第5章实验报告

1 实验名称

基于Paillier 算法的匿名电子投票流程实现

2 实验原理

Paillier算法具有加法和标量乘法加密同态性。

2.1 Paillier方案描述

2.1.1 密钥生成

1. 随机选择两个大素数p, q满足$\gcd(pq, (p-1)(q-q)) = 1$，且p, q长度相等（本次实验选择长度均为1024）；

2. 计算$n = pq$和$\lambda = \text{lcm}(m, n)$，这里$lcm$表示最小公倍数，$|n|$为$n$的比特长度；

3. 随机选择$g \leftarrow Z_{n^2}^*$（本次实验选择$g = n + 1$）；

4. 定义函数L：$L(x) = \dfrac{x-1}{n}$，计算$\mu = (L(g^\lambda \bmod n^2))^{-1}$

得到公钥：(n, g)，私钥(λ, μ)

2.1.2 加密

1. 输入明文消息m，满足$0 \le m \le n$；

2. 选择随机数r满足$0 \le r \le n$且$r \in Z_n^*$；

3. 计算密文$c = g^m r^n \bmod n^2$

2.1.3 解密

1. 输入密文c，满足$c \in Z_{n^2}^*$；

2. 计算明文消息$m = L(c^\lambda \bmod n^2) \cdot \mu \bmod n$；

$$
\begin{aligned}
d(c) &= L(c^\lambda \bmod n^2) \cdot \mu \bmod n \\
&= L((g^m r^n)^\lambda \bmod n^2) \cdot (L(g^\lambda \bmod n^2))^{-1} \bmod n \\
&= L((g^\lambda)^m \bmod n^2) \cdot (L(1 + kn))^{-1} \\
&= mk \cdot k^{-1} \\
&= m
\end{aligned}
$$

2.2 同态加法

对于密文c_1和c_2，计算$c = c_1 \cdot c_2 \bmod n^2$，明文实现$m_1 + m_2$；

$$
\begin{aligned}
d((c1 \cdot c2) \bmod n^2) &= d(g^{m_1} r^n \cdot g^{m_2} r^n \bmod n^2) \\
&= d(g^{m_1 + m_2} (r^2)^n \bmod n^2) \\
&= m_1 + m_2
\end{aligned}
$$

2.3 同态标量乘法

同态标量乘：对于密文c_1和标量a，计算$c = c_1^a \bmod n^2$，明文实现$a \cdot m1$；

$$\begin{aligned} d((c_1^a) \bmod n^2) &= d(g^{am_1} r^n \bmod n^2) \\ &= am_1 \end{aligned}$$

3 实验步骤

使用`Python`语言实现密钥生成、加密、解密、同态加运算、同态标量乘运算（完整代码见`../5/1.py`）

- 验证加法同态性

```
************************************************************************************************************************************************
↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓验证加法的同态性↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓
请输入第一个明文： 123
请输入第二个明文： 234
对第一个明文加密后结果为：
549694124357395087141551261468053080461606832145784008625968120101821685232896659388957905864914776764468410614564499679113581260590690133666559716013
697768736628099027866337383272987047028985174881854341966935618811993775540585527304117181577346042103269197429328206171459958382035669326798270607869
874504791796512126577785309967704007355383570758557397661150790593774300319280026443405072513180683858932422159865643744148756612198466993534130810782
266183177154792025659585263789913958153490151207890341478848012499409186268360443949835425196576350141391409955566986558792909998004591020847007974997
154430605699271322443089915382549267524275443106076753017168685961980572906983078742817507757870953856124742407365106982276484333690565955422539974239
243170385480586926723436208279603967609530753361230804595033449865014439059952588603332725168982600859391586843139902198566064305606262063753468392301
024654111800152393272174263887809338738641714888889792890387598135382851409048160337104223705311400178460234137088325038201568746589932974522739164213
885493346020850036676384009513116643591325375260717941991992383909346719289445168105700509696080871507664438689221803737454536347684645458343721622554
23347912808968618743368964260110
对第二个明文加密后结果为：
312376761049396477784095317499532306500271226078166557701060872387565502225647157408329860901505323654097064682083494534164601600285373821711922026148
761598517374624513839588411293248630694816705879997278824741390940745951752365275602859070506532159873246216258082544952261432785767606405711158088842
469601205761085997588939852704950828838313431141468059912538892156739324087946738046361956499236585772918769206945879072430686131272908146436705612254
646335105340834622177418692547334708563553439108234583509385114209605390856017528211629021193688956777143896212417313934434994237771926657665462374329
679116811089777183920836053179129387647742234388349232742896889764445173330874414094828798680293085495844756444504226168319082678258095497449755195517
275926064843882280308321240175903909923557536017961254793812578140565768712169577285563573168739258466483554675258086766608569394716221260074443851327
999435486790322159550592938712711005429287132806951891662768406330826451984527055146385077701499004173916621596455864238522048158249891846071194688437
331935880226119799927272201662772471608067486826824312743361523899408375714686550332771906534556064954086467692480399391213024101015870520316756554990
001120311617575947010728111132319
两密文相乘得到：
434989717690832833247716016730724798201496548144861404054245046080198891165140906362867309300253013457508953795416548978068394630925913633995890380120
847310831106756524752594282806434744901912561683935408478914227264602878122169859869520584566929149242863257996766543055734693367416639472829073928835
531905153869759338351480108182144409878353778562522926608123727358933553574557384129735236533613939217257896654762758935130040800329557375983713711911
372930776927868001532877452167070883925615724069903877124519892117292057950978960918995935251063079467363678472017514257800395233173779106000341918976
896107128992656439354140346699883507198196975181344598570039735122073866310409534450158692430483427125152387897781721875466669965449696412458198642018
809446637319810427071390224722318866017194176497331219806675739302279298866251277286605606361601334314533929470037482940618540779563154550201970575934
191092771654562545046957553156095504436252288961590565944469330848567910678270763380733012466663529441398832333929229815699293036788060205523514191111
811978796888547162229369251760037854699239355506242056895870191751318873237358484772626893288306459689757126095093007036615781661297593749504054860466
46185881189677372849254805091582
密文相乘后解密得到的明文为： 357
************************************************************************************************************************************************
```

- 验证标量乘法同态性

```
************************************************************************************************************************************************
↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓验证标量乘法的同态性↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓
请输入标量： 2
请输入明文： 123
对明文加密后得到密文： 79275149925471358747797801236779705193565264696325931259501332126195554457413412900302782848976795592599331891610241997726073554
584539550385183932023583075404216397651644363167823821695268588131368193782193759150064204619304523630407312116227067959750167752058363392360671182218
625262635466439529191191268728421639021362994824524186274685332621013587952097178609410403306680305827296526845568177324997187538541940970618516380037
299437984918793810963824327389076875617220246315772788460716724797521975426562517437979746894831834794269469893973062956577956798789956038578468137663
636617567654603077443185765674575680892325057223994243041687866991752438944321075881347130936547670490857239604538114515126952749561468550259168498269
695214670505745735631182445300992000250120864643287417918341591420312490815137638999015642704647696348549672718958619894719244914272034266202145001095
322196874407633642084437237081127022503137679297065704354386845548727825549093211147822569454101303899832784911499565113096594466522842670111297975628
399641630993097597070375666106865427316561007479402621942316250936233529242563669698391038645979009548490789743372663251682074339815089418026734643350
958309689106862673609918463556657975964485263690102668
密文的2次幂得到2529642236073130203752585784157646958401225631397310164298486143863383466846134935808806794247931708451228949814637196500588934164317 62
150021779465131395124432574144181276622550536056100021355302698294903876767266294400823925194825786984532095513671628780376508963946712039480653670674
395422024851934803408648526736091648822724239222273859560957672768415361012052319829802141235892094987532123126453951969098284294349994220541527702767
266640033455587235416485769723643303013229591781459321304494782096762511549317317696062657440230015080834030828396094373255498904429470066443202683416
177466365314270401712576771776093406051378447817475927256327622045284536768258649542137960113232620234910521844590458643236408254424444247275509047254
345227714734137582962757287001864462878295822138169139130505631758925464896032516642662401690201574654455796507637075374316340695099662728399980349095
159779922153814465278534056904800712725647624625596462625037844768036585008152951982923725787312333864990261454536923558934142297080581163091704687072
624600137314949221222050873382425035903757970189271236587123782618234095485245057084081832736241588406455443436103811695492145861439041650275439509779
325284754673373654235957665204783296872238926671
密文的2次幂后解密得到的明文为： 246
************************************************************************************************************************************************
```

- Paillier算法在电子投票中的应用（完整代码见`../5/2.py`）

```
**********此程序模拟了基于Paillier算法的匿名电子投票的流程**********
首先每位投票者为候选人投票并将结果加密发送给计票人，每人只有一张选票，选票上被投票的候选者得到一张选票，其他后选择得到0张选票；
然后计票人将所有选票上对应候选人的加密的投票结果相乘，并将加密的统计结果发送给公布人；
最后公布人对统计的票数进行解密并公布。
**********
请设置候选者人数： 3
请设置投票者人数： 3

----------请第1位投票者为候选者投票----------
请为第1位候选者投票： 1
请为第2位候选者投票： 0
请为第3位候选者投票： 0

----------请第2位投票者为候选者投票----------
请为第1位候选者投票： 1
请为第2位候选者投票： 0
请为第3位候选者投票： 0

----------请第3位投票者为候选者投票----------
请为第1位候选者投票： 0
请为第2位候选者投票： 1
请为第3位候选者投票： 0

对该投票结果进行加密并发送给计票人；
计票人对此投票结果进行计票。
----------计票人计票完成并将加密后的投票结果发送给公布人----------
加密后的投票结果为：
第1为候选者获得的选票票数的加密结果为： 5933889032089550384711383993897176756446903840281870630034893638726581103578528979505149392472107800400635715491233009097885185359115366931265022543605554241422468107815254061287835168347305665417578303068011507939029238400672753831463482153194381218388510298169704172115479794767959700662766598349599883857793696768804947307930413332710656151730633495838189898894265676380870775291831631917111730204611747331782201812605250206727355620290836104866311447417181056150608170262562518261811362403876861393874219986105410840518225826628026147398682656910594262836319259941404235052134766881537137395666073698891616589982210403984157275945779365233661396914984291962155694075847376829078084787624056962650611206373017966642806368483195430862649580414414335847605440706662880435271926331748931131826197336553322053795251127382846989410407204464380259887777392850279316444808526881892776538944580029911940409484931374942867334073753953449605710835218334142715389118023558118466031700076391495206385743266646824510656774536799804600038684197985330406854890257611976093503148723684860788823705771207128038494769592768655657658729626576720557595965011458271842093794245420127427534120684532180035856734530021535833358036778865942022028554930 3

第2为候选者获得的选票票数的加密结果为： 2026252986200200653762738365547447014285054354408077779516316548457176519625986541255375405771357655058663925828669292417012309750824781114863237046761458307585347689027829905704848263183218223099755213318029601111418254741711463283658107599009871117695982930638345038903427781772450391090634342171170552371501398375431859509865023801086439821255924564802669086520459568291132729314457283090864314595273215767153407182297522762490017327323721233900033174396990470109205366398615091423496148018665649046319742359848399557092816092197193865953097191549533234342985896552154760912693698699514819308039846684087799021197236728711127434630787669805428334088511187615022119653090955228764160630525446761345710699614812805314812304291834511675124917973097127789595808898177796180525065515200107402116042994492214324747870969508160398481990263806750843343294024718610940528266866486770778233335504388829279430061425146001508469203556753724862119708177661573170515999511302757705405964768287544634563549231062516868100061999360466309280032776811898878131890273980826624798326542817119726785815859280320857846831310572338443976205129123393600958631883353517394084168917733692279939574961133967846485976852485500341728206674341100510302189293 7

第3为候选者获得的选票票数的加密结果为： 5128184589213283543790640387122754917658669920764755033924890111747372510966461790937979782334102699215877844773793466754630493510070890811798199862661361544978460310103208956407337054886607766794821897984443936650344435132278291462097444556917520095655393474234192950092980453822178989045542533888854917927165728641449437812378274154057600164934279934918727284074444598560263239272751126622900104322805695673511273009976752499359351775398657971870599004870215718644785973891025358695458805407846689714332882196151064104720719109730139464653116647056018808268358852701865565663853909793191738189611875069642969715072321952687520991089171219496042339748424393111387079201392867651093146947964256992098592245893762833632641183312494566785985845332962804995766335099896291790760407344784736532505996629810921864445635124917391148240281478207148639803510651095428803666514362837485745739652555980548304567233195592006205632073261733200589693880286761761167441018707786705479819339585097570739471035496095960321971316699907413947259099095629010719901629545084264763759824433159592037821855304693563816913940938587559717124803824147501186724077663192527890829232311656214495579800671783692178488890958797845283827084318863992639443367067 22
----------公布人解密计票结果并公布最终的投票结果----------
第1位候选者获得了2张票；
第2位候选者获得了1张票；
第3位候选者获得了0张票；
最终第[1]位候选人获得的选票最多，为2张
```