基于 HElib 的安全电子投票方案*

王永恒[1,2]，徐 晨[2†]，陈经纬[2]，吴文渊[2]
(1. 中国科学院大学，北京 100049；2. 中国科学院重庆绿色智能技术研究院 自动推理与认知重庆市重点实验室，重庆 400714)

摘 要：传统的电子投票应用中，若投票服务器管理方出现安全问题，投票过程中的匿名性、完整性和公开可验证性将难以保证。针对此问题，设计实现了一个基于全同态加密技术的电子投票方案。首先，基于全同态加密算法，结合 PKI 和数字签名技术设计了一个安全电子投票方案；然后针对电子投票的特殊性，基于 HElib 同态算法库设计了一个高效的同态密文加法器；最后在同态密文加法器的基础上，实现了安全电子投票系统。安全性方面，该投票方案有效地解决了电子投票中匿名性、完整性和公开可验证性的难题；而在性能上，测试表明该投票系统可以基本满足应用场景的使用需求。

关键词：同态加密；电子投票；数字签名；公开可验证；HElib
中图分类号：TP309.2 **文献标志码**：A **文章编号**：1001-3695(2017)07-2167-05
doi:10.3969/j.issn.1001-3695.2017.07.055

Scheme on secure voting system based on HElib

Wang Yongheng[1,2], Xu Chen[2†], Chen Jingwei[2], Wu Wenyuan[2]
(1. *University of Chinese Academy of Sciences, Beijing* 100049, *China*; 2. *Chongqing Key Laboratory of Automated Reasoning & Cognition, Chongqing Institute of Green & Intelligent Technology, Chinese Academy of Sciences, Chongqing* 400714, *China*)

Abstract: In traditional electronic voting applications, if malwares infected the voting server, the anonymity, integrity and public verifiability of voting process would be difficult to guarantee. To solve this problem, this paper designed and implemented a secure voting system based on HElib. First, this paper designed a secure electronic voting scheme which was based on full homomorphic encryption algorithm and combined with PKI, digital signature technology. Then according to the particularity of electronic voting, it designed an efficient ciphertext adder based on HElib homomorphic algorithm library. Finally it implemented a secure electronic voting system by making use of the ciphertext adder. The voting system effectively solves the electronic voting's anonymity, integrity and public verifiability problems in terms of security. Through the system tests, the voting system can basically meet the needs of application scenarios.

Key words: homomorphic encryption; electronic voting; digital signature; public verifiability; HElib

0 引言

投票选举是现代公民日常重要的政治活动。电子投票系统以密码学为基础，以数字的形式存储、发送、处理选票信息。相较于传统的手工计票，电子投票更有助于实现公平、公正、公开的选举要求，同时也可以节约人力物力成本。

自电子投票方案于 1981 年由 Chaum[1] 提出至今，现有的电子投票方案按照实现方法不同可以分为三类：基于混合网络(mix net)协议[2~4]的电子投票方案、基于盲签名[5,6]的电子投票方案和基于同态加密[7~9]技术的电子投票方案。混合网络从理论上可以实现解密计票的公开可验证性，但因为其算法的复杂性，当选举规模扩大时，需要进行大量的计算以满足零知识证明的要求，方案计算效率低下。基于盲签名的方案需要预设较强的假设，如匿名信道和可信签名方等。该方案拥有较好的计算效率，所以市面上已经实现的电子投票系统以盲签名方案为主。盲签名方案的缺点是要求投票的组织者、监督者、计票人完全可信，对投票参与者的安全要求性高；此外，盲签名方案中只有投票者可以验证自己的选票是否被计入，无法满足公开可验证的安全需求。

相较而言，同态加密技术可以对密文本身进行任意计算，适合解决电子投票应用中核心的安全与信任问题。文献[10]介绍了基于 ElGamal 的电子投票方案，文献[11]提出了基于 Paillier 的电子投票方案。ElGamal 和 Paillier 都是以幂计算实现同态的功能，不仅算法效率低下，而且选票数据量的规模也会呈指数增长，只能做有限次的加法运算。直到 2009 年，Gentry[12] 基于理想格构造了第一个全同态加密方案，掀起了全同态加密方案的研究热潮。在此基础上，2013 年 Gentry 和 Halevi 发布了同态加密开源库——HElib[13,14]。HElib 在 BGV 同态加密方案[15]的基础上，加入了密文更新[14]、自举电路[17]等功能，满足了全同态的加密要求。

针对投票应用的特殊性，本文提出了一个基于全同态加密

收稿日期：2016-05-20；**修回日期**：2016-07-15 **基金项目**：国家自然科学基金资助项目(11471307,11501540)；重庆市基础与前沿研究计划资助项目(cstc2015jcyjys40001)；中国科学院西部之光博士项目(2014 年)

作者简介：王永恒(1991-)，男，重庆涪陵人，硕士研究生，主要研究方向为信息安全、公钥密码学与同态加密；徐晨(1986-)，男(通信作者)，陕西西安人，助理工程师，硕士，主要研究方向为全同态加密、并行计算(xuchen@cigit.ac.cn)；陈经纬(1984-)，男，四川巴中人，助理研究员，博士，主要研究方向为计算机数学、信息安全；吴文渊(1976-)，男，四川成都人，副研究员，博士，主要研究方向为自动推理、符号数值混合计算.

技术的电子投票方案。同时在 HElib 的编程接口上,设计了一个高效的同态密文加法器,在该加法器的基础上实现了该投票系统。与盲签名方案相比,此系统即使将计票过程交给不可信的第三方进行,也能满足选票的匿名性、机密性和公开可验证性的安全要求。

1 基于 R-LWE 问题的全同态加密方案

2009 年至今,全同态加密技术经历了两代发展。第一代是基于 Gentry 所提出的理想格上的同态加密技术和 2013 年前后相继提出的基于整数的 DGHV 方案[18]、CAFED 方案[19,20]等,它们都使用了相似的构造原理和构造工具。第二代以 BGV 方案为代表,于 2014 年提出,是基于 LWE 或 R-LWE 问题所提出的构造方案[15,16]。与第一代方案相比,基于 LWE 困难问题的 BGV 方案拥有更高的运行效率,工程上也更容易实现。

本章介绍 LWE 和 R-LWE 困难问题,以及基于该困难问题构造同态加密方案的思路。

1.1 LWE 与 R-LWE 困难问题

LWE 困难问题(learning with errors, LWE)。设安全参数 λ,整数 $n=n(\lambda)$、$q=q(\lambda)\geqslant 2$、$\chi=\chi(\lambda)$ 为 $\mathbb{Z}$ 上的一个随机分布。随机选取 $a_i\leftarrow Z^n, b_i\leftarrow Z, s\leftarrow Z^n, e_i\leftarrow\chi$,则 $(a_i, b_i=a_is+e)_i$ 与随机均匀选取的 $(a_i,b_i)\leftarrow Z^n\times Z$ 是计算不可区分的。

R-LWE 困难问题(learning with errors over ring, R-LWE)。设安全参数 λ,$f(x)=x^n+1$,整数 $n=n(\lambda)$ 是 2 的幂,素数 $q=q(\lambda)\geqslant 2$,$R=Z[x]/f(x)$,$R_q=Z_q[x]/f(x)$,$\chi=\chi(\lambda)$ 为 R 上的一个随机分布,随机均匀选取 $a_i\leftarrow R_q, s\leftarrow R_q, e\leftarrow\chi$,则 $(a, b=as+e)$ 与随机均匀选取的 $(a,b)\leftarrow R_q\times R_q$ 是计算不可区分的。

1.2 基于 R-LWE 困难问题的 SWHE 方案的构造

基于 R-LWE 的困难设计可以构造出部分同态加密方案(somewhat homomorphic encryption, SWHE),它具有加法和乘法同态性质,但仅能够支持有限次的密文计算。

1)参数设置 params

n,2 的幂次,多项式环 $R=Z[x]/f(x)$,其中 $f(x)=x^n+1$。

q,素数,且满足条件 $q\equiv 1 \bmod 2n$,密文空间为 $R_q=Z_q[x]/f(x)$。

$t, t<q$,明文空间为 $R_t=Z_t[x]/f(x)$。

特别地,在 BVG 方案中,明文空间取 $R_t=Z_t[x]/\Phi_m(x)$,其中 $\Phi_m(x)$ 表示 m 阶分圆多项式。

σ,高斯分布 $\chi=D_{z^n,\sigma}$ 的标准差。

2)密钥生成算法

KeyGen(params)。从分布 χ 随机选取 $s\leftarrow\chi$,从密文空间 R_q 上均匀随机选取 $e\leftarrow\chi$,计算 $a_0=-(a_1s+te)$,其中公钥 $pk=(a_0,a_1)$,私钥 $sk=s$。

3)加密算法

Enc(pk, m)。从明文空间 R_t 中选取 $m\leftarrow R_t$,从分布 χ 均匀随机选取三个样本 $u\leftarrow\chi, r\leftarrow, g\leftarrow\chi$,利用公钥计算出同态密文:

$$\mathrm{Enc}(pk,m)=ct=(c_0,c_1)=(a_0u+tr+m, a_1u+tg)$$

4)解密算法

Dec(sk, ct)。利用私钥 $sk=s$,解密密文 ct。计算公式为:$\mathrm{Dec}(sk,ct)=m'=(c_0+c_1s) \bmod q \bmod t$。

当密文多维时,密文 $ct=(c_0,c_1,\cdots,c_\xi)\in(R_q)^{\xi+1}$,私钥向量变为 $sk=(1,s,s^2,\cdots,s^\xi)$,解密计算公式为

$$\mathrm{Dec}(sk,ct)=m'=\sum_{i=0}^{\xi}c_is^i \bmod q \bmod t$$

5)同态加法

EvalAdd(ct, ct')。对多维密文 $ct=(c_0,c_1,\cdots,c_\gamma)$ 与 $ct'=(c'_0,c'_1,\cdots,c')$ 进行同态加法,即向量的对应分量相加,分量长度不足时,高位补 0,最后得到同态密文和为 $ct_{\mathrm{add}}=ct+ct'=(c_0+c'_0, c_1+c'_1, \cdots, c_{\max(\gamma,\eta)}+c'_{\max(\gamma,\eta)})$,则有 $ct_{\mathrm{add}}\in(R_d)^{\max(\gamma,\eta)+1}$。

6)同态乘法

EvalMult(ct, ct')。对多维密文 $ct=(c_0,c_1,\cdots,c_\gamma)$ 与 $ct'=(c'_0,c'_1,\cdots,c')$ 进行同态乘法,$ct_{\mathrm{mult}}=ct\times ct'$ 计算方式如下:引入变量 v,则有 $\sum_{i=0}^{\gamma}c_iv^i$、$\sum_{i=0}^{\eta}c'_iv^i$ 分别为关于变量 v 的一元多项式。令两个多项式相乘,则有 $\sum_{i=0}^{\gamma+\eta}\hat{c}v^i=\sum_{i=0}^{\gamma}c_iv^i\times\sum_{i=0}^{\eta}c'_iv^i$,比较对应项系数,求解 $\hat{c}_0,\cdots,\hat{c}_{\gamma+\eta}\in R_q$,则 $ct_{\mathrm{mult}}=ct\times ct'=(\hat{c}_0,\cdots,\hat{c}_{\gamma+\eta})$。

1.3 SWHE 方案到 FHE 方案

在电子投票应用中,需要进行大量的密文加法和乘法的操作,1.2 节所设计的部分同态加密方案将不能满足该场景的应用需求。利用密钥转换、模转换技术可以实现部分同态加密到全同态加密(fully homomorphic encryption, FHE)的转换。密钥交换技术[14]将由密文乘积 ct_{mult} 和对应的私钥 sk' 转换为另外一个与 sk 维度相同的密钥 sk'' 和新的密文 ct''_{mult},以此达到减少密文和密钥维度的目的;模交换技术[15]利用一个递减的模序列 q_i,将 ct_{mult} 的模计算的 q 转换为 $q_i=q/x^i$,使噪声的增长得到了有效控制。

2 同态密文加法计票器

本章主要介绍同态密文加法计票器的设计过程。在投票应用中,单张选票生成时,对一个候选人只有“选”与“不选”两种情况,可以使用包含 1 bit 明文信息的密文来表示。而计票时,可以使用单比特加法器将所有选票密文加总起来。由于将同态加密的明文空间信息缩减到 1 bit,可以减少密文生成和相加的计算时间,本章将介绍单比特加法器原理以及同态密文加法器的设计。

2.1 单比特半加器原理

单比特半加器用于将两个单比特二进制数进行加法计算,输出两个单比特二进制数,其中一个表示结果,另一个表示进位。半加器用于加法器的最低位,为全加器生成最初的进位信号。

单比特半加器的逻辑运算过程如下:

输入:两个单比特二进制数 A、B。

输入:两个单比特二进制数 S、C。其中 S 为计算结果,C 为进位符。

计算:$S=A\oplus B$

$C=A\otimes B$

其中:$\oplus$ 表示异或运算,$\otimes$ 表示与运算。

2.2 同态密文加法计票器的设计

从单比特加法器的原理可以看出,对于仅包含 1 bit 明文的同态密文,使用同态加法和同态乘法就可以实现异或运算和与运算,进而利用同态密文的特性实现加法器单比特同态密文加法器。此时,对 BVG 方案,令 $t=2$,得到明文空间为 $R_2=$

$Z_2[x]/f(x)$,同时得到对应的密文空间为 $R_q = Z_q[x]/f(x)$。此时,同态密文和明文有如下性质:

若明文 $p_1(x), p_2(x) \in R_2$ 对应的同态密文 $c_1(x), c_2(x) \in R_q$,则有

$$p_1(x) \oplus p_2(x) = \mathrm{dec}(c_1(x) + c_2(x))$$
$$p_1(x) \otimes p_2(x) = \mathrm{dec}(c_1(x) \times c_2(x))$$

根据以上性质,同态密文加法计票器的设计思路如下:

a)将整型数据转换为二进制数据,按位转化为明文空间 R_2 的明文数据并装入明文向量。

b)对明文向量逐个进行加密,将密文装入密文向量。

c)使用模 2 的同态加法和乘法替代加法器的门电路。

d)使用同态密文半加器串联,其中最低位接收新的选票密文作为输入。

对同态密文半加器,其逻辑运算过程如下:

输入:设包含 1 bit 信息的明文 $p_1(x), p_2(x) \in R_2$ 对应的同态密文 $c_1(x), c_2(x) \in R_q$;设半加器的输入 $\tilde{A} = c_1(x), \tilde{B} = c_2(x)$。

输出:使用同态加法得到密文和 $\tilde{S} = \tilde{A} + \tilde{B}$,使用同态乘法得到进位信号 $\tilde{C} = \tilde{A} \times \tilde{B}$。

记0、1为 1 bit 的 0、1 进行同态加密后的密文,得到同态密文半加器的真值表,如表 1 所示。

表 1　同态密文半加器的真值表

输入		输出	
$\tilde{A}$	$\tilde{B}$	$S = \mathrm{dec}(\tilde{S})$	$C = \mathrm{dec}(\tilde{C})$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

如图 1 所示,将多个同态密文半加器进行串联,可以得到同态密文加法计票器。

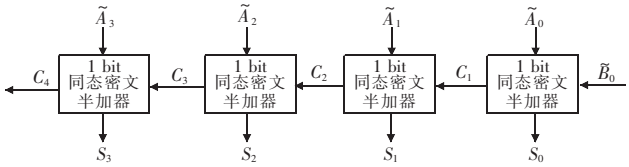

图 1　同态密文加法计票器

3　基于全同态加密的电子投票方案

本章主要介绍基于 2.2 节的密文加法计票器的全同态加密的电子投票方案的设计;此外,还介绍了该方案中各个功能角色的构成和交互关系。

3.1　方案描述

记 μ 个候选人为 $O_1, O_2, \cdots, O_\mu$,ω 个投票人为 $V_1, V_2, \cdots, V_\omega$。$C_\varepsilon^{V_\gamma}$ 表示投票人 V_γ 对于候选人 O_ε 选择情况,其中 $O_\varepsilon^{V_\gamma} \in \{0,1\}$ 且 $\varepsilon \in [1,\mu], \gamma \in [1,\omega]$。PKI 作为可信第三方,负责签发数字证书,确保各实体的真实性。选举发起人 H 负责生成同态公钥 pk 和私钥 sk,计票人 A 负责选票的甄别和统计。方案的运行流程如下。

1)系统初始化

PKI 系统对每个参与者进行身份认证,签发数字证书。将证书存储于目录数据库中,任何人都可以查验。

记投票人 V_i 的公钥为 PK_{V_i},私钥为 $SK_{V_i}, i \in [1,\omega]$;计票人 A 的公钥为 PK_A,私钥为 SK_A;投票发起人 H 的公钥为 PK_H,私钥为 SK_H。投票发起人将生成的同态公钥 pk 和 $\mathrm{sign}_{SK_\mathrm{H}}(H(pk))$公开,其中 $\mathrm{sign}_{SK_\mathrm{H}}(H(pk))$表示将 pk 的 hash 值使用 H 的私钥进行数字签名。

2)选票生成与投票

以投票人 V_i 为例,决定所选择的候选人 O_ε 以后,投票人会生成明文序列 $m_{V_i} = (O_1^{V_i}, O_2^{V_i}, \cdots, O_\varepsilon^{V_i}, \cdots, O_\mu^{V_i})$,其中令 $O_\varepsilon^{V_i}$,为 1,其他元素为 0。使用公钥 pk 对 m_{V_i}逐个元素进行同态加密操作,得到密文序列 $c_{V_i} = (C_1^{V_i}, C_2^{V_i}, \cdots, C_\mu^{V_i})$,其中 $C_\mu^{V_i} \in R_q = Z_q[x]/f(x)$。投票人 V_i 将身份标志 ID_{V_i}、密文序列 c_{v_i}和时间戳 time 进行数字签名,得到 $\mathrm{sign}_{SK_{V_i}}(H(c_{V_i} \| \mathrm{ID}_{V_i} \| \mathrm{time}))$。将 ID_{V_i}、c_{V_i}、time 和签名数据发送给计票人 A。

计票人 A 首先验证签名的合法性,通过验证后将 ID_{V_i}、c_{V_i}和 time 保存,而后使用自己的私钥 SK_A 计算签名 $\mathrm{sign}_{SK_\mathrm{A}}(H(c_{V_i} \| \mathrm{ID}_{V_i} \| \mathrm{time}))$发送给投票人 V_i。该签名作为投票回执由投票人 V_i 保存。

最后,为了使投票过程并行化,计票人将准备一个可以同时写入选票数据的选票缓冲池,不同投票终端可同时向缓冲池放入新的选票信息 c_{V_i},以便在后续的计票过程进行逐一的加总。

3)公开选票

计票人 A 将由投票人 V_i 发送的 ID_{V_i}、c_{V_i}和 time 以及 $\mathrm{sign}_{SK_{V_i}}(H(c_{V_i} \| \mathrm{ID}_{V_i} \| \mathrm{time}))$放入公告牌,以供任意人员验证。

4)计票与验票

在计票过程中,计票人 A 首先为每个候选人初始化一个同态密文加法计票器,然后从选票缓冲池中提取一张选票信息 c_{V_i},并将其从缓冲池中删去。以候选人 O_ε 为例,假设使用 32 bit 计票器,用同态公钥 pk 计算 $\mathrm{Enc}_{\mathrm{pk}}(0)$,作为初始值逐个装入密文向量 $\boldsymbol{S}_\varepsilon = (S_0, S_1, \cdots, S_{31})$。每当收到选票密文序列 c_V 后,取出序列中 C_ε^V 作为计票器最低位的 $\tilde{B}$ 输入,密文向量 $\boldsymbol{S}_\varepsilon$ 中的对应元素作为同态密文半加器的 $\tilde{A}$ 输入位。然后运行一次计票器,可以更新密文向量 $\boldsymbol{S}_\varepsilon$,完成 O_ε 候选人同态密文的计票工作。每张选票会更新所有候选人密文向量的内容。

投票结束后,计票人 A 完成对选票缓冲池所有选票密文的加总,而后公布每个候选人的密文向量 $\boldsymbol{S}$,同时将对应的签名 $\mathrm{sign}_{SK_\mathrm{A}}(H(S))$放入公告牌。投票发起人 H 验证签名无误后,将密文向量 $\boldsymbol{S}$ 解密,得到二进制的计票数据,从而获得投票结果。

3.2　方案功能角色

根据 3.1 节提出的方案,基于全同态加密的电子投票系统由 PKI、发起人、计票人、投票人、公告牌等六个主要的功能角色构成。图 2 为系统的整体结构图。

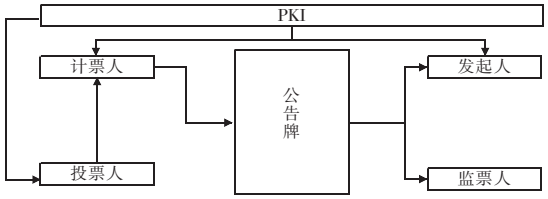

图 2　系统整体结构图

图 2 展示了各个功能角色的关系,除了 PKI 和发起人,其

余四个角色均可交给不可信的实体运行。公告牌满足了选举公平公开的要求,而监票人对选举过程和结果进行有效监督,防止计票人造假。

4 方案安全性分析

利用基于 2.2 节所设计的同态密文加法器计票器和 3.1 节所提出的全同态加密的电子投票方案,电子投票系统可以有效抵御对系统完整性、匿名性和公开可验证性的攻击。

以 3.2 节介绍的系统功能角色为基础,为方便讨论,设 Alice为投票人,Bob 为计票人,Carol 为投票发起人,Victor 为监票人,Eve 为攻击者,并假设 Eve 可以完全获得并更改 Bob 的所有数据。本章将介绍 Eve 试图破坏投票流程的完整性、匿名性和公开可验证性时,系统如何进行安全保护。

4.1 完整性的安全保护

Eve 可以从如下几个方面对投票过程的完整性进行攻击:更改 Alice 发给 Bob 的选票信息;更改公告牌上公示的选票信息;收到选票后,操纵 Bob 收到选票后不计票。下面介绍方案如何防护这些攻击手段。

a) Eve 更改 Alice 发给 Bob 选票信息。以 Alice 为例,Alice 将身份标志 ID_A、选票密文 c_A 和时间戳 time 进行数字签名 $sign_{SK_A}(H(c_A \parallel ID_A \parallel time))$。Eve 可以更改该选票的 ID_A 和 c_A 信息,但因为没有 Alice 的私钥,无法构造出新的数字签名,所以更改可以被 Bob 发现。即使 Bob 被 Eve 控制接收了选票,在公告牌进行选票公示时,也会因为数字签名不符而被 Victor 发现。

b) Eve 更改公告牌上公示的选票信息。在公告牌上,Eve 对每一个公示的选票的更改可以被 Victor 用数字签名发现。若 Eve 更改了最后加总的密文向量 S,因为 Bob 会使用自己的私钥生成签名 $sign_{SK_B}(H(S))$,Eve 的更改也能被 Victor 发现。若 Bob 被 Eve 控制,同时更改了密文向量 S 和 $sign_{SK_B}(H(S))$,Victor 也能重新计算密文向量 S',比较 S 和 S',进而发现密文被修改。

c) Eve 操纵 Bob 收到选票后不计票。Alice 投票以后,会收到使用 Bob 签名的 $sign_{SK_A}(H(c_A \parallel ID_A \parallel time))$ 作为回执。若 Eve 操纵 Bob 收到选票后不计票,公告牌将没有 Alice 的相关选票信息,Alice 可以持回执进行申述。

4.2 匿名性的安全保护

Alice 会生成明文序列 m_A,从 PKI 处获得同态加密公钥 pk 并对 m_A 逐个元素进行同态加密操作,从而得到密文序列 c_A 发给 Bob。Bob 进行计票以及 Victor 进行监票时,都只能看到密文 c_A,只有拥有同态加密私钥的 Carol 才能读到选票信息,从而确保了投票的匿名性。

4.3 公开可验证性的安全保护

Bob 将从 Alice 处获得的选票信息 ID_A、c_A、time 和 $sign_{SK_A}(H(c_A \parallel ID_A \parallel time)$ 放入公告牌公示,任何人都可以通过 Alice 的公钥检查选票的合法性。而 Victor 进行监票工作所需的所有信息都是公开的,任何人都可以充当 Victor 角色,对选举过程和最后所得的密文向量 S 进行验证。

5 性能测试

1 024 bit RSA 算法是目前最流行的公钥加密算法,而基于 HElib 的同态密文加法器拥有 RSA 算法同样的公钥加密功能,此外还可以支持密文的加法。为了测试投票系统加解密运算的效率,本文选择 1 024 bit RSA 和同态密文加法器对同样的明文进行加解密操作,比较二者的计算时间和所需的空间。由于1 024 bit RSA不支持密文加法,本文仅测试本投票系统的密文加法效率,并增加计算规模来分析其扩展性。

5.1 实验平台与参数

实验平台使用 Intel Core i7-4710MQ 2.50 GHz 的 CPU,12 GB 内存,运行 CentOS 6.6 的 64 位操作系统;同态密文加法计票器使用 gcc 4.4.7 进行编译。

加法器每次仅使用 1bit 明文信息,所以选取明文槽数目为 1。加法器使用 32 个同态密文半加器串联,支持最大 32 位的密文加法;而用作对比测试的 RSA 算法使用 OpenSSL 开源库编程实现。所加密的数据是包含 1 bit 明文数据的选票信息。

5.2 实验结果

表 2、3 为同态密文加法器和 1 024 bit RSA 算法运行效率的比较,二者所加密的信息均为 1 bit 的明文选票信息,即 0 或 1。比较二者运行时间还给出了加解密所需的平均时间,表 2 为运行时间的比较,表 3 为文件大小的比较。

表 2 同态密文加法器与 1 024 bit RSA 运行时间比较

测试项目	同态密文加法器耗时/ms	1 024 bit RSA 耗时/ms
密钥生成	13	80
公钥加密	31	8
私钥解密	11	10

表 3 同态密文加法器与 1 024 bit RSA 文件大小比较

生成文件	同态密文加法器文件大小/Byte	1 024 bit RSA 文件大小/Byte
公钥	6 658	272
私钥	7 515	891
密文	1 347	128

实验结果表明,对于生成的密文和密钥,加法器的公私钥文件为 6.6 KB 和 7.5 KB,密文文件为 1.3 KB,大于 1 024 bit RSA 算法所使用的密钥和密文。而在加解密算法的运行时间上,同态密文加法计票器在加解密的运行效率已经接近 RSA 算法。

同态密文加法计票器可以进行选票密文加法,表 4 为加法器进行不同次数的加法所花费的时间。

表 4 同态密文加法器密文加法运算时间比较

加法次数	同态密文加法器耗时/s
1	0.27
10	2.73
100	25.19
1 000	253.33

实验结果表明,每次运行密文加法耗时 0.27 s,并随着加法次数的增加,加法器所耗时间呈线性增长。以 1 000 人规模投票应用为例,系统可以在 5 min 内获得投票结果,可以基本满足该场景的应用需求。

6 结束语

本文使用 BGV 方案,利用 HElib 开源库设计并实现了基于全同态加密的电子投票系统。与现有的电子投票系统相比,该系统可以有效解决投票过程的匿名性和公开可验证性的难

题,从而防止计票人作弊。此外,针对该特殊的应用场景,借助 HElib 的编程接口,设计实现了同态密文加法计票器。测试表明,该加法器会产生较大的密文和密钥数据,但是加解密运算速度接近 RSA 算法,能够达到实用要求。

参考文献:

[1] Chaum D L. Untraceable electronic mail, return addresses, and digital pseudonyms[J]. Communications of the ACM, 1981, 24(2): 84-90.

[2] Park C, Itoh K, Kurosawa K. Efficient anonymous channel and all/nothing election scheme[C]//Advances in Cryptology. Berlin: Springer, 1993: 248-259.

[3] Golle P, Zhong Sheng, Boneh D, *et al*. Optimistic mixing for exit-polls [C]//Advances in Cryptology. Berlin: Springer. 2002: 451-465.

[4] Jakobsson M. Flash mixing[C]//Proc of the 18th annual ACM Symposium on Principles of Distributed Computing. New York: ACM Press, 1999: 83-89.

[5] Fujioka A, Okamoto T, Ohta K. A practical secret voting scheme for large scale elections[C]//Advances in Cryptology. London: Springer-Verlag, 1992: 244-251.

[6] Chen T S, Liu T P, Chung Y F. A proxy-protected proxy signature scheme based on elliptic curve cryptosystem[C]//Proc of IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering. 2002: 184-187.

[7] 张鹏,喻建平,刘宏伟. 同态签密方案及其在电子投票中的应用[J]. 深圳大学学报:理工版, 2011, 28(6): 489-94.

[8] Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978, 4(11): 169-180.

[9] Boneh D, Goh E J, Nissim K. Evaluating 2-DNF formulas on ciphertexts[C]//Proc of the 2nd International Conference on Theory of Cryptography. Berlin: Springer, 2005: 325-341.

[10] Cramer R, Gennaro R, Schoenmakers B. A secure and optimally efficient multi-authority election scheme [J]. European Trans on Telecommunications, 1997, 8(5): 481-90.

[11] Baudron O, Fouque P A, Pointcheval D, *et al*. Practical multi-candidate election system[C]//Proc of the 20th Annual ACM Symposium on Principles of Distributed Computing. New York: ACM Press, 2001: 274-283.

[12] Gentry C. Fully homomorphic encryption using ideal lattices[C]//Proc of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 169-178.

[13] Kocabas O, Soyata T. Utilizing homomorphic encryption to implement secure and private medical cloud computing[C]//Proc of the 8th IEEE International Conference on Cloud Computing. 2015: 540-547.

[14] Halevi S, Shoup V. Algorithms in Helib[C]//Advances in Cryptology. Berlin: Springer, 2014: 554-571.

[15] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE [J]. SIAM Journal on Computing, 2014, 43(2): 831-871.

[16] Dos Santos L C, Bilar G R, Pereira F D. Implementation of the fully homomorphic encryption scheme over integers with shorter keys[C]//Proc of the 7th International Conference on New Technologies, Mobility and Security. 2015: 1-5.

[17] Halevi S, Shoup V. Bootstrapping for Helib[C]//Advances in Cryptology. Berlin: Springer, 2015: 641-670.

[18] Cheon J H, Coron J S, Kim J, *et al*. Batch fully homomorphic encryption over the integers[C]//Advances in Cryptology. Berlin: Springer, 2013: 315-335.

[19] Gentry C. Computing arbitrary functions of encrypted data[J]. Communications of the ACM, 2010, 53(3): 97-100.

[20] Li Lang, Yu Xiaozhong, Yang Yaqiong. Compact CAFED fully homomorphic encryption scheme[C]//Proc of the 4th International Conference on Information Science and Cloud Computing. 2015: 1-8.

(上接第　页)提高了 CL-PKE 的安全性。本文 a)给出了 CL-PKIE 体制的形式化定义,然后给出了新体制的安全模型;b)给出了 CL-PKIE 体制的具体的方案;c)给出了在随机预言机模型里 CL-PKIE 的 IND-CCA2 安全性证明。

参考文献:

[1] Diffie W, Hellman M E. New directions in cryptography[J]. IEEE Trans on Information Theory, 1976, 22(6): 644-654.

[2] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems [J]. Communications of the ACM, 1983, 26(1): 96-99.

[3] Shamir A. Identity-based cryptosystems and signature schemes[C]//Advances in Cryptology. Springer, 1984.

[4] Al-Riyami S S, Paterson K G. Certificateless public key cryptography [C]//Advances in Cryptology. Berlin: Springer, 2003: 452-473.

[5] Hanaoka G, Hanaoka Y, Imai H. Parallel key-insulated public key encryption[C]//Public Key Cryptography-PKC. Berlin: Springer, 2006: 105-122.

[6] Boneh D, Franklin M K. Identity-based encryption from the Weil pairing[C]//Advances in Cryptology. London: Springer-Verlag, 2001: 213-229.

[7] Waters B. Efficient identity-based encryption without random oracles [C]//Advances in Cryptology. Berlin: Springer, 2005: 114-127.

[8] Gentry C. Practical identity-based encryption without random oracles [C]//Advances in Cryptology. Berlin: Springer, 2006: 445-464.

[9] Boneh D, Boyen X. Secure identity based encryption without random oracles[C]//Advances in Cryptology. Berlin: Springer, 2004: 443-459.

[10] Horwitz J, Lynn B. Toward hierarchical identity-based encryption [C]//Advances in Cryptology. Berlin: Springer, 2002: 466-481.

[11] Weng Jian, Liu Shengli, Chen Kefei, *et al*. Identity-based parallel key-insulated encryption without random oracles: security notions and construction[C]//Progress in Cryptology. Berlin: Springer, 2006: 409-423.

[12] Libert B, Quisquater J, Yung M. Parallel key-insulated public key encryption without random oracles[C]//Public Key Cryptography. Berlin: Heidelberg, 2007: 298-314.

[13] Hanaoka G, Weng Jian. Generic constructions of parallel key-insulated encryption[C]//Security and Cryptography for Networks. Berlin: Springer, 2010: 36-53.

[14] Wang Xu'an, Weng Jian, Yang Xiaoyuan, *et al*. Cryptanalysis of an (hierarchical) identity based parallel key-insulated encryption scheme[J]. Journal of Systems and Software, 2011, 84(2): 219-225.

[15] Ren Yanli, Wang Shuozhong, Zhang Xinpeng. Practical parallel key-insulated encryption with multiple helper keys[J]. Computers & Mathematics with Applications, 2013, 65(9): 1403-1412.