# Helios Voting 101

**Fachschaft Japanologie, Universität zu Köln**

Gregor Billing

gbilling@smail.uni-koeln.de

15. Mai 2020

## Einleitung

Helios Voting bietet die Möglichkeit, online anonyme Wahlen durchzuführen. Einzige Voraussetzung für die Teilnahme ist ein Zugang in Form einer sogenannten *Voter ID*, die euch vor Beginn der Wahl per E-Mail mitgeteilt wird.

## Inhaltsverzeichnis

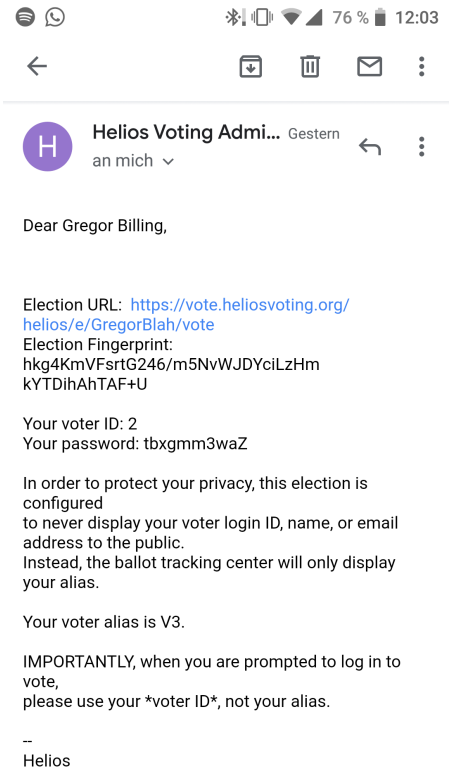


**Abbildung 1:** Die E-Mail mit allen Details die ihr benötigt, um an der Wahl teilnehmen zu können

# 1 Bedienung / Teilnahme an einer Wahl

Überprüft zunächst, ob eure E-Mail der Fachschaft bekannt ist. Wenn eine Wahl durchgeführt wird, erhaltet ihr eine E-Mail-Benachrichtigung (vgl. Abbildung 1) an die hinterlegte *smail*-Adresse[1] mit allen notwendigen Zugangsdaten.

## 1.1 Zugang zur Wahlkabine

Folgt dem in der E-Mail angegebenen Link, und gebt eure *Voter ID* sowie das zugehörige Passwort ein (vgl. Abbildung 2). Im Anschluss werdet ihr einzeln durch die der Wahl zugeordneten Fragen geleitet (vgl. Abbildung 3).[2]

[1] Aus Gründen der Authentizitätsprüfung werden ausnahmslos nur smail-Adressen der Uni Köln (mmuster@smail.uni-koeln.de) von den Wahlleitern zur Wahl zugelassen

[2] Normalerweise handelt es sich dabei um Fragen wie „Welchen der Kandidaten wählst Du als Fachschafts-Vorstand im SoSe 2042?“. Alle hier eingefügten Screenshots enthalten zu Demonstrationszwecken geschaffene Inhalte

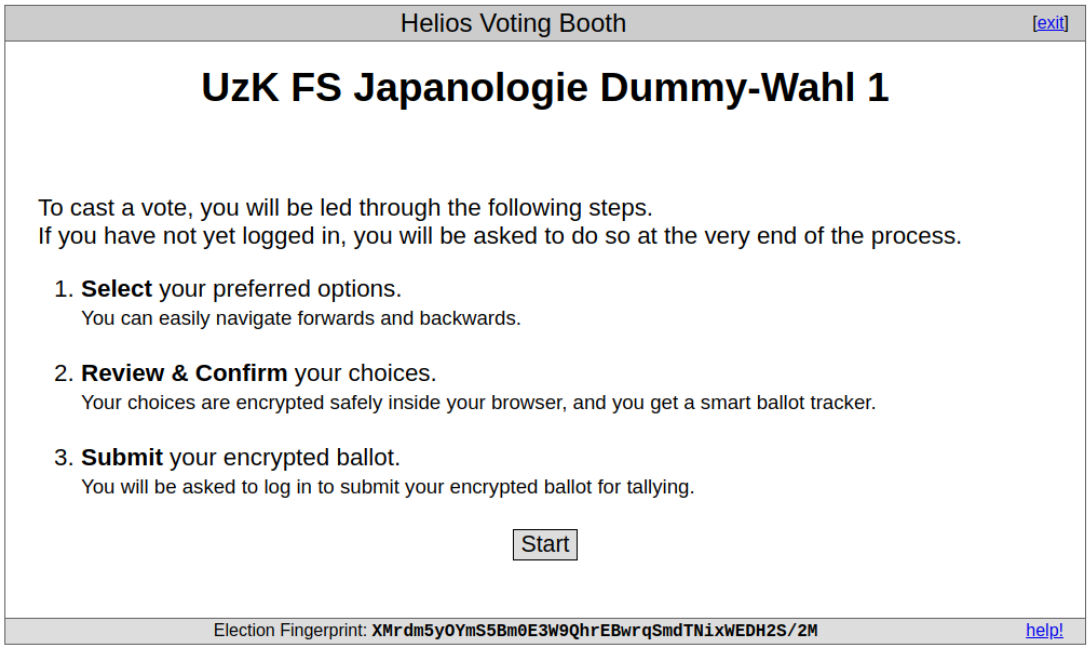


**Abbildung 2:** Der Eingang zur digitalen Wahlkabine

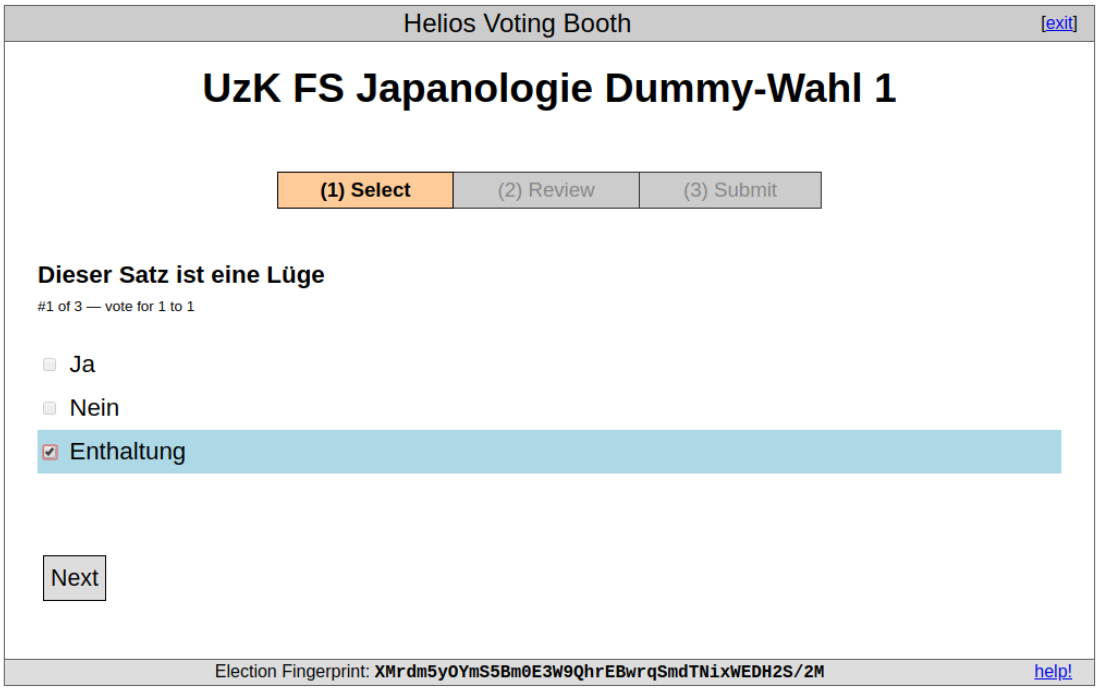


**Abbildung 3:** Beispielhafte Frage zur Abstimmung

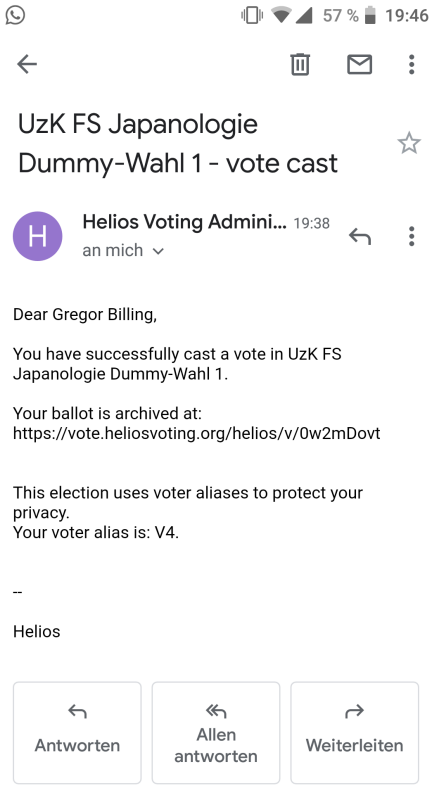


**Abbildung 4:** E-Mail zur Bestätigung deiner Stimmabgabe

## 1.2 Stimmabgabe

Abschließend siehst Du alle gewählten Antworten nochmals in einer kurzen Zusammenfassung. Wenn Du mit deiner Entscheidung zufrieden bist, folgt nun ein Prozess aus **zwei** Schritten.

1. Klicke auf *Submit my Vote!*
2. Klicke auf der darauffolgenden Seite auf *Cast this ballot!*

**WICHTIG Nur wenn *beide* Schaltflächen gedrückt wurden, wird deine Wahl übermittelt und damit im Gesamtergebnis berücksichtigt!** Anschließend erhältst du eine E-Mail (vgl. Abbildung 4) an deine smail-Adresse, die die korrekte Übermittlung bestätigt. Diese E-Mail ist eine verbindliche Bestätigung, dass alles funktioniert hat und deine Stimme zählt!

## 1.3 Ergebnisbekanntgabe

Sobald die Wahl beendet ist, werden die Stimmen automatisch ausgezählt. Das dauert üblicherweise nur wenige Minuten, und im Anschluss wird eine E-Mail an alle Wahlteilnehmer gesendet (vgl. Abbildung 5). Im Rahmen dieser Ergebnisbekanntgabe (s.

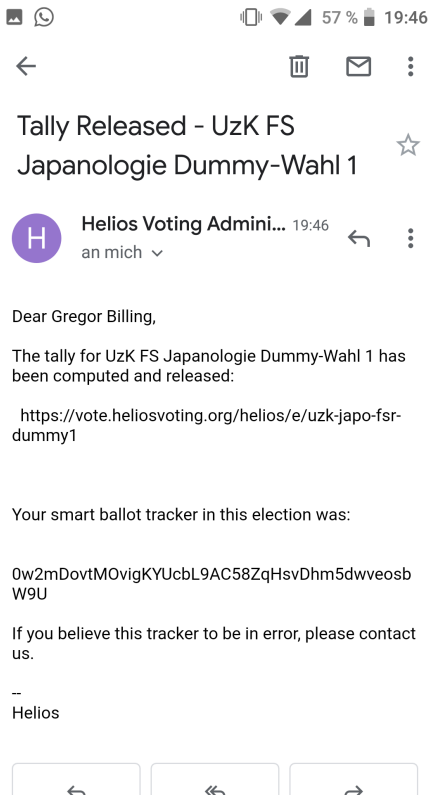


**Abbildung 5:** Benachrichtigung über Verfügbarkeit der Wahlergebnisse

Abbildung 6) kann bei Bedarf auch der *Ballot Tracker* genutzt werden, um anonym zu verifizieren dass deine Stimme ausgewertet und zum Gesamtergebnis hinzugerechnet wurde.

Damit weißt du jetzt, wie man mit *Helios Voting* abstimmt, und kannst dich am demokratischen Prozess in der Fachschaft beteiligen! Die folgenden Informationen sind nur Details für interessierte Leser und können im Sinne der Partizipation getrost ignoriert werden.

Happy voting!

# 2 Ansicht als Wahlleiter

Aus Gründen der Transparenz soll hier kurz darauf eingegangen werden, welche Informationen der Wahlleiter vor, während und nach der Durchführung der Wahl sieht und worauf er/sie Zugriff hat.

## 2.1 Erfassung stimmberechtigter Wahlteilnehmer

Zunächst müssen selbstverständlich alle stimmberechtigten Wahlteilnehmer erfasst werden, damit nicht jede Person mit einem Link zu der Wahl uneingeschränkt abstimmen

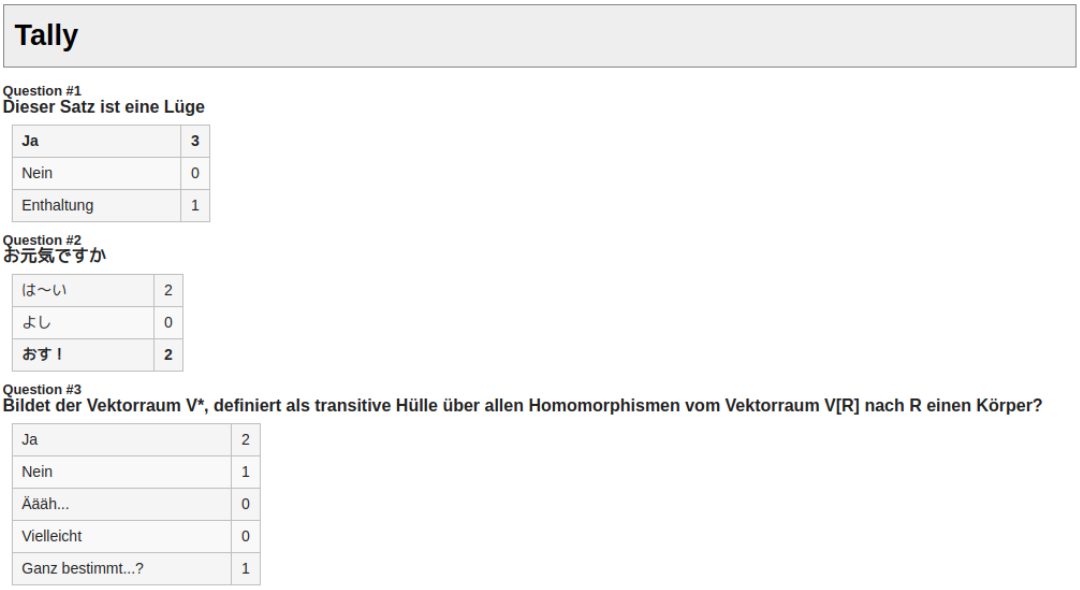


**Abbildung 6:** Wahlergebnisse im Browser

kann. Dies resultiert in einer Ansicht gemäß Abbildung 7

Insbesondere sieht man auf der rechten Seite Details über den jeweiligen Ballot[3] (vgl. Abbildung 8). Aus dieser Information kann abgeleitet werden, ob ein Wahlteilnehmer abgestimmt hat oder nicht. Diese Tatsache ist ein direktes Resultat aus der Notwendigkeit, die Legitimation in Form der Identität jeder abgegebenen Stimme zu überprüfen und doppelte Stimmabgaben zu vermeiden[4].

## 2.2 Detailansicht über Ballots

Aus diesem Ballot kann man insbesondere **nur schließen, ob jemand abgestimmt hat und *nicht, wofür die Stimme abgegeben wurde***! Das Wahlergebnis kann darüber hinaus jederzeit unabhängig verifiziert werden, siehe Abschnitt 3.

Die Grafik in Abbildung 8 zeigt die Detailansicht eines Ballots mit allen Informationen, die dem Wahlleiter zur Verfügung stehen. Dabei sind insbesondere die Rohdaten verschlüsselt. Eine exemplarische Kopie eines Ballots ist im *JSON*-Format als Abschnitt 4 angefügt.

## 2.3 Wahlergebnisse

Die Ansicht der Wahlergebnisse unterscheidet sich für den Wahlleiter nicht von der Ansicht eines regulären Wahlteilnehmers.

[3] Digitale Entsprechung eines Stimmzettels

[4] Der Autor weist freundlich darauf hin, dass in Deutschland zum Beispiel auch bei Bundestagswahlen eine Liste geführt wird, hinter der die Wahlhelfer abhaken *ob* ihr abgestimmt habt oder nicht

## UzK FS Japanologie Dummy-Wahl 1 — Voters and Ballot Tracking Center [back to election]

**Who can vote?** *Only the voters listed here.*

email voters

bulk upload voters

Prior Bulk Uploads:

- 52 bytes, at May 14, 2020, 10:35 a.m.: *done processing: 1 voters loaded*
- 151 bytes, at May 14, 2020, 10:19 a.m.: *done processing: 3 voters loaded*

**4 cast votes**

Voters 1 - 4 (of 4)

| Actions | Login | Email Address | Name | Alias | Smart Ballot Tracker |
|---|---|---|---|---|---|
| [email] [x] | tokahara | tokahara@smail.uni-koeln.de | Tomo Marc Okahara | V1 | uIfu3NWv2HfyA0VBe/3jJvTsnz0O7Q/DrcIEcppFuZw [view] |
| [email] [x] | mhoevel2 | mhoevel2@smail.uni-koeln.de | Marius Hövel | V2 | qZ9OmtlN5S/mCEwW3GzqXyAUe7oUXv08+23VaH9KoqE [view] |
| [email] [x] | fhass1 | fhass1@smail.uni-koeln.de | Florian Hass | V3 | s647c1H0DK8BpwIA3gNSlYEDrejQyyoriWT6xptRPIk [view] |
| [email] [x] | gbilling | gbilling@smail.uni-koeln.de | Gregor Billing | V4 | 0w2mDovtMOvigKYUcbL9AC58ZqHsvDhm5dwveosbW9U [view] |

**Abbildung 7:** Übersicht über stimmberechtigte Wahlteilnehmer

# Cast Vote ulfu3NWv

cast in UzK FS Japanologie Dummy-Wahl 1
Fingerprint: uIfu3NWv2HfyA0VBe/3jJvTsnz0O7Q/DrcIEcppFuZw
by V1

details

**Abbildung 8:** Detailansicht eines abgegebenen Ballots

# 3 Verifizierung der Wahlergebnisse als *Trustee*

Jede Person (außer Wahlteilnehmer) kann das Ergebnis extern verifizieren, indem sie sich vom Wahlleiter als *Trustee* hinzufügen lässt. Mehr als ein Trustee erhöht den Berechnungsaufwand bei der automatischen Stimmauszählung deutlich (verzögert also insbesondere die Ergebnisbekanntgabe), erhöht aber gleichzeitig Transparenz und Vertrauen in das Wahlergebnis.

Um als Trustee mit einer Wahl assoziiert zu werden, sind grundlegende Kenntnisse im Umgang mit Kryptographie und Datensicherheit erforderlich, da über sogenannte *SSL-Schlüssel* kommuniziert und chiffriert wird.

Auf die Details dieses Systems wird hier nicht weiter eingegangen. Sollte für die Fachschaft jemals der Bedarf eines Trustees entstehen, sei hier freundlich an die IT-Beauftragten und eventuelle HOWTOs verwiesen.

## 3.1 Helios Voting im internationalen Anwendungsfeld

Der Quelltext von Helios ist als *Open-Source*-Projektauf GitHub veröffentlicht und kann dort jederzeit eingesehen und auf Sicherheitsbedenken hin überprüft werden.

Diverse Institutionen und Sicherheitsforscher führen semi-regelmäßig sogenannte *Audits* durch, um die Glaubwürdigkeit und Integrität des Programms sicherzustellen. An dieser Stelle sei bei Interesse auf weiterführende Literatur verwiesen.

# 4 Anhang: Exemplarischer Ballot-Inhalt aus Sicht des Wahlleiters


```
{
    "answers": [
        {
            "choices": [
                {
                    "alpha": "50041076897578096208305092285767933470558736851175688822929140455811731555075306
364963013911833850713774888093493906757100402474586032878072282094752868194832177424792486297561378386611597770
925798545493562293379457450412656693897564970569219580118996462392119702290146453318334373152545107274535407 21
855832474200249541367450264361221973393864312365702454537785652424413821112856401985385696536589880729630350 01
376289870951404589116569809685524077954703564185439625434090680342251617300560645025431419000059370252044305 71
130491176718887068502416294082157727633987912747892527221974689948889443411926710654682111798164",
                    "beta": "241368034982957968429414881340378649513024982606137760256674191354641337355704974
745751374030026559409957505262075825557869717398241197446532373913434967813895945184666787732222162202520796 3
827597827618759956584649939688391230009470291728555754578053698212333200783875128528054972241192090340809127 1
076850140088802160846304733547305396561102502114875946397993233766856797184522478972543546300028832027615792 21
163024392116333950239395372852779698261032489793323510466271362453445949726739565289274708197397081136823387 71
579495920662426916308432114638911923613445133478915200716978262807142846032736894049103601159 28"
                },
                {
                    "alpha": "910566942057720453598536185255516907540560844020319386496384224957944257135598 21
448867900575815937080984504956953440119476022198897552651182185039189095101300195096823525022120442036207784 67
933969868780746374556279415716794532150747008919334439981980532015988727015066764379493356665912721451159390 96
648413510761774271779257110571857849479916866360358065911037957166740326157413465749642996019533385819692837 1
908069169731634111398207374605384896804521223958132594030595973253808645520752439096245907387774556666860706314
001566930699321615048379812926114055479966332857571555777987018882368823220055371144909797359433",
                    "beta": "575995586962227211601915069522386684729774056108514526673765275121708472546903 14
574875841642046717947740312473809293453114131400013958489458314234683160349227473104314252677894072255902034 80
906679293869972544141619412926517838336393613911616870769471755991049242712891023426552053584127379199823744 37
976804570815739688078692563978689199559402551667506496213019541250266747413857875899797836323400679951936718 93
923651538632955117148046264461953125944402893372156779423614285426844312871680249759262758815656131493269193 11
845431392850393402700491428026167683727707368480538820058000237920123499400301276618455781774 3"
                },
                {
                    "alpha": "158468061956343117207624246353477147057162199342781539980808874895627363555199 42
034935848278602032425929560668386633341739743993277321198105377548184202689209795619018562346334784585893299629
022680417583110046117577915378154978639653104223384143453262511199994181890105221682346602408905826463041361 19
041568963310799479757260058392335111313219543534313628199769721359458958669972620342316155739654975120650869 26
407036730979763914998346127856994108098924405802399149044442492922240384756882019683260889640243890916130986 06
945228315058749365729402687113687108428519415903624178221793644926542752000346918968181173062590 6",
                    "beta": "767339451627133720857048642467375340125199324665478192512383265916271084190416104
731425152110861317461166264623656501707201797857297337189049798043865394934062106487106070638729352104324583 71
752104701481605478944888086365716159540063194019532555678932590490471220204376091440735217925146176475297654 64
366970743400332628422807019449300391315556571566546697190671874350311042926295131995459648402155487227118971 70
809905945836234293760598681052901995399805207160101643631018655481859068968036881688093350397330260426626774 66
101411989827511245318687301600856285794770567160605216151415826239683341603593850862765125 1031"
                }
            ],
            "individual_proofs": [
                [
                    {
                        "challenge": "47033814826777507405096450796999189854420890055662798233810031403942714091795",
                        "commitment": {
                            "A": "10016712585041848274547544491888821422327531905929878564895824762533412196936413052427424290373137940062411105962452077349224384288906906013012847956970211979534443885613134782669969064061070748295266140304001808493957180621255102061035874744022903470200726048679236608136323314852087596957791502359746942593254747841154919518171592707650552042689951475311455101995901235343263901364103614780826091848429698208683180437058589226948747230918366733225086781260337577669859236067140787954083601560565262936352629995361985315293827857368642115535332684318117700251570796753870508915628312703026211098284892384863972247 52",
                            "B": "72790571072903469776045933109606448722913317802585110711315618010842213613396904687333067070003952887853888614875346148237168929869965452487823728497465863684879549655367467871359566079508124081180737661266400173258351079117844522885885781841733635217405842773083904947445507107365256104484057108954966732577964056640442820842903156357130538572186198788673249390287195707119517348366765950034145660299482723451732743281811960050656192597312237600197590937647122797967145380921793553537882407825140406696091106794958802870200735176197948922106633923655204904529001441680348349883351203007152773846341139047899568672640",
                            "response": "3576827581933952059163365454881198546890935451486101384907296681988961709 5790"
                        }
                    },
                    {
                        "challenge": "14295751421565393887447421973129870057078590124697752728597698232084620147463",
                        "commitment": {
                            "A": "44186351666552591543000226966597376327235330140828176233414603129736981364727825824058214540935016715792771400344387454291866130751563220241261330329950770480378376332604695578252034561706274636410084312681775799348324439124938822756465337990724034342030978029595539878528508306834197035457105678299387954964404655976463711184975091189334982996259266209932320733500384585714641118094386926752195857173089649588237690826069701095287692702057386624138685214101732380043149878328599688561721909395964013293617298708725 3
```

```
189970208809089481253915956943265563966879404655931494780685178106364596251060206743683027687229010 8",
                                "B": "153381335421071182541497166580324180351822969123895474581073289253863663491493820446529979132444856341266516053063199992372804387486430308134614253025651455661947326356820231505302341314388103013272320111511223527784767562314507630559862848750221390806771924677301736068433129327923792531360164625546104403241608731114147917760593863766604388711858233227719777099038708670315751820129832181074413824209901181958788115991608819195820372960689898044305028089570952603060792742002453736506094729800844818145258411024147123371368427437768030191537901892118379843063209682209357197293816349428483198793967411080306542876 8",
                            },
                            "response": "410543661249246007668127119125481579714584395578088206370657218100037177490 4"
                        }
                    ],
                    [
                        {
                            "challenge": "120213654803353883355395598173915229309512870653468730103454233076927082364 40",
                            "commitment": {
                                "A": "48215566686968560971671958494999340624106489464572243833600124501706339681100150007839669356182575398787184989137178819235502724349565260286150872225909489375793938580174779699108626571241356682142059965779968406484552476207310372619102106733934397717742228527973758839849849813339759871680965717830402816796224501729658226662653507900256725730571630126584422443288573347281792954094897372476223018718989658102839215727043307770488656532490259712606226570729144051768301194205730908404546344315995785943765796995205164505971543944635310830481938436824451918887992523034844673833061736770220664114516830864431645910 15",
                                "B": "119089424004128184768404097227948744028704511641992027233499258661105044681168909607083123731610723396702483564945687433893775931281881511226175195815160657651701367871008604489325327394821403280232745372095314959446709746026910984924935918853935946194703418969947232619394809160795167191243105653821319785119767260390063655569651556334294373127074495286468793677961802638843825784808063807427091357919099063855319495984541103308766326859480806662462020940041378846094952966745652590975137362863233696610261585358418492763483706208050621689577807817609560717188366956217473350448583962655413959538599671963145167992029 0",
                            },
                            "response": "389508405592852136553568517606685663152957365985306356862267621644383167778287 8",
                        },
                        {
                            "challenge": "493082007680075129570043129539061901835249911203724535296352265709027242043767 6",
                            "commitment": {
                                "A": "955453945793338315503550432777498187173893323466515461060137526203777413763164700973596703552633838920583988852386909058690862569688011904127418125712047219393695606891579299864098040777041765797295303792393501870505374689872506166600726590911691533506291322304238397214897625276709368734439399560373098827270826389566491018980913181268360069721299763606793903749280699245573099360313705085978089197585451405185141473227422675275759860149166692560449640107483555415418650111516030652372609964040375403122695825708495699240361472652081630380554549992763859330458743169483624927372914824726724734186535866268903614 2",
                                "B": "123344392736119914869924739348063170616751896427264585587695672288598300315931330817999022667053393936182304134257082595229005771368826736224538233346566263654825187173300102566176691903827087537865373553118763150282687512939067310033888102647628069201611673391037391457365542372540476898484748845948905829474119877895241281221198875031971882529799726321686897623355446795569957914384732958983525873589834415988668479732329414517721361010509322153848352753742848082499590822103705908671279302703566619248298766469302650038891728809560552169229622519004004829815235083739065804474497485028724720037795627484382277148 0",
                            },
                            "response": "477783244128796691696852775509858814028234442638791191100685755256648848041 6",
                        }
                    ],
                    [
                        {
                            "challenge": "245006203890956716634127677203554921511117374046802979917093484526122778021517",
                            "commitment": {
                                "A": "114288172255742407163504348024459099465634412490292421973790271656694754658607194554319676007056319116822058071144358996986075417449971982651481767772806235701161960724873221984205047132344189345334215117995402283745550891633503960494122034845561083375742493790398655729449623910548977571524295200299591871622078076697390212377204459992310724977531746753000927341234173486896048569759071453923153413804540164244552181008956979239826679116033700820318063985095086777508662742946232516773664313174899172996002516656372565746726609949045205827267125940366424443943118617201146115300812385278603063171502039384670853489 7",
                            },
                            "response": "636369710093185006228324139466662170199158555018921915257248916219678293271001864624122404601202351089260013417590735671475679929413228084011572144770764364920305048424897272337636568398005057646719882096548175571837492641444248706236936998287839206050885553324196069873562576037252975429394254487446355557686050252706083949456462194541230070145414805199645718525523406398140725941186228464986874586046358928719302200455928841360290131354545112011349703435803489796113981327381707072263844331802535099086099888211801588100005954077001772001900838474240737943274013631517814067399884934802379756814322857584632515221 2",
                            },
                            "response": "564761876057273904157419375327231291178396140403003019538281236063907671831 4",
                        },
                        {
                            "challenge": "368289458592472296291311050507185187811036182166171397527216785840059554028 99",
                            "commitment": {
                                "A": "137113893924476480781757168195670954459289372602306703429234248625769648104690773430635103186542431422209981997709294088542592951715798160353198906353890218343109259820961487272141852653367743770763619451341016263971183787583034530002612290912674944523855814270711631532235174040515538360065397762052768986722254998682593614820505687368178443649460457381564729396122722407912274055271592385395141893938900510876124038197080395772763653679670735827622362401800664598741995554145012626147689606588936617983046565395789 9",
```

```
48743268972303659610048524668640078654740352543580288192147261295716686154442690965612861090547113862",
                                "B": "91675561483853622063692249365558963724328340378997501430499661969628703312040737810891623739053306840750826492148680584129447929091736747927620759341626258194398718074582026536847683423755445060010018262278241720810838700399166336420668056486404441742456111983506487153225626621512747432031703315276249241368628530352864348346025883500540213392879820120866799371552960658501634038417958938197592247799293048544834909506850267960412184017825974110586940578924090393411603340344895730095390095439001005448925662745501649373100676124233184402230482124957038631559943123507613688403886681422696663161974653542053029923638"
                            },
                            "response": "4896978332447095706936244468163442937906694336703040366363375950525223783890"
                        }
                    ]
                ],
                "overall_proof": [
                    {
                        "challenge": "526484828806429448496274232059907150563844886 51",
                        "commitment": {
                            "A": "13870581593262803990101088261564903150547670360074317176657044171826717538862457856030276423522935496241946533702945297435990659660322200127420499612338136626695100016243877091455237371946343956349552943324199726575250362100927239139962068383105332838571113915606190818085701543071025006175735001269829885883314594408615297285216831773312262425758965164964214408467684204447238776578355398413038638916238035724121430436945322872018253674465440625630155395579764241626513407203947406383388539559573682732782935307482976666812579251800233236442033410726474497358143115675594877607043606569224664845433877835716087783338",
                            "B": "389982035046661978353566704082301582977857380067281279820865972958974041053045084070709494526878285035177215068063214814006513323536652853109141551409375698782921022065916236074718278596222960169135971326333337012132034434451255128373462446400415868867039519441377160453883612223798794558918238288236661002532043916550441771040006505443398103896962641880211907137415386317766633212828292698283104150141399598595457028649308841121293213451588372594814641879474909129478627975849780013686879021843454760361697421972514846879669622287920054395219636699075505593376114117990848071138052001706778954014409761944145315189 5",
                            "response": "4571734469959367169841654247150425381905672889514363586854767721476408180604 7"
                        }
                    ]
                },
                {
                    "choices": [
                        {
                            "alpha": "7613496922547827246461901351175389689509169588047058366697528422044567690598631709549772572305604229683495043561655561299593617941974262315207739680276158830752750941882340415014227276586994724159931442353939794255438244092603030022653353275008626892234508671179544187196151413694779644661402998300023437594247865996604875492834064653491237595241325409524648031483341239248962446601873946461980491477248355519487766936486698095801375408014531395283558224025134384298030686736078855988546194316780396923323638717288785717963708115826908163792767817107280070716692885595380888904926286884772289128499708789321406738909",
                            "beta": "13840610589378005949699947910129089664431234462390971423838847320244752874679320606649196226181401605083191448618160790496629349618786700443129474229685304255512243073743874157287312353161287977245380183863897636688316307480774451990182841574997857775904249172045943853045597042610435140866326625413690418734239207584281471691067970269057836009825046992337987717490607982208762398809922745382626840424186980408020747099340455635996265656159195659852300707279890173502673815984748190899572284495310802723035108591735603000462284219498629269320707521330663888894344815006789737118073069488951985339712139711939387222525"
                        },
                        {
                            "alpha": "71765871522817875270321266564127582733981804454146072337559371056060654948528712157926485119272822596390629105893069467627408995375727269682212695472700222378049308228029229299997058345834357664987537844733951036426466104611696695995018856102614512409019183670639817805924681174852557226307610080004924626602329545586354567877673350673227716915814080076537569095465721602627415448378902057618880671396620453825037388803374139693856219834541406611158928338053078697403182150192769411855857052922447156654213500826991086265310592916763298450198714291260813197146899388815820952938201244881885315937132871538659022 650",
                            "beta": "65633592517335253554497504083188569266326529019594523630954738913663516267849400039918096652706027549761941289047205055014952743596124592342417202394274835520098212999627317937222537417652695375091306841159657355252005158870453034098600721063695560040721484882886487304800010037290912309849012709278605512146971107418830664922373863546005191363588919042562860644248577517185535921935828531722092479430476965250546419660799004141193258547248521038049701191091582400964157415594494535455636333166211181798921713406143064553502287362197427202526854937840916967800811926531846290109584153684899578773945743623933707142 4",
                            "beta": "68450392210672217361794751372489822348060401355879317826492187649653167073669930276232264079108934687722287430465502314773710660648544267738176922802487447361835506287294688309791025436547125463218971482036915496077795374523484864826668308474541095351632059398426101073862682468013439317742591705438296176945888157268492014496357672993483412118862113045151401969880879684878623435133827871435028247300551498966000592102370621732551413704700245527122285810607286775640446462561299663579988339953792745621380157615195041290050368225152439046484059912378699105493457622661618736021656897604595112380156018883211645120"
                        }
                    ],
                    "individual_proofs": [
                        [
                            {
                                "challenge": "68233103710115837807992461943189582295561906266383787522062150809799756 9
```

```
9119",
                        "commitment": {
                            "A": "151939798342720360390839978261518983595594238790509371450654982797774041383564697587331269849569446245477252638419275661528774355696549270268469871582125131606990839629851682261060815247165165641235183959632919592118404184075636646989413356825955945730989248796419813739189691902752005335365619094612165705504668543489823978690235693025671732186214190836598928262867774094496389856959542606375802892095229289420101930803514099038118566469866323070361224214102777958313542806476314297765643482178634249666209726906870292603758325847524573286916663721036331763405390270458293938464116688665827907526869538997676007845869",
                            "B": "115785913177775820532812248645511675908164917557934165776699560337352229064757987850966366950394238711370121693022243902269986322619370767222949973247151935859017778763770749364726296959147452969838312233763121705249503271866694842352897537999878774440335129682316264476454772313793188032534091841794314715156257314136531281368543922614138606437193495445410984743309499762275875772701089532521163824376145770716055133130531037461698550359073882683888190306862989326570030272469339466889806844364719556615751027936488161774542139823300064102477997349389215139395207239698658835863236778275463672880823088558917431144040"
                        },
                        "response": "899819911389345323586975263557864789216193683324793243133146715486682474924
6"
                    },
                    {
                        "challenge": "5450625587733131751174462657654170308146458207612816276692015076473744105
51655",
                        "commitment": {
                            "A": "1288505265101990224020402966385019328580679992475920678169432335275418714675068274195621358657685111384105089841872236348752649555574532405382574958725026316378692491783555468752631845782760743424994251423402356514545530984724933357676835724283021595131915233100123980655041335964943885833680355178624168488726101500895197730230037414361363877502985215628019424424866755732037602792461061001340307323869323002735290014158604304253661885601637918367929381461033421743095453049289895944281780126641664591545553013207327951485469105376024852605844530111357047450274498848069420930581595246921346548037457792584045443058 3",
                            "B": "4405168820713116770727820110799926293289805715872345665217529211827211290549321020492112690087160177159890275062686915887855770749934583272856143790289740025897829757416234621038883302685109406628313504931123938333980220126057061816700551852440637328114437712433491965495236465550458554693684357046458364517910999757330021592402652903544088136585808684693290804727633986639617789608765753303826977041950201257698269003834809127660120145779827989723418282711127735020658801529362377480017438860332273319121966661032476974899936140146648261025257187864013690443991262213015780382011474346729119866590045534310109440356"
                        },
                        "response": "3025927184490515995873973131796781553663757588633813419339474260133513973
7310"
                    }
                ],
                [
                    {
                        "challenge": "3753527680893874126372222385687469890215419684773900790834173132437045435
386",
                        "commitment": {
                            "A": "906406266789289395405161157664113173516382375661116264466606455257288611461180087804693814491509903087957950912060228305237307344826650755158522103812116034061771100219878514473857466160209793368228432632117348225232943629304347272157995990698482759640872202956322795436488233586099811041390371167486916736867606573543929039948817174230980493636696339036152267117335867333023820508803207522084623292755837297923959662726766867770565967421241753130806746590670000372916509193228607057592982947561325158321817043304944549523527903704762345510382529360478358814010585887730599620048639199514495206435886616932658192220",
                            "B": "111918651725629168686501895504492700270440546049961925243008742291207047276073683737502550436415509540749920386860743575668719233795545630903380176558543231056800826016010970201473867984302577152759294968124434503258752398530539206809121758898190647414706698620508662831476323180726603319482635175634909248320850521241307706198638070537458567559311953714897500210833127728628098511939371809717999043174612622010663233320194825672268547452899355747529222846639480878121228700029181104366983995373060929287520729974140090113120764427433101405141110316389169423199286106649169046091205002411865316700201468660862006 99",
                            "response": "1202494558062157051516480579689872394164412493882282499567731708863450572
7605"
                        },
                        {
                            "challenge": "5757603856744902716617165038498378578189855807969194106960400162806296158
6906",
                            "commitment": {
                                "A": "614456353958407806085292776032626338520241577787436044385740172461156663836770481767848743557999476633129529612807715710448060531606410904253234475657173474311929395186937195327342424297514598802041744746630584836270939259010663579955353325022613140740969740823029470164228861365790058368896818933185547584058829522700225596478900342919892761728972638155935441741971063541395731344703318311705496189244321607365499650789443322308813110819122096086422714822528657571094185146464363473464478219214502879984077682660886166043488613290020551941386576187565785318833754808514352368705548487378908245387174488236937540532 5",
                                "B": "859204370259197485136511244291178363557608771938155716248497922008461500489057459887966079529363401293406793058039804814004992599938476708687907320794457503709983147491782321193189878896079915319955936011344603364592088242459600611658561285773132769012497611787672431255483364500874485530925038044559318040861650078514406446087646686279816341331920302610355344917924933076589296244103874760716889695766614723718747199666096074556014605635026769859952842042001394906082643047171467476926106545793063566676810049204991150487615749249115955398664981803355805061220199836209251617139896929456681540348261704905719839085",
                                "response": "2667655170256677355366166024392772665027944015470112973195249032262461407
1098"
                            }
                        ],
                        [
                            {
                                "challenge": "7088603787026383503810442856144897380295263041313241873191900093463807 88
```

```
6921",
                            "commitment": {
                                "A": "3078066103082166822425531043995978498672654737370946830239068936653599762125
74591972256568294267650917175670613614337505025348519450190556331655574177466476214024118841903757065671271584
55786775358769108473881124487357263560766107350600025882317035936331756147604018814095775121397749993559220299
67098715540647474188940789843426528102235330219357067367322828375225066975638425554876394256956675228533265583
12743536182534733418100324401013052599479855620832677881377485435269652240494139603710678969800370816224292058
88187226339239061493654158008565303845389115234263024653336527065323311346919229269740541899965016 76",
                            "B": "56170068401404558352202238309397488563981992122338683319133221891539264294397956655035977372467050873284138903647793777176803443471588889147852867753433946167472623489670545163017011309801715552634936880429038600075893530621478363438869433606318189686537909368780605900655492490177663630811444543422387092689534341806220373677191208158473196265697810117920244389079187215757967800493822153753430270478022615201584692828158516285576748621551621511665919083425309749821891732991825022619690241875044758547343340000558721157505317978594068243814812725734127694254252405712938521796781578369829624356150354344728303725 3",
                            },
                            "response": "4442748148159273725728225329648876701969929398222320955986240691521518274
4066"
                        },
                        {
                            "challenge": "5424096246131651778873342991436791867242865703690963372490833830898120719
90136",
                            "commitment": {
                                "A": "1036961452500937705342431014103778126723238573600618007529830874043364790434
98580512727938960108272164038477274372862076859181514967538409070194045795147160526215843033817758636593295026320799675975258721723084595438053238540884553549176586638968325003914016694929478691224410639014977597209699759505931088727968017863492464635636566942174860272502848677422229742081210032210970637744917405370000070180903207718263944031229229124528959589444961265758696217373768810980932089239689836025288480034554644170765847571230591306476500095647588359046868323075729815587137935400027909827780329793187543877291572320161606361 07",
                            "B": "1039793173637787865032386857874973198857436802620464141239154387802849469698693739030738248863388904233794664351616077277949485542823088074627581457406650907599806701951308467443855823252808193505110182573800560124898178984751099949812023788109260966681950092743487104902190743507623114962451798155125748734675003503466592230354549278157407729808316624199417999336234687009014944003429022428329971130753870273965285436496681969334626401825260324544907530183219914826563817987640932445732494208459754986244144134579252141530601710945295786745802942635127248430599844239336563334613713658546237123142908145931149857 6",
                            },
                            "response": "5884858512289547641463826277480072948513737530797013527888646162326015555
0469"
                        }
                    ]
                ],
                "overall_proof": [
                    {
                        "challenge": "3293526427057912969428690112673749288032951272449338575131838362897634658367
1",
                        "commitment": {
                            "A": "1689092382774736708368581219346533146743411032060811885608754604914266811824879612679344762857501285975638770592886618633994404176985902078170927506129582049749229613041676530051133515106414509475066921083346965860339514937977499452313384478350094314406123767288827131811122897858008539524537620091830311899370230484075903341009801013108763545690082535344937910683640108481314306219614631727867269233995636848054524597608572618259003605106185354839948534212790874648449228968353188821260903867188081571524419974782153464329664199130874462517379953405748482528095659104650775217373225302697871510720554495738058473941",
                            "B": "8314493581099069664994922033078755476685462942060682527634444013379931893691767698569426810581006171445708204650073279757719067968431424392307079466606439848725012590594427838846433291270521817494042399530478920706434983699177211879350085976094137627778580379899338293182897161598211799671070266001874568887997893636009848113525534363166048283510400961979385641044376784351575880989962815791356880991130082012541846329062465842333075186431697130996428359835126508729714121051435177188535519283886923464886186645830751441092518121189678987660870631861671115737453934586334263969537590180212802669338874142737981370 40",
                            },
                            "response": "2432797402955449239873566426274617026979263875635137861609870741584991380013
2"
                        },
                        {
                            "challenge": "2839430197776377159825697164460123115359788672003353709473100607517769663612
3",
                            "commitment": {
                                "A": "7525817712501169762650744681150631088223328989451472797658275666240362333604744390604666777134200713092718134017243030015668539980376005105068391481131430820807591200937941163424722483314586102044228350271623966105392837494546615723766836584071149592443278293435156638468234722569729737347731506987249642844807903742069763015290067373958034973008297039287280112112771262672754811322672780340292812837165069793391938155519325381390063160360000841692822825978155932504427521274937458195829784533485607973486825589167139692462024276982585148945113087247638746678549063220138042832668849006750245933499340627367686451449",
                            "B": "1523213720841060294154732687277607464817044956251864366538465005370076121681358697304386297936057936025235902808544033546178010922457141997100200145411517212278239920367952842565464840656467323941539984701647026740944842249961569735973090292594754803641688867289868955878424438078589406054576943040397292229827870396198345084636566453496131721029049997286621384344294705059790146234824264391685287533750256253096325285811137350379224255449511559037931633112561083955265832182276224899460815558746756017383653292486528075167240046921153220368551846433340586417280769471293159813845655652037512494116130926734863852175 77",
                            },
                            "response": "5494111361086932124141114340928011232095098143862350235423362524964703862401 4
"
                        }
                    ]
                },
                {
```

```
        "choices": [
            {
                "alpha": "413119588525158421196768603588406508931604590089615101904100430257728437893907858741721042321124778245782795290121118661183556458066909687092810934765611097848627854173563975884413020219007195227731011640040700482158976805754821439334605461609822153729826836167922790143372488127633765821947253979581457056638598811540656005249298422261942292796381302773739188133050280325967531973823969510150721793636989865130907123630689975308161125561408054419473694363533896263001517200046646515220622556801399222867072326256733440385358354791822797016558958608354326324576871239986471098709728726754027492993533030497217032630",
                "beta": "105311390096719247402340960484952444967407102858874923981051933655728818675116998885824710798901255772178699566489483804176262172913465247850939154143285484941717006575333830658811019228436785302988749820475102918669950493126449472898504021272201686888146671027172652153000434982092426779803350883003693403360380504521079066035062307341419735388150653400454307135436004031157102187571110708632438877910155318912593461917714223955624953581297131549863763075280073947167920749532745716080078395729654108540528306341095405934989772919412760718193665658389942851731049190823012889221519933061964872226053803322708350126061 8"
            },
            {
                "alpha": "135158176070860195946308768570251749991575652581238133695397459016493524649898798437976156858898526898848107045495494447386176556217348710608432449544085546661593175718324450353203778108438494777935641301464351142132875070416289137525400654480867074253595636807790449304180286228129600439141523630600748035408800475405149572752893257802272491596936065300193515195398515876608716534284598028343526607827426758327888722911799814033763914693995186255877298244872034675543474107615861603199746094438682646183139718559977783066232658218893894715293429994666925837918815267077449381921294817182714661902641396988277424983 6",
                "beta": "573436286274175231076173804245425207934839590866469335147236885923413942616454251438742172864705124691074152970530194419247744201036961977428841399274903340801570319969730686438852181939759694858628081764708144017640039670175550116759347909143066384924939844137778180018763978646131853245768274357884917421047370192574842143167301219883589998548715996079171580141499319398714986669860000165964604386833959407002997656165116918004890650599159522269408332813775475515344892881778771365089783245746757323870602679519631861647912647633586050611408718679777116919842255968997698674596872660454831763576806151729570929 7",
                "beta": "921037914862411515205503610241003518640910988493254700113956875706729757534067284744586439705275844505631809642897388730749532843547706993565905200829979797910842900254713462951968538466183902987549781168571811489907132920392574389414101440988190736139048944223931407454022595278138098000317675659083502233479300510368713889845986496279069639220872362868206765577081742350410369924467433870930192946420016105117491960868586915799961806733594313351109047934087946115404423752314030088001917186106885871561230980588893177137764816307861522530041760084423526779797096924290359814126844699580232491981926292215866958 7",
                "beta": "395576977183841859449591377552380847810766579748535502105466976959040237531618470629213183990320102045801054847389068296050151120381559845823755328309471622929712344079295288904667037328361280315684162237621303651576380968100559362633048158314861455120265160686812533070641719261051779062309587743951819181625561085599656029029621727505949470916019389496162600306468384398238694981378038929267011500093954476471687478543377498439495072629761961878662015760547471005349055111622290112889618015003184758463117698293681398843516627929335210352974666627330090649440658233636759587529554853973934910166766010203730032737 3",
                "beta": "130498445106787253926982976835532161203096901085348418547910876947441090167145695333226954008228113471465357904721959199279662204869475859636836208076845745123330103803297621398118570467348813905599082435810173322258026249776256071528206332326713620615499069780076369835670617650014804684953967043612395779112128463769744025124228541700008499513901163261489264366246910904281659554387218164268358906521806616502606320793921481287379769694753299157760571541823183585380648817288654344566105478794332461833955186590354711383725205688370410318362919096890120807943993659325759561773188523288401308235520065833473286926 8",
                "beta": "134648198465733639831684845583343305273773710447026243977441397507538068306927469589244791305066797666707254704854360213607634296374725823899258365984343783124348685369260724354816152149658418651666978458726350094359801952319584834713682487540081763386236218630243078947921591455224895967254155644542857355856260619040814009813993437940156145657288295800502958085678702331131573039997454747487063718751784988404064518543829091285173489035351170157817487299679315868297313564825817660874849527582391961156775192122686887853976443461575154536161944487320638509391089269789700996717905142995950625755212420569031692635 23",
                "beta": "323229431422135742533992259308037306664975795856115175207139174818200422649621528457686921971402824217421896008791957520731428486275139759137143134052738463671281679232078284100343549645333928284080457989270200599314569356249883845476711065905806471810804293682113293537024130714064681230405057917427919486570425369873562367477673049654591891709055044730701099683003777011589846439861004929063493406884993432402871088263028601132193831386480129876613707142266917151367511698317485674208756645137828009652606572446422284339567689077405495079446780914862598327055503146273747856077099173916636391909250266888464555710 0",
                "beta": "112497524413983610200527041647847504970901631932508253451029972877220825425362142145243834250021583525765785769979610493584720670863370003330214837150950257856294307536663779702080223329065075900495132971519018622334127939008205381817167745511189846252212082517768647195186997690174362616792631968724527205570799161015701724351004190625147794591954165248793848630361910299798435726881481212655936058623488129170088628464174573725405770422110464186220119325082073426200019381196164348250074905355698562567020769536262668475333526915735572387391721130742561433872125534591633985404366041516882879288198207480988957871747 "
            }
        ],
        "individual_proofs": [
            [
                {
                    "challenge": "2845740545411910487635791485225846892281228757107967926061993594411378080 11760",
                    "commitment": {
                        "A": "6846665041865213148216520452513645834798302956278358138412273929327854549205 5799756546945739589026387048567422866103562116865006942130712369673282285405167821816157595206368605469290706 8350267888677763857082681079950240368136190232884309604857328755277912662560535663351846312745376651198061383583222915638539531910334583232318575863159169849994030894526156397578765907492118110274030893272648406554839000 2030982138337425945447171063095817832586002888157502104838390671186460857965496276934968578590352514306293452198905859818886532542418922234621068137931251129074915044455837698687582692258626499437028268545377777 ",
```

```
                            "B": "57788117100840624966829336852411033894662606607585681432655359754542136481366009888941145108547568885455676589144655110549634936055037279362074394065849263058049325093981590827673932021014200584661923432192081090437014296529691638223785701813660149566570185370324297155370105229835343993125592977493888030579548544937734814294252362793348694813580658553593570564858654388359263660052217008077228080987029304717279204923477597768012401459230891420960468114491666503808406917356045800425514644273259839080330541145236039642852792808400092825003649781997967172972363479066569483635002364608967899256181460474145668227838"
                        },
                        "response": "5406291757945885514595752533195192006839686065747412208279627246821383058
1577"
                    },
                    {
                        "challenge": "32872160794223796416185957919085527641670312381758002584506489198712019853240",
                        "commitment": {
                            "A": "9010130418594344421077645294022578850826839662896639046151608861893848146189106098659730377656954551507350428327074116229129869456783793206798300933740937031475171420018893590649369123428074580385480022020041766039488635465150985705266972359762037060955650899920211391585063724154326282887585540301965499128225732728890549408313091253961142602498179833572744796469095158119795960219338391867960253181482061971282281611806946629806418847102724931345879733442455185702041109593420376084542123040014467742084531433537600615726926736872204437475972381061774921264606786597917629244015848360507659277902997821826117881085",
                            "B": "151115572878522203902598344773093866507781086410958313786133280622755553478588631305351527851297297137367861333570420543830098873722179488154300699133087340534704141160211145982060946507444373652187086223009962047043386506769207881968109170056372835658648939715280319035734872576098495310576212203521289463590292633647587344799294521825377499768580959407321164747499917818807103148722347946629791629166585206391742296683016504385322848719133535277650522969158238009853637409529120377008281731224255706371405185511143257264014078447052741406946278262937601988576439316437617256589781815565437037386911978848267486604"
                        },
                        "response": "3487057818877007370495637681788275012431325364937175325512854716458248699
6908"
                    }
                ],
                [
                    {
                        "challenge": "20990658395747824995787091925790647653664686354288450723197027378064870110894",
                        "commitment": {
                            "A": "9853675047877632783499030833972118938603150114772312646315574122405005947317072967997296340114579319160862459274872989247470065060955371468297646381245615943906730756534388005494587352309580341569115462048538006774311790127870731123941171367720482496565009471583141578468789809493696665426292907116570133130858250659655386131089288129901111060286188665996810029893989361310155178357955090582719130642931050231995481510267282366345542860522924368249248260262374954649143675652919948101783910649446534186791232089608306276742255975575873799284138480684327997528347323858185955071890219180324271015526975393922508129 9",
                            "B": "614489988162877014411349638198345843731961491942105279802165165982321169269828982192723480379816104477612776547922714938053862151696893985411746157548089940536590128802740783224762906247509724281529416481149937802726984081362171870280370958658906770013022155545616391292683443388240532365424380317369283776351582582836438300861013471222414608323450477971626816417957473225137273743976057891157218629178800550697219476108363929673503634851842417613521035809558442558823404046725655786124980481222336919394293394084826025973467207375547985300375126620326895141667895961893423958105951302141319992139211019317587805921 2",
                            "response": "1679023247847981761548858669519563525253639478782637550505193793756770689
6753"
                        },
                        {
                            "challenge": "40338907852595076296756780844954465674817594610984774164793321385841862565190",
                            "commitment": {
                                "A": "1162341987665098175561992696571860555661419817877155545425251863936229548556688469654872479001187276983083629823881200311930668515096843931883073225718431060936096504853934104192398220999407331779843427830247997183299833152687876808520710278746292627464895046843474794620245023139983145788750712853858927300834340283826058374112922433440129973657992086317951954126752178840759968778240239400755374642886683870821633666121755902804567670877165213644910806500160617985419180390928476762909270347234009096455780412935522634868791763956038979850979242475801366289272610606349230070360714280717621363748105286590411510",
                                "B": "2108992313658167661442545601048541675549689803550389904846751391942924018888835173801464520276866383304634230952347295163132232999996928638320861980688465443156518224026481741873640255615254468496948767571698463803518086664358218117676622086361031913319638504309634665262770195098299160203395653928192752412325632972561459276176598454844051931540773517272411787539136690706638481359562376863083288020096411818629251760931363581958573240329493226790164380779577527442551439638459931495642622228703219312141054511620394252831965164898744401833676161554568167146627014054927552114644949242094471661670291395014574313301 0",
                                "response": "4048149662811312128317450279369822123425943896336600406179158168544485250
8090"
                            }
                        ],
                        [
                            {
                                "challenge": "58644973382105112245914756692562919480117091830070307113352050509171405690728",
                                "commitment": {
                                    "A": "1534894352116024377940002905960653741049925787296616516450938669135056504931710739392947173848225344714344739467891140962543405265345917824638307279824731554624894241209025519882193511590746348424522236903891240303442769650491219954751709499150837863224991986904131784632410453814020871782670192215206843164732499192268227157656357440962193167627245615891961892706327598826223189230125127999290042858376507299571244777180503916063075060745926109619654764295579627883219116202768313876806156829073463266662355419464514510555429817292656065898107801991680331353614824219432860899968521878181291975658809420125400880756 9",
```

```
                            "B": "162453824684415815120151823901437691584567466212349513345787601145235024341583737547921012371046135816005149040259525460759769618473776774620281670399319773986725473075280473686390180757744491039768437206536763275637416278621139609025965805966344569334837109779072754487718446265104445145813108315274656771280058687329473392573937851324125080971042417662646799555235654620250671250911130666308121555527228587878101032193820894201884061989580563933623814513374777133149249140540036919316996650016968699571996800934220365835845893605041680657518363000114985345865433869520089527271385122606699723483055071195974141 6"
                        },
                        "response": "2383340869522566641040692672910945626858264647689940345246804154418524049 1901"
                    },
                    {
                        "challenge": "2684592866237789046629116078435906531790948662159834409832292655637451640470",
                        "commitment": {
                            "A": "1047785509275385018759638789856567793106611252046044890591727314858731554816597102732952506772755051071307433632260831494057022454701716884662494865533961544631281740930179997060551672661295427111881884429546523516630769304411437850277638751032312733700579414255729675182548618195723258569131314296518346504119587535051137794430392670294991919755551984390748444852911211747454558409589684855077386200999615357878698728271788329369683244150542839998495425541461737466166313199360503561373171181160470437266971197615085556082656732722464030034829577704244121401716586793608969112048459102939868602059918245488073865856",
                            "B": "109485571046736402120296366530816949128010149477431947149745203510888091932611328397543976692696644205611687586412202237719389336969648865015167271586483508851219565361459128786825418926959202949220981938931369380603411756604055589682861289961880848125262324950340651008992966412600831033775015237214290282457020894925643642639032457514322185849317709330910171287579787520607639772658565798742132501761498192959253785119996601254406560432253856662003868465946543822604360996589064163141524613441898814569225557046964242315976046064492983320081806557797522658726799671695420074956788918981845230176855471317211207506 10"
                        },
                        "response": "2113997367456778269488726344806027076758657544131250860330354747371408746 7588"
                    }
                ],
                [
                    {
                        "challenge": "4297746065720615670153331406276877343135739742507232056146140976059804687670",
                        "commitment": {
                            "A": "8314216158485184950790817066052647887321777645260790374593017198028531790889692049368665404243016300816170778583714580505721655635856577957076087437864740952762796030832143247624152361766208809251668057493068938708413300277756716566853310488550521708054792521874906790004833301846765470124673964249047114038344421233517184263642680758728037947274042776325117508572509082548480721706810195735264895365817488949223225803263314659533081903519271891964171333009366727678598286257731253428356092871012087744851815727338808988781691541511477380674525432782395173022474510299457449501192762961117054867160284795688308131078",
                            "B": "4655076593712632289516792722820805426461522494704502132911660541454250336129586248644529911578170990210878386600837681475921290166793548314138308357780138782437614854049166249255736568727871405203145445713125141457815971906719680669523321542149265256106758378611063739777315811392360788175376029797932721269825408717805110046053475025830801735666025053018782363519728851583242122257222113884816515911284759104358378076912618894423920226431720769320072682426008082248956308563260250346169607126349143486172802052734691701212998376565765478873612338833736208815708858667413572099199755289440710553092927371890175584929 9"
                        },
                        "response": "3395374552774737796138400574489286232194160907278976118238127256446959000 9102"
                    },
                    {
                        "challenge": "5703182018262228562239054136393097106393215384893398417232915798440673752978 3",
                        "commitment": {
                            "A": "3791016204607672977184428548196498359352669714573091872452566090879032096527663410400776595077538437481164331076412177084592281680842075830146559512701291761126214147988323499906273008484878642563025635700721775136711288631658213720446967763322060250499729690324753312130026090331298933679859057829791839809682720373234542760330188417907659779997745925603722347631515678877517023464103655971088509806142726000543104631551428003910421116179796021946773009347470768138897227079122302246420933868382887239396495356845764010985092822066968938799168257816037336952796872538377419775242939845300771127396383613452631349598",
                            "B": "4893826855772125744585601525237912217118590434916280940573680800046829914082381722001544672989305053840671372245120961984944963033471996954351482262410925287058450281976400597023545057301234578300480529500423966874119263036217796067764175186758707287116545693117763386852927091968974260465973560318525784831063241147650855589496756689350021146008706296903559845164986103494903224165777669119065115711825871900109419207028266471804076627479440723013978303365199191781860188897138107245687382591199957193433178949080325473926067656318658572195332256196773134987537902149544563865372098826117345833336382662334518 87"
                        },
                        "response": "4231008676393307310488481609690024700128318777460933104467135980286026843 3131"
                    }
                ],
                [
                    {
                        "challenge": "5875989311843107206551245432949722975165510635746772518618185711364949086 39182",
                        "commitment": {
                            "A": "7427639384932734024745204235864953625736278461263403646741365993664667694195310749382670187491549188582295453664666239323772158817422344570655015050768998467100224042813393625113770419729661180509485220850231706592347158756549891743934526556471639391342029277737767717370609230961238652312367800269253994234556787325208443599773149596603231528682156435793785084209836127202290446000347651703261913579456442322697290587260061804409264074921254839925781974119070497257201115661768275991438229322988480791581636372699358700163602424065332447163996347551366660631319212792462360173330036943141202478094205041805889000095",
```

```
                                "B": "444710679420691127832399172412605670028309007638348034933068500289115795807987242716223071513878267265171732875817296142962687238037819431663483488615220031528334812303761458635494480619165082379720834637846110837670828364899721934210357823358954213803182955973950152819558646379232185661231821810526154350472322185652301495514055425284451128423294754970897425437128559104307621135005997906070906243867662130747523948479528391633772946137249485626312016744684756884188846035740507277921701875453532820670115022964733344691243776906285005389040810724773975916229951546388962155622455200219503994676844822886318523233"
                            },
                            "response": "25330282525289949805811494952385696411509198980977400031394612619929821095675"
                        },
                        {
                            "challenge": "25696731299118292270314184415999349979912194308726757008076447606200226489928",
                            "commitment": {
                                "A": "35680729539318297626044354112357816879616789112432166027416764109534905910585813604701773155707464129596188596923334943109074328997097439915457930422329831982860951611898029446774837881014904075958755010356363462208099556327087315831070691161887599748506511990233636048370101274509339689015242741705606551273282825412885185985899816705924120590636968206751928655389474491079949046316828622910401946469524503632699566323603971578455024445552237142456321868930922570697575151890731678545975698963211667590809399299456635829834556170386556764796873102089852165872739490077676465215264984509444356593975817931960905428 3",
                                "B": "25831788260191389552656533796163432298027129713086086555579099601736594930733659266458327398070277291885318320606664064691506786736453790688195660672006175226528367985370329470472422312688311681861595060564293134035224054740240693868301313093069860715456507601756607557990217434501643642175402444155711836720025032222665624515457775436237469246572658944121566634302000009581219830532243176330753597905718230001269656668840245046287962412438140127058943199517337297239465478621595595030617600600400184406906818528548909250348133005416076656334541646593138769063767587911424283054396692482754129896161955754426871243889 6"
                            },
                            "response": "22523921325438549160070638454109894120547758153225744877786024862904218984943"
                        }
                    ]
                ],
                "overall_proof": [
                    {
                        "challenge": "830244221750017599749957092937086164704578536065411681581127767399654364902 2",
                        "commitment": {
                            "A": "11291792263607996337911175675079126659722619604594624859475994404960453150214203005314666312147870020289582856722921233059523453457295377216745238676064205357108612780325262943635008012824457967728793751532109045271880446930625752389018322245848722151974710893940665583690833857422338703036471398734414608286431093156043912488609378582529986427504737083700399433477653063497106165814535177888342695606734124808041251383358233129471323968588128738528569618048150566715113833632525606702837086318625149051559351781558682601126117477054802457737471175339935475279959028605739555461873175413501267818167404925190977010913", 
                            "B": "55777716244662353227656484266305684592589182330251006551839704298853174387757313247960919764288517092518578767152548740815196862748957766830170517716504335654909161830026521478174343995934284826635310172436713646887473335083831258595730733038980337786065328416913674085091586783178334457871784496826558148872405813769706045470765145895243759571384684178009329580211584009418538796144624116110388045661639059036821201513479520982625427885964560308433408121234189079837752962318585029688475405020403057653696254220072735076019569307050166504205037740503025285592228837110259481782390808360305347014029402123396508551 86",
                            "response": "13337559624933807640300801406556251777362177737097061962278413507571142307284"
                        },
                        {
                            "challenge": "530271240308427252950443018415442654698791614746475004740727031532095897257 20",
                            "commitment": {
                                "A": "11944086599333640657128029867102030555472573707914607795277936296866090770332694034089235118536915378256004184542255064371737289901912796444469588989629877736993147128648707252463386901660573384217018159075102757286437595410524824177686071356611683882526875153183835410503878855543128249676762261746481311368973558168580479464102222087932173099411264106375098127208818183341551154548830020817835808110696483756656421064564282903532286923843535057406735371503667823531874123808088611572087176656345038435263087433126532649834220325255799442371689080488100237604773117885911109254195858873897440417598836644405791940087", 
                                "B": "35031587766673657110213317388260847835689325707240889923124354091953160736036799597905302185859917065718361178514152666743395785686050992812999642412456915161551399485488756856481922523987390750516202056606090471974945469234696837156763273001657856361650781797331664603890530171526516450166783032604121249811601638559536450970279284397518880094714635805768162985306712759250090049967323163189729870591907667365796115184290354567021356656672700264861686714463340622440171556728790164038114235772920476739122117891846330076183205247204020817722868552498375182545133407140649638891813739219810867803058464879151309975144",
                                "B": "10666116694844888232559528581592346257655330057172959634354028666838424871483"
                            },
                            "response": "1066611669484488823255952858159234625765533005717295963435402866683842487148 3"
                        }
                    ]
                }
            ],
            "election_hash": "XMrdm5yOYmS5Bm0E3W9QhrEBwrqSmdTNkWEDH2S/2M",
            "election_uuid": "56c99b16-9606-11ea-8335-6a9a48152285"
}
```