Advances in Applied Mathematics 应用数学进展, 2022, 11(10), 7026-7032
Published Online October 2022 in Hans. http://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2022.1110745

Hans汉斯

基于全同态加密电子投票方案的研究

胡飞龙，何明翰，马广贞，张　健，张　平*

河南科技大学，数学与统计学院，河南　洛阳

收稿日期：2022年9月12日；录用日期：2022年10月2日；发布日期：2022年10月12日

摘　要

本文提出了一种能够进行任意次加乘运算的基于无噪声的全同态加密算法，以及椭圆曲线数字签名算法等技术来实现安全的电子投票方案，并给出了方案的安全性分析。该方案较好地解决了电子投票中的匿名性、完整性和公开可验证性难题，实现了安全、公开、公平和公正的电子投票。

关键词

全同态加密，电子投票，椭圆曲线，数字签名，无噪声

Research Based on Fully Homomorphic Encrypted Electronic Voting Scheme

Feilong Hu, Minghan He, Guangzhen Ma, Jiang Zhang, Ping Zhang*

School of Mathematics and Statistics, Henan University of Science and Technology, Luoyang Henan

Received: Sep. 12th, 2022; accepted: Oct. 2nd, 2022; published: Oct. 12th, 2022

Abstract

This paper proposes a noise-free fully homomorphic encryption algorithm capable of performing arbitrary multiplication operations, and an elliptic curve digital signature algorithm to implement a secure e-voting scheme, and gives a security analysis of the scheme. The scheme solves the problems of anonymity, integrity and public verifiability in e-voting, and achieves secure, open, fair and just e-voting.

Keywords

Fully Homomorphic Encryption, Electronic Voting, Elliptic Curve, Digital Signature, Without Noise

*通讯作者。

文章引用: 胡飞龙, 何明翰, 马广贞, 张健, 张平. 基于全同态加密电子投票方案的研究[J]. 应用数学进展, 2022, 11(10): 7026-7032. DOI: 10.12677/aam.2022.1110745

1. 引言

随着电子商务、电子选举、电子货币的普及，人们对公开网络所传输数据的安全性提出了更高要求，于是，全同态加密走进了人们的视野[1]。同态加密最早是由 Rivest [2]三人提出的，即在不知道加密密钥的情况下，对密文进行计算，其结果与明文作相同计算的结果相同。40 多年以来，人们提出的加密方案大多只满足加法同态或乘法同态，同时还有一些能够同时满足有限次加法与乘法的同态方案。直到 2009 年，由 Gentry 等人才构造出第一个真正意义上的全同态加密方案[3] [4]。在此文中，构造了一个可实现有限次同态计算的 Some What 方案，通过同态解密来实现密文的更新，从而实现全同态加密。但缺点是同态解密的效率低，复杂度相对较高[5] [6]。

近年来，人们基于 Gentry 的方案产生了许多全同态加密方案及优化。Dijk 等人提出了基于整数的全同态加密方案，称为 DGHV 方案，其完全基于整数上的算术运算，概念简单，易于理解，但缺点是计算复杂并且易受噪声的干扰[7]。于是本文从另外一个方面考虑，提出了一个没有噪声的全同态加密方案，该方案概念简单、易于理解，计算易于实现且不会受噪声干扰。

本文针对计票过程中存在的安全问题，面向中大型投票场景，综合采用全同态加密(FHE)、数字签名，设计实现了一个具有更高安全性保障的电子投票系统，并在保证安全的前提下，尽可能地提高了系统的性能[8] [9] [10]。针对电子投票中存在的问题，引入了椭圆曲线数字签名算法，签名速度更快，更适用于电子投票场景，能更好地解决电子投票中的身份认证问题。从初始化、注册投票、计票和验证查票四个阶段详细阐述了电子投票方案的具体流程。

2. 相关算法

2.1. 无噪声的全同态加密方案

2.1.1. 算法描述

目前提出的方案在进行同态运算时会受到噪声的干扰，这会影响运算速度，在大数据和云计算的环境下有很大的局限性，本文基于文献[8]在没有噪声的全同态加密基础上，提出了一个改进的无噪声全同态加密方案，提高了计算效率和安全性。

2.1.2. 具体方案

1) KeyGen：p 和 q 是两个比较大的素数且占 λ bits ($\lambda = 512$)，h 是一个小的正数($h \geq 2$)，令 $N = pq$，其中 h 和 N 是公开的，p 和 q 是保密的。

h 的约束条件：

初始化一个计数器和计时器，用来记录加密的次数和密钥的有效周期。

① 加密的次数小于 h，则不用更新密钥 K；

② 加密 $h-1$ 次后，重新分配密钥 $K_1\left(K_1 \neq K\right)$；

③ 密钥 K 在一个有效周期内最多允许加密 $h-1$ 次，完成 $h-1$ 次加密后，则立即更新密钥 K，并重新计时；

④ 当需要加密的次数为 $Y\left(Y > h\right)$ 次时，则密钥 K 可以变为 $\left(x_1, x_2, \cdots, x_{h_1}\right)$ $\left(h_1 > Y\right)$。

明文的集合是$\mathbb{Z}_p$，故所有加法或乘法的结果始终是集合$\{0,1,\cdots,p-1\}$中的整数，又因为$N=pq$，p是保密的，故在进行操作时，可直接对N取模。

密文的集合是有限的向量空间$\mathbb{Z}_p^h$，故所有的密文形式为$(\alpha_1,\alpha_2,\cdots,\alpha_h)$，且$\forall i\in(1,2,\cdots,h)$，$h\alpha_i\in\mathbb{Z}_N\cdot\mathbb{Z}_N^h$。密钥$K=(x_1,x_2,\cdots,x_h)\in\mathbb{Z}_N^h$。

2) Enc：生成明文$m\in Z_N$对应密文的过程如下

① 通过随机生成h个在0到$N-1$之间的数，生成向量$C=(\alpha_1,\alpha_2,\cdots,\alpha_h)\in\mathbb{Z}_N^h$；

② 令$m_1=\sum_{i=1}^{h}x_i\cdot\alpha_i$；

③ 若$m_1=m$则输出C作为m的密文；

④ 若$m_1\neq m$则随机选取一个$j\in[1,h]$要求$x_j\neq 0$，用$\alpha_j+(m-m_1)x_j^{-1}$替换C中α_j，其中$x_j^{-1}\cdot x_j=1$。那么$m_2=\sum_{i=1}^{h}x_i\cdot\alpha_i'$等于$m$即新的$C$为有效加密。

3) Dec：给定任意一个密文C和对应的私钥$K=(x_1,x_2,\cdots,x_h)$

① 解密函数$\Phi(x)=\sum_{i=1}^{h}x_i\cdot\alpha_i$的结果即为相应明文。

② 若加密次数小于h，则直接应用解密函数。若加密次数不小于h，则对前$h-1$次、h至$2h-2$次…分别应用解密函数。

4) Eval：给定一个希望对密文进行操作的函数和需要处理的密文，将个密文输入到函数中执行同态运算，输出密文c。函数可分解成加法和乘法的组合，对于两个密文c_1和c_2来说，同态加法和同态乘法的表示如下：

同态加法：$c_{add}=(c_1+c_2)\bmod N$；同态乘法：$c_{mul}=(c_1\cdot c_2)\bmod N$。

2.1.3. 同态性

将任意两个密文A和B之间的二元关系$\approx$定义如下：$A\approx B\Leftrightarrow D(A)=D(B)$

(加法同态)令$a=(\alpha_1,\alpha_2,\cdots,\alpha_h)$，$b=(\beta_1,\beta_2,\cdots,\beta_h)$是密文，也即是$\sum_{i=1}^{h}x_i\alpha_i=a$，$\sum_{i=1}^{h}x_i\beta_i=b$；那么既有如下所得：

$$\begin{aligned}D(\varepsilon(a)+\varepsilon(b))&=D((\alpha_1,\alpha_2,\cdots,\alpha_h)+(\beta_1,\beta_2,\cdots,\beta_h))\\&=D((\alpha_1+\beta_1),(\alpha_2+\beta_2),\cdots,(\alpha_h+\beta_h))\\&=\sum_{i=1}^{h}x_i(\alpha_i+\beta_i)=\sum_{i=1}^{h}x_i\cdot\alpha_i+\sum_{i=1}^{h}x_i\cdot\beta_i\\&=a+b=D(\varepsilon(a+b))\end{aligned}$$

所以$\varepsilon(a)+\varepsilon(b)\approx\varepsilon(a+b)$。

(乘法同态)

$$\begin{aligned}E(a)\times E(b)&=(\alpha_1,\alpha_2,\cdots,\alpha_h)\times(\beta_1,\beta_2,\cdots,\beta_h)\\&=\sum_{1\le i,j\le h}(\alpha_i\cdot\beta_j)E(x_i\cdot x_j)\\&\approx\sum_{1\le i,j\le h}E(\alpha_i\cdot\beta_j\cdot x_i\cdot x_j)\\&\approx E\left(\sum_{1\le i,j\le h}\left(\sum_{0\le i,j\le N-1}\alpha_i\cdot\beta_j\cdot x_i\cdot x_j\right)\right)\end{aligned}$$

$$\approx E\left(\sum_{1\le i,j\le h}\alpha_i\cdot x_i\cdot\left(\sum_{0\le i,j\le N-1}\beta_j\cdot x_j\right)\right)$$
$$\approx E\left(\sum_{1\le i,j\le h}\alpha_i\cdot x_i\cdot b\right)$$
$$\approx E\left(\left(\sum_{1\le i,j\le h}\alpha_i\cdot x_i\right)\cdot b\right)$$
$$= E(a\cdot b)$$

2.1.4. 正确性证明

对于任意给定的 $m\in Z_N$ 输出密文 $\varepsilon(m)$ 都有 $D(\varepsilon(m))=m$ 成立，通过定义 $\varepsilon(m)$ 可以输出任何密文 $C=(\alpha_1,\alpha_2,\cdots,\alpha_h)\in Z_N^h$ 使得 $\sum_{i=1}^{h}x_i\cdot\alpha_i=m$ C 被输出也就意味 $\varepsilon(m)=C$。因此，有

$$D(\varepsilon(m))=D(C)=D(\alpha_1,\alpha_2,\cdots,\alpha_h)=\sum_{i=1}^{h}x_i\cdot\alpha_i=m$$

2.1.5. 安全性证明

本文的安全性可以规约到的大数分解问题。

大数分解困难性分析：设 p,q 分别是编码在 λ 上的素数，$n=pq$。欧拉函数 $\psi(n)$ 表示不大于 n 且与 n 互素的正整数个数。当 n 是素数，则有 $\psi(n)=n-1$ 则有 $\psi(n)=\psi(p)\psi(q)=(p-1)(q-1)$。

由费马定理，若 p 是素数，数 a 与 p 互素，则 $a\wedge\psi(p)\equiv1(\mathrm{mod}\,p)$。那么，将 N 分解为素数 p，q 乘积的过程就是求解 $a\wedge\psi(N)\equiv1(\mathrm{mod}\,N)$，我们知道 $\psi(n)=(p-1)(q-1)$，则有 $a\wedge(q-1)(p-1)\equiv1(\mathrm{mod}\,N)$。容易看出，上一等式求解规模随 p,q 的增大成指数级别增加，而目前不能在多项式时间内求解出该问题。例如对十进制五十位的大数进行分解也需要 10 的 11 次方年，故而该问题目前仍是困难的。

引理 1：任意随机 h 个密文几乎可以表示为 h 个独立的方程

证明：概率 $P=\prod_{i=1}^{h}\left(1-N^{(i-h-1)}\right)$ 式子可知

随着 N 的增大，P 迅速趋近于 1。这就意味着人们可以安全地假设任意 h 给定的密文几乎肯定是独立的。

那么如果在已知 P 的情况下：

$$\begin{cases}=1-N^{-h}\\=\left(1-N^{-h}\right)\left(1-N^{1-h}\right)\\\cdots\\=\left(1-N^{-h}\right)\left(1-N^{1-h}\right)\cdots\left(1-N^{-1}\right)\end{cases}$$

那么可以得到 h 个方程，未知量个数也为 h 个，则方程有解系统不安全；为了保持安全性，密码系统不能发送超过 $h-1$ 条密文与已知明文。

2.1.6. 性能分析

本文方案采用了大数分解的困难问题，安全级别满足 IND-CPA 安全。密钥尺寸为 $O(\lambda^h)$，因为是无噪声的加密，所以密文膨胀率为 0，不需要进行密文清洗，计算复杂度为 $O(\lambda)$，优于文献[10]的计算复杂度。

2.2. 数字签名算法

2.2.1. 作用

1) 验证签名产生者的身份，以及产生签名的日期和时间；
2) 证实被签消息的内容；
3) 由第三方验证，解决争议。

2.2.2. 椭圆曲线离散对数问题 ECDSP

本文基于 ECDSA (Elliptic Curve Digital Signature Algorithm，椭圆曲线数字签名算法)来实现方案的公开可验证性。椭圆曲线离散对数问题是构造椭圆曲线密码体制的数学基础，即对于椭圆曲线 E 上两点 P、Q，如果已知存在 k 满足：$Q = kP$，则求解 k 的问题称为椭圆曲线上的离散对数问题。根据加法法则，计算 Q 很容易，但给定 Q 和 P，求 k 就相当困难。ECDSA 算法的求解难度是指数级的，因此椭圆曲线算法具有相当高的单位安全强度，具体原理如图 1 所示。

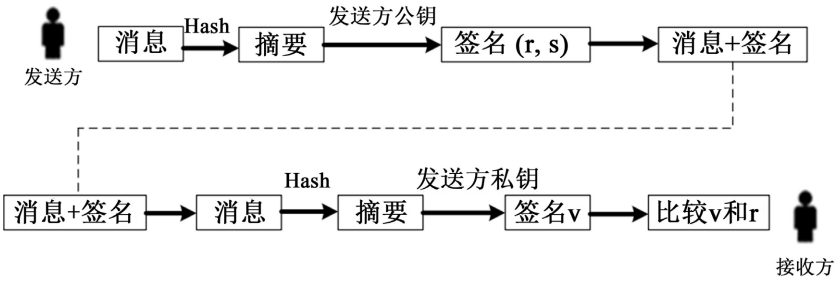

Figure 1. ECDSA schematic diagram
图 1. ECDSA 原理图

3. 全同态加密的电子投票方案

基于云端的电子投票的模型如图 2 所示，认证注册中心 CA 负责为参与投票的投票人、投票中心和计票中心等实体进行身份认证，为各方实体生成密钥，签发与管理数字证书，确保各实体的真实可靠。投票中心 VC 负责接受用户端投票人的合法注册，并为投票人分发选票。CA 用于存储用户提交的选票以及其它信息。计票中心 CC 负责验证投票人提交的选票的真实性与合法性，并统计选票结果。

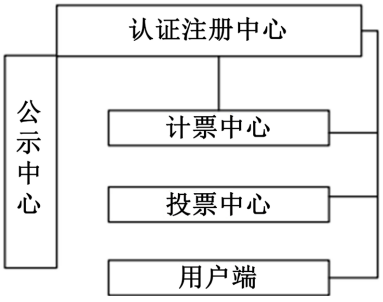

Figure 2. Electronic voting model diagram
图 2. 电子投票模型图

3.1. 系统初始化阶段

主要是 CA 对投票人 T、投票中心 VC 和计票中心 CC 等实体进行身份认证，这些实体使用 ECDSA

签名算法生成签名所需的密钥对，公钥为这些实体本身所有，CA 用自己的私钥对这些实体的公钥施加数字签名，生成证书并公布出来，其中证书包含这些实体的身份信息以及公钥。

各个实体的密钥对如下：

注册中心：$pk_R = Q_R$；$sk_R = d_R$；

投票中心：$pk_V = Q_V$；$sk_V = d_V$；

计票中心：$pk_S = Q_S$；$sk_S = d_S$；

投票人的：$pk_T = Q_T$；$sk_T = d_T$。

3.2. 投票人注册

投票人需要使用自己的身份材料在注册中心进行注册，注册中心会根据投票人递交的身份信息验证该投票人是否具有投票权以及是否为首次投票，一旦验证通过，则投票中心向该投票人发放与身份信息有关的唯一身份标识 ID_T、唯一投票标识 B_T、空白选票以及投票公钥 pk，并使用自己的私钥对 $ID_T \| B_T$ 进行签名并发送给投票人。将选票编号 B_T 与 ID_T 关联，以防止一个 ID_T 拥有多张选票。

投票人对收到的签名进行验证，若验证通过，确实为来自注册中心的合法签名，则投票人保存 $\left(ID_T \| B_T \| Sig_v\left(ID_T \| B_T\right)\right)$。同时注册中心需要将 $\left(ID_T \| B_T \| Sig_v\left(ID_T \| B_T\right)\right)$ 发送到公示中心，投票人可以到公示中心查看自己是否已经被公布为合法的投票人。

3.3. 投票阶段

设有 n 个候选人，投票时投票人选择同意(记为 1)或反对(记为 0)，若不选视为弃权，则任意一张选票一部分应当包含如下信息：$\{0,1\}^{n\times n}$。投票完成后对选票加密，得到 $Q = \left(C, ID_T \| B_T \| Sig_v\left(ID_T \| B_T\right)\right)$，之后发送给投票中心。

投票中心收到如上信息后，会调用解密算法验证 U_{id} 是否合法，若 id 合法并且在注册中心已被认证，则认为该选票有效。投票中心会把 Q 分别发送给注册中心和计票系统。

注册中心验证 id 是否合法。若认证成功则把 Q 发送给计票中心，同态运算完后返回给注册中心并上传到云端留档，以备将来查验。

3.4. 计票阶段

计票中心收到注册中心发来的密文 Q，验证 U_{id} 是否合法，若合法则应用同态运算，把计算后的结果发送给注册中心。注册中心在接收消息后验证其合法性，调用同态加密算法的私钥进行解密，并将相应的结果上传到公示板。

3.5. 安全性分析

1) 合法性：在注册时每个投票人都会用自己的身份材料在注册中心进行注册，注册中心在确保投票人身份信息后再进行投票，而数字签名算法确保了数据的可靠性。

匿名性：在投票人通过身份认证信息后，注册中心会发放一个与之身份无关的身份标识，用来隐藏投票人的真实身份信息；其次，在投票过程中采用同态加密对选票进行加密，除了投票人自己，其他任何人都不能获得选票的真实内容，也不能与投票人身份对应。

2) 公正性：通过全同态加密技术，选票信息只有在机票中心通过私钥才可以知晓，其他任何人都无法知道选票信息，因此保证了方案的公正性。

3) 唯一性：在注册阶段，注册中心采用一人一票，保证通过身份认证的投票人有唯一的投票标识。

4) 完备性：首先注册中心对投票人身份信息进行验证，确保身份合法，其次每个人选票有唯一编号，

防止重复选票，数字签名对选票内容完整性进行验证，只有全部通过才能被计票中心统计。

5) 可验证性：投票中心会将选票结果公之于众，每位投票人可根据公示信息来确认自己的投票是否被记入。

4. 总结

文中提出了一种基于全同态加密技术的电子投票方案，它综合利用了云计算的分布式特点、强大的计算能力以及安全的数字证书、数字签名、PKI 等安全技术，实现了一种安全的电子投票方案。该方案较好地解决了电子投票中的匿名性、完整性和公开可验证性难题，在一定程度上实现了安全、公开、公平和公正的电子投票。不过，相信但随着全同态加密技术研究的深入以及云计算的广泛应用，采用全同态加密技术的电子投票方案将会得到广泛应用。

基金项目

河南科技大学大学生研究训练计划(SRTP)项目(项目编号：2021175)。

参考文献

[1] 陈智罡, 宋新霞, 郑梦策, 等. 全同态加密文献计量分析研究[J]. 计算机工程与应用, 2022, 58(4): 40-51. https://doi.org/10.3778/j.issn.1002-8331.2107-0038

[2] 王彩芬, 成玉丹, 刘超, 等. 基于整数的多对一全同态加密方案[J]. 电子与信息学报, 2018, 40(9): 2119-2126. https://doi.org/10.11999/JEIT171194

[3] 何倩. 基于全同态加密的电子投票方案研究[D]: [硕士学位论文]. 杭州: 浙江理工大学, 2018.

[4] 汤殿华, 祝世雄, 曹云飞. 一个较快速的整数上的全同态加密方案[J]. 计算机工程与应用, 2012, 48(28): 117-122. https://doi.org/10.3778/j.issn.1002-8331.2012.28.023

[5] 刘雷燕. 基于全同态加密的电子投票方案设计[D]: [硕士学位论文]. 重庆: 重庆大学, 2017.

[6] 洪家军, 崔宝江. 一种基于全同态加密的安全电子投票方案[J]. 廊坊师范学院学报(自然科学版), 2015, 15(1): 5-10. https://doi.org/10.3969/j.issn.1674-3229.2015.01.001

[7] 冯超. 全同态加密的相关算法研究[D]: [博士学位论文]. 济南: 山东大学, 2015. https://doi.org/10.7666/d.Y2966761

[8] Ichibane, Y., Gahi, Y., Guennoun, M. and Guennoun, Z. (2019) Fully Homomorphic Encryption without Noise. *International Journal of Smart Security Technologies* (*IJSST*), **6**, 33-51. https://doi.org/10.4018/IJSST.2019070102

[9] 樊子娟. 基于整数的全同态加密技术的研究与优化[D]: [硕士学位论文]. 南京: 东南大学, 2016. https://doi.org/10.7666/d.Y3089390

[10] Feng, C., Xin, Y., Yang, Y.X. and Zhu, H.L. (2015) Multi-Integer Somewhat Homomorphic Encryption Scheme with China Remainder Theorem. *WSEAS Transactions on Computers*, **14**, 186-198.