标准模型下增强的无需安全信道的带关键词搜索的公钥加密

方黎明 黄志球 王建东
(南京航空航天大学计算机科学与技术学院 南京 210016)

摘 要 Baek,Safavi-Naini和Susilo提出了无需安全信道的带关键词搜索的公钥加密方案。该方案中的安全模型限制了攻击者的能力,并且方案是在随机预言模型下可证安全的。然而在随机预言模型下证明安全的方案在实际执行中会导致不安全。通过改进安全模型使得攻击者能力更强,即允许攻击者获得非挑战密文和陷门之间的关系,同时构造了在增强的安全模型下不使用随机预言机可证安全的带关键词搜索的公钥加密方案。

关键词 公钥加密,可搜索加密,无需安全信道,标准模型
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.11.041

Secure Channel Free Searchable Encryption in Standard Model

FANG Li-ming HUANG Zhi-qiu WANG Jian-dong
(College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract Recently, Baek et al. proposed an efficient public key encryption scheme with keyword search based on the scheme of Boneh et al. However, the security model of Baek et al. seriously limits the ability of the adversary. Rhee et al. enhanced the security model of the public key encryption with keyword search to properly incorporate the ability of an adversarys, and presented a PEKS in the random oracle model. Unfortunately, a proof in the random oracle model has shown that it possibly leads to insecure schemes when the random oracles are implemented in the standard model. This paper constructed an efficient public key encryption scheme with keyword search secure in the enhanced security model without random oracle.

Keywords Public key encryption, Searchable encryption, Secure channel free, Standard model

1 引言

随着互联网、云计算的发展,用户需要存储加密后的数据在云端,此时需要对密文进行搜索,于是提出了带关键词搜索的加密。典型的应用如下:假设Bob想发送加密的电子邮件给Alice,为了确保除Alice之外的任何人都不能解密电子邮件,Bob在发送电子邮件之前使用Alice的公钥加密该邮件,因此只有Alice拥有解密的能力。然而加密后的电子邮件是完全随机的,服务者(邮件服务器)将无法进行智能路由。比如,Alice想用她的手机接收那些包含关键词"紧急"的邮件,而其它关键词的邮件希望路由(下载)到电脑上以便读取。那么Alice需要与邮件服务者之间建立一种密文匹配机制,即服务者在不解密邮件密文的条件下测试(TEST)邮件是否包含关键词"紧急"。

文献[4]给出了一个基本的解决方案,即带关键词搜索的公钥加密方案(PEKS)。在Boneh等人[4]提出的方案之后,Waters等人[10]指出带关键词搜索的公钥加密方案能够被用来建立可搜索的加密日志审查。Golle,Staddon和Waters[11]构造了允许对加密数据的多关键词联接的搜索[14]。文献[18]提出了如何根据匿名的基于身份加密构造支持多关键词模糊匹配的可搜索公钥加密方案的通用构造方法。关键词往往来自于小的集合,而且普通用户经常使用大家熟知的关键词(如紧急、旅游等)来加密,文献[7,13,16,19]研究了关键词猜测攻击带关键词搜索的公钥加密。鉴于之前研究的带关键词搜索的公钥加密方案只提供了搜索方案,而没有提供用户解密加密后的信息的能力,文献[12,20]研究了可解密的带关键词搜索的加密方案。更进一步,Rhee,Park和Lee[17]提出了无需安全信道的可搜索公钥加密的一般化构造方法。文献[21]研究了基于模糊关键词搜索的无需安全信道的公钥加密方案,文献[22]提出了一种安全的匿名可搜索的加密方案,文献[24]提出了基于属性可搜索加密方案,文献[23]研究了云存储环境下多用户可搜索加密方案,文献[25]综述了PEKS中安全信道问题、改进查询功能等方面的研究成果。

文献[4]中方案的缺点是在Alice和服务者(邮件服务器)之间需要安全信道来发送陷门,而这个开销往往非常昂贵。于是,Baek,Safavi-Naini和Susilo[2]构造了无需安全信道

到稿日期:2014-11-12 返修日期:2015-02-19 本文受国家自然科学基金项目(61272083,61300236),江苏省自然科学基金青年项目(BK20130809),中国博士后科学基金(2013M530254),中国博士后科学基金特别资助(2014T70518),江苏省博士后基金(1302137C),中央高校基本科研业务费专项资金(NZ2013306)资助。

方黎明(1983-),男,博士后,副教授,主要研究方向为信息安全、密码学,E-mail:fangliming@nuaa.edu.cn;黄志球(1965-),男,博士,教授,博士生导师,主要研究方向为云计算安全、软件工程;王建东(1945-),男,教授,博士生导师,主要研究方向为信息安全、数据挖掘。

的带关键词搜索的公钥加密方案。在 2007 年，Gu，Zhu 和 Pan[9]提出了一个基于 Baek，Safavi-Naini 和 Susilo 方案的更有效的无需安全信道的带关键词搜索的公钥加密方案。之后，Rhee 等人[15]指出 Baek，Safavi-Naini 和 Susilo 模型的安全模型虽然解决了安全信道的问题，但是没有能够完全解决现实环境中的攻击。首先，在 Baek 的安全模型中攻击者只能获得关键词相关的陷门，而不能获得陷门和关键词之间的测试结果。现实中，一个恶意的接收者（攻击者）能够自己产生所选关键词的陷门，并且通过与服务者交互得到陷门和密文之间的关系，从而实现攻击。Rhee 等人[15]通过增加测试查询增强了安全模型，使得攻击者能够获得非挑战密文和陷门之间的关系，并给出了随机预言机模型中增强模型下安全的无需安全信道的带关键词搜索的公钥加密方案。

虽然 Rhee 的无需安全信道的带关键词搜索的公钥加密方案已经很完美，但是其只能在随机预言模型下是可证安全的，文献[5]指出随机预言模型是一个理想化的模型，在该模型下所有的参与方都可以通过黑盒来访问真正随机的哈希函数。不幸的是，随机预言模型下的证明仅仅能被当作一个启发式的论据，实际环境中会导致不安全[5]。

本文提出了高效的无需安全信道的带关键词搜索的公钥加密方案。在标准模型下基于 DBDH 和 truncated q-ABDHE 假设证明方案的安全性。相比之前的方案，本方案有如下优点：

(1)本方案有更强的安全模型。本方案的安全模型允许攻击者获得非挑战密文和陷门之间的关系，也即攻击者能力更强，那么在这一增强模型下可证安全的方案的安全性更高。

(2)本方案的证明不依赖随机预言模型。在随机预言模型下被证明是安全的方案在实际应用中可能会不安全[5]。

2 背景知识

2.1 可忽略函数

函数 $\varepsilon(n):N\to R$ 被称为可忽略的，如果对于所有的 n，$1/\varepsilon(n)$是一个非多项式界的量。

2.2 双线性对

设 G_1，G_2 是阶数为素数 p 的循环群，g 是群 G_1 的生成元（G_1^*，Z_p^* 分别表示 $G_1\backslash\{1\}$，$Z_p\backslash\{0\}$）。称 $e:G_1\times G_1\to G_2$ 是一个双线性对[3]，当且仅当如下的条件成立：

1. $e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$，其中 $a,b\in Z_P$，$g_1,g_2\in G_1$；

2. $e(g,g)\neq 1$；

3. 对于所有的 $g_1,g_2\in G_1$，$e(g_1,g_2)$是可计算的。

2.3 DBDH 假设

设 $e:G_1\times G_1\to G_2$ 是一个双线性对，定义敌手 B 的攻击优势函数 $Adv_{G_1,B}^{DBDH}(\lambda)$如下：

$$|Pr[B(g,g^a,g^b,g^c,e(g,g)^{abc})]=1-Pr[B(g,g^a,g^b,g^c,e(g,g)^r)]=1|$$

其中，$a,b,c,r\in Z_p$ 是随机选取的。如果对于所有的概率多项式时间敌手 B，$Adv_{G_1,B}^{DBDH}(\lambda)$是可忽略的，那么基于双线性对的决定性 Difife-Hellman 假设[3,8]成立。

2.4 Truncated (Decisional) q-ABDHE 假设

设 $e:G_1\times G_1\to G_2$ 是一个双线性对，定义敌手 B 的优势函数 $Adv_{G_1,B}^{q\text{-}ABDHE}(\lambda)$如下：

$$|Pr[B(g,g^x,\cdots,g^{x^q},g^z,g^{zx^{q+2}},e(g,g)^{zx^{q+1}})]=1-Pr[B(g,g^x,\cdots,g^{x^q},g^z,g^{zx^{q+2}},e(g,g)^r)]=1|$$

其中，$x,z,r\in Z_p$ 是随机选取的。如果对于所有的概率多项式时间敌手 B，$Adv_{G_1,B}^{q\text{-}ABDHE}(\lambda)$是可忽略的，那么决定性 Truncated q-ABDHE 假设[8]成立。

2.5 强不可伪造一次签名

强不可伪造一次签名[6]包含一个三元组算法 $Sig=(G,S,V)$。输入参数 λ，G 产生一对密钥（ssk,svk）。对于任意消息 M，当 $\sigma=S(ssk,M)$时 $V(svk,\sigma)=1$，否则 $V(svk,\sigma)=0$。强不可伪造一次签名指没有任何概率多项式时间攻击者 A 能够伪造一个新签名，即使是对曾经签过名的消息。

$Sig=(G,S,V)$是一个强不可伪造一次签名，当且仅当下面时间对于任何概率多项式时间伪造者 F 的概率是可忽略的：

$$\begin{aligned}Adv^{OTS}=Pr[&(ssk,svk)\leftarrow G(\lambda);\\&(m,St)\leftarrow F(svk);\sigma\leftarrow S(ssk,m);\\&(m',\sigma')\leftarrow F(m.,\sigma,svk,St):V(svk,\sigma',m')=\\&1\wedge(m',\sigma')\neq(m,\sigma)]\end{aligned}$$

其中，St 表示各个阶段 F 所获得的状态信息。

2.6 无需安全信道的带关键词搜索的公钥加密定义

定义 1（无需安全信道的带关键词搜索的公钥加密） 无需安全信道的带关键词搜索的公钥加密方案包含如下几个算法：

$-GloSetup(\lambda)$：输入安全参数 λ，输出全局公共参数 GP。

$-KeyGen_{receiver}(GP)$：以公共参数 GP 为输入，输出接收者 R 的公私钥对（pk_R,sk_R）。

$-KeyGen_{sever}(GP)$：以公共参数 GP 为输入，输出服务者 S 的公私钥对（pk_S,sk_S）。

$-SCF\text{-}PEKS(GP,pk_R,pk_S,\omega)$：输入公共参数 GP、接收者的公钥 pk_R、服务者的公钥 pk_S、关键词 ω，返回一个用关键词 ω 加密的 PEKS 密文 C。

$-Trapdoor(CP,sk_R,\omega)$：输入公共参数 GP、接收者的私钥 sk_R，以及关键词 ω，输出陷门 T_ω。

$-Test(GP,sk_S,C,T_\omega)$：输入公共参数 GP、服务者的私钥 sk_S、陷门 T_ω，以及 PEKS 密文 C，其中 $C=SCF\text{-}PEKS(GP,pk_R,pk_S,\omega')$。如果 $\omega=\omega'$，输出“Correct”；否则输出“Incorrect”。

类似文献[1]的一致性定义，无需安全信道的带关键词搜索的公钥加密方案的一致性定义如下。

定义 2（一致性） 假设存在一个敌手 A 想破坏方案的一致性，形式化地定义如下：

$Exp_A^{cms}(\lambda)$

$(pk_R,sk_R)\leftarrow KeyGen_{receiver}(GP)$；

$(pk_S,sk_S)\leftarrow KeyGen_{sever}(GP)$

$(\omega,\omega')\leftarrow A(pk_R,pk_S)$

$C\leftarrow SCF\text{-}PEKS(GP,pk_R,pk_S,\omega)$；

$T_{\omega'}\leftarrow Trapdoor(GP,sk_R,\omega')$

if $\omega\neq\omega'$ and $Test(GP,sk_S,C,T_{\omega'})=$“Correct”

then return 1,

else return 0。

其中 A 的优势如下：

$Adv_A^{cms}(\lambda)=Pr[Exp_A^{cms}(\lambda)=1]$

如果所有的概率多项式时间的敌手 A 赢得上述游戏的概率都是可忽略的，则方案是计算一致性的。

接下来给出无需安全信道的带关键词搜索的公钥加密的安全性定义，即无需安全信道的带关键词搜索的公钥加密抵抗选择关键词攻击的不可区分性（IND-DT-CKA）。与文献[2]类似，IND-DT-CKA 保证了在可以获得任何非挑战关键词陷门的情况下没有任何服务者能区分 PEKS 密文是由他所选择的关键词 ω_0、ω_1 中的哪个关键词加密得到的；并且，任何没有获得服务者私钥的外部攻击者（包括接收者）不能区分 PEKS 密文是由他所选择的关键词 ω_0、ω_1 中的哪个关键词加密得到的，即使他可以获得非挑战密文和陷门之间的关系。具体定义如下：

定义 3（IND-DT-CKA 游戏） λ 是安全参数，A 是攻击者。考虑下面的攻击者 A 和模拟者 B 的两个游戏。

游戏 1：假设 A 是服务者。

1. 系统建立：公共参数产生算法 $GloSetup(\lambda)$ 和两个密钥产生算法 $KeyGen_{receiver}(GP)$、$KeyGen_{sever}(GP)$ 被执行，产生公共参数 GP 及接收者和服务者的公私钥对 (pk_R, sk_R)、(pk_S, sk_S)，接着模拟者 B 把 (pk_S, sk_S) 和 pk_R 发送给攻击者 A。

2. 查询阶段一：攻击者 A 做如下查询：

· 陷门查询 $\langle\omega\rangle$：A 询问 B 关于关键词 ω 的陷门，B 返回给 A 陷门 $T_\omega=Trapdoor(GP, sk_R, \omega)$。

· 测试查询 $\langle C,\omega\rangle$：A 询问 B 关于关键词 ω 和 PEKS 密文的测试查询。B 首先做一个陷门查询 $\langle\omega\rangle$ 来得到陷门 T_ω，B 返回给 A 算法 $Test(GP, T_\omega, sk_S, C)$ 的结果。

3. 挑战：A 一旦决定查询阶段一结束，输出挑战关键词对 (ω_0, ω_1)（注意，ω_0、ω_1 不能是查询阶段一中 A 所做的任何陷门查询的关键词）。收到挑战关键词对后，B 随机地选择 $b\in\{0,1\}$，并且产生挑战密文 $C^*=SCF\text{-}PEKS(GP, pk_R, pk_S, \omega_b)$ 发送给 A。

4. 查询阶段二：A 做与阶段一相同的查询，唯一的限制是 A 不能对 ω_0、ω_1 做陷门查询，并且如果 $\langle C,\omega\rangle=\langle C^*,\omega_0\rangle$ 或者 $\langle C,\omega\rangle=\langle C^*,\omega_1\rangle$，则不允许做 $\langle C,\omega\rangle$ 的测试查询。

5. 猜测：攻击者输出他的猜测 b'。如果 $b=b'$，则攻击者获得胜利。

定义游戏 1 中攻击者 A 的优势：$Adv_A^{Game_1}(\lambda)=|Pr[b=b']-1/2|$。

游戏 2：假设 A 是外部的攻击者（包括接收者）。

1. 系统建立：公共参数产生算法 $GloSetup(\lambda)$ 和两个密钥产生算法 $KeyGen_{receiver}(GP)$、$KeyGen_{sever}(GP)$ 被执行，产生公共参数 GP 及接收者和服务者的公私钥对 (pk_R, sk_R)、(pk_S, sk_S)，接着模拟者 B 把 (pk_R, sk_R) 和 pk_S 发送给攻击者 A。

2. 查询阶段一：攻击者 A 做如下查询：

· 陷门查询 $\langle\omega\rangle$：A 询问 B 关于关键词 ω 的陷门，B 返回给 A 陷门 $T_\omega=Trapdoor(GP, sk_R, \omega)$。

· 测试查询 $\langle C,\omega\rangle$：A 询问 B 关于关键词 ω 和 PEKS 密文 C 的测试查询。B 首先做一个陷门查询 $\langle\omega\rangle$ 来得到陷门 T_ω，B 返回给 A 测试 $Test(GP, T_\omega, sk_S, C)$ 的结果。

3. 挑战：A 一旦决定查询阶段一结束，输出挑战关键词对 (ω_0, ω_1)（注意，ω_0、ω_1 不能是查询阶段一中 A 所做的任何陷门查询相关的关键词）。收到挑战关键词对后，B 随机地选择 $b\in\{0,1\}$，并且产生挑战密文 $C^*=SCF\text{-}PEKS(GP, pk_R, pk_S, \omega_b)$ 发送给 A。

4. 查询阶段二：A 做与阶段一相同的查询，限制是如果 $\langle C,\omega\rangle=\langle C^*,\omega_0\rangle$ 或者 $\langle C,\omega\rangle=\langle C^*,\omega_1\rangle$，则不允许做 $\langle C,\omega\rangle$ 的测试查询。与游戏 1 不一样，ω_0、ω_1 这里被允许做陷门查询。

5. 猜测：攻击者输出他的猜测 b'，如果 $b=b'$，则攻击者获得胜利。

定义游戏 1 中攻击者 A 的优势：$Adv_A^{Game_1}(\lambda)=|Pr[b=b']-1/2|$。如果 $Adv_A^{Game_i}(\lambda)$，$i=1$ 或 2 是可忽略的，那么无需安全信道的带关键词搜索的公钥加密方案是 IND-SCF-CKA 安全的。

3 增强的无需安全信道的带关键词搜索的公钥加密方案构造

接下来将给出增强的无需安全信道的带关键词搜索的公钥加密的方案构造及安全性证明。

3.1 方案构造

方案构造如下：

· $GloSetup(\lambda)$：λ 是安全参数，设 (p, g, G_1, G_2, e) 为双线性对的参数。选择单向哈希函数 $H:\{0,1\}^*\rightarrow Z_p^*$，设关键词域为 $KS_\omega=Z_p^*$。随机产生 $u, v\in G_1$ 和强不可伪造一次签名 $Sig=(G,S,V)$。输出全局公共参数 $GP=(p, g, G_1, G_2, e, u, v, Sig, H, KS_\omega)$。

· $KeyGen_{sever}(GP)$：随机选择 $x\in Z_P^*$，计算 $X=g^x$，随机选择 $Q\in G_1^*$，输出服务者的公私钥对 (pk_S, sk_S)，其中 $pk_S=(GP, X, Q)$，$sk_S=(pk_S, x)$。

· $KeyGen_{receiver}(GP)$：随机选择 $y\in Z_P^*$，计算 $Y=g^y$，随机选择 $h\in G_1^*$，输出接收者的公私钥对 (pk_R, sk_R)，其中 $pk_R=(GP, Y, h)$，$sk_S=(pk_R, y)$。

· $PEKS(GP, pk_R, pk_S, \omega)$：

1. 选择强不可伪造一次签名密钥对 $(ssk, svk)\leftarrow G(\lambda)$，设置 $C_0=svk$。

2. 随机选择 $s, r\in Z_p^*$，计算 $C_1=g^s$，$t=H(e(X,Q)^s)$，$C_2=(Yg^{-\omega})^{r/t}$，$C_3=e(g,g)^r$，$C_4=e(g,h)^r$，$C_5=(u^{svk}v)^s$。

3. 对五元组 $(C_1, C_2, C_3, C_4, C_5)$ 产生一个强不可伪造一次签名 $\sigma=S(ssk, (C_1, C_2, C_3, C_4, C_5))$。

4. PEKS 密文为 $C=(C_0, C_1, C_2, C_3, C_4, C_5, \sigma)$。返回 C。

· $Trapdoor(GP, sk_R, \omega)$：随机选择 $s_\omega\in Z_p^*$，计算 $d_\omega=(hg^{-s_\omega})^{1/(y-\omega)}$，陷门为 $T_\omega=(s_\omega, d_\omega)$，返回 T_ω。

· $Test(GP, sk_S, C, T_\omega)$：验证下面几个等式是否成立：

$V(C_0, \sigma, (C_1, C_2, C_3, C_4, C_5))=1$

$e(C_1, u^{C_0}v)=e(C_5, g)$

如果成立，则计算 $t=H(e(C_1, Q)^x)$，接着验证下式是否成立：

$e(C_2^t, d_\omega)C_3^{S_\omega}=C_4$

如果上面等式都成立，则返回“Correct”，否则返回“Incorrect”。

3.2 方案的一致性

定理 1 上述构造的无需安全信道的带关键词搜索的公

钥加密方案是计算一致性的。

证明：假设存在一个多项式时间攻击者 A 能够破坏上面方案的一致性。令(ω_0,ω_1)是一致性游戏中攻击者 A 返回的关键词对。不失一般性，假设 $\omega\neq\omega'$。

令 $s,r\in Z_p^*$ 是产生密文 $SCF\text{-}PEKS(GP,pk_R,pk_S,\omega)$时随机选择的。$(ssk,svk)$是强不可伪造一次签名的密钥对。$h=g^z,C_1=g^s,t=H(e(X,Q)^s),C_2=(Yg^{-\omega})^{r/t},C_3=e(g,g)^r,C_4=e(g,h)^r$。

$T_{\omega'}=(s_{\omega'},d_{\omega'})$

其中，$d_{\omega'}=(hg^{-s_{\omega'}})^{1/(y-\omega')}=g^{(z-s_{\omega'})/(y-\omega')}$是由关键词 ω' 所产生的陷门。

显然 A 获胜的条件是 $\omega\neq\omega'$，且需满足 $e(C_2^t,d_{\omega'})C_3^{S_{\omega'}}=C_4$。于是有：

$$
\begin{aligned}
&e(C_2^t,d_{\omega'})C_3^{S_{\omega'}}=C_4\\
&\Leftrightarrow e(((Yg^{-\omega})^{r/t})^t,g^{(z-s_{\omega'})/(y-\omega')})e(g,g)^{rs_{\omega'}}=e(g,g)^{zr}\\
&\Leftrightarrow e(g^{(y-\omega)r},g^{(z-s_{\omega'})'(y-\omega')})e(g,g)^{rs_{\omega'}}=e(g,g)^{zr}\\
&\Leftrightarrow e(g,g)^{((y-\omega)/(y-\omega'))zr}e(g,g)^{-((y-\omega)/y-\omega'))s_{\omega'}r}\cdot e(g,g)^{rs_{\omega'}}=e(g,g)^{zr}\\
&\Leftrightarrow((y-\omega)/(y-\omega'))zr-((y-\omega)/(y-\omega'))s_{\omega'}r+rs_{\omega'}=zr\\
&\Leftrightarrow((y-\omega)/(y-\omega')-1)zr-((y-\omega)/(y-\omega')-1)s_{\omega'}r=0\\
&\Leftrightarrow((\omega'-\omega)/(y-\omega'))(z-s_{\omega'})r=0
\end{aligned}
$$

因为 y、z 是私钥，对攻击者透明，所以，$Pr[s_{\omega'}=z]=1/(p-1)$，并且 $Pr[\omega'=y]=1/(p-1)$，其中 $p-1$ 是 Z_p^* 中元素的个数。如上所述，$\omega\neq\omega'$时，$Test(GP,sk_S,C,T_{\omega'})=$“Correct”。

$$
\begin{aligned}
&Adv_A^{cpks}(\lambda)=Pr[Exp_A^{cpks}(\lambda)=1]\\
&=Pr[(s_{\omega'}=z)\vee(\omega'=y)]\leqslant 2/(p-1)
\end{aligned}
$$

3.3 方案的安全性

定理 2 假设 DBDH 和 q-ABDHE 问题是难解的，那么上述方案是在标准模型下 IND-DT-CKA 安全的。

分两个引理来证明这一定理。

引理 1 设 $q\geqslant q_k+1$，其中 q_k 是攻击者所做陷门查询的总次数。假设 q-ABDHE 问题是难解的，上述的方案在游戏 1 中是标准模型下抗选择关键词攻击语义安全的。

证明：假设在游戏 1 中存在一个多项式时间攻击者 A 能够在标准模型下攻击上述方案。建立一个模拟者 B 能够解决 q-ABDHE 问题。具体模拟如下：

首先，挑战者设置群 G_1、G_2 和双线性对 e，以及群 G_1 的生成元 g。模拟者 B 被输入一个 q-ABDHE 问题实例$(g,g^r,g^{r^2},\cdots,g^{r^q},g^z,g^{zr^{q+2}},T)$，模拟者 B 的目标是区分 $T=e(g,g)^{zr^{q+2}}$ 或者 T 是群 G_2 中的一个随机数。

1. 系统建立：λ 是安全参数，(p,g,G_1,G_2,e)是双线性对参数，单向哈希函数 $H:\{0,1\}^*\rightarrow Z_p^*$，关键词域 $KS_\omega=Z_p^*$，产生 $u,v\in G_1$和强不可伪造一次签名 $Sig=(G,S,V)$。公共参数为 $GP=(p,g,G_1,G_2,e,u,v,Sig,H,KS_\omega)$。随机选取 $a\in Z_p^*$，计算 $X=g^a$，随机选择 $Q\in G_1^*$，设置服务者的公私钥分别为 $pk_S=(GP,X,Q),sk_S=(GP,a)$。

随机选取 q 阶多项式 $f(X)$，定义 $Y=g^x,h=g^{f(x)}$。接收者的公钥为 $pk_R=(pk_S,Y,h)$。发送(pk_R,pk_S,sk_S)给攻击者 A。

2. 查询阶段一：攻击者 A 做如下查询：

· 陷门查询$\langle\omega\rangle$：A 询问 B 关于关键词 ω 的陷门，B 设置 $s_\omega=f(\omega)$，计算 $d_\omega=g^{(f(x)-f(\omega))/(x-\omega)}$，发送陷门 $T_\omega=(s_\omega,d_\omega)$给 A。当 $q\geqslant q_k+1$ 时，$s_\omega=f(\omega)$对于 A 来说是一个随机数，因为 $f(X)$是一个随机的 q 阶多项式。

· 测试查询$\langle C,\omega\rangle$：A 询问 B 关于关键词 ω 和 PEKS 密文之间的测试结果。B 首先做一个陷门查询$\langle\omega\rangle$来得到陷门 T_ω，B 返回给 A 测试 $Test(GP,T_\omega,sk_S,C)$的结果。

3. 挑战：A 一旦决定查询阶段一结束，输出挑战关键词对(ω_0,ω_1)(注意，ω_0、ω_1 不能是查询阶段一中 A 所做的任何陷门查询的关键词)。B 随机地选择 $b\in\{0,1\}$，设置 $\omega^*=\omega_b$，产生强不可伪造一次签名的密钥对$(ssk^*,svk^*)\leftarrow G(\lambda)$，设置 $C_0^*=svk^*,\{s_{\omega^*}=f_k(\omega^*)\}$，计算 $d_{\omega^*}=g^{(f(x)-f(\omega^*))/(x-\omega^*)}$。

B 随机选择 $s^*\in Z_p^*$，并且计算 $C_1^*=g^{s^*}$，$t^*=H(e(X,Q)^{s^*})$，定义 $q+1$ 阶多项式 $F^*(X)=(X^{q+2}-(\omega^*)^{q+2})/(X-\omega^*)=\sum_{i=0}^{q+1}(F_i^*X^i)$。计算

$$
\begin{aligned}
&C_2^*=(g^{zr^{q+2}}(g^z)^{-(\omega^*)^{q+2}})^{1/t^*}\\
&C_3^*=T^{F_{q+1}^*}e(g^z,\prod_{i=0}^{q}(g^{r^i})^{F_i^*})\\
&C_4^*=e((C_2^*)^{t^*},d_{\omega^*})(C_3^*)^{s_{\omega^*}}
\end{aligned}
$$

产生一个强不可伪造一次签名 $\sigma^*=S(ssk^*,(C_1^*,C_2^*,C_3^*,C_4^*,C_5^*))$。发送挑战密文 $C^*=(C_0^*,C_1^*,C_2^*,C_3^*,C_4^*,C_5^*,\sigma^*)$给攻击者 A。

设 $r^*=zF^*(x)$，如果 $T=e(g,g)^{zr^{q+1}}$，那么

$$
\begin{aligned}
C_2^*&=(g^{zr^{q+2}}(g^z)^{-(\omega^*)^{q+2}})^{1/t^*}\\
&=g^{(x-\omega^*)(z(x^{q+2}-(\omega^*)^{q+2})/(x-\omega^*))/t^*}\\
&=g^{(x-\omega^*)r^*/t^*}=(Yg^{-\omega^*})^{r^*/t^*}
\end{aligned}
$$

$$
\begin{aligned}
&C_3^*=T^{F_{q+1}^*}e(g^z,\prod_{i=0}^{q}(g^{r^i})^{F_i^*})=e(g,g)^{r^*}\\
&C_4^*=e(g,h)^{r^*}
\end{aligned}
$$

4. 查询阶段二：A 做与阶段一相同的查询，限制是 A 不能对 ω_0、ω_1 做陷门查询，并且如果$\langle C,\omega\rangle=\langle C^*,\omega_0\rangle$或者$\langle C,\omega\rangle=\langle C^*,\omega_1\rangle$，则不允许对$\langle C,\omega\rangle$做测试查询。

5. 猜测：攻击者输出他的猜测 b'，如果 $b=b'$，则输出 1，表示 $T=e(g,g)^{zr^{q+1}}$；否则输出 0，表示 $T=e(g,g)^r$。

概率分析：如果 $T=e(g,g)^{zr^{q+1}}$，模拟是完美的，A 正确猜出 b 的概率为 $1/2+\varepsilon$；否则 T 是一个随机数，(C_2^*,C_3^*)完全随机且相互独立。在该情况下不等式 $C_3^*\neq e((C_2^*)^{t^*},g)^{1/(x-\omega^*)}$成立的概率为 $1-1/p$。当不等式成立时，因为私钥 s_{ω^*} 是随机的，所以 $C_4^*=e((C_2^*)^{t^*},d_{\omega^*})(C_3^*)^{s_{\omega^*}}=e((C_2^*)^{t^*},(h)^{1/(x-\omega^*)})(C_3^*)/(e((C_2^*)^{t^*},g)^{1/(x-\omega^*)}))^{s_{\omega^*}}$ 是随机的；并且从 A 获得信息的角度来看，C_4^* 与密文中其他元素是相互独立的(C_3^* 除外)。因此 C_4^* 是随机且相互独立的。因为 $s^*\in Z_p^*$ 是随机选取的，所以 $C_1^*=g^{s^*}$ 是随机且与(C_2^*,C_3^*,C_4^*)是相互独立的。挑战密文 $C^*=(C_0^*,C_1^*,C_2^*,C_3^*,C_4^*,C_5^*,\sigma^*)$没有泄露关于 b 的任何信息。到此完成游戏 1 的证明。

引理 2 假设 DBDH 问题是难解的，本文的方案在游戏

2 中是在标准模型下抗选择关键词攻击语义安全的。

证明：假设在游戏 2 中存在一个多项式时间攻击者 A 能够在标准模型下攻击本文构造的方案，建立一个模拟者 B 能够解决 DBDH 问题。具体模拟如下：

首先，挑战者设置循环群 G_1、G_2 和双线性对 e，以及群 G_1 的生成元 g。模拟者被输入一个 DBDH 问题实例 (g, g^a, g^b, g^c, T)，模拟者 B 的目标是区分 $T=e(g,g)^{abc}$ 或者 T 是群 G_2 中的一个随机数。

在描述 B 之前，首先定义事件 F_{OTS} 并给出它的概率范围。用 $C^*=(C_0^*, C_1^*, C_2^*, C_3^*, C_4^*, C_5^*, \sigma^*)$ 表示游戏中发送给攻击者 A 的挑战密文。F_{OTS} 表示 A 对密文 $C=(svk^*, C_1, C_2, C_3, C_4, C_5, \sigma)$ 进行解密查询，并且 $V(svk^*, \sigma, (C_1, C_2, C_3, C_4, C_5))=1$。在阶段一，$A$ 不知道关于 svk^* 的任何信息，因此事件 F_{OTS} 在阶段一发生的概率不超过 $q_k\theta$，其中 q_k 是测试查询的总次数，θ 表示一次签名的验证密钥 svk^* 出现的最大概率（不超过 $1/p$）。显然在阶段二，F_{OTS} 的发生等同伪造了强一次签名。因此 $Pr[F_{OTS}] \leqslant q_k/p + Adv^{OTS}$，第二部分是强不可伪造一次签名被破坏的概率，因此也是可忽略的。

在模拟过程中，如果事件 F_{OTS} 发生，则模拟者 B 停止游戏，并且输出一个随机数代表猜测的结果。在准备阶段 B 产生强不可伪造一次签名的密钥对 $(ssk^*, svk^*) \leftarrow G(\lambda)$，并且给攻击者 A 参数 $u=(g^a)^{\alpha_1}$ 和 $v=(g^a)^{-\alpha_1 svk^*} g^{\alpha_2}$，其中 $\alpha_1, \alpha_2 \in Z_p^*$ 是随机选择的。整个模拟过程如下：

1. 系统建立：λ 是安全参数，(p, g, G_1, G_2, e) 是双线性对的参数，单向哈希函数 $H: \{0,1\}^* \rightarrow Z_p^*$，公共参数为 $GP=(p, g, G_1, G_2, e, H, KS_\omega)$。$KS_\omega$ 表示关键词域。令 $X=g^a$，$Q=g^b$，设置服务者的公钥为 $pk_S=(GP, X, Q)$。

随机选择 $y \in Z_P^*$，计算 $Y=g^y$。随机选择 $h \in G_1^*$，输出接收者的公私钥对 (pk_R, sk_R)，其中 $pk_R=(GP, Y, h)$，$sk_S=(pk_R, y)$。(pk_R, sk_R) 和 pk_S 发送给攻击者 A。

2. 查询阶段一：攻击者 A 做如下查询：

· 陷门查询 $\langle\omega\rangle$：B 随机选择 $s_\omega \in Z_p^*$，计算 $d_\omega=(hg^{-s_\omega})^{1/(y-\omega)}$，发送陷门 $T_\omega=(s_\omega, d_\omega)$ 给 A。

· 测试查询 $\langle C, \omega\rangle$：A 询问 B 关于关键词 ω 和 PEKS 密文 $C=(C_0, C_1, C_2, C_3, C_4, C_5, \sigma)$ 之间的测试结果。B 首先做一个陷门查询 $\langle\omega\rangle$ 来得到陷门 T_ω，然后验证下式是否成立：

$$V(C_0, \sigma, (C_1, C_2, C_3, C_4, C_5))=1$$

$$e(C_1, u^{C_0} v)=e(C_5, g)$$

如果成立，分为下面两种情况：

(1) 如果 $C_0=svk=svk^*=C_0^*$，且 $(C_1, C_2, C_3, C_4, C_5, \sigma) \neq (C_1^*, C_2^*, C_3^*, C_4^*, C_5^*, \sigma^*)$。该情况下事件 F_{OTS} 发生，停止游戏（F_{OTS} 发生概率是可以忽略的，详见准备阶段的讨论）。

(2) 如果 $C_0=svk \neq svk^*=C_0^*$。密文的合法性使得

$$e(C_1, u^{C_0} v)=e(C_5, g)$$

且

$$C_5=(u^{svk} v)^s=((g^a)^{\alpha_1 svk}(g^a)^{-\alpha_1 svk^*} g^{\alpha_2})^s$$

$$=((g^{as})^{\alpha_1(svk-svk^*)} g^{s\alpha_2})$$

因为 $C_1=g^s$，B 能够计算 $g^{as}=(C_5/(C_1^{\alpha_2}))^{1/(\alpha_1(svk-svk^*))}$，然后 B 能够计算

$$t=H(e(C_1, Q)^x)=H(e(g^a, g^b)^s)$$

$$=H(e(g^{as}, g^b))$$

$$=H(e((C_5/(C_1^{\alpha_2}))^{1/(\alpha_1(svk-svk^*))}, g^b))$$

B 检查下式是否成立：

$$e(C_2^t, d_\omega) C_3^{S_\omega}=C_4$$

如果所有等式都成立，返回正确；否则返回错误。

3. 挑战：A 输出挑战关键词对。B 随机地选择 $b \in \{0,1\}$，令挑战关键词 $\omega^*=\omega_b$，$C_0^*=svk^*$，$C_1^*=g^c$，$t^*=H(T)$，随机选取 $r \in Z_p^*$，计算 $C_2^*=(Yg^{-\omega^*})^{r/t^*}$，$C_3^*=e(g,g)^r$，$C_4^*=e(g,h)^r$，$C_5^*=(u^{svk^*} v)^c=((g^a)^{\alpha_1 svk^*}(g^a)^{-\alpha_1 svk^*} g^{\alpha_2})^c=(g^c)^{\alpha_2}$。

产生一个强不可伪造一次签名 $\sigma^*=S(ssk^*, (C_1^*, C_2^*, C_3^*, C_4^*, C_5^*))$。返回密文 $C^*=(C_0^*, C_1^*, C_2^*, C_3^*, C_4^*, C_5^*, \sigma^*)$。发送 C^* 给 A。

4. 查询阶段二：A 做与阶段一相同的查询，限制是如果 $\langle C, \omega\rangle=\langle C^*, \omega_0\rangle$ 或者 $\langle C, \omega\rangle=\langle C^*, \omega_1\rangle$，则不允许做 $\langle C, \omega\rangle$ 的测试查询。与游戏 1 不一样，ω_0、ω_1 这里被允许做陷门查询。

5. 猜测：攻击者输出他的猜测 b'，如果 $b=b'$，输出 1，表示 $T=e(g,g)^{abc}$；否则输出 0，表示 $T=e(g,g)^r$。

概率分析：假设在游戏 2 中存在概率多项式时间攻击者 A 能够在标准模型下以优势 ε 赢得游戏。现在给出模拟者 B 的概率。

当 $T=e(g,g)^{abc}$ 时，A 满足 $|Pr[b=b']-1/2| \geqslant \varepsilon$。当 T 是 G_2^* 中一个随机数时，则 $t^*=H(T)$ 是随机的，同样 $C_2^*=(Yg^{-\omega^*})^{r/t^*}$ 是随机的，于是有 $Pr[b=b']=1/2$。a, b, c 是 Z_p^* 中的元素，T 是 G_2^* 中的元素，于是有

$$|Pr[B(g, g^a, g^b, g^c, e(g,g)^{abc})]=1-Pr[B(g, g^a, g^b, g^c, e(g,g)^r)]=1| \geqslant (1/2 \pm \varepsilon)-1/2=\varepsilon$$

即是不可忽略的。到此完成游戏 2 的证明。

4 性能比较

因为 Rhee 等人的安全模型[15] 比 Baek, Safavi-Naini 和 Susilo 的安全模型更强，所以只与 Rhee 等人在文献[15]描述方案比较。其中 G_1、G_2 表示循环群；t_e 表示群 G_1、G_2 上指数运算的花费，t_p 是双线性对运算的花费，而双线性对运算的花费 t_p 至少是指数运算的花费 t_e 的数倍；t_s，t_v 分别表示签名和验证的计算花费。本文将不考虑双线线性对 $e(Q, X)$、$e(g, g)$ 和 $e(g, Y)$ 的计算时间，因为它们可以被看成是公钥。同样不考虑 Rhee 等人的方案中双线性对 $e(g,h)$，$e(g,u)$ 和 $e(g, \tilde{u})$ 的计算时间。比较的结果如表 1 所列。“测试查询 C^*”表示对 $\langle C^*, \omega\rangle$ 的测试查询，其中 $\omega \neq \omega_0, \omega \neq \omega_1$。

表 1 与 Rhee 方案比较的结果

方案	Rhee 等人的方案[15]	本文方案
PK_{server}	$3\|G_1\|$	$2\|G_1\|$
$PK_{receiver}$	$3\|G_1\|$	$1\|G_1\|$
Trapdoor	$\|G_1\|$	$\|G_1\|+Z_p$
Ciphertext	$\|G_1\|+\|G_2\|$	$3\|G_1\|+2\|G_2\|+\|svk\|+\|\sigma\|$
$ComputeCost_{PEKS}$	$5t_p+2t_e$	$6t_e+t_p$
$ComputeCost_{Test}$	$1t_p+1t_e$	$3t_p+3t_e+t_v$
标准模型	否	是
测试查询 C^*	否	是

从表 1 中得出，本文的方案在接收者和服务者的公钥大小以及 PEKS 加密方面更高效，而其他方面不如 Rhee 等人的

方案。但是本文的方案在增强的安全模型下是可证安全的，即可以对挑战密文 C^* 做关于$\langle C^*, \omega\rangle$的测试查询，其中$\omega \neq \omega_0, \omega \neq \omega_1$；而且是标准模型下可证安全的，避免了 Rhee 的方案依赖随机预言机这一缺点。

结束语 本文提出了一个比 Rhee 等人的方案更强的安全模型，使得可以对包含挑战密文$\langle C^*, \omega\rangle$做测试查询，其中$\omega \neq \omega_0, \omega \neq \omega_1$；并在这一增强的安全模型下证明本文提出的增强的无需安全信道的带关键词搜索的公钥加密方案的安全性。在证明过程中克服了之前方案中使用随机预言机的缺点，从而安全性更高。

参 考 文 献

[1] Abdalla M, Bellare M, Catalano D, et al. Advances in Cryptology [C]// CRYPTO 2005. Springer Berlin Heidelberg, 2005: 205-222

[2] Baek J, Safavi-Naini R, Susilo W. Computational Science and Its Applications[C]// ICCSA 2008. Springer Berlin Heidelberg, 2008: 1249-1259

[3] Boneh D, Boyen X. Efficient selective-ID Identity based encryption without random oracles[C]//Proc. of EUROCRYPT 2004. Springer Berlin Heidelberg, 2004: 223-238

[4] Boneh D, Di C G, Ostrovsky R, et al. Public Key Encryption with Keyword Search [C]// Proc. of EUROCRYPT 2004. Springer Berlin Heidelberg, 2004: 506-522

[5] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited[C]//Proc. of 30th ACM STOC. ACM Press, 1998: 209-218

[6] Canetti R, Halevi S, Katz J. Chosen-Ciphertext Security from Identity-Based Encryption[C]// Proc. of EUROCRYPT 2004. Springer Berlin Heidelberg, 2004: 202-222

[7] Fang L, Susilo W, Ge C, et al. Public key encryption with keyword search secure against keyword guessing attacks without random oracle[J]. Information Sciences, 2013, 238: 221-241

[8] Gentry C. Practical identity-based encryption without random oracles[C]// Proc. of EUROCRYPT 2006. Springer-Verlag, 2006: 457-464

[9] Gu C, Pan Y, Z A H. Efficient Public Key Encryption with Keyword Search Schemes from Pairings[M]// Information Security and Cryptology: Third SKLOIS Conference. 2008: 372-382

[10] Waters B, Balfanz D, Durfee G, et al. Building an Encrypted and Searchable Audit Log[C]// Network and Distributed System Security Symposium (NDSS 2004). 2004

[11] Golle P, Staddon J, Waters B. Secure Conjunctive Search over Encrypted Data [C]// Jakobsson M, Yung M, Zhou J, eds. Proc. ACNS 2004. Springer-Verlag, 2004: 31-45

[12] Hofheinz D, Weinreb E. Searchable encryption with decryption in the standard model: Report 2008/423[R]. Cryptology ePrint Archive, 2008: 1-17

[13] Jeong I R, Kwon J O, Hong D, et al. Constructing PEKS schemes secure against keyword guessing attacks is possible? [J]. Computer Communications, 2009, 32(2): 394-396

[14] Park D J, Kim K, Lee P J. Public Key Encryption with Conjunctive Field Keyword Search[M]// Lim C H, Yung M, eds. Information Security Applications: 5th International Workshop, WISA 2004. Springer Berlin Heidelberg, 2005: 73-86

[15] Rhee H S, Park J H, Susilo W, et al. Improved searchable public key encryption with designated tester[C]// Proc. of the 4th international Symposium on information, Computer, and Communications Security (ASIACCS '09). ACM, New York, NY, 2009: 376-379

[16] Rhee H S, Susilo W, Kim H-J. Secure searchable public key encryption scheme against keyword guessing attacks[J]. IEICE Electron, 2009, 6(5): 237-243

[17] Rhee H S, Park J H, Lee D H. Generic construction of designated tester public-key encryption with keyword search[J]. Information Sciences, 2012, 205(1): 93-109

[18] Xu P, Jin H, Wu Q, et al. Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack[J]. IEEE Transactions on Computers, 2013, 62(11): 2266-2277

[19] Yau W C, Heng S H, Goi B. Off-Line Keyword Guessing Attacks on Recent Public Key Encryption with Keyword Search Schemes[C]// Proc. of ATC 2008. Springer-Verlag, 2008: 100-105

[20] Zhang R, Imai H. Generic combination of public key encryption with keyword search and public key encryption[C]// 6th International Conference Proc. of Cryptology and Network Security. Springer-Verlag, 2007: 159-174

[21] 孙婷，王建东. 基于模糊关键词搜索的无安全信道公钥加密[J]. 计算机应用与软件，2014，31(3)：308-309
Sun Ting, Wang Jian-dong. Encrypting pubilc key without secure channel based on fuzzy keyword search[J]. Computer Applications and Software, 2014, 31(3): 308-309

[22] 李双. 一种安全的具有匿名性的可搜索加密方案[J]. 计算机工程与应用，2013，49(16)：97-102
Li Shuang. Safe anonymous identity based public key encryption with keyword search[J]. Computer Engineering and Applications, 2013, 49(16): 97-102

[23] 王映康，罗文俊. 云存储环境下多用户可搜索加密方案[J]. 电信科学，2012，28(11)：103-107
Wang Ying-kang, Luo Wen-jun. A scheme of multi-user searchable encryption in clould storage[J]. Journal Electronic, 2012, 28(11): 103-107

[24] 李双，徐茂智. 基于属性的可搜索加密方案[J]. 计算机学报，2014，37(5)：1017-1024
Li Shuang, Xu Mao-zhi. Attribute based public key encryption with keyword search[J]. Chinese Journal of Computers, 2014, 37(5): 1017-1024

[25] 杨健，杨邓奇，王剑. 关键词可检索的公钥加密技术综述[J]. 计算机应用，2014，34(7)：1878-1883，1896
Yang Jian, Yang Deng-qi, Wang Jian. Overview of public key encryption with keyword search[J]. Journal of Computer Applications, 2014, 34(7): 1878-1883, 1896