基于 AES 和模运算的密文索引方案*

杨 刚, 陈 越, 李超零, 谭鹏许
(解放军信息工程大学 电子技术学院, 郑州 450004)

摘 要: 为密文添加安全索引是解决密文外包后检索困难问题的一种有效方法。针对安全密文索引建立问题,基于 AES 加密和模运算,提出了一种循环分区索引方案。该方案的索引由客户端对属性值进行 AES 加密和模运算得到,具有部分保序的性质。在有效支持范围查询的同时,该方案明显降低了等值查询时客户端的无效解密负载,且满足基本隐私保护需求。方案存储开销和安全性分析结果表明,其存储量在合理范围内。

关键词: 数据库服务; 密文索引; 循环分区; 模运算
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2013)01-0278-04
doi:10.3969/j.issn.1001-3695.2013.01.071

Cryptograph index scheme based on AES and modular arithmetic

YANG Gang, CHEN Yue, LI Chao-ling, TAN Peng-xu
(*Institute of Electronic Technology*, *PLA Information Engineering University*, *Zhengzhou* 450004, *China*)

Abstract: Adding secure index to the encrypted data is an available method handling the problem of executing queries on encrypted data in outsourcing scenarios. Aiming at the construction of secure index, this paper proposed a scheme of wrap-round partition cryptograph index (WPCI) based on advanced encryption standard(AES) and modular arithmetic. It obtained the index by encrypting attribute value using AES and modulo operation, which made the index partially order-preserving. This scheme reduced the useless decryption load of the users in equality queries extremely while supporting range queries effectively. Furthermore, storage burden evaluation and security analysis of WEPI show that storage burden is acceptable, and it meets the basic needs of privacy constraints.

Key words: database as a service(DaaS); cryptograph index; wrap-round partition; modular arithmetic

0 引言

数据库服务(DaaS),又称数据外包(data outsourcing, DO),是一种数据拥有者(data owner,DOwner)将自己所拥有的数据进行隐私保护处理后存储到数据库服务提供商(database service provider,DSP)处,由 DSP 来负责管理和维护数据并提供查询支持的服务模式[1]。通过数据外包,不仅将数据拥有者从繁重的数据管理中解放出来,而且 DSP 在专精于数据管理技术的同时,可以通过大量订单获得规模利润。因此,数据库服务展现出越来越广阔的发展前景。然而,由于 DOwner 将数据存储到 DSP 处后失去了对数据的完全控制,因此外包数据的安全性受到了极大的挑战。对数据加密固然有效地保证了外包数据的机密性,但由于加密失去了明文序的关系,因此,给数据的查询带来了极大困难[2]。

目前国内外学者和研究人员在外包数据的机密性保护方面做了大量的研究工作,主要有以下三类:

a)不解密而直接操作密文数据的方法。该类方法的典型研究包括全同态加密[3]和保序加密[4]。全同态加密同时实现了密文数据的加、乘运算,但在实际应用中构建一个高效的全同态加密算法较为困难。保序加密是从支持范围查询的角度出发,将明文按照其大小关系保序地映射到密文空间,但其并不支持密文运算,且抵抗选择密文攻击的能力较弱。

b)基于数据分布的方法。该类方法主要借鉴秘密共享的思想,通过将数据进行分布存储来实现数据的机密性保护[5~8]。数据拥有者首先在一定数据粒度(如关系数据库的表)上定义数据的隐私约束,然后以隐私约束为准则,对属性进行拆分,通过隐藏属性间的关系来实现数据的机密性保护。该类方法的优点在于:数据机密性的实现是通过属性分解,而不是对所有数据进行加密,所以降低了客户端的解密负载,提高了查询效率。但是该类方法要求在数据外包前就要做出正确、完备的隐私约束,这在实际应用中较为困难,也不能很好地支持数据更新。另外 DSP 共谋攻击也是该类方法需要解决的问题。

c)基于密文索引的方法。该类方法的主要思想是将所有数据加密,然后在需要进行查询的密文上添加安全索引来辅助 DSP 执行查询,本文的 WPCI 方案亦属于此类。文献[2]提出了一种基于桶分区的索引方法,即将明文属性属按照等宽或等深进行分区,索引值就是属性值所处分区的编号,并介绍了针对不同类型查询的查询转换方案,但其 DSP 返回给查询者的结果集中假阳性元组数量过大。文献[9]提出了一种优化的桶分区算法 QOB,能够有效地降低假阳性元组的数量。文献[10]以整体错检期望值为优化依据,提出一种包含等深桶划分和最小化整体错检期望值的复合桶划分索引技术,降低了错

收稿日期: 2012-05-27; **修回日期**: 2012-07-03 **基金项目**: 国家"973"计划资助项目(2012CB315901)

作者简介:杨刚(1987-),男,甘肃金塔人,硕士研究生,主要研究方向为云计算(yg2006nuaa@126.com);陈越(1965-),男,河南开封人,教授,博导,主要研究方向为网络与信息安全;李超零(1985-),男,四川眉山人,博士研究生,主要研究方向为可信计算、云计算;谭鹏许(1984-),男,河南许昌人,博士研究生,主要研究方向为云存储.

检率。文献[11]提出了一种面向服务的自适应密文分段索引方法,该方案能够结合数据分布划分和用户的访问特征自适应地进行数据划分,提高了索引方案的适应性和查询效率。

此外,还有一些其他加密数据查询方法。文献[12]提出了基于单断言的安全的密文区间检索方案,该方案将数据映射到单位圆上,并用三角函数表示,利用可逆矩阵 M 构造密钥,并证明了其方案是安全的。文献[13]提出了一种基于矩阵和向量运算的可计算加密方案 CESVMC,在实现对数据加密的同时,支持对数值型密文的加、减、乘、除四种算术运算和对字符型密文的模糊查询。

本文首先对循环分区的概念和外包数据形式作了介绍,然后利用 AES 加密算法和模运算提出了一种适用于 DaaS 环境的循环分区密文索引(wrap-round partition cryptograph index, WPCI)方案。WPCI 方案中的索引由对属性值的 AES 加密结果进行模运算得到,并满足部分保序的性质。最后对 WPCI 方案的性能和安全性进行了分析和验证。

1　WPCI 方案

1.1　基本思想

本文借鉴文献[2]中的数据外包形式,即 DOwner 将每个明文元组加密后作为整体加密得到一个密文元组,在需要进行查询的属性上建立密文索引,然后将该密文元组及相应属性上的索引一起存储到 DSP 端。为了简化问题描述,本文假定属性的值域是一个离散、有限域,如定长整数。同时,所对应的密文域也是一个离散、有限域,且密文域的规模大于等于明文域。以关系数据库为例,其数据外包形式如定义 1 所述。

定义 1　对于一个给定的关系 $R(A_1,A_2,\cdots,A_n)$,其经过加密处理后可外包的数据形式为 $R^S(\text{etuple},A_1^S,A_2^S,\cdots,A_n^S)$。其中:etuple 是指将 R 中的每一个元组 $t_i(t_i.A_1,t_i.A_2,\cdots,t_i.A_n)$作为一个整体用某种加密算法加密(如 AES 加密算法)所得的结果;A_i^S 表示元组在该属性上的密文索引。

在实际应用中,为了节省资源,并不需要在 R 的每个属性上都建立索引,只对需要进行查询的属性建立索引。

本文将明文域等宽地划分为 m 个分区,每个分区中包含潜在相等数量的元素,设 n 是明文域元素的总个数,则每个分区中包含的元素个数为 n/m。需要注意的是,相同情况下,分区中包含的元素越少,索引泄露的明文信息也就越多。因此,针对不同的安全级别需求,需要对每个分区中的元素个数的下限作出规定。对应地,密文域也要分为 m 个分区,每个分区中包含潜在相等数量的密文元素。

在本文的方案中,由于明文域和密文域的分区数目均为 m,不妨约定:对于明文域的任意一个分区 P_i,$i\in[1,m]$,其目标密文分区为 C_i。本方案引入安全参数 l,当 $l=0$ 时,分区 P_i 中的所有值都映射到对应的目标密文分区 C_i;当 $l\neq 0$ 时,分区 P_i 中的所有值将映射到密文目标分区 C_i 的左、右分别相邻的 l 个分区,即$\{C_{i-l},C_{i-l+1},\cdots,C_{i-1},C_i,C_{i+1},\cdots,C_{i+l-1},C_{i+l}\}$。例如,如果 $l=2$,明文分区 P_4 中的值将被映射到从 C_{4-2}到 C_{4+2},即 C_2 到 C_6 这 $2l+1=5$ 个分区中。对于起始和末尾的明文分区,本文借鉴循环链表的思想,将整个连续的密文分区首尾相接,形成一个循环分区。安全参数 $l=2$ 时,明、密文分区映射关系如图 1 所示。

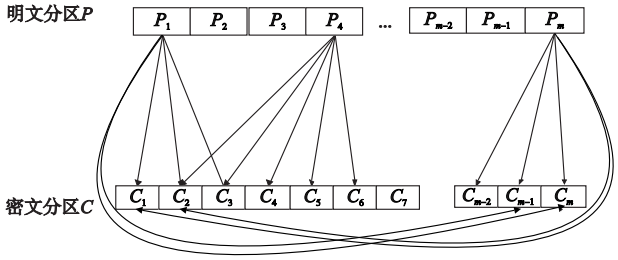

图1　安全参数l=2时明、密文循环分区映射

1.2　循环分区索引建立方法

WPCI 方案利用 AES 和模运算构造了一种满足单向性和计算结果范围可控的明、密文映射算法,利用该算法可以将属于某个明文分区 P_i 的属性值映射到 P_i 相应的密文分区中,从而完成索引的建立,具体实现流程如算法 1 所示。

算法 1　基于 AES 的可控范围密文索引建立算法

输入:元组在某属性上的值 value,AES 加密密钥 k, 安全参数 l,明文分区信息表 T_p,明文分区信息表 T_c。

输出:索引值 index。

a)对于输入的 value,根据 T_p 判断该明文所处的明文分区,记当前 value 所属分区为 P_i;

b)根据 P_i、T_c 和安全参数 l 确定对应密文所在分区(C_{i-l},C_{i+l}),取 C_{i-l}的下界为该明文的索引下界 $S_{\min}$,C_{i+l}的上界为该明文的索引上界 $S_{\max}$;

c)对每个属性值进行加密,采用 AES 加密算法,则有 index = AES(value,k);

d) while(!($S_{\min}\leqslant$index$\leqslant S_{\max}$))/* 通过模运算将加密值限定在指定范围内 */

e)　if(index $<S_{\min}$)

f)　　index = (index + $S_{\min}$) mod $S_{\max}$

g)　elseif(index $>S_{\max}$)

h)　　index = index mod $S_{\max}$

i)　endif

j)　end while

k) return index

由于本方案采用循环分区的方法,则明文分区的前 l 个分区和最后 l 个分区对应的密文分区可能会超出第一个或者最后一个分区,即存在 $i-l<1$ 和 $i+l>m$ 的情况。设 $C_{i,\text{Low}}$表示分区 C_i 的左边界(即下界),$C_{i,\text{High}}$表示分区 C_i 的右边界(即上界)。在算法 1 中的 b)确定密文的上下界时,若存在:a)$i-l<1$,则 P_i 对应的密文范围为$(C_{1,\text{Low}},C_{i+l,\text{High}})$和$(C_{m-j+1,\text{Low}},C_{m,\text{High}})$,其中 $j=l-i+1$;b)$i+l>m$,则 P_i 对应的密文范围为$(C_{i-l,\text{Low}},C_{m,\text{High}})$和$(C_{1,\text{Low}},C_{j,\text{High}})$,其中 $j=i+l-m$。

对应地,在 $i-l<1$ 和 $i+l>m$ 的情况下,当执行算法 1d)的 while 循环的判断时,index 只需要满足两个密文范围之一即可。若都不满足,为了尽量保持明文的大小关系,本文约定程序中 $S_{\min}$ 和 $S_{\max}$ 分别取以下值,即:(a)若 $i-l<1$,则 $S_{\min}=C_{1,\text{Low}}$,$S_{\max}=C_{i+l,\text{High}}$;(b)若 $i+l>m$,则 $S_{\min}=C_{i-l,\text{Low}}$,$S_{\max}=C_{m,\text{High}}$。

从上面的方案介绍中可以看出,WPCI 方案是一个部分保序的索引方案。每个属性上的索引在分区级是有序的,从而实现了对范围查询的有效支持;但在其可映射密文分区范围内又可以看做是随机的,不仅保证了等值查询的精确查询,也提高了索引的安全性。具体查询执行过程和安全性分析参看下面内容。

2　查询执行

为了更清楚地描述在本文的密文索引下如何完成查询,本文给出如图 2 所示的查询执行过程。该过程的关键在于客户端将用户发起的原始查询 q 转换成 DSP 能够识别、执行的密

文查询 q^s。为了描述方便,引入假阳性元组[9]的概念。所谓假阳性元组,即在 DSP 执行 q^s 所得的结果集中不满足用户原始查询 q 的元组。在本章中,将从等值查询和范围查询这两类查询的查询转换来介绍本方案的查询执行情况。

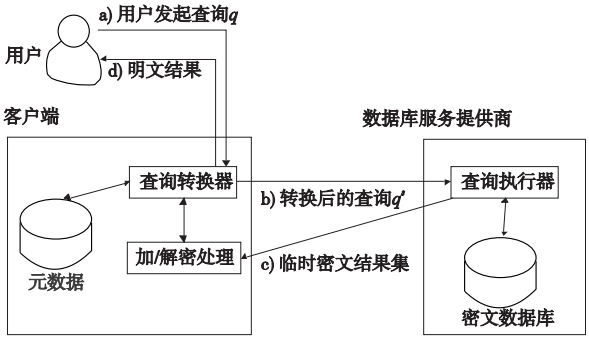

图2 用户查询执行过程

2.1 等值查询

使用 WPCI 方案建立索引时,对于确定的属性值,其密文索引是一定的,即映射满足确定性要求。虽然产生的索引可能发生碰撞,但在 AES 加密满足抗碰撞性和密文空间远大于明文空间的情况下,发生碰撞的概率非常小。因此,等值查询中的相等条件直接可以转换为 DSP 对相应索引的等值查询,而该查询与普通数据库中的等值查询类同。即使索引发生了碰撞,用户将 DSP 返回的查询结果集解密后,在解密的结果上执行初始查询 q 也可以将假阳性元组过滤掉,进而获得真正满足查询条件的结果。

2.2 范围查询

当用户发起一个基于明文某属性上的范围查询 $Q[A,B]$ 时,客户端首先根据存储的该属性的分区信息来确定包含明文 A 和 B 的分区 P_i 和 P_j,然后分别确定 P_i 和 P_j 的对应目标分区 C_i 和 C_j,再利用安全参数 l 就可以确定满足范围查询 $[A,B]$ 的所有元组一定会包含在 $\{C_{i-l},C_{i-l+1},\cdots,C_i,\cdots,C_j,\cdots,C_{j+l-1},C_{j+l}\}$ 这些分区中。记 C_{i-l} 分区的下界为 A^S,C_{j+l} 分区的上界为 B^S,则用户的范围查询 Q 可以转换为 DSP 端可以执行的 $Q'[A^S,B^S]$。然后 DSP 执行该查询,将结果集返回给用户。用户将结果集解密后再执行初始查询 Q,即可滤除其中的假阳性元组。

3 安全性与性能分析

3.1 安全性分析

在 WPCI 方案、OPE 方案[4]和 PPI 方案[9]中,OPE 方案在去除明文值的数据分布特性的同时保留了所有明文的大小关系,因此其泄露的信息最多;PPI 方案假设敌手已经获得了明文值的数据分布情况,它通过控制混淆的方法使得敌手仍然无法获得明文值与密文值之间的有效信息;本文 WPCI 方案也采用了类似混淆方法。

为了衡量明文索引的信息泄露程度,本文引入数据发布领域的 k-匿名[14]方法。k-匿名保护模型是通过检验视图中基于某些关键属性的相同元组个数是否为 $k(k\geq 2)$ 个来判定视图安全。其中,k 是数据发布者根据不同的隐私保护需求程度设定的,k 越大,数据的隐私性越高。如果视图不满足 k-匿名,则攻击者能够明确地知道秘密查询中的部分或全部元组信息,就不能发布这样的视图。因此,在密文索引的信息泄露问题上,只有在满足 k-匿名的条件下,密文索引才是安全的。在索引的建立过程中,WPCI 方案某一分区 P_i 内的属性值,不仅可以映射到其目标密文分区 C_i,还可以映射到另外 $2l$ 个安全密文分区,即对于任意一个密文分区,其中的每个索引值都对应着 $l\times(n/m)$ 个不可区分的明文值,因此,WPCI 满足 k-匿名,即满足基本的隐私保护需求。

定理 1 WPCI 方案是唯密文安全的。

证明 在查询过程中,DSP 只知道明文范围边界值及其所对应的密文分区。设用户发起的查询请求为 Q,则

1)Q 为等值查询,即 attribute = value 时

当客户端将 Q 转换得到的 Q' 发给 DSP 后,DSP 就获得了 value 的密文索引值 index,进而根据此索引值 index 能知道对应的密文分区。但是,由本文的混淆策略可知,每个密文分区中元组至少来自 l 个明文分区,从扩大的明文范围内确定 value 的值是困难的。

2)Q 为范围查询,即 attribute $\in[Q_{\text{Low}},Q_{\text{High}}]$ 时

当 DSP 收到经过转换后的范围查询 $Q'[A^S,B^S]$ 后,它能确定 A^S 和 A^S 分别对应的密文分区,也能获得该查询所包含哪些密文分区,但是不能获得用户查询 Q 的上下界 A 和 B,即不知道这些密文分区对应的明文范围。

综上所述,本方案是唯密文安全的。

3.2 性能分析

由于 WPCI 方案的适用场景是数据库服务,用户可以使用手持电脑(PDA)、手机等移动设备通过 Internet 享受数据库服务,而这种使用模式下,DO 不具备强大的存储能力或者计算能力,所以方案的性能分析主要集中于客户端的存储开销和计算开销[12]。

3.2.1 存储开销

WPCI 方案中,由于设定的明、密文域分区都是定宽的,只需要各自的范围和分区的数量即可重构出分区信息。因此,客户端仅需要存储明文域范围、密文域范围、分区数量、AES 加密密钥 k 和用来加密元组的主加密密钥 s。一旦分区方案确定了,其需要存储的数据量是一常数,与表中元组的规模无关。这些信息不仅在索引建立时需要,在用户查询转换,获得 DSP 能够有效执行的查询时同样需要;对于 DSP 端,只需要存储元组整体加密的结果和需要执行检索的属性上的辅助索引。因此,本方案的存储开销与文献[2,9]的方案大致相当。

3.2.2 用户计算开销

对于等值查询,结合 3.1 节中的分析,可以得出:在 DSP 返回给客户端的等值查询的结果集中,除了由于密文索引弱碰撞可能产生假阳性元组外,其他情况下均不存在假阳性元组。而在文献[2,9]的方案中,执行等值查询返回的结果集将包含该值所在分区的所有元组。因此,WPCI 方案明显降低了等值查询结果集中的假阳性元组数量,降低了客户端的无效解密操作量,提高了查询效率。

对于范围查询,设用户范围查询的上下界所包含明文分区的数量为 p,则 DSP 返回给用户的元组将包含这 p 个明文分区对应的 p 个目标密文分区和 $2l$ 个安全密文分区,即返回集中将包括 $p+2l$ 个密文分区。与文献[2,9]返回 p 个密文分区相比,WPCI 方案增加了结果集的规模,但是对于大元组量的范围查询,其查询范围所包含的明文分区的数量 p 就会非常大,而安全参数 l 可以由用户根据索引的安全性要求高低设定,且一般比较小,则有 $p>>2l$。所以,本方案增加的 $2l$ 个密文分区的元组对整个结果集的影响有限,在大元组量范围查询中其影

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.