RFID技术电子投票应用的探讨

刘 淳[1] 张建学[2]
(乐山师范学院计算机科学学院 乐山 614000)[1] (中国民用航空飞行学院计算机学院 广汉 618307)[2]

摘 要 无线射频识别(RFID)越来越广泛地运用在人们的日常生活和工作中。概述了RFID技术用于民意测验和区域选举的安全电子投票的软、硬件系统及其一般实施过程。与直接记录设备使用的选票和光学扫描相比,这种电子选票在选民身份的核实、快速重计和公式板上有一定的优越性。也讨论了电子选票的安全性问题,同时还对该系统用于远程投票的可行性进行了探讨。相对于现行诸如纸张选票的投票方式,RFID技术方法在理论上占有绝对的优势,它把数据(选票)从编程组件(投票软硬件)中分离出来,使投票系统具有可被验证性。

关键词 电子投票,RFID,安全性,可被验证性
中图法分类号 TP399 **文献标识码** A

Review on E-voting System Using RFID Technology and its Security

LIU Chun[1] ZHANG Jian-xue[2]
(Department of Computer Science, Leshan Teachers College, Leshan 614000, China)[1]
(Department of Computer, Civil Aviation Flight University of China, Guanghan 618307, China)[2]

Abstract Radio-frequency identification(RFID) is the use of a RFID tag applied to a product for identification and tracking using the radio waves. An active RFID tag contains a battery and is able to transmit signals when an external source has been successfully identified. RFID technology application has being applied in our life widely. In this paper, we viewed the RFID technology applied in a basic e-voting system and discussed its security. The RFID system shows the advantages over the currently existing optical voting system on verifying the voters, re-counting and public bulletin board. Remote voting may be realized based on the RFID technology. The RFID technology separates the votes from the voting equipments(software and hardware) and makes it more verifiable.

Keywords E-voting, RFID, Security, Verifiability

1 引言

无线射频识别(RFID)技术正在日常生活中得到广泛的应用。它最初用于制造业、链锁供应管理和库存控制,商用光学条形码在使用上占有一定优势。但近年来RFID技术已经涉足到消费者身份或物品识别领域,例如,道路收费站的车辆收费系统,护照的识别以及信用卡真伪的辨别系统等。半导体硅技术产业使用先进的技术能够制造出低成本的RFID识别系统,使得越来越多的RFID技术应用于我们所熟悉的各个领域。

基于Li博士等对RFID用于电子投票的一些基本构想[1],该构想是"frag"模型的延续[2],本文综述了实现这种投票方法的一些物理步骤和数学基础,并讨论了其存在的安全问题以及防范措施。文中详尽讨论了用作物理电子选票的活性RFID标签,提出的RFID方案即是这种模型的实现。廉价的RFID标签[1](几个k的字节)选票也能用于远程投票,作为解决缺席选票这类难题的理想替换。这种电子投票方式非常接近满足现有的选举法规,对其更改的要求很小,因而它在实践中易于实现。目前,一些欧美国家已开展对这种高效、安全和低碳的投票方式的前沿性和可实行性的研究,但在国内这一领域的研究还是空白。

首先,对这种电子投票系统提出4种理想假设:

• 具有一种低廉、易于读写的电子存储装置。

• 具有一种带读和(或)写软件能力的存储装置,它能可靠记录当地与外部公示板信息。换言之,我们不用担心软件送出错误的投票信息,因为只有恶意的外部干扰才会引起这类错误。

• 具有一个封闭的投票站和选区区域。例如,界定在一栋大楼内,所有人口和出口都能被监视。

• 具有投票者能够使用的触摸屏计算机设备和(或)标准PC HCI硬件,如键盘、鼠标、监视器和可携带移动存储小卡。

文献[3]讨论了在一些欧美国家里对投票技术和选举规则的实际考虑,论述了对投票规则和选举法如做很小修改,新的投票技术就可以得以运用的每一属性的特点。这种讨论也

刘 淳(1959—),男,硕士,讲师,主要研究方向为计算机及数字媒体应用,E-mail:liuc-xx@163.com。

[1]RFID标签是很小的廉价的包含一个IC卡和一个用于无线射频通讯的天线。通过无线射频通讯的读写器向RFID标签发射射频信号而记录它们的ID。有些读写器当发射射频信号时也可以向RFID标签传递能量。通常这种情况下,RFID标签没有能源的提供。因此人们普遍认为RFID会在今后取代光学码。

对我们在今后实行电子投票有着非常重要的借鉴作用，为了达到理想的研究目的，Li 博士等对文献[4,5]中描述的投票系统提出 5 项要求：

• 正确性：一次投票能被正确计票（仅仅一次）。

• 隐蔽性（匿名性）：每一具体投票人都不能从其投票结果中得以确认其身份。

• 无收据性：投票者不能得知其它人具体投票给谁。

• 可证实性：投票者具有在投票中再次确认的机会，特别情况下，要求有个人确认和普遍（区域）确认的措施。

• 稳健性：投票系统应能承受多种技术上的故障。

本文概述了一种满足以上 5 项要求的 RFID 电子投票系统。力求使可证实性和无收据性与非对称同构加密方案[6]和公示板[7]相结合。通过在网络上公布所有加密投票结果和投票的票根号码，选民可以了解他们的投票是否被计入。然而，票根号码与实际的选票可能没有联系（这两者在时间和可视空间上分开公布），不像在文献[8,9]中允许使用补名（writein）选票，我们运用同构加密方案中总计数的技术来避免投票人因胁迫或利诱而填写非其所意候选人的选票。

2 设备要求

我们提出的基于 RFID 技术的选举用电子投票系统有如下具体要求：

• 活性 RFID 标签：单一或集成的标签装置，能够被读取和被写入信息，具有存储完整选票的能力。将这种带有 RFID 标签、交给选民用的物理卡称为物理选票（PB：Physical Ballot）。选票即是存储在卡中的数据本身。

• 校验器：能够显示 PB 格式化内容的装置。

• 投票机：能够对 PB 进行读写操作的装置。

• 选票箱：一种能抗无线信号并用于存储和保护投票后 PB 内容的保护容器（法拉第盒子）。选票箱保持“锁定”状态，直到计票过程开始。

• 公示板（BB：Bulletin Board）用来在计票过程中记录选票。

• 一个中央数据库和（或）服务器，用于存储有效的 PB 信息，下面将作描述。

• 投票站工作人员使用 PB 激活器来激活 PB。

• 擦除器：安置在投票站每个出入口，用于检查和删除要离开投票区的 PB 装置。

我们对投票系统要求的流程做如下描述：RFID 标签用于投票过程，投票系统 5 个要求中的每一个都要被满足。在随后的投票过程中，投票者本人可以确定其投票既是匿名的，又能被正确计入系统。

我们假定系统使用的软件本身已经过检验并且安全可靠，不存在设计上的问题。软硬件必须依照选举管理法的要求来设置。对局域地区性的投票，安装一个局域网将能满足所需；对省或全国范围内的选举，如要求投票重计，则必须有中央数据库；而对远程互联网投票，将为缺席选票设计专门目的物理选票，我们将在后面的章节讨论其可能性。

3 投票、计票和核实过程

投票、计票和核实过程如下。

3.1 准备工作

在投票站开门前，假定已提前作好下列工作：

准备 1　投票工作人员安装好设备，一个校验器和投票机置于每个投票点，投票箱放于投票站中央位置。安装好公示板 BB 为本地写入和互联网读取，中央数据库安放于投票工作人员所在地。

准备 2　在投票系统中生成供一些非对称同构加密方案（这里不作专门论述）用的公钥和私钥。

准备 3　私钥通过非网络设备，如智能卡这样的装置，随机地放置于投票机和校验器中。然后从生成私钥的系统中删除私钥，智能卡在当日被锁存。

准备 4　工作人员在物理选票 PB 上设置公钥并使其激活（未锁定状态），然后交予所有已登记的选民。数据库存放每一个 PB 上的全球惟一标识符（GUID：Global Unique Identifiers），这样，保证每个 PB 的 GUID 一次投票仅能被计算一次。

3.2 投票过程

投票者按以下步骤进行投票：

步骤 1　投票者到达投票站。如果投票者携带有非屏蔽活性的 RFID 标签，它将被擦除器检测到并作处理（这样做用于阻止投票者携带预先装有病毒的 RFID 标签进入投票站）。

步骤 2　投票站工作人员核实投票者，确认其已经登记并能够投票（这一步骤是人工进行的）。工作人员交给投票者一个随机取出的有效、未锁定的物理选票 PB。

步骤 3　投票者进入投票室。

步骤 4　投票者插入 PB 到校验器中，校验器显示该 PB 还未被用过。

步骤 5　投票者从校验器中取出 PB 再插入投票机，投票机确认该 PB 还未被使用过并且有效，可允许投票者继续操作。

步骤 6　投票者进行投票。投票机显示填有内容的选票并询问投票者是否希望投送该选票，如果选民拒绝，回答不，投票机关闭显示，投票者取出 PB 并离去（交还还未使用的 PB 给投票站工作人员）；如果投票者同意，经再次确认，可继续进行操作。投票机向 PB 写入加密的选票并“锁定”PB，并对数据库中 PB 的 GUID 写入“锁定”信息，再将选票传送给用于更新被加密选票总数的公示板 BB 服务器。

步骤 7　投票机向投票者提示选票已经投交，在取出 PB 后关闭显示，等待下一个新的、未锁定的 PB。

步骤 8　投票者将投票机中取出的选票卡插入校验器，校验器读取 PB 并向投票者显示已投票，然后清屏。校验器不关机，投票者可以取出 PB 后再次插入校验器进行核实。

步骤 9　投票者从校验器中取出投票卡并离开投票室，将投票卡投入投票箱并离去。

3.3 计票过程

下面描述怎样计票：

步骤 1　投票站工作结束后，投票工作人员启用具有解密选票私钥的智能卡，因所在公示板 BB 上所有的选票已经加入了一个数据值。当这一数据被解密时，各自的表决信息依然是不可见的。

步骤 2　私钥附贴在 BB 上以方便任何人可以解密，在没有看单独个人表决的情况下，再次计票得出地区投票的总数。

步骤 3　投票工作人员向数据库查询已经投交的选票总数，并比较从公示板 BB 接收到的总数，如果有差异，就有问

题。

步骤 4　最后一步的检查，投票工作人员读投票箱中的内容，并再一次对应公示板和数据库中的计票进行检查，三方应匹配一致。这样，作为标准计票过程的一部分，快速实现了基于 RFID 的重新计票。

步骤 5　所有的选票存储设备被封存起来，直到选举最终完成。以后如果工作需要，物理选票 PB 的内容可以清空以备下次选举使用。

步骤 6　当选票被解密，计票开始时，BB 被作为混合网 MIX-net[6] 与数据库的接口界面来联合使用。

4　数学模型

要达到保密和审核目的，我们需要一个专用协议，即结合了同构加密[6]、混合网 MIX-nets[10] 和 非可见签名方案(blind signature scheme)[7] 的混合规定。Chaum[10] 提出的混合网 MIX-nets 作为匿名的途径被用于许多应用中。MIX-net 方法就是其接受一组加密的用户名后输出一组序列改变了的明码文本而没有显示它们之间的关联。Sako and Killian[11] 提出了建立在 Mix-net 方法上的电子投票系统，不过 Michels and Horster[12] 发现其系统在安全性和鲁棒性上存在问题。Golle 等[13] 提出一个通用重、再加密技术，其允许加密文本的通用再加密。类似于标准的再加密法，通用再加密把基于同样明码文本的加密文本转换成新的加密文本，另外他们提出了基于通用再加密的 MIX-net。我们在低带宽的 RFID 存贮设备上考虑密码设计，下面陈述著名的同构技术。

4.1　ElGamal 加密法[14]

接收方的私用密钥：随机产生 x

接收方的公用密钥：$g, h=g^x$

发送方用一随机数 w 加密纯文本(明文)

m：$(a,b)=(g^w, h^w m)$

接收方解密密码文本(a,b)：$b/a^x=m$

4.2　同构 ElGamal[6]

考虑一次投票 $v\in\{1,0\}\cong\{$真，假$\}$

选票是投票 g^v 的 ElGamal 加密值：

$(a,b)=(g^w, h^w g^v)$

其同构性质表现为：

$(a,b)*(a',b')=(g^{w+w'}, h^{w+w'} g^{v+v'})$

计票：对所有 ElGamal 加密结果进行解密，就可以得到表决的总结果。

4.3　同构方法[6]

每一投票 V_i 附上一 ElGamal 加密：

$(a_i,b_i)=(g^{wi}, h^{wi} g^{vi})$

加一个 $v_i=0$ 或 $v_i=1$ 的零所识证明，用 $W=\sum_i w_i$ and $T=\sum_i v_i$ 计算

$(\prod_i a_i, \prod_i b_i)=(g^W, h^W g^T)$

这里 T 是总计票。

计票员运用阈值解密(threshold-decrypt) (g^W, h^W, g^T) 先得到 g^T，最后得到 T。

4.4　通用再加密的 Mix-net 法

Golle 等提出的通用再加密的 Mix-net 法的基本框架如下[13]：

a. Mix-net 的每一输入都用接收方的公钥加密。

b. 与一般的再加密 Mix-net 不同，通用的 Mix-net 收到的是由接收方单个公钥加密的文本，而不是由单一的 Mix 系统的公钥加密。

c. 通用 Mix-net 的输出结果是一组加密文本。

d. 从一组加密文本里，接收方可对那些属于自己的加密文本进行解密。

钥的生成输出：$(y=gx, x)$，这里 $x\in_U Z_q$

加密输入包括文本 m，公钥 y，以及一个随机因子 $r=(k_0,k_1)\in Z_q^2$。

输出的加密文本 $C=[(\alpha_0,\beta_0);(\alpha_1,\beta_1)]=[(my^{k0}, g^{k0});(y^{k1}, g^{k1})]$。

解密的输入是用公钥加密了的文本 C。验证 $\alpha_0, \beta_0, \alpha_1, \beta_1$ 是否$\in g$，如果不满足，解密失败。

计算 $m_0=\alpha_0/\beta_0^x$ 和 $m_1=\alpha_1/\beta_1^x$，如果 $m_1=1$，输出 $m=m_0$；否则，解密失败。注意这里的内在含义是给定的加密文本只能被一个给定的钥来解密。

再加密的输入是加密文本 C 和一个随机的再加密因子 $r'=(k_0', k_1')\in Z_q^2$，输出是一个新的加密文本 $C'=[(\alpha_0',\beta_0');(\alpha_1',\beta_1')]=[(\alpha_0\alpha_1 k'0, \beta_0\beta_1^{k'0});(\alpha_1^{k'1}, \beta_1^{k'1})]$，这里 $k_0', k_0'\in Z_q^2$。

通用混合：任一个服务器都可以用以下两种方法之一来混合公示板的结果：i)服务器对加密文本再加密(如上所述)；ii)服务器重新按随机序列在公示板上排列新的加密文本。

5　安全问题

5.1　可行性

首先通过描述该投票系统 5 个要求中的每一个的可行性，讨论其存在的可能安全性问题。

5.1.1　正确性

正确地计入每一次的投票(即无重复又无遗漏)。通过通常的途径，一个投票者只能获得一个卡，因此只能进行一次表决。如果投票者试图用这个卡进行第二次投票，当投票机读这张卡时，它会识别出此卡已被上锁，拒绝投票者继续操作。我们有三重检查的投票表决系统：对比解密的公示板的镜像投票结果，对比记录到的物理选票的总数和解密的结果来检查投交选票的总数，所有这一切在选举日晚上进行。在选举期间检查公示板的结果可以收集部分镜像，以证实投票在没有任何明显干预的情况下被正确地总计(例如，如果下午 3 点的计票明显不同于下午 4 点的计票，我们就知道在那段时间可能有恶性事件发生，更多诡秘的攻击可能突破这样的保护)。

有两点需要考虑：如果选举人从外部自带设有 RFID 的空白选票，在进入投票工作区时，擦除器会检查到。选举人可以把自制的 RFID 放在很小的屏蔽金属盒内并放入口袋内而带入。对此，是否要引进像机场安检用的 X-Ray 机器来检测金属，这是涉及到选举法的规定。另外，即使有外面自制的空白选票带入，在投票时，投票器是否要设计成能检测伪造的选票，其设计的标准，以及数据库服务器对该选票的 GUID 进行真伪的识别，都是涉及到器件的硬件设计。

5.1.2　隐蔽性

无法根据选票或其内容来确定选民的身份。即，物理选票的 GUIDs 由数据库自动分配(或被 RFID 标签自身设定)，

无论是投票人触摸卡时留下的指印，还是投票站工作人员在交卡给投票人时人为地标识某个选票，都无法追踪到选民。工作人员被禁止写下任何有关选票的编号。在数据库或公示板中避免用到时间信息。公示板在线镜像会间隔性地定时更新，以阻止对选民投票的猜测。

5.1.3 无收据性

类似于百货商店中商品标签一样，同样地要求投票者通过门道入口进出：如果一个投票者试图带走他的物理选票，当他通过门口时其选票会被擦除器清空。投票者应该明白；如果其投票卡在选举日结束后不在投票箱中，就意味着其投票无效。选票保留在投票箱内以用于再次计票。在计票过程中认识这点对避免下面这种情况是必要的。依照选举法要求，如果允许填写非原定的选票，就会有任意的补名选票，在选举完成之后，RFID 读卡机及公之于众的私有钥匙就会对失窃选票生成一张真实的收据。因此，精心设计或无意保留收据的企图都要考虑到以防发生。但是每一次投票后，投票器会打印一个号码，该号码用于投票人过后在网上观察其投票是否被计入最后的计票结果(用于可证实性，下面将会讨论到)。该号码与物理选票的 GUID 以及投票内容毫无任何关系。任何人拿到该号码都不能搜索到其具体的物理选票和其投票结果。在投票过程中投票人被禁止携带任何可摄像的工具用以记录他们的投票过程及结果，如手机、相机等。

5.1.4 可证实性

这里有两层含义，其一是投票者在投票过程中检查其结果内容然后最后提交；其二是对于验票结果。每张选票被记录一次，投票器将加密的结果送到数据库服务器，后者解密后将其计入计票结果，在一定的时间间隔内将其新的计票结果输到公示板上显示计票结果。并“lock”物理选票的 GUID 以防止其二次投票。在选举结束后，工作人员统计投票箱中的物理选票和数据库服务器统计的结果，并与公示板的结果相比较，三者应该相符。如果公示板上的选票较投票箱中的少，就有窜改现象；反之，那么就有投票者试图带走他们的投票卡或发生了窜改，这些投票就变得无效(这种情况下，工作人员要查出失踪选票的 GUID，在数据库服务器中删除其投票结果)。相对于传统的计票体系，RFID 应用在统计计票和再验票的过程中具有很大的优势：其一，省略了大量的繁琐的计票工作，通过 RFID 和计算机系统，计票过程简单而快捷，避免了众多的人为差错；其二，发生再计票时，通过 RFID 和服务器的对比，可以很快找出失踪选票的号码，在最后计票结果中得以修改。

5.1.5 稳健性

对一些能够影响选举的事故要加以考虑。稳健性是硬件和软件的主要问题。以下讨论一些可能发生的事故：

• 物理选票加密/解密用的公钥/私钥生成出现故障，需要配备备用的密钥生成器。

• 验证器、投票器、服务器以及公示板出现故障，设备工程师和备用的设备必须配备。

• 投票场所周围环境不应该复杂，以防止外部恶意使用同一频率的信号干扰投票系统的 RFID。如果检测到此情况发生，应能快捷地查明外部信号的来源，使得投票得以正常继续。

• 投票人恶意携带 RFID 读写器，其体积可以很小，通过放在法拉第盒通过检查而被带入，它可以写那些被“unlock”的 RFID。虽然其内容会被验证器或投票器识别，但其引起的干扰还是比较严重，所以要监控投票场所的无线信号。

5.2 远程投票的设想

远程投票一直是人们想实现的梦想，其安全性也是多年来一直争议的焦点，不光牵扯到投票、验票、计票等技术问题，也涉及到投票法规的内容，尽管不少人提出过种种设想，但多年来都没有真正实现过。RFID 技术应用在物理选票上，使得远程投票的实现向前迈了一大步。如上述提出的 RFID 在电子投票中的应用，也可以在远程投票中采用。投票场所、投票设备和验票及其投票过程不用改变。所需的是要有网络连接投票器到数据库服务器，这应该是远程投票实现的关键。如今，网络已经很发达，一些地方由于地形的原因缺少网络，卫星无线通信可以替代，其安全性问题不在本文讨论之中。

结束语 本文概述了一种 RFID 技术用于电子投票系统，它较目前传统的纸张投票和人为计票在快速准确上具有很大的优势，尤其在再计票过程中，避免了大量的时间和人力的投入。实现该系统的 5 个要求的安全性得到了充分的讨论。现有的选举法规需做很少的修改，就可以使该系统得以实现。对远程投票的问题也进行了一定的探讨，在一定设备满足的条件下，远程投票基于 RFID 技术得以实现。

参 考 文 献

[1] Li Xiang-dong. Private communication

[2] Bruck S, Jefferson D, Rivest R. A Modular Voting Architecture [C]// Workshop on Trustworthy Electronic Voting 2001. August 2001

[3] Gritzalis D. Secure Electronic Voting[M]. Springer, 2003

[4] Okamoto T, Suzuki K, Tokunaga Y. Quantum Voting Cryptosystems(Invited Lecture)[C]// DIMACS Workshop on Electronic Voting - Theory and Practice. 2004

[5] Kwan A, Carlisle M. Privacy-preserving RFID-based Protocol for Electronic Voting[R]. November 2004

[6] Cramer R, Gennero R, Schoenmakers B. A secure and optimally efficient multi-party election scheme. Eurocrypt'96[C]// LNCS 1070. Springer-Verlag, 1997: 72-83

[7] Chaum D. Secret-ballot receipts: true voter-verifiable elections [J]. IEEE Security and Privacy, 2004, 2(1): 38-47

[8] Acquisti A. Receipt-free Homomorphic Elections and Write-in Ballots[R]. 2004/105, IACR. May 2004

[9] Kiayas A, Yung M. The vector-ballot E-voting Approach[C]// Financial Cryptography 2004, LNCS 2110. Springer, 2004: 72-89

[10] Neff A. A verifiable secret shuffle and its application to e-voting [C]// Proceedings of the 8th ACM conference on Computer and Communication Security. ACM, 2001: 116-125

[11] Sako K, Kilian J. Receipt-Free Mix-type Voting Scheme [C]// Proceeding of Eurocrypt 95, LNCS921. Springer-Verlag, 1995: 393-403

[12] Michels M, Horster P. Some remarks on a receipt-free and universally verifiable Mix-type voting scheme[C]// Asiacrypt'96. 1996: 125-132

[13] Golle P, Jakobsson M, Juels A, et al. The universal re-encryption for Mix-nets[C]// CT-RSA 2004, LNCS 2964. 2004: 163-178

[14] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms [C] // Crypto' 84, LNCS 718. Spring-Verlag, 1984: 10-18