保护隐私的数字产品网上交易方案

毛 剑[1],杨 波[2],王育民[1]
(1. 西安电子科技大学 ISN 实验室,陕西西安 710071;2. 北京交通大学计算机与信息技术学院,北京 100044)

摘 要: 电子商务中需要尽可能地保护用户隐私,而密码技术则是这一需求的重要保障. 在安全的 1/2 不经意传输存在这一假设下,本文提出了一个安全且具隐私保护的数字产品网上交易方案. 方案很好的考虑了实际交易中可能出现的情况,并针对可能出现的种种欺诈行为(如:商家以次充好,买家一次消费多次交易等问题)给予了有效的解决. 同时结合匿名支付和匿名通信技术保证了用户交易的匿名性.

关键词: 不经意传输; 不经意多项式估值; 数字签名; 匿名支付
中图分类号: TN918. 1 **文献标识码**: A **文章编号**: 0372-2112 (2005) 06-1053-03

A New Scheme for Privacy Protection in the E-Commerce of Digital Goods

MAO Jane[1], YANG Bo[2], WANG Yu-min[1]
(1. *National Key Lab. Of ISN, Xidian Univ., Xi'an, Shaanxi* 710071, *China*;
2. *Dept. of Computer Science & Information Technology, Beijing Jaotong Univ., Beijing* 100044, *China*)

Abstract: It is well known that customers' privacy in electronic commerce should be well protected. The solutions may come not only from the ethics education and legislation, but also from cryptographic technology. A scheme for privacy protection in the E-commerce is proposed which is based on the existence of secure 1/2 oblivious transfer. It takes oblivious polynomial evaluation as its technical means to realize privacy protection for online customers and prevent the merchant from cheating efficiently; In addition, the scheme also ensure customers dealing with merchants anonymously.

Key words: obliviously transfer; obliviously polynomial evaluation; digital signature; anonymous payment

1 引言

电子商务正以惊人的速度迅速发展,且日渐进入人们的日常生活. 如何在电子商务中完善的保护用户隐私成为了人们关注的焦点问题之一. 某些商家在交易同时收集用户信息(如:爱好,购买能力等)且将其发送给他人用于商业目的是目前对用户比较严重的一种隐私侵害.

数字产品网上交易的隐私保护问题是指,用户在购买数字产品(如,电子图书,电子期刊,音像制品等)时,往往不希望商家知道他(她)是何时购买的何种商品,因为这样会暴露出用户的兴趣,购买习惯等个人隐私信息. 在实际生活中购买物理产品时往往很难做到这一点,而对于数字产品交易而言,这一需求是可以实现的,且无需太多的额外开销. 通常在交易中有能力进行隐私保护的商家往往能争取到更多的顾客.

目前针对数字产品交易的隐私保护也有较多的研究[1,4],然后大部分已有方案大都只针对两种特殊情形给予了解决方案:(1)商品的价格完全相同的情形[1],如音像制品的售卖,商品均为统一定价;(2)商品的价格完全不同的情形[4],如电视节目的订购中,不同的频道和节目通常有不同的定价. 然而在实际交易中通常的情形则是:林林总总的商品拥有不尽相同的定价,而不同的商品也可能价格相同.

本文在假设存在安全的这一前提下,基于多项式不经意估值(Oblivious Polynomial Evaluation,OPE)问题给出了一个全新而完善的数字产品网上交易方案,在安全便利的交易同时,有效的保护了用户的隐私. 方案保证诚实用户在进行正确付费后,能够得到且仅能得自己所需的商品. 在商家以次充好;恶意用户意图小额付费而获得高价商品以及一次付费获得多个同价商品等欺诈问题给予了很好的解决.

2 不经意多项式估值(OPE)协议

本节我们将对方案的重要模块——不经意多项式估值协议加以介绍:

2.1 定义

背景:Alice 拥有多项式 $P(x)$;Bob 拥有输入;

问题:如何令 Bob 计算出 $P(x_*)$ 的值,且满足:

(1) Alice 无法得到有关 x_* 的任何信息;

(2) Bob 无法得知除 $P(x_*)$ 以为有关 $P(x)$ 的任何信息;

这一问题即被称为不经意多项式估值(OPE)问题.

目前有关 OPE 问题的研究成果颇多,由于篇幅有限,我们仅就方案中采用到的一个实例加以简单介绍. 有兴趣的读者可参阅文[5~9].

我们首先介绍一个非常重要的密码学原语——1/2 不经意传输(1 out-of-2 oblivious transfer),记做 OT_2^1. 令 F 为一有限域.

定义 1 OT_2^1 协议由两方参与:发送者拥有输入 $(x_0, x_1) \in F$;抉择者拥有对 $\{0,1\}$ 的一个抉择 c.

称 OT_2^1 协议是正确的,如果对于 $\forall (x_0, x_1), c$,抉择者均

收稿日期:2004-06-27;修回日期:2004-11-12
基金项目:国家自然科学基金(No. 60073052)

能得到 x_c.

称 OT_2^1 协议是安全的,如果(1)抉择者无法区分出来自发送者的消息是 x_c 还是 x_{1-c};(2)发送者无法区分出来自抉择者的是 c 还是 $1-c$.

定义 2 一个 OPE 协议由两方参与:Alice 拥有一个域 F 上的多项式 $P(x)$;Bob 拥有输入 $x_* \in F$.

称 OPE 协议是正确的,如果对于 $\forall x_*$, $P(x)$,Bob 均可计算出 $P(x_*)$ 的值.

称 OPE 协议是安全的,如果(1) Alice 无法区分来自 Bob 的信息是 x_* 还是其他的 x;(2) Bob 无法区分 Alice 的消息是多项式 $P(x)$ 的计算结果还是另一个多项式 $P'(x)$ 满足 $P(x_*) = P(x_*)$ 的计算结果.

2.2 初始化参数

n:正整数;$[n]$:集合$\{1,2,\cdots,n\}$;v:n 维向量;v_i:v 的第 i 维元素,$i \in [n]$;v 记做:$v = (v_1, v_2, \cdots, v_n) = (v_i)_{i\in[n]}$;$p$:素数;$F = GF(p)$.

Alice 拥有:系数取自 $F = GF(p)$ 上的 d 次多项式 $P(x) = \sum_{i=0}^{d} a_i x^i$;

Bob 拥有:输入 $x_* \in F$.

令 $m = \lceil \log_2 |F| \rceil$;做如下变换:

(1) $P(x)$ 的系数 a_i 可以表示为 $a_i = \sum_{j\in[m]} a_{ij} 2^{j-1}$, $a_{ij} \in [0,1]$;

(2) Bob 计算 $v_{ij} = 2^{j-1} x_*^i$, $i \in [d]$, $j \in [m]$,显然,对于 $\forall i \in [d]$,均有 $\sum_{j\in[m]} a_{ij} v_{ij} = a_i x_*^i$.

2.3 安全的 OPE 协议

假设:存在一个安全的 OT_2^1.

Step1:Bob 准备 dm 对 $(r_{ij}, v_{ij} + r_{ij})_{i\in[d], j\in[m]}$,其中 r_{ij} 为随机取自域 F 中的元素.

Step2:对每对 $(r_{ij}, v_{ij} + r_{ij})$,Alice 执行一个独立的与 Bob 的 OT_2^1,得到

$$u_{ij} = \begin{cases} r_{ij}, \text{若 } a_{ij} = 0 \\ v_{ij} + r_{ij}, \text{若 } a_{ij} = 1 \end{cases}, \quad i \in [d], j \in [m].$$

Step3:Alice 给予 Bob:$Sum = a_0 + \sum_{i\in[d], j\in[m]} u_{ij}$.

Step4:Bob 计算:$P(x_*) = Sum - \sum_{i,j} r_{ij}$.

定理 1 上面给出的 OPE 协议是正确的.

证明:Bob 由 Alice 获得的.

$$Sum = a_0 + \sum_{i,j} u_{ij} = a_0 + \sum_i \sum_j (a_{ij} v_{ij} + r_{ij}) = P(x_*) + \sum_{i,j} Y_{ij}.$$

定理 2 上面给出的 OPE 协议是安全的.

证明:略去,可参看文献[7].

下面我们利用安全的 OPE 作为构件构造保护用户隐私的数字产品交易方案.

3 具有隐私保护的数字产品交易方案

在安全的 OT_2^1 存在这一假设下,我们将在本节给出一个具有保护用户隐私的数字产品交易方案:

3.1 模型

问题:设商家有 n 种商品待售,分别表示为:$M_1, M_2, \cdots, M_n$.

用户要购买第 i 种商品,且不希望商家知道其所购买的是何种商品.

3.2 具体方案

参数设置:

$M_1, M_2, \cdots, M_n$:n 种待售商品;

$p_1, p_2, \cdots, p_n$:对应于商品 $M_1, M_2, \cdots, M_n$ 的价格;

p:大素数;

E:经典的对称加密体制,如:AES,DES;其加解密表示如下:

加密:$C = E(k, M)$; 解密:$M = E^{-1}(k, C)$;

Sig:经典的数字签名体制,如:RSA,ELGAMAL;其签字及验证表示如下:

签字:$S = Sig_k(M)$; 验证:$V = Ver(S) =$"Yes"or"No".

$H(\cdot)$:哈希函数;

k_v—商家的签字密钥;k_b—银行签字密钥;k_u—用户签字密钥.

<u>商家(Vendor)初始化:</u>

Step1:商家将 n 种商品 $M_1, M_2, \cdots, M_n$ 进行编号,并将产品序号 i 与对应的商品 M_i 的品名公开;

Step2:对 $\forall i, 1 \le i \le n$,商家随机选取 $k_i \in F$,商家计算:

$C_i = E(k_i, M_i)$; $H_i = H(k_i)$; $S_i = Sig_{k_v}(i \| C_i \| H(k_i))$

Step3:商家向公共目录(public directory)公布:(i, C_i, H_i, S_i), $1 \le i \le n$.

Step4:商家将商品报价 $p_1, p_2, \cdots, p_n$ 发送给银行,银行对 p_i, $1 \le i \le n$ 进行签字:

$S_{p_i} = Sig_{k_b}(H(i \| p_i))$;

银行将 (p_i, S_{p_i}), $1 \le i \le n$ 返还商家.

Step5:商家选取随机数 $S_{p_0}, k_0 \in F$.

Step6:商家利用 Lagrange 插值多项式构造经过点

$(S_{p_0}, k_0), (S_{p_1}, k_1), (S_{p_2}, k_2), \cdots, (S_{p_1}, k_i), \cdots, (S_{p_a}, k_n)$

的曲线方程 $P(x)$.

<u>用户(Alice)下载付费</u>

用户要购买商品 M_i:

Step1:Alice 由公开目录中匿名下载与 M_i 对应的 (i, C_i, H_i, S_i);

Step2:Alice 采用匿名支付手段向银行支付商品 M_i 的金额 p_i. 支付成功后,银行对 p_i 计算:

$S_{p_i} = Sig_{k_b}(H(i \| p_i))$ 给 Alice.

<u>获得产品</u>

Step1:商家拥有多项式 $P(x)$,用户拥有多项式的一个输入 S_{p_i},通过上节引入的协议 $OPE(P, S_{p_i})$ 即可在商家不知 S_{p_i} 的情形下使用户 Alice 获得其所要购买商品的解密密钥 $k_i = P(S_{p_i})$.

Step2:Alice 通过 H_i 验证计算所得 k_i 的正确性.

Step3:Alice 计算:$M_i = E^{-1}(k_i, C_i)$.

4 方案分析

本文给出的方案具有以下显著特性:

(1) 在安全的 OT_2^1 存在这一假设下,付费用户可以顺利

图 1　具有隐私保护的数字产品网上交易方案

的从商家出得到其所购买的商品,且商家无法从交易过程中得知任何有关用户所购买的商品信息(因为商家无从得知用户在交易过程中的输入).

(2)通过引入商家对公开信息和交易信息的签字承诺,能够有效的阻止[1]中提到的商家通过以次充好偷梁换柱的手段来欺瞒客户的情形出现.

(3)通过对商品下载版本下载率的统计,依然可以保证商家有效的统计其产品的受关注情况.

(4)用户无法通过合谋来获得他们所付费的商品以外的商品.

(5)与文[1,4]不同,方案对于商品标价无特殊要求,商品的价格无须全部相同也无须全部不同,更符合现实中商品售卖的情形.且方案有效防止用户妄图仅通过一次付费获得两个相同价格产品的欺诈行为,同时也防止了用户意图通过低价付费获得高价商品的欺诈行为.

5　其他相关问题

5.1　匿名交易

(1)用户可以从公开目录中匿名下载所需商品:通过某一代理,可以隐藏用户 IP,且若通过拨号上网,IP 更是一次一变;此外 Zero-Knowledge Inc[2]还提供了一些其他的匿名下载工具.

(2)用户可以通过隐匿信道(anonymous channel)收发信息而不被追踪.如:E-mail 的匿名性可通过 Mixmaster re-mailers[10]来实现;而 HTTP 的匿名性可通过葱头路由(Onion-Routing)系统来实现[11].

匿名的电子支付系统[3]与匿名下载、匿名通信相结合能够很好的保障用户匿名交易的实现.

5.2　版权问题

版权问题是数字产品在电子商务中的致命问题,遗憾的是至今仍无满意的解决方案,现阶段对数字水印在多媒体数字产品版权保护中的应用已进行了很多研究,而其着眼点主要在于追踪到非法盗版而非防止盗版.而文本形式的数字产品(如,电子图书,期刊等),则很难采用水印进行保护.

版权保护的另一种方法则是采用所谓的防篡改软件(tamper-resistant software).这种技术仍处于初级阶段,它保证所有数字产品的加解密均在防篡改软件中进行,我们可以尝试通过防篡改软件技术对商家提供的数字产品加以版权保护.

6　结论

本文在假设存在安全的 OT_2^1 这一前提下,基于多项式不经意估值协议给出了一个全新而证证诚实用户在进行正确付费后,能够得到且仅能得自己所需的商品.在商家以次充好,恶意用户意图小额付费而获得高价商品以及一次付费获得多个同价商品等欺诈问题给予了很好的解决.

参考文献:

[1] Feng Bao, Robert H Deng. An efficient and practical scheme for privacy protection in the E-commerce of digital goods[A]. Proc. ICICS'2000[C]. LNCS 2015, Springer Verlag, 2001. 162 - 170.

[2] Zero-Knowledge System Inc[EB/OL]. http://www.zero-knowledge.com/.

[3] Donal O'Mahony, Michael Peirece. Electronic Payment Systems[M]. Artech House, 1997. 145 - 190.

[4] B Aiello, Y Ishai, O Reingold. Priced oblivious transfer: How to sell digital goods[A]. Advances in Cryptology-Eurocrypt 2001[C]. LNCS 2045, Springer-Verlag, 2001. 119 - 135.

[5] M Naor, B Pinkas. Oblivious transfer and polynomial evaluation[A]. Proc. 31st Ann[C]. ACM Symp, Theory of Computing, 1999. 245 - 254.

[6] A C Yao. How to generate and exchange secrets[A]. Proc. 27th Ann. IEEE Symp[C]. Foundations of Computer Science, 1986. 162 - 167.

[7] Yan-Cheng Chang, Chi-Jen Lu. Oblivious polynomial evaluation and oblivious neural learning[A]. Proc. 31st ACM Symposium on Theory of Computing[C]. 1999. 245 - 254.

[8] Y Ishai, E Kushilevitz. Randomizing polynomials: A new representation with applications to round-efficient secure computation[A]. Proc. 41st Ann IEEE Symp[C]. Foundations of Computer Science, 2000. 294 - 304.

[9] O Goldreich, S Micali, A Wigdersion. How to play any mental game or a completeness theorem for protocols with honest majority[A]. Proc. 19th Ann[C]. ACM Symp, Theory of Computing, 1987. 218 - 229.

[10] Chaum D. Untraceable electronic mail, return addresses, and digital pseudonyms[J]. Communications of the ACM, 1981, 24(2): 84 - 88.

[11] Goldschlag D, Reed M, Syverson P. Onion routing for anonymous and private communications[J]. Communications of the ACM, 1999, 42(2): 39 - 41.

作者简介:

毛　剑　女,1978 年 2 月出生于宁夏银川市,西安电子科技大学博士生,主要研究方向:密码学及其应用,电子商务和网络安全.E-mail: maoxiaojane@hotmail.com

杨　波　男,1963 年 5 月出生于陕西富平,博士,北京交通大学计算机与信息技术学院教授、博士生导师,目前研究兴趣为密码学、网络安全.