安全数据库隐私保护和访问控制集成研究 *

余永红[1], 柏文阳[2]
(1. 安徽财经大学 信息工程学院, 安徽 蚌埠 233041; 2. 南京大学 计算机软件新技术国家重点实验室, 南京 210093)

摘 要: 数据库数据的合法使用和隐私保护是现代安全数据库系统面临的新挑战。针对目前单方面考虑隐私保护或访问控制技术难以同时满足数据库信息安全和处理性能需求的不足,提出一种集成访问控制和隐私保护技术的安全数据库模型,通过建立查询审计隐私保护模型中的查询可疑性与授权视图访问控制模型中查询有效性之间的关系,形成统一的查询判断方法,并给出多项式时间复杂度的审计算法和集成的安全检查框架,以同时实现数据库系统隐私保护和访问控制的安全功能。

关键词: 安全数据库; 隐私保护; 访问控制; 集成
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2010)10-3876-04
doi:10.3969/j.issn.1001-3695.2010.10.073

Integrating secure database access control and privacy protection

YU Yong-hong[1], BAI Wen-yang[2]
(1. *School of Information Engineering, Anhui University of Finance & Economics, Bengbu Anhui* 233041, *China*; 2. *State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing* 210093, *China*)

Abstract: The development of modern information technology and digitalization of the daily lives brings security database new challenges. It is necessary for a security database to provide access control and privacy protection mechanism to ensure the legal use of data and to prevent privacy breach. This paper introduced an integrated security model which could provide the functions of privacy protection and access control simultaneously by building the connection between the validity of query in parameterized authorization view model and the suspiciousness of a conjunctive select-project-join query in online query audit model, it also designed a polynomial time detecting algorithm and two incorporating frameworks for the integrated model to provide higher performance and fine-grained access control in modern database systems.

Key words: secure database; privacy protection; access control; integration

0 引言

隐私保护技术是一种新兴的信息安全技术,与传统的以保护数据不被非法访问为目的的数据库访问控制技术不同,隐私保护技术研究的是在数据被合法访问的情况下如何保护隐私信息不被泄露。目前有关安全数据库的研究分别集中在访问控制技术和隐私保护技术方面,较少考虑和利用两者之间的关系。如何在数据库系统中提供一种有效的可同时支持访问控制和隐私保护的机制,既实现数据的合法使用又保证隐私数据不泄露,是现代安全数据库研究的重要问题。

数据库隐私保护技术可分为交互式和非交互式两种,查询审计是交互式隐私保护技术中的一种,文献[1]提出的基于语义可疑审计的离线查询审计模型能够审计在过去时间里访问数据库系统中敏感数据的查询,具有细粒度、准确、直观和易于使用等特点,但该模型没有考虑综合多个查询的回答进行推理引起隐私信息泄露的问题,没有考虑拒绝查询引起隐私信息泄露的在线审计查询问题,也没有考虑基于数据库状态的拒绝查询带来泄露隐私信息的风险。文献[2]提出一种属性级控制粒度的实用和有效的合并隐私策略到已有应用程序和数据库的方法。文献[3]提出完美隐私的概念,并给出对不同类型的合取查询进行强制完美隐私检查的算法及相关算法复杂度的证明。文献[4]提出在线模拟审计批量查询的模型,并给出批量查询语义可疑审计的多项式时间算法证明,同时提出了独立于数据库状态只需对查询语句的结构进行审计的批量查询语法可疑的概念,但同时也证明了批量查询语法可疑审计是一个NP-Hard 问题。文献[5~8]提供了一些有效的算法和框架来实现查询审计,但它们全部关注于隐私保护,很少研究隐私保护与访问控制之间的关系和利用问题。基于数据库视图的访问控制是众多数据库访问控制模型中的一种,文献[9]最早使用视图实现透明授权访问控制模型,并讨论了多应用程序的有效性推理问题和使用查询处理技术进行等价测试等问题。文献[10]提出一种基于参数化授权视图的细粒度访问控制模型,通过检查查询语句是否有效来决定是执行查询还是拒绝查询,并给出了一个用于推断查询有效性的推理规则集。文献[11]讨论了基于授权视图的数据仓库应用问题,文献[12]讨论了基于规则的授权约束应用问题。

收稿日期: 2010-04-28; **修回日期**: 2010-06-18 **基金项目**: 国家"863"计划资助项目(2007AA01Z448);安徽省省级高校自然科学研究重点项目(KJ2010A003)

作者简介:余永红(1967-),男,江西南昌人,副教授,博士,主要研究方向为数据库、数据库安全(express_yu@163.com);柏文阳(1967-),男,江苏南京人,副教授,博士,主要研究方向为数据挖掘、数据库安全.

上述研究只是单方面探讨了隐私保护或访问控制问题,均未考虑隐私保护与访问控制之间是否存在关系及如何利用它们之间的关系等问题。本文通过综合现有数据库隐私保护技术和访问控制技术的概念、方法和特点,提出一种可有效集成数据库隐私保护和访问控制功能的安全数据库模型,该模型基于参数化授权视图,通过建立查询审计模型中的查询可疑性和授权视图模型中查询有效性之间的关系,形成统一的查询有效性或查询可疑性的判断方法,以同时实现数据库隐私保护和访问控制功能。

1　基本概念和定义

本文提出的安全模型的主要思想包括:

a)在信息表示形式上,统一采用类似 SQL 查询语句的语法形式,把数据库中所有需要进行隐私保护的信息定义为一个禁止视图集 V,把数据库中所有需要进行访问控制的信息定义为一个授权视图集 U。这里把禁止视图 V、授权视图 U 和查询 Q 统一形式化地表示为

$$V=\pi_{C_V}(\sigma_{P_V}(T\times S))$$

$$U=\pi_*(\sigma_{\overline{P_V}}(T\times S\times R))\text{或}\ U=\pi_{*/C_V}(\sigma_{P_V}(T\times S\times R))$$

$$Q=\pi_{C_Q}(\sigma_{P_Q}(T\times R))$$

其中:T 是禁止视图 V 和查询 Q 共有表的叉积;R 和 S 是从句中其他表的叉积;C_Q 是 Q 的选择数据集;P_Q 是 Q 的条件表达式;C_V 是 V 中的选择属性集;P_V 是 V 中的条件表达式;C_Q^* 是 Q 中出现的所有属性的集合。

b)把禁止视图 V 映射成对应查询审计中的审计表达式,把授权视图集 U 映射成查询审计中已经执行的数据库查询集(因为在数据库上执行授权视图是可以得到正确回答的),因此对某一新查询语句的在线检查可同时作用于基于查询审计的隐私保护和基于授权视图的访问控制。通过证明查询审计中的查询可疑与授权视图中查询有效性之间存在的关系,可以在数据库中集两种安全检查于一体,即通过检查查询 Q 是否关于禁止视图 V 可疑,可以判断查询 Q 是否关于 U 有效。

假设学生数据库中包含学生 Student(SID,SNAME,SAddr)和成绩 StudScore(SID,CName,Grade),如果既要保证学生记录的有效使用,又要防止泄露学生的隐私(成绩低于 60 分学生姓名),则可以把学生的隐私信息定义为一个禁止视图:

```
Create ForbiddenView V as
    Select SName, Grade
    From Student,StudScore
    Where Student. SID = StudScore. SID and StudScore. Grade <60
```

把可以对外公开的信息定义为参数化授权视图:

```
Create AuthorizedView U1 as
    Select *
    From Student,StudScore
    Where StudScore. SID = $ SID and StudScore. Grade > =60
Create AuthorizedView U2 as
    Select StudScore. *
    From Student,StudScore
    Where StudScore. SID = $ SID and StudScore. Grade <60
```

其中:$ SID 为参数,其值为运行时的授权用户标志,这样系统管理员可为多个用户创建同一个参数化授权视图以实现细粒度的访问控制功能。

现在给定查询 Q_1:

```
Select SID,CName,Grade
From Student,StudScore
Where StudScore. SID = 1001 and StudScore. Grade <60
```

如果基于 U_2 重写 Q_1,则表示为查询 Q_2:

```
Select SID,CName,Grade From U2
```

由于 Q_1 与 Q_2 的查询结果相同,Q_1 与 Q_2 等价。

现在给定两查询:

```
Q1:Select Grade
   From Student,StudScore
   Where Student. SID = StudScore. SID and StudScore. Grade <60
```

和

```
Q2: Select SName
    From Student,StudScore
    Where Student. SID = StudScore. SID and StudScore. Grade <60
And SName = 'abc'
```

表面看两个查询都没有违反隐私约束,但 Q_1 可以正确返回结果,而 Q_2 则被拒绝,因为 Q_2 会引起隐私泄露。

c)文献[4]已经证明批量 SQL 查询的语法审计是一个 NP-Hard 问题。通过弱化文献[4]中的查询语法可疑,提出查询弱语法可疑概念,并给出合取查询关于禁止视图弱语法可疑的多项式时间审计算法的证明和算法。

下面给出与安全模型相关的一些定义:

定义 1　查询包含。给定查询 Q 和 Q',如果查询 Q 的结果集是查询 Q'结果集的子集,则查询 Q 包含于查询 Q'。

定义 2　等价合取查询。给定合取查询 Q 和 Q',如果查询 Q 和查询 Q'互相包含,则查询 Q 与查询 Q'等价。

定义 3　无条件有效查询。给定查询 Q 和一个授权视图集 U,如果存在基于 U 定义的查询 Q'与查询 Q 等价,则 Q 是关于 U 的无条件有效查询。

定义 4　候选查询。如果查询 Q 访问禁止视图 V 中的至少一个选择属性,则 Q 是 V 的候选查询,即 $C_Q\cap C_V\neq 0$。

定义 5　关键元组。如果删除元组 $t\in T$,查询 Q 能产生不同的查询结果,则 t 是 Q 的关键元组,即 $\pi_{C_Q}(\sigma_{P_Q}(T\times R))\neq\pi_{C_Q}(\sigma_{P_Q}(T-\{t\}\times R))$。

定义 6　查询谓词兼容。如果存在任意一个元组同时满足查询 Q 与禁止试图 V 的条件谓词,则 Q 和 V 查询谓词兼容,即 $\exists t\in(T\times R\times S)$,$P_V(t)=1$ 和 $P_Q(t)=1$。

定义 7　查询完美可疑。如果候选查询 Q 与禁止试图 V 共享一个关键元组,则 Q 关于 V 查询完美可疑,即 $\sigma_{P_V}(\sigma_{P_Q}(T\times R\times S))\neq 0$。

定义 8　批量查询弱语法可疑。给定批量查询 Q,如果存在查询集 $Q'\subseteq Q$ 中的一些子集满足:a)元组 $t\in T$ 对 Q'和 V 中的每个查询都是关键元组;b)Q'中全部查询所涉及的属性至少包含 V 中的一个选择属性。这里 T 是同时出现在 V 和 Q'中的表的叉积,则 Q 关于 V 弱语法可疑。

2　可疑查询与有效查询之间的关系建立

通过建立基于授权视图的查询有效性检查和基于查询审计的可疑检查两者之间存在的有趣关系,可以提供一种统一集成的隐私保护和访问控制检查。

定理 1　给定一个禁止视图 V 和一个授权视图 U,在查询完美可疑概念下,一个查询 Q 关于 V 可疑,当且仅当 Q 不是关

于 U 的无条件有效查询。

证明　如果假设查询 $Q=\pi_{C_Q}(\sigma_{P_Q}(T\times R))$ 关于禁止视图 $V=\pi_{C_V}(\sigma_{P_V}(T\times S))$ 查询完美可疑，考虑授权视图 $U=\pi_*(\sigma_{\overline{P_V}}(T\times S\times R))$，由定义 7，$\exists t\in(T\times R\times S)$ 使 $P_V(t)=1$ 和 $P_Q(t)=1$。则对于由单个元组 $t\in(T\times R\times S)$ 构成的数据库实例 I，$P_Q(t)=1\leftrightarrow Q(I)$ 非空。但由于 $\overline{P_V}(t)=0$，则 U 不包含元组 t，基于 U 重写的 Q 对数据库实例 I 来说是空的，即不存在 U 上查询 Q' 与 Q 等价，所以 Q 不是关于 U 的无条件有效查询。

设 $Q=\pi_{C_Q}(\sigma_{P_Q}(T\times R))$ 关于 $V=\pi_{C_V}(\sigma_{P_V}(T\times S))$ 不可疑，则它们没有共同的关键元组，则 $\forall t\in(T\times R\times S)$ 有 $P_Q(t)=1\leftrightarrow P_V(t)=0$ 或 $P_Q\rightarrow\not\exists$。则基于 U 可重写 Q 使得选择条件 P_Q 和 $\overline{P_V}$ 都在 U 上成立，即存在 U 上的查询 Q' 与 Q 等价，由定义 3 可知，Q 是关于 U 的无条件有效查询。

定理 2　给定一个合取禁止视图 V（其中，$Q_V\cap P_V=0$）和一个授权视图集 U，在批量查询弱语法可疑概念下，一个带非平凡谓词的合取查询 Q 关于 V 可疑，当且仅当 Q 不是关于 U 的无条件有效查询。

证明　给定视图 $V=\pi_{C_V}(\sigma_{P_V}(T\times S))$，假设 $Q=\pi_{C_Q}(\sigma_{P_Q}(T\times R))$。不是关于 $U=\pi_*(\sigma_{\overline{P_V}}(T\times S\times R))$ 的无条件有效查询，则 $\exists t\in(T\times R\times S)$ 使 $P_Q(t)=1$ 和 $\not\exists(t)=0$ 或 $P_V(t)=1$，则 V 和 Q 有共同的关键元组 t，所以 Q 关于 V 可疑。

定理 3　给定数据库上的一个禁止视图 V 和一个弱语法审计器，存在数据库上的一个授权视图集 U，则一个 SPJ 查询 Q 关于禁止视图 V 可疑，当且仅当 Q 不是关于 U 的无条件有效查询。

证明　给定禁止视图 $V=\pi_{C_V}(\sigma_{P_V}(T\times S))$，数据库上的授权视图集为 $U_1=\pi_*(\sigma_{\overline{P_V}}(T\times S\times R))$ 或 $U_2=\pi_{*/C_V}(\sigma_{P_V}(T\times S\times R))$。设 $Q=\pi_{C_Q}(\sigma_{P_Q}(T\times R))$ 关于禁止视图弱语法可疑，则 $C_Q^*\cap C_V\neq 0$，且 $\exists t\in(T\times R\times S)$ 使 $P_V(t)=1$ 和 $P_Q(t)=1$。但没有满足 $P_V(t)=1$ 是 C_V 中的任意属性的元组包含在任何授权视图中，即对元组 t 来说至少有一个 C_Q^* 中的属性不包含在任何授权视图中，因此不存在基于授权视图的查询 Q' 与 Q 等价。即如果 Q 是弱语法可疑，则 Q 关于授权视图 U 不是无条件有效查询。

同样假设 Q 不是关于 V 弱语法可疑，则有：a）$C_Q^*\cap C_V\neq 0$；b）不存在元组 $t\in(T\times R\times S)$ 使 $P_V(t)=1$ 和 $P_Q(t)=1$。若 b）成立，则所有满足 $P_Q(t)=1$ 的元组也一定满足 $\overline{P_V}(t)=1$，则这些元组可以由 U_1 上的条件谓词返回。若 a）成立，则因为没有 C_Q^* 中的属性出现在 C_V 中，所以 U_1 和 U_2 两个授权视图中的所有元组都可以查询这些属性，因此存在基于授权视图的查询 Q' 与 Q 等价，即一个不是弱语法可疑的查询，也一定是授权视图下的无条件有效查询。

上述定理证明了基于查询审计的隐私保护下的查询弱语法可疑与基于授权视图的访问控制下的查询无条件有效之间的关系，因此可以在安全数据库中提供一种统一集成的实现隐私保护和访问控制功能的检查机制。

3　算法与体系结构

由于查询弱语法可疑与无条件有效查询的等价性，可以提供一种集成的、可同时实现隐私保护和访问控制功能的检查机制，通过把查询类型限制为合取 SPJ 查询，一个合取 SPJ 查询的形式可表示为

$$Q(X):-G_1(X_1)\wedge G_2(X_2)\wedge\cdots\wedge G_n(X_n)\wedge C_Q$$

其中：G_i 为目标 Q 中的子目标；C_Q 为 Q 中不相等约束集，而一个禁止视图可表示为

$$V(X):-G_1(X_1)\wedge G_2(X_2)\wedge\cdots\wedge G_n(X_n)\wedge C_Q$$

其中：G_i 为目标 V 中的子目标；C_Q 为 V 中不相等约束集。

通过检查 $Q(X)$ 和 $V(X)$ 两个查询的包含性来判断查询是否泄露隐私。可采用类似文献[3]的算法，在多项式时间内实现查询弱语法可疑的审计检查，为便于分析，定义下面一些符号：

Q：合取查询

V：禁止视图

n：所有子目标个数 $n=|Q|+|V|$

m：Q 和 V 中的关系个数

r：Q 和 V 中关系的最大元数

k：Q 和 V 中每个关系的最大自连接数

p：一个数据库实例上的查询输出

G_Q：Q 中的子目标集合

G_V：V 中的子目标集合

A_Q：出现在 Q 中的谓词集合

B_Q：出现在 Q' 中不出现在 Q 中的谓词集合

K_Q：Q 中所有关键字约束集合

G^*：$Q'\cup V'$ 中子目标的最广通代

算法 1　弱语法可疑审计

输入：禁止视图 V 和合取查询 Q；

输出：是否 Q 和 V 共享一个关键元组。

1. for all $Q'\subseteq G_Q$, $V'\subseteq G_V$ do
2. if $Q'\cup V'$ 是元数为 r 的关系 R 的谓词兼容子集 then
3. 设 G^* 为一个子目标，则：
   $1\leqslant i\leqslant r, \exists G\in Q'\cup V': G[i]=c_i\Rightarrow G^*[i]=c_i$
   $1\leqslant i,j\leqslant r, \exists G,G'\in Q'\cup V': G[i]=G'[j]\Rightarrow G^*[i]=G^*[j]$
4. $\rho_{G^*}: A_Q\cup B_Q\rightarrow A_Q\cup B_Q\cup K_Q\cup V$
   $$\rho_{G^*}(x_i)=\begin{cases}G_j^*, \text{if } G_1[j]=x_i, G_1\in Q'\cup V'\\ x_i, \text{otherwise}\end{cases}$$
5. $Q|_{(Q',G^*)}=\rho_{G^*}(Q-Q'), V|_{(V',G^*)}=\rho_{G^*}(V-V')$
6. if($Q|_{(Q',G^*)}\notin Q$ and $V|_{(V',G^*)}\notin V$) then
7. 返回 Q 和 V 共享一个关键元组
8. end if
9. end if
10. end for
11. 返回 Q 和 V 不共享一个关键元组

算法时间复杂性分析：给定查询 Q 和禁止视图 V 中兼容子集 Q' 和 V'，构造最广通代 G^* 的时间为 $O(r_R(|Q'|+|V'|)$，这里 r_R 是关系 R 的元数，构造 $Q|(Q',G^*)$ 和 $V|(V',G^*)$ 的时间为 $O(r_R(|Q|-|Q'|+|V|-|V'|)$，总的时间为 $O(nr)$。设 $T(c)$ 为检测（$Q|_{(Q',G^*)}\notin Q$ 和 $V|_{(V',G^*)}\notin V$）包含的时间，共享相同关系符号的子集 $Q'\cup V'$ 的集合个数至多为 $m2^{2k}$，因此运行时间为 $O(m2^{2k}(nr+T(c)))$。如果 k 是一个常量并限制查询类型为合取查询，$T(c)$ 可以在多项式时间内完成，则整个算法可在多项式时间内完成。

基于上述思想，本文设计了两种集成基于查询审计的隐私保护和基于授权视图的访问控制的检查框架，即安全增强型检查框架与内置型检查框架。

安全增强型检查框架如图 1 所示。

图 1 中虚线部分是一个逻辑上独立于后台数据库的软件系统,实现时首先将需要保护的隐私信息以类似 SQL 语句的禁止视图方式创建并保存在可信操作系统文件中,用于访问控制的参数化授权视图也同样以类似 SQL 语句的形式创建并存储在文件中。对查询进行检查时,通过 JDBC 驱动程序获取客户端发出的查询语句(假设已对参数化授权视图进行实例化即给视图参数固定值)并对查询进行重写,然后对查询语句进行审计检查,确定查询是否弱语法可疑,若查询检查无疑,则通过与数据库的接口访问后台数据库,若查询可疑则拒绝执行查询。

内置型检查框架如图 2 所示。

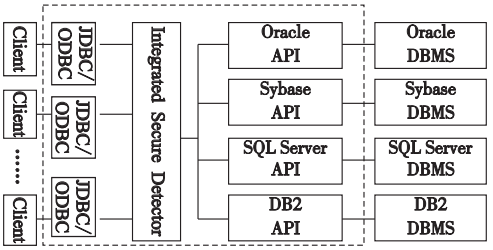

图1　安全增强型检查体系结构

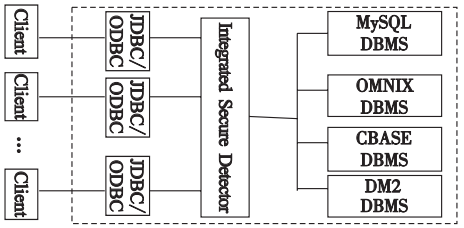

图2　内置型检查体系结构

图 2 中虚线部分是一个完全内置于后台数据库中的检查系统,实现时首先将需要保护的隐私信息以类似 SQL 语句的禁止视图方式创建并保存在数据库中,用于访问控制的参数化授权视图也同样以类似 SQL 语句的形式创建并存储在数据库中。检查方式与增强型检查方式相同,但检查通过执行查询时之间在数据库中执行,无须通过接口访问。

4　结束语

本文探讨了在传统数据库系统中同时实现敏感信息的保护和非敏感信息的合法访问的安全问题,提出一种通过建立参数化授权视图模型中的查询有效性与在线查询审计模型中的合取 SPJ 查询可疑性之间的关系,以同时实现隐私保护和访问控制功能的集成安全数据库模型,并为此模型设计了一个多项式时间的检查算法和两种体系结构。由于查询弱语法可疑与无条件有效查询的等价性,参数化授权视图的查询有效性可提供细粒度的访问控制,模型具有细粒度的访问控制能力,同时,安全检查时只要进行两种检查中的一种即可,因此模型又具有较高的处理性能。进一步的工作包括模型的无缝嵌入实际数据库系统、完善查询审计隐私保护和授权视图访问控制之间的关系证明及相关算法的优化。

参考文献:

[1] ARRAWAL R, BAYARDO R, FALOUTSOS C, *et al*. Auditing compliance with a Hippocratic database[C]//Proc of International Conference on Very Large Data Bases. San Fransisco:Morgan Kaufmann, 2004:516-527.

[2] LEFEVRE K, AGRAWAL R. Limiting disclosure in Hippocratic databases[C]//Proc of International Conference on Very Large Data Bases. San Fransisco:Morgan Kaufmann, 2004:108-119.

[3] MACHANAVAJJHALA A, GEHRKE J. On the efficiency of checking perfect privacy[C]//Proc of ACM Symposium on Principles Database Systems. New York:ACM Press, 2006:163-172.

[4] MOTWANI R, NABHA S, THOMAS D. Auditing batches of SQL queries[C]//Proc of PDM Workshop with ICDE. Washington DC: IEEE Computer Society, 2007:186-191.

[5] NABAR S, MARTHI B, KENTHAPADI K, *et al*. Towards robustness in query auditing[C]//Proc of VLDB. New York:ACM Press, 2006:151-126.

[6] THOMAS D. Algorithms and architectures for data privacy[D]. Standford: Department of Computer Science, Stanford University, 2007.

[7] 严和平, 王正飞, 汪卫, 等. 基于推理的安全数据库审计框架[J]. 计算机研究与发展, 2006,43(9):1630-1638.

[8] CHAWLA S, DWORK C, MCSHERRY F, *et al*. Toward privacy in public databases[C]//Proc of the 2nd Theory of Cryptography Conference. Berlin:Springer, 2005:363-385.

[9] MOTRO A. An access authorization model for relational database based on algebraic manipulation of view definitions[C]//Proc of ICDE. Washington DC:IEEE Computer Society, 1989:339-347.

[10] RIZVI S, MENDELZON A, SUDARHAN S, *et al*. Extending query rewriting techniques for fine-grained access control[C]//Proc of SIGMOD. New York:ACM Press, 2004:551-562.

[11] ROSENTHAL A, SCIORE E. View security as the basis for data warehouse security[C]//Proc of International Workshop on Design and Management of Data Warehouse. Aachen:CEUR-WS, 2000:8.

[12] AHN G, SANDHU R. Role-based authorization constraints specification[J]. ACM Trans on Information and System Security, 2000, 3(4):207-226.

(上接第 3875 页)

[3] RAY I, NATARAJAN N. An anonymous and failure resilient fair-exchange e-commerce protocol [J]. Decision Support Systems, 2005, 39(3):267-292.

[4] WANG Jian-hui, LIU Jing-wei, LI Xiao-hui, *et al*. Fair e-payment protocol based on blind signature[J]. The Journal of China Universities of Posts and Telecommunications, 2009,16(5):114-118.

[5] WANG C H, YIN C H, JUAN C H. How to protect exchanged secrets in the fair exchange protocol with off-line TTP[J]. Computers & Electrical Engineering, 2006, 32(5):364-375.

[6] JONES K, LEONARD L. Trust in consumer-to-consumer electronic commerce [J]. Information & Management, 2008, 45(2):88-95.

[7] 郭涛,李之棠,谭运猛,等.一种改进的离线电子现金方案[J]. 华中科技大学学报:自然科学版,2003,31(5):14-15.

[8] HUSSEIN J A, ALMUKHTAR M A. Fair exchange of digital signatures using RSA-based CEMBS and offline STTP [J]. Journal of Computing, 2009,1(1):87-91.

[9] ANDERSON B, HANSEN J, LOWRY P, *et al*. Standards and verification for fair-exchange and atomicity in e-commerce transactions [J]. Information Sciences, 2006, 176(8):1045-1066.

[10] MA Chang-she, LEI Fei-yu, CHEN Ke-fei. Optimistic fair exchange e-commerce protocol based on secret sharing [J]. Journal of Systems Engineering and Electronics, 2006, 17(4):858-863.