基于比特承诺的无可信第三方的电子彩票方案①

翟 耀 赵一鸣 (复旦大学 软件学院 上海 200433)

摘 要: 基于比特承诺，给出了一种无需可信第三方的电子彩票方案。该方案不要求购买者在线，不对购买者的计算能力做出苛刻限制，不要求可信第三方参与。该方案具有不可伪造性，公平性，公开验证性等特点。该方案还与传统彩票有良好的兼容性。

关键词: 比特承诺；数字签名；电子彩票

E-Lottery Scheme Without a Trusted Third Party Based on Bit Commitment

ZHAI Yao, ZHAO Yi-Ming

(Software School, Fudan University, Shanghai 200433, China)

Abstract: Based on bit commitment, this paper designs an e-lottery scheme which does not involve a trusted third party. This scheme does not assume all the purchasers are online. It overcomes the limitation of the purchasers' computing power and does not need to involve a trusted third party. There are many security properties in this scheme, such as unforgeability, impartiality, publicly verification and so on. This scheme also maintains compatibility with the traditional lottery.

Keywords: bit commitment; digital signature; E-Lottery

1 引言

随着电子商务的日益发展，电子商务终将不再局限于狭义的商务范畴，而将开始在与居民生活息息相关的各种服务之中起到重要作用。

因为传统彩票存在着诸多的缺点[1]，所以电子彩票的出现成为必然，并终将在彩票事业中成为不可缺少的业务之一，成为社会信息化的重要领域。通过互联网发行电子彩票，可以使投注者不受时间、地点的限制，随时随地都可以进行彩票的投注、查询以及兑奖，免去了投注者往返投注站和兑奖点的劳顿，同时也极大降低了彩票的发行成本。

目前，限制我国电子彩票发展的核心问题主要是技术问题[2]。技术问题解决了，电子彩票才能取得广大彩民的信任，从而使得电子彩票取得更大的市场空间，得到更快的发展。

电子彩票的发行，在技术上至少要保证满足传统彩票的性质，即对于每个彩票购买者都是公平的，而且彩票的发行者不能欺骗彩票的购买者。由于彩票涉及到巨大的经济利益，以及彩票中奖本身就存在着很大的随机性，所以在各个环节都可能出现不法分子。所以，彩民希望有个任何人无法控制抽奖结果，并且自己能够参与抽奖的可信彩票环境。并且，由于电子彩票方案还在研究中，而且在物质条件受限的地区下，传统彩票依然有自己的市场，所以现实中不宜在短期内将传统彩票全部升级为电子彩票，而是应该先试用与传统彩票有相当的兼容性的电子彩票方案，最终把传统彩票方案逐步过渡到电子彩票方案上。

关于电子彩票已经有不少学者做出了深入的研究。文献[3,4]中，要求购买者的计算能力是“中等”程度的，即要求购买者对抽奖结果的预料能力限制在一个时间区间内。这样苛刻的计算时间要求，在实现中是相当困难的。并且在文献[3]中，只有某一指定时段内的购买者参与到中奖数字的产生中，这使得管理者和部分购买者的勾结成为可能。文献[5]中，每个

① 基金项目:国家自然科学基金(60573054)
收稿时间:2009-09-30;收到修改稿时间:2009-10-26

购买者都可以参与到中奖数字的产生，但是该方案要求在一些过程中购买者在线，这点也是不现实的。在文献[6,7]中，存在着可信第三方，而且可信第三方的权限太大，发行机构很容易和可信第三方勾结。在文献[8]中，延迟函数计算仍然比较困难，并且不能抗拒拒绝服务攻击。

关于电子彩票方案的最新研究走向了基于彩票内容保护的方向，并取得很大的进展。文献[9]要求发行商和银行在兑奖前不能获得任何投注彩票号码，这样就可以有效防止发行商和银行勾结伪造彩票和虚构发售额，并同时保证彩票不可伪造。文献[10]在文献[9]的基础上做出了改进，该方案在链的最后一个节点加入投注承诺，使得发行商不能在此节点伪造彩票，并采用了公布平台。但是这两种电子方案都基于彩票内容保护，而与传统彩票相差甚远，难以进行平缓过渡。

根据以上分析，本文提出一种方案，较好的解决了上述问题：该方案不要求彩票购买者在线，不对彩票购买者的计算能力做出苛刻限制，不要求可信第三方参与，并且该方案与传统彩票有相当的兼容性。

2　安全电子彩票的一般性质

根据电子彩票的性质，电子彩票的安全性质需要满足：

(1) 可验证性：购买者的号码、注数以及真伪可验证，彩票的中奖结果、销售金额可验证，中奖号也可验证。

(2) 随机性：彩票的中奖结果是随机的。

(3) 公平性：每个投注号的中奖几率都是一样的，即使是发行方或者银行方亲自去购买彩票，它所选取的投注号的中奖几率也和普通购买者的选取的投注号的中奖几率相同。银行可以发送给自己或者朋友票据，只要自己承担彩票的面值即可。银行方这样做，同等情况下并不会比其他购买方更高的中奖可能。

(4) 不可伪造性：购买者获得彩票的唯一方式是从银行方购买彩票。任何时候，购买者都不能伪造彩票。

(5) 不可否认性：彩票活动中，任何一方都不能否认自己的行为。

(6) 不可预测性：没有哪一方能够提前知道中奖号，甚至得不到关于中奖号的任何信息。有限范围内的联合作弊也是不行的。

(7) 保密性：购买者的信息得到最大限度的保密，只有与其直接发生购买关系的银行知道购买者的个人信息。

票据的假设：首先假设存在一个独立的认证系统，可以用于彩票的真实性和完整性的检验。再假设彩票的弱公平交换：彩票出售后，出售彩票的银行能得到等于售出彩票的面值的货币；对应价值的货币交付后，购买者能得到相应的彩票凭据。彩票出售之前，要公开宣布出售彩票的开始时间和结束时间。购买者可以自由选择中奖号，不同购买者的选择的中奖号可以重复。

中奖者的决定方法：彩票方案输出一个和投注数字等长度的二进制格式的中奖数字。先计算所有实际投注数字与这个中奖数字的 Hamming 距离。(Hamming 距离是指代两个二进制数中不相同的位的个数，也就是两个数字异或操作的结果中 1 的个数)，按照 Hamming 距离的进行中奖数字的筛选。现行的办法是 Hamming 距离为 0 的投注数字获得一等奖，Hamming 距离为 1 的投注数字获得二等奖，Hamming 距离为 2 的投注数字获得三等奖。奖金数额一般由购买者总投注的一定比例决定，也可以在投注之前先决定。

决定出中奖等级之后，每个中奖等级中的中奖号的购买者按照投注数平分该中奖等级的奖金。

该方案是否公平，唯一因素是方案输出的中奖数字是否是随机的，不能被任何一方或者部分多方所篡改的。

3　预备知识和符号说明

本节先给出比特承诺的定义。

比特承诺方案是密码协议的重要成分，它最早由 Blum 于 1982 年提出。它的基本思想如下：承诺者 Alice 向接受者 Bob 承诺一个消息 m，承诺要求满足：Alice 向 Bob 承诺时，Bob 不可能获得承诺消息 m 的任何信息。一段时间后,Alice 能够向 Bob 证实所承诺的消息 m，但是 Alice 不能欺骗 Bob。一个直观的例子是，Alice 把消息 m 放在一个加锁的箱子里面送给 Bob，到 Alice 决定向 Bob 证实消息 m 时候，Alice 把消息以及箱子钥匙给 Bob，Bob 能够打开箱子并验证箱子里面的消息 m 同 Alice 出示的消息相同，且 Bob 确信箱子里的消息 m 在他保管期间没有

被篡改。

本文用到的符号说明如下：

(1) P 代表购买者，U 代表彩票发行商，Bi 代表第 i 家银行{i∈{1,⋯,k}}。

(2) L 代表投注数字，S 代表投注注数，BAN 代表购买者的银行账号，N 代表投注者的姓名，C 代表投注者的联系方式。Kc 代表某指定对称加密系统下，投注者所选的私钥。T 代表彩票售出时间。R 代表一个随机数。

(3) commit(x) 表示 x 的承诺值，H(x)表示使用 Hash 函数对 x 进行运算。

4 电子彩票方案

根据引言中的分析以及对安全电子彩票的一般性质的讨论，本文提出，一个安全的电子彩票方案中，最好不出现可信第三方，因为可信第三方的权限太大，发行机构有可能和可信第三方勾结，操纵整个彩票方案。此外，电子彩票方案也不能要求购买者一直在线，更不能对购买者的计算能力做出苛刻限制。

电子彩票方案是否安全，最重要的难题就是中奖号码是否安全。此处谈论的安全分两层含义：一是这个中奖号码一旦决定，没有任何一方或者部分多方可能更改它；二是在彩票购买阶段结束之前，即使这个中奖号码已经被决定了，任何一方或者部分多方也不可能知道它的值。经分析，在没有可信第三方参与的情况下，可以把中奖号码分解成多部分，每个银行用比特承诺的方式掌握中奖号码的一部分信息，而且每个银行掌握的信息都足以影响到中奖号码的每一位。到了开奖阶段，每个银行都不可否认的公布自己获得的那部分中奖号码的信息，这样就能解决中奖号码的安全问题。

基于如上分析，本文提出一种电子彩票方案。本方案把参与电子彩票分成三方：发行方，银行方和购买方。本方案的关键是：银行方不只一家银行，只要不是所有银行都勾结起来，就不能控制抽奖结果。购买方只需要相信在参与银行方的多个银行中，至少有一个是可以信任的，就能信任整个电子彩票环境是可信的。并且每个用户都很容易验证抽奖结果的产生是公平公正的。现在给出完整方案。

4.1 组织阶段

彩票发行方 U 申请到发行彩票的资格，进行前期宣传，公布整个电子彩票方案，以及对应阶段的开始时间和结束时间。

彩票发行方 U 和银行协商，选取 k 家银行，分别记作 $B_i\{i\in\{1,\cdots,k\}\}$。每个购买者都应该信任 $Bi\{i\in\{1,\cdots,k\}\}$中，至少有某一个银行是诚实的，不会作弊的。

彩票发行方 U 选定一个非对称加密系统，一个对称加密系统，一个比特承诺方案，一个 Hash 函数 H，并且公布。

每个银行 B_i 都选取一个公钥对，Ke_i，Kd_i。公布 Ke_i。

4.2 购买阶段

4.2.1 在可购买彩票的时间内，购买者 P_j 选择一个银行 B_i，从 B_i 处购买彩票。P_j 可以选取任意选择一家银行(可以不选自己认为诚实的那家银行)去购买彩票。P_j 向银行 B_i 提供 $Ke_i(L_j, S_j, BAN_j, N_j, C_j, Kc_j)$购买彩票。同时使用可信赖的支付方式进行货币支付。

4.2.2 银行 B_i 收到了 $Ke_i(L_j, S_j, BAN_j, N_j, C_j, Kc_j)$并且收到了足够的货币，计算 $Kd_i(Ke_i(L_j, S_j, BAN_j, N_j, C_j, Kc_j))$，得到$(L_j, S_j, BAN_j, N_j, C_j, Kc_j)$。然后尝试获得购买彩票的款项。 S_j*PRICE，PRICE 为每张彩票投注的价格。如果获取款项失败，则当即通知 P_j 购买失败。否则购买成功，银行返回 P_j 如下信息 $Kc_j(Kd_i(i, SERIAL, L_j, S_j, BAN_j, N_j, C_j, T_j))$， SERIAL 代表该张彩票在该银行的售出彩票的顺序号。用户可以计算 $Ke_i(Kc_j(Kc_j(Kd_i(i, SERIAL, L_j, S_j, BAN_j, Nj, Cj, T_j))))=(i, SERIAL, L_j, S_j, BAN_j, N_j, C_j, T_j)$来确定彩票信息是否正确。

4.2.3 每个银行 B_i 都维护着一个表，表的各列分别储存如下信息：SERIAL, L, S, BAN, N, C, T)。每当发售一张新彩票的时候，都把新彩票的信息加入到这个表的末尾，其中 SERIAL 项是在该银行出售彩票的次序号，依次递增 1。

4.2.4 可购买彩票的时间结束，每个银行 B_i 都关闭自己的出售渠道，都向外界公布自己所售出的彩票的张数，总注数，总营业额。

4.3 摇奖阶段

每个银行 B_i 选取一个和 L 等长的随机数 R_i。公布其承诺值 commit(Ri)。

4.4 同步阶段

每个银行 B_i 选出自己的售出彩票表的(SERIAL, L,

S)几列，设该子表为 T_i。每个银行 B_i 都对 T_i 做 H (T_i)运算，然后公布该值。

然后，每个银行 B_i 都把 T_i 给发行方以及其他所有银行一份拷贝。由发行方计算 H (T_1, T_2, …, T_k)并且公布。各银行有义务检查一下自己得到的 Tx{x ∈ {1,…,k}}，计算 H (T_x)，以及计算 H (T_1, T_2, …, T_k)，从而达到售出彩票的投注票号、注数等信息的一致共享。各个银行确认完毕之后，由彩票发行方公布售出总量，上期余额，本期奖池滚动奖金等信息。

4.5 开奖阶段

每个银行 B_i 公布自己的随机数 R_i，就得到了 R_1, R_2,…, R_k。任何一方均可用此前公布的 commit(R_i) 对其作验证。

计算 $R_0=R_1 \oplus R_2 \oplus \cdots \oplus R_k$，$R_0$ 为中奖号码。

4.6 兑奖阶段

公布 R_0 作为中奖号码。按照 Hamming 距离算法计算一等奖、二等奖、三等奖等获奖购买者的中奖号。发行方 U 委托各个银行 B_i 根据中奖算法公布获奖者并且按照预留的联系方式通知中奖者，同时对外界公布获奖彩票的中奖号以及序号。

4.7 结算阶段

当公示期结束而且没出现异议的情况下，发行方 U 根据各银行 B_i 售出彩票的收入、银行佣金比例、从该行售出的彩票的中奖情况等信息和各银行进行财务结算，同时每个银行 B_i 负责代替发行方发放在本行售出的中奖彩票的奖金。

4.8 清理阶段

发行方 U 和每个银行 B_i 做好必要的留档和公证之后，清理数据库和档案。

5 安全性与性能分析

5.1 安全分析

在本方案中，发行方没有作弊的能力，银行方的部分联合作弊也没有作用，购买者也不能作弊，而且中奖者的资金安全有充分保证。

(1) 发行方 U 不能作弊

中奖结果由购买者 P 选取的投注数字 L 和所有银行共同生成的中奖号码 R_0 决定，发行方不能干涉到其中任何一方面。

(2) 银行 B 不能部分联合作弊

银行方对中奖结果的影响，只能通过影响中奖号码 R_0 实现。但是 $R_0=R_1 \oplus R_2 \oplus \cdots \oplus R_k$，任何一个 Ri 都能影响 R_0 的所有的位。也就是说，只要有一个 Ri 没有被提前泄露，即使其他的所有的 R_j\{j ∈ {1,…,k},j ≠ i}都被泄露或者因为串通而被共享，作弊者也无法得到关于 R_0 的任何信息。所以，只要存在一个不作弊的银行，其他所有银行的联合作弊也将无效。

(3) 购买者 P 没有伪造彩票谎称中奖的能力

由于 P_j 所得到的彩票凭据 Kc_j (Kd_i (i, SERIAL, L_j, S_j, BAN_j, N_j, C_j, T_j))，其中 Kd_i 是银行 B_i 的秘密信息，购买者没有能力伪造这样的一张彩票凭据。

(4) 任何人不能冒充中奖者冒领奖金

在购买彩票的时期，购买者 P 已经提供了自己的银行账号 BAN，姓名 N，联系方式 C，银行经过核对之后，直接向购买者的银行账号 BAN 打入奖金，这个过程中，任何其他人无法干涉。

即使发行方、部分银行、部分购买者进行联合欺骗，只要能够保证存在一个不参与作弊的银行，就能保证整个方案的公平性。

5.2 性能分析

本方案的对计算能力的花费主要在三个方面：购买阶段，同步阶段，兑奖阶段。其中购买阶段中，每售出一张彩票都要需要银行和购买者在线各自进行 2 次非对称加解密计算和 1 次对称加解密计算，代价是十分轻微的。同步阶段需要发行者和银行各自对 N(N 代表彩票售出总张数)行大小的表进行 HASH 计算。兑奖阶段需要进行 N 次异或运算。总的说来，该方案仅需要 O(N)次计算，和同类方案相比，该方案的效率相当优秀。对于拥有一定计算能力的银行来说，这样的计算是很轻微的代价。

5.3 兼容性分析

在传统彩票方案下，本方案可以协同传统彩票方案工作，仅需做出不多的改变：购买阶段的末段，银行对外公布的售出的彩票的张数，总注数，总营业额等数据应为电子彩票业务与传统彩票业务之和；电子彩票的摇奖阶段移除；电子彩票的开奖阶段直接使用传统彩票方案的开奖结果。对用户来说，只要相信传统彩票方案的开奖结果是公平的，就完全可以相信包含了电子化部分的传统彩票方案是公平的。这样，电子彩票方案就能无缝的融入了传统彩票方案。

当电子彩票发展到一定阶段之后，电子彩票将成为彩票业的主流。但是由于物质条件的限制，传统彩

票并不能完全被移除，仍在一定程度上作为电子彩票的补充。而在该电子彩票方案下，传统彩票方案也能协同电子彩票方案工作，仅需做出不多的改变，并且不影响电子彩票方案的安全性：在购买阶段，传统彩票的购买者在投注点使用现金购买，而且获得的不是一个电子凭据，而是一个传统的纸张凭据，该凭据上打印着自己的原始投注信息，并且按照传统彩票方案加盖投注点公章以证明该彩票的合法性。凭据中的银行账号信息可以用身份证号码代替。兑奖阶段中，手持传统彩票的中奖者凭纸张凭据以及身份证去指定银行现场领取奖金。这样，传统彩票方案就能无缝的融入了电子彩票方案。

6 结语

本文以比特承诺为基础，给出了一种新的电子彩票方案。该方案不要求购买者在线，不对购买者的计算能力做出苛刻限制，不要求可信第三方参与，从而克服了以往的电子彩票方案的各种缺点。与以往的电子彩票方案相比，它具有更好的安全性和公平性，更有效的防止了各种攻击，效率也较高，还能和传统的彩票方案相互融合相互补充，从而具有高度的实用性。

参考文献

1 Ross A. How to cheat at the lottery. Computer Security Applications Conference. Phoenix, 1999.

2 祁明.电子商务实用教材.北京:高等教育出版社, 2000. 205－211.

3. Goldschiag D M, Stubblebine S G. Publicly Verifiable Lotteries: Applications of Delaying Functions: Financial Cryptography (FC'98): Preproceedings, Anguilla BWI, February, 1998. 214－226.

4 Weakly S P. Secret bit commitment: applications to lotteries and fair exchange. Proc. of 1998 IEEE Computer Secutity Foundations Workshop. Rockport Massachsetts, Cambridge, 1998. 211－326.

5 Zhou JY, Tan CF. Playing lottery on the internet. In ICICS'2001, LNCS 2229. Berlin: Springer, 2001.

6 Sako K. Implementation of a Digital Lottery Server on WWW. Secure Networking-CQRE(Secure)99, LNCS 1740, pages 101－108, Springer, 1999.

7 郑东,张彤,陈克非,王育民.基于比特承诺的电子彩票方案.电子学报, 2000,28(10):141－143.

8 Liu YN, Hu L, Liu HG, Tian JB. A New Efficient E-Lottery Scheme Using Multi-Level Hash Chain. Communicatiom Technology, ICCT'06, 2006. 1－4.

9 薛海峰,卿斯汉,张焕国.一种基于彩票内容保护的电子彩票方案.计算机工程与应用, 2007,43(21):26－28.

10 唐西林,郭海艮.一种基于彩票内容保护的电子彩票方案的改进.计算机应用研究, 2009,26(4):1506－1508.