。BBG-HIBE 方案是一个具有常密文长度的 HIBE 方案, 但它只有选择安全性, 且基于一个动态假设——$q$-BDHE 假设。我们利用上节的构造方法, 结合这两个方案构造出一个新的完全安全的 HIBE 方案, 同样具有常密文长度。此外, 我们去除了新方案中的冗余, 因此要比通用构造更为简洁高效。新方案构造如下:

**Setup**($1^\lambda$, $\ell$). 给定安全参数 $\lambda$ 和最大层级数 $\ell$, 该算法首先运行$\mathcal{G}(\lambda)$得到$[p,\mathbb{G},\mathbb{G}_1, g\in\mathbb{G}, e]$。接着随机选取 $v, v_1, v_2, w, u_1, \cdots, u_\ell, h\in\mathbb{G}$ 及整数 $a_1, a_2, b, \alpha\in\mathbb{Z}_p$。然后算法设置 $\tau_1=vv_1^{a_1}$, $\tau_2=vv_2^{a_2}$, $Y=e(g,g)^{\alpha\cdot a_1\cdot b}$。

最后算法发布公钥 $PK=(Y, g, g^b, g^{a_1}, g^{a_2}, g^{b\cdot a_1}, g^{b\cdot a_2}, \tau_1, \tau_2, \tau_1^b, \tau_2^b, v, v_1, v_2, w, u_1, \cdots, u_\ell, h)$, 主密钥 $MK=(g^\alpha, g^{\alpha\cdot a_1})$。身份空间为$\mathbb{Z}_p^*$。

**KeyGen**($PK$, $MK$, $ID$). 给定身份向量 $ID=(I_1, I_2, \cdots, I_n)\in(\mathbb{Z}_p^*)^n$, 为生成对应的密钥, 该算法随机选取 $r_1, r_2, z_1, z_2, \mathrm{tag}_k\in\mathbb{Z}_p$并计算 $D_1=g^{\alpha\cdot a_1}v^{r_1+r_2}$, $D_2=g^{-\alpha}v_1^{r_1+r_2}g^{z_1}$, $D_3=(g^b)^{-z_1}$, $D_4=v_2^{r_1+r_2}g^{z_2}$, $D_5=(g^b)^{-z_2}$, $D_6=(g^b)^{r_2}$, $D_7=g^{r_1}$, $K=(u_1^{I_1}\cdots u_n^{I_n}w^{\mathrm{tag}_k}h)^{r_1}$, $K_{n+1}=(u_{n+1})^{r_1}$, $\cdots$, $K_\ell=(u_\ell)^{r_1}$。生成的密钥为 $SK_{ID}=(D_1, D_2, \cdots, D_7, K, \mathrm{tag}_k, K_{n+1}, \cdots, K_\ell)$。

**KeyGenSF**($PK$, $MK$, $ID$). 给定身份向量 $ID=(I_1, I_2, \cdots, I_n)$, 该算法随机选取 $r_1, r_2, z_1, z_2, \mathrm{tag}_k\in\mathbb{Z}_p$并计算 $D_1=g^{\alpha\cdot a_1}v^{r_1+r_2}g^{-a_1a_2\gamma}$, $D_2=g^{-\alpha}v_1^{r_1+r_2}g^{z_1}g^{a_2\gamma}$, $D_3=(g^b)^{-z_1}$, $D_4=v_2^{r_1+r_2}g^{z_2}g^{a_1\gamma}$, $D_5=(g^b)^{-z_2}$, $D_6=(g^b)^{r_2}$, $D_7=g^{r_1}$, $K=(u_1^{I_1}\cdots u_n^{I_n}w^{\mathrm{tag}_k}h)^{r_1}$, $K_{n+1}=(u_{n+1})^{r_1}$, $\cdots$, $K_\ell=(u_\ell)^{r_1}$。半功能密钥为 $(D_1, D_2, \cdots, D_7, K, \mathrm{tag}_k, K_{n+1}, \cdots, K_\ell)$。

**Derive**($PK$, $SK_{ID_{|n}}$, $ID_{|n+1}$). 给定 $n$ 层身份向量 $ID_{|n}=(I_1, I_2, \cdots, I_n)$ 及对应的密钥 $SK_{\mathrm{ID}_{|n}}=(D'_1, D'_2, \cdots, D'_7, K', \mathrm{tag}_k, K'_{n+1}, \cdots, K'_\ell)$, 该算法为 $n+1$ 层身份向量 $ID_{|n+1}=(I_1, I_2, \cdots, I_n, I_{n+1})$,生成密钥如下。首先随机选取 $r_1, r_2, z_1,$

$z_2$, $z \in G_p$ 并计算 $D_1 = D'_1 \cdot v^{r_1+r_2}$, $D_2 = D'_2 \cdot v_1^{r_1+r_2} g^{z_1}$, $D_3 = D'_3 \cdot (g^b)^{-z_1}$, $D_4 = D'_4 \cdot v_2^{r_1+r_2} g^{z_2}$, $D_5 = D'_5 \cdot (g^b)^{-z_2}$, $D_6 = D'_6 \cdot (g^b)^{r_2}$, $D_7 = D'_7 \cdot g^{r_1}$, $K = K' \cdot (u_1^{I_1} \cdots u_{n+1}^{I_{n+1}} w^{\mathrm{tag}_k} h)^{r_1} K_{n+1}^{I_{n+1}}$, $K_{n+2} = K'_{n+2} \cdot (u_{n+1})^{r_1}$, …, $K_\ell = K'_\ell \cdot (u_\ell)^{r_1}$。生成的密钥为 $SK_{ID_{|n+1}} = (D_1, D_2, \cdots, D_7, K, \mathrm{tag}_k, K_{n+2}, \cdots, K_\ell)$。

**Encrypt**($PK$, $M$, $ID$). 给定要加密的消息 $M$ 和身份向量 $ID = (I_1, I_2, \cdots, I_n)$, 该算法随机选取 $s_1$, $s_2$, $t$, $\mathrm{tag}_c \in \mathbb{Z}_p$ 并计算 $C_0 = MY^{s_2}$, $C_1 = (g^b)^{s_1+s_2}$, $C_2 = (g^{b \cdot a_1})^{s_1}$, $C_3 = (g^{a_1})^{s_1}$, $C_4 = (g^{b \cdot a_2})^{s_2}$, $C_5 = (g^{a_2})^{s_2}$, $C_6 = \tau_1^{s_1} \tau_2^{s_2}$, $C_7 = (\tau_1^b)^{s_1} (\tau_2^b)^{s_2} w^{-t}$, $E_1 = (u_1^{I_1} \cdots u_n^{I_n} w^{\mathrm{tag}_c} h)^t$, $E_2 = g^t$。对应的密文为 $CT = (C_0, C_1, \cdots, C_7, E_1, E_2, \mathrm{tag}_c)$。

**EncryptSF**($PK$, $M$, $ID$). 半功能密文可以如下生成。首先该算法运行加密算法, 为消息 $M$ 和身份向量 $ID$ 生成正常密文 $C'_0, C'_1, \cdots, C'_7, E'_1, E'_2$, $\mathrm{tag}_c$。然后随机选取 $x \in \mathbb{Z}_p$ 并令 $C_0 = C'_0$, $C_1 = C'_1$, $C_2 = C'_2$, $C_3 = C'_3$, $E_1 = E'_1$, $E_2 = E'_2$。接着设置 $C_4 = C'_4 \cdot g^{ba_2x}$, $C_5 = C'_5 \cdot g^{a_2x}$, $C_6 = C'_6 \cdot v_2^{a_2x}$, $C_7 = C'_7 \cdot v_2^{ba_2x}$。对应的半功能密文为 $(C_0, C_1, \cdots, C_7, E_1, E_2, \mathrm{tag}_c)$。

**Decrypt**($SK_{ID}$, $CT$). 给定为身份向量 $ID$ 加密的密文 $CT = (C_0, C_1, \cdots, C_7, E_1, E_2, \mathrm{tag}_c)$, 设对应的密钥为 $SK_{ID} = (D_1, D_2, \cdots, D_7, K, \mathrm{tag}_k, K_{n+1}, \cdots, K_\ell)$, 解密密文步骤如下:

(1) $A_1 = e(C_1, D_1) \cdot e(C_2, D_2) \cdot e(C_3, D_3) \cdot e(C_4, D_4) \cdot e(C_5, D_5)$;

(2) $A_2 = e(C_6, D_6) \cdot e(C_7, D_7)$;

(3) $A_3 = A_1 / A_2$;

(4) $A_4 = (e(E_1, D_7) / e(E_2, K))^{1/(\mathrm{tag}_c - \mathrm{tag}_k)}$;

(5) $M = C_0 / (A_1 / A_2)$。

容易验证解密过程的正确性。注意到我们给出的方案具有常密文长度, 因此它比 Waters 提出的双重系统加密 HIBE 方案更高效, 因为后者的密文长度是随着身份向量的层数增加而增加的。

对于提出的 HIBE 方案, 我们有如下结论:

**定理**　如果判定线性假设和判定 BDH 假设成立, 提出的 HIBE 方案是完全安全的。

定理的证明使用了 Waters 的双重系统加密 IBE 的证明路线。首先证明游戏 $\mathbf{Game}_{Real}$ 和游戏 $\mathbf{Game}_0$ 在判定线性假设下是不可区分的, 然后再证明对 $0 \leqslant k < q$, 游戏 $\mathbf{Game}_k$ 和游戏 $\mathbf{Game}_{k+1}$ 在判定线性假设下是不可区分的, 最后证明游戏 $\mathbf{Game}_q$ 和游戏 $\mathbf{Game}_{Final}$ 在判定 BDH 假设下是不可区分的。从这些游戏的不可区分性,我们就得到了定理的证明。限于篇幅, 我们省略了具体的证明过程。

## 4　结　论

本文研究了双重系统加密技术的应用。通过结合一个双重系统加密 IBE 方案和普通的方案, 给出了一个完全安全方案的通用构造方法。所构造的 HIBE 实例表明其在判定线性假设和判定 BDH 假设下是完全安全的。该 HIBE 方案同时还具有常密文长度, 比 Waters 构造的双重系统加密 HIBE 方案更为高效。

## 参考文献(References)


[1] Shamir A. Identity-based cryptosystems and signatures schemes [C]// Proc of CRYPTO 1984, LNCS 196: 47 – 53.

[2] Boneh D, Franklin M. Identity-based encryption from the weil pairing [C]// Proc of CRYPTO 2001, LNCS 2139: 213 – 229.

[3] Cocks C. An identity based encryption scheme based on quadratic residues[C]// Proc of IMACC 2001, LNCS 2260: 360 – 363.

[4] Waters B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions [C]// Proc of CRYPTO 2009, LNCS 5677: 619 – 636.

[5] Lewko A, Waters B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts[C]// Proc of TCC 2010, LNCS 5978: 455 – 479.

[6] Caro A D, Iovino V, Persiano G. Fully secure anonymous HIBE and secret-key anonymous IBE with short ciphertexts [EB/OL]. Cryptology ePrint Archive, Report 2010/197, 2010. http://eprint. iacr. org.

[7] Seo J H, Cheon J H. Fully secure anonymous hierarchical identity-based encryption with constant size ciphertexts [EB/OL]. Cryptology ePrint Archive, Report 2011/021, 2011. http://eprint. iacr. org.

[8] Chow S S M, Dodis Y, Rouselakis Y, et al. Practical leakage-resilient identity-based encryption from simple Assumptions [C]// Proc of ACM-CCS 2010: 152 – 161.

[9] Lewko A, Okamoto T, Sahai A, et al. Fully secure functional encryption: attribute-based encryption and hierarchical inner product encryption[C]// Proc of EUROCRYPT 2010, LNCS 6110: 62 – 91.

[10] Okamoto T, Takashima K. Fully secure functional encryption with general relations from the decisional linear assumption [C]// Proc of CRYPTO 2010, LNCS 6223: 191 – 208.

[11] Okamoto T, Takashima K. Hierarchical predicate encryption for inner-products[C]// Proc of ASIACRYPT 2009, LNCS 5912:214 – 231.

[12] Waters B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions[R]. Cryptology ePrint Archive, Report 2009/385, 2009.

[13] Boneh D, Boyen X, Goh E J. Hierarchical identity based encryption with constant size ciphertext [C]// Proc of EUROCRYPT 2005, LNCS 3494: 440 – 456.