Journal of Computer Applications
计算机应用,2014,34(9):2635 -2638
ISSN 1001-9081
CODEN JYIIDU
2014-09-10
http://www.joca.cn

文章编号:1001-9081(2014)09-2635-04
doi:10.11772/j.issn.1001-9081.2014.09.2635

可隐私保护的电子交易新方案

杨　波[1,2*],李顺东[2]
(1.兰州文理学院 电子信息工程学院,兰州 730010;　2.陕西师范大学 计算机科学学院,西安 710062)
(*通信作者电子邮箱 lz-yb@foxmail.com)

摘　要:针对电子交易中的隐私安全问题,提出了一个可保护用户隐私的电子交易方案。方案将不经意传输协议和 ElGamal 签名相结合,实现了电子交易中交易双方的隐私安全。用户使用序号选择商品,匿名付费给银行;银行将商品的数字签名发送给用户,用户使用数字签名和商家进行不经意信息交互;对序号进行幂运算加密得到密钥,商家不知道用户订购何种数字商品,序号的隐蔽性和制约性也使得用户不能以没有选择的序号打开消息,用户得到且只能得到自己订购的数字商品。正确性证明和安全性分析结果表明,方案保护了交易双方在电子交易过程中的交互信息,同时防止商家恶意欺诈行为。方案签名短,计算量小,密钥动态变化,安全性强。

关键词:隐私保护; 不经意传输;签名;电子交易;密钥协商
中图分类号: TP309　　**文献标志码**:A

New scheme for privacy-preserving in electronic transaction

YANG Bo[1,2*], LI Shundong[2]
(1. *School of Electronics and Information Engineering, Lanzhou University of Arts and Science, Lanzhou Gansu* 730010, *China*;
2. *School of Computer Science, Shaanxi Normal University, Xi'an Shaanxi* 710062, *China*)

Abstract: For the users' privacy security in electronic transactions, an electronic transaction scheme was proposed to protect the users' privacy. The scheme combined the oblivious transfer and ElGamal signature, achieved both traders privacy security in electronic transactions. A user used a serial number to choose digital goods and paid the bank anonymously and correctly. After that, the bank sent a digital signature of the digital goods to the user, then the user interacted with the merchant obliviously through the digital signature that he had paid. The user got the key though the number of exponentiation encryption, the merchant could not distinguish the digital goods ordered. The serial number was concealed and restricted, so the user could not open the message with the unselected serial number, they could and only could get the digital goods they paid. Correctness proof and security analysis shows that the proposed scheme can protect both traders mutual information in electronic transactions and prevent merchant's malicious fraud. The scheme has short signature, small amount of calculation and dynamic changed keys, its security is strong.

Key words: privacy-preserving; oblivious transfer; signature; electronic transaction; key agreement

0　引言

在网络迅速发展的今天,电子交易正在改变传统商业形式,安全的电子交易成为重中之重,将密码学知识与电子交易相结合,可实现对交易用户的隐私信息保护[1]。电子交易过程中的用户隐私安全问题主要涉及用户在选择商品后如何匿名付费,以及如何得到自己选择的商品[2]。本文研究的是用户在电子交易中已经安全完成了匿名付费后如何得到自己选择的商品,并且在隐私信息不泄露的情况下只得到自己选择的商品问题。文献[3]采用对称密钥,适用于价格相同的商品,但不能解决商家可能存在的欺诈问题;文献[4]在方案中引入了不经意传输协议,实现了发送方不知道接收方所选择商品的具体信息,但加密密钥固定,存在攻击者明文攻击安全问题;文献[5-6]分别采用 RSA(Rivest-Shamir-Adleman)签名方案和 Schnorr 签名方案,解决了可能存在的商家恶意欺诈问题,但在计算签名时签名文件较长,计算开销大,并且发送方在进行信息预处理时,没有对信息进行加密保护;文献[7]将不经意传输协议与商品价格相结合,提出了一种基于价格的不经意传输的隐私保护方案,方案的前提需要限定发送者消息的价格;文献[8]在电子交易动态环境中引入向量计算,设计了一个基于向量运算的可计算加密方案,通过对数据的加密实现隐私保护;文献[9]基于匿名链提出一种在电子交易动态环境中保护用户位置隐私的算法。本文提出一种在电子交易过程中可以保护用户隐私信息的方案,该方案将 1-out-n不经意传输协议和 ElGamal 签名相结合,用户使用序号选择商品,每次选择商品序号都不同;引入幂运算参与序号处理,得到密钥,实现密钥动态协商;商家利用序号的隐蔽性和制约性,使得用户不能以没有选择的序号打开消息,用户得到且只能得到自己订购的数字商品,实现整个交易中关键位置隐私保护。在这个交易方案中,对用户的授权无须提前对用户进行认证,对商品价格不作限定,这就保证了用户隐私信息不泄露,并且用户可以通过向银行申请仲裁来防止商家可能存在的恶意欺诈行为,保证了方案的安全性。

收稿日期:2014-03-31;**修回日期**:2014-05-23。　**基金项目**:国家自然科学基金面上资助项目(61272435)。
作者简介:杨波(1978-),女,甘肃庆阳人,副教授,硕士,主要研究方向:网络信息安全;　李顺东(1963-),男,河南鲁山人,教授,博士生导师,主要研究方向:密码学与信息安全、电子商务。

1 模型

定义 1 ElGamal 算法。

输入安全参数,输出系统参数。p 是一个大素数,两个随机数是 g 和 x,g 是一个阶为 $p-1$ 的生成元,$g<p$,$x<p$,p 和 g 可由一组用户共享,x 是私钥,$y=g^x \pmod p$ 是公钥,算法的安全性依赖于计算有限域上离散对数的难度。

加密和解密[10]:对消息 M 进行加密,选取 $k \in_R \mathbf{Z}_{p-1}^*$,运算 $a=g^k \pmod p$,$b=y^k h(M) \bmod p$,得到 (a,b),计算 $\frac{b}{a^x \pmod p}$ 得到消息 M。

签名和验证[10]:对消息 M 进行签名,选取 $k \in_R \mathbf{Z}_{p-1}^*$,运算 $s=(h(M)-xr)k^{-1} \bmod (p-1)$,$r=g^k \pmod p$,得到签名 (r,s),如果方程 $y^r r^s \equiv g^{h(M)} \pmod p$ 成立,则认可数对 (r,s) 对消息 M 的签名有效。

定义 2 1-out-n 不经意传输协议。

1-out-n 不经意传输协议[11]模型包括发送方和接收方,记作 S 和 R,接收方拥有的证书内容为 M,模型有一个可信任的权威机构 CA,以一个签名方案的参数作为系统建立的参数,S 有 n 个消息 $m_i(i=1,2,\cdots,n)$,S 恰能提供给 R 所选择的一个,但 R 不希望 S 知道自己选中的是哪一个消息。

系统建立[12]:CA 输入安全参数,产生系统密钥 x、公钥 y 和签名 (r,s),G 是一个 $p-1$ 阶循环群,g 是 G 的一个生成元,$x \in \mathbf{Z}_{p-1}^*$,$y=g^x$,(r,s) 是对 M 的 ElGamal 签名,公布 p、g 和 y,并由安全秘密信道将签名 (r,s) 发送给接收方。

交互信息:发送方 S 拥有消息 $m_1,m_2,\cdots,m_n \in G$;对消息的选择是 $\alpha(1 \leqslant \alpha \leqslant n)$ 的接收方 R 拥有对 M 的签名 (r,s);协议各方均拥有证书 M。发送方 S 不知道接收方是哪一个,在发送方和接收方之间匿名进行交互式的认证。

打开信封:持有签名 (r,s) 的接收方才能够与发送方进行密钥协商,才可以打开所选择的消息 m_α。

协议参与的双方都是概率多项式时间图灵机[13],若双方都能正确执行协议,协议完成后接收方可以得到所选择的消息。接收方的不同选择所对应的传输副本对于发送方的计算性是不可区分的,保证了接收方的隐私安全;接收方不能得到没有选择的消息,接收方只能得到所选择的消息所对应的密文,其余密文与随机数据对接收方的计算性是不可区分的,保证了发送方的安全性。

在协议参与的双方都是概率多项式时间图灵机的情况下,协议依然有失败的概率。在该协议执行过程中,若接收方打开信封得到的消息 m_α,不是所选择的消息 α,则说明协议执行失败,这时接收方可以依据发送方所公布的信息和自己通过计算得到的消息向 CA 提起仲裁,CA 通过计算可以判断并进行裁决,保护接收方的信息安全。

定义 3 电子交易模型。

电子商务模式下的交易模型[14]由三部分组成,分别是商家、用户和银行。其中权威机构 CA 由银行充当,发送方是商家,选择了数字商品并且正确付费了的用户是接收方;用 M_1,M_2,…,M_n 标识数字商城中的上架商品,$p_1,p_2,\cdots,p_n$ 为 M_1,M_2,…,M_n 所对应的价格。

在电子交易模型中,用户在数字商城中选择自己想要购买的商品,按照商品对应的价格向银行付费;银行成功收取商品费用后,用户和商家执行具有不经意性的信息传输协议;协议完成后,用户得到且只能得到自己选择并且付费了的数字商品。

2 电子交易方案

2.1 相关标识

p 表示一个大素数;g 表示 $\mathbf{Z}_p^*$ 的生成元;G 表示一个 $p-1$ 阶循环群;$h:\mathbf{Z}_p^* \to \{0,1\}^*$ 是哈希函数;sig 表示数字签名体制;$\|$ 是连接操作。

2.2 银行预处理

银行在这里充当可信的权威机构 CA,银行初始化的过程就是系统建立的过程,M 是发放给接受方的证书的内容,系统首先输入安全参数 t,运行 ElGamal 签名算法,产生 ElGamal 签名算法的参数 (p,g,y,x),同时产生和 t 同阶的安全参数 t_1,在这里 x 是系统私钥,Hash 函数是 $h:\mathbf{Z}_p^* \to \{0,1\}^*$,接着银行对证书 M 签名,然后系统通过安全秘密信道将银行对证书 M 签名发送给接收方,同时系统对外公布 (p,g,y)。

2.3 商家预处理

商家在这里相当于发送方,负责提供待出售的 n 种数字商品 $m_i(i=1,2,\cdots,n)$,以 $number_i(i=1,2,\cdots,n)$ 作为编号,$Q_i(m_i)(i=1,2,\cdots,n)$ 用来表示对某种数字商品 m_i 的具体描述;对外公布 $(number_i,Q_i(m_i))(i=1,2,\cdots,n)$。

商家分别计算:

$h_i^1=h(number_i \| M_i)$,$h_i^2=h(number_i \| p_i)$,

$s_i=sig(number_i \| h_i^1 \| h_i^2)$;$\forall i(1 \leqslant i \leqslant n)$

$a=g^k \pmod p$,$b=y^k h(number_i,p_i) \bmod p$;$i=1,2,\cdots,n$

公布 $(i,h_i^1,h_i^2,s_i)(i=1,2,\cdots,n)$,将密文对 (a,b) 发送给银行。

2.4 用户选择数字商品

用户从 $(number_i,Q_i(m_i))(i=1,2,\cdots,n)$ 中选定数字商品 m_i,这里选中的是一个数字序号 $\alpha(1 \leqslant \alpha \leqslant n)$,采用匿名支付手段向银行支付数字商品 m_i 的金额 p_i,匿名支付成功后,银行计算 $b/[a^x \pmod p]$,得到 $\{(number_i,p_i),i=1,2,\cdots,n\}$,然后运行 ElGamal 签名算法生成签名 $r=g^k \pmod p$,$s=(h(M)-xr)k^{-1} \bmod (p-1)$,并将 (r,s) 通过安全秘密信道发送给用户。

用户收到银行发来的 ElGamal 签名 (r,s) 并计算:$s'=(t+s) \bmod (p-1)(t \in_R [1\cdots 2^{t_1}(p-1)])$,得到 (r,s',g^u,y^α),并发送给商家,$u \in_R [1\cdots 2^{t_1}(p-1)]$。

商家收到 $(r,s',g^u y^\alpha)$,选择 $l,v_i \in_R Z_{p-1}/\{0\}$,计算:

$a=r^l$

$c_i=m_i(r^{s'}y^r/g^{h(M)})^l(g^u y^\alpha/y^i)^{v_i}$

$b_i=g^{v_i}$

其中 $1 \leqslant i \leqslant n$。

然后将 (a,b_i,c_i) 发送给用户。

只有选择 $i=\alpha$ 的用户可得 (a,b_α,c_α),$c_i=m_i(r^{s'}y^r/g^{h(M)})^l(g^u y^\alpha/y^i)^{v_i}$ 也相应地成为 $c_\alpha=m_\alpha(r^{s'}y^r/g^{h(M)})^l(g^u y^\alpha/y^\alpha)^{v_\alpha}$,又 r、t 和 u 已知,由 a 和 b_α 得 $r^{tl}g^{uv_\alpha}$,得 $m_\alpha=c_\alpha/a^t b_\alpha^u$。

3 方案分析

3.1 方案的正确性证明

证明 方案中接收方是用户,并持有签名 (r,s),所以可

得到

$$r^{s} = g^{k(h(M)-xr)k^{-1}} = g^{h(M)-xr} = g^{h(M)}/g^{xr} = g^{h(M)}y^{-r}$$

所以以下等式成立:

$$(r^{s'}y^{r}/g^{h(M)})^{l} = (r^{s+t}y^{r}g^{-h(M)})^{l} = (g^{h(M)}y^{-r}r^{t}y^{r}g^{-h(M)})^{l} = r^{tl}$$

t 和 l 分别是用户接收方和发送方商家选择的随机数,因此双方可以有条件进行密钥协商。只有用户才知道在选择数字商品阶段的选择 α,也只有用户才知道在信息交互阶段选取的随机数 t 和 u,这使得只有当 $i=\alpha, 1\leqslant i\leqslant n, 1\leqslant\alpha\leqslant n$ 时,持有签名的用户才能解密得到且只能得到自己选择的消息,以下等式成立:

$$c_{\alpha} = m_{\alpha}(r^{s'}y^{r}/g^{h(M)})^{l}(g^{u}y^{\alpha}/y^{\alpha})^{v_{\alpha}} = m_{\alpha}r^{tl}g^{uv_{\alpha}}$$

用户知道 t 和 u, a, b_{α},计算出 l 和 v_{α},得到 $r^{tl}g^{uv_{\alpha}}$,则可得消息 $m_{\alpha} = c_{\alpha}/a^{t}b_{\alpha}^{u}$。

3.2　防欺诈性分析

在动态的电子交易环境中,交易双方的诚信需要技术的约束,安全有效的交易方案应该具有防止商家恶意欺诈行为的功能。

该方案中用户拥有的签名和用户在网上购物时的选择 α 是无条件安全的。在计算性 Diffie-Hellman(CDH)假设成立的条件下,只有拥有签名的用户才可能进行密钥协商,如果有恶意攻击者在协议执行过程中进行攻击,由于不拥有签名,攻击者在执行协议后也不可能和商家进行密钥协商。在判定性 Diffie-Hellman(DDH)假设是困难的条件下,用户只能得到 m_i,这里 $1\leqslant i\leqslant n, 1\leqslant\alpha\leqslant n, i=\alpha$,用户得不到其余消息的任何信息(即 $m_i, 1\leqslant i\leqslant n, 1\leqslant\alpha\leqslant n, i\neq\alpha$)。

在系统建立阶段,k 是一个随机数,用户拥有签名 (r,s),商家不拥有签名 (r,s)。在信息交互阶段,用户随机选择了 t 和 u,因此商家不可能通过计算得到 s 和 r,也就不可能得到用户是否拥有签名的任何信息,同时也不可能通过比较知道用户是否拥有签名。所以说,无论是在方案的哪个阶段,发送方都无法得到接收方个人信息,接收方的隐私得到了保护。

在方案的整个执行过程中,用户如果怀疑商家有欺诈行为,可以向方案中的权威机构 CA(这里是银行系统)提交商家公布的 $(i,h_i^1,h_i^2,s_i),(i=1,2,\cdots,n)$ 以及自己打开消息时得到的 $m_{\alpha} = c_{\alpha}/a^{t}b_{\alpha}^{u}$,提请银行进行仲裁。银行可以通过计算:$h_i^{1\prime} = h(number_i \mid M_i)$, $h_i^{2\prime} = h(number_i \mid p_i)$, $s_i' = sig(number_i \mid h_i^{1\prime} \mid h_i^{2\prime})$,然后比较 s_i 是否等于 s_i' 来判断商家是否存在欺诈行为。图 1 描述了方案详细的执行过程。

3.3　安全性分析

定理 1　基于 ElGamal 和 1-out-n 的可保护授权隐私网上交易方案具有不经意性。

证明　设 R' 为不拥有签名的其他接收方,在信息交互阶段拥有签名的用户接收方 R 发送的信息 (r,s') 的概率分布族为

$$\delta^{0}(k,t) = \langle g^{k} \bmod p, (t+s) \bmod (p-1) \mid k\in_R \mathbf{Z}_{p-1}^{*}, l\in_R [1\cdots 2^{t_1}(p-1)]\rangle$$

R' 不拥有签名,发送的随机信息的概率分布族为

$$\delta^{1}(k',t') = \langle g^{k'} \bmod p, t' \bmod (p-1) \mid k'\in_R \mathbf{Z}_{p-1}^{*}, l'\in_R [1\cdots 2^{t_1}(p-1)]\rangle$$

如果这里 t_1 给定,可以发现两个概率分布族均有 $(p-1)\Phi(p-1)$ 个点,取任意点的概率差不超过 $1/2^{t_1}(p-1)\Phi(p-1)$,概率差总体小于 $1/2^{t_1}$,因此从统计上 $\delta^{0}(k,t)$ 与 $\delta^{1}(k',t')$ 是不可区分的,对于 t_1 来说是可以忽略的,相对于 t 也是可以忽略的,所以说发送方得不到接收方是否拥有签名的任何信息,接收方是否拥有签名是无条件安全的。

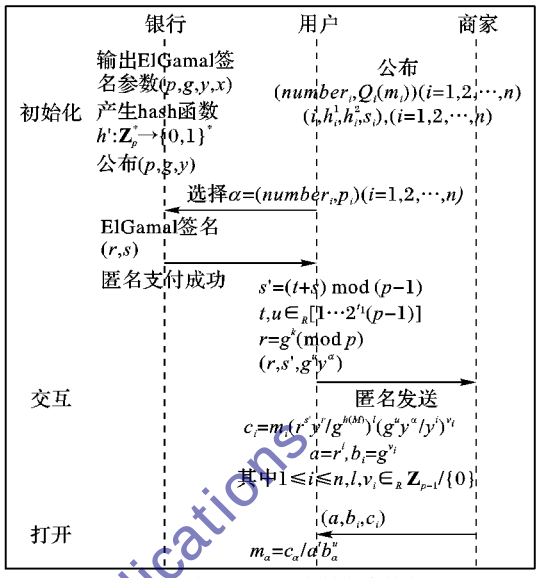

图 1　可隐私保护的电子交易方案执行过程

定理 2　接收方的选择 α 是无条件安全的,在交易的过程中发送方得不到接收方选择消息 α 的任何信息。

证明　假设存在 u' 和 α',使得 $g^{u}y^{\alpha} = g^{u'}y^{\alpha'}$,$u$ 是接收方在协议的信息交互阶段随机选择的,$u\in_R[1\cdots 2^{t_1}(p-1)]$,$\alpha$ 是接收方在协议的初始阶段选择的,这样接收方就可以通过求解离散对数得到两个秘密消息,但在 DDH 假设条件下这种情况是不可能发生的,因此正是基于离散对数的安全性,所以接收方的选择 α 是无条件安全的,也就是说发送方不能够通过计算得到发送方选择消息 α 的任何信息。

定理 3　在计算性 Diffie-Hellman 假设成立的条件下只有拥有 M 的 ElGamal 签名的接收方才能得到密钥。

证明　在协议的信息交互阶段发送方 S 对消息 $m_i(1\leqslant i\leqslant n)$ 进行了两次幂指数运算,这样做使得接收方如果想要解密成功就必须拥有签名和选择 α,也就是说需要知道 $(r^{s'}y^{r}/g^{h(M)})^{l}$ 和 $(g^{u}y^{\alpha}/y^{i})^{v_i}$,并且只能解密得到一个消息 $m_i(1\leqslant i\leqslant n, 1\leqslant\alpha\leqslant n, i=\alpha)$。假设攻击者为 R',在信息交互阶段完成后,攻击者 R' 通过某种方式得到了 $(r^{s'}y^{r}/g^{h(M)})^{l}$,令 $s = k'^{-1}(h(M)-xr') \bmod (p-1)$, $r' = g^{k'} \bmod p$,则数对 (r',s) 是对消息 M 的一个 ElGamal 签名。

因为 $s = k'^{-1}(h(M)-xr') \bmod (p-1)$,可以得到 $g^{s} = g^{k'^{-1}(h(M)-xr')} \bmod p$,所以有以下方程成立:

$$(r^{s'}y^{r}/g^{h(M)})^{l} \bmod p = (r^{s'}g^{(xr'-h(M))})^{l} \bmod p = (r^{s'}g^{-k'k'^{-1}(h(M)-xr')})^{l} \bmod p = (r^{s'}g^{-k's})^{l} \bmod p = r'^{(s'-s)l} \bmod p$$

以上分析可知,在计算性 Diffie-Hellman 假设成立的条件下只有拥有对 M 的 ElGamal 签名的接收方才能计算出密钥 $(r^{s'}y^{r}/g^{h(M)})^{l} \bmod p$,才可能得到消息 m_{α}。

4　结语

本文依据 1-out-n 不经意传输协议,提出了一个电子交易

方案。该方案基于 ElGamal 签名,结合 1-out-*n* 不经意传输协议,可用来保护电子交易动态环境中的授权隐私;方案中用户对自己的选择使用的是序号,具有制约性和隐蔽性,用序号作幂运算,加密得到密钥,完成密钥协商;商家运用这种对序号的制约,使得用户不能以没有选择的序号打开消息,用户可以得到且只能得到自己订购的数字商品;并对方案进行了正确性证明和安全性分析,结果表明方案具有不经意性、接收方选择的无条件安全性和在 CDH 假设下的安全性。方案和现有的网上交易方案相比不拘泥于价格的限定,依据用户选择的自选序号以及所拥有的加密签名,可以有效防止商家以次充好的恶意欺诈行为;采用 ElGamal 签名,生成的签名文件相对较短,签名时计算量较小;密钥协商时利用序号幂运算,实现密钥动态变化,整个方案在电子交易动态环境中适应性更好,安全性更强。方案目前的研究仍有不足之处:整个协议中没能考虑签名和用户对应的唯一性,也就是说,用户如果将拥有的签名给予第三方,协议无法识别拥有签名的第三方是否用户本身,这也是下一步研究的方向。

参考文献:

[1] TONG Y, TAO Y, TANG S, *et al*. Identity-reserved anonymity in privacy preserving data publishing [J]. Journal of Software, 2010, 21(4): 771 - 781. (童云海, 陶有东, 唐世渭, 等. 隐私保护数据发布中身份保持的匿名方法[J]. 软件学报, 2010, 21(4): 771 - 781.)

[2] LINDELL Y, PINKAS B. Secure two-party computation via cut-and-choose oblivious transfer [C]// TCC 2011: Proceedings of the 2011Theory of Cryptography Conference, LNCS 6597. Berlin: Springer-Verlag, 2011: 329 - 346.

[3] BAO F, DENG R H, FENG P. An efficient and practical scheme for privacy protection in the e-commerce of digital goods [C]// ICISC 2001: Proceedings of the 3rd International Conference on Information Security and Cryptology. London: Springer-Verlag, 2001: 162 - 170.

[4] MAO J, YANG B, WANG Y. A new scheme for privacy protection in the e-commerce of digital goods [J]. Acta Electronica Sinica, 2005, 33(6): 1053 - 1055. (毛剑, 杨波, 王育民. 保护隐私的数字产品网上交易方案[J]. 电子学报, 2005, 33(6): 1053 - 1055.)

[5] JIANG Y, ZHANG M, YANG B, *et al*. An online ordering scheme for privacy protection [J]. Journal of Human University: Natural Science Edition, 2010, 37(3): 77 - 79. (蒋亚军, 张明武, 杨波, 等. 一个具有隐私保护的网上订购方案[J]. 湖南大学学报: 自然科学版, 2010, 37(3): 77 - 79.)

[6] SHEN Y, LIN X. Schnorr signature-based privacy protection online ordering scheme [J]. Application Research of Computers, 2013, 30(3): 882 - 884. (申艳光, 林祥龙. 基于 Schnorr 签名的隐私保护网上订购方案[J]. 计算机应用研究, 2013, 30(3): 882 - 884.)

[7] ZHANG Y, ZHU Y. Price oblivious transfer based privacy protection transaction scheme [J]. Computer Application and Software, 2012, 29(5): 35 - 37. (张云鹤, 朱艳琴. 基于价格不经意传输的隐私保护交易方案[J]. 计算机应用与软件, 2012, 29(5): 35 - 37.)

[8] HUANG N, GUI X, YU S, *et al*. Privacy-preserving computable encryption scheme of cloud computing [J]. Chinese Journal of Computers, 2011, 34(12): 2391 - 2402. (黄汝雄, 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)

[9] XU J, HUANG X, GUO M, *et al*. Location privacy through anonymous chain in dynamic P2P network[J]. Journal of Zhejiang University: Engineering Science Edtion, 2012, 46(4): 712 - 718. (徐建, 黄孝喜, 郭鸣, 等. 动态 P2P 网络中基于匿名链的位置隐私保护[J]. 浙江大学学报: 工学版, 2012, 46(4): 712 - 718)

[10] ElGAMAL T. A public-key cryptosystem and a signature scheme based on discrete logarithms [J]. IEEE Transactions on Information Theory, 1985, 31(4): 469 - 472.

[11] TZENG W. Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters [J]. IEEE Transactions on Computers, 2004, 53(2): 232 - 240.

[12] LI N, DU W, BONEH D. Oblivious signature - based envelope [C]// PODC 2003: Proceedings of the 22nd ACM Symposium on Principles of Distributed Computing. New York: ACM, 2003: 182 - 189.

[13] OGAWA K, HANAOKA G, KOBARA K, *et al*. Anonymous pay-TV system with secure revenue sharing [C]// KES 2007: Proceedings of the 11th International Conference on Knowledge-based Intelligent Information and Engineering Systems, LNCS 4694. Berlin: Springer-Verlag, 2007: 984 - 991.

[14] JIAO Y, FU D. A sequential multi-signature scheme based on ElGamal [J]. Journal of Sichuan University: Natural Science Edition, 2013, 50(4): 757:759. (焦阳, 傅德胜. 基于 ElGamal 的有序多重数字签名方案[J]. 四川大学学报: 自然科学版, 2013, 50(4): 757 - 759.)

(上接第 2607 页)

[7] LAO N, COHEN W. Fast query execution for retrieval models based on path constrained random walks [C]// Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM, 2010: 881 - 888.

[8] SUN Y, HAN J, AGGARWAL C, *et al*. When will it happen? — Relationship prediction in heterogeneous information network [C]// Proceedings of the Fifth ACM International Conference on Web Search and Data Mining. New York: ACM, 2012: 663 - 672.

[9] YU X, SUN Y, NORICK B, *et al*. User guided entity similarity search using meta-path selection in heterogeneous information network [C]// Proceedings of the 21st ACM International Conference on Information and Knowledge Management. New York: ACM, 2012: 2025 - 2029.

[10] SHI C, KONG X, YU P, *et al*. Relevance search in heterogeneous networks [C]// Proceedings of the 15th International Conference on Extending Database Technology. New York: ACM, 2012: 180 - 191.

[11] JI M, SUN Y, DANILEVSKY M, *et al*. Graph regularized transductive classification on heterogeneous information networks [C]// Proceedings of the 21th European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases. Berlin: Springer-Verlag, 2010: 570 - 586.

[12] SUN Y, HAN J, ZHAO P, *et al*. RankClus: integrating clustering with ranking for heterogeneous information network analysis [C]// Proceedings of the 12th International Conference on Extending Database Technology. New York: ACM, 2009: 565 - 576.

[13] SHI J, MALIK J. Normalized cuts and image segmentation [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2000, 22(8): 888 - 905.