doi:10.3969/j.issn.1000-436x.2012.z1.014

基于 DC-net 的会议室电子选举方案

李龙海，付少锋，黄诚强
（西安电子科技大学 计算机学院，陕西 西安 710071）

摘 要：提出了一种新的适用于小规模选举活动的电子选举方案，其最大特点是能够提供无条件的完美选票秘密性保障。方案具有自计票功能，能够实现公平性和可验证性。敌手对选举结果的破坏等同于解离散对数问题。该方案建立在 DC-net 匿名广播协议基础之上，其安全性不依赖于任何信任中心，但需假定任意投票者之间存在秘密信道。

关键词：电子选举；匿名广播；选票秘密性；零知识证明
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2012)Z1-0103-07

Boardroom electronic voting scheme based on DC-net

LI Long-hai, FU Shao-feng, HUANG Cheng-qiang
(School of Computer Science and Technology, Xidian University, Xi'an 710071, China)

Abstract: A novel electronic voting scheme was proposed which was quite suitable for small scale election setting. An outstanding characteristic of the design was its guarantee of unconditionally perfect ballot secrecy. It satisfied self-tallying, fairness and verifiability. Disruption of the result of an election equals to breaking the discrete logarithm problem. The scheme is built on top of the DC-net (dining cryptographers network) anonymous broadcast protocol. It needs no trusted authority to guarantee its security, but assumes a complete network of private channels between voters.

Key words: electronic voting; anonymous broadcast; ballot secrecy; zero knowledge proof

1 引言

会议室选举特指那些投票人数较少的小规模的选举活动，如一个公司的董事会选举或某国家的议会选举。在大规模电子选举方案中，主要关注的是效率问题。当大量的选票被收集到计票中心之后，应该在选民可接受的时限范围内完成解密和计票工作。而在小规模的选举活动中，主要关注的是选票的保密性问题。因为参选人数较少，每个投票者的投票都至关重要，所以让每个投票者都确信其投票内容没有被泄漏是实现公平选举的关键所在。

Kiayias 和 Yung 在文献[1]中首次提出了完美选票保密性(perfect ballot secrecy)的概念并设计了具有该特性的会议室电子选举方案。完美选票保密性是指要想获得某个投票者的投票信息必须和所有其他的投票者进行勾结，换句话讲，除了选举结果和不诚实的投票者的投票信息之外，攻击者无法再通过电子选举活动本身获得关于诚实投票者投票情况的任何有用信息。之后一些效率更高的具有完美选票保密性的电子选举方案[2~4]被提出，但这些方案所提供的完美选票保密性都建立在某个困难问题假设基础之上，即只具有计算意义上的选票安全性。将来一旦有更高性能的计算设备出现，如目前倍受关注的量子计算机和生物计算机，那么这些方

收稿日期：2012-07-10
基金项目：国家自然科学基金资助项目(61101142)；中央高校基本科研基金资助项目(K50510030012)
Foundation Items: The National Natural Science Foundation of China (61101142); The Fundamental Research Funds for the Central Universities(K50510030012)

案将不再安全，并且现在已经完成的选举活动中被保留下来的选票数据也将受到极大的威胁。

为此，本文利用 DC-net(dining cryptographer networks)匿名广播协议[5]设计了一种具有无条件完美选票保密性(Unconditionally Perfect Ballot Secrecy)的电子选举方案，该方案能够提供信息论意义上的选票秘密性保障。虽然该方案以用户间的秘密信道为基础，但在小规模选举中建立这些信道是可行的。例如可以要求 2 个不同的投票者事先已经利用非密码学的安全方法建立了大量共享密钥，以备在后面的多次选举中使用。该方案无需信任中心，且具有自计票功能，能够实现公平性和可验证性。敌手对选举结果的破坏等同于解离散对数问题。以基本的二选一投票方案为基础，本文还设计了针对多个候选人的投票方案和否决性投票方案。

2 相关工作

在近二、三十年中，已经有相当多的基于密码学技术的电子选举方案被提出。从实现方法角度可以将它们分为 3 大类：①基于同态加密算法的电子选举方案，其中典型的例子如文献[6,7]；② 基于 Mix-net[8]系统的电子选举方案，典型的例子如文献[9,10]；③ 基于盲签名的电子选举方案，典型的例子如文献[11,12]。盲签名技术主要被用在保证选民合法性或选票有效性上，并且严格地讲利用盲签名技术只能实现部分选票匿名性，要获得完整的匿名性必须借助于一种匿名通信工具，如 Mix-net 或 DC-net。所以很多基于盲签名的电子选举方案也可以被归到第 2 类。这些方案一般都被用在大规模的选举中，并且大都需要一个或多个信任中心完成收集选票、验证选票、对选票解密和计票工作。

会议室电子选举方案适用于小规模的选举活动，在设计时一般不设信任中心，并且可以牺牲部分效率而提供更好的选票秘密性保障。Kiayias 和 Yung 在文献[1]中首次提出了完美选票保密性的概念并设计了具有该特性的会议室电子选举方案。Kiayias 和 Yung 的方案还具有自计票功能，即一旦投票结束任何人都可以计算投票结果，因此不需要依靠信任中心完成解密工作。之后，Damgard 和 Jurik[2]、Groth[3]、Hao[4]又分别提出了具有类似性质的但效率更高的电子选举方案。这 4 种方案所提供的完美选票保密性都建立在某个困难问题假设基础之上，即只具有计算意义上的选票安全性。

DC-net[5]是由 Chaum 首先提出的一种匿名广播通信协议。DC-net 协议无需信任中心，在实现匿名性时利用了各个参与者之间的共同协作和相互保护。如果参与者之间存在绝对安全的秘密信道，则能够实现无条件的发送者匿名性。DC-net 协议的这些特点使其非常适合在小规模的选举活动中用于隐藏选票和投票者之间的对应关系。因此，本文利用 DC-net 协议设计了一种具有无条件完美选票保密性(unconditionally perfect ballot secrecy)的电子选举方案，该方案能够提供信息论意义上的选票秘密性保障。虽然该方案以用户间的秘密信道为基础，但在小规模选举中建立这些信道是可行的。例如可以要求 2 个不同的投票者事先已经利用非密码学的安全方法建立了大量共享密钥，以备在后面的多次选举中使用。

目前，能够检索到的基于 DC-net 协议的电子选举方案还包括文献[13]和文献[14]，并且它们同样能够实现无条件的保密性。但它们都只是将 DC-net 系统作为一种匿名通信工具使用，并且如果有 n 个投票者则至少要运行 n 次 DC-net 协议，因此其效率是非常低的。而本节的方案巧妙地利用了 DC-net 的叠加性，在 DC-net 的 1 次运行中完成所有用户的投票，并且这些选票被自动叠加到一起，即具有自计票功能。在没有错误的情况下整个选举过程只需运行 2 轮 DC-net 协议，因而效率比文献[13]和文献[14]要高得多。同文献[1,3]方案类似，本文的方案仅在实现公平性时需要一个信任中心的参与，而选票的秘密性和完整性与该中心是否可靠无关。

3 方案详细设计

3.1 安全性要求

在会议室选举方案设计中希望获得如下安全属性。

完美选票保密性。攻击者要想获得某个投票者集合的投票信息必须和所有其他的投票者进行勾结，即除了选举结果和不诚实的投票者的投票信息之外，攻击者无法再通过电子选举活动本身获得关于诚实投票者投票情况的任何有用信息。本方案还能提供更强的秘密性保护，即在攻击者具有无限计算能力的前提下也能保持完美选票保密性。

完整性。除了自己的选票外，任何投票者都无法对选举结果产生更多的影响；任何投票者都无法以不被觉察的方式破坏选举结果。

自计票性。所有投票者投票完成之后，任何人都可以计算投票结果。

可验证性。任何投票者都可以验证计票结果的正确性。

公平性。所有投票人同时得到投票结果，单个实体无法提前统计选票。

3.2 投票过程

设 $P=\{P_1, \cdots, P_n\}$表示投票者集合，G 表示一个有限循环群，$q=|G|$为素数，g、h 为 G 中任取的生成元，在 G 中离散对数问题难解。假设任意 2 个投票者之间都存在一个绝对安全的秘密信道用于协商会话密钥。另外还需要一个可靠的广播系统。如果基础网络无法在物理上保证可靠广播，则采用可靠的基于 Web 的 BBS 系统或利用拜占庭协定技术在异步点对点通信网络上实现[15,16]。为保证公平性，可令 BBS 作为第 n+1 个投票者参与选举协议，并且总是在最后一个广播数据，整个协议由 2 轮 DC-net 协议和 3 轮广播组成，即每个投票者共计要参与 5 轮广播过程。其中第 1 轮用于确认会话密钥协商结果，第 2 轮用于投票，第 3、4、5 轮用于验证投票结果的正确性。

在这里给出的是一个表决式选举，即针对某项提议或某个候选人进行的投票，投票为 1 表示赞同，投票为−1 则表示反对，这样最终的计票结果就等于赞同者和反对者之间的差值。当然该方法也可以用于只包括 2 个候选人的选举。

3.2.1 第 1 轮广播——验证密钥

1) 任意 2 个投票者 P_i 和 P_j 之间通过秘密信道建立 2 个共享密钥 $t_{ij}=t_{ji}\in\mathbb{Z}_q$ 和 $k_{ij}=k_{ji}\in\mathbb{Z}_q$；

2) 共享密钥协商完成之后，任意投票者 P_i 计算其会话密钥：

$$k_i=\sum_{j=1}^{n+1} sign(i-j)k_{ij},\quad t_i=\sum_{j=1}^{n+1} sign(i-j)t_{ij}$$

P_i 同时任选 $u_i, c_i \in_R \mathbb{Z}_q$，其中，$c_i$ 用于生成选票有效性证明协议中的质询。

3) 任意投票者 P_i 广播输出：

$$V_{1,i}=g^{k_i}h^{t_i},\quad R_i=h^{u_i}g^{c_i}$$

$V_{1,i}$ 可以被看成是对密钥 k_i 的 Pedersen 承诺[17]，t_i 是承诺密钥。R_i 看成是对 c_i 的 Pedersen 承诺，u_i 是承诺密钥。

4) 等待所有用户广播完毕之后，任意投票者计算并验证：

$$V_1=\prod_{i=1}^{n+1}V_{1,i}=1 \tag{1}$$

如果上式不成立则说明有人在作弊，此时要求所有用户都公开自己的共享密钥和会话密钥以找出不诚实的投票者，并重新运行协议。如果在公开过程中有 2 个投票者产生了密钥争议，则在下一次运行时 2 个成员之间不再建立共享密钥，即相当于在密钥图上去掉这 2 个成员所对应的 1 条弧。这样使得一个作弊者最多只能制造 n 次密钥争议。此后他将被排除出系统。

3.2.2 第 2 轮广播——投票

真正的投票过程在本轮进行。设 $P_i(1\leqslant i\leqslant n)$ 的投票意见为 $b_i\in\{1,-1\}$，并令 P_{n+1}(即 BBS)的投票意见 b_{n+1} 为 0。P_i 在本轮广播输出：

$$V_{2,i}=k_i+b_i$$

等所有投票者广播完毕之后，任何人都可以计算投票结果：

$$V_2=\sum_{i=1}^{n+1}V_{2,i}$$

当然是否接受该投票结果还要看是否能通过后面的验证过程。

3.2.3 第 3/4/5 轮广播——验证选票

后 3 轮广播过程主要用于执行如图 1 所示的交互式证明协议，以证明任意投票者 P_i 在第 2 轮广播的选票 $V_{2,i}$ 是有效的。

在第 3 轮中，P_i 计算并广播：A_i 和 B_i。

在第 4 轮中，P_i 广播输出自己先前已经选好的 c_i。等所有用户广播完毕之后，计算 $c=c_1+\cdots+c_{n+1}$ 作为证明协议中的质询 c。

在第 5 轮中，P_i 根据 c 计算并广播：$d_{1,i}, d_{2,i}, r_{1,i}, r_{2,i}$ 以及 u_i。然后由其他成员按照图 1 所示的方式验证 P_i 的输出 $d_{1,i}, d_{2,i}, r_{1,i}, r_{2,i}$ 是否有效，以及是否满足 $R_i=h^{u_i}g^{c_i}$。

如果某成员无法通过第 5 轮的验证，或者拒绝参与证明过程，都将被视为作弊者从合法投票者集合中删除，然后重新执行选举协议。如果所有成员都可以通过验证，则认为第 2 轮的计票结果是正确的，协议终止。

关于特殊成员 P_{n+1} 的证明协议与上面有所不同，但基本思想是类似的。其具体构造方法这里就不再给出了。

4 分析

4.1 安全性分析

下面将分析和证明上述选举协议满足的安全特性。

自计票性：第 1 轮的共享密钥协商和广播验证过程保证了 n+1 个投票者所持有的会话密钥满足：

$$\sum_{i=1}^{n+1} k_i = 0\ ,\quad \sum_{i=1}^{n+1} t_i = 0$$

因此，如果所有投票者都按照协议规定构造了选票 $V_{2,i}$，则必然有：

$$V_2 = \sum_{i=1}^{n+1} V_{2,i} = \sum_{i=1}^{n+1} k_i + \sum_{i=1}^{n+1} b_i = \sum_{i=1}^{n+1} b_i$$

无条件的完美选票保密性：

定理 1 在任意 2 个投票者之间都存在秘密信道的假设下，如果系统中存在 2 个或以上的诚实投票者，则所提方案具有无条件的完美选票保密性。

证明 下面主要通过证明协议所有公共输出的概率分布与诚实投票者的投票(秘密值 $b_i \in \{1,-1\}$)无关，来证明定理成立。

1) 对于任意诚实的投票者 P_i 而言，由于其会话密钥 $k_i = \sum_j sign(i-j)k_{ij}$，$t_i = \sum_j sign(i-j)t_{ij}$，所以其他 n 个投票者中只要有 1 个诚实地随机选取了共享密钥 k_{ij} 和 t_{ij} 就可以保证 k_i 和 t_i 在 $\mathbb{Z}_q$ 上是均匀分布的，除非攻击者能够控制除 P_i 之外的所有成员，但这与系统中存在 2 个或以上的诚实投票者相矛盾。因为 t_i 是随机的，所以承诺值 $V_{1,i}$ 在 G 上均匀分布，$V_{1,i}$ 不会暴露关于密钥 k_i 的任何信息；因为 k_i 是随机的，所以 $V_{2,i} = k_i + b_i$ 在 $\mathbb{Z}_q$ 上均匀分布，$V_{2,i}$ 不会暴露关于选票 b_i 的任何信息。因此，协议前 2 轮的广播输出对攻击者猜测选票信息没有任何帮助，即便攻击者具有无限的计算能力。

2) 图 1 是按照文献[18]的原理构造的证据不可区分(witness indistinguishable)的交互式证明协议，即协议输出的概率分布与证明者的证据(即 b_i 和 t_i)无关，因此不会暴露关于证据的香农信息。具体地讲，在该协议输出中，显然 A_i、B_i 在 G 上均匀分布，因此它们的概率分布与 b_i 无关。而 $d_{1,i}$ 和 $d_{2,i}$ 的联合分布只与 c 的概率分布有关。由于满足 $h^{r_{1,i}} = A_i(Y_i g)^{d_{1,i}}$，$h^{r_{2i}} = B_i(Y_i/g)^{d_{2,i}}$，所以 $r_{1,i}$、$r_{2,i}$ 的取值只决定于 A_i、B_i、$d_{1,i}$、$d_{2,i}$，和 b_i 无关。因此在 b_i=1 和 b_i=−1 2 种情况下 Prover 的输出都具有完全相同的联合概率分布，它们对攻击者猜测选票信息没有任何帮助，即便攻击者具有无限的计算能力。因此第 3、4、5 轮的广播过程也不会泄漏选票信息。□

完整性：所提协议能够对投票结果提供如下完整性保护：任何参与者能够提交无效选票而不被发现的概率是可忽略的，除非该参与者能够在多项式时间内解决 G 上的离散对数问题。下面简要分析原因。

1) 在第 1 轮广播中，不诚实的成员 P_i 如果没有按规定构造 k_i 和 t_i，那么 $\prod V_{1,i} = 1$ 的概率是可忽略的，协议因此将进入公开过程然后重新执行。为了避免被确认为作弊者，P_i 在公开过程中只能制造密钥争议，将错误转嫁给他人。最多在制造 n 次密钥争议之后，P_i 被排除出系统并且被确定为作弊者。

2) 在第 2 轮广播中，假设 P_i 没有按规定构造

Prover(P_i)			Verifier
Public Parameter：$Y_i = V_{1,i} g^{-V_{2,i}} = h^{t_i} g^{-b_i}$			
$b_i = 1$	$b_i = -1$		
$\alpha_i, \beta_i, d_{2,i} \in_R \mathbb{Z}_q$,	$\alpha_i, \beta_i, d_{1,i} \in_R \mathbb{Z}_q$,		
$A_i = h^{\alpha_i}$,	$A_i = (Y_i g)^{-d_{1,i}} h^{\alpha_i}$,	$A_i, B_i \rightarrow$	
$B_i = (Y_i/g)^{-d_{2,i}} h^{\beta_i}$	$B_i = h^{\beta_i}$		
		$\leftarrow c$	$c \in_R \mathbb{Z}_q$
$d_{1,i} = c - d_{2,i}$,	$d_{2,i} = c - d_{1,i}$,		$c \stackrel{?}{=} d_{1,i} + d_{2,i}$,
$r_{1,i} = \alpha_i + d_{1,i} t_i$,	$r_{1,i} = \alpha_i$,	$r_{1,i}, r_{2,i}, d_{1,i}, d_{2,i} \rightarrow$	$h^{r_{1,i}} \stackrel{?}{=} A_i (Y_i g)^{d_{1,i}}$,
$r_{2,i} = \beta_i$	$r_{2,i} = \beta_i + d_{2,i} t_i$		$h^{r_{2,i}} \stackrel{?}{=} B_i (Y_i/g)^{d_{2,i}}$

图 1 证明选票 $V_{2,i}$ 的有效性

其加密选票 $V_{2,i}$。如果 P_i 能够通过第 5 轮的验证，那么只有 3 种可能：① P_i 使用了与 k_i 不同的密钥 k_i' 加密 b_i，且 P_i 知道 $t_i' \neq t_i$ 满足 $g^{k_i'}h^{t_i'} = V_{1,i} = g^{k_i}h^{t_i}$，但这与离散对数问题假设矛盾；② P_i 事先猜中了第 4 轮由所有成员共同生成的质询 c，但该概率只有 $1/q$；③ 在第 4 轮中 P_i 通过最后广播一个做了适应性调整的 c_i' 来改变质询 c 的概率分布，但 P_i 必须知道 $u_i' \neq u_i$ 满足 $h^{u_i'}g^{c_i'} = R_i = h^{u_i}g^{c_i}$，这与离散对数问题假设矛盾。因此，$P_i$ 在第 2 轮的作弊行为必然会被第 5 轮的验证过程发现。证明协议也保证了 b_i 只能为 1 或−1，所以 P_i 无法对计票结果 V_2 施加更多的影响。

3) 图 1 所示证明协议的正确性和完整性保证了不诚实投票者在第 3 轮或第 5 轮中的作弊行为必然会被发现。而在第 4 轮中，不诚实投票者要想公布一个与事先选定的 c_i 值不同的质询值必将面临解离散对数问题。

基于以上 3 点原因，在离散对数问题假设下，任意投票者使协议输出错误结果而不被发现的概率是可忽略的。

与文献[1]和文献[3]的选举方案相比，在这里只能实现较弱的容错性，即在发现某成员作弊或者在运行过程中突然退出之后，协议只能重新执行，而无法由剩余的成员恢复该错误使协议继续执行。这实际上是使用用户间秘密信道带来的固有问题。但是在小规模选举中，协议重新执行的代价是可以接受的。通过加大对作弊者的惩罚力度也可以避免协议被反复执行的情况。

可验证性：BBS 系统保证了任意投票者都可以看到协议的所有公开输出，而且看到的内容是相同的。通过验证式(1)成立，任意投票者可以确信各成员的会话密钥的正确性；通过参与第 3、4、5 轮的交互式证明过程，任意投票者可以确信各个选票都是有效的，因此第 2 轮的计票结果 V_2 也是正确的。

需要指出的是，这里实现的只是内部可验证性(internal verifiability)，即只有在线参与了交互证明协议的投票者才能够验证投票结果的正确性。第 3、4、5 轮的证明协议输出对于未参与协议的观察者来讲是没有意义的，因为如果所有投票者勾结在一起则可以制造出任意有效的证明输出(先选择 c 再构造证明)。因此第 3、4、5 轮的输出不能使任意观察者确信结果是正确的。

为了让任意观察者都能够验证投票结果的正确性，即实现公开可验证性(public verifiability)，可以利用 Fiat-Shamir 的技术[19]将图 1 的证明协议改造为非交互式证明，最后每个投票者在第 2 轮中将证明结果和其选票 $V_{2,i}$ 同时广播出去。改造后方案的安全性分析中必须引入 Random Oracle 模型[20]。

公平性：在 P_{n+1}(即 BBS)广播之前，其他 n 个真正的投票者无法看到投票结果；因为 P_{n+1} 的投票为 0，所以在他广播之后其他 n 个投票者才能够同时看到投票结果。

4.2 效率分析

因为无法精确估算，所以下面的分析中未考虑利用秘密信道建立用户间共享密钥的开销。设 n 表示投票者人数，l 表示生成群 G 时的安全参数。每个用户在第 1 轮广播中需要进行 4 次指数运算，第 3 轮中需要进行 3 次指数运算，第 5 轮中为验证其他用户输出的有效性需要进行 $6n$ 次指数运算。第 2 轮和第 4 轮的运算量可以忽略不计。整个协议过程中，每个用户共需要广播 $O(l)$ bit 的数据。因此，如果不计建立共享密钥的开销，所提协议的计算和通信复杂度分别为 $O(n)$和 $O(l)$，与方案[1,3,4]是相当的。

5 多选一投票方案

上述方案只适用于包含两个候选人的二选一选举。下面分析如何将其改造为多选一的投票方案。

第一种改造方法是采用文献[6,7]中的技术。假设有 m 个候选人，从 G 中任取 m 个生成元 $f_1, f_2, \cdots, f_m$。建立和验证会话密钥的过程不变。在第 2 轮广播中，如果 P_i 选择第 $b_i \in \{1,\cdots,m\}$ 个候选人，则广播 $V_{2,i} = g^{k_i}f_{b_i}$，然后在第 3、4、5 轮中证明 P_i 知道秘密值 k_i、t_i 满足命题：

$$V_{1,i} = g^{k_i}h^{t_i} \wedge V_{2,i} = g^{k_i}f_{b_i} \wedge b_i \in \{1,\cdots,m\}$$

相应证明协议的构造方法与图 1 类似，具体可以参考文献[18]。

为了获得各个候选人的选票数目，首先计算：

$$V_2 = \prod\nolimits_i V_{1,i} = g^{\sum_{i=1}^{n}k_i} f_1^{v_1} f_2^{v_2} \cdots f_m^{v_m} = f_1^{v_1} f_2^{v_2} \cdots f_m^{v_m}$$

上式中的 $v_1, v_2, \cdots, v_m$ 都小于等于 n，所以可以通过 V_2 获得 $v_1, v_2, \cdots, v_m$ 的值(例如用暴力搜索法)，即各个候选人的选票数目。

如果投票者数目 n 和候选人数目 m 满足 $m\lceil \mathrm{lb}n \rceil \leqslant \lfloor \mathrm{lb}q \rfloor$，则还可以给出一种效率更高的方

法以避免上述的暴力搜索问题。设 $e=\lceil \mathrm{lb}n \rceil$，在第 2 轮广播中，如果 P_i 选择第 b_i 个候选人，则令其广播输出为

$$V_{2,i}=k_i+2^{e(b_i-1)}$$

显然，$V_{2,i}\in \mathbb{Z}_q$，因此 P_i 的输出长为 lb$q$ bit。上述方法相当于将这 lb$q$ bit 的输出划分为 m 子信道，每个子信道占 e 个比特并分别对应 1 个候选人。如果想为某个候选人投票，则在相应子信道内发送 1，而在其他子信道内发送 0。在第 3、4、5 轮广播中 P_i 还需要证明他知道秘密值 k_i、t_i 满足命题：

$$V_{1,i}=g^{k_i}h^{t_i}\wedge g^{V_{2,i}}=g^{k_i}g^{2^{e(b_i-1)}}\wedge b_i\in\{1,\cdots,m\}$$

设 $V_2=\sum_i V_{2,i}$，则新的计票算法如图 2 所示。

```
for i = 1 to m
    v_i = V_2 mod 2^e ,   output v_i
    V_2 = V_2 >> e        // 将 V_2 右移 e 位
end of for
```

图 2 计票算法

上面算法输出的 $v_1, v_2, \cdots, v_m$ 即分别为 m 个候选人所对应的选票数目。

第 2 种改造方法在第 2 轮广播和计票过程中只用到了 $\mathbb{Z}_q$ 上的加法运算，因此其效率要比文献[6,7]的方法高得多。

6 匿名否决投票方案

在否决投票中，只要有一个投票者投了反对票就会否决某项提议。下面将第 3 节的二选一投票方案修改为否决投票方案。

用于建立和验证会话密钥的第 1 轮广播过程中不再需要广播 R_i，其他保持不变。在第 2 轮广播中，如果 P_i 投否决票，则任取 $r\in_R \mathbb{Z}_q^*$，然后输出 $V_{2,i}=k_i+r$；否则输出 $V_{2,i}=k_i$。第 2 轮广播完毕之后，计算 $V_2=\sum_i V_{2,i}$，如果 $V_2\neq 0$ 则表示有人投了否决票；如果 $V_2=0$ 则表示全体赞成。如果有成员没有按规定构造 $V_{2,i}$，则相当于投了否决票，因此该方案不需要第 3、4、5 轮的交互证明过程。

上述方案失败的概率，等于多个投票者所选随机数 r 相加为 q 的概率，也等于作弊者能成功破坏诚实投票者选票的概率。该概率为 $1/q$，是可忽略的。很容易证明，该否决投票方案也具有无条件的完美选票保密性。

与已知的效率最高的匿名否决方案[21]相比，所提方案同样只需 2 轮广播，每轮广播中同样只需要 2 个模指数运算，然而能够提供比文献[21]更强的安全性保护。

7 结束语

本文利用基于秘密信道的 DC-net 协议设计了一种会议室电子选举方案。该方案的最大特点是能够提供无条件的完美选票秘密性保障，即信息论意义上的保密性。该方案具有自计票功能，并且能够实现公平性和可验证性。选票结果的完整性保护基于求解离散对数问题困难性假设。本文的另一贡献以基本的二选一投票方案为基础，还设计了针对多个候选人的投票方案和否决性投票方案。二选一投票方案和否决投票方案与已知的具有完美选票保密性的会议室选举方案[1~4]效率相当，而多选一投票方案的效率优于同类方案。

参考文献：

[1] KIAYIAS A, YUNG M. Self-tallying elections and perfect ballot secrecy[A]. Proceedings of PKC'02[C]. Paris, France, 2002. 141-158.

[2] DAMARD I, JURIK M. A length-flexible threshold cryptosystem with applications[A]. Proceedings of ACISP'03[C]. Wollongong, Australia, 2003. 350-364.

[3] GROTH J. Efficient maximal privacy in boardroom voting and anonymous broadcast[A]. Proceedings of Financial Cryptography 2004[C]. Florida, USA, 2004. 90-104.

[4] FENG HAO, PETER R, PIOTR Z. Anonymous voting by 2-round public discussion[J]. IET Information Security, 2010, 4(2) : 62-67.

[5] CHAUM D. The dining cryptographers problem: unconditional sender and recipient untraceability[J]. Journal of Cryptology, 1988, 1(1): 65-75.

[6] CRAMER R, FRANKLIN M, SCHOENMACKERS B, YUNG M. Multi-Authority secret-ballot elections with linear work[A]. Advances in Cryptology –Eurocrypt '96[C]. Zaragoza, Spain, 1996. 72-83.

[7] CRAMER R, FRANKLIN M, SCHOENMACKERS B. A secure and optimally efficient multi-authority election scheme[A]. Advances in Cryptology–Eurocrypt'97[C]. Konstanz, Germany, 1997. 113-118.

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

[9] FUJIOKA A, OKAMOTO T, OHTA K. A practical secret voting scheme for large scale elections[A]. Advances in Cryptology-Asiacrypt '92[C]. Queensland, Australia, 1992. 244-251.

[10] NEFF A. A verifiable secret shuffle and its application to E-voting[A].

Proceedings of ACM CCS ’01[C]. New York, USA, 2001. 116-125.

[11] OKAMOTO T. An electronic voting scheme[A]. Proceedings of IFIP’96[C]. 1996. 21-30.

[12] OHKUBO M, MIURA F, ABE M, *et al*. An improvement on a practical secret voting scheme[A]. Proceedings of ISW’99[C]. Lumpur, Malaysia, 1999. 255-234.

[13] CHAUM D. Elections with unconditionally secret ballots and disruption equivalent to breaking RSA[A]. Proceedings of Eurocrypt’ 88[C]. Davos, Switzerland, 1988. 177-182.

[14] PFITZMANN B, WAIDNER M. Unconditionally untraceable and fault-tolerant broadcast and secret ballot election[J]. Communications of the ACM, 1992, 21(21) : 7-18.

[15] DOLEV D, STRONG H. Authenticated alogorithms for byzantine agreement[J]. SIAM Journal on Computing, 1983, 12(4) : 656-666.

[16] CACHIN C, KURSAWE K, SHOUP V. Random oracles in constantinople: practical asynchronous byzantine agreement using cryptography[J]. Journal of Cryptology, 2005, 18(3) : 219-246.

[17] PEDERSEN P. Non-interactive and information theoretic secure verifiable secret sharing[A]. Advances in Cryptology-Crypto'91[C]. Santa Barbara, California, USA, 1991. 129-140.

[18] CRAMER R, DAMGARD I, SCHOENMAKERS B. Proofs of partial knowledge and simplified design of witness hiding orotocols[A]. Advances in Cryptology-Crypto ’94[C]. Santa Barbara, California, USA, 1994. 174-187.

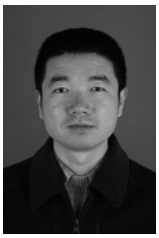
[19] FIAR A, SHAMIR A. How to prove yourself: practical solutions to identification and signature problems[A]. Advances in Cryptology-Crypto ’86[C]. Santa Barbara, California, USA, 1986.186-194.

[20] BELLARE M, ROGAWAY P. Random oracles are practical: a paradigm for designing efficient protocols[A]. Proceedings of ACM CCS’ 93[C]. Fairfax, Virginia, USA, 1993. 62-73.

[21] HAO F, ZIELINSKI P. The power of anonymous veto in public discussion[J]. Trans on Computational Science, 2009, 4: 41-52.

作者简介：

李龙海（1976-），男，河北冀州人，博士，西安电子科技大学副教授、硕士生导师，主要研究方向为匿名通信、隐私保护技术和计算机网络安全。



付少锋（1975-），男，陕西户县人，西安电子科技大学副教授，主要研究方向为计算机网络安全和嵌入式系统。

黄诚强（1989-），男，福建连江人，西安电子科技大学研究生，主要研究方向计算机与网络安全。