计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190900125

安全性电子投票方案研究综述

蒲泓全[1,2,3]　崔　喆[1,2]　刘　霆[1,2,3]　饶金涛[1,2]
1 中国科学院成都计算机应用研究所　成都 610041
2 中国科学院大学　北京 100049
3 广西混杂计算与集成电路设计分析重点实验室　南宁 530006
(774149765@qq.com)

摘　要　近年来,电子投票因可以大幅度提高投票活动的效率和结果的准确性而得到高度关注。安全性问题一直是制约电子投票发展的瓶颈,许多研究者针对某一应用功能场景提出了相关的电子投票方案。结合电子投票的学术研究现状,详细分析了电子投票的类型、模型和安全性要求,并结合盲签名、秘密分享等相关密码学技术对4种类型的典型电子投票方案进行了综述和分析,然后介绍了成熟的电子投票系统,最后研究了电子投票未来可能的发展方向,对电子投票方案的进一步优化和改进提供借鉴和参考。

关键词:电子投票;安全性要求;盲签名;秘密分享;密码学技术
中图法分类号　TP309.2

Comprehensive Review of Secure Electronic Voting Schemes

PU Hong-quan[1,2,3],CUI Zhe[1,2],LIU Ting[1,2,3] and RAO Jin-tao[1,2]
1 Chengdu Institute of Computer Applications,Chinese Academy of Sciences,Chengdu 610041,China
2 University of Chinese Academy of Sciences,Beijing 100049,China
3 Guangxi Key Laboratory of Hybrid Computation and IC Design Analysis,Nanning 530006,China

Abstract　In recent years,electronic voting has been highly concerned because it can greatly improve the efficiency of voting activities and the accuracy of the results. The security problem has been the bottleneck of the development of electronic voting. Many researchers put forward relevant electronic voting schemes for a certain application function scenario. Combined with the academic research status of electronic voting,this paper analyzes the types,models and security requirements of electronic voting in detail,summarizes and analyzes four types of typical electronic voting schemes by combining blind signature,secret sharing and other related cryptography technologies,then introduces the mature electronic voting system,and finally this paper studies the possible development direction of electronic voting in the future,which provides reference for further optimization and improvement of electronic voting schemes.

Keywords　Electronic voting,Security requirements,Blind signature,Secret sharing,Cryptography technology

1　引用

投票对于社会文明的发展起着重要的作用。随着科技的进步,投票的工具和形式逐渐由最初古希腊使用的“陶片”演化到纸质投票,目前已出现了电子投票。电子投票的出现克服了过去唱票表决耗时耗力的缺点,大幅提高了投票过程的效率和投票结果的准确性。目前,巴西、爱沙尼亚、印度、委内瑞拉等已在全国范围内使用电子投票,加拿大、美国、阿根廷等在议会和立法投票中也已使用电子投票,英国、意大利、挪威、澳大利亚等对电子投票的使用已经通过测试,我国在部分领域也有了电子投票的应用。电子投票的安全性一直是制约其发展的瓶颈,比利时、法国等因为安全性已停止使用电子投票,挪威的互联网电子投票系统也被发现存有严重的漏洞,因此研究电子投票的安全性,设计保护隐私的电子投票方案,是十分必要的。许多研究者针对电子投票的安全性,利用各种密码学技术提出了大量安全性的电子投票方案。根据投票过程中所采用的流行密码技术,现有的电子投票方案可分成4种类型[1-5]:基于混合网络的电子投票方案、基于盲签名的电

到稿日期:2019-09-18　返修日期:2020-03-15　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金(61501064);四川省科技支撑计划项目(2015GZ0088);广西混杂计算与集成电路设计分析重点实验室开放基金(HCIC201701)
This work was supported by the National Natural Science Foundation of China(61501064),Sichuan Technology Support Program(2015GZ0088) and Guangxi Key Laboratory of Hybrid Computation and IC Design Analysis (HCIC201701).
通信作者:崔喆(cuizhe@casit.com.cn)

子投票方案、基于秘密分享的电子投票方案和基于同态加密的电子投票方案。

本文结合相关秘密学工具对目前典型的电子投票方案类型进行了深入分析和研究；第 2 节分析了当前主流的电子投票类型和通用模型；第 3 节详细分析了电子投票的安全性要求；第 4 节分析基于混合网络的典型电子投票方案；第 5 节结合盲签名分析典型的基于盲签名的电子投票方案；第 6 节深入研究了基于秘密分享的电子投票方案；第 7 节分析了 3 种同态加密类型及其在电子投票方面的应用情况；第 8 节对 4 种电子投票类型进行部分安全性和通信复杂度的对比分析；第 9 节介绍了成熟的电子投票系统；最后对电子投票的发展方向进行了分析，例如区块链、云计算等相关技术的运用，并对全文进行总结。

2 电子投票的类型和模型

电子投票方案需要考虑投票的类型。文献[1]根据选票的形式，将电子投票分成 6 类。

(1) yes/no：投票者填写选票的时候只有 yes 或者 no 选项。

(2) 1-out-of-L：投票者从 L 个候选人中选择一个。

(3) K-out-of-L：投票者从 L 个候选人中选择 K 个，其中 K 个人没有次序之分。

(4) K-out-of-L order voting：投票者从 L 个候选人中选择 K 个人，并且 K 个人是有次序之分的。

(5) 1-L-K voting：投票者先从 L 集合中选择一个，再从对应的集合中选择 K 个。例如，班级选代表时，有 L 个不同的小组，投票者先从 L 个小组中选择自己所在的小组，再从自己选择的小组的候选人中选择 K 个代表。

(6) Write-in voting：在投票时，可以选择不在候选者名单中的人。

大多电子投票最初只支持第一种类型[2-3]，为了满足实践需求，越来越多的电子投票方案被提出，陆续出现后面几种类型的投票协议[4-7]。

按照票的权重进行分类[1]，电子投票可以分为 equal-voting 和 weighted-voting。equal-voting 中每个投票者投出的票的权重一样，weighted-voting 中每个投票者投出的票的权重不一样，在实践中这两种类型使用得较少[8]。

一个完整的电子投票模型[9-10]应当包括投票者、注册机构、选票发放机构、计票机构和监票机构。其中，投票者是参与投票的主体；注册机构是电子投票系统的注册和审批机构，为满足条件的投票者发放资格证书；选票发放机构在电子投票开始之后，将合法的空白选票发放给有投票资格的投票者；计票机构核查选票的合法性，并执行计票职能；监票机构对投票的结果进行监督。其中，注册机构、选票发放机构、计票机构、监票机构假定是完全可信任的，是逻辑上必备的，具体的电子投票方案和实际应用可能将其中一个机构扩展成多个机构，或者将几个功能机构合并成一个机构。整个电子投票系统的流程如图 1 所示。

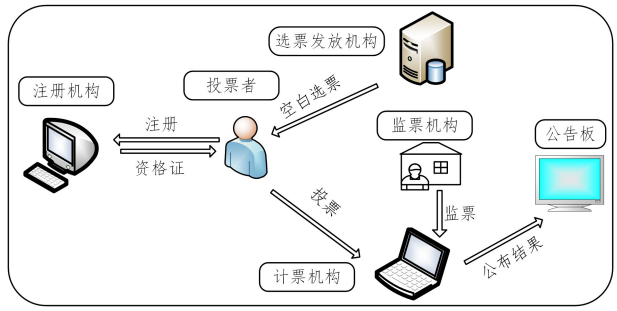

图 1 电子投票流程

Fig. 1 Electronic voting process

(1)具有投票权利的投票者向注册机构申请投票的资格证书；

(2)注册机构收到申请后，审核申请投票者的投票资格，如果满足则发放资格证书，否则拒绝发放；

(3)选票发放机构将空白的选票发送给有资格的投票者；

(4)有资格的投票者收到空白选票后进行填写，然后将自己的资格证和选票一并发送给计票机构；

(5)投票结束后，计票机构审核所有的资格证及对应的选票，并统计资格证和选票均有效的选票内容；

(6)监票机构根据资格证和选票对结果进行监督，若计票机构统计无误，由计票机构公布投票结果。

3 电子投票的安全性

电子投票的发展受到实践中安全性要求的制约，因此电子投票协议中的隐私性保护越来越受到许多国家研究者的关注和重视。日本学者 Fujioka 等[11]提出的电子投票方案 FOO 中定义了电子投票的 7 个安全性要求，被视为电子投票协议的基本安全要求。

(1)完整性：所有有效的票被正确统计。

(2)正确性：所有无效的票都不能被计入。

(3)秘密性：投票者所投的票必须被保密。

(4)不可重用性：投票者不能重复投票两次以上。

(5)适格性：只有具有投票权的投票者才能进行投票活动。

(6)公平性：没有人知道投票的中间结果。

(7)可验证性：没有人能够伪造投票结果。

之后，随着网络安全事件的不断发生，又有一些学者提出了更高的安全性要求。Benaloh 等[2]首次提出了无收据性概念，即投票者不能构造收据向贿选者证明自己投票的选票内容，主要用来抵御贿选者扰乱投票活动。Juels 等[12]提出了抗威胁性的概念，保证在少数存在安全问题的计票器情况下，其可以抵御随机化攻击。抗威胁性假设在投票者投票的那一刻，威胁者不能跟踪或监视投票者。Sako 等[13]提出了广泛可验证性的概念，要求不仅投票者可以验证自己的选票是否被正确计入结果，其他任何人都可以验证投票结果的正确性。Riera 等[14]提出了抗强制性的概念，用于防止攻击者强迫投票者投票或者强迫其弃权。

4 基于混合网络的电子投票方案

混合网络(mix-net)是一种实现通信匿名性的关键技术，

可以保证用户在访问资源或者服务时不泄露其身份信息。混合网络由多个混合服务器组成，每个混合服务器都有自己的公钥，在接收到加密的信息后进行解密、处理和置乱排序，然后将处理结果发送给接收者[1]。

1981 年，Chaum[15] 提出了电子邮件中的匿名通信问题，设计了基于 RSA 公钥密码体制的匿名通信协议，并指出可以将其应用到电子投票中实现投票者的匿名性。Chaum 的方法是一种基于混合网络的电子投票方案，可以抵抗被动攻击，使得被动攻击者可以监控混合服务器之间的通信，但不能够得到混合服务器内部置乱的情况，从而达到抵御攻击的目的。该方法中的一个混合服务器被攻击后，整个置乱过程将失效，因此很难适用于大规模的投票活动。2001 年，Furukawa 等[16] 提出了一种基于混合网络的电子投票方案，该方案能够证明置乱过程的正确性，且不泄露置乱是如何操作的。该方案置乱 n 个数据，大致有 $18n$ 的指数运算次数，比文献[17]方案的 $642n$ 和文献[18]的 $22n\log n$ 更优。同年，Neff[19] 提出了可对数据进行置乱或者混淆的实现方法，并证明了其正确性。该方案在理论和实现上大大提高了效率，其置乱 n 个数据大致需要 $8n+5$ 的指数运算次数，比文献[16-18]的方案更高效；同时，该方法的结构性特征也便于系统的实现。基于该方法，Neff 实现了一种基于混合网络的可验证多候选人的电子投票方案，并验证了其满足相关的安全性要求。

基于混合网络的电子投票方案中的一个置乱过程需要一个零知识证明，因此针对大规模的投票活动，其开销较大，难以用于实际的投票活动中，目前仍停留在理论阶段。

5 基于盲签名的电子投票方案

5.1 盲签名

1982 年，Chaum[20] 提出了盲签名的概念。该方案是基于 RSA 关于大整数分解的公钥秘密体制，用户对需要签名的消息进行盲化处理后再发送至签名者，签名者对盲化后的消息进行签名后返回给用户，用户脱盲处理后获得签名者的签名。在这一过程中，用户的消息内容不会被签名者所掌握。图 2 给出盲签名的过程，其类似于用户将消息装进信封发送给签名者，签名者在信封外面签名后再返还给用户。

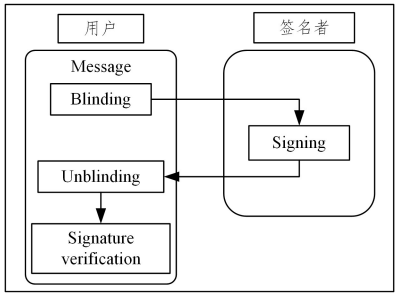

图 2 盲签名过程

Fig. 2 Blind signature process

盲签名因在签名过程中能有效实现匿名性，避免签名信息被泄露，因此被广泛应用在多个领域，如电子商务、电子投票和电子支付等。许多研究者提出了多种不同的盲签名方案。1992 年，Okamoto 等[21] 提出了基于 Schnorr 签名的盲签名方案，Schnorr 签名是对 Elgamal 签名的改进，它们都是基于离散对数问题，其签名安全性更高。2000 年，我国研究者 Yao 等[22] 提出了基于二元仿射变换的广义 ELGamal 型盲签名方案；同年，Fan 等[23] 提出了基于 Chaum 方案的改进方案。在 Chaum 的盲签名方案中，签名者进行签名时，将一个随机化因子注入被签名的消息中，并且用户不能消除签名过程中嵌入的随机化因子，可以有效防止攻击者在 Chaum 方案中获得多个签名而进行伪造的情形。2003 年，Shi 等[24] 提出了一种基于 RSA 的 XML 盲签名方案，该方案结合了 XML 和盲签名的特点，具有更高的安全性。此外，国内外学者还提出了多种不同的盲签名方案[25-30]。

5.2 典型的盲签名电子投票方案

1992 年，日本学者 Fujilka 等[11] 提出了著名的 FOO 电子投票方案。该方案基于 RSA 盲签名，解决了大规模电子投票中的安全性问题，并提出了至今仍然适用的电子投票过程中的 7 个安全要求。该方案包括投票者、管理机构、机票机构 3 个实体，包括初始化、注册、投票、收票、核票、计票 6 个阶段。该方案的整个过程如图 3 所示，图中的符号和公式含义如表 1 所列。

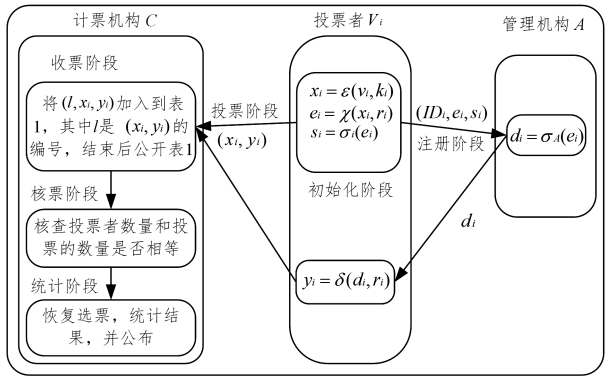

图 3 FOO 的整个过程

Fig. 3 Whole process of FOO

表 1 FOO 方法中符号及公式的含义

Table 1 Symbol and formula meaning in FOO method

符号/公式	含义
V_i	投票者
A	管理机构
C	计票机构
$\varepsilon(v,k)$	使用密钥 k 用比特承诺函数 ε 加密 v
$\sigma_i(m)$	投票者 V_i 的签名
$\sigma_A(m)$	管理者 A 的签名
$\chi(m,r)$	随机选择盲化因子 r 对 m 盲签名
$\delta(s,r)$	对 s 脱盲处理
ID_i	投票者 V_i 的身份标识
v_i	投票者 V_i 的选票

许多著名的电子投票系统都是基于该方案设计而成，如华盛顿大学的 Sensus 系统[31]、麻省理工大学的 EVOX 系统[32]。FOO 投票方案也存在一些安全性问题，比如投票者无法弃权、选票可能存在碰撞、无法满足无收据性、投票过程过度依赖于计票机构等[33]。许多学者针对部分安全性问题，提出了相应的改进策略。

1997 年，Okamoto[34] 提出了适用于大规模投票活动的无收据性电子投票方案，这是基于盲签名的第一个无收据性的

电子投票方案，其基于不可追踪匿名通信信道和一定的物理假设。2004 年，Shubina 等[35]基于盲签名和投票亭提出了一个抗威胁性的电子投票方案，该方案存在设计问题，无法满足无收据性、普遍验证性、匿名性等相关要求。2006 年，Chang 等[36]利用 Chaum 盲签名方案和 Diffie-Hellman 密钥交换协议提出了安全投票方案。该方案在各个实体机构之间共享一个密钥以保护选票的安全；但方案中可以将盲化因子作为投票者的收据，因此无法满足无收据性。2008 年，Fan 等[37]利用盲签名和随机化方法降低投票系统受威胁的概率，提出了一种高效的电子投票方案。该方案中每个投票者与管理机构均随机选择一个长度固定的串，并将串合并后作为选票的一部分，这样每张选票的串各不相同，可以有效阻止攻击者把选票与随机串关联，保证了投票和计票环节的安全性。2009 年，Guo 等[38]提出了基于群盲签名的电子投票方案，该方案基于群签名和盲签名各自的特点而提出。该方案还基于可信任第三方 CA 为安全可信任的假设，这属于理想情况，很难应用到实际中。2011 年，Chen 等[39]提出了一种基于双门陷承诺的盲签名电子投票方案，该方案是对 Okamoto[34]方案的改进，可适用于大规模的电子投票活动，同时不需要选举机构和投票站物理机构。2015 年，Luo 等[33]提出了无收据性的电子投票方案，该方案基于 FOO，并引入了投票编号、申诉标识，能够满足无收据性和匿名性等安全性要求，但无法满足普遍验证性。此外，还有许多其他基于盲签名的电子投票方案[40-44]，此处不做详细讨论。

基于盲签名的电子投票方案实用性较强，并且满足基本的安全性需求，但随着人们对信息安全重视程度的提高，电子投票方案还须满足无收据性和可验证性等要求。现有的改进方案均无法满足全部相关要求，若能解决此类方案中的安全性问题，则能够使电子投票系统更好地应用于各国的选举活动。

6 基于秘密分享的电子投票方案

6.1 秘密分享

秘密分享(Secret Sharing，SS)的概念最早由 Shamir[45]和 Blakley[46]于 1979 年独立提出，两人分别提出了(t,n)秘密分享方案。随后，基于中国剩余定理的秘密分享方案[47]、基于向量空间的秘密分享方案[48]、基于矩阵运算的秘密分享方案[49]等被提出。Shamir 秘密分享方案是最常用的方案，其基于 Lagrange 差值定理，具有以下特点。

(1)任何少于 t 个秘密份额都无法恢复分享的秘密。

(2)只要获得 t 个及以上的秘密份额就可以恢复出分享的秘密；即使 $n-t$ 个秘密份额丢失或者遭到破坏，也可以恢复出分享的秘密。

Shamir 的秘密分享过程如下：假设有一个可信赖的秘密分发者 D 和 n 个参与者的集合$\{P_1,P_2,\cdots,P_n\}$，D 需要分发的秘密为 s，$GF(q)$(q 为大素数)是有限域，D 随机从 $GF(q)$中选择 $t-1$ 个元素 $a_1,a_2,\cdots,a_{t-1}$。D 首先构造多项式 $f(x)=s+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}$，然后从 $GF(q)$中随机选择 n 不同的元素 $x_1,x_2,\cdots,x_n$(这 n 个元素是公开的)，并发送给 n 个参与者，计算 $y_i=f(x_i)$，并通过安全信道将(x_i,y_i)发送至 P_i。不妨设 n 个参与者中的任意 t 个参与者收到的秘密份额和公开的 x 值为$(x_1,y_1),(x_2,y_2),\cdots,(x_t,y_t)$，通过下式其可恢复出秘密 s。

$$s=\sum_{i=1}^{t}y_i\prod_{j=1,j\neq i}^{t}\frac{x_j}{x_j-x_i}$$

秘密分享概念被提出之后，许多研究者提出了相应的秘密分享方法，如多阶段秘密分享[50-51]、多重秘密分享[52]、无秘密分发者的秘密分享[53]、可视秘密分享[54-55]、量子秘密分享[56]等，这些秘密分享在许多应用领域，如安全多方计算(SMPC)、电子投票、电子拍卖、电子支付、数字签名等得到了广泛的应用。本文对秘密分享在电子投票中的应用进行了深入的研究和分析。

6.2 典型的秘密分享电子投票方案

1999 年，Schoenmakers[57]提出了基于公开可验证的秘密共享电子投票方案，该方案中任何一方都可以验证秘密分发者分发秘密份额的有效性，验证不限于接收秘密份额的各个参与者，因此该方案具有一定的实用性。2007 年，Iftene[58]提出了一种基于中国剩余定理的秘密分享技术，并讨论了该方案的可验证性、秘密共享同态和乘法性质；基于这些性质进一步提出了电子投票方案，该方案只介绍了 Yes/no 电子投票这一简单情形，从集合$\{\beta+1,\cdots,\alpha-1\}$秘密选择一个值 $value_{yes}$ 赋给 Yes 选票，秘密选择一个值 $value_{no}$ 赋给 No 选票，每个投票者都进行上面的操作，然后利用提出的秘密分享方法进行投票活动。2007 年，Zwierko 等[59]基于秘密分享和 Merkle 难题，提出了分布式信任的轻量级电子投票模型，该方法可适用于基于互联网的各类电子设备。秘密分享是基于文献[47]，Merkle 用于在不安全信道中间保证通信双方的安全性，分布式信任体系结构使得投票发送阶段具有鲁棒性、可靠性和有效性[60]，该电子投票方案整体高效，且具有实用性。2014 年 Nair 等[61]提出了基于安全多方计算的秘密分享的电子投票方案，用位表示选票，使用秘密份额来传输和计算，用 shamir 方法对秘密份额进行安全求和。该方法不需要任何安全性的数学假设，并可证明是安全可靠的。其还提出了在满足匿名性的前提下计算候选人得票数的方法。2017 年，Zhao 等[62]提出了基于 Shamir 秘密分享和 K-匿名的电子投票方案，所提方案结合 Shamir 秘密分享的同态性，满足整个投票过程的正确性、匿名性、一致性和抗欺骗性。2017，Yuan 等[63]提出了基于 Mignotte 秘密分享[64]的分布式可验证电子投票方案，该方案基于中国剩余定理有效地平衡了投票人与计票中心的冲突；此外，该方案投票者承担了本方案的主要计算量，有效地减轻了计票器的计算负担。

基于秘密分享的电子投票方案需要可信任的秘密分发机构和多个计票机构等，投票者、秘密分发机构、计票机构之间的通信复杂度是影响使用的核心要素。

7 基于同态加密的电子投票方案

7.1 同态加密

1978 年，Rivest 等[65]首次提出了同态加密的概念。同态加密的思想是对一些加密后的数据进行运算后再解密，得到的结果与未加密的数据运算后的结果一致。同态加密可描述

为：假设 m_1 和 m_2 是需要被加密的明文，e_1 和 e_2 是加密后的密文，f_1 和 f_2 分别是加密函数和解密函数，则有 $e_1=f_1(m_1)$，$e_2=f_1(m_2)$。若 $m_1 \otimes m_2=f_2(e_1 \otimes e_2)$ 成立，则该密码系统是⊗同态的。符号⊗表示对明文 m_1 和 m_2 的运算。

同态加密概念被提出之后，许多研究者对其进行了深入的研究并在算法上取得了大量成果。目前，理论界的同态加密文献可以分为 3 类[66]：部分同态加密[67-69]（Partial Homomorphic Encryption，PHE）、浅同态加密[68,70-72]（Somewhat Homomorphic Encryption，SHE）、全同态加密[73-74]（Fully Homomorphic Encryption，FHE）。部分同态指的是只能实现加法同态和乘法同态中的一种；浅同态指的是可以实现有限次的加法同态和乘法同态；全同态指的是可以实现任意次的加法同态和乘法同态。一些传统的公钥加密算法中，ELGamal 算法满足乘法同态，RSA 算法满足乘法同态，Paillier 算法满足加法同态。同态加密技术运用广泛，在电子投票、安全云计算、安全多方计算、远程文件存储、电子签名等领域都有很好的应用[66]。本文重点研究同态加密技术在电子投票领域的应用情况。

7.2 典型的同态加密电子投票方案

2000 年，Damgard 等[75]提出了基于 Paillier 加密的电子投票方案。2002 年，Damgard 等[76]提出了基于 Elgamal 同态加密的电子投票方案，并给出了有效的零知识证明，使得本方案中的投票信息比已知方案的更短，更容易计算和验证，最大限度地降低了无法用密码技术处理的风险。2004 年，Acquisti 提出了基于匿名信道的 Paillier 加密的电子投票方案，该方案中的投票结果管理机构获得两张表，一张是管理机构自己生成的信任状密文执行混淆操作的结果，另一张是信任状和票的密文执行混淆后的结果，两张表中的参数都是基于 Paillier 加密。

根据文献[1]，该方法不支持确定性，不具有无收据性，且不能防止 1009 攻击。2006 年，Meng 等[77]针对 Acquisti 的方案进行改进，提出了一种基于 ELGamal 加密的无收据性和抗威胁性的远程网络投票协议，该协议支持多种类型的选票。

2008 年，Han 等[78]提出了一种基于同态加密的电子投票方案，该方案通过随机化器和投票者合作产生最终的选票，投票者不能获得随机化器产生的信息，也不能向他人证明自己最初的选票与最终的选票之间的关系，因此即便攻击者获得了投票者最初的选票内容，也无法知道最终的投票信息是否为最初的选票内容，满足无收据性。2017 年，Wang 等[79]提出了基于全同态加密的电子投票方案，该方案设计了同态密文加法器，并利用数字签名技术，实现了电子投票的匿名性、完整性和整体可验证性。2019 年，He 等[80]提出了基于数字签名和全同态加密的多候选人电子投票方案，该方案采用椭圆曲线数字签名算法解决电子投票中的身份认证问题，利用全同态加密实现对选票的加密以及对加密选票的求和。但是，该方法的效率不高，难以运用到实践中。

基于同态加密的电子投票方案通过对选票进行加密来实现投票过程的安全性，可以满足无收据性和可验证性等要求；同时，全同态加密方法的出现，为电子投票的不同规模应用提供了可能。因此，基于同态加密的电子投票方案理论上是完备的，加密和解密运算的复杂度将是影响此类方法的关键。

8 对比分析 4 种投票方案

下面对 4 种电子投票方案的安全性和通信复杂度进行对比分析，如表 2 所列。文中选取 4 项重要的安全性要求进行分析，Y 代表满足，N 代表不满足。

表 2 4 种电子投票类型的对比

Table 2 Comparison of four types of electronic voting

	混合网络	盲签名	秘密分享	同态加密
秘密性	Y	Y	Y	Y
正确性	Y	Y	Y	Y
无收据性	Y	N	Y	Y
广泛可验证性	Y	N	Y	Y
通信复杂度	低	中等	高	中等

从表 2 中可以看出 4 种方案都满足秘密性和正确性要求。基于盲签名的电子投票方案不满足无收据性，因为管理者在对盲化后的选票进行签名时需要验证其以前是否投过票，这一过程说明管理者存储了不同投票者的身份信息，即无法满足无收据性；同时，其不满足广泛可验证性，因为只有投票者自己才能检验选票是否被正确计入。对于通信复杂度，基于秘密分享的电子投票方案由于需要将选票分拆成多个秘密份额，再发送给计票中心，因此通信复杂度最高；基于盲签名和同态加密的电子投票过程中的通信复杂度相对较低，因为这两种方法依赖于所选取的可行的密码学方法；而基于混合网络的电子投票的通信复杂度最低，因为其仅仅是对数据进行扰乱再重置，这一过程不会额外增加通信复杂度。

9 电子投票系统

目前比较成熟的电子投票系统有 Sensus 系统、EVOX 系统、基于物理设备的电子投票系统等。

9.1 Sensus 系统

Sensus 系统[31]是华盛顿大学的研究者基于 FOO 设计的可以应用于实际的电子投票系统，其满足 FOO 提出的安全性要求，即便是选举机构互相串通，也能保护投票者的隐私。投票者可以验证自己的票是否被正确计入，若自己的票没有被正确计入，可以匿名质疑选举结果的正确性。该系统不会接受没有经过注册的投票者，也不会接受每个经过注册的投票者投出的超过一张的选票。实践表明，Sensus 系统便于投票者使用，投票者可以在很短的时间内填写选票，系统对填写的选票加密后投出；基于网页的可视化界面使得 Sensus 系统更人性化。但是，由于该系统基于 FOO 协议，因此 FOO 协议中的缺陷无法避免地出现于该系统中，如投票者的弃权问题、选票碰撞问题等。

9.2 EVOX 系统

麻省理工学院研究者基于 FOO 开发出的 EVOX 系统[32,81]，已成功用于该学院的本科生联合选举。该系统完成电子投票的过程需要过 5 个阶段：准备阶段、授权阶段、匿名化阶段、收集阶段和计票阶段。由于该系统过度依赖于管理中心，安全性得不到保证，因此后期又开发了多管理中心的 EVOX 系统，但其同样无法避免 FOO 协议的缺陷。

9.3 基于物理设备的电子投票系统

虽然基于不同密码学技术的电子投票在理论上能够保证不同要求的投票活动，但在实践中完全依靠网络通信和密码学技术的电子投票系统并不多见，因为密码协议、设备和网络通信还没有达到完全可靠、安全的程度，同时也难以平衡安全性和时间效率。对此，很多现有的电子投票系统引入了物理设备来解决以上问题。例如，基于投票站点的电子投票系统对选票进行优化设计，同时结合前面分析的4类投票方案可以解决投票者匿名性和合法性的矛盾以及选举结果的可验证性和无收据性之间的矛盾，同时效率得到有效提升。在当前阶段基于物理设备的电子投票系统是一种符合实际情况且能够大规模应用的投票系统。

结束语 一些新的安全技术的出现和大数据时代的到来，为电子投票的发展提供了更多方法和机遇。区块链是随着比特币等数字加密货币的出现而兴起的技术，其最大的特点在于去中心化的思想和架构，目前得到了政府部门、金融机构以及科技公司的高度重视，同时也成为学术界的研究热点。区块链去中心化的特点与电子投票的安全性要求正好相符。目前电子投票系统均存在假设的信任机构，造成实践中可能受到攻击而导致泄密的风险，区块链可以很好地解决这一问题。实现投票过程的去中心化，能促进电子投票系统的大规模使用。在大规模的电子投票活动中使用密码学技术能够在一定程度上解决安全性问题，但随之会产生计算效率问题，云计算的兴起为解决这一问题带来了机遇。但是，云计算在提高投票过程效率的同时，也会带来云安全问题，只有解决好安全问题，云计算才能更好地适用于电子投票系统。由此可见，研究云计算环境下的安全电子投票方案是十分有意义的，这也将是未来电子投票领域研究的热点之一。

本文对电子投票的类型、模型、安全性以及4类电子投票方案和成熟的电子投票系统进行了综述和分析。在具体应用中，须结合实际情况选择和设计具体方案，使安全性要求和效率得到平衡。最后，对未来可能的研究方向进行了分析。我国在电子投票理论研究领域起步较晚，现有的方案大多基于国际上的成熟方案，结合我国选举的特点设计具有实用意义的电子投票方案将是后续研究的重点。

参 考 文 献

[1] MENG B, WANG D J. Secure remote network voting protocol [M]. Beijing: Science Press, 2013: 3-4, 16-18, 76-81.

[2] BENALOH J, TUINSTRA D. Receipt-free secret-ballot elections[C]// Twenty-sixth ACM Symposium on Theory of Computing. 1994: 544-553.

[3] CANETTI R, DWORK C, NAOR C, et al. Deniable encryption [C]// Annual International Cryptology Conference on Advances in Cryptology-CRYPTO '97. 1997: 90-104.

[4] CRAMER R, FRANKLIN M, SCHOENMAKERS B, et al. Multi-authority secret ballot elections with linear work[C]// Proceedings of the 15th Annual International Conference on Theory and Application of Cryptographic Techniques. 1996: 72-83.

[5] LEE B, KIM K. Reciept-free electronic voting scheme with a tamper resistant randomizer [C]// Proceedings of the 5th International Conference on Information Security and Cryptology. 2002: 405-422.

[6] DAMAGARD I, JURIK M, NIELSEN J B. A generalization of Paillier's public-key system with applications to electronic voting[J]. International Journal of Information Security, 2010, 9(6): 371-385.

[7] KIAYIAS A, YUNG M. The voctor-ballot approach for online voting procedures[J]. Lecture Notes in Computer Science, 2010, 6000(1): 155-174.

[8] MENG B. A critical review of receipt-freeness and coercion-resistance[J]. Information Technology Journal, 2009, 8(7): 934-964.

[9] SUN M H. Modern cryptography research on secure multi-party computation protocols[M]. Beijing: Publishing House of Electronics Industry, 2016: 72-74.

[10] CHEN K B. The research and application on the electronic voting protocol[D]. Hefei: Hefei University of Technology, 2006.

[11] FUJILKA A, OKATOMA T, OHTA T. A practical secret voting scheme for large-scale elections[C]// Advances in Cryptology-AUSCRYPT'92. 1992: 244-251.

[12] JUELS A, CATALANO D, JAKOBSSON M. Coercion-resistant electronic elections [J/OL]. Towards Trustworthy Elections, 2010: 37-63. http://www.arijuels.com/wp-content/uploads/2013/09/JCJ05.pdf

[13] SAKO K, KILIAN J. Receipt-free mix-type voting scheme-A practical solution to the implementation of a voting booth[C]// International Conference on the Theory and Application of Cryptographic Techniques in Cryptology-EUROCRYPT' 95. 1995: 393-403.

[14] RIERA A, RIFA J, BORRELL J. Efficient construction of vote-tags to allow open objection to the tally in electronic elections [J]. Information Processing Letters, 2000, 75(5): 211-215.

[15] CHAUM D. Untraceable electronic mail, return address, and digital pseudonyms[J]. Communications of the ACM, 1981, 24(2): 84-90.

[16] FURUKAWA J, SAKO K. An efficient scheme for proving a shuffle[C]// The 21st Annual International Cryptology Conference on Advances in Cryptology-CRYPTO'2001. 2001: 19-23.

[17] SAKO K, KILIAN J. Receipt-free mix-type voting scheme [C]// International Conference on the Theory and Applications of Cryptographic Techniques-EUROCRYPT'95. 1995: 393-403.

[18] ABE M. Mix-Networks on Permutation Networks[C]// International Conference on the Theory and Application of Cryptology and Information Security-ASIACRYPT'99. 1999: 258-273.

[19] NEFF C A. A verifiable secret shuffle and its application to e-voting[C]// Proceedings of the 8th ACM Conference on Computer and Communications Security. 2001: 116-125.

[20] CHAUM D. Blind signatures for untraceable payment[C]// Advances in Cryptology Proceedings of CRYPTO'82. 1983: 199-203.

[21] OKAMOTO T. Provably secure and practical identification schemes and corresponding signature schemes[C]// Advances in Cryptology-CRYPTO'92. 1992: 31-53.

[22] YAO Y F, ZHU H F, CHEN K S. Generalized ELGamal type

blind signature schemes based on affine transform[J]. Acta Electronica Sinica,2000,28(7):128-129.

[23] FAN C I,CHEN W K,YEH Y S. Randomization enhanced Chaum's blind signature scheme[J]. Computer Communications,2000,23(17):1677-1680.

[24] SHI Y H,LI W S. XMLblind signature scheme based on RSA public key system[J]. Computer Engineering,2004,30(19):101-103.

[25] XIA M M,GU L Z. A new proxy blind signature scheme[J]. Journal of Beijing University of Posts & Telecommunications,2006,29(3):48-52.

[26] ZHANG J H,GAO S N. Efficient provable certificateless blind signature scheme[C]// Proceedings of the IEEE International Conference on Networking,Sensing and Control(ICNSC 2010). 2010:10-12.

[27] FAN C I,SUN W Z,HUANG S M. Provably secure randomized blind signature scheme based on bilinear pairing[J]. Computers & Mathematics with Applications,2010,60(2):285-293.

[28] SHAO J G,XUE B,CHEN M. Certificateless partially blind signature scheme based on the elliptic curve discrete logarithm problem[J]. Advanced Engineering Science,2012,44(1):112-117.

[29] SINGH N,DAS S,SINGH N,et al. A novel proficient blind signature scheme using ECC[C]// International Conference on Emergent Trends in Computing and Communication. International Journal of Computer Applications,2014:66-72.

[30] ZHANG J L,ZHAGN J Z,XIE S C. Improvement of a quantum proxy blind signature scheme[J]. International Journal of Theoretical Physics,2018,57(6):1612-1621.

[31] CRANOR L F,CYTRON R K. Sensus:a security-conscious electronic polling system for the Internet[C]// Proceedings of The Thirtieth Annual Hawwaii International Conference on System Sciences. IEEE Computer Society,1997.

[32] HERSCHBERG M A. Secure electronic voting over the World Wide Web[R/OL]. http://dspace. mit. edu/handle/1721. 1/43497.

[33] LUO F F,LIN C L,ZHAGN S Y,et al. Receipt-freeness electronic voting scheme based on FOO voting protocol[J]. Computer Science,2015,42(8):180-184.

[34] OKAMOTO T. Receipt-free electronic voting schemes for large scale elections[C]// International 5th Workshop on Security Protocols. 1997:25-35.

[35] SHUBINA A M,SMITH S W. Design and prototype of a coercion resistant,voter verifiable electronic voting system[C]// Proceedings of the 22nd Annual Conference on Privacy,Security and Trust. 2004:29-39.

[36] CHANG C C,LEE J S. An anonymous voting mechanism based on the key exchange protocol[J]. Computers & Security,2006,25(4):307-314.

[37] FAN C I,SUN W Z. An efficient multi-receipt mechanism for uncoercible anonymous electronic voting[J]. Mathematical and Computer Modelling,2008,48(9/10):1611-1627.

[38] GUO L L,GU L Z,LI Z X. The scheme of non-receipt electronic voting based on group and blind signature[C]// Proceedings of Academic Conference on Communications in China Colleges and Universities. 2009:225-230.

[39] CHEN X F,WU Q H,ZHANG F G,et al. New receipt-free voting scheme using double-trapdoor commitment[J]. Information Sciences,2011,181(8):1493-1502.

[40] WANG B Y,YANG F,HU Y F. Online Voting Scheme Based on Blind Digital Signature[J]. Journal of Chinese Mini-Micro Computer Systems,2003,24(3):587-591.

[41] YE W. FOO protocol and its improvement in electronic voting system[D]. Wuhan:Wuhan University of Technology,2009.

[42] MOHANTY S,MAJHI B. A secure multi authority electronic voting protocol based on blind signature[C]// 2010 International Conference on Advances in Computer Engineering. 2010:271-273.

[43] LOPEZ-GARCIA L,PEREZ L J D,RODRIGUEZ-HENRIQUEZ F. A pairing-based blind sgnature e-voting scheme[J]. The Computer Journal,2014,57(10):1460-1471.

[44] KUMAR M,KATTI C P,SAXENA P C. A secure anonymous e-voting system using identity-based blind signature scheme[C]// International Conference on Information Systems Security. 2017:29-49.

[45] SHAMIR A. How to share a secret[J]. Communications of the ACM,1979,22(11):612-613.

[46] BLAKLEY G. Safeguarding cryptographic key[C]// AFIPS 1979 National Computer Conference. 1979:313-317.

[47] ASMUTH C,BLOOM J. A modular approach to key safeguarding[J]. IEEE Transactions on Information Theory,1983,29(2):208-210.

[48] PADRO C,SAEZ G,VILLAR J L. Detection of cheaters in vector space secret sharing schemes[J]. Designs,Codes and Cryptography,1999,16(1):75-85.

[49] KARNIN E D,GREENE J,HELLMAN M E. On secret sharing systems[J]. IEEE Transaction on Information Theory,1983,29(1):35-41.

[50] HE J,DAWSON E. Multistage secret sharing based on one-way function[J]. Electronics Letters,1994,30(19):1591-1592.

[51] HARN L. Comment:Multistage secret sharing based on one-way function[J]. Electronics Letters,1995,31(4):262.

[52] GENG Y J,GUO L Z,ZHEGN M H. Improved Multi-secret Sharing Scheme Based on One-Way Function[J]. TELKOMNIKA Indonesian Journal of Electrical Engineering,2014,12(6):4463-4467.

[53] LINKS N N,SIMMONS G J. A protocol to set up shared secret schemes without the assistance of a mutually trusted party[C]// Advances in Cryptology-EUROCRYPT'90. Springer-Verlag,1991:266-282.

[54] NAOR M,SHAMIR A. Visual Cryptography[C]// Advances in Cryptology-EUROCRYPT'94. 1995:1-12.

[55] HSU H C,CHEN T S,LIN Y H. The ringed shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing[C]// 2004 IEEE International Conference on Networking,Sensing and Control. 2004:996-1001.

[56] QIN S J, LIU T L, WEN Q Y. Quantum secret sharing based on entanglement swapping and local operation[J]. Journal of Beijing University of Posts and Telecommunications, 2005, 28(4): 74-77.

[57] SCHOENMAKERS B. A simple publicly verifiable secret sharing scheme and its application to electronic voting[C]// Annual International Cryptology Conference-CRYPTO'99. 1999: 148-164.

[58] IFTENE S. General secret sharing based on the Chinese Remainder Theorem with applications in e-voting[J]. Electronic Notes in Theoretical Computer Science, 2007, 186(1): 67-84.

[59] ZWIERKO A, KOTULSKI Z. A light-weight e-voting system with distributed trust[J] Electronic Notes in Theoretical Computer Science, 2007, 168: 109-126.

[60] CHEN Q M. Research on verifiable secret sharing based on Chinese Remainder Theorem[D]. Hefei: Hefei University of Technology, 2011.

[61] NAIR D G, BINUV P, KUMAR G S. An improved e-voting scheme using secret sharing based secure multi-party computation[C]// 8th International Conference on Communication Networks (ICCN-2014). 2014: 130-137.

[62] ZHAO Q Y, LIU Y N. E-voting scheme using secret sharing and K-anonymity[C] // International Conference on Broadband & Wireless Computing. 2017: 893-900.

[63] YUAN L F, LI M C, GUO C, et al. A verifiable e-voting scheme with secret sharing[J]. International Journal of Network Security, 2017, 19(2): 260-271.

[64] MIGNOTTE M. How to Share a Secret[C]// Proceedings of the Workshop on Crytography. Burg Feuerstein, Germany, 1983: 371-375.

[65] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms [J/OL]. Foundations of Secure Computation, 1978: 169-179. http://people.csail.mit.edu/rivest/RivestAdlemanDertouzos-OnDataBanksAndPrivacyHomomorphisms.pdf.

[66] GONG L M, LI S D, GUO Y. The development and applications of homomorphic encryption[J]. ZTE Technology Journal, 2016, 22(1): 26-29.

[67] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985, 31(4): 469-472.

[68] PAILLIER P. Public-key cryptosystems based on composite degree Residuosity Classes[C]// International Conference on the Theory and Application of Cryptographic Techniques in Cryptology-EUROCRYPT'99. 1999: 223-238.

[69] GOLDWASSER S, MICALI S. Probabilistic encryption [J]. Journal of Computer and System Sciences, 1984, 28(2): 270-299.

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

[71] DOMINGO-FERRER J. A provably secure additive and multiplicative privacy homomorphism. [C]// The 5th International Conference on Information Security. 2002: 471-483.

[72] MELCHOR C A, GABORIT P, HERRANZ J. Additively homomorphic encryption with d-operand multiplications[C]// Advances in Cryptology(CRYPTO'2010). 2010: 138-154.

[73] PLANTARD T, SUSILO W, ZHANG Z. Fully homomorphic encryption using hidden ideal lattice[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(12): 2127-2137.

[74] GARG S, GENTRY C, HALEVI S, et al. Attribute-based encryption for circuits from multilinear maps[J]. Computer Science, 2012, 45(6): 479-499.

[75] DAMGARD I, JURIK M. A generalisation, a simplification and some applications of Paillier's probabilistic public-key system [J]. Lecture Notes in Computer Science, 2000, 7(45): 119-136.

[76] DAMGARD I, GROTH J, SALOMONSEN G. The theory and implementation of an electronic voting system[M/OL]. Secure Electronic Voting. 2002: 77-99. http://www.instore.gr/evote/evote_end/htm/3public/doc3/public/crm/the_theory_and_implementation_of_an_electronic_voting_system.pdf.

[77] MENG B. A secure internet voting protocol based on non-interactive deniable authentication protocol and proof protocol that two ciphertexts are encryption of the same plaintext[J]. Journal of Networks, 2009, 4(5): 370-377.

[78] HAN W, ZHENG D, CHEN K F. A receipt-free punch-hole ballot electronic voting scheme[C]// The Third International IEEE Conference on Signal-Image Technologies and Internet-Based System. 2008.

[79] WAGN Y H, XU C, CHEN J W, et al. Scheme on secure voting system based on HElib[J]. Application Research of Computers, 2017, 34(7): 2167-2171.

[80] HE Q, SHEN W. Multi-candidate electronic voting scheme based on homomorphic encryption[J]. Computer Systems & Applications, 2019, 28(2): 146-151.

[81] Durette B W. Multiple Administrators for Electronic Voting[J/OL]. Bachelor's Thesis Mit, 1999. http://groups.csail.mit.edu/cis/theses/DuRette-bachelors.pdf.

PU Hong-quan, born in 1990, Ph.D. His main research interests include electronic voting and information security.

CUI Zhe, born in 1970, Ph.D, professor, doctoral supervisor. His main research intersts include pattern recognition and information security.