Computer Science and Application 计算机科学与应用, 2019, 9(5), 941-946
Published Online May 2019 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2019.95107

Hans汉斯

Design of Privacy Protection Electronic Voting Scheme Based on ElGamal Homomorphic Encryption

Jing Liu

School of Information and Security Engineering, Zhongnan University of Economics and Law, Wuhan Hubei
Email: liujing0110@gmail.com

Received: May 7th, 2019; accepted: May 20th, 2019; published: May 27th, 2019

Abstract

Realizing the true anonymity is a research hot spot in the field of electronic voting. This paper proposes an electronic voting framework based on ElGamal homomorphic encryption. It counts ciphertext votes and then the statistical data is decrypted to obtain the voting result. This scheme greatly improves the anonymity of voting and data security at the time of counting. Further, experiments based on real-world scenario show that execution time and operational efficiency of the framework, and the feasibility of the framework is verified.

Keywords

Electronic Voting, Homomorphic Encryption, Anonymity, Privacy Preserving

基于ElGamal同态加密的隐私保护电子投票方案设计

刘　静

中南财经政法大学信息与安全工程学院，湖北　武汉
Email: liujing0110@gmail.com

收稿日期：2019年5月7日；录用日期：2019年5月20日；发布日期：2019年5月27日

摘　要

实现电子投票真正地匿名性是电子投票领域的一个研究热点。本文提出一种基于ElGamal同态加密的电

文章引用: 刘静. 基于 ElGamal 同态加密的隐私保护电子投票方案设计[J]. 计算机科学与应用, 2019, 9(5): 941-946.
DOI: 10.12677/csa.2019.95107

子投票方案，利用ElGamal加密同态性对多张密文选票进行统计，然后解密统计后的数据，得到投票结果。该方案极大的提高了投票的匿名性和计票时的数据安全性。最后模拟现实投票场景具体分析了该框架执行时间和运行效率，验证了该框架的可行性。

关键词

电子投票，同态加密，匿名性，隐私保护

1. 引言

近年来随着人们参与社会管理的意识逐渐升高，安全、充分地表达个人观点成为人们行使公民权利的基本需求。投票作为表达个人观点的重要方式，一直随着社会科学水平的进步而变化。传统的纸质选票模式不仅统计效率低，成本高，也无法有效的保障投票的公开可验证性和投票过程中的公正性。相对于传统的纸质投票模式，电子投票节约大量的人力物力，还突破了时间空间限制。市场上的投票软件虽然形式众多，但均没有真正地保护投票者的信息，发起投票的人可以清楚地看到投票者的投票情况。匿名和实名会对人的心理产生不同的影响，匿名可以使投票者自由地发表意见，使得投票结果体现投票者意志。因此，这样的设计显然没有考虑到人性的弱点，明显不符合投票公平公正的要求。

1981 年，David Chaum 首次提出了基于 Mix-net 的电子投票协议[1]，这是第一个现代意义上的安全电子投票方案，但该方法使用的公钥密码体制算法复杂度较高。1997 年，基于 ElGamal 加密同态性的电子投票方案第一次被提出，但是该方案并没有给出选票的编码格式[2]。这些年，在电子投票方案不断发展的过程中，有些方案过于复杂，不适合大型投票，而有些则是安全方面存在较大的漏洞。第一个实用的适合大规模投票的方案，是由 Fujioka，Okamoto 和 Ohta 在 1992 年提出的 FOO 方案[3]，方案的核心采用了比特承诺技术[4]和盲签名技术[5]。国内对电子投票系统进行各类研究和创新，以克服其缺点。但大多为理论成就，没有实际应用真正地实现了匿名投票功能。

本文提出一种基于 ElGamal 同态加密的电子投票方案，利用 ElGamal 加密同态性对多张密文选票进行统计，然后解密统计后的数据，得到投票结果。该方案极大的提高了投票的匿名性和计票时的数据安全性。

2. 同态加密原理

1978 年，Ron Rivest 等人首次提出了同态加密(Homomorphic Encryption)的概念[6]。同态加密算法颠覆了传统形式下的加密模式。传统的加密算法关注的是数据存储的安全性，它不允许用户对密文进行任何计算，否则密文解密不正确。而同态加密算法关注的是数据处理过程的安全问题，它允许第三方对密文进行特定的运算，在处理密文数据的过程中不会泄露原始的数据内容；并且用户用私钥对处理过的数据解密，得到的是处理后的数据结果。同态加密算法的信息处理过程如图 1 所示。

在本文提出的电子投票方案，我们利用了 ElGamal 密码系统的乘法同态特性[7]。ElGamal 密码系统包括三部分：密钥的生成算法 G，加密算法 E，解密算法 D。任选一大素数 p，使得 $p-1$ 有大素因子，任选一个 $\bmod p$ 的本原根 g，公布 p 和 g。任选一个私钥 $x \in \{1,\cdots,p-1\}$，并计算公钥 $y = g^x \bmod p$。

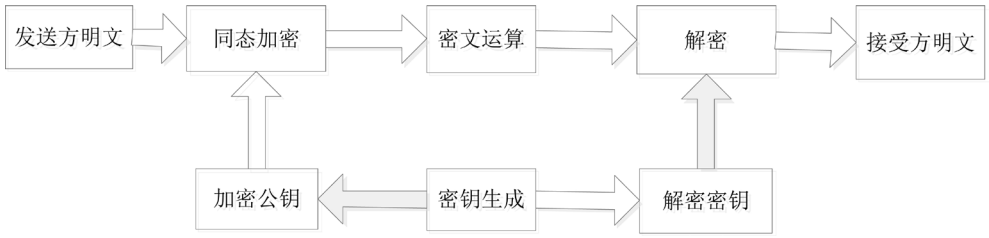

Figure 1. Information processing of homomorphic encryption algorithm
图 1. 同态加密算法的信息处理过程

任选随机数 $r \in \{1,\cdots,p-1\}$，满足 $\gcd(r,p-1)=1$。给定明文 m，其对应的密文为：

$$c = E(m) = (c_1, c_2) = \left(g^r \bmod p, m \times y^r \bmod p\right)$$

密文 c 解密为明文 m：

$$m = \frac{c_2}{c_1^x} \bmod p = \frac{m \times y^r}{g^{xr}} \bmod p = \frac{m \times g^{xr}}{g^{xr}} \bmod p = m$$

ElGamal 同态加密算法具有如下的乘法同态特性：

$$E(m_1) \times E(m_2) = \left(g^{r_1} \bmod p, m_1 \times y^{r_1} \bmod p\right) \times \left(g^{r_2} \bmod p, m_2 \times y^{r_2} \bmod p\right)$$
$$= \left(g^{(r_1+r_2)} \bmod p, m_1 \times m_2 \times y^{(r_1+r_2)} \bmod p\right) = E(m_1 \times m_2)$$

3. 隐私保护电子投票系统

3.1. 基本框架

本文提出的隐私保护电子投票系统采用客户－服务器结构。用户投票和数据聚集分别处于客户端和服务器端，并各自完成相应的数据处理过程。系统的基本流程框架如图 2 所示，主要包括以下几个步骤：

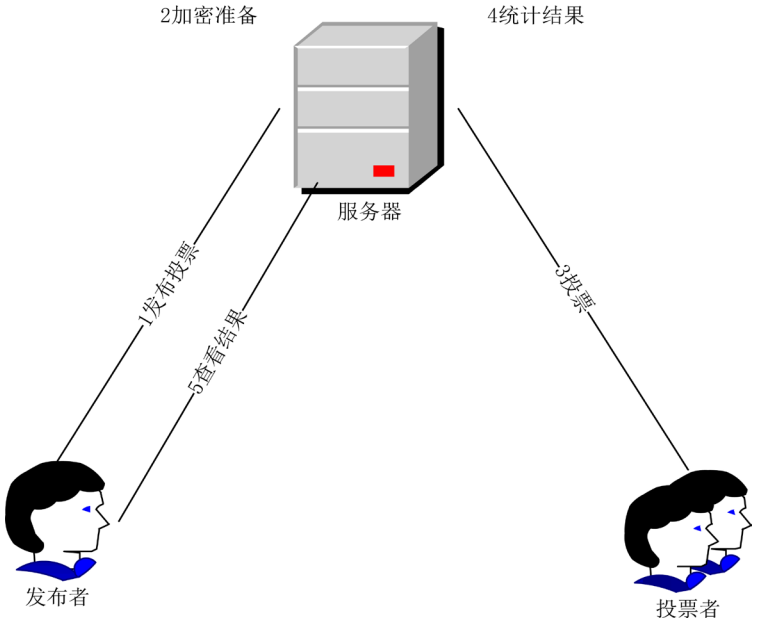

Figure 2. The framework of system
图 2. 系统框架

1) 发布投票。投票发起者在客户端填写投票内容及投票相关设置，并将投票信息上传至服务器。

2) 加密准备。服务器为投票信息中的每个投票项设置不同的标识符，并利用密钥生成函数生成该投票对应的公钥和私钥，将公钥和私钥依据其不同的保密程度分开保管。

3) 投票。投票者分别从服务器和数据库得到处理好的投票信息和投票对应的公钥，在客户端依据自己的意愿针对投票选项进行投票，将投票结果发送给服务器。

4) 统计结果。服务器持续收集来自投票者的投票结果，并进行数据处理。此时，服务器收集到的投票结果是密文。

5) 查看结果。发布者在客户端解密从服务得到的投票结果，查看自己发起投票的结果。

3.2. 实现流程

1) 发布投票

发布者 S_1 在客户端填写投票目的和相应的投票选项，并设置一些投票的限制信息，如单选或多选、投票的开始日期和截止日期等。发布者填写完相关内容后将投票信息上传至服务器。

2) 加密准备

为了利用 ElGamal 密码系统的乘法同态特性，服务器(表示为 T)为每个投票项设置一个标识符 tag_i，每个投票项的标识符 tag_i 都不同，其中标识符 tag_i 必须是素数，标识符构成集合 A。如表 1 所示：

Table 1. Example of tag in vote
表 1. 投票选项标志符举例

投票选项	投票选项标识符
A	2
B	3
C	5
D	7
E	11
F	13
G	17
H	19
…	…

服务器 T 利用 ElGamal 密码系统中密钥生成函数，针对该投票生成公钥 $PublicKey_1$ 和私钥 $PrivateKey_1$。公钥 $PublicKey_1$ 被存储到数据库中，便于投票者的访问。私钥 $PrivateKey_1$ 通过加密传输秘密地发送给发布者 S_1，在 S_1 本地保存。

3) 投票

投票者 $V_i\left(i \in (1,2,3,\cdots,k)\right)$ 在客户端进行投票。投票者 V_i 分别从服务器和数据库中获取投票信息和该投票的公钥 $PublicKey_1$。投票者 V_i 投票生成所选投票选项的标识符集合 T_i。在客户端得到投票者 V_i 投票结果的明文 M_i：

$$M_i = \prod_{tag_i \in T_i} tag_i$$

因为 M_i 可以唯一地被解析为质因子表达式，泄露投票信息，所以在提交给服务器之前需要将其加密。

投票者 V_i 使用该投票对应的公钥 $PublicKey_1$，利用 ElGamal 密码系统中加密算法对结果 M_i 进行加密得到密文 C_i。

投票者 V_i 将密文 C_i 传给服务器。由于没有私钥 $PrivateKey_1$，服务器无法得到密文 C_i 对应的明文 M_i，即投票者 V_i 的投票信息。

4) 统计结果

服务器 T 在投票截止日期前接受来自各个投票者 $V_i\left(i\in(1,2,3,\cdots,k)\right)$ 客户端的密文 C_i。累乘 C_i，得到最终乘积 TC_1：

$$TC_1=\prod_{i\in(1,2,3,\cdots,k)}C_i$$

服务器在各个客户端得到的投票结果是密文，并且将新得到的投票结果与原来的投票结果相乘，使得投票结果信息完全失去投票者痕迹。即使服务端受到了已知私钥攻击，攻击者也无法得知具体投票者 V_i 的投票情况，真正实现了投票的匿名性。

5) 查看结果

在投票截止日期后，发布者 S_1 向服务器 T 请求查看投票结果，服务器 T 将最后结果 TC_1 发送给发布者 S_1。发布者 S_1 通过本地私钥 $PrivateKey_1$ 解密 TC_1，得到明文 TM_1，根据“质因子唯一分解定理”得到 TM_1 对应的唯一质因子表达式。

$$TM_1=\prod_{tag_i\in A}tag_i^{f_i}\left(f_i\geq 0\right)$$

这里的 f_i 是选择标识符为 tag_i 投票选项的总人数。通过质因子分解 TM_1 能够得到投票选项的分布，如表 2 所示：

Table 2. The distribution of tag
表 2. 投票选项分布

投票选项	tag_1	tag_2	…	tag_i	…	$tag_{\|A\|}$
票数	f_1	f_2	…	f_i	…	$f_{\|A\|}$

4. 实验结果

本文模拟了一个具体的投票过程，来验证该框架的可行性。本次实验通过使用了 python 中的加密工具包 PyCrypto 来实现 ElGamal 加密系统。本次实验运行在参数为 1.7 GHz Intel Core i5-3317U CPU 4GB RAM 的 Windows8 系统上。实验分别模拟了投票中有[200, 400, 600, 800, 1000]个候选人参评，[200, 400, 600, 800, 1000]人参与投票，每次每人投票数为[5, 10, 15, 20]的情况，该框架均能成功运行，加密前的统计数据与加密后质因子分解的结果完全一致。

执行时间 T_{exe} 由四部分组成:

$$T=T_{en}+T_{de}+T_{agg}+T_{factor}$$

其中 T_{en} 是加密时间，在每个投票者客户端完成；T_{agg} 是服务器生成投票选项标识符和密钥的时间；T_{de} 是在发起者端解密的时间，在发起者客户端完成；T_{factor} 是在发起者端质因子分解的时间。在实际中，T_{factor} 对 T 影响最大。本次实验采用了 1024 位的密钥。在实验中，加解密 2^{1000} 分别需要花费大约 0.03 ms 和 6.5 ms。固定长度密钥的生成时间与具体的投票情况无关，生成候选人为 10,000 人的标识符大约需要 850 ms。所以我们对 T_{factor} 进行了进一步实验。表 3 展示了 T_{factor} 随投票人数 $|V|$ 和候选人 $|Tag|$ 变化情况：

Table 3. The varity of T_{fac}

表 3. T_{fac} 变化情况

$\|V\|$	T_{fac} (毫秒)				
	$\|Tag\|=200$	$\|Tag\|=400$	$\|Tag\|=600$	$\|Tag\|=800$	$\|Tag\|=1000$
200	344.3	331.1	346.9	339.1	341.5
400	656.9	689.2	658.8	689.0	677.0
600	995.1	1007.7	1021.6	1015.6	1030.9
800	1329.9	1355.0	1355.7	1368.0	1342.7
1000	1643.0	1643.1	1668.30	1696.6	1681.0

5. 结束语

本文提出一种基于 ElGamal 同态加密的电子投票方案，利用 ElGamal 加密同态性对多张密文选票进行统计，然后解密统计后的数据，得到投票结果。该方案极大的提高了投票的匿名性和计票时的数据安全性。最后实验具体分析了该框架执行时间和运行效率，验证了该框架的可行性。

参考文献

[1] Chaum, D.L. (1981) Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. *Communications of the ACM*, **24**, 84-88. https://doi.org/10.1145/358549.358563

[2] Cramer, R., Gennaro, R. and Schoenmakers, B. (1997) A Secure and Optimally Efficient Multi-Authority Election Scheme. *European Transactions on Telecommunications*, **8**, 481-490. https://doi.org/10.1002/ett.4460080506

[3] Fujioka, A., Okamoto, T. and Ohta, K. (1992) A Practical Secret Voting Scheme for Large Scale Election. *Advances in Crytpology-Auscrypt*, 224-260. https://doi.org/10.1007/3-540-57220-1_66

[4] Sverson, P. (1998) Weakly Secret Bit Commitment: Applications to Lotteries and Fair Exchange. *Computer Security Foundations Workshop*, 9-11. https://doi.org/10.21236/ADA464109

[5] Chaum, D. (1983) Blind Signature System. *Proceedings of Crypto*, 153-154. https://doi.org/10.1007/978-1-4684-4730-9_14

[6] Rivest, R.L., Adleman, L. and Dertouzos, M.L. (1978) On Data Banks and Privacy Homomorphisms. *Foundations of Secure Computation*, 169-179.

[7] 王方鑫. 基于 Elgamal 加密体制安全性分析[J]. 科技风, 2018(36): 97.