基于比特承诺的电子彩票方案

郑 东[1],张 彤[2],陈克非[1],王育民[2]
(1. 上海交通大学计算机科学系,上海 200030;2. 西安电子科技大学 INS 国家重点实验室,西安 710071)

摘 要: 随着电子商务的日益成熟,电子彩票也将是人们生活中不可缺少的商务活动. 本文给出了一种基于比特承诺的电子彩票发行方案——有可信方参与的"在线"方案,此方案克服了已有方案对时间要求苛刻的缺陷,与现有的结果相比,具有更好的公平性.

关键词: 电子彩票方案; 比特承诺
中图分类号: TN918 **文献标识码**: A **文章编号**: 0372-2112 (2000) 10-0141-02

Lottery Scheme Based on Bit Commitment

ZHENG Dong[1], ZHANG Tong[2], CHEN Ke-fei[1], WANG Yu-min[2]
(1. *Dept. of Computer Science and Engineering, Shanghai Jiaotong Univ., Shanghai* 200030, *China*;
2. *Key Lab. on ISN, Xidian Univ. Xi'an* 710071, *China*)

Abstract: With the growing popularity of electronic commerce, electronic lottery will be one of the necessary businesses in the Internet. One "on-line" lottery scheme based on bit commitment is presented, which has the advantage of fairness and that it overcome the limitation on time.

Key words: electronic lottery scheme; bit commitment

1 引言

随着电子商务的日益发展,网上的彩票交易——电子彩票也将成为不可缺少的业务之一. 这种彩票的发行至少需要满足传统彩票的性质,即对于每个彩票的购买者都是公平的,且彩票的发行者不能欺骗彩票的购买者. 关于电子彩票的讨论已有一些论文,但大多数是讨论电子彩票的支付系统. 与本文最相关的是文献[1]. 但文献[1]给出的方案中,要求客户的计算能力是"中等"程度,即客户对抽奖结果的预料能力限制在一个时间区间内,这在实现过程中是非常困难的,主要原因是无法把所有客户的计算速度限制在一个合适的范围内. 为了克服这种对计算时间要求的苛刻性,本文提出基于比特承诺的实现方案,此方案克服了文[1]中存在的缺陷,同时,对客户及彩票发行者,满足更好的公平性.

1.1 电子彩票的一般性质

本文给出的电子彩票发行方案具有下列性质:

(1) 中彩结果完全由购买彩票者的票号及他们提交的随机数决定;

(2) 奖金的数额不超过售出彩票的金额总和;

(3) 随机性与公平性,即任何一个随机选取的票号都能使得最终结果随机化;

(4) 可验证性,任何人都可以验证上述几条,同时,卖出的总票数,票号,得奖结果的标准及奖金分配标准是可以公开验证的.

票据的假设 首先,假设有独立的认证系统可用于票据的真实性与完整性检验,即假设所有流通的票据都是有效的. 本文还假设票据的弱公平交换,即当票据出售后,票据出售者能够得到卖票的货币(若发行者愿意,也可以免费发送给自己或其朋友票据),如果奖金的结构是合理的,发行者这样做,没有比其它彩票购买者有获利优势). 在彩票出售之前,要公开宣布出售票据的开始时间和结束时间,票号可以重复,即多个人可以选择同一票号,购买者可以选择自己喜欢的票号,如果抽彩的结果是公平地基于所卖的票号,且票号表单(出售的所有票号列表)在售票结束之前是不可预料的.

获胜者的决定方法 在决定获胜者时,彩票发行系统输出一个决定获胜者的数字. 只考虑第一赢者(赢者平分所有奖金). 如果彩票号和输出数字是用二进制表示,且票号是随机选取的,决定获胜者最自然的方法是,赢者为其彩票号码与输出数字的 Hamming 距离最小者. 奖金数额可以预先决定(不依赖于参与者),还可以由参加者总赌注的一定比例决定.

2 基于"比特承诺"的彩票发行方案

2.1 比特承诺

比特承诺方案是密码学协议的重要成分,基本思想如下:承诺者 Alice 向接受者 Bob 承诺一个消息,承诺过程要求满

收稿日期:1999-07-05;修回日期:2000-04-19
基金项目:国家自然科学基金(No. 69773013,69973031)

足:(1) Alice 向 Bob 承诺时,Bob 不可能获得承诺消息的任何信息;(2) 一段时间后,Alice 能够向 Bob 证实她所承诺的消息,但是 Alice 不能欺骗 Bob.

Alice 要向 Bob 承诺一个消息 M,简单的承诺方法是:承诺者 Alice 生成两个随机数 $R1$ 和 $R2$,利用 Hash 函数 h 计算 Hash 值 $h(R1, R2, M)$,并向 Bob 发送 $R1$ 和 $h(R1, R2, M)$. 当 Alice 向 Bob 出示消息 M 时,她向 Bob 发送 $R2$、M,由 Hash 函数的性质,在 Alice 向 Bob 发送 $R1$、$h(R1, R2, M)$ 后,Bob 不知道 M. 同样,由 Hash 函数的性质,Alice 不能找到 R'_2,M',满足 $h(R1, R2, M) = h(R1, R'_2, M')$,这使得 Alice 不能够欺骗 Bob.

2.2 基于"比特承诺"的彩票发行方案

本节给出基于比特承诺的一种方案——具有可信任第三方 C 参与的"在线"方案. 彩票发行方案步骤如图 1 所示.

(1) 可信任的第三方 C 向公众公布彩票发行时间 T、抽彩算法 F(如 Hash 函数)的承诺值 $commit(F)$,该算法依赖于每个购买彩票的票号,计算结果是不可预料的,即改变输入的每个比特都使得输出的几乎一半比特发生改变;

(2) 发行彩票开始时,购买者 P_i ($i = 1, 2, \cdots$) 才能够向彩票发行者 Z 购买彩票,购买者可以挑选自己喜欢的票号 $numberi$,票号可以重复,即多个人可以购买同样的票号(一旦购买成功,票号将是不可伪造和不可更改的);

(3) 发行机构要把售出的票号公布给每个购买者,在售票关闭时间,要把最终出售的票号表单给出(这使得每个参与者可以验证抽彩结果);

(4) 可信任方 C 出示抽彩算法 $F(.)$,并计算抽彩值 $F(list)$ 及每个票号的函数值 $F(numberi)$;

(5) 满足 $F(list) = F(numberi)$ 的票号为中奖号或使得 $F(list)$ 与 $F(numberi)$ 的 Hamming 距离最小的票号为中奖号.

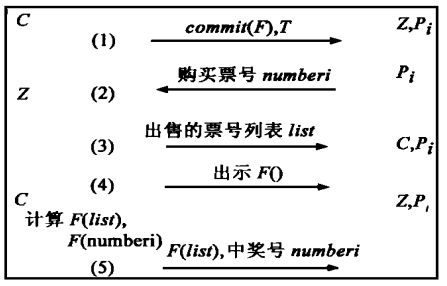

图 1 彩票发行"在线"方案

方案的可行性分析:

(1) 由于在客户购买彩票结束之前,任何人都不知道具体的算法 F,而抽彩算法的计算结果是依赖于所有购买的票号 $(list)$,因此,在售票结束之前($list$ 公布之前),任何人不可能预计算哪一个票号更容易得奖.

(2) 即使彩票的发行者 Z,由于不知道算法 F,所以也不可能控制票号进行一些预计算,找到有利于自己的票号. 因此,彩票的发行者也不可能作弊,即结果对每个人都是随机和公平的.

(3) 快速可验证性. 在进行抽彩计算时,算法和所有票号的表单($list$)是公开的,任何参与者都可以快速验证抽奖结果.

2.3 与文献[1]中方案的比较

文[1]讨论的方案如下:(1) 有一个公开的抽彩算法 h(如 Hash 算法),一个弱比特承诺函数(WSBC function) ω; (2) 每个客户可以选择自己喜欢的票号; (3) 在最终票号表单给出后,计算 $h(list)$,并求满足 $\omega(o) = h(list)$ 的号码 o,则 o 是中奖号码. 文献[1]所提方案存在的问题:

问题 1 为了防止彩票发行者在售票期间内,根据已售的票号,计算出结果,并添加新的票号以影响输出结果,方案要求计算 o 的时间要足够长(其实,这并不能防止发行者的攻击,例如,假设在售票时间关闭之前,只有两个人买票,而发行者不希望某客户 C 中奖,他可以很快计算出 $h(list)$,$\omega(numC)$,若 $\omega(numC) = h(list)$,则发行者增加一个票号. 这里我们注意到,计算 $\omega(numC)$ 是容易的).

问题 2 发行者的选择性攻击. 当出售一部分票号后,售票者中断与客户的联系,然后选择一些票号,根据出售的票号和选择的票号计算输出结果,若他能够选择充分多的票号集合,有一集合使得所选的某一票号中奖,他建立最后的表单(出售的票号和所选的票号集合),然后恢复与客户的联系,并公布建立的表单. 这样,他就成为中奖者. 防止此攻击的方法是,给每个票号添加时戳,要依赖于一个可信的时间服务器,对时间的严格要求在实现过程中是困难的.

本文方案的特点

本文方案利用比特承诺函数,首先克服了对计算时间要求的苛刻性,归纳起来,有如下优点:

(1) 客户所选择的票号可以重复,即不同的客户可以拥有相同的票号;

(2) 发行者没有机会欺骗客户,这是由于在售票期间,他无法进行预计算.

(3) 对每个客户是公平的,他可以选择自己喜欢的票号.

(4) 克服了对时间的苛刻要求,即不需要对每张票据加盖不同的时戳,只需要验证票据是否在有效期间内出售即可,这在实际实施时,容易实现.

3 结语

本文讨论了电子彩票与传统彩票的区别,并提出了基于比特承诺的电子彩票发行"在线"方案,这种电子彩票的发行比传统的彩票发行更公平. 只有少数文献讨论电子彩票抽奖方案,为电子彩票真正成为实现,需要进一步研究方便、实用的发行方案.

参考文献:

[1] David M. Goldschiag and Stuart G. Stubblebine. Prblically verfiable lotteries: financial Cryptography (FC '98) [C]: Preproceedings, Anguilla BWI, February, 1998: 214 - 226, Final proceedings forthcoming from Springer-Verlag.

(下转第 35 页)

值为 0 或 255 的点,如果原图像中包含很多取值为 0 或 255 的点,FDWM 将导致图像失真,而且 FDWM 不能直接应用于高斯噪声和噪声点在 0 到 255 之间随机取值的图像,直接应用的效果是很差的,必须加以算法改进,对于 FDWM 应用于随机噪声消除的算法改进将另撰文论述.

参考文献:

[1] Abreu E., Lightstone M., Mitra S. K. and Arakawa K., A new efficient approach for the removal of impulse noise from highly corrupted images [J]. IEEE Tran. on Image Proc., June 1996, 5 (6): 1012 - 1025.

[2] Sun T. and Neuvo Y., Detail-preserving median based filters in image processing [J]. Pattern Recognition Letters, Apr. 1996, 15: 341 - 347.

[3] Wang Z. and Zhang D., Restoration of impulse noise corrupted image using long-range correlation [J]. IEEE Signal Processing Letters, 1998, 5(1): 4 - 6.

[4] Zhang D. and Wang Z., Impulse noise detection and removal using fuzzy techniques [J]. IEE Electronics Letters, Feb. 1997, 33(5): 378 - 379.

[5] Wang Z. and Zhang D., Progressive switching median filter for the removal of impulse noise from highly corrupted images [J]. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, Jan. 1999, 46(1): 78 - 80.

[6] Lee C. S., Kuo Y. H. and Yu P. T., Weighted fuzzy mean filters for image processing [J]. Fuzzy Sets and Systems, 1997, 89: 157 - 180.

[7] Peng S. and Lucke L., Multi-level adaptive fuzzy filter for mixed noise removal [J]. Proc. IEEE Int. Symp. Circuit Syst., April 1995, 2: 1524 - 1527.

作者简介:

杨群生　1965 年 4 月出生,1987 年毕业于江西赣南师范学院数学系,1997 年获华中理工大学应用数学专业硕士学位,现为华南理工大学通信与信息系统博士研究生. 主要研究方向包括图像处理、神经网络、模糊技术等.

陈　敏　1980 年 12 月出生,1999 年获华南理工大学通信与信息系统专业学士学位. 现为华南理工大学通信与信息系统专业硕士研究生. 主要研究方向包括视频编码与图像处理、神经网络、模糊技术等.

余英林　1932 年生,1961 年获中国科学院所副博士学位. 现为华南理工大学电子与通信工程系教授、博士导师. 目前的主要研究方向包括图像与图形处理、神经网络、信号处理、模式识别、模糊技术等.

(上接第 142 页)

[2] David Wheeler. Transactions using bets [A]. In security protocols: 4th International Workshop [C]. M. Lomas (ed), Springer-Verlag, LNCS 1189: 89 - 92, 1996.

[3] Paul Syverson. Weakly secret bit commitment: Applications to lotteries and fair exchange [A]. In Proceedings of 1998 IEEE Computer Secutity Foundations Workshop [C], Rockport Massachsetts; 211 - 326, June, 1998.

[4] Ronald L. Rivest. Electronic lottery tickets as micropayments [A]. In Financial Cryptography: FC '97 [C], Proceedings, R. Hirschfeld (ed.), Springer-Verlag, LNCS, 1998, 1318: 307 - 314.

作者简介:

郑　东　1964 年生于山西翼城县,1999 年获西安电子科技大学密码学博士学位,现在上海交通大学计算机系从事博士后研究工作,研究方向是密码学与信息安全.

张　彤　1966 年出生,1987 年毕业于西安交通大学自动控制系,1990 年于国防科技大学获工学硕士,现在西安电子科技大学攻读密码学博士学位,主要研究方向是密码学与保密通信.