一种可信安全的层次式基于身份加密系统

王小峰,陈培鑫,周 寰,苏金树
(国防科学技术大学计算机学院,湖南长沙 410073)

摘 要: 本文提出一种可信安全的层次式基于身份加密系统T-HIBE,通过层次式分布化的用户私钥产生,以及私钥用户盲因子、用户私钥编号因子和PKG私钥编号因子技术,解决了层次式私钥生成机构的密钥托管和私钥安全传输问题,支持系统高效的用户身份一次认证和可追责性.基于标准的BDH难题假设,文章证明了基本T-HIBE机制和完全T-HIBE机制分别具有IND-sID-OWE和IND-sID-CCA安全性.

关键词: 层次化基于身份加密;密钥托管;密钥安全传输;认证可追责;抗串谋
中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112 (2016)07-1521-09
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.07.001

A Trustworthy and Secure Hierarchical Identity-Based Encryption System

WANG Xiao-feng, CHEN Pei-xin, ZHOU Huan, SU Jin-shu
(*College of Computer, National University of Defense Technology, Changsha, Hunan* 410073, *China*)

Abstract: The paper proposes a trustworthy and secure HIBE (hierarchical identity-based encryption) system named T-HIBE. It generates private keys in a hierarchical and distributed manner. By using the user blinding index, user private key index and PKG private key index, T-HIBE can achieve the trustworthy private key generation and secure private key distribution. Moreover, the T-HIBE system needs one single user authentication whose accountability is traceable. Based on the standard BDH assumption, we prove that the basic T-HIBE and full T-HIBE have the IND-sID-OWE and IND-sID-CCA security respectively.

Key words: HIBE; key escrow; secure key transmission; accountable authentication; collusion resistant

1 引言

针对传统非对称加密机制的公钥随机化问题,Shamir[1]提出基于身份的加密机制(IBE,Identity Based Encryption).通过将用户的身份信息(如姓名、邮件、IP地址等)直接作为用户的公钥,无需通过数字证书绑定用户身份和公钥,从而避免了管理公钥证书带来的开销.Boneh[2]基于双线性对映射,提出了第一个实用的IBE方案.进一步Horwitz和Gentry等人提出层次化的HIBE(Hierarchical IBE)方案,通过高层级用户为低层级子孙用户生成私钥,有效解决了IBE中私钥生成机构PKG(Private Key Generator)负载过重,规模扩展受限等问题.

由于用户私钥由私钥生成机构PKG生成,(H)IBE机制在具体应用时必须面对以下三个问题:

(1)PKG的可信问题,即密钥托管问题,PKG生成并保存用户的私钥信息,可能破坏用户私钥的保密性.

(2)密钥传输问题,用户必须采用安全信道从PKG获取私钥,增加了系统的部署代价.

(3)密码系统的效率和身份认证可追责问题,为解决PKG可信问题,现有解决方案大多提出分布式PKG方式,但如果多个PKG各自认证用户,将大大增加系统开销;如果采用单个PKG认证共享方案,则可能存在单个PKG虚假身份认证导致非法用户私钥获取的可能性.

针对以上三个问题,目前的研究主要集中在IBE领域,而HIBE密码系统缺少针对PKG密钥托管、密钥安全传输、身份认证效率和可追责问题的系统解决方案.

本文提出一种可信安全的层次式基于身份加密系统T-HIBE(Trustworthy HIBE),它既能解决系统的密钥

收稿日期:2015-01-13;修回日期:2015-03-25;责任编辑:孙瑶
基金项目:国家自然科学基金(No.61103194,No.61202119);国家863高技术研究发展计划(No.2011AA01A103)

托管和私钥安全传输问题,支持高效的用户身份一次认证和可追责性,又能实现 IND-sID-CCA(不可区分选择身份-选择密文攻击)安全的抗串谋 HIBE 机制. 论文具体贡献如下:

(1)提出分布式基本 T-HIBE 机制,通过层次式 PKG 和多个 KPA(Key Privacy Authority)共同为用户产生私钥,解决了层次式 PKG 的密钥托管问题.

(2)基于简单的 BDH 和 DL 难题假设,使用 Fujisaki-Okamoto 填充技术,实现了 IND-sID-CCA 安全的完全 T-HIBE 机制.

(3)设计了高效的 T-HIBE 安全机制,增加私钥用户盲因子,使得只有掌握秘密值的合法用户才能得到私钥,无需私钥传输安全信道;采用 PKG 一次认证,多个 KPA 检查 PKG 签名,避免了多个机构认证用户身份的开销;通过用户私钥编号因子和 PKG 私钥编号因子共同组成用户私钥编号,实现了 PKG 用户身份认证和密钥产生的可追责.

2 相关研究

密钥托管问题是(H)IBE 系统的固有问题,解决方法可分为两类:用户选择秘密值方法[3,4]和分布式方法[5~8]. 用户选择秘密值方法是用户在申请私钥前选择秘密值用于修改 PKG 颁发的私钥,使得 PKG 不知道用户实际使用的私钥,但该方法牺牲了 IBE 将用户身份作为公钥的优势. 分布式方法将系统对单个机构的信任分散到多个机构,防止单个机构解密用户密文或泄漏用户私钥. Boneh[2]最先采取(t,n)门限思想缓解 IBE 中的密钥托管问题,可抵抗 t 个 PKG 的串谋攻击. Kate[5]实现了利用秘密共享机制的分布式 PKG,为 Internet 上的用户实现分布式私钥生成. 上述分布式方法中,系统中每个机构独立检验用户身份,且需通过安全信道传输密钥部件,增加了系统的通信和计算开销. Lee 等人提出串行的分布式结构[8],用户私钥由 PKG 颁发并由多个 KPA 顺序地加固密钥隐私,解决了密钥托管问题,同时降低了系统的用户身份验证开销. 但是该方法无法保证 PKG 验证用户身份的真实性. 文献[9]基于遮蔽技术,提出一个解决密钥托管和身份认证可追责的 IBE 方案,但是该方案仅具有 CPA(Chosen plaintext attack)安全性,安全性不够强.

目前针对 IBE 系统安全性的研究较多[10,11],但由于 HIBE 和 IBE 在密钥产生和加解密算法上的不同[12],上述针对 IBE 的解决方案无法直接用到 HIBE 机制中. Gentry[13]提出第一个完全防串谋 HIBE 机制,该机制被证明为基于随机预言机模型下的 CCA 安全. Waters 首次提出了双系统加密方式,实现了一个基于简单假设下的完全安全 HIBE 机制[14],并在此基础上进行改进[15],有效减小系统的密文长度. 但两者专注密码机制本身,没有考虑密码应用的密钥传输、身份认证及可追责问题. 而本文提出的 T-HIBE 密码系统既能实现 IND-sID-CCA 安全的完全抗串谋 HIBE 机制,又能解决密钥托管、密钥安全传输、身份高效认证和可追责性的问题.

3 预备知识

3.1 符号说明

q 是大素数,$\mathbb{Z}_q$ 为模 q 的剩余类,$\mathbb{Z}^+$ 为正整数集合,G_1 是 q 阶加法群,G_2 是 q 阶乘法群,$x \in_u S$ 表示均匀随机地在集合 S 中选取元素 x.

3.2 双线性映射

满足以下性质的映射关系 $e: G_1 \times G_1 \to G_2$ 称为双线性映射:

(1)双线性. $\forall P, Q \in G_1$ 以及 $\forall a, b \in_u \mathbb{Z}_q$,有 $e(aP, bQ) = e(P, Q)^{ab} = e(P, aQ)^b = e(bP, Q)^a$.

(2)非退化性. $\exists P, Q \in G_1$, s. t. $e(P, Q) \in G_2$ 不是 G_2 的单位元.

(3)可计算性. $\forall P, Q \in G_1$,存在计算 $e(P, Q) \in G_2$ 的有效算法.

3.3 难题假设

(1)DL 问题(离散对数问题)

输入:已知加法群 G_1 的生成元为 P,$a \in_u \mathbb{Z}_q$,则输入 P,aP.

输出:计算值 a.

(2)BDH 问题

输入:群 G_1、G_2 的描述,双线性映射 $e: G_1 \times G_1 \to G_2$,$G_1$ 的生成元 P,以及群元素 aP、bP、cP($a, b, c \in_u \mathbb{Z}_q$)

输出:计算值 $e(P, P)^{abc}$

3.4 安全性定义

密码体制的形式化安全定义依赖于攻击游戏的描述. 攻击游戏通常包括两个实体:敌手 A 以及挑战者 C.

单向加密(OWE,One Way Encryption)安全. 给定敌手 A 一个随机公钥 K_{pub} 以及密文 $C = \mathrm{Enc}(K_{pub}, M)$,A 给出明文的猜测 M'. 如果不存在敌手 A 可以在多项式时间内以不可忽略的优势得到 $M' = M$,则称该密码体制是 OWE 安全的.

IND-sID-CCA(选择身份-选择密文攻击)安全. 敌手 A 和挑战者 C 之间进行如下安全游戏:

(1)C 输入安全参数 K 进行系统初始化,并将系统公共参数提供给 A.

(2)A 选择两个等长的明文 M_0、M_1,以及要攻击的公钥 ID_0,发送给 C;C 以等同的概率选择 $b \in_u \{0, 1\}$,加密得到 $C = \mathrm{Enc}(ID_0, M_b)$.

(3)A 向 C 提交两种类型的服务请求:私钥查询服务(ID_i),C 返回;解密服务(ID_i, C),C 返回 $M = \mathrm{Dec}$

(ID_i, C). 此处须满足条件 $ID_i \neq ID_0, M \neq M_i, i = 1, 2$;否则,终止该游戏.

(4) A 给出 $b \in \{0,1\}$ 的猜测 b'.

如果不存在敌手 A 可以在多项式时间内以不可忽略的优势得到 $b' = b$,则称该密码体制是 IND-sID-CCA 安全的.

4　T-HIBE 系统结构

为了解决 HIBE 中 PKG 的密钥托管问题,T-HIBE 系统采用层次化分布式的私钥产生机制,即通过层次化 PKG 和多个密钥隐私机构(Key Privacy Authority) KPA 共同为用户产生私钥. T-HIBE 的系统结构如图 1 所示,系统的参与方包括根 PKG,域 PKG_t^i ($1 \leqslant t \leqslant m, 1 \leqslant i \leqslant n_t$,即共 m 层域 PKG,第 t 层有 n_t 个域 PKG),n 个密钥隐私机构 KPA_i ($1 \leqslant i \leqslant n$),以及若干用户. 系统中每个用户具有唯一的身份标识 $ID\text{-tuple}_t^i$ (t 表示该实体处于第 t 层 $level_t$, i 为用户编号). 为方便描述,定义 PKG_t^i 及 $ID\text{-tuple}_t^i$ 在 k 层的父 PKG 为 PKG_k^j ($j = p(i,k), 0 \leqslant k < t$),即 $p(i,k)$ 为 PKG 的上标计算函数.

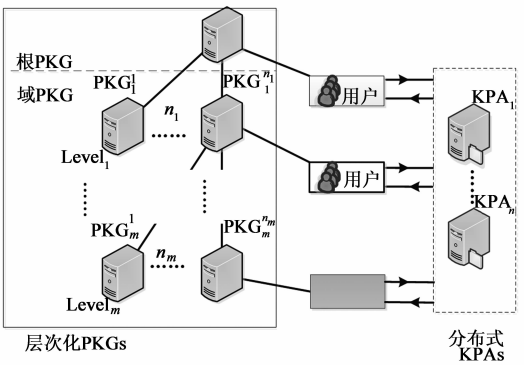

图1　T-HIBE系统结构

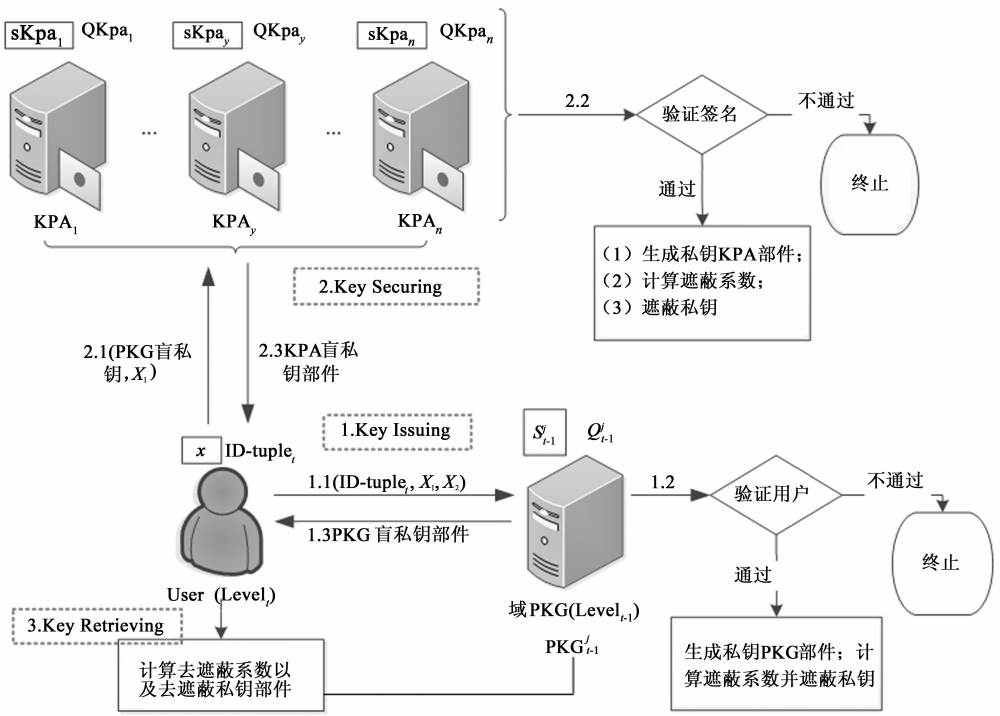

图2　T-HIBE私钥生成协议

T-HIBE 机制包括四个算法:Setup(系统初始化)、KeyGen(私钥生成)、Encryption(加密)和 Decryption(解密).

Setup　系统初始化,输入系统安全参数,产生各个机构的主密钥和系统参数.

KeyGen　为用户生成私钥,用户与层次化 PKG 和 KPAs 的交互协议如图 2 所示,包括 PKG 密钥颁发(Key Issuing),KPA 私钥加固(Key Securing)和私钥恢复(Key Retrieving)三个步骤:

(1) Key Issuing:某个处于 t 层的用户 $ID\text{-tuple}_t^i$ 产生盲因子 X_1 和私钥编号因子 X_2,将 $(ID\text{-tuple}_t^i, X_1, X_2)$ 提交给上一级 PKG;上一级 PKG 认证用户身份,计算 PKG 盲私钥部件并签名将结果发送给用户;用户验证 PKG 返回的结果.

(2) Key Securing:用户将 PKG 盲私钥部件和签名、盲因子 X_1 提交给每个 KPA;KPA 通过验证签名来共享 PKG 用户身份认证,然后产生 KPA 盲私钥部件并将结果传输给用户.

(3) Key Retrieving:用户收到所有 KPA 响应后,计算私钥编号,通过去遮蔽因子得到自己的私钥.

Encryption 输入接收方 ID、系统参数和消息,输出密文.

Decryption 输入密文、系统参数和接收方私钥,输出消息.

5 T-HIBE 机制设计

基于层次分布的 T-HIBE 结构,本节首先提出一个满足系统设计目标且具有 IND-sID-OWE 安全的基本 T-HIBE 机制;在基本 T-HIBE 基础上,文章进一步通过使用 Fujisaki-Okamoto[16] 数据填充技术,实现具有 IND-sID-CCA 安全的完全 T-HIBE 机制.

5.1 基本 T-HIBE 机制

基本 T-HIBE 机制包括 Setup(系统初始化)、KeyGen Protocol(私钥生成协议)、Encryption(加密)和 Decryption(解密)四个算法.

Setup 系统初始化算法输入安全参数 $k\in\mathbb{Z}^+$,输出系统参数. 整个系统初始化包括三个部分:根 PKG、域 PKG 以及 KPA 的初始化.

(1)根 PKG 初始化执行步骤.

(a)P 运行群生成器 IG 生成阶为 q 的群 G_1、G_2,以及双线性映射 $e:G_1\times G_1\to G_2$.

(b)选择任意生成元 $P_0\in G_1$.

(c)取 $s_0\in_u\mathbb{Z}_q$,计算 $Q_0=s_0P_0$.

(d)选择单向散列函数 $H_1:\{0,1\}^*\to G_1$,$H_2:G_2\to\{0,1\}^n$(n 表示消息长度),$H_3:G_1\to\mathbb{Z}_q^*$.

(e)公开 PKG 参数$(G_1,G_2,e,P_0,Q_0,H_1,H_2)$,保留 $s_0\in\mathbb{Z}_q$ 作为根的 PKG 私钥.

(2)域 PKG 初始化执行步骤.

域 PKG 按照层级从低到高的次序依次进行初始化,假设现在进行 level_t 的初始化,该层每个 $\text{PKG}_t^i(1\leqslant i\leqslant m_t)$ 分别选择 $s_t^i\in_u\mathbb{Z}_q$ 作为秘密值. PKG_t^i 向其父 PKG 节点 $\text{PKG}_{t-1}^j(j=p(i,t-1))$ 发送身份标识$(ID_1,\cdots,ID_t)$,PKG_{t-1}^j 执行如下步骤:

(a)计算 $P_t=H_1(ID_1,\cdots,ID_t)$.

(b)计算 $S_t^i=s_{t-1}^jP_t+S_{t-1}^j$(定义 S_0^j 为 G_1 的单位元).

(c)计算 $Q_{t-1}^j=s_{t-1}^jP_0$.

(d)将$(S_t^i,\{Q_k^{p(i,k)}\}_{k=1,\cdots,t-1})$发送至 PKG_t^i.

(3)KPA 初始化执行步骤.

$\text{KPA}_y(1\leqslant y\leqslant n)$ 选择秘密值 $\text{sKpa}_y\in_u\mathbb{Z}_q$,计算并公开 $\text{QKpa}_y=\text{sKpa}_yP_0$.

KeyGen 密钥生成 假设某个处于 t 层的用户 ID-tuple_t^i 申请用户私钥. 用户选取秘密值 $x\in_u\mathbb{Z}_q$,计算盲因子 $X_1=xP_0$,私钥编号因子 $X_2=xP_t(P_t=H_1(ID_1,\cdots,ID_t))$,将$(\text{ID-tuple}_t^i,X_1,X_2)$发送给处于 $t-1$ 层的父私钥生成机构 $\text{PKG}_{t-1}^j(j=p(i,t-1))$.

(1)PKG_{t-1}^j 收到用户请求,执行下述动作:

(a)PKG_{t-1}^j 验证用户身份.

(b)计算隐藏系数:$\text{bId}_t=H_3(s_{t-1}^jX_1)$.

(c)随机选择 $x'\in_u\mathbb{Z}_q$,计算 $D_{x'}=x'\text{bId}_t$,$R=x's_{t-1}^jX_2$.

(d)计算 $P_t=H_1(ID_1,\cdots,ID_t)$.

(e)计算 $SK=S_{t-1}^j+s_{t-1}^jP_t+R$.

(f)计算 $Q_{t-1}^j=s_{t-1}^jP_0$.

(g)用隐藏系数遮蔽私钥部件 SK,得到 $D_0=\text{bId}_t\cdot SK$.

(h)PKG 签名用户的盲私钥部件 $\text{Sig}(D_0)=s_{t-1}^jD_0$.

(i)将$(D_{x'},D_0,\text{Sig}(D_0),\{Q_k^{p(i,k)}\}_{k=1,\cdots,t-1})$发送给用户.

(2)用户 ID-tuple_t^i 收到 PKG 的响应后,执行下述动作:

(a)验证 PKG 的签名:$e(\text{Sig}(D_0),P_0)\overset{?}{=}e(D_0,Q_{t-1}^{p(i,t-1)})$,检验 PKG 的合法性.

(b)将$(D_0,\text{Sig}(D_0),X_1,Q_{t-1}^{p(i,t-1)})$分别发送给各 $\text{KPA}_y(1\leqslant y\leqslant n)$.

(3)$\text{KPA}_y(1\leqslant y\leqslant n)$ 收到用户的请求后,执行下述动作:

(a)验证 PKG 的签名:$e(\text{Sig}(D_0),P_0)\overset{?}{=}e(D_0,Q_{t-1}^{p(i,t-1)})$,检验用户的合法性.

(b)计算隐藏系数$\text{bKpa}_y=H_3(\text{sKpa}_yX_1)$.

(c)计算 $P_1=H_1(ID_1)$,$P_t=H_1(ID_1,\cdots,ID_t)$.

(d)计算KPA_y 私钥部件:$\text{SKpa}_y=\text{sKpa}_y(P_1+P_t)$.

(e)用隐藏系数遮蔽私钥部件SKpa_y,得到 $D_y=\text{bKpa}_y\cdot\text{SKpa}_y$.

(f)将 D_y 发送给用户.

(4)用户 ID-tuple_t^i 接收到父PKG_{t-1}^j响应$(D_{x'},D_0,\text{Sig}(D_0),\{Q_k^{p(i,k)}\}_{k=1,\cdots,t-1})$和各$\text{KPA}_y$响应 $D_y(1\leqslant y\leqslant n)$后,执行下述动作:

(a)计算PKG_{t-1}^j去遮蔽因子

$$\begin{aligned}\text{unbId}_t&=H_3(xQ_{t-1}^j)=H_3(xs_{t-1}^jP_0)\\&=H_3(s_{t-1}^jxP_0)=H_3(s_{t-1}^jX_1)=\text{bId}_t.\end{aligned}$$

(b)计算$\text{KPA}_y(1\leqslant y\leqslant n)$的去遮蔽因子

$$\begin{aligned}\text{unbKpa}_y&=H_3(x\text{QKpa}_y)=H_3(x\text{sKpa}_xP_0)\\&=H_3(\text{sKpa}_yxP_0)=H_3(\text{sKpa}_yX_1)\\&=\text{bKpa}_y\end{aligned}$$

(c)计算私钥编号 $\theta=x\cdot\text{unbId}_t^{-1}D_{x'}=xx'$.

(d)用去遮蔽因子unbId_t 和$\text{unbKpa}_y(1\leqslant y\leqslant n)$计算得到私钥部件:$\text{unbId}_t^{-1}(D_0)=SK$,$\text{unbKpa}_y^{-1}(D_y)=\text{SKpa}_y(1\leqslant y\leqslant n)$,得到完整的私钥$(\theta,SK,\{Q_k^{p(i,k)}\}_{k=1,\cdots,t-1},\{\text{SKpa}_y\}_{y=1,\cdots,n})$.

Encryption　假设使用ID-tuple$_t$ = (ID_1,…,ID_t)作为公钥对明文 $M \in \mathrm{M}$ 进行加密,执行如下步骤:

(1)计算 $P_i = H_1(ID_1,\cdots,ID_i)$,$1 \leqslant i \leqslant t$.

(2)选择 $r \in_u \mathbb{Z}_q$.

(3)计算密文:

$$C = [rP_0, rP_2, \cdots, rP_t, M \oplus H_2(g_1^r) \oplus H_2(g_2^r)],$$

其中 $g_1 = e(Q_0, P_1)$,$g_2 = e(\sum_{i=1}^{n} \mathrm{QKpa}_i, P_1)$.

Decryption　记密文 $C = [U_0, U_2, \cdots, U_t, V] \in \mathbb{C}$ 是使用 ID-tuple$_t$ = (ID_1,…,ID_t)加密所得,用户接收密文后,计算

$$V \oplus H_2\left(\frac{e(U_0, SK)}{e(U_t, Q_{t-1}^i)^{\theta} \prod_{j=2}^{t} e(Q_{j-1}^i, U_j)}\right) \oplus H_2\left(\frac{e(U_0, \sum_{i=1}^{n} \mathrm{SKpa}_i)}{\prod_{i=1}^{n} e(\mathrm{QKpa}_i, U_t)}\right) = M.$$

正确性验证:

$$\frac{e(U_0, SK)}{e(Q_{t-1}^i, U_t)^{\theta} \prod_{j=2}^{t} e(Q_{j-1}^i, U_j)}$$

$$= \frac{e(rP_0, \sum_{j=1}^{t} s_{j-1}^i P_t + R)}{e(s_{t-1}^i P_0, rP_t)^{\theta} \prod_{j=2}^{t} e(s_{j-1}^i P_0, rP_j)}$$

$$= \frac{e(rP_0, x' s_{t-1}^i x P_t)\, e(rP_0, s_0 P_1) \prod_{j=2}^{t} e(rP_0, s_{j-1}^i P_t)}{e(rP_0, s_{t-1}^i P_t)^{xx'} \prod_{j=2}^{t} e(rP_0, s_{j-1}^i P_j)}$$

$$= e(s_0 P_0, rP_1) = e(Q_0, P_1)^r = g_1^r,$$

$$\frac{e(U_0, \sum_{i=1}^{n} \mathrm{SKpa}_i)}{\prod_{i=1}^{n} e(\mathrm{QKpa}_i, U_t)}$$

$$= \frac{\prod_{i=1}^{n} e(rP_0, \mathrm{sKpa}_i(P_1 + P_t))}{\prod_{i=1}^{n} e(\mathrm{sKpa}_i P_0, rP_t)}$$

$$= \frac{\prod_{i=1}^{n} e(rP_0, \mathrm{sKpa}_i P_1) \prod_{i=1}^{n} e(rP_0, \mathrm{sKpa}_i P_t)}{\prod_{i=1}^{n} e(rP_0, \mathrm{sKpa}_i P_t)}$$

$$= \prod_{i=1}^{n} e(\mathrm{sKpa}_i P_0, rP_1) = e(\sum_{i=1}^{n} \mathrm{QKpa}_i, P_1)^r = g_2^r$$

故使用 ID-tuple 加密的密文 C,使用用户私钥进行解密运算,可以得到明文 M.

5.2　完全 T-HIBE 机制

基本 T-HIBE 机制满足基于随机预言机的 IND-sID-OWE 安全性. 为了抵御对 T-HIBE 密码机制的复杂攻击,本小节在基本 T-HIBE 机制的基础上进一步提出完全 T-HIBE 机制,使用 Fujisaki-Okamoto 填充技术[2]使得 T-HIBE 机制能够达到基于随机预言机的 CCA 安全. 完全 T-HIBE 机制描述如下:

Setup　与基本 T-HIBE 大致相同,增加选择两个单向散列函数:$H_4: \{0,1\}^n \times \{0,1\}^n \to \mathbb{Z}_n$,$H_5: \{0,1\}^n \to \{0,1\}^n$.

KeyGen　与基本 T-HIBE 机制相同.

Encryption　使用ID-tuple$_t$ = (ID_1,…,ID_t)作为公钥对明文 $M \in \mathrm{M}$ 进行加密,执行如下步骤:

(1)计算 $P_i = H_1(ID_1,\cdots,ID_i)$,$1 \leqslant i \leqslant t$.

(2)选择 $\sigma \in_u \{0,1\}^n$.

(3)计算 $r = H_4(\sigma, M)$.

(4)计算密文

$$C = [rP_0, rP_2, \cdots, rP_t, \sigma \oplus H_2(g_1^r) \oplus H_2(g_2^r)\, M \oplus H_5(\sigma)],$$

其中 $g_1 = e(Q_0, P_1)$,$g_2 = e(\sum_{i=1}^{n} \mathrm{QKpa}_i, P_1)$.

Decryption　记密文 $C = [U_0, U_2, \cdots, U_t, V, W] \in \mathbb{C}$ 是使用 ID-tuple(ID_1,…,ID_t)加密所得,用户接收密文后,

(1)计算

$$V \oplus H_2\left(\frac{e(U_0, SK)}{e(U_t, Q_{t-1}^i)^{\theta} \prod_{j=2}^{t} e(Q_{j-1}^i, U_j)}\right) \oplus H_2\left(\frac{e(U_0, \sum_{i=1}^{n} \mathrm{SKpa}_i)}{\prod_{i=1}^{n} e(\mathrm{QKpa}_i, U_t)}\right) = \sigma.$$

(2)计算 $W \oplus H_5(\sigma) = M$.

(3)计算 $r = H_4(\sigma, M)$,使用 r 和(ID_1,…,ID_t)对 M 进行 T-HIBE 加密,检验结果是否与[U_0,U_2,…,U_t,V]一致. 如果不一致,则拒绝密文.

(4)输出解密 C 得到的明文 M.

6　T-HIBE 安全性分析

为了证明基本 T-HIBE 机制的安全性,首先介绍基本公钥加密机制 BasicPub 以及基本 HIBE 加密机制 BasicHIBE. BasicPub 最初介绍于文献[2],本文采用的机制与其大致相同,包括 KeyGen(密钥生成)、Encryption(加密)和 Decryption(解密)三个步骤:

KeyGen

(1)运行群生成器 IG,输入安全参数 K,输出阶为 q 的两个群 G_1、G_2,以及双线性映射 $e: G_1 \times G_1 \to G_2$. 随机选择群生成元 $P_0 \in G_1$.

(2)随机选择 $s \in_u \mathbb{Z}_q$,计算 $Q_0 = sP_0$.

(3)随机选择群元素 $P_1 \in_u G_1$.

(4)选择哈希函数 $H_2: G_2 \rightarrow \{0,1\}^n$.

Encryption 选择随机数 $r \in \mathbb{Z}_q$,对明文 $M \in \mathrm{M}$ 进行加密,密文为:$C = [rP_0, M \oplus H_2(g^r)]$,其中 $g = e(Q_0, P_1)$.

Decryption 记密文为 $C = [U, V] \in \mathbb{C}$,解密步骤为:$V \oplus H_2(e(U, S_1)) = M$.

BasicHIBE 加密机制与本文提出的基本 T-HIBE 机制基本相同,区别在于没有 KPA 和盲因子的使用. 各算法的描述如下[10]:

Setup 没有 KPA 的初始化,其余初始化步骤相同.

KeyGen 没有与 KPA_i 相关的密钥部件,不使用遮蔽因子对私钥部件进行遮蔽,即密钥生成获得的完整私钥部件为:

$$\left(S_t = \sum_{i=1}^{t} s_{i-1} P_i, Q_i = s_i P_0 \mid i = 0, \cdots, t\right)$$

Encryption 计算密文 $C = [rP_0, rP_2, \cdots, rP_t, M \oplus H_2(g^r)]$,其中 $g = e(Q_0, P_1)$.

Decryption 解密明文:$V \oplus H_2\left(\dfrac{e(U_0, S_t)}{\prod_{i=2}^{t} e(Q_{i-1}, U_i)}\right) = M$.

定理 1 假设存在一个可以对私钥进行无限次查询以及对函数 H_2 进行 q_{H_2} 查询的敌手 A,能够以一个不可忽略的优势 ε 在 IND-sID-OWE 模式下攻破基本 T-HIBE 机制(BasicHIBE + KPA 方案),并且 H_1 和 H_2 都是随机预言机. 那么存在算法 B 可以以不小于 $\dfrac{\left(\varepsilon - \dfrac{1}{2^n}\right)}{q_{H_2}}$ 的优势在多项式时间内解决由 IG 生成的群的 BDH 难题.

定理 1 说明攻破基本 T-HIBE 机制的任务可以规约到解决 BDH 难题的能力,其证明可以表述为引理 1、2、3 的证明. 如图 3 所示,引理 1、2、3 分别证明了各密码机制之间以及 BDH 难题的规约关系.

引理 1 假设存在敌手 A 可以以一个不可忽略的优势 ε 在 IND-sID-OWE 模式下攻破基本 T-HIBE 机制,则存在一个算法 B 可以以不小于 ε 的优势在多项式时间内攻破 BasicHIBE.

证明 敌手 A 对基本 T-HIBE 机制的攻击如图 4 所示,并在多项式时间内以不可忽略的优势输出明文的有根据猜测 M',使得 $M' = M$. 敌手 B 与 HIBE 的挑战者进行攻击游戏,为了获得攻击优势 ε,使用如图 5 所示的方法进行基本 T-HIBE 机制的仿真,具体包括如下四个步骤.

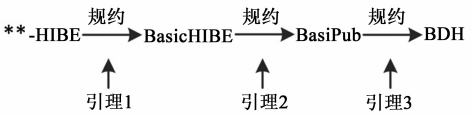

图3 各密码机制以及BDH难题的规约关系

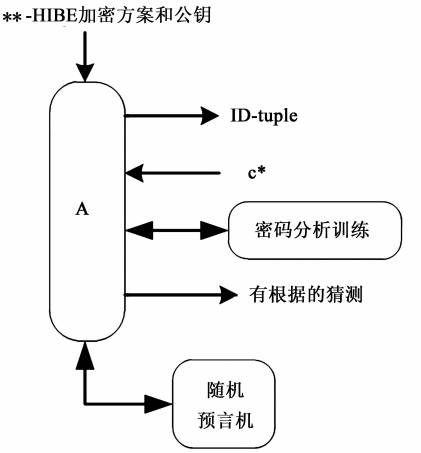

图4 敌手A对基本T-HIBE机制的攻击流程

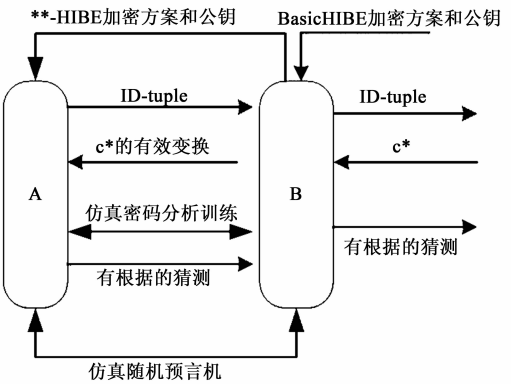

图5 敌手B仿真基本T-HIBE机制

Setup 初始化阶段,敌手 A 向基本 T-HIBE 机制挑战者查询公共参数,敌手 B 仿真挑战者为 A 返回公共参数.

(1)敌手 B 从 HIBE 挑战者处获取公共参数 $K_{\mathrm{pub}} = (G_1, G_2, e, P_0, Q_0, H_1, H_2, H_3)$.

(2)选择 n 个随机数 $s_i' \in \mathbb{Z}_q (i = 0, \cdots, n)$,计算 $Q_i' = s_i' P_0$,记录 $(\{s_i', Q_i'\}_{i=1,\cdots,n})$.

(3)将公共参数 $K_{\mathrm{pub}} = (G_1, G_2, e, P_0, Q_0, H_1, H_2)$ 和 $K_{\mathrm{pub}}' = (Q_1', \cdots, Q_n')$ 返回给 A.

KeyGen 私钥查询阶段,敌手 B 需要维护一个用户秘密值表 B^{list},用于存放敌手 A 查询的 $\mathrm{ID\text{-}tuple}_t$ 的秘密值,该表初始化为空. 敌手 A 向基本 T-HIBE 机制的挑战者查询 $\mathrm{ID\text{-}tuple}_t$ 的私钥时,敌手 B 执行相应动作:

(1)敌手 B 计算 $P_t = H_1(ID_1, \cdots, ID_t)$,在 B^{list} 中查询 P_t.

(a)如果 P_t 在 B^{list} 中,返回 $\mathrm{ID\text{-}tuple}_t$ 的秘密值 $x \in \mathbb{Z}_q$;否则,随机选择 $x \in_u \mathbb{Z}_q$,将 (P_t, x) 加入 B^{list} 中.

(*b*)计算用户的盲因子 $X_1 = xP_0$,私钥编号因子 $X_2 = xP_t$.

(*c*)计算 $b_{ID} = \mathrm{unb}_{ID} = H_3(xs_{t-1}P_0) = H_3(xQ_{t-1})$.

(2)敌手 B 仿真 PKG 为敌手 A 提供预言服务:

(*a*)向 BasicHIBE 挑战者查询 ID-tuple$_t$ 的私钥$(S_t, \{Q_i\}_{i=1,\cdots,t-1})$.

(*b*)向 BasicHIBE 挑战者查询 ID-tuple$_{t-1}$ 的私钥$(S_{t-1}, \{Q_i\}_{i=1,\cdots,t-2})$.

(*c*)选择 $x' \in_u \mathbb{Z}_q$,计算 $D_{x'} = x'b_{ID}$, $R = x'x(S_t - S_{t-1}) = x'xs_{t-1}P_t$.

(*d*)计算 $SK = S_t + R$.

(*e*)计算 $D_0 = b_{ID}SK$.

(*f*)选取 $s_{\mathrm{fake}} \in_u \mathbb{Z}_q$,利用 s_{fake} 签名用户的盲私钥部件 $\mathrm{Sig}(D_0) = s_{\mathrm{fake}}D_0$.

(*g*)将$(D_{x'}, D_0, \mathrm{Sig}(D_0), \{Q_i\}_{i=1,\cdots,t-1})$作为基本 T-HIBE 机制私钥的 PKG 部件发送给敌手 A.

(3)敌手 B 接收敌手 A 进行私钥加固的请求,仿真 KPA 为 A 提供预言服务:

(*a*)计算 $S_i' = s_i'(P_1 + P_t)$, $i = 0, \cdots, n$,作为基本 T-HIBE 机制私钥的 KPA 部件.

(*b*)计算 $b_i = H_3(s_i'X)$, $D_i = b_iS_i'$, $i = 1, \cdots, n$.

(*c*)将$\{D_i\}_{i=1,\cdots,n}$发送给 A.

敌手 A 收到敌手 B 的所有私钥部件后,可提取完整的私钥.

Challenge　挑战阶段,敌手 A 向基本 T-HIBE 机制挑战者请求使用公钥 ID-tuple$_0$ 加密的挑战密文,敌手 B 执行相应动作.

(1)敌手 B 向 BasicHIBE 挑战者请求 ID-tuple$_0$ 加密的挑战密文 $C = [U_0, U_2, \cdots, U_t, V] \in \mathbb{C}$.

(2)敌手 B 计算 $V' = V \oplus H_2((g')^r)$,其中 $g' = e(\sum_{i=1}^{n} \mathrm{QKpa}_i, P_1) \in G_2$. 向敌手 A 返回密文 $C' = [U_0, U_2, \cdots, U_t, V'] \in \mathbb{C}$.

根据第 5 节对基本 T-HIBE 机制的描述可知,明文 M 经过加密可得到密文

$$C = [rP_0, rP_2, \cdots, rP_t, M \oplus H_2(g_1{}^r) \oplus H_2(g_2{}^r)]$$

其中 $g_1 = e(Q_0, P_1) \in G_2$, $g_2 = e(\sum_{i=1}^{n} \mathrm{QKpa}_i, P_1) \in G_2$.

敌手 B 将 BasicHIBE 的密文部件 $V = M \oplus H_2(g^r)$ 经过变换得到 $V' = M \oplus H_2(g^r) \oplus H_2((g')^r)$,其中 $g = g_1$, $g' = g_2$. 可知敌手 B 正确模拟了基本 T-HIBE 机制的加密步骤,即 B 返回给敌手 A 的密文是使用 ID-tuple$_0$ 加密的有效密文.

Guess　敌手 A 输出明文的有效猜测 M'. 敌手 B 将 M' 作为攻击的猜测明文,提交给 BasicHIBE 挑战者.

由引理的假设可知,敌手 A 在多项式时间内以不可忽略的优势 ε 提交的猜测明文 $M' = M$,故敌手 B 可以在多项式时间内以不可忽略的优势 ε 攻破 BasicHIBE.

引理 2　假设一个可以进行无限次私钥查询的 NHID-OWE(Non chosen adaptively OWE)敌手 A 具有攻破 BasicHIBE 的优势 ε,并且哈希函数 H_1 是一个随机预言机. 则存在一个 OWE 敌手 B,具有至少为 ε 的优势,在 A 的多项式时间内攻破 BasicPub.

引理 3　假设存在一个可以对函数 H_2 进行 q_{H_2} 查询的敌手 A,能够以不可忽略的优势 ε 在 OWE 模式下攻破 BasicPub,并且 H_2 是一个随机预言机. 则存在算法 B 可以以不小于 $\dfrac{\left(\varepsilon - \dfrac{1}{2^n}\right)}{q_{H_2}}$ 的优势在多项式时间内解决由 IG 生成的群的 BDH 难题.

引理 2 和引理 3 的证明与文献[10]的 A.3 引理 1 一致,本文不加以赘述.

定理 2　假设存在敌手 A 可以在多项式时间内以不可忽略的优势在 IND-sID-CCA 模式下攻破完全 T-HIBE 机制. 那么则存在算法 B 可在多项式时间内以不可忽略的优势在 IND-sID-CPA 模式下攻破基本 T-HIBE 机制.

证明　完全 T-HIBE 机制在基本 T-HIBE 机制的基础上使用 Fujisaki-Okamoto 填充技术[16]. 定理 2 的证明可见参考文献[16].

定理 3　T-HIBE 中,用户只能计算出自己私钥的隐藏系数.

证明　由于秘密值 x 由用户生成,由 DL 难题假设得到已知 $X, P \in G_1$,计算 x 使得 $X = xP$ 是困难的,所以秘密值不会被泄漏. PKG 的私钥为 s,其公共参数包括 $Q, P \in G_1$,其中 $Q = sP$,因此已知 Q, P 的情况下,根据 DL 难题,计算 s 是困难的,故 PKG 私钥不会泄露. 由以上的推导可知,已知 Q, X 的情况下,不能计算出 s 和 x,则不能计算出 sxP. 因此,隐藏系数的计算方法可以保证只有私钥对应用户和 PKG 能够计算出隐藏系数(去隐藏系数),即 $unb = H(xQ) = H(xsP) = H(sxP) = H(sX) = b$. 由于用户秘密值 x 以及 PKG 私钥 s 的保密性,隐藏系数 b 不会被泄漏. 而每个用户仅仅知道自己的秘密值 x,所以用户只能计算出自己私钥所对应的隐藏系数.

定理 3 说明经过遮蔽的用户私钥传输不需要安全信道传输,即 T-HIBE 解决了密钥安全传输问题.

引理 4　T-HIBE 机制下,PKG 为非法用户生成私钥,无法计算合法用户的私钥编号.

证明　用户私钥的私钥编号 θ 由 PKG 秘密值 x' 以及用户秘密值 x 共同控制. 定理 3 证明基于 DL 难题假

设,PKG 无法在多项式时间内有效计算用户秘密值 x,同时 DL 难题假设保证虽然 PKG 已知 $R=\theta s_{t-1}^{i}P_t$ 以及 $s_{t-1}^{i}P_t$ 的值,也无法有效计算 θ. 因此 PKG 无法在多项式时间内计算用户的私钥编号 θ. 由于不能有效控制 θ 取值,PKG 无法为非法用户生成与合法用户相同私钥编号的用户私钥.

引理 5 利用已有私钥信息,用户无法计算出编号不同的良构的用户私钥.

证明 用户使用身份信息 ID-tuple 向 PKG 申请私钥,其私钥部件 $SK=S_{t-1}^{i}+s_{t-1}^{i}P_t+R$ 中 $R=x'xs_{t-1}^{i}P_t=\theta s_{t-1}^{i}P_t$ 是由 θ 以及 s_{t-1} 控制的私钥编号部件. 用户利用个人私钥,修改私钥编号为 $\theta_{\text{new}}=x_{\text{new}}x'$,其对应的良构私钥部件为 $SK_{\text{new}}=S_{t-1}^{i}+s_{t-1}^{i}P_t+\theta_{\text{new}}s_{t-1}^{i}P_t$. 可知 $SK_{\text{new}}=SK+(\theta_{\text{new}}-\theta)s_{t-1}^{i}P_t$,由于 s_{t-1} 是 PKG 使用的随机秘密值,故用户无法有效计算值 $(\theta_{\text{new}}-\theta)s_{t-1}^{i}P_t$,因此用户无法计算具有不同私钥编号的良构的用户私钥.

定理 4 在 T-HIBE 机制下,PKG 为非法用户生成私钥的行为可追责.

证明 引理 5 说明,用户无法通过已有私钥信息,计算具有不同私钥编号的良构的用户私钥,引理 4 说明 PKG 通过恶意认证用户生成的私钥,无法与合法用户共享相同的私钥编号. 因此,当出现相同身份信息 ID-tuple 的两把私钥 $\text{Key}_1=(\theta, SK, \{Q_j^i\}_{j=1,\cdots,t-1}, \{\text{SKpa}_i\}_{i=1,\cdots,n})$ 和 $\text{Key}_2=(\theta', SK', \{Q_j^i\}_{j=1,\cdots,t-1}, \{\text{SKpa}_i\}_{i=1,\cdots,n})$,验证 $\theta\overset{?}{=}\theta'$ 即可判定私钥泄漏方. 如果 $\theta\neq\theta'$,则判定 PKG 为不诚实认证用户,为非法用户生成私钥的行为. 因此,PKG 为非法用户生成私钥的行为可追责.

前面是对两种 T-HIBE 机制的安全性证明,表 1 对 T-HIBE 和相关工作进行了对比分析,n 为系统中私钥产生机构数目,t 为门限值,身份验证开销由参与用户身份验证的机构数量表示. 可以发现完全 T-HIBE 机制在解决密钥托管问题、密钥安全通道需求、PKG 身份认证开销和可追责、安全性方面具有系统优势. T-HIBE 密钥托管问题由分布式密钥生成机制解决,用户需获得所有 n 个私钥生成机构的私钥构件才能计算得到自己的私钥,即系统的容忍度为 $(n-1)/n$. T-HIBE 无需安全通道即可实现私钥的安全传输由定理 3 证明,PKG 用户认证的可追责性由定理 4 证明,而基本 T-HIBE 机制的 IND-sID-OWE 安全性和完全 T-HIBE 机制的 IND-sID-CCA 安全性则分别由定理 1 和定理 2 证明.

表 1 方案对比分析

方案	PKG 密钥托管	系统容忍度	需安全通道	身份认证开销	身份认证可追责	支持层次性	安全性
门限[5]	是	t/n	是	n	否	否	IND-ID-CCA
串行模式[8]	是	$(n-1)/n$	否	1	否	否	—
SA-IBE[9]	是	$(n-1)/n$	否	1	是	否	IND-sID-CPA
GS-HIBE[13]	否	0	是	1	否	是	IND-ID-CCA
LW-HIBE[15]	否	0	是	1	否	是	IND-ID-CCA
基本 T-HIBE	是	$(n-1)/n$	否	1	是	是	IND-sID-OWE
完全 T-HIBE	是	$(n-1)/n$	否	1	是	是	IND-sID-CCA

7 总结

本文提出一种可信安全的层次式基于身份加密系统 T-HIBE. 通过层次式分布化的用户私钥产生、私钥用户盲因子和用户私钥编号,解决了层次式私钥生成机构的密钥托管和私钥安全传输问题,支持系统高效的用户身份一次认证和可追责性. 基于标准的 BDH 难题假设,文章证明了基本 T-HIBE 机制和完全 T-HIBE 机制分别具有 IND-sID-OWE 和 IND-sID-CCA 安全性. 同时文章在理论上证明了 T-HIBE 机制有效解决了密钥托管问题,能够实现无安全通道的私钥安全传输以及 PKG 用户认证的可追责性.

参考文献

[1] Samir A. Identity-based cryptosystems and signature schemes[A]. Advances in Cryptology-Crypto (LNCS 0196)[C]. Berlin: Springer-Verlag, 1984. 47-53.

[2] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[A]. Advances in Cryptology-Crypto (LNCS 2139)[C]. Berlin: Springer-Verlag, 2001. 213-229.

[3] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[A]. Advances in Cryptology-ASIACRYPT (LNCS 2894)[C]. Berlin: Springer-Verlag, 2003. 452-473.

[4] Gentry C. Certificate-based encryption and the certificate Revocation problem[A]. Advances in Cryptology-EUROCRYPT (LNCS 2656)[C]. Berlin: Springer-Verlag, 2003. 272-293.

[5] Kate A, Goldberg I. A Distributed Private-Key Generator for Identity-Based Cryptography[R]. Centre for Applied

Cryptographic Research (CACR 2007 – 33). 2007.

[6] Chen L, Harrison K, Soldera D, Smart N P. Applications of multiple trust authorities in pairing based cryptosystems [A]. Proceedings of the International Conference on Infrastructure Security (LNCS 2637) [C]. Berlin: Springer-Verlag, 2003. 260 – 275.

[7] Wang J, Bai X, Yu J, Li D. Protecting against key escrow and key exposure in identity-based cryptosystem [A]. Proceedings of the 4th International Conference on Theory and Applications of Models of Computation-TAMC (LNCS 4484) [C]. Berlin: Springer-Verlag, 2007. 148 – 158.

[8] Lee B, Boyd C, Dawson E, Kim K, Yang J, Yoo S. Secure key issuing in ID-based cryptography [A]. Proceedings of Australasian Information Security Workshop-AISW [C]. Dunedin, New Zealand: IEEE Press, 2004. 69 – 74.

[9] 曹丹,王小峰,王飞,胡乔林,苏金树. SA-IBE:一种安全可追责的基于身份加密方案[J]. 电子与信息学报, 2011,33(12):2922 – 2928.
CAO Dan, WANG Xiao-feng, WANG Fei, HU Qiao-lin, SU Jin-su. SA-IBE: A secure and accountable identity-based encryption scheme [J]. Journal of Electronics & Information Technology, 2011, 33 (12): 2922 – 2928. (in Chinese)

[10] 葛爱军,马传贵,程庆丰. 标准模型下 CCA2 安全且固定密文长度的模糊基于身份加密方案[J]. 电子学报, 2013,41(10):1948 – 1952.
GE Ai-jun, MA Chuan-gui, CHENG Qing-feng. CCA2 secure fuzzy identity-based encryption with constant size ciphertexts in the standard model [J]. Acta Electronica Sinica, 2013, 41(10): 1948 – 1952. (in Chinese)

[11] 明洋,王育民. 标准模型下可证安全的通配符基于身份加密方案[J]. 电子学报,2013,41(10):2082 – 2086.
Ming Yang, Wang Yu-min. Provably secure identity-based encryption scheme with wildcard in the standard model [J]. Acta Electronica Sinica, 2013, 41(10): 2082 – 2086. (in Chinese)

[12] Lewko A B, Waters B. Why proving HIBE systems secure is difficult [A]. Advances in Cryptology-EUROCRYPT (LNCS 8441) [C]. Berlin: Springer-Verlag, 2014. 58 – 76.

[13] Gentry C, Silverberg A. Hierarchical id-based cryptography [A]. Advances in Cryptology-ASIACRYPT (LNCS 2501) [C]. Berlin: Springer-Verlag, 2002. 548 – 566.

[14] Waters B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions [A]. Advances in Cryptology-CRYPTO (LNCS 5677) [C]. Berlin: Springer-Verlag, 2009. 619 – 636.

[15] Lewko A, Waters B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts [A]. Theory of Cryptograpy Conference (LNCS 5978) [C]. Berlin: Springer-Verlag, 2010. 455 – 479.

[16] Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes [J]. Journal of cryptology, 2013, 26(1): 80 – 101.

作者简介

王小峰　男,1982 年 4 月出生,江苏海安人. 2009 年在国防科技大学计算机学院获博士学位,现为国防科技大学计算机学院助理研究员,主要从事可信网络系统、密码应用、网络安全、智能数据处理研究.
E-mail: xf_wang@nudt.edu.cn

陈培鑫　男,1987 年 6 月出生,广东普宁人. 2009、2012 年毕业于国防科技大学计算机学院,获学士、硕士学位,现为博士研究生,主要从事基于身份的加密、域间路由安全相关研究.
E-mail: chenpeixin@nudt.edu.cn