抗自适应泄漏的基于身份加密方案

汤佳惠[1,2]，朱艳琴[1,2]，罗喜召[1,2]

（1. 苏州大学 计算机科学与技术学院，江苏 苏州 215006；2. 苏州大学 江苏省计算机信息处理技术重点实验室，江苏 苏州 215006）

摘 要：针对基于身份的加密（IBE）体制中缺乏有效抗自适应泄漏方案的问题，运用熵抗泄漏的基本思想，定义了自适应泄漏攻击下 IBE 的安全性；利用基于身份的散列证明系统（IB-HPS）和提取器，提出了抗自适应泄漏的 IBE 方案；并对其进行实例化，构建了基于 q-TABDHE 假设的抗自适应泄漏的 IBE 方案。安全性分析表明，设计的 IBE 方案是选择明文攻击安全的，它不仅能够有效地抵抗自适应泄漏，而且能够容忍较大的密钥泄漏量。

关键词：自适应泄漏；基于身份的加密；熵抗泄漏；q-TABDHE 假设

中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2012)07-0090-06

Identity-based encryption scheme against adaptive leakage

TANG Jia-hui[1,2], ZHU Yan-qin[1,2], LUO Xi-zhao[1,2]

(1. College of Computer Science and Technology, Soochow University, Soochow 215006, China;

2. Province Key Laboratory for Computer Information Processing Technology, Soochow University, Soochow 215006, China)

Abstract: In allusion to the problem that scheme resilient to adaptive leakage was lacked in identity-based encryption, a notion of entropic leakage-resilient was used to define the security against adaptive leakage in IBE. Then by using identity-based hash proof system and extractors, an adaptive-leakage secure IBE scheme was proposed. And for instantiation, an IBE scheme against adaptive leakage based on q-TABDHE assumption was constructed. Security analysis shows that the scheme achieves chosen-plaintext attack security, and it can not only resist adaptive leakage effectively, but also tolerate more key leakage.

Key words: adaptive leakage; identity-based encryption; entropic leakage-resilient; q-TABDHE assumption

1 引言

现代密码学的前提条件是假定密钥对攻击者来说是完全隐藏的，即完备保密的。20 世纪 90 年代，Kocher 等人提出的时间攻击[1]、电源分析[2]在密码学界引起了不小的轰动。人们发现在密码算法的实际实现中，有些物理特征信息（比如运行时间、电源损耗、电磁辐射、声学特征等）和密钥存在某种映射关系，如果攻击者反复运行某个泄漏攻击程序，对这些物理信息进行统计分析，往往可以提取出部分关于密钥的信息。

近年来各种各样的抵抗上述泄漏攻击的方案被提出[3~11]，包括抗泄漏的加密方案[6~9]。文献[6]首次解决了公钥密码体制下的抗泄漏问题，证明了 Regev[12]基于格的公钥加密方案在相对泄漏模型下是抗泄漏的。文献[7]提出了数个基于其他假设的公钥加密方案，这些方案能够抵抗更多泄漏并且是选择密文攻击安全的。文献[6,7]中的方案并非基于身

收稿日期：2011-07-15；**修回日期**：2011-09-20

基金项目：国家自然科学基金资助项目（61070170）；苏州市应用基础研究计划基金资助项目（SYJG09024）；苏州市融合通信重点实验室基金资助项目（SZS0805）

Foundation Items: The National Natural Science Foundation of China (61070170); Suzhou Application Foundation Research Project (SYJG09024); The Fund for Suzhou Key Laboratory of Converged Communication (SZS0805)

份环境中的加密方案。文献[8]在文献[7]的基础上，构建了首个在有界提取模型下的抗泄漏公钥加密方案以及相对泄漏模型下的抗泄漏基于身份加密方案。文献[9]设计了抗持续泄漏的公钥加密方案、基于身份加密方案以及签名方案。

但上述抗泄漏加密方案都有一个限制条件，那就是只允许攻击者在挑战密文产生之前进行泄漏查询。然而，事实上攻击者在得到挑战密文之后能够直接构造一个泄漏函数去解密挑战密文，得到明文的部分信息。由于该泄漏攻击的特征是攻击者能根据前面返回的值（挑战密文）作出后面的泄漏查询，因此把此种泄漏攻击称为自适应泄漏攻击。Naor 和 Segev 在文献[7]中曾提到“找到一个能够抵抗依赖于挑战密文的泄漏攻击的方法将是非常有意义的”。直到 2011 年 Halevi 和 Lin[13]提出熵抗泄漏的概念，才首次证明了存在抗自适应泄漏的公钥加密方案。但在基于身份的加密体制中并没有提出有效的抗自适应泄漏方案。

为了解决上述问题，本文基于熵抗泄漏的基本思想，定义了自适应泄漏攻击下 IBE 的安全性，构造了抗自适应泄漏的 IBE 方案，并对该方案进行了实例化。安全性分析表明，本文构造的方案具有选择明文攻击安全性，它在成功抵抗自适应泄漏攻击的同时，能够容忍较大的密钥泄漏量。

2　基础知识

本文需要的基础知识主要包括最小熵和平均最小熵、提取器、基于身份的散列证明系统。

2.1　最小熵和平均最小熵

统计距离[14]：2 个随机变量 X 和 Y 的统计距离记为 $\Delta(X,Y)=\frac{1}{2}\sum_{\omega}\left|\Pr[X=\omega]-\Pr[Y=\omega]\right|$。如果 $\Delta(X,Y)\leqslant\varepsilon$，则称这 2 个变量是$\varepsilon$-接近的。

最小熵[15]：一个随机变量 X 的最小熵定义为 $H_{\infty}(X)=-\log(\max_x \Pr[X=x])$。

平均最小熵[15]：平均最小熵是指给定另外一个随机变量 Y 值的条件下随机变量 X 的不可预测性，定义为

$$\tilde{H}_{\infty}(X\mid Y)=-\log\left(E_{y\leftarrow Y}\left[\max_x \Pr[X=x\mid Y=y]\right]\right)$$

$$=-\log\left(E_{y\leftarrow Y}\left[2^{-H_{\infty}(X|Y=y)}\right]\right)。$$

给定 3 个随机变量 X、Y、Z，其中，Y 最多有 2^l 可能的值，则

$$\tilde{H}_{\infty}\left(X\mid(Y,Z)\right)\geqslant\tilde{H}_{\infty}\left(X\mid Z\right)-l$$

2.2　提取器

提取器[15]：若函数 $\mathrm{Ext}:\{0,1\}^u\times\{0,1\}^r\rightarrow\{0,1\}^v$ 是(m,ε)-强提取器。则对任意变量 X，Y 满足 $X\in\{0,1\}^u$ 以及 $\tilde{H}_{\infty}(X\mid Y)\geqslant m$，能够得到 $\Delta\left(\left(\mathrm{Ext}(X,S),S,Y\right),\left(U_v,S,Y\right)\right)\leqslant\varepsilon$，其中，$S$ 是 $\{0,1\}^r$ 的均匀随机分布。

ρ-通用散列函数族[15]：设 H 是由函数 $h:\{0,1\}^u\rightarrow\{0,1\}^v$ 所组成的函数族。若对任意 $a\neq b\in\{0,1\}^u$ 有 $\Pr_{h\leftarrow H}\left[h(a)=h(b)\right]\leqslant\rho$，则称 H 为 ρ-通用散列函数族。

残留散列引理[15]：假定由 $h:\{0,1\}^u\rightarrow\{0,1\}^v$ 组成的函数族 H 是ρ-通用散列函数族。若 $m\geqslant v+2\log(1/\varepsilon)-1$ 且 $\rho\leqslant\frac{1}{2^v}(1+\varepsilon^2)$，则称 $\mathrm{Ext}(x,h)=h(x)$ 为(m,ε)-强提取器。

残留散列引理表明任何通用散列函数族都是一个强提取器。

2.3　基于身份的散列证明系统

散列证明系统（HPS）由 Cramer 与 Shoup[16]提出，Alwen[8]等人把 HPS 推广到身份环境中，提出了基于身份的 HPS，即 IB-HPS。

IB-HPS 实际上是一个具有特殊结构的密钥封装方案，主要由多项式时间算法(Setup, KeyGen, Encap, Encap*, Decap)组成。

1) Setup(1^{λ})→(mpk,msk)：该算法以安全参数λ为输入，输出主公钥 mpk 和主密钥 msk。mpk 定义了身份的集合 ID，以及被封装的密钥集合 $\mathcal{K}$。以下算法 KeyGen，Encap，Encap*，Decap 都隐含地将 mpk 作为输入。

2) KeyGen(ID,msk)→$\mathrm{sk}_{\mathrm{ID}}$：对任何身份 $\mathrm{ID}\in ID$，该算法以 ID、msk 为输入，输出该身份所对应的身份密钥 $\mathrm{sk}_{\mathrm{ID}}$。

3) Encap(ID)→(c,k)：该有效的密钥封装算法以身份 ID 为输入，输出为(c,k)，其中，c 为有效密文，$k\in\mathcal{K}$ 为被封装的密钥。

4) Encap*(ID)→c：该无效的密钥封装算法以身份 ID 为输入，输出一个无效密文 c。

5) Decap(c,$\mathrm{sk}_{\mathrm{ID}}$)→$k$：该解封装算法以密文 c 和身份 ID 所对应的密钥 $\mathrm{sk}_{\mathrm{ID}}$ 为输入，输出被封装的

密钥 k。

IB-HPS 满足如下性质。

1) 解封装的正确性

对任何由算法 Setup(1^{λ})生成的主公钥与主私钥(mpk, msk)以及任何身份 $\mathrm{ID}\in ID$，均有

$$\Pr\left[k\neq k' \,\middle|\, \begin{matrix}\mathrm{sk}_{\mathrm{ID}}\leftarrow \mathrm{KeyGen}(\mathrm{ID},\mathrm{msk})\\ (c,k)\leftarrow \mathrm{Encap}(\mathrm{ID}),\ k'=\ \mathrm{Decap}(c,\mathrm{sk}_{\mathrm{ID}})\end{matrix}\right]$$

$\leqslant \mathrm{negl}(\lambda)$。

2) 不可区分性

对攻击者来说，即使知道身份密钥 $\mathrm{sk}_{\mathrm{ID}}$，Encap 算法产生的有效密文与 Encap*算法产生的无效密文之间也是不可区分的。

3) 平滑性

如果对任何由算法 Setup(1^{λ})生成的(mpk,msk)以及对任何 $\mathrm{ID}\in ID$，有：

$$\Delta\big((c,k),(c,k')\big)\leqslant \mathrm{negl}(\lambda)$$

其中，$c\leftarrow$Encap*(ID)，$k'\leftarrow U_K$ 以及 k 是通过选择 $\mathrm{sk}_{\mathrm{ID}}\leftarrow$KeyGen(ID, msk)，并计算 $k\leftarrow$Decap(c,$\mathrm{sk}_{\mathrm{ID}}$)而获得，则称 IB-HPS 是平滑的。

3 抗自适应泄漏的 IBE 方案

本节首先定义 IBE 中抗自适应泄漏的安全性，然后构造符合安全性定义的 IBE 方案。

3.1 安全性定义

在设计抗自适应泄漏的 IBE 方案之前，首先根据熵抗泄漏的概念给出自适应泄漏攻击下 IBE 的安全性定义。熵抗泄漏[13]是指：假设攻击者在得到挑战密文后获得了 k bit 的泄漏信息，那么攻击者得到的关于消息明文的信息量也不会超过 k bit，即消息明文仍旧保持了较大的最小熵，那么就称这个加密方案是熵抗泄漏的，也即抗自适应泄漏的。

一个普通的 IBE 方案Ψ主要由多项式时间算法(Setup, KeyGen, Encrypt, Decrypt)组成。下面通过攻击者与挑战者之间的一系列游戏定义抗选择明文攻击 IBE 的自适应泄漏安全性。这个安全游戏依赖于以下参数：m 是消息明文在泄漏之前的最小熵，l_{pre} 和 l_{post} 分别限制了挑战密文产生之前和之后能够容忍的泄漏量。所有这些参数都是安全参数λ的函数。

1) Setup：挑战者运行 Setup 并转发主公钥 mpk 给攻击者 A。

2) Pre-Challenge Query：在该阶段攻击者 A 自适应地对挑战者进行下列查询。

① 密钥查询：若输入是身份 $\mathrm{ID}\in ID$，则挑战者用该身份所对应的身份密钥 $\mathrm{sk}_{\mathrm{ID}}$ 做出响应。

② 泄漏查询：若输入是身份 $\mathrm{ID}\in ID$，以及概率多项式函数 $f^{\mathrm{pre}}(\cdot)$，如果 f^{pre} 的输出长度最多是 l_{pre}，则挑战者用 $f^{\mathrm{pre}}(\mathrm{sk}_{\mathrm{ID}})$ 做出响应（否则挑战者拒绝响应）。

3) Challenge：攻击者 A 随机选择 2 个消息 $\mathrm{m}_0,\mathrm{m}_1\in \mathcal{M}$以及挑战的身份 $\mathrm{ID}^*\in ID$；注意：该身份从未在密钥查询阶段出现，且最多在泄漏查询中泄漏了 $l_{\mathrm{pre}}+l_{\mathrm{post}}$；挑战者随机选择$b\in\{0,1\}$，并计算 Encrypt ($\mathrm{ID}^*$, m_b)$\rightarrow c$；最后送密文 c 给攻击者 A。

4) Post-Challenge Query：在该阶段攻击者 A 自适应地对挑战者进行下列查询。

① 密钥查询：攻击者 A 自适应地向挑战者进行身份 $\mathrm{ID}\neq\mathrm{ID}^*$查询，挑战者用 $\mathrm{sk}_{\mathrm{ID}}$ 做出响应。

② 泄漏查询：若输入是身份 $\mathrm{ID}\in ID$，以及概率多项式函数 $f^{\mathrm{post}}(\cdot)$，如果 f^{post} 的输出长度最多是 l_{post}，则挑战者用 $f^{\mathrm{post}}(\mathrm{sk}_{\mathrm{ID}})$ 做出响应（否则挑战者拒绝响应）。

注意，在 Pre-Challenge Query 与 Post-Challenge Query 中，挑战者在第一次对 ID 查询获得 $\mathrm{sk}_{\mathrm{ID}}\leftarrow$KeyGen(ID,msk)后，仍使用同样的 $\mathrm{sk}_{\mathrm{ID}}$ 做出对同样的 ID 查询的响应。

$$\mathrm{View}_A(\Psi)=\big(\mathrm{randomness},\mathrm{mpk},f^{\mathrm{pre}}(\mathrm{sk}_{\mathrm{ID}}),c,f^{\mathrm{post}}(\mathrm{sk}_{\mathrm{ID}})\big)$$

表示在上述游戏中攻击者 A 能获取的信息集合，M 表示游戏开始时选择的消息。

定义 1 抗自适应泄漏的 IBE：给定上文中定义的参数 m、l_{pre}、l_{post} 以及另一个“松弛参数”δ，对于 IBE 方案 Ψ=(Setup,KeyGen,Encrypt,Decrypt)，对任一 PPT 攻击者 A，如果满足以下 2 个条件。

① IBE 方案满足解密的正确性。

② M 的平均最小熵：

$\tilde{H}_{\infty}\left(M|\mathrm{View}_A(\Psi)\right)\geqslant m-l_{\mathrm{post}}-\delta$。

那么，这个 IBE 方案是抗自适应泄漏的。由②可知，除去挑战密文产生之后 l_{post}bit 的泄漏以及δbit 可能的“负载”，M 依旧保持了原始的熵，符合熵抗泄漏的定义。

3.2 方案构造

在 2.3 节介绍 IB-HPS 基础上，下面提出抗自适应泄漏的 IBE 方案。此时 Encap*并不出现在构建中，只是在该方案的安全性证明中使用。

定义 ID 为身份空间，M 为报文空间，封装

密钥的大小为 $t_1$bit，即 $K=\{0,1\}^{t_1}$。$\mathrm{Ext}:\{0,1\}^{t_1}\times\{0,1\}^{t_2}\to\{0,1\}^{t_3}$ 是(t_4,ε)-强提取器，该提取器有 $t_1$bit 的输入，$t_2$bit 的种子，$t_3$bit 的输出，并且对于一个随机种子和一个最小熵为 $t_4$bit 的输入，输出是ε接近于 $t_3$bit 的均匀分布。构造的 IBE 方案 Ψ=(Setup, KeyGen, Encrypt, Decrypt)如下。

1) Setup(1^λ)：该算法以安全参数λ为输入，输出主公钥 mpk 和主密钥 msk。mpk 定义了身份的集合 ID，以及被封装的密钥集合 K。以下算法 KeyGen，Encrypt，Decrypt 都隐含地将 mpk 作为输入。

2) KeyGen(ID,msk)：该算法以 $\mathrm{ID}\in ID$ 与 msk 为输入，输出该身份所对应的身份密钥 $\mathrm{sk}_{\mathrm{ID}}$。

3) Encrypt(ID,m)：该加密算法以 $\mathrm{ID}\in ID$ 与 $m\in\{0,1\}^{t_3}$ 为输入，首先调用密钥封装算法 Encap(ID)生成(c_1,k)；然后提取一个随机种子 $s\in\{0,1\}^{t_2}$，计算 $c_m=\mathrm{Ext}(k,s)\oplus m$；最后输出密文 c=(c_1,s,c_m)。

4) Decrypt(c, $\mathrm{sk}_{\mathrm{ID}}$)：该解密算法首先解析 c=(c_1,s,c_m)；然后调用解封装算法 Decap(c_1, $\mathrm{sk}_{\mathrm{ID}}$)得到被封装的密钥 k；最后输出 $m=\mathrm{Ext}(k,s)\oplus c_m$。

4　安全性证明与分析

本节根据安全性定义给出上述 IBE 方案 Ψ的安全性证明，并分析该方案能够容忍的密钥泄漏量。

下面首先给出方案的安全性证明。

1) 解密的正确性：根据 IB-HPS 解封装的正确性，显然该方案 Ψ满足解密的正确性，即解密算法能正确地恢复出原始明文。

2) 证明方案 Ψ是抗自适应泄漏的，即消息 m 能保持至少($t_3-l_{\mathrm{post}}-\delta$)bit 的平均最小熵，证明过程如下。

引理 1　在泄漏参数分别是 l_{pre}、l_{post} 以及“负载”是δ的 IBE 方案 Ψ中，只要满足 $l_{\mathrm{pre}}\leqslant\log|K|-t_4$，$\delta\leqslant t_3-\log\dfrac{1}{2^{-t_3}+\varepsilon}$，则该 IBE 方案 Ψ是抗自适应泄漏的。

证明　首先在安全性游戏中，对挑战阶段进行修改，让挑战者使用无效的封装过程计算密文 c，即

$c_1\leftarrow\mathrm{Encap}^*(\mathrm{ID})$，

$k\leftarrow\mathrm{Decap}(c_1,\mathrm{sk}_{\mathrm{ID}})$，

$c_m=\mathrm{Ext}(k,s)\oplus m$，

c=(c_1,s,c_m)。

根据 IB-HPS 中有效密文与无效密文的不可区分性可知，修改过后的游戏与原游戏是计算不可区分的。所以接下来仅仅需要在修改过的安全性游戏下证明该方案是否能使消息 m 保持至少($t_3-l_{\mathrm{post}}-\delta$)的平均最小熵。证明包括以下 2 步。

① 证明从 Setup 到 Challenge 阶段，在攻击者获取了所有泄漏信息的情况下，消息 m 仍然具有较高的平均最小熵，即至少 $t_3-\delta$。

设 f^{pre} 是具有 l_{pre} 输出的泄漏函数；$\mathrm{SK}_{\mathrm{ID}}$、$C_1$、$K$ 分别是由 KeyGen(ID,msk)、Encap*(ID)、Decap(C_1, $\mathrm{SK}_{\mathrm{ID}}$)生成的随机变量，$S$ 是随机独立的提取器种子；概率函数 $f'^{\mathrm{pre}}(c_1,k)$ 条件分布 $(\mathrm{SK}_{\mathrm{ID}}\,|\,C_1=c_1, K=k)$ 中提取样本 $\mathrm{sk}_{\mathrm{ID}}$，输出 $f^{\mathrm{pre}}(\mathrm{sk}_{\mathrm{ID}})$。则有：

$$\left\langle C_1,S,f^{\mathrm{pre}}(\mathrm{SK}_{\mathrm{ID}}),\mathrm{Ext}(K,S)\right\rangle$$

$$\equiv\left\langle C_1,S,f'^{\mathrm{pre}}(C_1,K),\mathrm{Ext}(K,S)\right\rangle \tag{1}$$

$$\approx\left\langle C_1,S,f'^{\mathrm{pre}}(C_1,U_K),\mathrm{Ext}(U_K,S)\right\rangle \tag{2}$$

$$\approx\left\langle C_1,S,f'^{\mathrm{pre}}(C_1,U_K),U_{t_3}\right\rangle \tag{3}$$

$$\approx\left\langle C_1,S,f'^{\mathrm{pre}}(C_1,K),U_{t_3}\right\rangle \tag{4}$$

$$\equiv\left\langle C_1,S,f^{\mathrm{pre}}(\mathrm{SK}_{\mathrm{ID}}),U_{t_3}\right\rangle \tag{5}$$

上述公式中，从式(1)到式(2)由 IB-HPS 的平滑性直接可以得到；对于从式(2)到式(3)，由平均最小熵定义可知，$\tilde{H}_\infty\left(U_K\,|\,C_1,f'^{\mathrm{pre}}(C_1,U_K)\right)\geqslant\tilde{H}_\infty(U_K\,|\,C_1)-l_{\mathrm{pre}}$，由 C_1,U_K 是相互独立的可知，$\tilde{H}_\infty(U_K\,|\,C_1)-l_{\mathrm{pre}}\geqslant\log|K|-l_{\mathrm{pre}}\geqslant t_4$，接着根据提取器定义可得式(3)；由式(3)到式(4)根据 IB-HPS 的平滑性直接可得。根据式(5)可知，即使攻击者获得了 c_1、随机种子 s 和 Pre-Challenge Query 的泄漏信息，提取器 $\mathrm{Ext}(k,s)$ 的输出结果依然是极其接近于随机分布的。所以消息 m 是ε-接近均匀随机分布 $\{0,1\}^{t_3}$ 的（即使给定 c_1、随机种子 s、Pre-Challenge Query 的泄漏信息和值 c_m）。也就是说，直到 Challenge 阶段，消息 m 依然有至少($t_3-\delta$)bit 的平均最小熵。

② 证明在 Post-Challenge Query 后，m 最终还有至少($t_3-l_{\mathrm{post}}-\delta$)bit 的平均最小熵。显而易见，因为 Post-Challenge Query 的泄漏查询最多是 l_{post} bit，也即 Post-Challenge Query 的泄漏查询后，m 的最小熵最多减少 l_{post}bit，所以 m 还有至少($t_3-l_{\mathrm{post}}-\delta$)bit 的平均最小熵。

至此证明了该 IBE 方案 Ψ 是抗自适应泄漏的。

下面分析该方案能够容忍的密钥泄漏量。

定理 1 只要该 IBE 方案 Ψ 中使用的提取器非常好，如果引理 1 成立，那么该 IBE 方案能够容忍挑战密文产生之前的泄漏量为 $t_1\left(1-o(1)\right)$。

证明 因为该 IBE 方案 Ψ 中使用的提取器非常好，即对于最小熵 $t_4<<\log|K|=t_1$ 的输入，输出结果与均匀分布 $\{0,1\}^{t_3}$ 之间的统计距离 $\varepsilon<2^{-t_3}$。则根据引理 1，该方案能容忍挑战密文产生之前的泄漏 $l_{\text{pre}}\leqslant\log|K|-t_4\approx t_1-t_4=t_1\left(1-o(1)\right)$，负载 $\delta<1$ bit。

可见，该 IBE 方案 Ψ 能够容忍较大的密钥泄漏量，允许密钥泄漏量几乎等于密钥总量。

5 实例化

本节首先对上述自适应泄漏安全的 IBE 方案 Ψ 进行实例化，然后对该实例化方案进行效率分析，证明其能够容忍较大的密钥泄漏量，并且是计算可行的。

5.1 基于 q-TABDHE 假设的抗自适应泄漏的 IBE 方案

下面在基于 q-TABDHE 假设的 IB-HPS[8]的基础上，按照 3.2 节的抗自适应泄漏 IBE 方案构造方法，设计基于 q-TABDHE 假设的 IBE 方案。显然，该实例化方案也是抗自适应泄漏的。

基于 q-TABDHE 假设的抗自适应泄漏的 IBE 方案 $\Pi=(Set^{\text{Ins}},Gen^{\text{Ins}},Enc^{\text{Ins}},Dec^{\text{Ins}})$ 构建如下。其中，$\text{Ext}:G_T\times\{0,1\}^d\to\{0,1\}^\gamma$ 是 (t,ε)-强提取器，$t\leqslant\log(p)-l_{\text{pre}}$。

1) $\text{Set}^{\text{Ins}}(1^\lambda)$：设 $(G,G_T,g,e,p)\leftarrow\zeta(1^\lambda)$，其中，$G$ 与 G_T 是阶为 p 的循环群，g 是循环群 G 的生成元，以及 $e:G\times G\to G_T$ 为双线性映射。随机选取 $h\leftarrow G,\alpha\leftarrow Z_p$，并计算 $g_1:=g^\alpha$，定义主公钥 $\text{mpk}=(G,G_T,g,e,p,g_1,h)$，主密钥 $\text{msk}=\alpha$，身份空间 $ID=Z_p\setminus\{\alpha\}$，被封装的密钥集合 $K=G_T$。

2) $\text{Gen}^{\text{Ins}}(ID,\text{msk})$：对于任何身份 $\text{ID}\in ID$，该算法随机选择 $r_{\text{ID}}\in Z_p$，并计算 $h_{\text{ID}}=\left(hg^{-r_{\text{ID}}}\right)^{1/(\alpha-\text{ID})}$，输出 $\text{sk}_{\text{ID}}=(r_{\text{ID}},h_{\text{ID}})$。

3) $\text{Enc}^{\text{Ins}}(\text{ID},m)$：该加密算法以 $\text{ID}\in ID$ 与 $m\in\{0,1\}^\gamma$ 为输入，首先随机选取 $\beta\in Z_p$，调用密钥封装算法 Encap(ID) 生成 $c_1=((u,v),k)$，其中，$u=g_1^\beta g^{-\beta\text{ID}},v=e(g,g)^\beta,k=e(g,h)^\beta$；然后提取一个随机种子 $s\in\{0,1\}^d$，计算 $c_m=\text{Ext}(k,s)\oplus m$；最后输出密文 $c=(c_1,s,c_m)$。

4) $\text{Dec}^{\text{Ins}}(c,\text{sk}_{\text{ID}})$：该解密算法首先解析 $c=(c_1,s,c_m)$；然后调用解封装算法 $\text{Decap}(c_1,\text{sk}_{\text{ID}})$ 得到被封装的密钥 $k=e(u,h_{\text{ID}})v^{r_{\text{ID}}}$；最后输出 $m=\text{Ext}(k,s)\oplus c_m$。

5.2 效率分析

此实例化 IBE 方案 Π 的效率主要从容忍密钥泄漏量和计算可行性 2 个方面来分析。

首先分析该方案能够容忍的密钥泄漏量。该方案中实际的身份密钥大小为 $2\log(p)+o(1)$，其中，有效的身份密钥大小（sk_{ID} 能够取值的总数的对数）为 $\log(p)$，被封装的密钥大小为 $\log(p)$。由定理 1 可知，允许挑战密文产生之前的密钥泄漏量 l_{pre} 为 $\log(p)(1-o(1))$，几乎等于有效密钥总量。那么不管挑战密文产生之后的泄漏量 l_{post} 是多少，总泄漏量 $l_{\text{pre}}+l_{\text{post}}$ 都几乎达到有效密钥总量，即该方案能够容忍较大的密钥泄漏量。

下面考察该方案的计算可行性。为了实现抗自适应泄漏，该方案在基于 q-TABDHE 假设的 IB-HPS[8]的基础上，在加密和解密步骤中分别增加了一个强提取运算以及一个异或运算。根据 2.2 节中的残留散列引理可知，强提取器可由通用散列函数族实现。目前已知的许多通用散列函数族[17~19]都是有效的，即函数族是多项式时间内可求解的。所以该实例化 IBE 方案是计算可行的。

6 结束语

传统意义上，密码学方案在证明其安全性时假定密钥对攻击者来说是完备保密的。但事实上，诸多称之为边信道攻击，例如时间攻击、电源损耗、冷启动攻击、音频分析等攻击均能从保密密钥或者加密系统的内部状态提取出部分关于密钥的信息，从而泄漏系统或者密钥的安全性。随着 20 世纪 90 年代边信道攻击的提出，抗泄漏密码学逐渐成为国际密码学领域中的一个研究热点。本文分析了现有的抗泄漏加密方案，发现抗自适应泄漏攻击是目前的研究难点之一。本文为解决 IBE 环境中如何抗自适应泄漏的问题，借鉴 Halevi 和 Lin 提出的熵抗泄漏的思想，定义了自适应泄漏攻击下的 IBE 安全性；

结合基于身份的散列证明系统和提取器，提出了抗自适应泄漏的 IBE 方案；基于 q-TABDHE 困难性假设，设计了抗自适应泄漏的实例化 IBE 方案。安全性分析表明，构建的 IBE 方案是选择明文攻击安全的，它不仅能够成功抵抗自适应泄漏，而且能够容忍较大的密钥泄漏量。

本文所提出的 IBE 方案主要抵抗身份密钥泄漏，如何把它转换为既容忍身份密钥泄漏，又允许主密钥泄漏的加密方案是下一步的工作重点。

参考文献：

[1] KOCHER P. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems[A]. CRYPTO 1996[C]. Santa Barbara, California, USA, 1996. 104-113.

[2] KOCHER P, JAFFE J, JUN B. Differential power analysis[A]. CRYPTO 1999[C]. Santa Barbara, California, USA, 1999. 388-397.

[3] ISHAI Y, SAHAI A, WAGNER D. Private circuits: securing hardware against probing attacks[A]. CRYPTO 2003[C]. Santa Barbara, California, USA, 2003. 463-481.

[4] MICALI S, REYZIN L. Physically observable cryptography[A]. TCC 2004[C]. Cambridge, MA, USA, 2004. 278-296.

[5] DZIEMBOWSKI S, PIETRZAK K. Leakage-resilient cryptography[A]. FOCS 2008[C]. Philadelphia, PA, USA, 2008. 293-302.

[6] AKAVIA A, GOLDWASSER S, VAIKUNTANATHAN V. Simultaneous hardcore bits and cryptography against memory attacks[A]. TCC 2009[C]. San Francisco, CA, USA, 2009. 474-495.

[7] NAOR M, SEGEV G. Public-key cryptosystems resilient to key leakage [A]. CRYPTO 2009[C]. Santa Barbara, California, USA, 2009. 18-35.

[8] ALWEN J, DODIS Y, NAOR M, *et al*. Public-key encryption in the bounded-retrieval model[A]. EUROCRYPT 2010[C]. Monaco and Nice, French Riviera, 2010. 113-134.

[9] BRAKERSKI Z, KALAI Y T, KATZ J, *et al*. Cryptography resilient to continual memory leakage[A]. FOCS 2010[C]. Las Vegas, Nevada, USA, 2010. 501-510.

[10] JUMA A, VAHLIS Y. Protecting cryptographic keys against continual leakage[A]. CRYPTO 2010[C]. Santa Barbara, California, USA,2010. 41-58.

[11] GOLDWASSER S, ROTHBLUM G N. Securing computation against continuous leakage[A]. CRYPTO 2010[C]. Santa Barbara, California, USA, 2010. 59-79.

[12] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[A]. STOC 2005[C]. 2005. 84-93.

[13] HALEVI S, LIN H J. After-the-fact leakage in public-key encryption[A]. TCC 2011[C]. 2011. 107-124.

[14] GOLDREICH O. Foundations of Cryptography: Volume 1-Basic Tools[M]. New York: Cambridge University Press, 2001.

[15] DODIS Y, OSTROVSKY R, REYZIN L, *et al*. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data[J]. SIAM Journal on Computing, 2008, 38(1): 97-139.

[16] CRAMER R, SHOUP V. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption[A]. EUROCRYPT 2002[C]. Amsterdam, 2002. 45-64.

[17] CARTER J L, WEGMAN M N. Universal classes of hash functions[J]. Journal of Computer and System Sciences, 1979, 18: 143-154.

[18] CARTER J L, WEGMAN M N. New hash functions and their use in authentication and set equality[J]. Journal of Computer and system sciences, 1981, 22: 265-279.

[19] HASTAD J, IMPAGLIAZZO R, LEVIN L A, *et al*. A pseudorandom generator from any one-way function[J]. SIAM Journal on Computing, 1999, 28(4): 1364-1396.

作者简介：

汤佳惠（1987-），女，江苏溧阳人，苏州大学硕士生，主要研究方向为网络与信息安全。

朱艳琴（1964-），女，江苏苏州人，博士，苏州大学教授，主要研究方向为计算机网络和信息安全。

罗喜召（1978-），男，河南漯河人，博士，苏州大学讲师，主要研究方向为密码学和计算复杂度。