基于区块链技术的匿名电子投票协议设计

周 振,严广乐

(上海理工大学 管理学院,上海 200093)

摘 要:投票选举是集体决议与意见征求的有效方式,电子投票是密码学的研究热点之一。为此,设计一种基于区块链技术与椭圆曲线盲签名以及时间释放加密算法的匿名电子投票协议。该方案采用以太坊作为平台,利用椭圆曲线盲签名密钥长度短、安全等级高的特点,解决了投票系统的匿名性、唯一性等问题。同时利用时间释放加密算法,解决了公平性与保密性问题,保证了基于区块链技术投票系统的安全性。

关键词:区块链;电子投票;智能合约;盲签名;时间释放加密

DOI:10.11907/rjdk.191416 **开放科学(资源服务)标识码(OSID):**

中图分类号:TP399 **文献标识码:**A **文章编号:**1672-7800(2020)001-0229-05

Design of Block Chain-based Anonymous E-Voting Scheme

ZHOU Zhen, YAN Guang-le

(*Business School*, *University of Shanghai for Science and Technology*, *Shanghai* 200093, *China*)

Abstract: Voting is an effective way to collect suggestions and make joint decisions. Electronic voting has always been a hot research field in cryptography. This paper proposed an anonymous electronic voting protocol based on block chain technology, elliptic curve blind signature and time-release encryption algorithm. The scheme takes Ethereum as the platform, and makes use of the characteristics of short key length and high security level of elliptic curve blind signature to ensure the anonymity and uniqueness of the voting system. At the same time, time-release encryption algorithm solves the problems of confidentiality and fairness. Therefore, it guarantees the security requirement of voting system based on block chain.

Key Words: block chain; electronic voting; smart contracts; blind signature; time-release encryption

0 引言

投票决议与选举是现代民主的根基所在。1981年,电子投票(E-voting)首先由 Chaum[1]提出,即在电子信息与互联网选举场景中实现投票功能,并保证投票过程的安全性。相比传统纸质投票,电子投票在计票准确性、人力成本与实现范围等方面都有明显优势。

电子投票系统的属性要求主要包括保密性、完整性、可验证性、不可篡改与伪造性、可验证性等[2]。根据采用的密码学技术方案可以将现有电子投票系统分为3类:基于混网(Mix-Net)方案[3-5]、基于盲签名方案[6]与基于同态加密方案[7-9]。

基于混网方案最先由 chaum 提出。混网方案理论上可实现选票的公开验证,但因其算法较为复杂,协议运行效率低下,在选举规模扩大时尤为明显;基于同态加密方案最早在1985年由 Cohen & Fischer[10]提出,常见协议方案有采用 EIGamal[11]或 Pailler[12]的加密算法。同态加密方案运行效率高、实现难度小,但计算成本较高;基于盲签名方案计算量小、运行效率高、保密性强,是一种较为主流的电子投票实施方案。

基于盲签名技术的电子投票协议最开始是由 Fujioka[13]提出的 FOO 协议,该协议可以实现基于盲签名的大规模电子投票,但不具有抗伪造性及抗共谋攻击性。为了解决盲签名问题,一些新的方案随后被提出,如部分盲签名[14]、基于双线性对的部分盲签名[15]等方案,但是依然存在待完善的地方,如对于验证机构的依赖程度过高等问题。

区块链具有去中心化、数据可靠、交易可追溯等特点。引入区块链技术可以为电子投票系统提供去中心可信第三方 TTP 服务,以保证投票过程的透明化与公平性,使选民具有更强的自主性,并增强了选民对协议的信任程度,扩大了协议适用范围。

收稿日期:2019-03-28

基金项目:上海高原学科建设项目(10-17-303-004)

作者简介:周振(1994-),男,上海理工大学管理学院硕士研究生,研究方向为社会经济金融复杂系统与区块链;严广乐(1957-),男,上海理工大学管理学院教授,研究方向为社会经济金融复杂系统、系统科学、系统动力学。

基于以上研究，总结电子投票系统发展现状与存在问题，具体包括：①选票碰撞问题；②公平性问题；③保密性问题；④唯一性问题。对此，本文提出基于区块链的匿名电子投票方案，利用椭圆曲线盲签名技术增强系统的安全性、保密性，并以时间释放加密解决公平性问题。同时区块链技术解决了盲签名体制对第三方过度依赖的问题，通过身份认证书的方式保证选票的抗碰撞、唯一性等要求。此外，智能合约维护两份用户表单，可有效防止复制攻击和“双花”问题。

通过以上方式可在同一协议中同时满足多种性能需求，有效解决了电子投票系统的安全性问题，并提高了系统性能。

1 以太坊智能合约

以太坊提供了一套完整的区块链分布式应用平台。使用以太坊进行数字货币交易时，任何人都可在上面发布与使用分布式应用程序。相比于比特币，以太坊的优势在于其为分布式应用程序开发、部署提供了完整的工具链，以及更为灵活的操作指令。

以太坊分为 4 个阶段：Frontier、Homestead、Metropolis 和 Serenity。在第 3 阶段的拜占庭硬分叉（Byzantium Hard Fork）中，引入了许多新特性，包括椭圆曲线与标量乘法以及大数模幂的运算实现等，因此具有更高复杂度的加密算法得以被采用。此前，使用以太坊虚拟机 EVM 无法支持直接验证 ECC 盲签名[16]。以下是在 EVM 中采用 OVN（Open Vote Network）、RSA 盲签名与椭圆曲线 ECC 算法在验证过程中的 Gas 消耗量比较，如图 1 所示。本协议整体框架如图 2 所示。

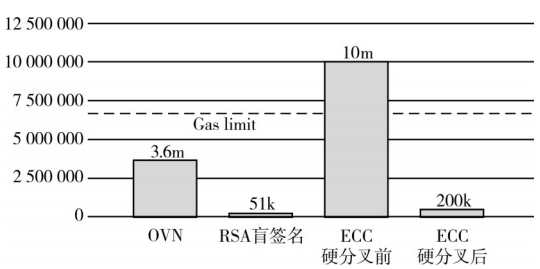

图 1 在以太坊验证不同签名算法 Gas 消耗分析

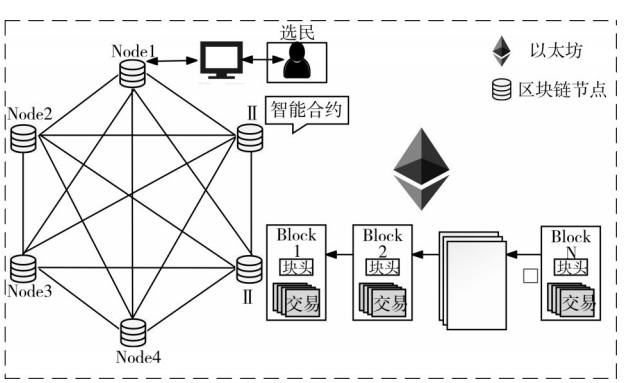

图 2 协议框架

2 算法方案

本方案算法包括椭圆曲线密码体制盲签名与时间释放加密算法两部分。

盲签名方案中，椭圆曲线密码体制（Elliptic Curve Cryptography，ECC）是一种基于椭圆曲线离散对数问题难解性的高效密码体制。ECC 使用较短的操作数即可实现与 RSA 及离散对数系统 DL 相同安全等级的密码服务。与其它公钥算法体制相比，其在带宽与复杂度方面性能优势非常明显，并且以太坊在升级后也允许使用椭圆曲线进行加密。如张方国等[17]提出了多种基于椭圆曲线的盲签名方案。

为了保证投票系统的公平性，本设计希望设置选票开启门阀，在投票结束后统一进行结算公布。在此之前，任何一方都无法获得选票信息，并且其对于外界攻击也具有防御功能。

时间加密算法（Timed-Release Encryption）是一种基于时间参数的加密算法，通过添加时间阀，使目的操作只有在指定时间节点后才可以进行，从而完成具有时间节点限制的任务。解决此类问题的方案主要有两种：一种是时间锁难题（TLP），通过设计具有相当复杂度的解密算法，实现操作延后。但该方案造成算力资源严重浪费，且对于不同运算环境不具有普适性；另一种是时间服务器方案（Time Server），通过使用时间陷门实现时间节点控制，即可避免 TLP 方案中的问题。

通过时间服务器实现时间释放加密的方案最早由 Crescenzo[18]提出，但无法保证匿名性。后来 Blake 等[19]提出的基于 Bilinear Diffie-Hellman 问题的方案具有良好性能，可摆脱对于时间服务器的信任依赖，并能保证匿名性。本协议是将以上算法结合区块链技术进行方案设计的首次尝试。

2.1 椭圆曲线密码体制与盲签名

盲签名算法包含用户方与签名方两种角色。使用该算法的目的在于让用户方在不向签名方透露消息内容的前提下获得对方签名信息。因此，盲签名技术在匿名投票场景中对于保护用户隐私可起到关键作用。

2.1.1 参数设置

本投票方案采用盲签名方案的算法参数，$E(F_q)$是定义在有限域上的椭圆曲线。

参数可以表述为：$D=(q,FR,a,b,G,H,n,h)$，符号含义为：

（1）q 是有限域的元素个数，这里 $q=p$，或者 $q=2^m$。

（2）FR 有限域中元素的表示方法（多项式或正规基表示等）。

（3）$a,b\in F_q$，用于定义曲线方程：

$$y^2=x^3+ax+b \quad p>3$$

$$y^2+xy=x^3+ax^2+b \quad p=2$$

（4）$G\in E(F_q)$是曲线上的 n 阶基点，H 是另一个基点，取法同 G。

(5)n 为一个素数,$n>2^{160}$ 且 $n>4\sqrt{q}$。

(6)SHA-1:$\{0,1\}^{*}\rightarrow\{0,1\}^{160}$ 是美国 NIST 和 NSA 设计的安全 Hash 算法。一般要求输入信息不大于 2^{64} bit。

(7)$h=\#E(F_q)/n$ 称为余因子,h 远小于 n,利用 h 可以较快地找到满足以上条件的基点 G;随机选择 $G'\in E(GF(q))$,计算 hG',如果 h$G'\neq 0$,则令 G= hG'。

算法流程可分为以下几个步骤,其中当签名私钥为 d、f,公钥则表示为 $Q=dG+fH$,记号(·‖·)表示两个比特串连接,R_x(A)表示取点 A 的坐标。

2.1.2　签名过程

(1)签名者生成私钥 $t,u\in{}_RZ_n^{*}$,然后计算公钥 $A=tG+uH$,并将其公布给用户。

(2)用户生成盲化因子 $\beta,\gamma,\delta\in{}_RZ_n^{*}$,然后进行操作计算。

$$A+\beta G+\gamma H+\delta Q=(x,y)$$

$$a=x \bmod n$$

$$c=SHA\text{-}1(m\|a)$$

$$e=c-\delta$$

m 为原始明文消息,c 是盲化后的消息。将消息 e 发送给签名者。

(3)签名者进行操作计算。

$$r=t-ed$$

$$s=u-ef$$

签名者进行签名操作后,将处理好的消息 (r,s) 发送回用户方。

(4)用户再次进行操作计算。

$$\rho=r+\beta$$

$$\sigma=s+\gamma$$

从而得到签名者对于原消息的盲签名 (c,ρ,σ)。

(5)验证过程。验证过程只需计算下式是否成立。

$$c=SHA\text{-}1(m\|R_x(cQ+\rho G+\sigma H)\bmod n)$$

2.2　时间释放加密算法

2.2.1　参数设定

时间服务器 CS 输入安全参数 k,生成参数 $P=(k,q,G_1,G_2,e,G,H_1,H_2,n)$,TS 公私钥对 (X_{CS},Y_{CS})。

(1)G_1、G_2 为有限域上椭圆曲线 q 阶群,q 为素数。

(2)G_1 为加法群,G_2 为乘法群。

(3)映射 $e:G_1\times G_1\rightarrow G_2$ 为双线性映射。

(4)G 为 G_1 生成元。

(5)$H_1:\{0,1\}^{*}\rightarrow G_1$ 的哈希函数,$H_2:G_2\rightarrow\{0,1\}^{n}$ 的哈希函数。n 为明文长度。

2.2.2　算法描述

(1)时间广播算法(Time Broadcasting Algorithms,TBCT)。时间服务器 CS 输入时钟实例 $T\in\{0,1\}^{*}$,输出时间陷门 $S_r=sH_1(T)$。时间服务器对所有时钟实例计算时间陷门,可以通过计算 $e(sG,H_1(T))=e(P,sH_1(T))$ 进行有效性公开验证。

(2)加密算法 EnAL。由选民进行操作,输入投票选项 v_i,计票合约公钥 X_J,时间服务器公钥 X_{CS} 和一个时钟实例 $T\in\{0,1\}^{*}$,输出选项密文 $v_i^{'}$。具体流程为:①计算 $e(aG,sG=e(G,asG))$,完成前提检验,否则回滚;②选择 $r\in Z_q^{*}$,计算 rG 和 $rasG$;③计算 $K=e(rasG,H_1(T))=e(G,H_1(T))^{ras}$;④输出 $v_i^{'}=<U,V>=<rG,M\oplus H_2(K)>$。

(3)解密算法 DeAL。由计票管理合约进行操作,输入项密文 $v_i^{'}$,计票合约公钥 Y_J 与时间服务器给出时钟实例对应的时间陷门 S_r,得到最终的选票选项 v_i。具体流程为:①计算 $K^{'}=e(U,S_r)^{a}$;②计算 $V\oplus H_2(K^{'})$,得到选项 v_i。

3　电子投票协议方案

本协议结构使用盲签名算法与时间释放加密算法,结合运行在以太坊上的智能合约完成电子投票过程。智能合约分为投票管理合约与计票管理合约。协议中盲签名算法的引入为参与投票的选民进行身份合法性认证授权,不仅保护了选民隐私安全,还可有效防止外界攻击破坏匿名性。时间释放加密算法可实现选举结束后统一计票,保证唯一性与公平性。智能合约将取代传统可信第三方(TTP)的工作,摆脱信任依赖,保证投票过程的完整性与安全性。本协议流程如图 3 所示。

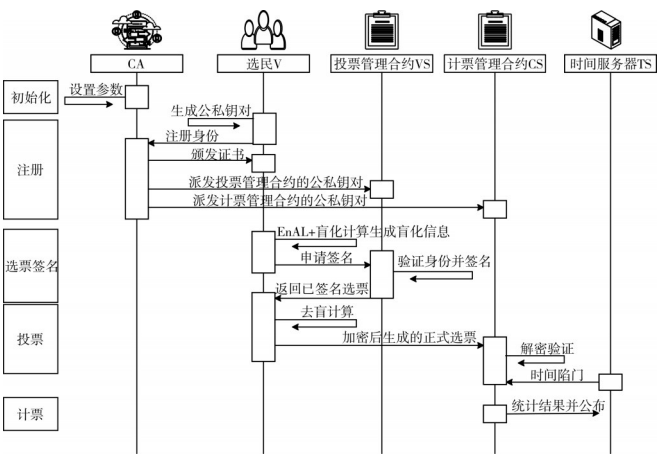

图 3　协议流程

3.1　角色定义

投票组织者:管理参与投票的合法选民名单、决议内容与选项、投票环节时间节点设置,以及椭圆曲线参数设置。

中央信任机构 CA:负责为合法选民颁发资格认证,生成与分配公私钥对给对应的智能合约。

投票管理合约 VC:自动审核选民身份的合法性,并参与选票信息盲签名,包括接受、签名与反馈。

计票管理合约 SC:自动统计收到的选票,并公布最终选票与选举结果。

时间服务器 CS:时钟 T 与时钟陷门 S_r。

另外还有一些参数定义,如表 1 所示。

表 1 参数定义

参数	定义
$t_{RegistionBegin}$	注册起始时间
$t_{RegistionEnd}$	注册结束时间
$t_{ElectionBegin}$	投票起始时间
$t_{ElectionEnd}$	投票结束时间
$t_{interval}$	各阶段间隔
RegList	注册记录表,避免“双花”问题
BallotList	选票记录表,防止复制攻击

3.2 协议设计

3.2.1 系统初始化

作为投票活动的发起与管理单位,根据投票目标,组织者将进行投票参数的设定与公布,保证投票规则的透明化。

(1)投票组织者设置待决议问题与对应选项 $\{v|v \in N\}$。

(2)根据选举周期设计各时间节点参数,规划投票进程。

(3)确定参数。

(4)参数设置完备,进行信息公开,并激发管理合约,进入注册阶段。

3.2.2 选民注册

权威机构 CA 对选民合法身份准入进行认证。选民 V_i 向其表明身份,等待机构审核,若合法则发放证书。同时,CA 负责颁发公私钥对给智能合约。具体步骤如下:

(1)选民 V_i 生成随机数密钥 (x_i, y_i),则可以得到公钥为:$z_i = x_i G + y_i H$。

(2)选民 V_i 发送注册消息 $\{z_i, ID_i\}$ 给中央信任机构 CA 进行身份审核。

(3)中央信任机构 CA 完成认证,若注册申请人 V_i 具有投票资格,则 CA 随后为其颁发资格证书 $CERT_i$。

(4)中央信任机构 CA 为选票管理合约生成两组签名密钥 $((X_{VC}, Y_{VC}), Z_{VC})$ 和 $((d,f), Q)$。其中 $Z_{VC} = X_{VC}G + Y_{VC}H$,$Q = dG + fH$。两组私钥 (X_{VC}, Y_{VC})、(d,f) 通过安全信道传递给投票管理合约并保密。

(5)投票管理合约根据选民注册情况生成注册记录表 *RegList*。*RegList* 包括身份认证书 $CERT_i$ 以及表决标识位,申请标志位用于标记选民是否完成选票申请,默认值为“0”,当用户完成申请则标识位置“1”,从而避免“双花”问题。注册记录表如表 2 所示。

表 2 注册记录

序号	身份认证书	申请标志位
1	$CERT_1$	1
2	$CERT_2$	0
…	…	…

(6)中央信任机构 CA 为计票管理合约生成密钥对 $((X_{SC}, Y_{SC}), Z_{SC})$。同样,将私钥 (X_{SC}, Y_{SC}) 通过安全信道传递给计票管理合约并保密。

3.2.3 选票签名

投票者请求管理合约对选票进行签名操作。要求 $t_{RegistionBegin} < \text{timeNow}() < t_{RegistionEnd}$,步骤如下:

(1)选民 V_i 的投票选项为 v_i,V_i 首先使用加密算法 EnAL 进行时间释放加密运算操作,得到 v_i'。

(2)选民 V_i 生成盲化因子 $\beta_i, \gamma_i, \delta_i \in {}_R Z_n^*$,然后进行操作计算。

$$Z_{VC} + \beta_i G + \gamma_i H + \delta_i Q = (x_i, y_i)$$

$$Z_{VC} + \beta_i G + \gamma_i H + \delta_i Q = (x_i, y_i)$$

$$a_i = x_i \bmod n$$

$$c_i = SHA\text{-}1(v_i' \| a_i)$$

$$e_i = c_i - \delta_i$$

v_i' 作为原始内容,首先进行盲化;选民 V_i 将 $\{CERT_i,\ e_i\}$ 发送给投票管理合约;投票管理合约 VC 收到 V_i 消息,判断证书有效性与 Re*gList* 标志位是否为“0”,若同时满足则签名。VC 对盲化选票进行签名计算。

$$r_i = t - e_i d$$

$$s_i = u - e_i f$$

操作完成后将 *RegList* 中 $CERT_i$ 位置“1”,并将 $\{(r,s)\}$ 传送回 V_i。

3.2.4 投票

选民 V_i 对返回值进行计算,获得原始选票签名信息,生成正式选票。正式选票需通过匿名加密方式发送给计票管理合约。

要求 $t_{ElectionBegin} < \text{timeNow}() < t_{ElectionEnd}$,步骤如下:

(1)选民 V_i 对返回值进行脱盲计算。

$$\rho_i = r_i + \beta_i$$

$$\sigma_i = s_i + \gamma_i$$

即可得到原始选票的盲签名 (c_i, ρ_i, σ_i)。

(2)选民 V_i 根据选票信息 $\{(c_i, \rho_i, \sigma_i) \| v_i'\}$ 生成正式选票,并利用计票管理合约公钥进行加密运算,即:

$$Ballot_i = ENC\{(c_i, \rho_i, \sigma_i) \| v_i'\}_{Z_{SC}}$$

(3)选民 V_i 将选票 $Ballot_i$ 匿名发送给计票合约。

3.2.5 统计与公布

(1)计票合约 SC 收到 V_i 的选票,利用私钥 (X_{SC}, Y_{SC}) 解密选票,验证签名 (c_i, ρ_i, σ_i) 的有效性,即计算:

$$c_i = SHA\text{-}1(v_i' \| R_x(c_i Q + \rho_i G + \sigma_i H) \bmod n)$$

(2)签名有效性验证通过后,在 *BallotList* 中查询 c_i 以防止复制攻击,若有记录,则抛弃选票。

(3)时间服务器 CS 进行 TBCT 运算,计算并广播时钟实例时间陷门,直到计票合约收到指定统计时间 T_T 的门限 $(S_r)_T$。

(4)计票合约收到 $(S_r)_T$,运行 DeAL 解密算法,对保存的选票选项 $\{v_i'\}$ 进行解密操作得到 $\{v_i\}$。最终公布统计结果,并通过共识算法进行节点认证后写入账本。

4 安全性分析

按照电子投票系统的属性要求,对本方案进行安全性分析。

(1)保密性。椭圆曲线算法的难解性首先保证了几乎无法破解与伪造签名,其次 TRE 技术基于离散对数与 BDH 难题,也具有很高的安全性。

(2)身份合法性。本方案通过中央信任机构 CA 对选民身份进行审核,设定准入机制,保证了选民群体身份的合法性。

(3)匿名性。本协议采用的时间释放加密算法可保证选票信息维持加密状态,直至统计阶段。潜在攻击者从投票合约与计票合约可以窃听的数据 $\{e_i,(r_i,s_i),CERT_i\}$ 与 $\{(\rho_i,\sigma_i),v_i'\}$ 中无法推断出关联性。

(4)唯一性。计票合约维护 *BallotList*,防止复制攻击,保证唯一性。

(5)公平性。使用 TRE 对选票加密,在指定统计时间 T_T 到达前,V_i、CA、VS、CS、TS 以及任何第三方都无法查看选票内容,保证了公平性。

(6)不可伪造,不可重复性。*RegList* 与 *BallotList* 使系统具有抗伪造性。

(7)抗共谋性。区块链智能合约按照协议设定运行的逻辑性代码,用户可以公开审查以确定其安全性。其次,分布式结构使得系统具有很强的鲁棒性。

另外,通过与一些基于区块链的电子投票协议[20-21]进行对比,本协议在各方面都具有良好的性能表现(见表 3)。

表 3　协议性能比较

项目	Bitcongress	FollowMyVote	本协议
身份合法认证	否	是	是
公平性	是	否	是
匿名性	是	否	是
完整性	是	否	是
投票方式	单选	多选	多选

5　结语

本文提出一种基于盲签名与时间释放加密的区块链匿名电子投票方案,采用时间释放加密算法 TRE 以及基于椭圆曲线的盲签名算法,有效保障了电子投票系统的匿名性、安全性与可验证性等。与现有电子投票系统相比,本方案利用区块链技术降低了投票成本,减少了信任依赖,从而提升了投票系统的便利性及安全性,同时也验证了区块链技术在电子投票领域的适用性。

参考文献:

[1] CHAUM D L. Untraceable electronic mail return addresses, and digital pseudonyms[J]. Commun ACM (USA), 1981, 24(2): 84-88.

[2] DONG L, CHEN K. Cryptographic protocol[C].Proceedings of the Proc ACM Symposium on Theory of Computing, 1982:383-400.

[3] LEE B, BOYD C, DAWSON E, et al. Providing receipt-freeness in mixnet-based voting protocols[J]. Lecture Notes in Computer Science, 2004, 2971:245-258.

[4] PARK C. Efficient anonymous channel and all/nothing election scheme [J]. Eurocrypt, 1993, 765:248-259.

[5] ZHONG S, BONEH D, JAKOBSSON M, et al. Optimistic mixing for exit-polls[J]. Proceedings of Asiacrypt Dec, 2002, 2501:451-465.

[6] 宋程远,张申绒,曹帅.一种盲签名方案及其在电子投票协议中的应用[J].计算机工程,2012, 38(6):139-141.

[7] HIRT M, SAKO K. Efficient receipt-free voting based on homomorphic encryption[J]. Lecture Notes in Computer Science, 2000, 1807: 539-556.

[8] RIVEST R. On data banks and privacy homomorphisms[J]. Foundations of Secure Compuation, 1978, 169-179.

[9] BONEH D, GOH E J, NISSIM K. Evaluating 2-DNF formulas on ciphertexts[C]. Theory of Cryptography Conference, 2005:325-341.

[10] BENALOH J, FISCHER M J. A robust and verifiable cryptographically secure election scheme[C]. Symposium on Foundations of Computer Science. IEEE, 1985:372-382.

[11] CRAMER R, GENNARO R, SCHOENMAKERS B. A secure and optimally efficient multi-authority election scheme[J]. Transactions on Emerging Telecommunications Technologies, 2012, 8 (5): 481-490.

[12] BAUDRON O, FOUQUE P A, POINTCHEVAL D, et al. Practical multi-candidate election system[C]. Twentieth Acm Symposium on Principles of Distributed Computing, 2001: 274-283.

[13] FUJIOKA A, OKAMOTO T, OHTA K. A practical secret voting scheme for large scale elections [C]. Advances in Cryptology - AUSCRYPT '92 Workshop on the Theory and Application of Cryptographic Techniques Proceedings, 1993:244-251.

[14] ABE M, FUJISAKI E. How to date blind signatures[C]. International Conference on the Theory & Application of Cryptology & Information Security. Springer Berlin Heidelberg, 1996: 244-251.

[15] ZHANG F, SAFAVI-NAINI R, SUSILO W. Efficient verifiably encrypted signature and partially blind signature from bilinear pairings [C]. 4th International Conference on Cryptology, 2004:191-204.

[16] ISTVAN S. Implementing an e-voting protocol with blind signature on Ethereum [EB/OL]. https://medium.com/coinmonks/.

[17] 张方国,王常杰,王育民.基于椭圆曲线的数字签名与盲签名[J].通信学报, 2001, 22(8): 22-28.

[18] CRESCENZO G D, OSTROVSKY R, RAJAGOPALAN S. Conditional oblivious transfer and timed-release encryption[C]. International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1999:74-89.

[19] CHAN A C F, BLAKE I F. Scalable, server-passive, user-anonymous timed release cryptography[C]. IEEE International Conference on Distributed Computing Systems. IEEE Computer Society, 2005: 504-513.

[20] BitCongress. Control the world from your phone[EB/OL]. http://www.bitcongress.com/Bitcongress/_whitepaper.pdf.

[21] The Online Voting Platform of the Future.Follow my vote[EB/OL]. http://followmyvote.com.

[22] MCCORRY P, SHAHANDASHTI S F, HAO F. A smart contract for boardroom voting with maximum voter privacy[C]. Financial Cryptography and Data Security, 2017: 357-375.

[23] NIR K, JEFFREY V. Blockchain-enabled e-voting[J]. IEEE Software, 2018, 35(4):95-99.

[24] 苑浩,杨宝霖.一种改进的预加密可验证电子投票方案[J].计算机应用研究, 2012, 29(8):3048-3052.

[25] 吴腾,黄锴,周琳琳.具有状态合法性验证的区块链一致性算法研究[J].计算机工程, 2018, 44(1):160-164.

(责任编辑:黄　健)