改进的无证书混合签密方案*

周才学
(九江学院 信息科学与技术学院, 江西 九江 332005)

摘 要: 对金春花等人提出的无证书混合签密方案进行了密码分析,分析表明其方案在内部攻击模型下存在保密性攻击,基于双线性对提出了一个改进的无证书混合签密方案。在随机预言机模型中,基于间隙双线性 Diffie-Hellman 问题和计算 Diffie-Hellman 问题证明了改进方案的安全性。改进方案在克服原方案的安全缺陷的基础上保持了原方案的高效性。

关键词: 混合签密; 无证书混合签密; 保密性攻击; 双线性对; 密钥封装
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2013)01-0273-05
doi:10.3969/j.issn.1001-3695.2013.01.070

Improved certificateless hybrid signcryption scheme

ZHOU Cai-xue
(*School of Information Science & Technology, University of Jiujiang, Jiujiang Jiangxi* 332005, *China*)

Abstract: This paper analyzed the Jin et al.'s certificateless hybrid signcryption scheme. It showed that there existed confidentiality attacks in their scheme under insider-security model. This paper proposed an improved certificateless hybrid signcryption scheme based on the bilinear pairings. The improved scheme was proven to be secure under GBDH assumption and CDH assumption in the random oracle model. The improved scheme overcomes the security flaw of the original one without sacrificing its high efficiency.

Key words: hybrid signcryption; certificateless hybrid signcryption; confidentiality attack; bilinear pairings; key encapsulation

签密能在一个逻辑步骤内同时实现加密和认证,而其所需的计算和通信代价大大低于传统的先签名后加密,是 Zhang[1] 于 1997 年提出的概念,自它被提出后,迅速成为了研究热点。

基于身份的密码体制的概念由文献[2]于 1984 年提出。在这种体制中,用户的公钥可由用户的身份信息直接计算得到,从而省去了公钥证书,自它被提出后,也迅速成为了研究热点。但是,基于身份的密码体制有个天生的缺陷,就是存在密钥托管问题,即可信中心知道所有用户的私钥。为克服这种不足,文献[3]于 20003 年提出了无证书密码体制。在无证书密码体制中,用户的私钥由两部分组成,一部分由可信中心产生,另一部分由用户自己生成。这样就解决了密钥托管问题,同时公钥也不需要证书,因此这种密码体制具有巨大的优越性。

无证书签密[4]把无证书体制和签密的思想相结合,既具有无证书体制的优点又具有签密的高效率。然而,一般的签密方案不能签密任意长的消息,一般的公钥加密也存在同样的问题,于是文献[5]提出了混合加密的思想。混合加密由密钥封装技术(KEM)和数据封装技术(DEM)两部分组成。KEM/DEM 混合结构的最大优点是将整个加密算法分为相互独立的两部分,各部分的安全性可以分别研究。2005 年,文献[6]引入了一种新的混合加密结构 tag-KEM/DEM。Tag-KEM 是在密钥封装 KEM 中连同另外一个信息 tag 一起封装,它实际上是一种可认证的 KEM,可如同一般 KEM 那样与 DEM 结合形成混合密码体制,但用 tag-KEM 代替 KEM 可以得到性能更好的混合密码。已有研究表明,在这种新的混合结构下,如果 tag-KEM 是 CCA2 安全的,DEM 只要是被动攻击安全的就可使整个混合加密达到 CCA2 安全水平。2005 年,借鉴加密的 KEM/DEM 思想,文献[7,8]提出了混合签密的概念。2009 年,文献[9]将混合签密的概念推广到无证书体制,提出了无证书混合签密的概念并给出一个具体方案。2011 年,文献[10]提出一个新的无证书混合签密方案。

本文对文献[10]进行了安全性分析,分析表明文献[10]在内部安全模式下存在保密性攻击。本文基于双线性对提出一个改进的无证书混合签密方案,在随机预言机模型中,对改进方案进行了安全性证明。

1 预备知识

1.1 定义

定义 1 双线性对。设 G_1 为循环加群,其阶为素数 q;G_2 为具有相同阶的循环乘群。称 $\hat{e}: G_1 \times G_1 \to G_2$ 为一个双线性映射,如果满足以下性质:

a)双线性性:对所有 $P, Q \in G_1$, $a, b \in Z_q$,有 $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$。

b)非退化性:存在 $P, Q \in G_1$,满足 $\hat{e}(P, Q) \neq 1_{G_2}$。

c)可计算性:对所有 $P, Q \in G_1$,存在一个有效算法计算 $\hat{e}(P, Q)$。

定义 2 计算 Diffie-Hellman 问题,简称 CDH 问题(compu-

收稿日期: 2012-06-10; **修回日期**: 2012-07-12 **基金项目**: 江西省教育厅科技资助项目(GJJ12614)
作者简介:周才学(1966-),男,副教授,硕士,CCF 会员,主要研究方向为密码学与信息安全(charlesjjjx@126.com).

tational Diffie-Hellman problem)。已知$(P, aP, bP) \in G_1^3$, $a, b \in {}_RZ_q^*$,具体 a、b 的值未知,要求计算 abP。

定义 3 双线性 Diffie-Hellman 问题,简称 BDH 问题(bilinear Diffie-Hellman problem)。已知(P, aP, bP, cP), $a, b, c \in {}_RZ_q^*$,具体 a、b、c 的值未知,要求计算 $e(P,P)^{abc}$。

定义 4 决定性双线性 Diffie-Hellman 问题,简称 DBDH 问题(decisional bilinear Diffie-Hellman problem)。已知(P, aP, bP, cP, T), $a, b, c \in {}_RZ_q^*$,具体 a、b、c 的值未知,要求判断等式 $e(P,P)^{abc} = T$ 是否成立。

定义 5 间隙双线性 Diffie-Hellman 问题,简称 GBDH 问题(gap bilinear Diffie-Hellman problem)。已知(P, aP, bP, cP), $a, b, c \in {}_RZ_q^*$,具体 a、b、c 的值未知,要求在 DBDH 预言机的帮助下计算 $e(P,P)^{abc}$。

1.2 无证书混合签密(tag-KEM)算法构成

包含以下八个算法:

a)初始化。输入参数 k。输出主密钥 s。计算 $P_{\text{Pub}} = sP$ 并输出系统参数 Params。

b)部分私钥提取。输入 Params、主密钥 s 和用户身份 $\text{ID}_i \in \{0,1\}^*$。输出用户的部分私钥 D_i。

c)设置秘密值。输入 Params 和用户身份 ID_i。输出用户的秘密值 x_i。

d)设置私钥。输入 Params、用户的部分私钥 D_i 和用户的秘密值 x_i。输出用户的私钥 S_i。

e)设置公钥。输入 Params、用户身份 ID_i 以及用户的秘密值 x_i。输出用户的公钥 PK_i。

f)对称密钥产生。输入 Params,发送者的私钥 S_A、身份 ID_A 和公钥 PK_A,接收者的身份 ID_B 和公钥 PK_B。输出对称密钥 K 和内部状态信息 ω。

g)封装。输入内部状态信息 ω 和任意比特串 τ。输出封装 φ。

h)解封装。输入 Params,封装 φ,标志 τ,发送者身份 ID_A 和公钥 PK_A,接收者的身份 ID_B、公钥 PK_B 和私钥 S_B。输出对称密钥 K 或 $\perp$。

1.3 无证书混合签密安全模型

无证书密码体制存在两类攻击者[3]:第 I 类攻击者 A_I,他不知道系统主密钥,但是他可以替换任意用户的公钥,模拟的是除 KGC 之外的攻击者;第 Ⅱ 类攻击者 $A_\text{Ⅱ}$,他知道系统主密钥,所以他可以计算出每个用户的部分私钥,但不可以替换用户的公钥,模拟的是恶意 KGC 的非法攻击。

无证书混合签密(tag-KEM)在第 I 类攻击者 A_I 和第 Ⅱ 类攻击者 $A_\text{Ⅱ}$ 下都需要满足机密性和不可伪造性。下面分别以游戏的方式直观给出无证书混合签密的安全模型。

定义 6 类型 I 攻击下的保密性。若不存在任何多项式有界的敌手 A_I 以不可忽略的优势赢得以下游戏,则称该无证书混合签密(tag-KEM)在适应性选择密文攻击下具有不可区分性(IND-CLSC-TKEM-CCA2-I)。

a)初始化。挑战者 C 输入安全参数 k,运行 setup,并发送系统参数 Params 给敌手 A_I,保密主密钥。

b)阶段 1。敌手 A_I 可以适应性地执行多项式有界次的以下询问:

(a)部分私钥生成询问。A_I 输入一个身份 ID,挑战者 C 计算身份 ID 的部分私钥 D_{ID}并返回给 A_I。

(b)私钥生成询问。A_I 选择一个身份 ID,挑战者 C 计算相应的私钥 sk_{ID}并返回给 A_I。如果相应的公钥被替换,则不允许询问该预言机。这是因为挑战者不知道相应的秘密值所以不能提供完整私钥。

(c)公钥询问。A_I 输入身份 ID,挑战者 C 计算相应的公钥 pk_{ID}并返回给 A_I。

(d)替换公钥询问。在任何时间,A_I 选择一个新的值 pk'_{ID} 替换原来的公钥 pk_{ID}。

(e)对称密钥产生询问。A_I 选择身份 ID_A、ID_B,设 sk_A 为 ID_A 的私钥、pk_B 为 ID_B 的公钥,C 计算对称密钥 K 和一个内部状态信息 ω,C 记录并保存 ω,ω 对 A_I 保密,C 将对称密钥 K 发送给 A_I。假如 ID_A 的公钥被替换,为了产生正确的回答,要求 A_I 另外提供 ID_A 的秘密值给 C。

(f)密钥封装询问。A_I 产生一个任意 tag τ,C 查看是否存在一个存储的内部状态信息 ω。假如存在,C 用 ω 和 τ 计算封装 φ,删除内部状态信息 ω 返回封装 φ;否则返回 $\perp$ 表示失败。假如 ID_A 的公钥被替换,为了产生正确的回答,要求 A_I 另外提供 ID_A 的秘密值给 C。

(g)密钥解封装询问。A_I 选择身份 ID_A、ID_B,封装 φ 和 tag τ,设 sk_B 为 ID_B 的私钥、pk_A 为 ID_A 的公钥,C 计算对称密钥 K,最后返回 K 或 $\perp$ 给 A_I。如果 ID_B 的公钥被替换,为了产生正确的回答,要求 A_I 另外提供 ID_B 的秘密值给 C。

挑战。当 A_I 决定阶段 1 结束,它产生两个希望挑战的身份 ID_A^*、ID_B^*,ID_B^* 不能是已经执行过私钥生成询问的身份,假如 ID_B^* 的公钥被替换则也不能对 ID_B^* 执行过部分私钥生成询问。C 计算对称密钥 K_1 和内部状态信息 ω^*,然后随机选择一个 K_0 和一个比特值 $b \in \{0,1\}$,发送 K_b 给 A_I。A_I 收到 K_b 后,它可以询问如前所述的询问,然后 A_I 产生一个 tag τ^*。C 计算 ω^* 和 τ^* 的封装 φ^* 并返回 φ^*。

阶段 2。A_I 可以如阶段 1 一样执行多项式有界次的适应性的询问,但不能对 ID_B^* 执行私钥生成询问,假如 ID_B^* 的公钥被替换则也不能对 ID_B^* 执行部分私钥生成询问;另外,他也不能对封装 φ^*、发送者 ID_A^*、接收者 ID_B^* 和 τ^* 执行解封装询问,除非 ID_A^* 或 ID_B^* 的公钥被替换。

猜测。A_I 输出一个比特值 b'作为对 b 的猜测,若 $b' = b$,则 A_I 赢得游戏。

A_I 的优势定义为 $\text{ADV}_{\text{CLSC-TKEM}}^{\text{IND-CCA2-I}}(A_\text{I}) = |2Pr[b' = b] - 1|$。

定义 7 类型 Ⅱ 攻击下的保密性。若不存在任何多项式有界的敌手 $A_\text{Ⅱ}$ 以不可忽略的优势赢得以下游戏,则称该无证书混合签密在适应性选择密文攻击下具有不可区分性(IND-CLSC-TKEM-CCA2-Ⅱ)。

a)初始化。挑战者 C 输入安全参数 k,运行 setup,并发送系统参数 Params 和主密钥给敌手 $A_\text{Ⅱ}$。

b)阶段 1。$A_\text{Ⅱ}$ 可以执行定义 6 中除公钥替换询问和部分密钥生成询问以外的所有询问。

挑战。当 $A_\text{Ⅱ}$ 决定阶段 1 结束,它产生两个希望挑战的身份 ID_A^*、ID_B^*,ID_B^* 不能是已经执行过私钥生成询问的身份。C 计算对称密钥 K_1 和内部状态信息 ω^*,然后随机选择一个 K_0 和一个比特值 $b \in \{0,1\}$,发送 K_b 给 $A_\text{Ⅱ}$。$A_\text{Ⅱ}$ 收到 K_b 后,可以询问如前所述的询问,然后 $A_\text{Ⅱ}$ 产生一个 tag τ^*。C 计算 ω^* 和

τ^* 的封装 φ^* 并返回 φ^*。

阶段 2。$A_{\text{Ⅱ}}$ 可以如阶段 1 一样执行多项式有界次的适应性的询问,但不能对 ID_B^* 执行私钥生成询问;另外,它也不能对封装 φ^*、发送者 ID_A^*、接收者 ID_B^* 和 τ^* 执行解封装询问。

猜测。$A_{\text{Ⅱ}}$ 输出一个比特值 b' 作为对 b 的猜测,若 $b'=b$,则 $A_{\text{Ⅱ}}$ 赢得游戏。

$A_{\text{Ⅱ}}$ 的优势定义为 $\text{ADV}^{\text{IND-CCA2-Ⅱ}}_{\text{CLSC-TKEM}}(A_{\text{Ⅱ}})=|2Pr[b'=b]-1|$。

定义 8　类型 I 攻击下的不可伪造性。若不存在任何多项式有界的敌手 $A_{\text{Ⅰ}}$ 以不可忽略的优势赢得以下游戏,则称该无证书混合签密在适应性选择消息攻击下具有不可伪造性(EUF-CLSC-TKEM-CMA-I)。

初始化和阶段 1 同定义 6。

伪造。$A_{\text{Ⅰ}}$ 产生一个元组 $(\tau^*,\varphi^*,ID_A^*,ID_B^*)$。$ID_A^*$ 不能是已经执行过私钥生成询问的身份,假如 ID_A^* 的公钥被替换则也不能对 ID_A^* 执行过部分私钥生成询问。另外,φ^* 也不是在输入 ID_A^*、ID_B^* 和 τ^* 时由封装预言机产生,如果 $(\tau^*,\varphi^*,ID_A^*,ID_B^*)$ 的解封装不是 $\perp$,则 $A_{\text{Ⅰ}}$ 赢得游戏。$A_{\text{Ⅰ}}$ 的优势定义为它获胜的概率。

定义 9　类型Ⅱ攻击下的不可伪造性。若不存在任何多项式有界的敌手 $A_{\text{Ⅱ}}$ 以不可忽略的优势赢得以下游戏,则称该无证书混合签密在适应性选择消息攻击下具有不可伪造性(EUF-CLSC-TKEM-CMA-Ⅱ)。

初始化和阶段 1 同定义 7。

伪造。$A_{\text{Ⅱ}}$ 产生一个元组 $(\tau^*,\varphi^*,ID_A^*,ID_B^*)$。$ID_A^*$ 不能是已经执行过私钥生成询问的身份,另外,φ^* 也不是在输入 ID_A^*、ID_B^* 和 τ^* 时由封装预言机产生,如果 $(\tau^*,\varphi^*,ID_A^*,ID_B^*)$ 的解封装不是 $\perp$,则 $A_{\text{Ⅱ}}$ 赢得游戏。$A_{\text{Ⅱ}}$ 的优势定义为它获胜的概率。

2　文献[10]方案及分析

2.1　文献[10]方案

a)系统参数建立。设 G_1、G_2 分别是阶为 q 的加法循环群和乘法循环群,P 为 G_1 的生成元,ID_A 和 ID_B 分别为发送者和接收者的身份。三个 hash 函数 $H_1:\{0,1\}^*\rightarrow G_1$,$H_2:\{0,1\}^*\rightarrow Z_q^*$,$H_3:\{0,1\}^*\rightarrow\{0,1\}^n$,其中 n 为 DEM 的长度。KGC 随机选取主密钥 $s\in Z_q^*$,并计算系统公钥 $P_{\text{Pub}}=sP$。令 $T=e(P,P)$,则 KGC 公开系统参数 $\text{Params}=(G_1,G_2,P,P_{\text{Pub}},T,q,e,n,H_1,H_2,H_3)$,保密主私钥 s。

b)部分私钥提取。输入用户的身份 ID_i,KGC 计算 $Q_i=H_1(ID_i)$,输出部分私钥 $D_i=sQ_i$。

c)设置秘密值。用户随机选取 $x_i\in Z_q^*$ 作为自己的秘密值。

d)设置私钥。用户运行此算法,计算自己的私钥 $S_i=(D_i,x_i)$。

e)设置公钥。用户运行此算法,计算自己的公钥 $PK_i=T^{x_i}$。

f)对称密钥产生。输入发送者的私钥 S_A,身份 ID_A 和公钥 PK_A,接收者的身份 ID_B 和公钥 PK_B,算法如下:

(a)随机选取 $b,b_1,b_2\in Z_q^*$,计算 $R_1=T^{b_1}$,$R_2=T^{b_2}$。

(b)计算 $Z=bQ_A$(原文为 $Z=bQ$,系笔误)。

(c)计算 $t=e(D_A,Q_B)^bPK_B^{x_A}$(原文为 $t=e(S_A,Q_B)PK_B^{x_A}$,系笔误)。

(d)$K=H_3(t)$。

(e)$\omega=(b,R_1,R_2,Z,S_A,ID_A,PK_A,ID_B,PK_B)$。

(f)输出 K 和 ω。

g)封装。输入任意的比特串标志 τ 和内部状态信息 ω,算法如下:

(a)计算 $h=H_2(\tau\|R_1\|R_2\|PK_A\|PK_B)$。

(b)计算 $U=b_1P-hD_A$,$u=b_2-x_Ah$。

(c)输出 $\varphi=(Z,U,u,h)$。

g)解封装。输入发送者的身份 ID_A、公钥 PK_A,接收者的私钥 S_B、身份 ID_B 公钥 PK_B,封装 φ 和标志 τ,算法如下:

(a)计算 $t=e(D_B,Z)PK_A^{x_B}$(原文为 $t=e(S_B,Z)PK_A^{x_B}$,系笔误)。

(b)计算 $K=H_3(t)$。

(c)验证 $h=H_2(\tau\|e(U,P)e(Q_A,P_{\text{Pub}})^h\|T^uPK_A^h\|PK_A\|PK_B)$ 是否成立,若成立,输出 K;否则,输出 $\perp$。

2.2　文献[10]方案的保密性攻击

a)攻击方法 1。设 K_b 和 $\varphi^*=(Z^*,U^*,u^*,h^*)$ 分别是发送者为 A、接收者为 B、标签 tag 为 τ^* 的挑战对称密钥和挑战封装。考虑内部攻击者 A,A 产生另外一个封装 $\varphi'=(Z',U',u',h')$ 如下:设 $Z'=Z^*$,$\tau'=\tau^*$,任取 $b'_1,b'_2\in Z_q^*$,计算 $R'_1=T^{b'_1}$,$R'_2=T^{b'_2}$,$h'=H_2(\tau'\|R'_1\|R'_2\|PK_A\|PK_B)$,$U'=b'_1P-h'D_A$,$u'=b'_2-x_Ah'$。显然 $\varphi'=(Z',U',u',h')$ 是发送者为 A、接收者为 B、标签 tag 为 τ^* 的另一个封装,由于 $K=H_3(t)$,$t=e(D_A,Q_B)^bPK_B^{x_A}$ 并没有改变,所以 φ' 和 φ^* 封装的是同一个对称密钥。A 要求挑战者解封装 φ',从而能正确猜测 b 的值,攻击成功。

b)攻击方法 2。设 K_b 和 $\varphi^*=(Z^*,U^*,u^*,h^*)$ 分别是发送者为 A、接收者为 B、标签 tag 为 τ^* 的挑战对称密钥和挑战封装。考虑类型Ⅱ攻击者 $A_{\text{Ⅱ}}$,在内部安全模式下,$A_{\text{Ⅱ}}$ 可以询问 ID_A^* 的私钥,另外,$A_{\text{Ⅱ}}$ 还可以计算任何用户的部分私钥,于是 $A_{\text{Ⅱ}}$ 可以直接计算 $t^*=e(D_B^*,Z^*)(PK_B^*)^{x_A^*}$,$K_b=H_3(t^*)$,从而能正确猜测 b 的值。

3　改进的无证书混合签密方案

a)系统参数建立。

b)部分私钥提取。

c)设置秘密值。

d)设置私钥同原方案。

e)设置公钥。用户运行此算法,计算自己的公钥 $PK_i=x_iP$。

f)对称密钥产生。输入发送者的私钥 S_A,身份 ID_A 和公钥 PK_A,接收者的身份 ID_B 和公钥 PK_B,算法如下:

(a)选取 $b_1,b_2,b_3\in_R Z_q^*$,计算 $R_1=T^{b_1+b_3}$,$R_2=(b_2+b_3)P$。

(b)计算 $Z=b_3P$。

(c)计算 $t_1=e(P_{\text{Pub}},Q_B)^{b_3}$,$t_2=b_3PK_B$。

(d)$K=H_3(t_1\|t_2)$。

(e)$\omega=(b_1,b_2,b_3,R_1,R_2,Z,S_A,ID_A,PK_A,ID_B,PK_B)$。

(f)输出 K 和 ω。

g)封装。输入任意的比特串标志 τ 和内部状态信息 ω,算法如下:

(a)计算 $h=H_2(\tau\|R_1\|R_2\|PK_A\|PK_B)$。

(b)计算 $U=(b_1+b_3)P-hD_A$,$u=b_2+b_3-x_Ah$。

(c)输出 $\varphi=(Z,U,u,h)$。

h)解封装。输入发送者的身份 ID_A,公钥 PK_A,接收者的私钥 S_B,身份 ID_B,公钥 PK_B,封装 φ 和标志 τ,算法如下:

(a)计算 $t_1=e(D_B,Z)$,$t_2=x_BZ$。

(b)计算 $K=H_3(t_1\|t_2)$。

(c)验证 $h=H_2(\tau\|e(U,P)e(Q_A,P_{Pub})^h\|(uP+hPK_A)\|PK_A\|PK_B)$是否成立,若成立,输出 K;否则,输出 $\perp$。

4 改进方案的分析

不可否认性、前向安全性和可公开验证性的分析与原方案的分析类似,下面对保密性、不可伪造性和效率进行分析。

4.1 保密性

定理 1 类型 I 攻击下的保密性。在随机预言机模型中,若存在一个(IND-CLSC-TKEM-CCA2-I)的攻击者 A_1,能够在多项式时间内以 ε 的优势在定义 6 中获胜,它最多能进行 q_i 次 H_i 询问($i=1,2,3$)、q_{CAP}次封装询问、$q_{D\text{-}CAP}$次解封装询问,则存在一个区分者 C 在多项式时间内以以下优势解决 GBDH 问题:

$$\varepsilon'\geqslant\varepsilon/q_1(1-q_{CAP}(q_2+q_{CAP})/2^k)(1-q_{D\text{-}CAP}/2^k)$$

证明 设区分者 C 接收一个随机的 GBDH 问题实例$(P,P_1,P_2,P_3)=(P,aP,bP,cP)$,$a,b,c\in Z_q^*$,具体 a,b,c 的值未知,它的目标是在 DBDH 预言机的帮助下,计算 $e(P,P)^{abc}$。游戏一开始,C 将系统参数发送给 A_1,其中,$P_{Pub}=aP$。C 维护 L_1、L_2、L_3、L_K、L_{CAP}、$L_{D\text{-}CAP}$六张表,这些表开始都为空,L_1、L_2、L_3 分别用于跟踪 A_1 对预言机 H_1、H_2、H_3 的询问,L_K 用于跟踪公钥询问,L_{CAP}用于模拟密钥封装预言机,$L_{D\text{-}CAP}$用于模拟解密钥封装预言机。下面详细解释这些表的建立。

H_1 询问 C 首先从$\{1,2,\cdots,q_1\}$中选取一个随机数 λ,假设 A_1 不会作重复询问。对于 A_1 的第 i 次询问,若 $i=\lambda$,返回 $Q_{ID_\lambda}=bP$,把$(ID_\lambda,bP,\perp)$放入表 L_1;否则随机选取 $r\in Z_q^*$,并设 $Q_{ID}=rP$,把(ID,rP,r)放入表 L_1 并返回 Q_{ID}。

H_2 询问 如果$(\tau,R_1,R_2,PK_A,PK_B,h_2)$在表 L_2 中,返回 h_2;否则,随机选取 $h_2\in Z_q^*$,将$(\tau,R_1,R_2,PK_A,PK_B,h_2)$加入 L_2,返回 h_2。

H_3 询问 如果(t_1,t_2,h_3)在表 L_3 中,返回 h_3;否则进行如下处理:

(a)检验当输入元组(aP,bP,cP,t_1)时 DBDH 预言机是否输出 1,若是,C 输出 $e(P,P)^{abc}=t_1$ 并停止;否则继续。

(b)随机选取 $h_3\in\{0,1\}^n$,将(t_1,t_2,h_3)加入 L_3,返回 h_3。

部分私钥询问 假设 A_1 在此之前已经询问过 H_1。如果 $ID=ID_\lambda$,C 失败并终止模拟;否则在表 L_1 中查找对应的条目,返回 $D_{ID}=raP$。

公钥询问 如果(ID,PK,x)在表 L_K 中,返回此 PK;否则随机选取 $x\in Z_q^*$ 作为秘密值,计算公钥 $PK=xP$,返回该公钥并更新表 L_K。

替换公钥询问 输入(ID,PK'),C 用$(ID,PK',\perp)$更新表 L_K。

私钥询问 假设 A_1 在此之前已经询问过 H_1。如果 $ID=ID_\lambda$,C 失败并终止模拟;否则 C 在表 L_K 中查找 ID 对应的条目,如果没找到就作公钥询问,返回(x,raP)。

对称密钥产生询问 输入(ID_A,PK_A,ID_B,PK_B)。如果 $ID_A\neq ID_\lambda$,这时由于 C 可以得到 ID_A 的私钥,于是 C 只需按正常方式生成对称密钥 K 和内部状态信息 ω,此时 C 必须存储 ω 值并覆盖任何以前的值,并返回 K 给 A_1;如果 $ID_A=ID_\lambda$,C 作如下处理:

(a)选取 $b_2,b_3,h\in_R Z_q^*$,$U\in_R G_1$,计算 $R_1=e(U,P)e(Q_A,P_{Pub})^h$,$R_2=(b_2+b_3)P$,计算 $Z=b_3P$,计算 $K=H_3(e(P_{Pub},Q_B)^{b_3}\|b_3PK_B)$。其中,$Q_A$、$Q_B$、$PK_B$ 的值都可从相应表中或询问获得。

(b)此时内部状态信息为 $\omega=(b_2,b_3,h,U,R_1,R_2,Z,ID_A,PK_A,ID_B,PK_B)$。

(c)存储 ω 并覆盖以前的值,ω 值对 A_1 保密,返回 K 给 A_1。

密钥封装询问 A_1 产生一个任意 tag τ。C 检查是否存在一个存储的 ω 值。若不存在,C 返回 $\perp$ 并终止;否则 C 作如下处理:

(a)若 $ID_A\neq ID_\lambda$,这时由于 C 可以得到 ID_A 的私钥,于是 C 只需按正常方式生成密钥封装并返回给 A_1。

(b)若 $ID_A=ID_\lambda$,C 定义 $h=H_2(\tau\|R_1\|R_2\|PK_A\|PK_B)$,假如表 L_2 中已经存在该条目具有不同的 h 值,C 失败并终止模拟;否则把$(\tau,R_1,R_2,PK_A,PK_B,h)$加到表 L_2。C 计算 $u=b_2+b_3-x_Ah$,其中 x_A 可由表 L_K 获得。最后,C 返回 $\varphi=(Z,U,u,h)$。假如 ID_A 的公钥被替换,要求 A_1 另外提供 ID_A 的秘密值 x_A 给 C。

解密钥封装询问 输入(φ,τ),$\varphi=(Z,U,u,h)$,身份 ID_A 和 ID_B,C 作如下处理:

(a)假如 $ID_B\neq ID_\lambda$,这时由于 C 可以得到 ID_B 的私钥,于是 C 只需按正常方式计算 K 并验证等式是否成立,成立则返回 K,不成立则返回 $\perp$ 给 A_1。

(b)假如 $ID_B=ID_\lambda$,这时 ID_B 的私钥未知,C 作如下处理:遍历 L_3 中的条目(t_1,t_2,h_3),看谁能满足当询问(aP,bP,Z,t_1)时,DBDH 预言机输出 1。假如这样的元组存在,则 $K=h_3$,然后验证等式是否成立,成立则返回 K,不成立则返回 $\perp$ 给 A_1;假如这样的元组不存在,则返回 $\perp$。

挑战 当 A_1 决定阶段 1 结束,它产生两个希望挑战的身份 ID_A^*、ID_B^*。假如 $ID_B^*\neq ID_\lambda$,C 失败并终止;否则 C 设置 $Z^*=cP$,选择一个 $h_3^*\in_R\{0,1\}^n$,设置 $K_1=h_3^*$,C 再随机选择一个 K_0 和一个比特 $b\in\{0,1\}$,发送 K_b 给 A_1。然后 A_1 发送一个 τ^* 给 C。C 选取 $U^*\in_R G_1$,$u^*\in_R Z_q^*$,$h^*\in_R Z_q^*$,发送封装 $\varphi^*=(Z^*,U^*,u^*,h^*)$ 给 A_1,然后计算 $R_1^*=e(U^*,P)e(Q_A^*,P_{Pub})^{h^*}$,$R_2^*=(u^*P+h^*PK_A^*)$,把$(\tau^*,R_1^*,R_2^*,PK_A^*,PK_B^*,h^*)$放入表 L_2。

A_1 经过阶段 2 询问,这些询问同阶段 1,最后 A_1 输出一个 $b'\in\{0,1\}$ 作为对 b 的猜测。A_1 不知道 $\varphi^*=(Z^*,U^*,u^*,h^*)$不是一个正确的封装,除非它用挑战元组$(t_1^*,t_2^*)$询问 H_3。如果这种情况发生,由于 $t_1^*=e(P_{Pub},Q_B^*)^c=e(aP,bP)^c=e(P,P)^{abc}$,则 GBDH 问题的候选答案在表 L_3 中,由 H_3 询问的第一步,C 可成功计算 $e(P,P)^{abc}=t_1^*$。

下面求 C 成功的概率。ID_λ 被选为挑战身份的概率为$\frac{1}{q_1}$,在密钥封装询问时由于 H_2 碰撞,C 终止的概率为 $\frac{q_{CAP}(q_2+q_{CAP})}{2^k}$。在解封装询问中,拒绝有效封装的概率为 $\frac{q_{D\text{-}CAP}}{2^k}$。

定理 2　类型Ⅱ攻击下的保密性。在随机预言机模型中,若存在一个(IND-CLSC-TKEM-CCA2-Ⅱ)的攻击者 $A_{Ⅱ}$,能够在多项式时间内以 ε 的优势在定义 7 中获胜,它最多能进行 q_i 次 H_i 询问($i=1,2,3$)、q_{CAP}次封装询问、$q_{D\text{-}CAP}$次解封装询问,则存在一个区分者 C 在多项式时间内以以下优势解决 CDH 问题:

$$\varepsilon' \geqslant \varepsilon/q_1q_3(1-q_{CAP}(q_2+q_{CAP})/2^k)(1-q_{D\text{-}CAP}/2^k)$$

证明　设区分者 C 接收一个随机的 CDH 问题实例(P, aP,bP),它的目标是计算 abP。游戏一开始,C 将系统参数和主私钥 s 发送给 $A_{Ⅱ}$。C 随机选取 ID_λ($1\leqslant\lambda\leqslant q_1$)作为挑战身份。$C$ 维护 L_1、L_2、L_3、L_K、L_{CAP}、$L_{D\text{-}CAP}$六张表,这些表的说明同定理 1。下面详细解释这些表的建立,对于类型Ⅱ攻击者 $A_{Ⅱ}$,部分私钥解析询问和公钥替换询问已无必要。

H_1 询问　如果($\mathrm{ID},Q_{\mathrm{ID}},r$)在表 L_1 中,返回 Q_{ID};否则,随机选取 $r\in Z_q^*$,并设 $Q_{\mathrm{ID}}=rP$,把($\mathrm{ID},Q_{\mathrm{ID}},r$)放入表 L_1 并返回 Q_{ID}。

H_2 询问同定理 1。

H_3 询问　如果(t_1,t_2,h_3)在表 L_3 中,返回 h_3;否则随机选取 $h_3\in\{0,1\}^n$,将(t_1,t_2,h_3)加入 L_3,返回 h_3。

公钥询问　如果(ID,PK,x)在表 L_K 中,返回此 PK;否则如果 $\mathrm{ID}=\mathrm{ID}_\lambda$,$C$ 设 $PK=aP$,把($\mathrm{ID},aP,-$)加入表 L_K 并返回 aP;否则,C 随机选取 $x\in Z_q^*$ 作为秘密值,计算公钥 $PK=xP$,返回该公钥并把(ID,xP,x)加到表 L_K 中。

私钥询问　假设 $A_{Ⅱ}$在此之前已经询问过 H_1。如果 $\mathrm{ID}=\mathrm{ID}_\lambda$,$C$ 失败并终止模拟;否则 C 在表 L_K 中查找 ID 对应的条目,如果没找到就作公钥询问,返回(x,rsP)。

对称密钥产生询问　输入($\mathrm{ID}_A,PK_A,\mathrm{ID}_B,PK_B$)。如果 $\mathrm{ID}_A\neq\mathrm{ID}_\lambda$,这时由于 C 可以得到 ID_A 的私钥,于是 C 只需按正常方式生成对称密钥 K 和内部状态信息 ω,此时 C 必须存储 ω 值并覆盖任何以前的值,并返回 K 给 $A_{Ⅱ}$;如果 $\mathrm{ID}_A=\mathrm{ID}_\lambda$,$C$ 作如下处理:

(a)选取 $b_1,b_3,h,u\in_R Z_q^*$,计算 $R_1=T^{b_1+b_3}$,$R_2=(uP+hPK_A)$,计算 $Z=b_3P$,$K=H_3(e(P_{\mathrm{Pub}},Q_B)^{b_3}\parallel b_3PK_B)$。其中 PK_A、Q_B、PK_B 的值都可从相应表中或询问获得。

(b)此时内部状态信息为 $\omega=(b_1,b_3,h,u,R_1,R_2,Z,\mathrm{ID}_A,PK_A,\mathrm{ID}_B,PK_B)$。

(c)存储 ω 并覆盖以前的值,ω 值对 $A_{Ⅱ}$保密,返回 K 给 $A_{Ⅱ}$。

密钥封装询问　$A_{Ⅱ}$产生一个任意 tag τ。C 检查是否存在一个存储的 ω 值。假如不存在,C 返回 $\perp$ 并终止;否则 C 如下处理:

(a)若 $\mathrm{ID}_A\neq\mathrm{ID}_\lambda$,这时由于 C 可以得到 ID_A 的私钥,于是 C 只需按正常方式生成密钥封装并返回给 $A_{Ⅱ}$。

(b)若 $\mathrm{ID}_A=\mathrm{ID}_\lambda$,$C$ 定义 $h=H_2(\tau\parallel R_1\parallel R_2\parallel PK_A\parallel PK_B)$,假如表 L_2 中已经存在该条目具有不同的 h 值,C 失败并终止模拟;否则把(τ,R_1,R_2,PK_A,PK_B,h)加到表 L_2。C 计算 $U=(b_1+b_3)P-hD_A$,其中 D_A 可由 $A_{Ⅱ}$直接计算获得。最后,C 返回 $\varphi=(Z,U,u,h)$。

解密钥封装询问　输入(φ,τ),$\varphi=(Z,U,u,h)$,身份 ID_A 和 ID_B,C 作如下处理:

(a)假如 $\mathrm{ID}_B\neq\mathrm{ID}_\lambda$,这时由于 C 可以得到 ID_B 的私钥,于是 C 只需按正常方式计算 K 并验证等式是否成立,成立则返回 K,不成立则返回 $\perp$ 给 $A_{Ⅱ}$。

(b)假如 $\mathrm{ID}_B=\mathrm{ID}_\lambda$,$C$ 如下处理:遍历 L_3 中的条目(t_1,t_2,h_3),看谁能满足 $e(Z,aP)=e(P,t_2)$。假如这样的元组存在,则 $K=h_3$,然后验证等式是否成立,成立则返回 K,不成立则返回 $\perp$ 给 $A_{Ⅱ}$;假如这样的元组不存在,则返回 $\perp$。

挑战　当 $A_{Ⅱ}$决定阶段 1 结束,它产生两个希望挑战的身份 ID_A^*,ID_B^*。假如 $\mathrm{ID}_B^*\neq\mathrm{ID}_\lambda$,$C$ 失败并终止;否则 C 设置 $Z^*=bP$,选择一个 $h_3^*\in_R\{0,1\}^n$,设置 $K_1=h_3^*$,C 再随机选择一个 K_0 和一个比特 $b\in\{0,1\}$,发送 K_b 给 $A_{Ⅱ}$。$A_{Ⅱ}$然后发送一个 τ^* 给 C。C 选取 $Z^*,U^*\in_R G_1$,$u^*,h^*\in_R Z_q^*$,发送封装 $\varphi^*=(Z^*,U^*,u^*,h^*)$给 $A_{Ⅱ}$。然后 C 计算 $R_1^*=e(U^*,P)e(Q_A^*,P_{\mathrm{Pub}})^{h^*}$,$R_2^*=(u^*P+h^*PK_A^*)$,把($\tau^*,R_1^*,R_2^*,PK_A^*,PK_B^*,h^*$)放入表 L_2。

$A_{Ⅱ}$经过阶段 2 询问,这些询问同阶段 1,最后,$A_{Ⅱ}$输出一个 $b'\in\{0,1\}$作为对 b 的猜测。$A_{Ⅱ}$不知道 $\varphi^*=(Z^*,U^*,u^*,h^*)$不是一个正确的封装,除非它用挑战元组($t_1^*,t_2^*$)询问 H_3。如果这种情况发生,由于 $t_2^*=bPK_B=abP$,则 CDH 问题的候选答案在表 L_3 中,C 随机从 L_3 中选择一个 t_2^* 作为 CDH 问题的答案。

下面求 C 成功的概率。ID_λ 被选为挑战身份的概率为$\frac{1}{q_1}$。在密钥封装询问时由于 H_2 碰撞,C 终止的概率为$\frac{q_{CAP}(q_2+q_{CAP})}{2^k}$。在解封装询问中,拒绝有效封装的概率为$\frac{q_{D\text{-}CAP}}{2^k}$。$C$ 随机从 L_3 中选择一个 t_2^* 作为 CDH 问题的答案,正确的概率为$\frac{1}{q_3}$。

4.2　不可伪造性

本文方案具有不可伪造性。它是在无证书签名方案(文献[11]方案 2)的基础上构造的,文献[11]已证明该无证书签名方案在类型Ⅰ和类型Ⅱ攻击者下都是不可伪造的,所以本文方案也是不可伪造的。

4.3　效率

本文方案对原方案作了如下一些改动:

a)把对称密钥产生阶段的 $R_1=T^{b_1}$、$R_2=T^{b_2}$ 改为 $R_1=T^{b_1+b_3}$、$R_2=(b_2+b_3)P$,增加了 2 个加法运算。

b)把 $t=e(D_A,Q_B)^bPK_B^{x_A}$ 改为 $t_1=e(P_{\mathrm{Pub}},Q_B)^{b_3}$,$t_2=b_3PK_B$,把 G_2 中的一个指数运算改为 G_1 中的一个点乘运算(G_2 中的指数运算与 G_1 中的点乘运算可以互换)。

c)把封装阶段的 $U=b_1P-hD_A$,$u=b_2-x_Ah$ 改为 $U=(b_1+b_3)P-hD_A$,$u=b_2+b_3-x_Ah$,增加了 2 个加法运算。

d)把解封装阶段的 $h=H_2(\tau\parallel e(U,P)e(Q_A,P_{\mathrm{Pub}})^h\parallel T^uPK_A^h\parallel PK_A\parallel PK_B)$改为 $h=H_2(\tau\parallel e(U,P)e(Q_A,P_{\mathrm{Pub}})^h\parallel(uP+hPK_A)\parallel PK_A\parallel PK_B)$,把 G_2 中的 2 个指数运算改为 G_1 中的 2 个点乘运算。

从这些改动可以看出,本文方案并没有增加耗时的双线性对运算、点乘运算、指数运算和求逆运算,而效率分析一般只需考虑这些耗时的运算,因而改进方案保持了原方案的高效率。

5　结束语

本文对金春花等人的无证书混合签密方案进(下转第 281 页)

响甚至可以忽略。

为了更直观地表示 WPCI 的计算开销优势,本文给出其与 BI[2] 方案和 PPI[9] 方案在等值查询和范围查询时 DSP 返回结果集中的元组数量的对比数据,如表 1 所示。

表 1　BI、PPI 与 WPCI 方案的查询结果元组数量对比

密文索引方案	等值查询	范围查询
BI	n/m	p
PPI	n/m	p
WPCI	1	$p+2l$

综合上述分析和表 1 的数据,可以得出:WPCI 方案在明显降低等值查询结果集中无效解密操作量的同时仍然能很好地支持范围查询,且没有增加存储开销,实现了在同一索引方案下对等值查询和范围查询的高效支持。

4　结束语

本文通过引入安全参数和循环密文分区的概念,为密文数据建立了部分保序的索引。WPCI 方案能在满足基本隐私保护需求的前提下,较好地辅助 DSP 高效执行等值查询和范围查询。与其他同类索引方案相比,一方面采用循环分区方法,在同样的分区数目下扩大了索引的混淆范围,提高了索引的安全性;另一方面 DSP 返回的等值查询结果集中不再包含假阳性元组(索引发生碰撞时除外),具有更低的通信量和客户端解密操作量,同时又不以显著增加范围查询结果集中的假阳性元组数量为代价。

下一步的工作主要集中在:进一步寻找满足确定性、抗弱碰撞性、随机性和结果范围可控性的函数来高效、安全地生成索引值;综合考虑数据库中多种查询的特点,建立自适应、动态更新支持的密文索引方案。

参考文献:

[1] 田秀霞,王晓玲,高明,等. 数据库服务——安全与隐私保护[J]. 软件学报, 2010,21(5):991-1006.

[2] HACIGUMUS H, IYER B, LI Chen, *et al*. Executing SQL over encrypted data in the database-service-provider model[C]//Proc of ACM SIGMOD International Conference on Management of data. New York: ACM Press, 2002:216-227.

[3] GENTRY C. Fully homomorphic encryption using ideal lattices[C]//Proc of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009:169-178.

[4] AGRAWAL R, KIEMAN J, SRIKANT R, *et al*. Order preserving encryption for numeric data[C]//Proc of ACM SIGMOD International Conference on Management of Data. New York: ACM Press, 2004: 563-574.

[5] EMEKCI F, AGRAWAL D, ABBADI A E, *et al*. Privacy preserving query processing using third parties[C]//Proc of the 22nd International Conference on Data Engineering. Washington DC: IEEE Computer Society, 2006:27-36.

[6] AGGARWAL G, BAWA M, GANESAN P, *et al*. Two can keep a secret: a distributed architecture for secure database services[C]//Proc of the 2nd Conference on Innovative Data System Research. 2005: 186-199.

[7] 余永红,柏文阳. 基于加密技术的外包数据库服务集成安全[J]. 计算机应用, 2011,31(1):110-114.

[8] 张坤,李庆忠,史玉良. 面向 SaaS 应用的数据组合隐私保护机制研究[J]. 计算机学报,2010,33 (11):2044-2054.

[9] HORE B, MEHROTRA S, TSUDIK G. A privacy-preserving index for range queries[C]//Proc of the 30th International Conference on Very Large Data Bases. New York: ACM Press, 2004:720-731.

[10] 赵丹枫,高峰,金顺福,等. 基于错检期望值的密文索引技术[J]. 小型微型计算机系统,2010,31(1):113-118.

[11] 宋伟,彭智勇,程芳权,等. 可信数据库环境下面向服务的自适应密文数据查询方法[J]. 计算机学报,2010,33 (8):1324-1338.

[12] 蔡克,张敏,冯登国. 基于单断言的安全的密文区间检索[J]. 计算机学报,2011,34(11):2094-2103.

[13] 黄汝维,桂小林,余思,等. 云环境中支持隐私保护的可计算加密方法[J]. 计算机学报,2011,34(12):2391-2402.

[14] SWEENEY L. K-anonymity: a model for protecting privacy[J]. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 2002,10(5):557-570.

(上接第 277 页)行了分析,并指出其方案存在内部攻击模式下的保密性攻击,给出了具体的攻击方法并提出一个改进的无证书混合签密方案。本文在随机预言机模型中证明了改进方案的安全性,改进方案能有效克服原方案的安全缺陷同时又保持了原方案的高效性。无证书签密在很多领域具有广阔的应用前景,笔者期待着更多安全的无证书混合签密方案的出现。

参考文献:

[1] ZHENG Yu-liang. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)[C]// Advances in Cryptology-CRYPTO. Berlin: Springer-Verlag, 1997: 165-179.

[2] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Advances in Cryptology-CRYPTO. Berlin: Springer-Verlag, 1984: 47-53.

[3] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Asiacrypt. Berlin: Springer-Verlag, 2003:452-473.

[4] BARBOSA M, FARSHIM P. Certificateless signcryption[C]//Proc of Asiaccs. New York: ACM, 2008:369-372.

[5] CRAMER R, SHOUP V. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack [J]. SIAM Journal on Computing, 2003,33(1):167-226.

[6] ABE A, GENNARO R, KUROSAWA K, *et al*. Tag-KEM/DEM: a new framework for hybrid encryption and a new analysis of Kurosawa-Desmedt KEM[C]//Advance in Cryptology-Eurocrypt. Berlin: Springer-Verlag, 2005:12-46.

[7] DENT A W. Hybrid signcryption schemes with outsider security [C]//Proc of the ISC. Berlin: Springer-Verlag, 2005:203-217.

[8] DENT A W. Hybrid signcryption schemes with insider security[C]// Proc of the ACISP. Berlin: Springer-Verlag, 2005:253-266.

[9] LI Fa-gen, SHIRASE M, TAKAGI T. Certificateless hybrid signcryption[C]//Proc of the 5th Information Security Practice and Experience Conference. Berlin: Springer-Verlag, 2009:112-123.

[10] 金春花,李学俊,魏鹏娟,等. 新的无证书混合签密[J]. 计算机应用研究,2011,28(9):3527-3531.

[11] HUANG Xin-yi, MU Yi, SUSILO W, *et al*. Certificateless signature revisited[C]//Lecture Notes in Computer Science, vol 4586. 2007: 308-322.