Multi-Key Shuffle: Network Application for Prover

Author: Aaron Kimmig <kimmiga@informatik.uni-freiburg.de> <academia@aaronkimmig.de>
Last Edited: 2023-12-11

Implementing prover component in network application for efficient Multi-Key Shuffle Argument

For a fast start, go to section "Configuration" > "Set Notebook Context and Kernel".

See
[Master's Thesis] Efficient Zero-Knowledge Multi-Key Verifiable Shuffles: Implementation, Security and Applications
[BünzDraft23] Bünz, B., Raykova, M., & Sarathy, J. (2023, Draft). Efficient Multi-Key Verifiable Shuffles from Short Arguments for Randomized Algorithms.
for Shuffle Argument and
[Bünz18] Bünz, B., Bootle, J., Boneh, D., Poelstra, A., & Maxwell, G. (2018). Bulletproofs: Short proofs for confidential transactions and more. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 315-334). IEEE.
for Inner Product argument.

Configuration options:

Shuffle Data
- `names`: List of names of users
- `secretKeys`: List of corresponding secret keys of users
- `senders`: Senders of secret messages (index into names and secretKeys)
- `secretMessages`: Secret Messages to be sent
- `receivers`: Receivers for secret messages (index into names and secretKeys)

Crypto & Protocol
- `useElGamal:` Choose between El Gamal and Elliptic Curve Cryptography (only EC is implemented; configuration option left for demonstration of El Gamal setup)
- `interactive:` Whether to use interactive protocol or Fiat-Shamir transform
- `p, q, (implicit: cofactor), g:` Trapdoor Function / Schnorr Group
- `p, n`$_{EC}$`, h`$_{EC}$`, (implicit: q), a`$_{EC}$`, b`$_{EC}$`, g:` Trapdoor Function / Elliptic Curve (Weierstrass representation)
- `useInnerProductProtocol:` Whether to use the communication-cost-efficient inner product protocol

– `rngMethod:` “OpenSSL”, “ExtendedCA”, ... (All of Mathematica’s options)
– `fixedNUMSRandomSeed:` Fixed random seed which will be used for calculating the generators for Pedersen Commitments

Network, Communication & Environment
– `myId`: Choose a name that identifies the prover. Could be replaced by a public key if a public key infrastructure was implemented
– `interactiveVerifierId:` ID of interactive verifier
– `room:` “address” of the proof and where messages are routed over
– `roomPassword:` password needed to access the room
– `inspectionEnabled`: Publish variables to Inspector for educational purposes
– `routerConfig`: Connection to message router and inspector
– `useLocalRouter`: Whether to use a self-hosted local router instance or a public router server on the internet
– `fiatShamirSingleKernel:` Set to True when using a mathematica test license (which allows only one kernel to be run simultaneously) and not running prover and verifier on different machines
– `proverKernelName:` Name of kernel this notebook shall be run on if fiatShamirSingleKernel = False
– `verbosity settings:` Set verbosity levels for different components

Verifier’s Notebook: “MultiKeyShuffle-Verifier.nb”

Start the router and inspector before running this notebook when using a local router:
`$ python3 RoomServer.py`
To get live inspection, visit http://localhost:11080 when running your local server or https://aaronkimmig.de/crypto-insight if you want to use the standard external server.

Reset – Clean up Notebook, Clear states

If fiatShamirSingleKernel is set in section “Configuration” run CLEAR ALL in the verifier’s notebook after this notebook has been run!

CREATE NEW KERNEL IF NEEDED:
Menu **>** Evaluation > Kernel Configuration Options > Add > Name: Prover > OK

The following helper actions are useful for cleanup and debugging. They are not required to correctly execute the protocols.

CLEAR ALL

In[ ]:=
```
FrontEndTokenExecute["DeleteGeneratedCells"];
(führe Front-End-Befehlselement aus)
Print["Deleted all generated output cells"];
(gib aus)
Print["Quit Kernel"];
(gib aus  beende Kernel)
Quit[];
(beende Kernel)
```

```
Deleted all generated output cells
```

```
Quit Kernel
```

DELETE ROOM (Can only be executed after initialization)

In[ ]:=
```
SendVariables["Router", {"__delete_room__" → True}];
                                                (wahr)
WaitForVariable["__delete_room__", "Router"];
```

RECONNECT (Can only be executed after initialization)

In[ ]:=
```
(*Reconnect with new socket*)
router = ConnectToRouter[routerConfig, True];
                                          (wahr)
```

CLEAR SAVED STATES (Can only be executed after initialization)

```
StateMachineClear[];
```

Configuration

Set Notebook Context and Kernel

- Using a payed license?
- YES: On your first run, make sure the kernel for the prover has been created: Menu **>** Evaluation > Kernel Configuration Options > Add > Name: Prover > OK
- NO: set option fiatShamirSingleKernel = True and read the instructions in the comment above it.

- To run the whole notebook, place the cursor into this cell, press “Shift-Enter” and click “Yes” to evaluate the whole notebook. Select “No” to only evaluate this cell. Go on to the next cells to run them one by one with “Shift-Enter”.

- To clean up the notebook and start with a new run, execute the first cell (“Shift-Enter”) in section “Reset”. Re-evaluating cells is possible because a state machine allows protocol rewinding.

Re-evaluate after changes

In[449]:=

```
(*Whether to run notbook on default kernel.
Useful with Mathematica Test License where only a single kernel can be run at a time.
Remark: Running the interactive protocol is not possible on a single kernel!
Also apply this setting to the verifier and run it after the prover.
Quit Kernel after prover has been run and before verifier is started!
interactive = False has to be set in the configuration.*)
fiatShamirSingleKernel = False;(*Default: False*)
(*Name of kernel this notebook should be run on.
Does not take effect if fiatShamirSingleKernel = True (the notebook will then be run on Kernel
proverKernelName = "Prover";(*Default: "Prover"*)

(*=== don't change between here >>> ===*)
(*Context*)
Print["Setting Cell Context to Notebook only"]
SetOptions[EvaluationNotebook[],CellContext→Notebook];
(*Kernel*)
kernelName = If[fiatShamirSingleKernel,"Local",proverKernelName];
(*Make sure that a kernel with this name has been created via Menu→Evaluation→Kernel Configur
SetOptions[EvaluationNotebook[],Evaluator→kernelName];
Print["Evaluating on Kernel named \""<>kernelName<>"\""]
(*=== <<< and here ===*)
```

```
Setting Cell Context to Notebook only
```

```
Evaluating on Kernel named "Prover"
```

User's Keys and Messages to be Shuffled

In[8]:=

```
(*secret keys*)
names = {"Alice", "Bob", "Charly", "Dave"};
secretKeys = {
    "Alice' Secret Key", (*1*)
    "Bobs Secret Key", (*2*)
    "Charlie's Secret Key", (*3*)
    "Dave's Secret Key" (*4*)
};
(*senders with corresponding receivers and their secret messages to be shuffled*)
(*Example:
Alice → "Wien" → Bob
Bob → "München" → Dave
Charly → "Bozen" → Dave*)
senders = {1, 2, 3};
secretMessages = {"Wien", "München", "Bozen"};
receivers = {2, 4, 4};
```

Crypto & Protocol

In[13]:=

```
(*Whether to use El Gamal or Elliptic Curves*)
useElGamal = False;(*Only case "False" is implemented (Elliptic Curve Cryptography). El Gamal
(*Whether to use the interactive protocol or apply Fiat-Shamir transform*)
interactive = True;
(*trapdoor function configuration*)
cryptFuncs = <|
    (*y^2 ≡p x^3 + 7*)
    "EllipticCurve"→<|
        "curve_representation"→"Weierstrass",
        (*prime modulus*)
        "p"→2^256-2^32-2^9-2^8-2^7-2^6-2^4-1,
        (*linear coefficient*)
        "a"→0,
         (*constant coefficient*)
        "b"→7,
        (*number of points on elliptic curve*)
         "n"→Interpreter["HexInteger"]@"FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E
        (*cofactor*)
        "h"→1,
        (*Standard generator point*)
         "g"→{
            Interpreter["HexInteger"]@"79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F281
            Interpreter["HexInteger"]@"483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08
        }
    |>,
    "ElGamal"→<|
        (*prime modulus*)
        "p"→104171412955797345374825306094587137358185828944419116766145103921246769115772826
        (*prime order of subgroup*)
        "q"→11549553772186584188675359812679062341080376555551416651626700667761738457273 3,
        (*generator for subgroup*)
        "g"→16225073285608633302419870876955211912413277113870123069832109110376611008557169 91
    |>
|>;
(*Whether to use the inner product protocol for logarithmic communication cost; set to True if
useInnerProductProtocol = True;(*Default: True*)
(*How random numbers should be generated, choose from
"ExtendedCA" (built-in pseudo random number generator) or
"OpenSSL", (cryptographic random number generator from OpenSSL)
(*to be implemented: "DevRandom" (use system entropy from /dev/random)*)
Automatically set to "ExtendedCA" if a fixed random seed is used for the prover to demonstrate
rngMethod = "OpenSSL";(*Default: "OpenSSL"*)
(*Fixed random seed which will be used for calculating the generators for Pedersen Commitments
fixedNUMSRandomSeed = 314159000001;(*Default: 314159000001*)
```

Network, Communication & Environment

In[19]:=
```
(*Unique ID*)
myId = "Bob-Shuffle-Pro";
(*ID of interactive verifier; needed if Fiat-Shamir is disabled*)
interactiveVerifierId = "Alice-Shuffle-Ver";
(*Room the communication is routed over*)
room = "BobsBPShuffle2";
roomPassword = "mediumBPShuffle";
(*Enable/Disable publishing (secret) variables to Inspector for educational purposes*)
inspectionEnabled = True;(*Default: True*)
(*Connection to router*)
useLocalRouter = False;
routerConfig = <|
    "Host"→If[useLocalRouter,"127.0.0.1",TextString[HostLookup["aaronkimmig.de"][[1]][[1]]],
    "Port"→25080,
    "Password"→"Drehkreuz64",
    "ConnectionPassword"→"My name is Bob"
|>;
(*Verbosity Levels: 0, 1, 2*)
stateMachineVerbosity = 0;
fiatShamirVerbosity = 0;
```

Initialization and Setup

Symbolize all Variables with Special Appearance

In[28]:=
```
(*Load notation package for pretty variables*)
Needs["Notation`"]
SymbolQ = MatchQ[#, t_Symbol /; AtomQ[t]] &;
If[SymbolQ[guard_symbolize],
Print["Special symbols already set up"],
(*Else: Symbolize variables with special appearance*)
Symbolize[ guard_symbolize ];
(*User's secrets*)
Symbolize[ x⃗ ];
Symbolize[ γ⃗ ];
Symbolize[ m⃗ ];
(*Prover*)
(*Elliptic curve*)
Symbolize[ a_EC ];
Symbolize[ b_EC ];
Symbolize[ h_EC ];
Symbolize[ n_EC ];
```

```
(*generators*)
Symbolize[ $\vec{g}$ ];
(*public input and output values to shuffle argument*)
Symbolize[ $\vec{h}$ ];
Symbolize[ $\vec{b}$ ];
Symbolize[ $\vec{c}$ ];
Symbolize[ $\vec{d}$ ];
Symbolize[ $\vec{h'}$ ];
Symbolize[ $\vec{b'}$ ];
Symbolize[ $\vec{c'}$ ];
Symbolize[ $\vec{d'}$ ];
Symbolize[ $\vec{h^*}$ ];
Symbolize[ $\vec{b^*}$ ];
Symbolize[ $\vec{c^*}$ ];
Symbolize[ $\vec{d^*}$ ];
(*commitments to secret shuffle s and s^n*)
(*Symbolize[ $\sigma_V$ ];*)
Symbolize[ $\sigma_W$ ];
(*Helper scalars and vectors*)
Symbolize[ $\vec{y^n}$ ];
Symbolize[ $\vec{y_z^{n-1}}$ ];
Symbolize[ $y^{-1}$ ];
Symbolize[ $\vec{y^{-n}}$ ];
Symbolize[ $\vec{w^n}$ ];
Symbolize[ $\vec{w_0^{n-1}}$ ];
(*shuffle protocol*)
Symbolize[ $\pi^{-1}$ ];
Symbolize[ $\vec{k}$ ];
Symbolize[ $\hat{k}$ ];
Symbolize[ $\bar{k}$ ];
Symbolize[ $A_{R,h}$ ];
```

```
Symbolize[ A_{R,b} ];
Symbolize[ A_{R,c} ];
Symbolize[ A_{R,d} ];
Symbolize[ \vec{a}_L ];
Symbolize[ \vec{a}_R ];
Symbolize[ \vec{s}_L ];
Symbolize[ \vec{s}_R ];
Symbolize[ \rho_h ];
Symbolize[ \rho_b ];
Symbolize[ \rho_c ];
Symbolize[ \rho_d ];
Symbolize[ A_L ];
Symbolize[ S_L ];
Symbolize[ S_{R,h} ];
Symbolize[ S_{R,b} ];
Symbolize[ S_{R,c} ];
Symbolize[ S_{R,d} ];
Symbolize[ \vec{l}_0 ];
Symbolize[ \vec{l}_2 ];
Symbolize[ \vec{r}_1 ];
Symbolize[ \vec{r}_3 ];
Symbolize[ \delta_{yz} ];
Symbolize[ t_1 ];
Symbolize[ t_3 ];
Symbolize[ t_5 ];
Symbolize[ \vec{l} ];
Symbolize[ \vec{r} ];
Symbolize[ \tau_3 ];
Symbolize[ \tau_5 ];
Symbolize[ \tau_x ];
Symbolize[ T_3 ];
```

```
Symbolize[ T_5 ];
Symbolize[ \hat{t} ];
Symbolize[ \mu_h ];
Symbolize[ \mu_b ];
Symbolize[ \mu_c ];
Symbolize[ \mu_d ];
Symbolize[ P_h^+ ];
Symbolize[ P_b^+ ];
Symbolize[ P_c^+ ];
Symbolize[ P_d^+ ];
(*PR protocol*)
Symbolize[ \overrightarrow{a_{L,w}} ];
Symbolize[ \overrightarrow{a_{R,w}} ];
Symbolize[ \overrightarrow{s_{L,w}} ];
Symbolize[ \overrightarrow{s_{R,w}} ];
Symbolize[ \alpha_w ];
Symbolize[ \beta_w ];
Symbolize[ \gamma_w ];
Symbolize[ A_w ];
Symbolize[ S_w ];
Symbolize[ \overrightarrow{l_{0,w}} ];
Symbolize[ \overrightarrow{l_{1,w}} ];
Symbolize[ \overrightarrow{r_{0,w}} ];
Symbolize[ \overrightarrow{r_{1,w}} ];
Symbolize[ \delta_{yzw} ];
Symbolize[ t_{0,w} ];
Symbolize[ t_{1,w} ];
Symbolize[ t_{2,w} ];
Symbolize[ \overrightarrow{l_w} ];
Symbolize[ \overrightarrow{r_w} ];
Symbolize[ \tau_{1,w} ];
```

```
Symbolize[ τ_{2,W} ];
Symbolize[ τ_{x,W} ];
Symbolize[ T_{1,W} ];
Symbolize[ T_{2,W} ];
Symbolize[ t̂_W ];
Symbolize[ μ_W ];
Symbolize[ P⁺_W ];
(*inner product protocol*)
Symbolize[ n_2 ];
Symbolize[ n_{pow2} ];
Symbolize[ g' ];
Symbolize[ u_{IP} ];
Symbolize[ n_0 ];
Symbolize[ k_2 ];
Symbolize[ k_0 ];
Symbolize[ P*_h ];
Symbolize[ P*_b ];
Symbolize[ P*_c ];
Symbolize[ P*_d ];
Symbolize[ P*_W ];(*PR*)
Symbolize[ P´_h ];
Symbolize[ P´_b ];
Symbolize[ P´_c ];
Symbolize[ P´_d ];
Symbolize[ P´_W ];(*PR*)
Symbolize[ P_{2,h} ];
Symbolize[ P_{2,b} ];
Symbolize[ P_{2,c} ];
Symbolize[ P_{2,d} ];
Symbolize[ P_{2,W} ];(*PR*)
Symbolize[ P_{next,h} ];
Symbolize[ P_{next,b} ];
```

```
Symbolize[ P_{next,c} ];
Symbolize[ P_{next,d} ];
Symbolize[ P_{next,W} ];(*PR*)
Symbolize[ \vec{a}_2 ];
Symbolize[ \vec{a}_{IP} ];
Symbolize[ \vec{a}_{lo} ];
Symbolize[ \vec{a}_{hi} ];
Symbolize[ \vec{a}_{next} ];
Symbolize[ \vec{b}_2 ];
Symbolize[ \vec{b}_{IP} ];
Symbolize[ \vec{b}_{lo} ];
Symbolize[ \vec{b}_{hi} ];
Symbolize[ \vec{b}_{next} ];
(*Symbolize[ c_2 ];*)
Symbolize[ \vec{a}_{2,W} ];(*PR*)
Symbolize[ \vec{a}_W ];(*PR*)
Symbolize[ \vec{a}_{lo,W} ];(*PR*)
Symbolize[ \vec{a}_{hi,W} ];(*PR*)
Symbolize[ \vec{a}_{next,W} ];(*PR*)
Symbolize[ \vec{b}_{2,W} ];(*PR*)
Symbolize[ \vec{b}_W ];(*PR*)
Symbolize[ \vec{b}_{lo,W} ];(*PR*)
Symbolize[ \vec{b}_{hi,W} ];(*PR*)
Symbolize[ \vec{b}_{next,W} ];(*PR*)
Symbolize[ \vec{c}_W ];(*PR*)
Symbolize[ \vec{G}_2 ];
Symbolize[ \hat{G} ];
Symbolize[ \vec{G}_{lo} ];
Symbolize[ \vec{G}_{hi} ];
```

```
Symbolize[ $\overrightarrow{G_{next}}$ ];
Symbolize[ $\vec{H}_2$ ];
Symbolize[ $\vec{H}$ ];
Symbolize[ $\overrightarrow{H_{lo}}$ ];
Symbolize[ $\overrightarrow{H_{hi}}$ ];
Symbolize[ $\overrightarrow{H_{next}}$ ];
Symbolize[ $\vec{B}_2$ ];
Symbolize[ $\vec{B}$ ];
Symbolize[ $\overrightarrow{B_{lo}}$ ];
Symbolize[ $\overrightarrow{B_{hi}}$ ];
Symbolize[ $\overrightarrow{B_{next}}$ ];
Symbolize[ $\vec{C}_2$ ];
Symbolize[ $\vec{C}$ ];
Symbolize[ $\overrightarrow{C_{lo}}$ ];
Symbolize[ $\overrightarrow{C_{hi}}$ ];
Symbolize[ $\overrightarrow{C_{next}}$ ];
Symbolize[ $\vec{D}_2$ ];
Symbolize[ $\vec{D}$ ];
Symbolize[ $\overrightarrow{D_{lo}}$ ];
Symbolize[ $\overrightarrow{D_{hi}}$ ];
Symbolize[ $\overrightarrow{D_{next}}$ ];
Symbolize[ $L_h$ ];
Symbolize[ $L_b$ ];
Symbolize[ $L_c$ ];
Symbolize[ $L_d$ ];
Symbolize[ $L_W$ ];(*PR*)
Symbolize[ $L_{2,h}$ ];
Symbolize[ $L_{2,b}$ ];
Symbolize[ $L_{2,c}$ ];
```

```
Symbolize[ L_{2,d} ];
Symbolize[ L_{2,W} ];(*PR*)
Symbolize[ R_h ];
Symbolize[ R_b ];
Symbolize[ R_c ];
Symbolize[ R_d ];
Symbolize[ R_W ];(*PR*)
Symbolize[ R_{2,h} ];
Symbolize[ R_{2,b} ];
Symbolize[ R_{2,c} ];
Symbolize[ R_{2,d} ];
Symbolize[ R_{2,W} ];(*PR*)
Symbolize[ u_2 ];
Symbolize[ u^{-1} ];
Symbolize[ a_0 ];
Symbolize[ b_0 ];
Symbolize[ c_0 ];
Symbolize[ a_{0,W} ];(*PR*)
Symbolize[ b_{0,W} ];(*PR*)
Symbolize[ c_{0,W} ];(*PR*)
Symbolize[ G_0 ];
Symbolize[ H_0 ];
Symbolize[ B_0 ];
Symbolize[ C_0 ];
Symbolize[ D_0 ];
Symbolize[ P_{0,h} ];
Symbolize[ P_{0,b} ];
Symbolize[ P_{0,c} ];
Symbolize[ P_{0,d} ];
Symbolize[ P_{0,W} ];(*PR*)
Print["Finished setting up special symbols"]
];
```

```
Finished setting up special symbols
```

Apply Configuration, Load Libraries, Set up Network and Communication

Re-evaluate after changes to configuration

In[31]:=

```
(*Check Configuration*)
If[fiatShamirSingleKernel,
    If[interactive,
        Print["fiatShamirSingleKernel only works with Fiat-Shamir activated, but it is not. Fo
        interactive = False;
    ];
];
(*Trapdoor function*)
If[useElGamal,
(*Load ElGamal library*)
    Print["Looking for SchnorrPrimes library: "<>TextString[FindFile["SchnorrPrimes`"]]];
    Needs["SchnorrPrimes`"],
(*Else*)
(*Load EC library*)
    Print["Looking for elliptic curve library with overloaded + and * operators (ECOverloaded
    Needs["ECOverloaded`"];
];
(*Load Sigma Tools library*)
Print["Looking for Sigma Protocol Tools library (SigmaTools): "<>TextString[FindFile["SigmaTo
Needs["SigmaTools`"];
(*Fiat-Shamir*)
If[interactive,
    semanticsOfRandomChallenge = "Random Challenge";
    (*Default setting is no Fiat-Shamir transform; just to be explicit*)
    DisableFiatShamir[];
(*Else*),
    semanticsOfRandomChallenge = "Fiat-Shamir transform\nof Random Challenge";
    EnableFiatShamir[];
    Print["Looking for Fiat-Shamir library (FiatShamir): "<>TextString[FindFile["FiatShamir`"
    Needs["FiatShamir`"];
    Print["Non-interactive mode. Using Fiat-Shamir heuristic."];
];
(*Success/failure creating proof*)
ProofFinished[] := Module[{},
    Print["Creating proof finished."];
]
Error[reason_:""] := Module[{},
    Print[If[reason=="","Error.","Error: "<>reason]];
    FrontEndTokenExecute["EvaluatorAbort"];
]
(*Random Number Generator*)
SetRNGMethod[rngMethod];
SetFixedRandomSeeds[False];
SeedRandom[Method→rngMethod];
SetStateMachineVerbosity[stateMachineVerbosity];
SetFiatShamirVerbosity[fiatShamirVerbosity];
(*Communication setup*)
SetMyRole["Prover"];
```

```
SetMyId[myId];
SetRoom[room];
SetInspection[inspectionEnabled];
(*Network: set up connection to router / force authorization but not reconnection*)
router = ConnectToRouter[routerConfig,False,True];
(*Network: join room*)
roomConfig = {
    "password"→roomPassword,
    "ownership_type"→"creator",
    "create_if_non_existing"→True,
    "external_keys"→{
        "_verification_result_",
        "_inspection_request_",
        "_inspection_result_"
    }
};
If[interactive,
    AppendTo[roomConfig, "ids_allowed"→{interactiveVerifierId}];
    AppendTo[roomConfig, "role_restrictions"→{myId→"Prover", interactiveVerifierId→"Interacti
(*Else: Fiat-Shamir*),
    AppendTo[roomConfig, "role_restrictions"→{myId→"Prover"}];
];
StateMachineClear[];
roomInfo = JoinRoomAndWaitUntilComplete[roomConfig];
memberIds = roomInfo["members"];
(*Verify room and members*)
If[interactive,
    If[Length[memberIds]≠2,
        Print["Assertion failure: Expecting two members in room '"<>room<>"' but members are
    (*Else If*)
    If[!(memberIds⟦1⟧==myId && memberIds⟦2⟧==interactiveVerifierId) && !(memberIds⟦1⟧==interac
        Print["Assertion failure: Expecting to be member of room '"<>room<>"' but members are
    ]];
(*Else: Fiat-Shamir*),
    If[Length[memberIds]≠1||memberIds⟦1⟧≠myId,
        Print["Assertion failure: Expecting to be the only member in room '"<>room<>"' but: "
    ];
];
StateMachineSave["Init"];
```

```
Looking for elliptic curve library with overloaded + and * operators (ECOverloaded):
  C:\Users\Aaron\AppData\Roaming\Mathematica\Applications\ECOverloaded.wl

Looking for Sigma Protocol Tools library (SigmaTools):
  C:\Users\Aaron\AppData\Roaming\Mathematica\Applications\SigmaTools.wl

Network connection to router:
```

SocketObject[Foreign IPAddress: 5.189.143.94 Foreign Port: 25080 Protocol: TCP (Client) UUID: ff2fbd0e-c848-4491-97b1-9a18b3c7f486]

```
Authorizing, waiting for confirmation ...

Waiting to receive __authorize__ ...

Handling Event: success: __authorize__ (Router): Authorization successful
```

```
Sending message:
Prover@Bob-Shuffle-Pro:Router:BobsBPShuffle2:json:{"__join_room__":{"password":"
  mediumBPShuffle","ownership_type":"creator","create_if_non_existing":true,"external_keys":
  ["_verification_result_","_inspection_request_","_inspection_result_"],"ids_allowed":["
  Alice-Shuffle-Ver"],"role_restrictions":{"Bob-Shuffle-Pro":"Prover","Alice-Shuffle-Ver":"
  InteractiveVerifier"}}}

Joining room 'BobsBPShuffle2'. Waiting for
  confirmation and for all members to have joined to room ...

Waiting to receive __join_room__, __room_complete__ ...

Handling Event: success: __join_room__ (Router): Created and joined room 'BobsBPShuffle2'

Handling Event: success: __member_joined__ (Router):
  Event Data: Alice-Shuffle-Ver
  Keys: {__member_joined__, _Message, _Valid, _SenderRoleAtId,
  _SenderRole, _SenderId, _ReceiverRoleAtId, _ReceiverRole, _ReceiverId,
  _UniqueKey, _Room, _DataFormat, _Data, _UnderscoreVars1, _UnderscoreVars2}

Handling Event: success: __room_complete__ (Router):
  Event Data: <|Length:1|>
  Keys: {__room_complete__, _Message, _Valid, _SenderRoleAtId,
  _SenderRole, _SenderId, _ReceiverRoleAtId, _ReceiverRole, _ReceiverId,
  _UniqueKey, _Room, _DataFormat, _Data, _UnderscoreVars1, _UnderscoreVars2}
```

Check Input Data

Performing some sanity checks on input data.
The size of the shuffle n is the length of the list of secret messages and has to match the sender and receiver lists which by them have to point to a valid index in the list of secret keys.

In[55]:=
```
inputError = "";

n = Length[secretMessages];
usersCount = Length[secretKeys];
If[Length[senders] ≠ n, inputError = "Mismatch between number of secret messages and senders"]
If[MemberQ[senders, # ≤ 0 || # > usersCount &], inputError = "Invalid sender index"];
If[Length[receivers] ≠ n, inputError = "Mismatch between number of secret messages and senders
If[MemberQ[receivers, # ≤ 0 || # > usersCount &], inputError = "Invalid receiver index"];
If[Length[names] ≠ usersCount, inputError = "Mismatch between number of secret keys and user n

Print[Grid[{
    {Style["Input Value",Bold],Style["Value/Equality",Bold]},
     {"Input Valid?",If[inputError==="","Yes","No: "<>inputError]},
    {"Size of Shuffle",n},
    {"Secret Messages",secretMessages},
    {"Number of Users",usersCount},
    {"Secret Keys",Thread[names→secretKeys]},
    {"Message Routes",Thread[names[[senders]]→Thread[secretMessages→names[[receivers]]]]}
}, Alignment→{{Left,Left,Left,Left}},Frame→All]];

If[inputError ≠ "", Error[inputError]];
```

Input Value	Value/Equality
Input Valid?	Yes
Size of Shuffle	3
Secret Messages	{Wien, München, Bozen}
Number of Users	4
Secret Keys	{Alice → Alice' Secret Key, Bob → Bobs Secret Key, Charly → Charlie's Secret Key, Dave → Dave's Secret Key}
Message Routes	{Alice → Wien → Bob, Bob → München → Dave, Charly → Bozen → Dave}

Trapdoor Function: El Gamal or Elliptic Curve

Set up crypto algorithm. The group parameters may be modified.

In[65]:=
```
StateMachineRestore["Init"];
GiveInsight[{"__clear_inspection__"→True}];
WaitForVariable["__clear_inspection__","Inspector"];
setupParameters = <|
    "room"→room,
    "prover"→myId,
    "interactive"→interactive,
    "n"→n
|>;
If[interactive, setupParameters["verifier"] = interactiveVerifierId];
If[useElGamal,
(*Use Schnorr-Prime-Generator.nb to generate your own Schnorr Primes*)
    setupParameters["encryption_method"] = "ElGamal";
    cryptFunc = cryptFuncs["ElGamal"];
    Scan[
        (setupParameters["crypt_"<>#] = cryptFunc[#])&,
        Keys[cryptFunc]
    ];
```

```
    p = cryptFunc["p"];
    h = cryptFunc["h"];
    g = cryptFunc["g"];
    q = (p - 1) / h;
    pBits = Length[IntegerDigits[p,2]];
    qBits = Length[IntegerDigits[q,2]];
    entropyParameters = <|"group"→qBits,"scalar"→qBits|>;
    setupParameters["entropy_parameters"] = entropyParameters;
    securityParameters = <|"group"→pBits,"scalar"→qBits|>;
    setupParameters["security_parameters"] = securityParameters;
    SetCostSpecification[securityParameters];
    modq = Mod[#,q]&;
    modinvq = ModularInverse[#,q]&;
    powermodq = PowerMod[#1,#2,q]&;
    modp = Mod[#,p]&;
    modinvp = ModularInverse[#,p]&;
    powermodp = PowerMod[#1,#2,p]&;
    Print[Grid[{
        {"p is prime",PrimeQ[p]},
        {"bits of p",pBits},
        {"q is prime",PrimeQ[q]},
        {"bits of q",qBits},
        {"bits of cofactor",Length[IntegerDigits[cofactor,2]]},
        {"cofactor * q ≟ p - 1",cofactor*q==p-1},
        {"g^q ≟_p 1",PowerMod[g,q,p]==1}
    },Alignment→{{Left,Left}},Frame→All]];
(*Else*),
(*Use Elliptic Curve*)
    setupParameters["encryption_method"] = "EllipticCurve";
    cryptFunc = cryptFuncs["EllipticCurve"];
    Scan[
        (setupParameters["crypt_"<>#] = If[ListQ[cryptFunc[#]],
            ecPnt[cryptFunc[#][[1]], cryptFunc[#][[2]]],
            cryptFunc[#]
        ])&,
        Keys[cryptFunc]
    ];
    If[cryptFunc["curve_representation"] ≠ "Weierstrass", Error["Only Weierstrass representat
    (*EC modulus*)
    p = cryptFunc["p"];
    (*linear coefficient*)
    a_EC = cryptFunc["a"];
    (*constant coefficient*)
    b_EC = cryptFunc["b"];
    (*number of points on elliptic curve*)
    n_EC = cryptFunc["n"];
    (*cofactor*)
    h_EC = cryptFunc["h"];
    (*group modulus*)
    q = n_EC / h_EC;
    (*standard generator point*)
    g = ecPnt[cryptFunc["g"][[1]], cryptFunc["g"][[2]]];
    pBits = Length[IntegerDigits[p,2]];
```

```
    qBits = Length[IntegerDigits[q,2]];
    entropyParameters = <|"group"→qBits,"scalar"→qBits|>;
    setupParameters["entropy_parameters"] = entropyParameters;
    securityParameters = <|"group"→pBits+1(*sign bit*),"scalar"→qBits|>;
    setupParameters["security_parameters"] = securityParameters;
    SetCostSpecification[securityParameters];
    setEC[ecCurve[a_EC,b_EC,{p,h_EC}]];
    compressPoint[point_ecPnt] := point[[1]] + If[point[[2]] > p/2, 2^pBits, 0];
    modq = Mod[#,q]&;
    modinvq = ModularInverse[#,q]&;
    powermodq = PowerMod[#1,#2,q]&;
    Print[Grid[{
        {"p is prime",PrimeQ[p]},
        {"bits of p",pBits},
        {"|n_EC - (p+1)| <= 2√n_EC;\n(n_EC = number of points on EC)\n(Hasse's Theorem on ECs)",
        {"q is prime",PrimeQ[q]},
        {"bits of q",qBits},
        {"h_EC",h_EC},
        {"h_EC * q ≟ n_EC",h_EC * q == n_EC},
        {"qg = O",q * g == O}
    },Alignment→{{Left,Left}},Frame→All]];

If[!interactive,
    setupParameters["nums_seed"] = fixedNUMSRandomSeed;
    Scan[
        FiatShamirAdd[
            #,
            If[StringQ[setupParameters[#]],
                StringToInteger[setupParameters[#]],
                setupParameters[#]
            ]
        ]&,
        (*sort to ensure fixed order*)
        Sort[Keys[setupParameters]]
    ];
];

TellVerifier[{"setup"→setupParameters}];
GiveInsight[{"__setup__"→setupParameters}];

If[!interactive, Print[FiatShamirGrid[]]];
ProcessNewMessages[];
StateMachineSave["Setup"];
```

```
Waiting to receive __clear_inspection__ from Inspector ...

Handling Event: success: __clear_inspection__
  (Inspector): Clearing values in BobsBPShuffle2 successful
```

p is prime	True
bits of p	256
$\lvert n_{EC} - (p+1) \rvert <= 2\sqrt{n_{EC}}$; (n_{EC} = number of points on EC) (Hasse's Theorem on ECs)	True
q is prime	True
bits of q	256
h_{EC}	1
$h_{EC} * q \stackrel{?}{=} n_{EC}$	True
qg = O	True

NUMS Generators for Pedersen Commitments

"NUMS" ("nothing up my sleeve") generators for Pedersen Commitments: Every sceptical individual will be able to create the same generators based on the public fixed random seed 314159000001 and *n*.

In[77]:=
```
StateMachineRestore["Setup"];

(*Standard "NUMS" generator point g is already given*)
(*Get more "NUMS" generator points with pseudorandom number generator initialized by fixed cor
(*Standard behaviour*)
BlockRandom[
    SeedRandom[fixedNUMSRandomSeed,Method→"ExtendedCA"];
    numsGenerators = ecRandomGenerators[p,h_EC,n+2];
];
h = numsGenerators⟦1⟧;
g⃗ = numsGenerators⟦2;;n+1⟧;
g' = numsGenerators⟦n+2⟧;
GiveInsight[{"h"→h,"gvec"→g⃗,"g'"→g'}];
Print[Grid[Join[
    {
        {Style["Name",Bold],Style["Knowledge",Bold],Style["Value",Bold]},
        {"g","public",g},
        {"h","public",h}
    },
    MapIndexed[{"g⃗."<>IntegerString[First[#2]],"public (implicit)",#1}&,g⃗],
    {
        {"g'","public",g'}
    }
], Alignment→{{Left,Left,Left}},Frame→All]]

If[!interactive,
    numsParameters = Join[
        <|
            (*Already added:
            "nums_seed"→fixedNUMSRandomSeed*)
            "nums_method"→StringToInteger["Mathematica-ExtendedCA"],
            "g"→compressPoint[g],
            "h"→compressPoint[h]
        |>,
        Association[Map["g."<>IntegerString[#]→compressPoint[g⃗⟦#⟧]&, Range[n]]],
        <|
            "g'"→compressPoint[g']
        |>
    ];
    Scan[
        FiatShamirAdd[#, numsParameters[#], 0]&,
        Sort[Keys[numsParameters]]
    ];
    Print[FiatShamirGrid[]];
]

ProcessNewMessages[];
StateMachineSave["NUMS"];
```

Name	Knowledge	Value
g	public	ecPnt[55 066 263 022 277 343 669 578 718 895 168 534 326 250 603 453 777 594 175 500 - 187 360 389 116 729 240, 32 670 510 020 758 816 978 083 085 130 507 043 184 471 273 380 659 243 275 938 - 904 335 757 337 482 424]
h	public	ecPnt[96 137 567 500 391 445 872 529 956 175 960 328 224 372 161 700 720 340 121 622 - 040 718 272 419 693 213, 70 732 012 083 304 338 620 554 688 440 613 834 674 667 959 557 579 739 145 719 - 658 468 136 375 884 866]
$\vec{g}$.1	public (implicit)	ecPnt[101 548 470 124 358 210 188 072 679 181 678 188 450 387 789 916 654 718 462 374 - 321 277 161 805 765 354, 70 108 350 633 035 199 759 065 376 354 370 719 210 357 510 544 392 766 796 027 - 711 414 587 086 150 112]
$\vec{g}$.2	public (implicit)	ecPnt[81 881 281 191 882 355 160 881 140 819 926 411 859 223 579 216 161 786 219 247 - 020 789 084 841 886 435, 40 551 526 063 420 644 421 580 965 386 725 729 859 544 147 053 123 598 525 382 - 531 556 934 666 119 757]
$\vec{g}$.3	public (implicit)	ecPnt[27 427 957 168 767 222 510 921 650 620 077 570 798 709 753 797 557 336 240 233 - 137 618 475 833 226 690, 42 650 441 509 520 284 448 005 737 515 710 331 630 163 209 846 762 957 134 645 - 512 392 724 356 208 176]
g'	public	ecPnt[56 472 720 079 496 714 458 128 130 368 877 680 293 647 814 114 642 090 837 679 - 403 063 618 918 620 862, 14 095 742 162 302 059 280 857 313 602 183 952 549 169 355 861 567 402 651 092 - 841 186 912 433 952 389]

Register Event Handlers for Verification Results and Pedersen Commitment Inspection Requests

Functions will be called after the proof has been finished

Reveal Pedersen Commitments V, W, A_L, S_L, $S_{R,h}$, $S_{R,b}$, $S_{R,c}$, T_3 and T_5 when requested.

In[87]:=
```
GenericParseResult[action_String, result_]:=
    action<>" "<>
    If[result["status"] == "success",
        "succeeded",
        "failed"
    ]<>
    If[KeyExistsQ[result, "msg"],
        ": "<>result["msg"],
        "!"
    ]
SetEventHandler["_verification_result_", Function[{msgParsed},
    Print[
        "Received verification result from "<>msgParsed["_SenderRoleAtId"]<>
        ": "<>GenericParseResult["Verification", msgParsed["_verification_result_"]]
```

```
    ];
]];

SetEventHandler["_inspection_request_", Function[{msgParsed},
    Print[
        "Received inspection request from "<>msgParsed["_SenderRoleAtId"]<>
        ". Revealing secrets of Pedersen commitments V, W, A_W, S_W, A_L, S_L, S_R,h, S_R,b, S_R,c, S_R,d,
    ];
    inspectionReply = {
        "s"→s,
        "sigmaW"→σ_W,
        "alphaW"→α_W,
        "betaW"→β_W,
        "gammaW"→ɣ_W,
        "pi"→π,
        "alpha"→α,
        "beta"→β,
        "rhoh"→ρ_h,
        "rhob"→ρ_b,
        "rhoc"→ρ_c,
        "rhod"→ρ_d,
        "sL"→⃗s_L,
        "sR"→⃗s_R,
        "t3"→t_3,
        "tau3"→τ_3,
        "t5"→t_5,
        "tau5"→τ_5,
        "t1W"→t_1,W,
        "tau1W"→τ_1,W,
        "t2W"→t_2,W,
        "tau2W"→τ_2,W
    };
    SendVariables[
        msgParsed["_SenderRoleAtId"],
        {"_inspection_reply"→inspectionReply}
    ];
]];

SetEventHandler["_inspection_result_", Function[{msgParsed},
    Print[
        "Received inspection result from "<>msgParsed["_SenderRoleAtId"]<>
        ": "<>GenericParseResult["Inspection", msgParsed["_inspection_result_"]]
    ];
]];
```

Users Prepare Their Messages for the Shuffler

Calculate $\vec{h}, \vec{b}, \vec{c}$ from $\vec{x}, \vec{\gamma}, \vec{m}$

The senders who want their messages be anonymized by using the multi-key verifiable shuffle encrypt their messages. Actually, this is done by separate clients. These calculations were added to

the shuffler's notebook for simplicity.

Secrets of each user:

$\vec{x}$: secret keys of users

$\vec{\gamma}$: secret blinding values

$\vec{m}$: secret messages

Posted to the public bulletin board

$\vec{h}$: public keys of receivers - to allow receivers to identify their messages

$\vec{b}$: commitments to blinding values - ElGamal randomizers

$\vec{c}$: blinded commitments to messages - ElGamal message

$\vec{d}$: public keys of senders - to allow receivers to reply

$\vec{h}, \vec{b}, \vec{c}, \vec{d}$ form the common reference string (CRS) together with g and $\vec{g}$.

In[91]:=
```
StateMachineRestore["NUMS"];

(*Users: Setup*)
(*secret keys of receivers*)
x⃗ = StringToInteger /@ (secretKeys[[#]] & /@ receivers);
(*public keys of receivers - to allow receivers to identify their messages*)
h⃗ = x⃗ * g;
(*secret random blinding values γ for first part of ElGamal ciphertext*)
γ⃗ = BPRandomIntegerVector[0,q-1,n];
(*first part of ElGamal ciphertext - randomizer*)
b⃗ = γ⃗ * g;
(*second part of ElGamal ciphertext - message*)
c⃗ = g * (StringToInteger /@ secretMessages) + γ⃗ * h⃗;
(*public keys of senders - to allow receivers to reply*)
d⃗ = (StringToInteger /@ (secretKeys[[#]] & /@ senders)) * g;

SendCRS[{"hvec"→h⃗, "bvec"→b⃗, "cvec"→c⃗, "dvec"→d⃗}];

StateMachineSave["ShuffleInput"];
```

Mix Server Performs Multi-Key Shuffle

- CRS Check
- Choose random shift s and permutation π
- Transform shuffle input $\vec{h}, \vec{b}, \vec{c}$ into $\vec{h'}, \vec{b'}, \vec{c'}$
- Create commitments V to s and W to s^n
- Commit to s by V and s^n by W

Secret:

s: secret key shift

π: secret permutation

π^{-1}: inverse of π

Public:

$\vec{h}$: public keys of receivers - to allow receivers to identify their messages

$\vec{b}$: commitments to blinding values - ElGamal randomizers
$\vec{c}$: blinded commitments to messages - ElGamal message
$\vec{d}$: public keys of senders - to allow receivers to reply
$\vec{h}'$: shuffled and shifted $\vec{h}$
$\vec{b}'$: shuffled and shifted $\vec{b}$
$\vec{c}'$: shuffled and shifted $\vec{c}$
$\vec{d}'$: shuffled and shifted $\vec{d}$
$\vec{h}'$, $\vec{b}'$, $\vec{c}'$ and $\vec{d}'$ are added to the CRS

In[100]:=

```
StateMachineRestore["ShuffleInput"];

(*Perform CRS Check*)
GroupOK = True; (*Assume choice of group is compliant with CRS requirements*)
If[!GroupOK || !PrimeQ[q], Error["CRS check on group"]];
If[g == o, Error["CRS check on g"]];
If[MemberQ[ĝ, o], Error["CRS check on ĝ"]];
If[MemberQ[ĥ, o], Error["CRS check on ĥ (depending on user value x̂)"]];
If[MemberQ[b̂, o], Error["CRS check on b̂ (depending on user value ŷ)"]];
If[MemberQ[ĉ, o], Error["CRS check on ĉ (depending on user values x̂, ŷ and their messages)"]]
If[MemberQ[d̂, o], Error["CRS check on d̂ (depending on user value x̂)"]];

Unprotect[π];
While[True,
    (*Choose random permutation and random key shift*)
    s = BPRandomInteger[1,q-1];
    π = BPRandomPermutation[n];
    π^-1 = InversePermutation[π];
    (*Transform input ĥ, b̂, ĉ, d̂ into ĥ', b̂', ĉ', d̂' by shuffling and key-shifting*)
    ĥ' = s * Permute[ĥ, π];
    b̂' = s * Permute[b̂, π];
    ĉ' = s * Permute[ĉ, π];
    d̂' = s * Permute[d̂, π];
    If[!MemberQ[ĥ', o] && !MemberQ[b̂', o] && !MemberQ[ĉ', o] && !MemberQ[d̂', o], Break[]];
];
(*Commit to key shift;
V will be sent to the verifier alongside commitment W in the next step of the prover*)
V = s*g;

(*Add ĥ', b̂', ĉ' and d̂' to the CRS*)
SendCRS[{"hprimevec"→ĥ',"bprimevec"→b̂','cprimevec"→ĉ','dprimevec"→d̂'}];

If[!interactive,
    Map[FiatShamirAdd["h."<>ToString[#], ĥ[[#]], 0]&, Range[n]];
```

```
    Map[FiatShamirAdd["b."<>ToString[#], b⃗[[#]], 0]&, Range[n]];
    Map[FiatShamirAdd["c."<>ToString[#], c⃗[[#]], 0]&, Range[n]];
    Map[FiatShamirAdd["d."<>ToString[#], d⃗[[#]], 0]&, Range[n]];
    Map[FiatShamirAdd["h'."<>ToString[#], h⃗'[[#]], 0]&, Range[n]];
    Map[FiatShamirAdd["b'."<>ToString[#], b⃗'[[#]], 0]&, Range[n]];
    Map[FiatShamirAdd["c'."<>ToString[#], c⃗'[[#]], 0]&, Range[n]];
    Map[FiatShamirAdd["d'."<>ToString[#], d⃗'[[#]], 0]&, Range[n]];
];

Print[Grid[{
    {Style["Name/Equation",Bold],Style["Semantics",Bold],Style["Knowledge",Bold],Style["Value
    {"","CRS Check passed?","P,V",True},
    {"x⃗","Secret Keys","P",x⃗},
    {"ϒ⃗","Secret Blinding Values","P",ϒ⃗},
    {"m⃗","Secret Messages","P",m⃗},
    {"s","Secret Shift","P",s},
    {"π","Secret permutation","P",π},
    {"h⃗","Public Keys of Receivers for Message Identification","P,V",h⃗},
    {"b⃗","Commitments to ϒ⃗: ElGamal randomizer part","P,V",b⃗},
    {"c⃗","Blinded Commitments m⃗: ElGamal message part","P,V",c⃗},
    {"d⃗","Public Keys of Senders to Allow Receivers to Reply","P,V",d⃗},
    {"h⃗'","Shuffled and Shifted h⃗","P,V",h⃗'},
    {"b⃗'","Shuffled and Shifted b⃗","P,V",b⃗'},
    {"c⃗'","Shuffled and Shifted c⃗","P,V",c⃗'},
    {"d⃗'","Shuffled and Shifted d⃗","P,V",d⃗'}
},Alignment→{{Left,Left,Left,Left}},Frame→All]]

If[!interactive, Print[FiatShamirGrid[]]];
ProcessNewMessages[];
StateMachineSave["ShuffleOutput"];
```

Name/Equation	Semantics	Knowledge	Value/Equality
	CRS Check passed?	P,V	True
$\vec{x}$	Secret Keys	P	{344 950 740 119 085 939 192 637 238 - 618 580 345, 23 268 750 808 893 157 627 298 718 655 - 763 563 898 233, 23 268 750 808 893 157 627 298 718 655 - 763 563 898 233}

$\vec{\gamma}$	Secret Blinding Values	P	{52 093 256 664 501 778 662 372 936 909 - 708 382 162 942 289 714 557 862 541 - 089 351 537 281 044 846 458, 49 124 052 705 495 879 986 257 686 989 - 648 802 267 959 695 213 933 441 572 - 102 172 344 506 073 586 801, 67 282 687 737 075 567 226 760 131 190 - 784 874 828 378 341 479 968 943 702 - 936 555 505 998 073 246 424}
$\vec{m}$	Secret Messages	P	$\vec{m}$
s	Secret Shift	P	77 055 416 219 496 477 297 458 718 029 - 586 723 439 661 366 871 894 090 478 - 002 190 167 067 968 031 603
π	Secret permutation	P	{3, 1, 2}
$\vec{h}$	Public Keys of Receivers for Message Identification	P,V	{ecPnt[78 567 409 798 129 814 866 150 056 - 060 307 810 399 673 849 671 094 211 - 427 553 792 618 009 791 659 223, 50 464 327 830 870 926 983 164 620 - 566 499 054 037 449 550 745 776 160 - 850 919 973 618 220 747 519 859], ecPnt[112 833 199 765 439 381 220 313 056 - 754 339 883 049 575 956 772 957 261 - 999 371 154 938 084 814 614 071, 55 162 480 627 138 884 082 362 925 - 002 107 050 797 199 473 890 589 593 - 047 995 087 693 795 006 543 339], ecPnt[112 833 199 765 439 381 220 313 056 - 754 339 883 049 575 956 772 957 261 - 999 371 154 938 084 814 614 071, 55 162 480 627 138 884 082 362 925 - 002 107 050 797 199 473 890 589 593 - 047 995 087 693 795 006 543 339]}

$\vec{b}$	Commitments to $\vec{\gamma}$: ElGamal randomizer part	P,V	{ecPnt[59 043 719 839 056 093 060 455 647 - 773 031 110 426 513 415 445 959 592 - 906 283 022 536 109 982 690 406, 15 581 121 562 794 375 473 593 189 - 690 062 526 490 521 359 132 176 103 - 829 752 471 918 632 370 295 336], ecPnt[28 042 937 753 915 930 788 547 013 - 599 645 448 755 092 123 652 825 491 - 664 072 915 209 989 352 569 125, 66 178 112 684 916 740 202 185 738 - 178 122 665 166 924 136 365 485 410 - 183 964 496 421 067 142 001 343], ecPnt[111 806 062 643 405 673 294 107 625 - 231 702 294 233 837 817 439 330 823 - 704 476 585 911 809 812 118 278, 96 271 173 562 246 442 335 118 096 - 000 002 956 980 355 600 440 300 789 - 883 776 848 991 926 176 478 624]}
$\vec{c}$	Blinded Commitments $\vec{m}$: ElGamal message part	P,V	{ecPnt[82 677 993 194 665 902 474 541 122 - 728 628 239 106 974 633 730 721 916 - 315 448 799 654 380 724 509 062, 82 899 414 855 368 741 404 724 030 - 068 539 514 612 899 114 324 925 700 - 999 638 050 403 382 505 421 116], ecPnt[23 172 912 405 278 733 415 435 710 - 602 144 815 479 916 588 170 014 597 - 418 408 278 116 825 280 333 989, 103 053 985 343 021 334 474 673 990 - 248 945 730 573 913 269 602 423 282 - 983 912 391 604 393 736 989 700], ecPnt[69 270 902 698 455 010 981 224 283 - 044 038 765 996 830 111 243 173 979 - 719 663 665 285 099 745 648 151, 112 380 697 802 250 453 283 363 092 - 945 878 117 421 176 770 345 454 476 - 832 123 069 113 820 053 308 875]}

$\vec{d}$	Public Keys of Senders to Allow Receivers to Reply	P,V	{ecPnt[97 038 873 997 667 556 164 890 627 - 159 143 816 584 036 737 601 412 047 - 181 786 115 325 137 586 601 893, 28 632 182 194 222 295 567 409 644 - 033 114 434 203 763 962 660 717 808 - 858 714 880 991 421 895 676 479], ecPnt[78 567 409 798 129 814 866 150 056 - 060 307 810 399 673 849 671 094 211 - 427 553 792 618 009 791 659 223, 50 464 327 830 870 926 983 164 620 - 566 499 054 037 449 550 745 776 160 - 850 919 973 618 220 747 519 859], ecPnt[53 729 729 513 994 595 695 462 455 - 195 591 489 616 567 069 832 745 850 - 818 442 954 791 457 454 586 503, 46 689 817 571 753 923 136 101 794 - 604 835 956 974 062 844 035 967 844 - 446 006 462 798 830 494 937 046]}
$\overrightarrow{h'}$	Shuffled and Shifted $\vec{h}$	P,V	{ecPnt[6 558 194 356 193 927 639 634 647 444 - 743 031 456 563 167 434 835 963 901 - 306 302 749 414 625 082 577, 52 488 910 954 347 611 664 776 036 - 389 515 076 273 016 905 927 124 685 - 240 883 874 979 762 544 524 251], ecPnt[6 558 194 356 193 927 639 634 647 444 - 743 031 456 563 167 434 835 963 901 - 306 302 749 414 625 082 577, 52 488 910 954 347 611 664 776 036 - 389 515 076 273 016 905 927 124 685 - 240 883 874 979 762 544 524 251], ecPnt[108 307 431 480 415 358 180 321 645 - 455 139 043 814 092 501 321 721 357 - 106 162 810 647 213 997 236 025, 36 351 342 789 842 377 099 456 363 - 842 641 744 188 644 647 315 961 192 - 968 880 873 781 984 072 160 774]}

$\overrightarrow{b'}$	Shuffled and Shifted $\vec{b}$	P,V	{ecPnt[2 101 504 872 291 888 883 716 359 192 - 847 722 039 905 370 848 787 468 118 - 146 221 520 733 335 251 689, 65 115 508 047 731 923 893 233 981 - 475 555 061 524 146 271 691 497 591 - 331 496 761 282 280 449 337 031], ecPnt[66 927 383 522 976 304 236 157 101 - 480 591 736 579 847 132 736 714 888 - 515 043 427 037 606 902 257 812, 107 572 068 642 340 469 124 979 747 - 235 810 229 109 194 492 671 695 182 - 627 325 466 548 702 521 834 811], ecPnt[54 597 720 163 964 310 354 822 001 - 511 722 288 403 820 425 105 673 732 - 255 729 486 794 940 621 160 858, 20 908 987 614 905 642 180 155 174 - 127 108 215 487 754 334 737 572 205 - 712 326 950 797 042 952 996 262]}
$\overrightarrow{c'}$	Shuffled and Shifted $\vec{c}$	P,V	{ecPnt[76 450 461 576 675 914 792 965 722 - 051 180 943 565 094 428 358 813 161 - 074 795 175 962 142 897 288 719, 38 216 996 469 148 933 963 905 268 - 396 466 886 302 699 197 112 751 046 - 297 550 831 186 589 191 968 048], ecPnt[33 216 804 232 678 278 471 260 719 - 141 100 536 638 697 095 655 969 466 - 196 649 583 487 480 597 031 229, 50 837 094 068 179 798 642 615 040 - 674 478 571 973 683 896 170 876 032 - 187 756 757 016 184 304 763 337], ecPnt[23 640 495 355 202 491 608 554 493 - 225 393 530 525 357 933 254 580 711 - 519 395 220 804 879 644 232 744, 63 745 865 814 030 357 294 809 620 - 337 129 418 176 053 657 581 482 167 - 229 204 651 942 724 506 248 630]}

$\vec{d}'$	Shuffled and Shifted $\vec{d}$	P,V	{ecPnt[108 307 431 480 415 358 180 321 645 - 455 139 043 814 092 501 321 721 357 - 106 162 810 647 213 997 236 025, 36 351 342 789 842 377 099 456 363 - 842 641 744 188 644 647 315 961 192 - 968 880 873 781 984 072 160 774], ecPnt[93 761 287 190 244 431 849 790 270 - 254 133 790 130 036 432 308 725 545 - 404 277 055 640 994 232 068 357, 35 500 574 849 318 626 019 937 037 - 834 919 246 834 175 404 043 884 801 - 123 182 806 451 365 357 886 461], ecPnt[112 929 678 132 582 868 571 013 728 - 088 079 645 858 007 540 176 146 226 - 385 430 663 184 270 576 277 149, 14 824 914 823 240 419 034 627 386 - 886 119 912 697 597 949 803 924 732 - 256 908 023 900 511 111 437 483]}

Users Identify and Decrypt the Messages they Received

After the multi-key shuffle has been completed, the users can go on to identify and decrypt the messages that they anonymously received from other users. Usually, this happens after the proof of shuffle has been finished, but to avoid spacially separating encryption, shuffling and decryption, it has been put here.

Each user individually checks the shuffled messages at the public bulletin board and identifies the ones dedicated to him. On each shifted public key in $\vec{h}'$ he tests [pub_key$*s = g*$priv_key$*s =] h_j' \stackrel{?}{=} V*$ priv_key [$= g*s*$priv_key]. In case of equality the corresponding message can be decrypted as $b_j'*(-$priv_key$) + c_j' = m_j*V$. Finally, the exponent m_j has to be extracted from this result.

Actually, these calculations are performed secretly by each user as a separate client of the system. For simplicity, this was added to the shuffler's notebook.

Variables:

index: position of user in arrays *names* and *secretKeys*

j: position of encrypted message on public bulletin board, i.e. index in $\vec{h}', \vec{b}', \vec{c}', \vec{d}'$

In[118]:=

```
StateMachineRestore["ShuffleOutput"];

rows = {};

Scan[Function[{index}, Block[
    {secretKey, shiftedPublicKeyOfReceiver, keyCandidate, messageAsGroupElement, message, shif
    (*Each User executes one iteration of this loop for himself*)
    secretKey = StringToInteger[secretKeys[[index]]];
    shiftedPublicKeyOfReceiver = secretKey*V;
    Scan[Function[{j},
        (*The User scans all shuffled and shifted messages on the public anonymouse bulletin b
        and checks if the shifted public key of the intended receiver matches his own*)
        keyCandidate = h'[[j]];
        If[keyCandidate == shiftedPublicKeyOfReceiver,
            messageAsGroupElement = (-secretKey)*b'[[j]] + c'[[j]];
            message = "ERROR: Unknown exponent";
            (*Twisted ElGamal: Extract exponent in ElGamal message part*)
            Scan[
                If[StringToInteger[#]*V == messageAsGroupElement,
                    message = #;
                ]&,
                {"Berlin", "Dresden", "Köln", "München", "Frankfurt",
                "Hamburg", "Wien", "Budapest", "Prag", "Bozen", "Basel",
                "Straßburg", "Saarbrücken", "Aachen", "Innsbruck", "Bern"}
            ];
            (*Reply Key*)
            shiftedPublicKeyOfSender = d'[[j]];
            AppendTo[rows, {names[[index]], j, message, shiftedPublicKeyOfSender}];
            (*User could reply with the shifted public key of the sender on shuffling back. Th
        ];
    ], Range[1, Length[h']]];
]], Range[1, Length[secretKeys]]];

Print[Grid[Join[
    {
        {Style["Decrypted Messages",Bold], SpanFromLeft, SpanFromLeft, SpanFromLeft},
        {Style["Receiver",Bold], Style["Index in Shuffle",Bold], Style["Decrypted Message",Bo
    },
    rows
], Alignment→{{Left,Left,Left}},Frame→All]];

StateMachineSave["NeedShuffleProof"];
```

Decrypted Messages			
Receiver	Index in Shuffle	Decrypted Message	Shifted Public Key of Sender (Reply Key)
Bob	3	Wien	ecPnt[112 929 678 132 582 868 571 013 728 088 079 645 858 007 - 540 176 146 226 385 430 663 184 270 576 277 149, 14 824 914 823 240 419 034 627 386 886 119 912 697 597 - 949 803 924 732 256 908 023 900 511 111 437 483]
Dave	1	München	ecPnt[108 307 431 480 415 358 180 321 645 455 139 043 814 092 - 501 321 721 357 106 162 810 647 213 997 236 025, 36 351 342 789 842 377 099 456 363 842 641 744 188 644 - 647 315 961 192 968 880 873 781 984 072 160 774]
Dave	2	Bozen	ecPnt[93 761 287 190 244 431 849 790 270 254 133 790 130 036 - 432 308 725 545 404 277 055 640 994 232 068 357, 35 500 574 849 318 626 019 937 037 834 919 246 834 175 - 404 043 884 801 123 182 806 451 365 357 886 461]

Proof of Multi-Key Shuffle

The mixing server proves that mixing and key-shifting has been done correctly by transforming the permutation and key shifting conditions into an inner product relation which can then be compressed by an inner product argument, resulting in a log-sized communication cost between prover (mixing server) and verifier.

Commitments Needed to Prove W is Well-Formed w.r.t. V

The prover commits to the shift s by $V = s*g$ and $W = s^n*g + \sigma_W*h$ (σ_W can be set to zero but is left to demonstrate how the standalone PR protocol would deal with blinding factors). The structure of the bulletproof shuffle argument requires a separate commitment W to s^n. This commitment can not be deduced from V and therefore it has to be proved that W is well-formed with respect to V in addition to the proof of shuffle. The paper draft does not explain how to do this in detail but it is implemented in this notebook nevertheless. It could be separated into its own sigma protocol but this would require some additional challenge values. This is the reason it is woven into the shuffle argument.

The PR argument uses $\overrightarrow{a_{R,W}} : \equiv_q \{s, s, \ldots, s\}$ (n times) and $\overrightarrow{a_{L,W}} : \equiv_q \{1, s, s^2, \ldots, s^{n-1}\}$ similar to how the shuffle argument uses $\overrightarrow{a_R}$ and $\overrightarrow{a_L}$. The additional challenge value w is needed to prove that all entries of $\overrightarrow{a_{R,W}}$ are equal. Up to the constraints the structure of the PR argument is exactly like the Bulletproof range proof protocol.

All variables exclusive to the PR argument contain a “W” in their names:
$\overrightarrow{a_{R,W}}$, $\overrightarrow{a_{L,W}}$, α_W, β_W, γ_W, $\overrightarrow{s_{R,W}}$, $\overrightarrow{s_{L,W}}$, A_W, S_W, w, $\overrightarrow{l_{0,W}}$, $\overrightarrow{l_{1,W}}$, $\overrightarrow{r_{0,W}}$, $\overrightarrow{r_{1,W}}$,
δ_{yzw}, $t_{0,W}$, $t_{1,W}$, $t_{2,W}$, $\overrightarrow{l_W}$, $\overrightarrow{r_W}$, $\tau_{1,W}$, $\tau_{2,W}$, $\tau_{x,W}$, $T_{1,W}$, $T_{2,W}$, $\hat{t_w}$, μ_W, P_W^+

Equivalent in the inner product protocol.

The PR protocol is based on the following linear constraints:

$a_{R,W_1} \equiv_q s$

$\wedge a_{R,W_i} \equiv_q a_{R,W_{i-1}}$

$\wedge a_{L,W_1} \equiv_q 1$

$\wedge a_{L,W_i} \equiv_q a_{L,W_{i-1}}\, a_{R,W_{i-1}}$

This implies that $a_{L,W_1}\, a_{R,W_1} \equiv_q s$ and $a_{L,W_n}\, a_{R,W_n} \equiv_q s^n$. By linking V to the first and W to the second of those products the required relation between V and W is proven in a zero-knowledge manner.

In[123]:=

```
StateMachineRestore["NeedShuffleProof"];

(*Commitments V and W to s and s^n.
As s is a random value, a blinding value for s can be omitted. By calculating V^x_i
which is equal to h^s_i the receiver i can identify the messages intended to be read by him*)
(*V = s*g; (*Already calculated in while calculating the shuffle output*)*)
TellVerifier[{"V"→V,"_cost"→"group"}];
σ_W = BPRandomInteger[0,q-1];
W = powermodq[s,n]*g + σ_W*h;
TellVerifier[{"W"→W,"_cost"→"group"}];
If[!interactive,
    FiatShamirAdd["V", compressPoint[V], entropyParameters["group"]];
    FiatShamirAdd["W", compressPoint[W], entropyParameters["group"]];
];

a⃗_R,W = ConstantArray[s, n];
a⃗_L,W = Thread[powermodq[a⃗_R,W, Range[0,n-1]]];
α_W = BPRandomInteger[0,q-1];
β_W = BPRandomInteger[0,q-1];
ϒ_W = BPRandomInteger[0,q-1];
s⃗_R,W = ConstantArray[ϒ_W, n];
s⃗_L,W = Thread[powermodq[ConstantArray[ϒ_W,n], Range[0,n-1]]];

A_W = a⃗_L,W.g⃗ + a⃗_R,W.h⃗ + α_W*h;
TellVerifier[{"AW"→A_W,"_cost"→"group"}];
If[!interactive,FiatShamirAdd["AW",compressPoint[A_W],entropyParameters["group"]]];

S_W = s⃗_L,W.g⃗ + s⃗_R,W.h⃗ + β_W*h;
TellVerifier[{"SW"→S_W,"_cost"→"group"}];
If[!interactive,FiatShamirAdd["SW",compressPoint[S_W],entropyParameters["group"]]];

Print[Grid[{
    {Style["Name",Bold],Style["Semantics",Bold],Style["Knowledge",Bold],Style["Value",Bold]},
    {"V := sg","Commitment to s","P,V",V},
    {"σ_W ←$ ℤ_q","Blinding Value for Commitment W to s^n","P",σ_W},
    {"W := s^n g + σ_W h","Blinded Pedersen Commitment to s^n","P,V",W},
    {"a⃗_R,W :≡_q {s, s, ..., s}","Constant vector of s","P",a⃗_R,W},
    {"a⃗_L,W :≡_q {1, s, s^2, ..., s^(n-1)}","Aggregation of a⃗_R,W","P",a⃗_L,W},
    {"α_W ←$ ℤ_q","Blinding\nValue","P",α_W},
    {"β_W ←$ ℤ_q","Blinding\nValue","P",β_W},
```

```
    {"γ_W ←$ ℤ_q\{0}","Blinding\nValue","P",γ_W},
    {"s⃗_R,W :≡_q {γ_W, γ_W, ..., γ_W}","Blinding\nVector for a⃗_R,W","P",s⃗_R,W},
    {"s⃗_L,W :≡_q {1, γ_W, γ_W^2, ..., γ_W^(n-1)}","Blinding\nVector for a⃗_L,W","P",s⃗_L,W},
    {"A_W := <a⃗_L,W, g⃗> + <a⃗_R,W, h⃗> + α*h","Blinded\nPedersen\nVector\nCommitment","P,V",A_W},
    {"S_W := <s⃗_L,W, g⃗> + <s⃗_R,W, h⃗> + β*h","Blinded\nPedersen\nVector\nCommitment","P,V",S_W}
  }, Alignment→{{Left,Left,Left,Left}},Frame→All]]

Print[CommunicationCostGrid[]]
If[!interactive,Print[FiatShamirGrid[]]];
ProcessNewMessages[];
StateMachineSave["VWAWSW"];
```

Name	Semantics	Knowledge	Value
V := sg	Commitment to s	P,V	ecPnt[80 311 418 295 773 201 369 - 076 106 032 905 885 135 762 - 203 375 069 519 910 440 352 - 607 757 637 919 026, 72 330 072 365 709 643 804 - 368 075 438 580 117 209 924 - 633 474 527 671 615 978 853 - 661 751 055 433 193]
$\sigma_W \xleftarrow{\$} \mathbb{Z}_q$	Blinding Value for Commitment W to s^n	P	22 366 834 116 192 821 394 599 - 891 845 776 596 947 965 960 - 535 147 048 644 883 938 592 - 576 580 123 496
$W := s^n g + \sigma_W h$	Blinded Pedersen Commitment to s^n	P,V	ecPnt[103 906 792 605 577 532 175 - 755 598 396 156 158 461 452 - 152 976 375 149 011 426 016 - 206 021 735 424 243, 86 390 539 398 352 229 318 - 624 618 945 653 159 494 571 - 754 482 845 117 036 288 422 - 074 734 839 991 103]
$\vec{a}_{R,W} :\equiv_q \{s, s, ..., s\}$	Constant vector of s	P	{77 055 416 219 496 477 297 - 458 718 029 586 723 439 661 - 366 871 894 090 478 002 190 - 167 067 968 031 603, 77 055 416 219 496 477 297 - 458 718 029 586 723 439 661 - 366 871 894 090 478 002 190 - 167 067 968 031 603, 77 055 416 219 496 477 297 - 458 718 029 586 723 439 661 - 366 871 894 090 478 002 190 - 167 067 968 031 603}

$\overrightarrow{a_{L,W}} :\equiv_q \{1, s, s^2, \ldots, s^{n-1}\}$	Aggregation of $\overrightarrow{a_{R,W}}$	P	{1, 77 055 416 219 496 477 297 - 458 718 029 586 723 439 661 - 366 871 894 090 478 002 190 - 167 067 968 031 603, 103 335 486 851 699 772 897 - 719 005 055 135 192 021 025 - 792 828 614 314 763 993 575 - 677 057 000 300 108}
$\alpha_W \overset{\$}{\leftarrow} \mathbb{Z}_q$	Blinding Value	P	80 097 486 922 389 020 855 145 - 666 582 067 090 346 471 173 - 415 549 129 384 999 818 876 - 148 705 557 598
$\beta_W \overset{\$}{\leftarrow} \mathbb{Z}_q$	Blinding Value	P	59 943 451 627 612 448 924 676 - 484 334 164 735 008 594 061 - 016 410 731 728 968 786 172 - 837 127 467 984
$\gamma_W \overset{\$}{\leftarrow} \mathbb{Z}_q \setminus \{0\}$	Blinding Value	P	103 449 002 380 076 435 222 - 853 190 046 878 651 498 924 - 569 833 450 391 518 456 216 - 468 185 080 813 412
$\overrightarrow{s_{R,W}} :\equiv_q \{\gamma_W, \gamma_W, \ldots, \gamma_W\}$	Blinding Vector for $\overrightarrow{a_{R,W}}$	P	{103 449 002 380 076 435 222 - 853 190 046 878 651 498 924 - 569 833 450 391 518 456 216 - 468 185 080 813 412, 103 449 002 380 076 435 222 - 853 190 046 878 651 498 924 - 569 833 450 391 518 456 216 - 468 185 080 813 412, 103 449 002 380 076 435 222 - 853 190 046 878 651 498 924 - 569 833 450 391 518 456 216 - 468 185 080 813 412}
$\overrightarrow{s_{L,W}} :\equiv_q \{1, \gamma_W, \gamma_W^2, \ldots, \gamma_W^{n-1}\}$	Blinding Vector for $\overrightarrow{a_{L,W}}$	P	{1, 103 449 002 380 076 435 222 - 853 190 046 878 651 498 924 - 569 833 450 391 518 456 216 - 468 185 080 813 412, 9 669 727 685 888 435 741 682 - 791 084 323 628 869 249 804 - 294 902 520 995 644 873 285 - 051 619 396 679}
$A_W := \langle \overrightarrow{a_{L,W}}, \vec{g} \rangle + \langle \overrightarrow{a_{R,W}}, \vec{h} \rangle + \alpha * h$	Blinded Pedersen Vector Commitment	P,V	ecPnt[102 533 074 015 578 785 830 - 435 668 723 656 382 032 639 - 089 329 076 188 012 258 139 - 630 558 261 897 965, 46 049 899 562 897 304 560 - 334 445 879 497 416 924 158 - 280 040 071 140 643 789 946 - 815 220 981 299 101]

$S_W := \langle \overrightarrow{s_{L,W}}, \vec{g} \rangle + \langle \overrightarrow{s_{R,W}}, \vec{h} \rangle + \beta * h$	Blinded Pedersen Vector Commitment	P,V	ecPnt[60 802 009 577 214 426 038 - 022 799 869 417 466 939 097 - 580 576 611 454 797 233 973 - 333 907 472 889 599, 4 544 274 886 182 003 749 351 - 257 221 639 993 502 991 294 - 730 296 803 633 157 620 175 - 479 609 245 008]

Total Communication Cost			
Type	**Count**	**Names**	**Bits**
group	4	V, W, AW, SW	1028
total	4		1028

Commitment to Random Linear Combination of Output Secret Keys, Randomizers and Ciphertexts

Begin Shuffle Proof: Receive Challenges r and u, calculate $\vec{k}$ and $A_{R,\{h,b,c,d\}}$

$k_i : \equiv_q r - u^i$ for all i in the range of 1 to n

$A_{R,\{h,b,c,d\}} := \Sigma_{i=1}^{n} k_i * \{h_i', b_i', c_i', d_i'\}$

In[147]:=

```
StateMachineRestore["VWAWSW"];

If[interactive,
(*Random challenges from interactive verifier*)
    r = WaitForRandomChallenge["r"];
    u = WaitForRandomChallenge["u"];
(*Else*),
(*Fiat-Shamir*)
    r = FiatShamirGet["r",q,entropyParameters["scalar"]];
    TellVerifier[{"r"→r,"_cost"→"scalar"}];
    u = FiatShamirGet["u",q,entropyParameters["scalar"]];
    TellVerifier[{"u"→u,"_cost"→"scalar"}];
];

uPowers = Thread[powermodq[ConstantArray[u,n], Range[1,n]]];
k⃗ = modq[r - uPowers];
k̂ = modq[Fold[Times, 1, k⃗]];
k̄ = modq[Fold[Plus, 0, k⃗]];
A_{R,h} = Total[k⃗ * h⃗'];
A_{R,b} = Total[k⃗ * b⃗'];
A_{R,c} = Total[k⃗ * c⃗'];
A_{R,d} = Total[k⃗ * d⃗'];

Print[Grid[{
    {Style["Name",Bold],Style["Semantics",Bold],Style["Knowledge",Bold],Style["Value",Bold]},
    {"r",semanticsOfRandomChallenge,"P,V",r},
    {"u",semanticsOfRandomChallenge,"P,V",u},
    {"u_powers :≡_q {u,u^2,u^3,...,u^n}","","P,V (implicit)",uPowers},
    {"k⃗ :≡_q r - u_powers","","P,V (implicit)",k⃗},
    {"A_{R,h} := Σ{k⃗ ∘ h⃗'}","","P,V (implicit)",A_{R,h}},
    {"A_{R,b} := Σ{k⃗ ∘ b⃗'}","","P,V (implicit)",A_{R,b}},
    {"A_{R,c} := Σ{k⃗ ∘ c⃗'}","","P,V (implicit)",A_{R,c}},
    {"A_{R,d} := Σ{k⃗ ∘ d⃗'}","","P,V (implicit)",A_{R,d}}
}, Alignment→{{Left,Left,Left,Left}},Frame→All]]

Print[CommunicationCostGrid[]]
If[!interactive,Print[FiatShamirGrid[]]];
ProcessNewMessages[];
StateMachineSave["ruk"];
```

Waiting to receive r from InteractiveVerifier ...

Waiting to receive u from InteractiveVerifier ...

Name	Semantics	Knowledge	Value
r	Random Challenge	P,V	37 072 487 844 121 016 544 199 508 458 - 329 903 725 504 628 962 986 741 349 - 058 985 323 004 642 065 609

u	Random Challenge	P,V	112 269 625 660 350 362 882 863 760 160 - 812 690 082 016 551 740 788 795 940 - 136 101 880 060 177 832 694
$u_{powers} :\equiv_q \{u, u^2, u^3, \ldots, u^n\}$		P,V (implicit)	{112 269 625 660 350 362 882 863 760 - 160 812 690 082 016 551 740 788 795 - 940 136 101 880 060 177 832 694, 11 890 542 273 519 331 462 425 038 986 - 914 051 559 507 417 469 516 314 676 - 862 227 906 964 884 492 193, 33 387 804 159 995 661 087 204 252 238 - 941 081 331 379 259 117 507 535 049 - 098 238 738 582 016 269 690}
$\vec{k} :\equiv_q r - u_{powers}$		P,V (implicit)	{40 594 951 421 086 849 084 906 733 306 - 205 121 496 325 641 501 272 849 791 - 528 046 584 462 625 727 252, 25 181 945 570 601 685 081 774 469 471 - 415 852 165 997 211 493 470 426 672 - 196 757 416 039 757 573 416, 3 684 683 684 125 355 456 995 256 219 - 388 822 394 125 369 845 479 206 299 - 960 746 584 422 625 795 919}
$A_{R,h} := \Sigma\{\vec{k} \circ \overrightarrow{h'}\}$		P,V (implicit)	ecPnt[75 827 213 137 871 704 164 931 521 628 - 089 874 212 004 001 725 498 144 777 - 005 823 861 414 415 878 326, 85 558 088 274 753 361 702 239 458 714 - 109 752 170 257 343 893 657 124 488 - 281 320 372 885 377 844 970]
$A_{R,b} := \Sigma\{\vec{k} \circ \overrightarrow{b'}\}$		P,V (implicit)	ecPnt[101 490 138 278 120 560 054 535 134 - 112 685 149 527 531 186 110 662 767 - 547 021 801 145 903 939 319 509, 45 189 396 226 369 639 764 475 183 750 - 210 875 191 161 366 914 100 613 038 - 683 080 011 606 878 795 742]
$A_{R,c} := \Sigma\{\vec{k} \circ \overrightarrow{c'}\}$		P,V (implicit)	ecPnt[80 032 568 196 835 196 626 944 046 435 - 262 813 649 995 163 939 592 905 385 - 880 753 783 724 791 743 679, 23 552 969 371 290 033 158 266 674 238 - 835 159 465 211 446 720 669 348 929 - 745 850 171 431 031 988 187]
$A_{R,d} := \Sigma\{\vec{k} \circ \overrightarrow{d'}\}$		P,V (implicit)	ecPnt[2 407 103 694 493 959 746 503 196 603 - 452 329 517 078 614 148 064 293 342 - 612 912 008 722 177 884 863, 56 880 823 889 132 509 467 030 174 309 - 379 436 312 737 498 520 799 651 845 - 161 746 864 517 931 461 934]

Total Communication Cost			
Type	Count	Names	Bits
group	4	V, W, AW, SW	1028
scalar	2	r, u	512
total	6		1540

Construct Vectors $\vec{a_L}$, $\vec{a_R}$, Choose $\vec{s_L}$, $\vec{s_R}$ and Commit to them with A_L, S_L, $S_{R,\{h,b,c,d\}}$

$\vec{a_R}$: shifted and inversely shuffled version of $\vec{k}$ (the discrete logarithms in $A_{R,\{h,b,c,d\}}$ w.r.t. bases $\{\vec{h}, \vec{b}, \vec{c}, \vec{d}\}$).

$\vec{a_L}$: aggregation of $\vec{a_R}$ (blinding value α for commitment A_L), $\vec{a_L} \equiv_q \{1, a_{R_1}, a_{R_1} a_{R_2}, \ldots, \Pi_{i=1}^{n-1} a_{R_i}\}$

$\vec{s_L}$: blinding values for $\vec{a_L}$ (blinding value β for commitment S_L)

$\vec{s_R}$: blinding values for $\vec{a_R}$ (blinding values $\rho_{\{h,b,c,d\}}$ for commitments $S_{R,\{h,b,c,d\}}$ based on $\{\vec{h}, \vec{b}, \vec{c}, \vec{d}\}$)

The prover is left to argue that $\vec{a_R}$ satisfies three conditions (see paper draft pg. 21 and 22):

1. $\Pi_i a_{R_i} \equiv_q s^n \Pi_i k_i$. This shows, using a polynomial identity test, that there exists a permutation π of length n such that a_{R_i} contains $c_i * k_{\pi^{-1}(i)}$, where c_i is any constant.

2. $\Sigma_i a_{R_i} \equiv_q s\Sigma_i k_i$. This shows, using a random linear combination check, that there exists an $s \in \mathbb{Z}_q^*$ such that for all a_{R_i}, c_i is equal to s.

3. a_R is the committed value in $A_{R,\{h,b,c,d\}}$ w.r.t. bases $\{\vec{h}, \vec{b}, \vec{c}, \vec{d}\}$.

These conditions need to be transformed into a Hadamard product or linear combination of vectors to feed them into a “Bulletproofs sub-routine”, as it is called in the paper draft. The product relation in condition 1 can be transformed into a Hadamard product with the help of $\vec{a_L}$ by $a_{L_n} a_{R_n} \equiv_q \Pi_i a_{R_i}$. Conditions 1 and 2 are then captured by:

$a_{L_1} \equiv_q 1$

$\wedge a_{L_i} \equiv_q a_{L_{i-1}} a_{R_{i-1}}$

$\wedge a_{L_n} a_{R_n} \equiv_q s^n \Pi_i k_i$

$\wedge \Sigma_i a_{R_i} \equiv_q s\Sigma_i k_i$

In[162]:=

```
StateMachineRestore["ruk"];

aR = modq[s * Permute[k, π^-1]];
aL = {1};
For[i = 1, i ≤ n-1, i++,
    AppendTo[aL, modq[aL[[i]] * aR[[i]]]]
];
α = BPRandomInteger[0,q-1];
β = BPRandomInteger[0,q-1];
ρh = BPRandomInteger[0,q-1];
ρb = BPRandomInteger[0,q-1];
ρc = BPRandomInteger[0,q-1];
ρd = BPRandomInteger[0,q-1];
sL = BPRandomIntegerVector[0,q-1,n];
sR = BPRandomIntegerVector[0,q-1,n];
```

```
A_L = a_L.g + α*h;
TellVerifier[{"AL"→A_L,"_cost"→"group"}];
If[!interactive,FiatShamirAdd["AL",compressPoint[A_L],entropyParameters["group"]]];

S_L = s_L.g + β*h;
TellVerifier[{"SL"→S_L,"_cost"→"group"}];
If[!interactive,FiatShamirAdd["SL",compressPoint[S_L],entropyParameters["group"]]];

S_{R,h} = s_R.h + ρ_h*h;
TellVerifier[{"SRh"→S_{R,h},"_cost"→"group"}];
If[!interactive,FiatShamirAdd["SRh",compressPoint[S_{R,h}],entropyParameters["group"]]];

S_{R,b} = s_R.b + ρ_b*h;
TellVerifier[{"SRb"→S_{R,b},"_cost"→"group"}];
If[!interactive,FiatShamirAdd["SRb",compressPoint[S_{R,b}],entropyParameters["group"]]];

S_{R,c} = s_R.c + ρ_c*h;
TellVerifier[{"SRc"→S_{R,c},"_cost"→"group"}];
If[!interactive,FiatShamirAdd["SRc",compressPoint[S_{R,c}],entropyParameters["group"]]];

S_{R,d} = s_R.d + ρ_d*h;
TellVerifier[{"SRd"→S_{R,d},"_cost"→"group"}];
If[!interactive,FiatShamirAdd["SRd",compressPoint[S_{R,d}],entropyParameters["group"]]];

Print[Grid[{
    {Style["Name",Bold],Style["Semantics",Bold],Style["Knowledge",Bold],Style["Value",Bold]},
    {"a_R :≡_q s * π^{-1}(k)","Shifted Inverse Shuffle of k","P",a_R},
    {"a_L :≡_q {1,sk_{π^{-1}(1)},s^2 k_{π^{-1}(1)} k_{π^{-1}(2)},...}","Aggregation of a_R","P",a_L},
    {"α ←$ Z_q","Blinding\nValue","P",α},
    {"β ←$ Z_q","Blinding\nValue","P",β},
    {"ρ_h ←$ Z_q","Blinding\nValue","P",ρ_h},
    {"ρ_b ←$ Z_q","Blinding\nValue","P",ρ_b},
    {"ρ_c ←$ Z_q","Blinding\nValue","P",ρ_c},
    {"ρ_d ←$ Z_q","Blinding\nValue","P",ρ_d},
    {"s_L ←$ Z_q^n","Blinding\nVector for a_L","P",s_L},
    {"s_R ←$ Z_q^n","Blinding\nVector for a_R","P",s_R},
    {"A_L := <a_L,g> + α*h","Blinded\nPedersen\nVector\nCommitment","P,V",A_L},
    {"S_L := <s_L,g> + β*h","Blinded\nPedersen\nVector\nCommitment","P,V",S_L},
    {"S_{R,h} := <s_R,h> + ρ_h*h","Blinded\nPedersen\nVector\nCommitment","P,V",S_{R,h}},
    {"S_{R,b} := <s_R,b> + ρ_b*h","Blinded\nPedersen\nVector\nCommitment","P,V",S_{R,b}},
    {"S_{R,c} := <s_R,c> + ρ_c*h","Blinded\nPedersen\nVector\nCommitment","P,V",S_{R,c}},
    {"S_{R,d} := <s_R,d> + ρ_d*h","Blinded\nPedersen\nVector\nCommitment","P,V",S_{R,d}}
}, Alignment→{{Left,Left,Left,Left}},Frame→All]]
```

```
Print[CommunicationCostGrid[]]
If[!interactive,Print[FiatShamirGrid[]]];
ProcessNewMessages[];
StateMachineSave["AS"];
```

Name	Semantics	Knowledge	Value
$\overrightarrow{a_R} :\equiv_q s * \pi^{-1}(\vec{k})$	Shifted Inverse Shuffle of $\vec{k}$	P	{62 223 084 126 069 293 449 - 907 123 587 300 367 585 137 - 348 102 814 299 326 270 755 - 703 956 945 378 646, 64 027 596 083 704 852 344 - 642 434 235 899 983 634 919 - 620 536 252 763 289 502 880 - 999 778 876 922 170, 30 898 189 362 326 642 401 - 605 487 281 842 185 430 970 - 644 239 067 292 734 447 129 - 498 769 242 998 106}
$\overrightarrow{a_L} :\equiv_q \{1, s\vec{k}_{\pi^{-1}(1)}, s^2\vec{k}_{\pi^{-1}(1)}\vec{k}_{\pi^{-1}(2)}, \ldots\}$	Aggregation of $\overrightarrow{a_R}$	P	{1, 62 223 084 126 069 293 449 - 907 123 587 300 367 585 137 - 348 102 814 299 326 270 755 - 703 956 945 378 646, 13 975 690 864 423 647 027 - 715 690 152 343 446 907 448 - 362 062 379 445 489 462 722 - 761 419 995 928 202}
$\alpha \xleftarrow{\$} \mathbb{Z}_q$	Blinding Value	P	17 398 176 202 481 637 751 860 - 114 248 176 047 760 531 156 - 697 850 321 616 127 992 279 - 049 328 252 413
$\beta \xleftarrow{\$} \mathbb{Z}_q$	Blinding Value	P	27 219 552 920 418 278 154 622 - 008 378 385 320 785 396 869 - 030 159 780 024 013 163 024 - 974 396 033 246
$\rho_h \xleftarrow{\$} \mathbb{Z}_q$	Blinding Value	P	102 986 942 228 350 997 637 - 870 447 182 702 336 728 859 - 860 977 331 651 452 906 247 - 885 964 411 195 770
$\rho_b \xleftarrow{\$} \mathbb{Z}_q$	Blinding Value	P	67 750 394 590 451 778 158 204 - 940 167 618 240 646 217 008 - 969 775 154 608 541 150 812 - 022 072 315 973
$\rho_c \xleftarrow{\$} \mathbb{Z}_q$	Blinding Value	P	74 713 749 057 188 690 237 921 - 443 254 967 297 886 915 577 - 695 515 183 681 394 976 026 - 396 939 778 234
$\rho_d \xleftarrow{\$} \mathbb{Z}_q$	Blinding Value	P	55 739 259 823 876 949 789 125 - 654 739 186 763 620 164 839 - 911 902 539 974 830 065 163 - 733 528 027 333

$\overrightarrow{s_L} \xleftarrow{\$} \mathbb{Z}_q^n$	Blinding Vector for $\overrightarrow{a_L}$	P	{3 490 043 951 473 342 957 863 - 269 612 888 825 370 966 098 - 959 732 202 668 461 366 396 - 201 773 608 447, 81 026 870 043 438 310 759 - 789 738 090 565 752 971 348 - 726 422 705 469 591 555 083 - 035 827 778 970 747, 109 413 017 180 886 544 487 - 921 683 678 413 534 566 795 - 499 839 518 913 016 004 076 - 708 382 233 891 835}
$\overrightarrow{s_R} \xleftarrow{\$} \mathbb{Z}_q^n$	Blinding Vector for $\overrightarrow{a_R}$	P	{12 507 601 888 368 634 928 - 041 736 808 448 324 961 591 - 369 924 503 374 677 351 026 - 235 158 490 466 997, 63 313 909 303 783 745 204 - 827 875 316 592 779 921 398 - 731 751 274 269 282 817 433 - 014 526 141 649 354, 27 472 217 458 736 686 113 - 325 566 075 209 874 854 922 - 345 264 255 234 592 930 381 - 510 746 121 210 239}
$A_L := <\overrightarrow{a_L}, \vec{g}> + \alpha * h$	Blinded Pedersen Vector Commitment	P,V	ecPnt[6 587 839 308 200 477 344 056 - 289 937 852 477 545 542 855 - 779 583 120 343 135 425 480 - 544 699 054 079, 2 185 727 872 912 664 248 596 - 558 371 241 923 997 051 231 - 854 180 743 555 974 368 558 - 112 945 768 953]
$S_L := <\overrightarrow{s_L}, \vec{g}> + \beta * h$	Blinded Pedersen Vector Commitment	P,V	ecPnt[4 034 094 399 684 424 483 307 - 446 142 353 323 528 168 707 - 067 153 775 234 243 263 723 - 285 535 027 265, 105 719 365 290 533 780 380 - 052 039 872 682 080 848 414 - 207 099 695 078 768 961 388 - 028 092 136 442 987]
$S_{R,h} := <\overrightarrow{s_R}, \vec{h}> + \rho_h * h$	Blinded Pedersen Vector Commitment	P,V	ecPnt[110 628 460 759 275 561 610 - 186 686 680 845 830 158 167 - 592 932 204 791 477 090 968 - 094 876 973 217 838, 5 304 693 054 449 904 688 326 - 008 829 038 550 901 554 024 - 028 550 115 729 307 204 635 - 136 817 245 677]

$S_{R,b} := <\vec{s_R}, \vec{b}> + \rho_b * h$	Blinded Pedersen Vector Commitment	P,V	ecPnt[42 640 815 911 507 716 472 - 477 938 340 233 126 446 598 - 231 831 337 676 705 110 847 - 057 191 691 627 240, 41 259 033 927 332 187 352 - 077 874 555 881 525 500 144 - 635 031 111 699 813 138 487 - 260 070 252 465 805]
$S_{R,c} := <\vec{s_R}, \vec{c}> + \rho_c * h$	Blinded Pedersen Vector Commitment	P,V	ecPnt[62 635 959 701 511 398 581 - 525 732 065 492 888 015 851 - 399 229 301 995 870 753 638 - 223 458 110 077 747, 85 310 810 054 037 865 183 - 042 977 962 233 049 541 249 - 821 571 800 238 984 522 867 - 038 773 595 657 876]
$S_{R,d} := <\vec{s_R}, \vec{d}> + \rho_d * h$	Blinded Pedersen Vector Commitment	P,V	ecPnt[93 333 551 283 426 889 209 - 650 746 890 228 923 405 712 - 607 594 824 962 743 876 131 - 424 188 627 252 440, 12 336 277 386 395 050 805 - 637 224 061 380 236 860 277 - 223 773 540 742 993 587 606 - 337 362 283 853 740]

Total Communication Cost			
Type	**Count**	**Names**	**Bits**
group	10	V, W, AW, SW, AL, SL, SRh, SRb, SRc, SRd	2570
scalar	2	r, u	512
total	12		3082

Receive V's Random Challenges y, z and w or Generate Fiat-Shamir Transform

Receive random challenges to prove constraints on $\vec{a_L}$, $\vec{a_R}$, $\vec{a_{L,W}}$ and $\vec{a_{R,W}}$.

In[197]:=

```
StateMachineRestore["AS"];
If[interactive,
(*Random challenges from interactive verifier*)
    y = WaitForRandomChallenge["y"];
    z = WaitForRandomChallenge["z"];
    w = WaitForRandomChallenge["w"];
(*Else*),
(*Fiat-Shamir*)
    y = FiatShamirGet["y",q,entropyParameters["scalar"]];
    TellVerifier[{"y"→y,"_cost"→"scalar"}];
    z = FiatShamirGet["z",q,entropyParameters["scalar"]];
    TellVerifier[{"z"→z,"_cost"→"scalar"}];
    w = FiatShamirGet["w",q,entropyParameters["scalar"]];
    TellVerifier[{"w"→w,"_cost"→"scalar"}];
];

y⃗^n = Thread[powermodq[ConstantArray[y,n], Range[0,n-1]]];
y⃗_z^(n-1) = Join[{z},y⃗^n[[1;;n-1]]];
y^-1 = modinvq[y];
y⃗^-n = Thread[powermodq[ConstantArray[y^-1,n], Range[0,n-1]]];
w⃗^n = Thread[powermodq[ConstantArray[w,n], Range[0,n-1]]];
w⃗_0^(n-1) = Join[{0},w⃗^n[[1;;n-1]]];
δ_yz = modq[-z^3 * (z + (n-1) * y^-1) - z];
δ_yzw = modq[-z * (2 + z + (n-1) * y^-1) + (y^-1 - w) * (
    Total[Thread[powermodq[ConstantArray[w*y,n-1], Range[0,n-2]]]]
)];

Print[Grid[{
    {Style["Name",Bold],Style["Semantics",Bold],Style["Knowledge",Bold],Style["Value",Bold]},
    {"y",semanticsOfRandomChallenge,"P,V",y},
    {"z",semanticsOfRandomChallenge,"P,V",z},
    {"w",semanticsOfRandomChallenge,"P,V",w},
    {"δ_yz :≡_q -z^3(z + (n-1)y^-1) - z","","P,V",δ_yz},
    {"δ_yzw :≡_q -z (2 + z + (n-1)y^-1) + (y^-1-w)Σ_(i=0)^(n-2)(wy)^i","","P,V",δ_yzw}
}, Alignment→{{Left,Left,Left,Left}},Frame→All]]

Print[CommunicationCostGrid[]]
If[!interactive,Print[FiatShamirGrid[]]];
ProcessNewMessages[];
StateMachineSave["yzw"];
```

```
Waiting to receive y from InteractiveVerifier ...

Waiting to receive z from InteractiveVerifier ...

Waiting to receive w from InteractiveVerifier ...
```

Name	Semantics	Knowledge	Value
y	Random Challenge	P,V	34 071 807 136 020 401 556 542 966 - 374 520 839 966 408 801 837 667 695 - 887 196 400 659 657 467 356 250
z	Random Challenge	P,V	51 229 650 329 065 518 720 689 096 - 099 379 898 312 022 759 911 804 433 - 524 422 971 782 942 501 299 478
w	Random Challenge	P,V	42 781 056 564 410 839 501 179 897 - 936 311 018 651 211 153 484 828 394 - 010 058 930 403 301 036 390 238
$\delta_{yz} :\equiv_q -z^3 (z + (n-1) y^{-1}) - z$		P,V	80 655 863 109 809 954 281 040 981 - 808 557 398 115 356 422 816 035 440 - 745 191 521 875 586 723 707 423
$\delta_{yzw} :\equiv_q -z (2 + z + (n-1) y^{-1}) + (y^{-1}-w) \sum_{i=0}^{n-2} (wy)^i$		P,V	36 280 791 154 615 824 673 741 371 - 562 371 573 961 477 989 289 960 370 - 376 293 582 689 521 148 309 524

Total Communication Cost			
Type	Count	Names	Bits
group	10	V, W, AW, SW, AL, SL, SRh, SRb, SRc, SRd	2570
scalar	5	r, u, y, z, w	1280
total	15		3850

Construct $\vec{l}(X)$, $\vec{r}(X)$ and $\vec{t}(X)$, Commit to Coefficients of $\vec{t}(X)$ for Polynomial Identity Test, $\vec{l_W}(X)$, $\vec{r_W}(X)$ and $\vec{t_W}(X)$ Similar

Shuffle argument:

Polynomials

Vectors of polynomials:

$\vec{l}(X) \equiv_q \vec{a_L} + z^3 \vec{y^{-n}} + \vec{s_L} X^2$

$\vec{r}(X) \equiv_q \vec{y^n} \circ (\vec{a_R} X + \vec{s_R} X^3) - \vec{y_z^{n-1}} X$

Their inner product:

$t(X) \equiv_q < \vec{l}(X), \vec{r}(X) > \equiv_q t_1 X + t_3 X^3 + t_5 X^5$

These polynomials encode the initial conditions as a ZK-proof with an inner product. Construct them by calculating their coefficients. The validity of the polynomials can be proved with logarithmic communication cost by using the Bulletproof inner product protocol.

Commitments

Commit to t_3 and t_5. Committing to t_1 is not required because the value of t_1 solely depends on r, u, y, z (which are already known to the verifier) and s, s^n which the prover already committed to by the Pedersen Commitments V and W:

$t_1 \equiv_q < \vec{a_L} + z^3 \vec{y^{-n}}, \vec{a_R} \circ \vec{y^n} - \vec{y_z^{n-1}} >$

$\equiv_q z^3 s\Sigma\{\vec{k}\} + y^{n-1} s^n \Pi\{\vec{k}\} - z^3 (z + (n-1) y^{-1}) - z$

Given r, u, y, z the Commitments V and W to s and s^n are also binding t_1.

Pedersen Commitments $T_{\{3,5\}}$ to $t_{\{3,5\}}$ with blinding values $\tau_{\{3,5\}}$ are sent to the Verifier.

PR argument:

Polynomials

$\overrightarrow{l_W}(X) \equiv_q \overrightarrow{a_{L,W}} + z\,\overrightarrow{y^{-n}} + \overrightarrow{w^n} - \overrightarrow{w_0^{n-1}}\,y^{-1} + \overrightarrow{s_{L,W}}\,X$

$\overrightarrow{r_W}(X) \equiv_q \overrightarrow{y^n} \circ \left(\overrightarrow{a_{R,W}} + \overrightarrow{s_{R,W}}\,X\right) - \overrightarrow{y_z^{n-1}}$

$t_W(X) \equiv_q <\overrightarrow{l_W}(X), \overrightarrow{r_W}(X)> \equiv_q t_{0,W} + t_{1,W}\,X + t_{2,W}\,X^2$

Commitments

Commit to $t_{1,W}$ and $t_{2,W}$. Committing to $t_{0,W}$ is not required because its value only depends on y, z, w (which are already known to the verifier) and s, s^n which the prover already committed to by the Pedersen Commitments V and W:

$t_{0,W} \equiv_q <\overrightarrow{a_{L,W}} + z\,\overrightarrow{y^{-n}} + \overrightarrow{w^n} - \overrightarrow{w_0^{n-1}}\,y^{-1}, \overrightarrow{y^n} \circ \left(\overrightarrow{a_{R,W}} + \overrightarrow{s_{R,W}}\,X\right) - \overrightarrow{y_z^{n-1}}>$

$\equiv_q s^n\,y^{n-1} + s(\text{wy})^{n-1} + \text{snz} - z\left(2 + z + (n-1)\,y^{-1}\right) + \left(y^{-1} - w\right)\Sigma_{i=0}^{n-2}\,(\text{wy})^i$

Given y, z, w the commitments V and W to s and s^n are also binding $t_{0,W}$.

Pedersen Commitments $T_{\{1,2\},W}$ to $t_{\{1,2\},W}$ with blinding values $\tau_{\{1,2\},W}$ are sent to the Verifier.

In[212]:=

```
StateMachineRestore["yzw"];
(*Polynomials l⃗(X), r⃗(X) and t(X)=<l⃗(X),r⃗(X)>*)
l⃗₀ = modq[a⃗_L + powermodq[z, 3] * y⃗^-n⃗];
l⃗₂ = s⃗_L;
r⃗₁ = modq[y⃗^n⃗ * a⃗_R - y⃗_z^(n-1)⃗];
r⃗₃ = modq[y⃗^n⃗ * s⃗_R];
t₁ = modq[l⃗₀.r⃗₁];
t₃ = modq[l⃗₀.r⃗₃ + l⃗₂.r⃗₁];
t₅ = modq[l⃗₂.r⃗₃];

t1SanityCheck = (t₁ == modq[powermodq[y,n-1]*powermodq[s,n]*k̂ + z^3*s*k̄ + δ_yz]);

τ₃ = BPRandomInteger[0,q-1];
T₃ = t₃*g + τ₃*h;
TellVerifier[{"T3"→T₃,"_cost"→"group"}];
If[!interactive,FiatShamirAdd["T3",compressPoint[T₃],entropyParameters["group"]]];

τ₅ = BPRandomInteger[0,q-1];
T₅ = t₅*g + τ₅*h;
TellVerifier[{"T5"→T₅,"_cost"→"group"}];
If[!interactive,FiatShamirAdd["T5",compressPoint[T₅],entropyParameters["group"]]];

Print[Grid[{
    {Style["Name",Bold],Style["Semantics",Bold],Style["Knowledge",Bold],Style["Value",Bold]},
    {"l⃗₀ :≡_q a⃗_L + z^3*y⃗^-n⃗","","P",l⃗₀},
    {"l⃗₂ :≡_q s⃗_L","","P",l⃗₂},
    {"r⃗₁ :≡_q y⃗^n⃗*a⃗_R - y⃗_z^(n-1)⃗","","P",r⃗₁},
```

```
    {"r⃗3 :≡q y⃗^n*s⃗R","","P",r⃗3},
    {"t1 :≡q <l⃗0,r⃗1>","","P",t1},
    {"t1 ≡?q y^(n-1)s^n k̂ + z^3 sk̄ + δyz","Sanity\nCheck","P",t1SanityCheck},
    {"t3 :≡q <l⃗0,r⃗3> + <l⃗2,r⃗1>","","P",t3},
    {"τ3 ←$ ℤq","Blinding\nValue","P",τ3},
    {"T3 := t3g + τ3h","Blinded\nPedersen\nCommitment","P",T3},
    {"t5 :≡q <l⃗2,r⃗3>","","P",t5},
    {"τ5 ←$ ℤq","Blinding\nValue","P",τ5},
    {"T5 := t5g + τ5h","Blinded\nPedersen\nCommitment","P,V",T5}
}, Alignment→{{Left,Left,Left,Left}},Frame→All]]

l⃗0,W = modq[a⃗L,W + z*y⃗^-n + w⃗^n - w⃗0^(n-1)*y^-1];
l⃗1,W = s⃗L,W;
r⃗0,W = modq[a⃗R,W*y⃗^n - y⃗z^(n-1)];
r⃗1,W = modq[s⃗R,W*y⃗^n];

t0,W = modq[l⃗0,W.r⃗0,W];
t1,W = modq[l⃗0,W.r⃗1,W + l⃗1,W.r⃗0,W];
t2,W = modq[l⃗1,W.r⃗1,W];

t0WSanityCheck = (t0,W == modq[powermodq[s,n]*powermodq[y,n-1] + s*powermodq[w*y,n-1] + s*n*z

τ1,W = BPRandomInteger[0,q-1];
T1,W = t1,W*g + τ1,W*h;
TellVerifier[{"T1W"→T1,W,"_cost"→"group"}];
If[!interactive,FiatShamirAdd["T1W",compressPoint[T1,W],entropyParameters["group"]]];

τ2,W = BPRandomInteger[0,q-1];
T2,W = t2,W*g + τ2,W*h;
TellVerifier[{"T2W"→T2,W,"_cost"→"group"}];
If[!interactive,FiatShamirAdd["T2W",compressPoint[T2,W],entropyParameters["group"]]];

Print[Grid[{
    {Style["Name",Bold],Style["Semantics",Bold],Style["Knowledge",Bold],Style["Value",Bold]},
    {"l⃗0,W :≡q a⃗L,W + zy⃗^-n + w⃗^n - w⃗0^(n-1)y^-1","","P",l⃗0,W},
    {"l⃗1,W :≡q s⃗L,W","","P",l⃗1,W},
    {"r⃗0,W :≡q y⃗^n∘a⃗R,W - y⃗z^(n-1)","","P",r⃗0,W},
    {"r⃗1,W :≡q y⃗^n∘s⃗R,W","","P",r⃗1,W},
    {"t0,W :≡q <l⃗0,W,r⃗0,W>","","P",t0,W},
    {"t0,W ≡?q s^n y^(n-1) + s(wy)^(n-1) + snz + δyzw","Sanity\nCheck","P",t0WSanityCheck},
    {"t1,W :≡q <l⃗0,W,r⃗1,W> + <l⃗1,W,r⃗0,W>","","P",t1,W},
```

```
    {"τ1,W ←$ ℤq","Blinding\nValue","P",τ1,W},
    {"T1,W := t1,Wg + τ1,Wh","Blinded\nPedersen\nCommitment","P",T1,W},
    {"t2,W :≡q <l1,W⃗,r1,W⃗>","","P",t2,W},
    {"τ2,W ←$ ℤq","Blinding\nValue","P",τ2,W},
    {"T2,W := t2,Wg + τ2,Wh","Blinded\nPedersen\nCommitment","P,V",T2,W}
}, Alignment→{{Left,Left,Left,Left}},Frame→All]]

Print[CommunicationCostGrid[]]
If[!interactive,Print[FiatShamirGrid[]]];
ProcessNewMessages[];
StateMachineSave["T3T5T1WT2W"];

If[!t1SanityCheck, Error["Sanity check on t1 failed"]];
If[!t0WSanityCheck, Error["Sanity check on t0,W failed"]];
```

Name	Semantics	Knowledge	Value
$\vec{l_0} :\equiv_q \vec{a_L} + z^3 * \vec{y^{-n}}$		P	{41 657 547 058 195 369 887 969 380 379 391 826 870 - 689 859 531 449 638 952 980 121 370 454 726 046 738, 106 298 129 028 940 068 718 446 818 765 598 914 310 - 163 520 912 662 135 604 879 656 710 678 866 680 784, 112 187 184 766 458 299 600 187 014 231 777 667 882 - 396 181 865 332 448 266 817 570 389 648 165 255 801}
$\vec{l_2} :\equiv_q \vec{s_L}$		P	{3 490 043 951 473 342 957 863 269 612 888 825 370 - 966 098 959 732 202 668 461 366 396 201 773 608 447, 81 026 870 043 438 310 759 789 738 090 565 752 971 - 348 726 422 705 469 591 555 083 035 827 778 970 747, 109 413 017 180 886 544 487 921 683 678 413 534 566 - 795 499 839 518 913 016 004 076 708 382 233 891 835}
$\vec{r_1} :\equiv_q \vec{y^n} * \vec{a_R} - \vec{y_z^{n-1}}$		P	{10 993 433 797 003 774 729 218 027 487 920 469 273 - 114 588 191 009 865 801 847 783 921 014 444 079 168, 11 354 026 302 141 574 451 034 441 182 404 490 723 - 723 477 775 467 803 440 545 870 650 161 445 488 981, 105 706 180 023 698 065 997 628 478 104 086 474 248 - 873 435 575 500 703 138 718 731 566 008 233 226 456}
$\vec{r_3} :\equiv_q \vec{y^n} * \vec{s_R}$		P	{12 507 601 888 368 634 928 041 736 808 448 324 961 - 591 369 924 503 374 677 351 026 235 158 490 466 997, 75 063 628 109 797 149 256 105 527 927 449 488 258 - 930 503 270 355 261 261 081 058 934 516 068 355 931, 102 600 916 682 950 816 645 279 194 971 871 331 028 - 630 335 245 819 709 075 407 615 110 362 150 482 917}
$t_1 :\equiv_q <\vec{l_0}, \vec{r_1}>$		P	93 602 564 524 346 269 892 139 081 003 287 774 548 992 - 121 120 157 431 994 066 307 419 111 641 258 652
$t_1 \overset{?}{\equiv}_q y^{n-1} s^n \hat{k} + z^3 s\overline{k} + \delta_{yz}$	Sanity Check	P	True
$t_3 :\equiv_q <\vec{l_0}, \vec{r_3}> + <\vec{l_2}, \vec{r_1}>$		P	17 310 733 161 837 013 592 816 310 149 157 017 810 465 - 542 261 843 218 431 452 323 969 115 777 752 129
$\tau_3 \overset{\$}{\leftarrow} \mathbb{Z}_q$	Blinding Value	P	103 025 787 400 053 846 491 173 493 263 859 547 421 - 436 948 279 868 469 816 606 692 097 792 288 570 268
$T_3 := t_3 g + \tau_3 h$	Blinded Pedersen Commitment	P	ecPnt[14 448 711 964 151 254 610 079 813 969 094 599 304 - 991 556 686 032 655 240 425 388 262 152 998 792 866, 35 818 652 155 586 706 410 279 698 238 883 774 802 - 777 588 417 348 300 197 902 141 088 629 232 808 578]
$t_5 :\equiv_q <\vec{l_2}, \vec{r_3}>$		P	79 350 839 946 051 578 713 775 231 271 034 862 562 040 - 122 148 254 790 044 338 660 946 167 057 333 318
$\tau_5 \overset{\$}{\leftarrow} \mathbb{Z}_q$	Blinding Value	P	95 538 448 397 885 489 565 925 196 202 909 322 984 569 - 275 766 270 781 222 063 297 280 902 331 526 819
$T_5 := t_5 g + \tau_5 h$	Blinded Pedersen Commitment	P,V	ecPnt[95 840 125 068 125 223 175 775 950 838 735 910 594 - 996 026 329 945 329 600 069 894 500 083 191 471 477, 92 410 008 359 066 548 507 274 553 560 973 459 366 - 308 871 128 888 129 891 539 618 716 611 325 817 962]

Name	Semantics	Knowledge	Value
$\overrightarrow{l_{0,W}} :\equiv_q \overrightarrow{a_{L,W}} + z\overrightarrow{y^{-n}} + \overrightarrow{w^n} - \overrightarrow{w_0^{n-1}} y^{-1}$		P	{51 229 650 329 065 518 720 689 096 099 - 379 898 312 022 759 911 804 433 524 - 422 971 782 942 501 299 480, 77 079 792 619 893 203 207 390 047 713 - 451 532 103 437 765 986 802 911 443 - 855 568 027 938 366 025 167, 109 616 591 388 320 226 103 025 361 083 - 127 875 271 381 440 895 268 887 107 -

$\overrightarrow{l_{1,W}} :\equiv_q \overrightarrow{s_{L,W}}$		P	{1, 103 449 002 380 076 435 222 853 190 046 - 878 651 498 924 569 833 450 391 518 - 456 216 468 185 080 813 412, 9 669 727 685 888 435 741 682 791 084 - 323 628 869 249 804 294 902 520 995 - 644 873 285 051 619 396 679}
$\overrightarrow{r_{0,W}} :\equiv_q \overrightarrow{y^n} \circ \overrightarrow{a_{R,W}} - \overrightarrow{y_z^{n-1}}$		P	{25 825 765 890 430 958 576 769 621 930 - 206 825 127 638 606 960 089 656 953 - 579 218 384 125 466 732 125, 115 786 897 504 926 759 496 674 515 511 - 597 565 609 294 417 497 090 911 830 - 825 553 814 493 135 569 221, 85 238 881 810 462 861 778 154 634 566 - 274 840 669 309 115 995 383 175 922 - 195 334 731 544 491 411 290}
$\overrightarrow{r_{1,W}} :\equiv_q \overrightarrow{y^n} \circ \overrightarrow{s_{R,W}}$		P	{103 449 002 380 076 435 222 853 190 046 - 878 651 498 924 569 833 450 391 518 - 456 216 468 185 080 813 412, 81 291 812 613 426 233 599 865 925 245 - 264 344 266 181 313 482 798 641 891 - 693 887 914 853 309 758 911, 111 678 130 623 575 204 275 990 686 680 - 453 005 379 845 562 243 200 444 033 - 306 720 120 664 769 523 117}
$t_{0,W} :\equiv_q <\overrightarrow{l_{0,W}}, \overrightarrow{r_{0,W}}>$		P	115 428 419 536 990 563 622 497 737 220 - 890 433 953 385 650 229 883 155 466 883 - 980 685 552 757 962 124
$t_{0,W} \stackrel{?}{\equiv_q} s^n y^{n-1} + s(wy)^{n-1} + snz + \delta_{yzw}$	Sanity Check	P	True
$t_{1,W} :\equiv_q <\overrightarrow{l_{0,W}}, \overrightarrow{r_{1,W}}> + <\overrightarrow{l_{1,W}}, \overrightarrow{r_{0,W}}>$		P	42 934 228 482 704 277 171 589 913 215 - 541 505 806 599 900 158 099 704 059 586 - 670 717 978 694 400 618
$\tau_{1,W} \stackrel{\$}{\leftarrow} \mathbb{Z}_q$	Blinding Value	P	91 690 863 698 252 499 759 127 603 862 - 000 154 779 781 812 325 324 670 430 965 - 064 128 712 168 545 446
$T_{1,W} := t_{1,W} g + \tau_{1,W} h$	Blinded Pedersen Commitment	P	ecPnt[5 443 615 670 032 252 682 449 032 168 - 926 607 403 789 720 879 129 525 399 - 520 688 082 435 286 679 707, 11 580 758 803 798 338 542 986 116 920 - 898 026 390 002 352 514 999 381 201 - 524 511 845 767 931 697 226]
$t_{2,W} :\equiv_q <\overrightarrow{l_{1,W}}, \overrightarrow{r_{1,W}}>$		P	31 797 358 138 604 843 034 824 747 433 - 975 683 328 471 314 573 082 373 928 816 - 157 681 987 041 467 600
$\tau_{2,W} \stackrel{\$}{\leftarrow} \mathbb{Z}_q$	Blinding Value	P	4 010 814 831 465 664 235 548 265 476 115 - 974 139 001 360 816 736 986 103 882 851 - 010 375 142 831 463

$T_{2,w} := t_{2,w} g + \tau_{2,w} h$	Blinded Pedersen Commitment	P,V	ecPnt[46 991 716 425 756 598 968 559 577 543 - 620 785 423 160 955 041 139 713 706 - 964 410 377 968 981 965 216, 46 577 312 793 355 582 843 140 851 773 - 728 623 285 608 758 891 207 244 980 - 306 676 861 718 908 945 325]

Total Communication Cost			
Type	**Count**	**Names**	**Bits**
group	14	V, W, AW, SW, AL, SL, SRh, SRb, SRc, SRd, T3, T5, T1W, T2W	3598
scalar	5	r, u, y, z, w	1280
total	19		4878

Evaluate $t(X)$ and $t_W(X)$ with Random Challenge x

Receive random challenge x which is the evaluation point of $t(X = x)$ and $t_W(X = x)$

In[253]:=

```
StateMachineRestore["T3T5T1WT2W"];

(*Get random challenge x (evaluation point of t(X=x))*)
If[interactive,
(*Random challenge from interactive verifier*)
    x = WaitForRandomChallenge["x"];
(*Else*),
(*Fiat-Shamir*)
    x = FiatShamirGet["x",q,entropyParameters["scalar"]];
    TellVerifier[{"x"→x,"_cost"→"scalar"}];
];

Print[Grid[{
    {Style["Name",Bold],Style["Semantics",Bold],Style["Knowledge",Bold],Style["Value",Bold]},
    {"x",semanticsOfRandomChallenge,"P,V",x}
}, Alignment→{{Left,Left,Left,Left}},Frame→All]]


Print[CommunicationCostGrid[]]
If[!interactive,Print[FiatShamirGrid[]]];
ProcessNewMessages[];
StateMachineSave["x"];
```

Waiting to receive x from InteractiveVerifier ...

Name	Semantics	Knowledge	Value
x	Random Challenge	P,V	113 126 916 120 434 927 118 052 636 603 002 490 980 047 778 302 346 487 - 448 691 688 890 663 263 893 727

Total Communication Cost			
Type	**Count**	**Names**	**Bits**
group	14	V, W, AW, SW, AL, SL, SRh, SRb, SRc, SRd, T3, T5, T1W, T2W	3598
scalar	6	r, u, y, z, w, x	1536
total	20		5134

Commit to $t(x)$ and $t_W(x)$

Shuffle argument:

Calculate a combined commitment $\hat{t}$ to $t(X)$ at the challenge point $X = x$ using blinding factors τ_3, τ_5 and σ_W from previous Pedersen Commitments T_3, T_5, V and W as well as blinding factors α, β and $\rho_{\{h,b,c,d\}}$ of previous Pedersen Vector Commitments A_L, S_L and $S_{R,\{h,b,c,d\}}$ resulting in

$\tau_x := \sigma_W \, \text{ny}^{n-1} \, \hat{k} \, x \, + \, \tau_3 \, x^3 \, + \, \tau_5 \, x^5$,

$\mu_{\{h,b,c,d\}} := \alpha + \beta x^2 + \rho_{\{h,b,c,d\}} \, x^3$ and

$\hat{t} := < \vec{l}, \vec{r} >$

which are sent to V.

Without the inner product protocol

$\vec{l}$ and $\vec{r}$ have to be sent to V to verify the correctness of the inner product. This causes the communication cost to become linear in the length of $\vec{l}$ and $\vec{r}$, which is n.

PR argument:

Calculate a combined commitment $\hat{t_W}$ to $t_W(X)$ at the challenge point $X = x$ using blinding factors $\tau_{1,W}$, $\tau_{2,W}$ and σ_W from previous Pedersen Commitments $T_{1,W}$, $T_{2,W}$, V and W as well as blinding factors α_W and β_W of previous Pedersen Vector Commitments A_W and S_W resulting in

$\tau_{x,W} := \sigma_W \, y^{n-1} \, + \, \tau_{1,W} \, x \, + \, \tau_{2,W} \, x^2$,

$\mu_W := \alpha + \beta x$ and

$\hat{t_W} := < \overrightarrow{l_W}, \overrightarrow{r_W} >$

which are sent to V.

Without the inner product protocol

$\overrightarrow{l_W}$ and $\overrightarrow{r_W}$ have to be sent to V to verify the correctness of the inner product. This causes the communication cost to become linear in the length of $\overrightarrow{l_W}$ and $\overrightarrow{r_W}$, which is n.

In[260]:=

```
StateMachineRestore["x"];

τx = modq[(σw*powermodq[y,n-1]*k̂)*x + τ3*x^3 + τ5*x^5];
TellVerifier[{"taux"→τx,"_cost"→"scalar"}];
If[!interactive,FiatShamirAdd["taux",τx,entropyParameters["scalar"]]];

μh = modq[α + β*x^2 + ρh*x^3];
μb = modq[α + β*x^2 + ρb*x^3];
μc = modq[α + β*x^2 + ρc*x^3];
μd = modq[α + β*x^2 + ρd*x^3];
TellVerifier[{"muh"→μh,"_cost"→"scalar"}];
TellVerifier[{"mub"→μb,"_cost"→"scalar"}];
TellVerifier[{"muc"→μc,"_cost"→"scalar"}];
TellVerifier[{"mud"→μd,"_cost"→"scalar"}];
If[!interactive,
    FiatShamirAdd["muh",μh,entropyParameters["scalar"]];
    FiatShamirAdd["mub",μb,entropyParameters["scalar"]];
    FiatShamirAdd["muc",μc,entropyParameters["scalar"]];
    FiatShamirAdd["mud",μd,entropyParameters["scalar"]];
];
```

```
l̂ = modq[l⃗0 + l⃗2*x^2];
r̂ = modq[r⃗1*x + r⃗3*x^3];
t̂ = modq[l⃗.r⃗];
TellVerifier[{"t"→t̂,"_cost"→"scalar"}];
If[!interactive,FiatShamirAdd["t",t̂,entropyParameters["scalar"]]];

h⃗* = y⃗^-n*h⃗;
b⃗* = y⃗^-n*b⃗;
c⃗* = y⃗^-n*c⃗;
d⃗* = y⃗^-n*d⃗;

(*For sanity checks*)
P_h^+ = A_L + A_R,h*x + S_L*x^2 + S_R,h*x^3 + g⃗.(z^3*y⃗^-n) + h⃗*.(-x*y⃗_z^n-1);
P_b^+ = A_L + A_R,b*x + S_L*x^2 + S_R,b*x^3 + g⃗.(z^3*y⃗^-n) + b⃗*.(-x*y⃗_z^n-1);
P_c^+ = A_L + A_R,c*x + S_L*x^2 + S_R,c*x^3 + g⃗.(z^3*y⃗^-n) + c⃗*.(-x*y⃗_z^n-1);
P_d^+ = A_L + A_R,d*x + S_L*x^2 + S_R,d*x^3 + g⃗.(z^3*y⃗^-n) + d⃗*.(-x*y⃗_z^n-1);

Print[Grid[{
    {Style["Name",Bold],Style["Semantics",Bold],Style["Knowledge",Bold],Style["Value",Bold]},
    {"τ_x :≡_q σ_W*y^n-1*k̂x + τ_3*x^3 + τ_5*x^5","Combined Commitment\nto Blinding Values\nof Commitments\
    {"μ_h :≡_q α + β*x^2 + ρ_h*x^3","Combined Commitment\nto Blinding Values\nof Vector Commitments\n
    {"μ_b :≡_q α + β*x^2 + ρ_b*x^3","Combined Commitment\nto Blinding Values\nof Vector Commitments\n
    {"μ_c :≡_q α + β*x^2 + ρ_c*x^3","Combined Commitment\nto Blinding Values\nof Vector Commitments\n
    {"μ_d :≡_q α + β*x^2 + ρ_d*x^3","Combined Commitment\nto Blinding Values\nof Vector Commitments\n
    {"l⃗ :≡_q l⃗0 + l⃗2*x^2 = a⃗_L + z^3*y⃗^-n + s⃗_L*x^2","Left side of inner product",If[useInnerProductProto
    {"r⃗ :≡_q r⃗1*x + r⃗3*x^3 = (y⃗^n*a⃗_R - y⃗_z^n-1)*x + y⃗^n*s⃗_R*x^3","Right side of inner product",If[useInnerPr
    {"t̂ :≡_q <l⃗,r⃗>","Inner Product","P,V",t̂},
    {"P_h^+ := A_L + A_R,h*x + S_L*x^2 + S_R,h*x^3 + <g⃗,z^3*y⃗^-n> + <h⃗*,-x*y⃗_z^n-1>","Combination of\nShuffle Proof
    {"P_b^+ := A_L + A_R,b*x + S_L*x^2 + S_R,b*x^3 + <g⃗,z^3*y⃗^-n> + <b⃗*,-x*y⃗_z^n-1>","Combination of\nShuffle Proof
    {"P_c^+ := A_L + A_R,c*x + S_L*x^2 + S_R,c*x^3 + <g⃗,z^3*y⃗^-n> + <c⃗*,-x*y⃗_z^n-1>","Combination of\nShuffle Proof
    {"P_d^+ := A_L + A_R,d*x + S_L*x^2 + S_R,d*x^3 + <g⃗,z^3*y⃗^-n> + <d⃗*,-x*y⃗_z^n-1>","Combination of\nShuffle Proof
}, Alignment→{{Left,Left,Left,Left}},Frame→All]]

τ_x,W = modq[σ_W*powermodq[y,n-1] + τ_1,W*x + τ_2,W*x^2];
TellVerifier[{"tauxW"→τ_x,W,"_cost"→"scalar"}];
If[!interactive,FiatShamirAdd["tauxW",τ_x,W,entropyParameters["scalar"]]];

μ_W = modq[α_W + β_W*x];
TellVerifier[{"muW"→μ_W,"_cost"→"scalar"}];
If[!interactive, FiatShamirAdd["muW",μ_W,entropyParameters["scalar"]]];
```

```
l⃗_W = modq[l⃗_{0,W} + l⃗_{1,W}*x];
r⃗_W = modq[r⃗_{0,W} + r⃗_{1,W}*x];
t̂_W = modq[l⃗_W.r⃗_W];
TellVerifier[{"tW"→t̂_W,"_cost"→"scalar"}];
If[!interactive,FiatShamirAdd["tW",t̂_W,entropyParameters["scalar"]]];

(*For sanity checks*)
P⁺_W = A_W + S_W*x + g⃗.(z*y^-n⃗ + w⃗^n⃗ - w⃗_0^{n-1}*y^{-1}) + h⃗*.(-y⃗_z^{n-1});

Print[Grid[{
    {Style["Name",Bold],Style["Semantics",Bold],Style["Knowledge",Bold],Style["Value",Bold]},
    {"τ_{x,W} :≡_q σ_W y^{n-1} + τ_{1,W}x + τ_{2,W}x^2","Combined Commitment\nto Blinding Values\nof Commitments\
    {"μ_W :≡_q α_W + β_W x","Combined Commitment\nto Blinding Values\nof Vector Commitments\nto a⃗_...,
    {"l⃗_W :≡_q l⃗_{0,W} + l⃗_{1,W}x = a⃗_{L,W} + z y^-n⃗ + w⃗^n⃗ - w⃗_0^{n-1} y^{-1} + s⃗_{L,W}x","Left side of inner product (W)",I
    {"r⃗_W :≡_q r⃗_{0,W} + r⃗_{1,W}x = a⃗_{R,W}∘y⃗^n⃗ - y⃗_z^{n-1} + s⃗_{R,W}∘y⃗^n⃗ x","Right side of inner product (W)",If[useInn
    {"t̂_W :≡_q <l⃗_W,r⃗_W>","Inner Product","P,V",t̂_W},
    {"P⁺_W := A_W + S_W x + <g⃗,z y^-n⃗ + w⃗^n⃗ - w⃗_0^{n-1} y^{-1}> + <h⃗*,-y⃗_z^{n-1}>","Combination of\nProof Conditions","P,V
}, Alignment→{{Left,Left,Left,Left}},Frame→All]]

If[useInnerProductProtocol,
    Print[CommunicationCostGrid[]];
    If[!interactive,Print[FiatShamirGrid[]]];
];
ProcessNewMessages[];
StateMachineSave["mk_shuffle_argument"];

If[!useInnerProductProtocol,
    TellVerifier[{"lvec"→l⃗,"rvec"→r⃗,"_cost"→"scalar"}];
    TellVerifier[{"lWvec"→l⃗_W,"rWvec"→r⃗_W,"_cost"→"scalar"}];
    Print[CommunicationCostGrid[]];
    If[!interactive,Print[FiatShamirGrid[]]];
    ProcessNewMessages[];
    StateMachineSave["inner_product_argument_linear"];
];
```

Name	Semantics	Knowledge	Value
$\tau_x :\equiv_q \sigma_W n y^{n-1} \hat{k} x + \tau_3 x^3 + \tau_5 x^5$	Combined Commitment to Blinding Values of Commitments to Coefficiencts of t(X)	P,V	90 664 101 823 773 446 617 - 843 295 664 000 476 824 - 583 008 189 854 797 930 - 932 933 141 663 523 670 972
$\mu_h :\equiv_q \alpha + \beta x^2 + \rho_h x^3$	Combined Commitment to Blinding Values of Vector Commitments to $\vec{a}_{...}$ and $\vec{s}_{...}$ Based on $\vec{h}$	P,V	92 385 493 365 820 873 701 - 351 823 187 030 658 379 - 688 852 573 645 079 038 - 085 937 803 029 996 581 426

$\mu_b :\equiv_q \alpha + \beta x^2 + \rho_b x^3$	Combined Commitment to Blinding Values of Vector Commitments to $\overrightarrow{a_{\ldots}}$ and $\overrightarrow{s_{\ldots}}$ Based on $\vec{b}$	P,V	80 465 903 251 238 947 246 - 948 019 231 634 112 958 - 643 085 797 558 256 913 - 390 431 732 924 637 611 796
$\mu_c :\equiv_q \alpha + \beta x^2 + \rho_c x^3$	Combined Commitment to Blinding Values of Vector Commitments to $\overrightarrow{a_{\ldots}}$ and $\overrightarrow{s_{\ldots}}$ Based on $\vec{c}$	P,V	95 467 333 988 398 325 705 - 770 893 951 601 989 203 - 373 334 565 084 410 378 - 751 725 991 298 886 477 561
$\mu_d :\equiv_q \alpha + \beta x^2 + \rho_d x^3$	Combined Commitment to Blinding Values of Vector Commitments to $\overrightarrow{a_{\ldots}}$ and $\overrightarrow{s_{\ldots}}$ Based on $\vec{d}$	P,V	20 751 440 986 732 760 450 - 071 315 784 341 311 844 - 859 651 372 502 581 770 - 822 695 204 710 647 943 339
$\vec{l} :\equiv_q \overrightarrow{l_0} + \overrightarrow{l_2} x^2 = \overrightarrow{a_L} + z^3 \overrightarrow{y^{-n}} + \overrightarrow{s_L} x^2$	Left side of inner product	P	{61 442 343 775 113 140 880 - 034 650 887 022 378 965 - 571 424 979 173 001 973 - 397 458 542 222 999 566 - 892, 112 164 513 297 470 756 - 571 473 984 141 438 273 - 936 195 334 402 062 428 - 015 459 026 081 712 107 - 932 702, 100 474 102 720 414 684 - 705 898 037 977 251 389 - 482 922 603 087 723 310 - 707 681 533 634 105 023 - 940 360}
$\vec{r} :\equiv_q \overrightarrow{r_1} x + \overrightarrow{r_3} x^3 = (\overrightarrow{y^n} * \overrightarrow{a_R} - \overrightarrow{y_z^{n-1}}) x + \overrightarrow{y^n} * \overrightarrow{s_R} x^3$	Right side of inner product	P	{62 425 708 243 501 832 904 - 842 395 569 180 717 767 - 201 166 970 569 719 744 - 186 579 509 066 013 239 - 789, 108 894 093 373 790 087 - 805 981 249 637 450 006 - 012 557 717 717 172 910 - 157 161 661 185 273 450 - 166 896, 80 085 874 135 138 745 719 - 381 189 911 405 897 849 - 137 938 574 627 947 766 - 879 149 979 384 405 495 - 240}
$\hat{t} :\equiv_q \langle \vec{l}, \vec{r} \rangle$	Inner Product	P,V	61 129 420 188 541 223 894 - 451 420 484 118 730 665 - 755 170 250 056 245 755 - 694 030 172 042 596 198 303

$P_h^+ := A_L + A_{R,h}x + S_L x^2 + S_{R,h}x^3 + \langle \vec{g}, z^3 \overrightarrow{y^{-n}} \rangle + \langle \overrightarrow{h^*}, -x\overrightarrow{y_z^{n-1}} \rangle$	Combination of Shuffle Proof Conditions Based on $\vec{h}$	P,V (implicit)	ecPnt[68 134 367 815 685 539 320 - 190 632 885 130 065 825 - 701 945 083 234 713 508 - 025 960 470 144 473 344 - 675, 57 057 786 625 709 188 163 - 226 575 896 005 778 466 - 275 330 778 044 925 156 - 082 592 124 488 928 313 - 021]
$P_b^+ := A_L + A_{R,b}x + S_L x^2 + S_{R,b}x^3 + \langle \vec{g}, z^3 \overrightarrow{y^{-n}} \rangle + \langle \overrightarrow{b^*}, -x\overrightarrow{y_z^{n-1}} \rangle$	Combination of Shuffle Proof Conditions Based on $\vec{b}$	P,V (implicit)	ecPnt[8 381 827 224 951 560 516 - 410 678 631 442 837 234 - 140 159 317 202 180 585 - 971 642 325 678 405 568 - 599, 55 294 642 855 621 885 832 - 206 585 462 356 149 779 - 761 500 855 110 315 060 - 905 091 944 627 323 232 - 720]
$P_c^+ := A_L + A_{R,c}x + S_L x^2 + S_{R,c}x^3 + \langle \vec{g}, z^3 \overrightarrow{y^{-n}} \rangle + \langle \overrightarrow{c^*}, -x\overrightarrow{y_z^{n-1}} \rangle$	Combination of Shuffle Proof Conditions Based on $\vec{c}$	P,V (implicit)	ecPnt[71 060 614 614 726 964 844 - 841 050 209 662 544 841 - 436 795 838 725 410 843 - 630 775 082 526 405 660 - 776, 51 060 476 566 888 976 486 - 057 719 488 149 331 904 - 233 889 574 405 726 895 - 197 173 183 965 366 374 - 158]
$P_d^+ := A_L + A_{R,d}x + S_L x^2 + S_{R,d}x^3 + \langle \vec{g}, z^3 \overrightarrow{y^{-n}} \rangle + \langle \overrightarrow{d^*}, -x\overrightarrow{y_z^{n-1}} \rangle$	Combination of Shuffle Proof Conditions Based on $\vec{d}$	P,V (implicit)	ecPnt[66 465 324 627 263 336 532 - 146 408 729 756 836 335 - 057 582 441 146 307 404 - 090 554 564 562 609 272 - 383, 74 976 372 031 831 417 982 - 725 102 916 500 867 410 - 765 456 237 244 437 849 - 779 579 427 264 167 479 - 480]

Name	Semantics	Knowledge	Value
$\tau_{x,W} :\equiv_q \sigma_W y^{n-1} + \tau_{1,W}x + \tau_{2,W}x^2$	Combined Commitment to Blinding Values of Commitments to Coefficiencts of $t_W(X)$	P,V	113 405 409 346 918 773 496 - 790 428 795 432 108 361 - 840 287 177 160 539 700 - 287 912 972 625 911 562 666

$\mu_W :\equiv_q \alpha_W + \beta_W x$	Combined Commitment to Blinding Values of Vector Commitments to $\overrightarrow{a_{\ldots,W}}$ and $\overrightarrow{s_{\ldots,W}}$	P,V	58 938 274 415 372 746 259 - 906 244 789 991 376 153 - 504 860 263 629 609 061 - 215 650 209 757 990 735 313
$\overrightarrow{l_W} :\equiv_q \overrightarrow{l_{0,W}} + \overrightarrow{l_{1,W}} x = \overrightarrow{a_{L,W}} + z\overrightarrow{y^n} + \overrightarrow{w^n} - \overrightarrow{w_0^{n-1}} y^{-1} + \overrightarrow{s_{L,W}} x$	Left side of inner product (W)	P	{48 564 477 212 184 250 415 - 170 747 693 694 481 439 - 232 973 935 076 016 590 - 509 497 532 087 603 698 - 870, 8 819 342 647 412 475 122 - 593 262 319 876 611 403 - 831 739 595 798 027 640 - 620 830 864 043 632 355 - 299, 115 268 474 747 795 881 - 775 546 216 783 739 194 - 713 511 413 966 655 407 - 981 146 926 754 407 903 - 409 076}
$\overrightarrow{r_W} :\equiv_q \overrightarrow{r_{0,W}} + \overrightarrow{r_{1,W}} x = \overrightarrow{a_{R,W}} \circ \overrightarrow{y^n} - \overrightarrow{y_z^{n-1}} + \overrightarrow{s_{R,W}} \circ \overrightarrow{y^n} x$	Right side of inner product (W)	P	{73 357 405 155 266 425 915 - 543 821 545 319 812 280 - 870 144 848 159 677 532 - 949 644 361 748 894 556 - 594, 26 473 080 131 638 368 664 - 311 419 668 052 580 406 - 527 293 561 077 903 757 - 204 398 370 221 010 052 - 161, 8 085 424 818 135 938 036 - 088 244 802 558 875 166 - 648 813 733 660 931 210 - 189 856 208 497 918 675 - 798}
$\hat{t_W} :\equiv_q \langle \overrightarrow{l_W}, \overrightarrow{r_W} \rangle$	Inner Product	P,V	90 204 149 990 177 783 895 - 906 378 904 605 018 924 - 475 164 996 067 056 805 - 508 398 362 658 462 387 712
$P_W^+ := A_W + S_W x + \langle \vec{g}, z\overrightarrow{y^{-n}} + \overrightarrow{w^n} - \overrightarrow{w_0^{n-1}} y^{-1} \rangle + \langle \overrightarrow{h^*}, -\overrightarrow{y_z^{n-1}} \rangle$	Combination of Proof Conditions	P,V (implicit)	ecPnt[62 669 714 302 428 955 472 - 761 791 525 432 435 845 - 370 874 536 737 033 196 - 110 472 891 537 070 589 - 279, 65 866 759 044 570 794 612 - 429 414 870 223 877 980 - 436 386 678 506 116 073 - 507 246 268 188 823 492 - 288]

Total Communication Cost			
Type	Count	Names	Bits
group	14	V, W, AW, SW, AL, SL, SRh, SRb, SRc, SRd, T3, T5, T1W, T2W	3598
scalar	15	r, u, y, z, w, x, taux, muh, mub, muc, mud, t, tauxW, muW, tW	3840
total	29		7438

Verifier's Last Checks Before the Inner Product Protocol

Performing the checks that V will do to confirm P's proof convinces V. Checks for PR argument are postfixed with "W".

In all cases:

1) $\hat{t}\, g + \tau_x\, h \stackrel{?}{=} z^3\, \overline{k}\, \mathrm{xV} + y^{n-1}\, \hat{k}\, \mathrm{xW} + \delta_{\mathrm{yz}}\, \mathrm{xg} + x^3\, T_3 + x^5\, T_5$

1W) $\hat{t_W}\, g + \tau_{x,W}\, h \stackrel{?}{=} \left((\mathrm{wy})^{n-1} + \mathrm{nz}\right) V + y^{n-1}\, W + \delta_{\mathrm{yzw}}\, g + \mathrm{xT}_{1,W} + x^2\, T_2$

Without the Inner Product Protocol

2) $P^{+}_{\{h,b,c,d\}} \stackrel{?}{=} \mu_{\{h,b,c,d\}}\, h + < \vec{g},\ \vec{l} > + < \overrightarrow{\{h,\, b,\, c,\, d\}^*},\ \vec{r} >$

3) $\hat{t} \stackrel{?}{=} < \vec{l},\ \vec{r} >$

2W) $P^{+}_{W} \stackrel{?}{=} \mu_W\, h + < \vec{g},\ \overrightarrow{l_W} > + < \overrightarrow{\{h\}^*},\ \overrightarrow{r_W} >$

3W) $\hat{t_W} \stackrel{?}{=} < \overrightarrow{l_W},\ \overrightarrow{r_W} >$

When using the Inner Product Protocol 2), 3), 2W) and 3W) are proved indirectly.

In[304]:=

```
StateMachineRestore[If[useInnerProductProtocol,"mk_shuffle_argument","inner_product_argument_

(*1) t̂g + τₓh ≟ z³k̄xV + y^(n-1)k̂xW + δ_yzxg + x³T₃ + x⁵T₅*)
selfCheck1 = (g*t̂+h*τₓ==V*(z^3*k̄*x) + W*(powermodq[y,n-1]*k̂*x) + g*(δ_yz*x) + T₃*x^3 + T₅*x^5)
Print[Grid[{
    {Style["Name",Bold],Style["Semantics",Bold],Style["Value",Bold]},
    {"gt̂ + hτₓ","",g*t̂ + h*τₓ},
    {"≟ z³k̄xV + y^(n-1)k̂xW + δ_yzxg + x³T₃ + x⁵T₅","V's Check",selfCheck1}
}, Alignment→{{Left,Left,Left}},Frame→All]]
If[!selfCheck1, Error["Assertion failure on self-check 1 (gt̂ + hτₓ ≟ ...)"]];

(*2) P⁺_{h,b,c,d} ≟ hμ_{h,b,c,d} + <g⃗,l⃗> + <{h,b,c,d}*,r⃗>*)
selfCheck2h = (P⁺ₕ==h*μₕ+g⃗.l⃗+h⃗*.r⃗);
Print[Grid[{
    {Style["Name",Bold],Style["Semantics",Bold],Style["Value",Bold]},
    {"P⁺ₕ ≟ A_L + A_{R,h}x + S_Lx² + S_{R,h}x³ + <g⃗,z³y⃗^-n> + <h⃗*,-xy⃗^(n-1)>","Definition of P⁺ₕ",P⁺ₕ == A_L + A_{R,
    {"≟ hμₕ + <g⃗,l⃗> + <h⃗*,r⃗>","V's Check\nWithout Inner\nProduct Protocol",selfCheck2h}
}, Alignment→{{Left,Left,Left}},Frame→All]];
If[!selfCheck2h, Error["Assertion failure on self-check 2h (P⁺ₕ ≟ hμₕ + <g⃗,l⃗> + <h⃗*,r⃗>)"]];
selfCheck2b = (P⁺_b==h*μ_b+g⃗.l⃗+b⃗*.r⃗);
Print[Grid[{
```

```
    {Style["Name",Bold],Style["Semantics",Bold],Style["Value",Bold]},
    {"P_b^+ ≟ A_L + A_R,b x + S_L x^2 + S_R,b x^3 + <g⃗,z^3 y^-n⃗> + <b⃗*,-x y_z^n-1⃗>","Definition of P_b^+",P_b^+ == A_L + A_R,
    {"≟ hμ_b + <g⃗,l⃗> + <b⃗*,r⃗>","V's Check\nWithout Inner\nProduct Protocol",selfCheck2b}
}, Alignment→{{Left,Left,Left}},Frame→All]];
If[!selfCheck2b, Error["Assertion failure on self-check 2b (P_b^+ ≟ hμ_b + <g⃗,l⃗> + <b⃗*,r⃗>)"]];
selfCheck2c = (P_c^+==h*μ_c+g⃗.l⃗+c⃗*.r⃗);
Print[Grid[{
    {Style["Name",Bold],Style["Semantics",Bold],Style["Value",Bold]},
    {"P_c^+ ≟ A_L + A_R,c x + S_L x^2 + S_R,c x^3 + <g⃗,z^3 y^-n⃗> + <c⃗*,-x y_z^n-1⃗>","Definition of P_c^+",P_c^+ == A_L + A_R,
    {"≟ hμ_c + <g⃗,l⃗> + <c⃗*,r⃗>","V's Check\nWithout Inner\nProduct Protocol",selfCheck2c}
}, Alignment→{{Left,Left,Left}},Frame→All]];
If[!selfCheck2c, Error["Assertion failure on self-check 2c (P_c^+ ≟ hμ_c + <g⃗,l⃗> + <c⃗*,r⃗>)"]];
selfCheck2d = (P_d^+==h*μ_d+g⃗.l⃗+d⃗*.r⃗);
Print[Grid[{
    {Style["Name",Bold],Style["Semantics",Bold],Style["Value",Bold]},
    {"P_d^+ ≟ A_L + A_R,d x + S_L x^2 + S_R,d x^3 + <g⃗,z^3 y^-n⃗> + <d⃗*,-x y_z^n-1⃗>","Definition of P_d^+",P_d^+ == A_L + A_R,
    {"≟ hμ_d + <g⃗,l⃗> + <d⃗*,r⃗>","V's Check\nWithout Inner\nProduct Protocol",selfCheck2d}
}, Alignment→{{Left,Left,Left}},Frame→All]];
If[!selfCheck2d, Error["Assertion failure on self-check 2d (P_d^+ ≟ hμ_d + <g⃗,l⃗> + <d⃗*,r⃗>)"]];

(*3) t̂ ≟_q <l⃗,r⃗>*)
selfCheck3 = (t̂ == modq[l⃗.r⃗]);
Print[Grid[{
    {Style["Name",Bold],Style["Semantics",Bold],Style["Value",Bold]},
    {"t̂ ≟_q <l⃗,r⃗>","V's Check\nWithout Inner\nProduct Protocol",selfCheck3}
}, Alignment→{{Left,Left,Left}},Frame→All]];
If[!selfCheck3, Error["Assertion failure on self-check 3 (t̂ ≟_q <l⃗,r⃗>)"]];

(*1W) t̂_W g + τ_x,W h ≟ ((wy)^n-1+nz)V + y^n-1 W + δ_yzw g + x T_1,W + x^2 T_2,W*)
selfCheck1W = (g*t̂_W + h*τ_x,W == V*(powermodq[w*y,n-1]+n*z) + W*powermodq[y,n-1] + g*δ_yzw + T_1,W
Print[Grid[{
    {Style["Name",Bold],Style["Semantics",Bold],Style["Value",Bold]},
    {"gt̂_W + hτ_x,W","",g*t̂_W + h*τ_x,W},
    {"≟ (wy)^n-1+nz)V + y^n-1 W + δ_yzw g + x T_1,W + x^2 T_2,W","V's Check",selfCheck1W}
}, Alignment→{{Left,Left,Left}},Frame→All]]
If[!selfCheck1W, Error["Assertion failure on self-check 1W (gt̂_W + hτ_x,W ≟ ...)"]];

(*2W) P_W^+ ≟ hμ_W + <g⃗,l⃗_W> + <h⃗*,r⃗_W>*)
```

```
selfCheck2W = (P_W^+ == h*μ_W + g⃗.l⃗_W + h⃗*.r⃗_W);
Print[Grid[{
    {Style["Name",Bold],Style["Semantics",Bold],Style["Value",Bold]},
    {"P_W^+ ≟ A_W + S_W x + <g⃗,zy^-n⃗ + w^n⃗ - w_0^n-1⃗> + <h⃗*,-y_z^n-1⃗>","Definition of P_W^+",P_W^+ == A_W + S_W*x + g⃗.(z*y
    {"≟ hμ_W + <g⃗,l⃗_W> + <h⃗*,r⃗_W>","V's Check\nWithout Inner\nProduct Protocol",selfCheck2W}
}, Alignment→{{Left,Left,Left}},Frame→All]];
If[!selfCheck2W, Error["Assertion failure on self-check 2W (P_W^+ ≟ hμ_W + <g⃗,l⃗_W> + <h⃗*,r⃗_W>)"]];

(*3W) t̂_W ≟_q <l⃗_W,r⃗_W>*)
selfCheck3W = (t̂_W == modq[l⃗_W.r⃗_W]);
Print[Grid[{
    {Style["Name",Bold],Style["Semantics",Bold],Style["Value",Bold]},
    {"t̂_W ≟_q <l⃗_W,r⃗_W>","V's Check\nWithout Inner\nProduct Protocol",selfCheck3W}
}, Alignment→{{Left,Left,Left}},Frame→All]];
If[!selfCheck3W, Error["Assertion failure on self-check 3W (t̂_W ≟_q <l⃗_W,r⃗_W>)"]];

If[useInnerProductProtocol,
    StateMachineSave["mk_shuffle_argument_selfcheck"];
(*Else*),
    ProofFinished[];
    Print["Continuing to inner product protocol not required, but possible."];
    StateMachineSave["mk_shuffle_argument_selfcheck"];

    If[fiatShamirSingleKernel,
    Print["Can't answer requests without multi-kernel or multi-machine setup"];
    (*Else*),
    WaitForVariables[{
        "_verification_result_",
        "_inspection_request_",
        "_inspection_result_"
    }];
    ];

    StateMachineSave["mk_shuffle_argument_selfcheck"];
    FrontEndTokenExecute["EvaluatorAbort"];
]
```

Name	Semantics	Value
$g\hat{t} + h\tau_x$		ecPnt[84 221 947 031 621 106 753 128 767 877 505 500 063 - 296 672 991 606 492 996 073 553 947 585 878 630 - 245, 52 570 167 137 227 745 050 217 253 766 965 056 131 - 545 854 005 981 366 395 868 066 499 760 183 049 - 215]
$\stackrel{?}{=} z^3\overline{k}xV + y^{n-1}\hat{k}xW + \delta_{yz}xg + x^3T_3 + x^5T_5$	V's Check	True

Name	Semantics	Value
$P_h^+ \stackrel{?}{=} A_L + A_{R,h} x + S_L x^2 + S_{R,h} x^3 + \langle \vec{g}, z^3 \overrightarrow{y^{-n}} \rangle + \langle \overrightarrow{h^*}, -x \overrightarrow{y_z^{n-1}} \rangle$	Definition of P_h^+	True
$\stackrel{?}{=} h\mu_h + \langle \vec{g}, \vec{l} \rangle + \langle \overrightarrow{h^*}, \vec{r} \rangle$	V's Check Without Inner Product Protocol	True

Name	Semantics	Value
$P_b^+ \stackrel{?}{=} A_L + A_{R,b} x + S_L x^2 + S_{R,b} x^3 + \langle \vec{g}, z^3 \overrightarrow{y^{-n}} \rangle + \langle \overrightarrow{b^*}, -x \overrightarrow{y_z^{n-1}} \rangle$	Definition of P_b^+	True
$\stackrel{?}{=} h\mu_b + \langle \vec{g}, \vec{l} \rangle + \langle \overrightarrow{b^*}, \vec{r} \rangle$	V's Check Without Inner Product Protocol	True

Name	Semantics	Value
$P_c^+ \stackrel{?}{=} A_L + A_{R,c} x + S_L x^2 + S_{R,c} x^3 + \langle \vec{g}, z^3 \overrightarrow{y^{-n}} \rangle + \langle \overrightarrow{c^*}, -x \overrightarrow{y_z^{n-1}} \rangle$	Definition of P_c^+	True
$\stackrel{?}{=} h\mu_c + \langle \vec{g}, \vec{l} \rangle + \langle \overrightarrow{c^*}, \vec{r} \rangle$	V's Check Without Inner Product Protocol	True

Name	Semantics	Value
$P_d^+ \stackrel{?}{=} A_L + A_{R,d} x + S_L x^2 + S_{R,d} x^3 + \langle \vec{g}, z^3 \overrightarrow{y^{-n}} \rangle + \langle \overrightarrow{d^*}, -x \overrightarrow{y_z^{n-1}} \rangle$	Definition of P_d^+	True
$\stackrel{?}{=} h\mu_d + \langle \vec{g}, \vec{l} \rangle + \langle \overrightarrow{d^*}, \vec{r} \rangle$	V's Check Without Inner Product Protocol	True

Name	Semantics	Value
$\hat{t} \stackrel{?}{=}_q \langle \vec{l}, \vec{r} \rangle$	V's Check Without Inner Product Protocol	True

Name	Semantics	Value
$g\hat{t_W} + h\tau_{x,W}$		ecPnt[71 170 761 461 806 575 056 988 777 799 149 753 - 588 821 351 113 719 544 888 720 840 260 093 - 735 125 151, 106 798 938 098 835 152 551 452 979 329 939 - 804 728 745 954 689 213 102 953 909 532 759 - 353 150 174 279]
$\stackrel{?}{=} (wy)^{n-1} + nz) V + y^{n-1} W + \delta_{yzw} g + x T_{1,W} + x^2 T_{2,W}$	V's Check	True

Name	Semantics	Value
$P_W^+ \stackrel{?}{=} A_W + S_W x + \langle \vec{g}, z \overrightarrow{y^{-n}} + \overrightarrow{w^n} - \overrightarrow{w_0^{n-1}} \rangle + \langle \overrightarrow{h^*}, -\overrightarrow{y_z^{n-1}} \rangle$	Definition of P_W^+	True
$\stackrel{?}{=} h\mu_W + \langle \vec{g}, \overrightarrow{l_W} \rangle + \langle \overrightarrow{h^*}, \overrightarrow{r_W} \rangle$	V's Check Without Inner Product Protocol	True

Name	Semantics	Value
$\hat{t_W} \stackrel{?}{=}_q \langle \overrightarrow{l_W}, \overrightarrow{r_W} \rangle$	V's Check Without Inner Product Protocol	True

Message Processing: Event Loop

Recommended to run when not using the inner product protocol and Fiat-Shamir transform is activated: Answer inspection requests and receive verification and inspection results after proof has been finished

Abort after all expected messages have been received

```
StateMachineRestore["mk_shuffle_argument_selfcheck"];
ProcessIncomingMessages[router, {""}];
```

Inner Product Protocol

Set up vectors and variables for successive halving

Pad $\vec{g}, \vec{h^*}, \vec{b^*}, \vec{c^*}, \vec{d^*}, \vec{l}, \vec{r}, \vec{l_W}$ and $\vec{r_W}$ such that their lengths become a power of two, resulting in the vectors $\vec{G}, \vec{H}, \vec{B}, \vec{C}, \vec{D}, \vec{a}, \vec{b}, \vec{a_W}$ and $\vec{b_W}$. Pad vectors of scalars with zeros and vectors of elliptic curve points with points at infinity. *$\vec{b}$ has a name colission with the randomizers of the ElGamal ciphertexts. Thus, $\vec{a}$ and $\vec{b}$ are indexed with "IP" in the code.*

Define $P^*_{\{h,b,c,d\}} := <\vec{a}, \vec{G}> + <\vec{b}, \overrightarrow{\{H, B, C, D\}}>, c := \equiv_q <\vec{a}, \vec{b}>$ and $P'_{\{h,b,c,d\}} := P^*_{\{h,b,c,d\}} + c * g'$.

Equivalently for PR: $P^*_W := <\vec{a_W}, \vec{G}> + <\vec{b_W}, \vec{H}>, c_W := \equiv_q <\vec{a_W}, \vec{b_W}>$ and $P'_W := P^*_W + c_W * g'$. Iteratively adding up those and all "halved" versions of $P'_{\{h,b,c,W\}}$ (which are yet to be calculated) is the central part of the inner product protocol which ensures the correctness of the inner product after verification.

The verifier calculates

$P'_{\{h,b,c,d\}} :=$

$$A_L + A_{R,\{h,b,c,d\}}\, x + S_L\, x^2 + S_{R,\{h,b,c,d\}}\, x^3 + <\vec{g}, z^3\, \overrightarrow{y^{-n}}> + <\overrightarrow{\{h, b, c, d\}^*}, -x\, \overrightarrow{y_z^{n-1}}> - \mu_{\{h,b,c,d\}}\, h + \hat{t}\, g'$$

and

$P'_W := A_W + S_W\, x + <\vec{g}, z\, \overrightarrow{y^{-n}} + \overrightarrow{w^n} - \overrightarrow{w_0^{n-1}}\, y^{-1}> + <\vec{h^*}, -\overrightarrow{y_z^{n-1}}> - \mu_W\, h + \hat{t_W}\, g'$ which are equal to the $P'_{\{h,b,c,d,W\}}$ of the prover which are calculated based on the knowledge of $\vec{a}$ and $\vec{b}$ resp. $\vec{a_W}$ and $\vec{b_W}$ (P'_W).

In[333]:=

```
StateMachineRestore["mk_shuffle_argument"];

n_pow2 = 2^Ceiling[Log2[n]];
(*pad vectors*)
G⃗ = Join[g⃗[[1;;Min[{n_pow2,n}]]],ConstantArray[ecPnt[∞,∞],Max[0,n_pow2-n]]];
H⃗ = Join[h*⃗[[1;;Min[{n_pow2,n}]]],ConstantArray[ecPnt[∞,∞],Max[0,n_pow2-n]]];
B⃗ = Join[b*⃗[[1;;Min[{n_pow2,n}]]],ConstantArray[ecPnt[∞,∞],Max[0,n_pow2-n]]];
C⃗ = Join[c*⃗[[1;;Min[{n_pow2,n}]]],ConstantArray[ecPnt[∞,∞],Max[0,n_pow2-n]]];
D⃗ = Join[d*⃗[[1;;Min[{n_pow2,n}]]],ConstantArray[ecPnt[∞,∞],Max[0,n_pow2-n]]];
```

```
a⃗IP = Join[l⃗[[1;;Min[{npow2,n}]]],ConstantArray[0,Max[0,npow2-n]]];
b⃗IP = Join[r⃗[[1;;Min[{npow2,n}]]],ConstantArray[0,Max[0,npow2-n]]];
c = modq[a⃗IP.b⃗IP];

a⃗W = Join[l⃗W[[1;;Min[{npow2,n}]]],ConstantArray[0,Max[0,npow2-n]]];
b⃗W = Join[r⃗W[[1;;Min[{npow2,n}]]],ConstantArray[0,Max[0,npow2-n]]];
cW = modq[a⃗W.b⃗W];

(*P* is called P in the Bulletproof paper (not to be confused with the equally named variable
Ph* = a⃗IP.G⃗ + b⃗IP.H⃗;
Pb* = a⃗IP.G⃗ + b⃗IP.B⃗;
Pc* = a⃗IP.G⃗ + b⃗IP.C⃗;
Pd* = a⃗IP.G⃗ + b⃗IP.D⃗;
PW* = a⃗W.G⃗ + b⃗W.H⃗;

Ph' = Ph* + c*g';
Pb' = Pb* + c*g';
Pc' = Pc* + c*g';
Pd' = Pd* + c*g';
PW' = PW* + cW*g';

(*Keep track of different versions of G⃗, H⃗, B⃗, C⃗, D⃗, a⃗, b⃗ and P{h,b,c,d,W} throughout halving st
The 2 in the base indicates that those lists contain variables or vectors from the halving ste
G⃗2 = {G⃗};
H⃗2 = {H⃗};
B⃗2 = {B⃗};
C⃗2 = {C⃗};
D⃗2 = {D⃗};
a⃗2 = {a⃗IP};
b⃗2 = {b⃗IP};
a⃗2,W = {a⃗W};
b⃗2,W = {b⃗W};
P2,h = {Ph'};
P2,b = {Pb'};
P2,c = {Pc'};
P2,d = {Pd'};
P2,W = {PW'};

Print[Grid[{
    {Style["Name",Bold],Style["Semantics",Bold],Style["Knowledge",Bold],Style["Value",Bold]},
    {"npow2 := 2^⌈log2 n⌉","Smallest power of 2\ngreater than\nor equal to n","P,V",npow2},
    {"G⃗ := padded g⃗","","P,V",G⃗},
    {"H⃗ := padded h⃗*","","P,V",H⃗},
    {"B⃗ := padded b⃗*","","P,V",B⃗},
    {"C⃗ := padded c⃗*","","P,V",C⃗},
```

```
    {"D⃗ := padded d⃗*","","P,V",D⃗},
    {"a⃗_IP := padded l⃗","","P",a⃗_IP},
    {"b⃗_IP := padded r⃗","","P",b⃗_IP},
    {"c :≡_q <a⃗_IP,b⃗_IP> ≟_q <l⃗,r⃗> ≡_q: t̂","Inner Product","P,V",t̂==c},
    {"a⃗_W := padded l⃗_W","","P",a⃗_W},
    {"b⃗_W := padded r⃗_W","","P",b⃗_W},
    {"c_W :≡_q <a⃗_W,b⃗_W> ≟_q <l⃗_W,r⃗_W> ≡_q: t̂_W","Inner Product","P,V",t̂_W==c_W},
    {"(1) P*_{h,b,c,d} :=\n(2) <a⃗,G⃗> + <b⃗,{H,B,C,D}⃗> ≟\n(3) <g⃗,l⃗> + <{h,b,c,d}⃗*,r⃗> =\n(4) P+_{h,b,c
    {"(1) P*_W :=\n(2) <a⃗_W,G⃗> + <b⃗_W,H⃗> ≟\n(3) <g⃗,l⃗_W> + <h⃗*,r⃗_W> =\n(4) P+_W - hμ_W","","1,4: P,V (i
    {"P'_{h,b,c,d} := P*_{h,b,c,d} + cg'","Combination of\nShuffle Proof\nConditions\nBased on h⃗, b⃗, c
    {"P'_{h,b,c,d} ≟ P+_{h,b,c,d} - μ_{h,b,c,d}h + t̂g'","The way V\nis calculating P'_{h,b,c,d}","P,V",{P'_h==P+_h-
    {"P'_W := P*_W + c_Wg'","Combination of\nPR Proof\nConditions","P,V (implicit)",P'_W},
    {"P'_W ≟ P+_W - μ_Wh + t̂_Wg'","The way V\nis calculating P'_W","P,V",P'_W==P+_W-μ_W*h+t̂_W*g'}
}, Alignment→{{Left,Left,Left,Left}},Frame→All]]

If[!interactive,Print[FiatShamirGrid[]]];
Print[CommunicationCostGrid[]]
ProcessNewMessages[];
StateMachineSave["inner_product_setup"];
```

Name	Semantics	Knowledge	Value
$n_{pow2} := 2^{\lceil \log_2 n \rceil}$	Smallest power of 2 greater than or equal to n	P,V	4

$\vec{G}$:= padded $\vec{g}$		P,V	{ecPnt[101 548 470 124 358 210 - 188 072 679 181 678 - 188 450 387 789 916 - 654 718 462 374 321 - 277 161 805 765 354, 70 108 350 633 035 199 - 759 065 376 354 370 - 719 210 357 510 544 - 392 766 796 027 711 - 414 587 086 150 112], ecPnt[81 881 281 191 882 355 - 160 881 140 819 926 - 411 859 223 579 216 - 161 786 219 247 020 - 789 084 841 886 435, 40 551 526 063 420 644 - 421 580 965 386 725 - 729 859 544 147 053 - 123 598 525 382 531 - 556 934 666 119 757], ecPnt[27 427 957 168 767 222 - 510 921 650 620 077 - 570 798 709 753 797 - 557 336 240 233 137 - 618 475 833 226 690, 42 650 441 509 520 284 - 448 005 737 515 710 - 331 630 163 209 846 - 762 957 134 645 512 - 392 724 356 208 176], ecPnt[∞, ∞]}

$\vec{H}$:= padded $\overrightarrow{h^*}$		P,V	{ecPnt[78 567 409 798 129 814 - 866 150 056 060 307 - 810 399 673 849 671 - 094 211 427 553 792 - 618 009 791 659 223, 50 464 327 830 870 926 - 983 164 620 566 499 - 054 037 449 550 745 - 776 160 850 919 973 - 618 220 747 519 859], ecPnt[16 230 325 873 944 567 - 770 651 181 130 303 - 324 912 121 224 490 - 802 407 282 022 789 - 649 993 284 143 768, 13 743 595 330 208 364 - 632 961 058 787 086 - 372 972 527 668 621 - 267 658 729 713 274 - 917 516 765 878 025], ecPnt[73 955 863 155 933 535 - 982 859 074 509 836 - 995 565 814 682 227 - 118 115 222 970 062 - 094 871 722 157 004, 12 661 142 626 516 128 - 143 965 107 877 524 - 977 948 748 772 063 - 737 046 982 621 034 - 957 911 954 836 350], ecPnt[∞, ∞]}

$\vec{B}$:= padded $\overrightarrow{b^*}$		P,V	{ecPnt[59 043 719 839 056 093 - 060 455 647 773 031 - 110 426 513 415 445 - 959 592 906 283 022 - 536 109 982 690 406, 15 581 121 562 794 375 - 473 593 189 690 062 - 526 490 521 359 132 - 176 103 829 752 471 - 918 632 370 295 336], ecPnt[112 521 091 029 611 710 - 525 094 888 851 919 - 040 284 401 236 803 - 289 858 290 779 025 - 976 942 166 966 892, 71 802 849 234 922 876 - 881 679 460 540 584 - 158 214 170 652 826 - 348 764 564 492 847 - 489 002 175 595 813], ecPnt[35 174 235 482 391 906 - 576 550 590 433 357 - 833 240 355 046 807 - 245 255 381 964 494 - 894 476 083 182 660, 55 925 870 782 800 122 - 155 770 079 253 820 - 122 879 523 420 329 - 479 534 761 202 990 - 107 031 888 939 945], ecPnt[∞, ∞]}

$\vec{C}$:= padded $\overrightarrow{c^*}$		P,V	{ecPnt[82 677 993 194 665 902 - 474 541 122 728 628 - 239 106 974 633 730 - 721 916 315 448 799 - 654 380 724 509 062, 82 899 414 855 368 741 - 404 724 030 068 539 - 514 612 899 114 324 - 925 700 999 638 050 - 403 382 505 421 116], ecPnt[45 422 098 385 527 520 - 105 729 242 155 385 - 912 239 396 352 275 - 187 691 869 915 510 - 620 991 934 660 246, 42 981 417 682 506 542 - 040 834 084 511 832 - 054 752 082 115 267 - 275 737 379 170 623 - 738 544 398 871 700], ecPnt[79 731 591 686 381 398 - 751 792 815 416 125 - 448 258 844 377 845 - 199 135 938 472 730 - 072 263 316 128 928, 14 986 293 206 980 309 - 680 514 267 840 081 - 157 662 963 426 467 - 477 088 209 824 552 - 014 914 871 589 040], ecPnt[∞, ∞]}

$\vec{D}$:= padded $\overrightarrow{d^*}$		P,V	{ecPnt[97 038 873 997 667 556 - 164 890 627 159 143 - 816 584 036 737 601 - 412 047 181 786 115 - 325 137 586 601 893, 28 632 182 194 222 295 - 567 409 644 033 114 - 434 203 763 962 660 - 717 808 858 714 880 - 991 421 895 676 479], ecPnt[114 943 785 603 625 565 - 834 113 287 895 479 - 632 817 105 457 530 - 959 156 178 552 924 - 525 977 788 156 149, 75 005 268 061 152 234 - 748 488 293 094 956 - 398 629 562 793 675 - 286 378 681 571 354 - 303 324 894 122 899], ecPnt[34 283 013 894 072 667 - 721 275 831 653 793 - 797 981 117 913 068 - 563 331 324 282 032 - 073 934 983 384 369, 16 444 072 431 226 081 - 049 726 942 532 624 - 576 021 955 849 773 - 018 079 843 576 838 - 182 070 874 161 038], ecPnt[∞, ∞]}
$\overrightarrow{a_{IP}}$:= padded $\vec{1}$		P	{61 442 343 775 113 140 - 880 034 650 887 022 378 - 965 571 424 979 173 001 - 973 397 458 542 222 999 - 566 892, 112 164 513 297 470 756 - 571 473 984 141 438 273 - 936 195 334 402 062 428 - 015 459 026 081 712 107 - 932 702, 100 474 102 720 414 684 - 705 898 037 977 251 389 - 482 922 603 087 723 310 - 707 681 533 634 105 023 - 940 360, 0}

$\overrightarrow{b_{IP}}$:= padded $\vec{r}$		P	{62 425 708 243 501 832 - 904 842 395 569 180 717 - 767 201 166 970 569 719 - 744 186 579 509 066 013 - 239 789, 108 894 093 373 790 087 - 805 981 249 637 450 006 - 012 557 717 717 172 910 - 157 161 661 185 273 450 - 166 896, 80 085 874 135 138 745 - 719 381 189 911 405 897 - 849 137 938 574 627 947 - 766 879 149 979 384 405 - 495 240, 0}
c :≡$_q$ <$\overrightarrow{a_{IP}}$,$\overrightarrow{b_{IP}}$> $\overset{?}{\equiv}_q$ <$\vec{l}$,$\vec{r}$> ≡$_q$: $\hat{t}$	Inner Product	P,V	True
$\overrightarrow{a_W}$:= padded $\overrightarrow{l_W}$		P	{48 564 477 212 184 250 - 415 170 747 693 694 481 - 439 232 973 935 076 016 - 590 509 497 532 087 603 - 698 870, 8 819 342 647 412 475 122 - 593 262 319 876 611 403 - 831 739 595 798 027 640 - 620 830 864 043 632 355 - 299, 115 268 474 747 795 881 - 775 546 216 783 739 194 - 713 511 413 966 655 407 - 981 146 926 754 407 903 - 409 076, 0}
$\overrightarrow{b_W}$:= padded $\overrightarrow{r_W}$		P	{73 357 405 155 266 425 - 915 543 821 545 319 812 - 280 870 144 848 159 677 - 532 949 644 361 748 894 - 556 594, 26 473 080 131 638 368 - 664 311 419 668 052 580 - 406 527 293 561 077 903 - 757 204 398 370 221 010 - 052 161, 8 085 424 818 135 938 036 - 088 244 802 558 875 166 - 648 813 733 660 931 210 - 189 856 208 497 918 675 - 798, 0}
c_W :≡$_q$ <$\overrightarrow{a_W}$,$\overrightarrow{b_W}$> $\overset{?}{\equiv}_q$ <$\overrightarrow{l_W}$,$\overrightarrow{r_W}$> ≡$_q$: $\hat{t}_W$	Inner Product	P,V	True

(1) $P^*_{\{h,b,c,d\}}$:= (2) $\langle \vec{a}, \vec{G} \rangle$ + $\langle \vec{b}, \overrightarrow{\{H, B, C, D\}} \rangle \stackrel{?}{=}$ (3) $\langle \vec{g}, \vec{l} \rangle$ + $\langle \overrightarrow{\{h, b, c, d\}^*}, \vec{r} \rangle$ = (4) $P^+_{\{h,b,c,d\}}$ $- h\mu_{\{h,b,c,d\}}$		1,4: P,V (implicit) 2,3: P	{True, True, True, True}
(1) P^*_W := (2) $\langle \overrightarrow{a_W}, \vec{G} \rangle + \langle \overrightarrow{b_W}, \vec{H} \rangle \stackrel{?}{=}$ (3) $\langle \vec{g}, \overrightarrow{l_W} \rangle + \langle \overrightarrow{h^*}, \overrightarrow{r_W} \rangle$ = (4) $P^+_W - h\mu_W$		1,4: P,V (implicit) 2,3: P	True

$P'_{\{h,b,c,d\}} :=$ $P^{+}_{\{h,b,c,d\}} + cg'$	Combination of Shuffle Proof Conditions Based on $\vec{h}$, $\vec{b}$, $\vec{c}$ resp. $\vec{d}$	P,V (implicit)	{ecPnt[42 427 373 215 793 781 - 659 408 924 843 768 - 227 225 882 770 225 - 375 757 126 397 503 - 527 068 891 674 844, 25 721 469 407 782 422 - 059 186 990 187 869 - 888 211 409 564 752 - 656 079 140 365 100 - 434 148 494 723 328], ecPnt[53 093 155 971 198 350 - 375 134 075 441 510 - 772 569 193 709 629 - 578 094 931 141 813 - 154 602 240 565 106, 55 938 320 630 024 527 - 613 951 665 036 283 - 624 008 160 716 735 - 992 177 830 942 127 - 603 092 847 901 156], ecPnt[87 623 278 363 384 013 - 501 616 299 287 548 - 132 476 250 177 902 - 650 041 648 463 953 - 140 336 403 353 190, 41 060 481 386 143 080 - 378 375 521 196 934 - 627 853 309 131 610 - 093 864 338 133 773 - 149 938 053 272 351], ecPnt[81 848 919 976 003 370 - 114 473 563 771 257 - 237 692 448 808 430 - 626 166 945 431 568 - 046 554 818 008 682, 2 643 826 270 596 107 - 626 712 310 049 127 - 795 608 650 776 351 - 598 726 801 898 843 - 301 631 070 212 794]}
$P'_{\{h,b,c,d\}} \stackrel{?}{=} P^{+}_{\{h,b,c,d\}} - \mu_{\{h,b,c,d\}} h + \hat{t} g'$	The way V is calculating $P'_{\{h,b,c,d\}}$	P,V	{True, True, True, True}

$P'_W := P^*_W + c_W g'$	Combination of PR Proof Conditions	P,V (implicit)	ecPnt[98 991 610 698 448 567 - 601 040 979 656 886 525 - 408 488 940 163 120 548 - 218 252 896 669 433 046 - 079 564, 52 231 224 843 856 607 - 266 205 397 725 579 670 - 752 662 648 688 237 226 - 846 639 049 801 479 304 - 835 028]
$P'_W \stackrel{?}{=} P^+_W - \mu_W h + \hat{t}_W g'$	The way V is calculating P'_W	P,V	True

Total Communication Cost			
Type	**Count**	**Names**	**Bits**
group	14	V, W, AW, SW, AL, SL, SRh, SRb, SRc, SRd, T3, T5, T1W, T2W	3598
scalar	15	r, u, y, z, w, x, taux, muh, mub, muc, mud, t, tauxW, muW, tW	3840
total	29		7438

Halving Iterations

Let $P_{\{h,b,c,d\}} := P'_{\{h,b,c,d\}}$

Continue to:

- Split and halve $\vec{G}$, $\vec{H}$, $\vec{B}$, $\vec{C}$, $\vec{D}$, $\overrightarrow{a_{IP}}$ and $\overrightarrow{b_{IP}}$ based on challenges from V,

- Make commitments $L_{\{h,b,c,d\}}$ and $R_{\{h,b,c,d\}}$ to $\vec{a}$ and $\vec{b}$ and send them to V,

- Calculate halved versions of $P'_{\{h,b,c,d,W\}}$:

Split into lower and higher parts:

$\overrightarrow{G_{lo}} <> \overrightarrow{G_{hi}} := \vec{G}$

$\overrightarrow{H_{lo}} <> \overrightarrow{H_{hi}} := \vec{H}$

$\overrightarrow{B_{lo}} <> \overrightarrow{B_{hi}} := \vec{B}$

$\overrightarrow{C_{lo}} <> \overrightarrow{C_{hi}} := \vec{C}$

$\overrightarrow{D_{lo}} <> \overrightarrow{D_{hi}} := \vec{D}$

$\overrightarrow{a_{lo}} <> \overrightarrow{a_{hi}} := \overrightarrow{a_{IP}}$

$\overrightarrow{b_{lo}} <> \overrightarrow{b_{hi}} := \overrightarrow{b_{IP}}$

$\overrightarrow{a_{lo,W}} <> \overrightarrow{a_{hi,W}} := \overrightarrow{a_W}$

$\overrightarrow{b_{lo,W}} <> \overrightarrow{b_{hi,W}} := \overrightarrow{b_W}$

Make commitments $L_{\{h,b,c,d\}}$ and $R_{\{h,b,c,d\}}$ which are sent to V:

$L_{\{h,b,c,d\}} := <\overrightarrow{a_{lo}}, \overrightarrow{G_{hi}}> + <\overrightarrow{b_{hi}}, \overrightarrow{\{H, B, C, D\}_{lo}}> + <\overrightarrow{a_{lo}}, \overrightarrow{b_{hi}}> g'$

$R_{\{h,b,c,d\}} := <\overrightarrow{a_{hi}}, \overrightarrow{G_{lo}}> + <\overrightarrow{b_{lo}}, \overrightarrow{\{H, B, C, D\}_{hi}}> + <\overrightarrow{a_{hi}}, \overrightarrow{b_{lo}}> g'$

and equivalently for L_W and R_W:

$L_W := <\overrightarrow{a_{lo,W}}, \overrightarrow{G_{hi}}> + <\overrightarrow{b_{hi,W}}, \overrightarrow{H_{lo}}> + <\overrightarrow{a_{lo,W}}, \overrightarrow{b_{hi,W}}> g'$

$R_W := <\overrightarrow{a_{hi,W}}, \overrightarrow{G_{lo}}> + <\overrightarrow{b_{lo,W}}, \overrightarrow{H_{hi}}> + <\overrightarrow{a_{hi,W}}, \overrightarrow{b_{lo,W}}> g'$

Receive challenge u_{IP} (called x in the Bulletproof paper). *To avoid name collission with previous*

challenge u index with "IP".

Calculate halves:

$\overrightarrow{G_{\text{next}}} := u^{-1}\,\overrightarrow{G_{\text{lo}}} + u\,\overrightarrow{G_{\text{hi}}}$

$\overrightarrow{H_{\text{next}}} := u\,\overrightarrow{H_{\text{lo}}} + u^{-1}\,\overrightarrow{H_{\text{hi}}}$

$\overrightarrow{B_{\text{next}}} := u\,\overrightarrow{B_{\text{lo}}} + u^{-1}\,\overrightarrow{B_{\text{hi}}}$

$\overrightarrow{C_{\text{next}}} := u\,\overrightarrow{C_{\text{lo}}} + u^{-1}\,\overrightarrow{C_{\text{hi}}}$

$\overrightarrow{D_{\text{next}}} := u\,\overrightarrow{D_{\text{lo}}} + u^{-1}\,\overrightarrow{D_{\text{hi}}}$

$\overrightarrow{a_{\text{next}}} := u\,\overrightarrow{a_{\text{lo}}} + u^{-1}\,\overrightarrow{a_{\text{hi}}}$

$\overrightarrow{b_{\text{next}}} := u^{-1}\,\overrightarrow{b_{\text{lo}}} + u\,\overrightarrow{b_{\text{hi}}}$

$\overrightarrow{a_{\text{next},W}} := u\,\overrightarrow{a_{\text{lo},W}} + u^{-1}\,\overrightarrow{a_{\text{hi},W}}$

$\overrightarrow{b_{\text{next},W}} := u^{-1}\,\overrightarrow{b_{\text{lo},W}} + u\,\overrightarrow{b_{\text{hi},W}}$

$P_{\text{next},\{h,b,c,d,W\}} := P_{\{h,b,c,d,W\}} + u^2\,L_{\{h,b,c,d,W\}} + u^{-2}\,R_{\{h,b,c,d,W\}}$

The equalities $P_{\text{next},\{h,b,c,d\}} = <\overrightarrow{a_{\text{next}}}, \overrightarrow{G_{\text{next}}}> + <\overrightarrow{b_{\text{next}}}, \overrightarrow{\{H, B, C, D\}_{\text{next}}}> + <\overrightarrow{a_{\text{next}}}, \overrightarrow{b_{\text{next}}}>\,g'$ and $P_{\text{next},W} = <\overrightarrow{a_{\text{next},W}}, \overrightarrow{G_{\text{next}}}> + <\overrightarrow{b_{\text{next},W}}, \overrightarrow{H_{\text{next}}}> + <\overrightarrow{a_{\text{next},W}}, \overrightarrow{b_{\text{next},W}}>\,g'$ will hold. This equalities form the backbone of the Bulletproof inner product protocol.

Set $P_{\{h,b,c,d,W\}} := P_{\text{next},\{h,b,c,d,W\}}$ and go to next iteration until the size of the halved vectors has reached 1.

Last single-valued step:

$G_0 := \overrightarrow{G_{\text{next}}}[1]$

$H_0 := \overrightarrow{H_{\text{next}}}[1]$

$B_0 := \overrightarrow{B_{\text{next}}}[1]$

$C_0 := \overrightarrow{C_{\text{next}}}[1]$

$D_0 := \overrightarrow{D_{\text{next}}}[1]$

$a_0 := \overrightarrow{a_{\text{next}}}[1]$

$b_0 := \overrightarrow{b_{\text{next}}}[1]$

$a_{0,W} := \overrightarrow{a_{\text{next},W}}[1]$

$b_{0,W} := \overrightarrow{b_{\text{next},W}}[1]$

$P_{0,\{h,b,c,d,W\}} := P_{\{h,b,c,d,W\}}$

Send a_0, b_0, $a_{0,W}$ and $b_{0,W}$ to the verifier.

The "anatomy" of $P_{0,\{h,b,c,d,W\}}$ is: $P_{0,\{h,b,c,d,W\}} = P'_{\{h,b,c,d,W\}} + <u_2^2, L_{2,\{h,b,c,d,W\}}> + <u_2^{-2}, R_{2,\{h,b,c,d,W\}}>$. This can be calculated as a sanity check at the end.

The verifier will calculate $c_0 := a_0\,b_0$ and $c_{0,W} := a_{0,W}\,b_{0,W}$ and check if his version of $P_{0,\{h,b,c,d\}}$ resp. $P_{0,W}$ equals $a_0 * G_0 + b_0 * \{H, B, C, D\}_0 + c_0 * g'$ resp. $a_{0,W} * G_0 + b_{0,W} * H_0 + c_{0,W} * g'$. These final verification steps mark the end of the inner product protocol.

Note on implementation: Indices of vectors count up from 1 to $\log_2 n_{\text{pow2}} + 1$ (`currentIteration`) and numbers for names of elements of vectors count down from $\log_2 n_{\text{pow2}}$ to 0 (`k, ciStr`), i.e. for $n_{\text{pow2}} = 16$: w[1]=w.4, w[2]=w.3, ... w[5]=w.0

In[375]:=

```
StateMachineRestore["inner_product_setup"];
```

```
n2 = {npow2};
k2 = {Log2[npow2]};

(*Re-initialize G, H, B, C, D, a, b and P in case of multiple cell evaluations*)
G2→ = {G2→[[1]]};
H2→ = {H2→[[1]]};
B2→ = {B2→[[1]]};
C2→ = {C2→[[1]]};
D2→ = {D2→[[1]]};
a2→ = {a2→[[1]]};
b2→ = {b2→[[1]]};
a2,W→ = {a2,W→[[1]]};
b2,W→ = {b2,W→[[1]]};
P2,h = {P2,h[[1]]};
P2,b = {P2,b[[1]]};
P2,c = {P2,c[[1]]};
P2,d = {P2,d[[1]]};
P2,W = {P2,W[[1]]};

L2,h = {};
L2,b = {};
L2,c = {};
L2,d = {};
L2,W = {};
R2,h = {};
R2,b = {};
R2,c = {};
R2,d = {};
R2,W = {};
u2 = {};

currentIteration = 1;

While[n2[[currentIteration]] ≠ 1,
    ciStr = IntegerString[k2[[currentIteration]]];
    Print[Grid[{
        {Style["Iteration "<>ciStr<>" (Counting from "<>IntegerString[k2[[1]]]<>" to 0)"], Spa
        {Style["Name",Bold],Style["Semantics",Bold],Style["Knowledge",Bold],Style["Value",Bol
         {"k := k2."<>ciStr,"Current Iteration\n(counting down)","P,V",k2[[currentIteration]]},
        {"n2."<>ciStr<>" = 2^k","Current Length\nof Vectors","P,V",n2[[currentIteration]]},
        {"G→ := G2→."<>ciStr,"","P,V (implicit)",G2→[[currentIteration]]},
        {"H→ := H2→."<>ciStr,"","P,V (implicit)",H2→[[currentIteration]]},
        {"B→ := B2→."<>ciStr,"","P,V (implicit)",B2→[[currentIteration]]},
        {"C→ := C2→."<>ciStr,"","P,V (implicit)",C2→[[currentIteration]]},
        {"D→ := D2→."<>ciStr,"","P,V (implicit)",D2→[[currentIteration]]},
```

```
    {"a⃗ := a⃗2."<>ciStr,"","P",a⃗2[[currentIteration]]},
    {"b⃗ := b⃗2."<>ciStr,"","P",b⃗2[[currentIteration]]},
    {"a⃗W := a⃗2,W."<>ciStr,"","P",a⃗2,W[[currentIteration]]},
    {"b⃗W := b⃗2,W."<>ciStr,"","P",b⃗2,W[[currentIteration]]},
    {"P{h,b,c,d,W} := P2,{h,b,c,d,W}."<>ciStr,"","P,V (implicit)",{P2,h[[currentIteration]], P2,b[[c
  }, Alignment→{{Left,Left,Left,Left}},Frame→All]];
currentN = n2[[currentIteration]];
halfN = currentN/2;
k = k2[[currentIteration]];
G⃗ = G⃗2[[currentIteration]];
H⃗ = H⃗2[[currentIteration]];
B⃗ = B⃗2[[currentIteration]];
C⃗ = C⃗2[[currentIteration]];
D⃗ = D⃗2[[currentIteration]];
a⃗IP = a⃗2[[currentIteration]];
b⃗IP = b⃗2[[currentIteration]];
a⃗W = a⃗2,W[[currentIteration]];
b⃗W = b⃗2,W[[currentIteration]];
Ph = P2,h[[currentIteration]];
Pb = P2,b[[currentIteration]];
Pc = P2,c[[currentIteration]];
Pd = P2,d[[currentIteration]];
PW = P2,W[[currentIteration]];
(*Split into lower and higher parts*)
G⃗lo = G⃗[[1;;halfN]];
G⃗hi = G⃗[[halfN+1;;-1]];
H⃗lo = H⃗[[1;;halfN]];
H⃗hi = H⃗[[halfN+1;;-1]];
B⃗lo = B⃗[[1;;halfN]];
B⃗hi = B⃗[[halfN+1;;-1]];
C⃗lo = C⃗[[1;;halfN]];
C⃗hi = C⃗[[halfN+1;;-1]];
D⃗lo = D⃗[[1;;halfN]];
D⃗hi = D⃗[[halfN+1;;-1]];
a⃗lo = a⃗IP[[1;;halfN]];
a⃗hi = a⃗IP[[halfN+1;;-1]];
b⃗lo = b⃗IP[[1;;halfN]];
b⃗hi = b⃗IP[[halfN+1;;-1]];
a⃗lo,W = a⃗W[[1;;halfN]];
a⃗hi,W = a⃗W[[halfN+1;;-1]];
b⃗lo,W = b⃗W[[1;;halfN]];
b⃗hi,W = b⃗W[[halfN+1;;-1]];
(*Digest into L{h,b,c,d} and R{h,b,c,d}*)
Lh = a⃗lo.G⃗hi + b⃗hi.H⃗lo + a⃗lo.b⃗hi*g';
Rh = a⃗hi.G⃗lo + b⃗lo.H⃗hi + a⃗hi.b⃗lo*g';
AppendTo[L2,h,Lh];
AppendTo[R2,h,Rh];
```

```
L_b = a_lo.G_hi + b_hi.B_lo + a_lo.b_hi*g';
R_b = a_hi.G_lo + b_lo.B_hi + a_hi.b_lo*g';
AppendTo[L_{2,b},L_b];
AppendTo[R_{2,b},R_b];
L_c = a_lo.G_hi + b_hi.C_lo + a_lo.b_hi*g';
R_c = a_hi.G_lo + b_lo.C_hi + a_hi.b_lo*g';
AppendTo[L_{2,c},L_c];
AppendTo[R_{2,c},R_c];
L_d = a_lo.G_hi + b_hi.D_lo + a_lo.b_hi*g';
R_d = a_hi.G_lo + b_lo.D_hi + a_hi.b_lo*g';
AppendTo[L_{2,d},L_d];
AppendTo[R_{2,d},R_d];
L_W = a_{lo,W}.G_hi + b_{hi,W}.H_lo + a_{lo,W}.b_{hi,W}*g';
R_W = a_{hi,W}.G_lo + b_{lo,W}.H_hi + a_{hi,W}.b_{lo,W}*g';
AppendTo[L_{2,W},L_W];
AppendTo[R_{2,W},R_W];
TellVerifier[{
    "Lh."<>ciStr→L_h,
    "Rh."<>ciStr→R_h,
    "Lb."<>ciStr→L_b,
    "Rb."<>ciStr→R_b,
    "Lc."<>ciStr→L_c,
    "Rc."<>ciStr→R_c,
    "Ld."<>ciStr→L_d,
    "Rd."<>ciStr→R_d,
    "LW."<>ciStr→L_W,
    "RW."<>ciStr→R_W,
    "_cost"→"group"
}];
If[!interactive,
    FiatShamirAdd["Lh."<>ciStr,compressPoint[L_h],entropyParameters["group"]];
    FiatShamirAdd["Rh."<>ciStr,compressPoint[R_h],entropyParameters["group"]];
    FiatShamirAdd["Lb."<>ciStr,compressPoint[L_b],entropyParameters["group"]];
    FiatShamirAdd["Rb."<>ciStr,compressPoint[R_b],entropyParameters["group"]];
    FiatShamirAdd["Lc."<>ciStr,compressPoint[L_c],entropyParameters["group"]];
    FiatShamirAdd["Rc."<>ciStr,compressPoint[R_c],entropyParameters["group"]];
    FiatShamirAdd["Ld."<>ciStr,compressPoint[L_d],entropyParameters["group"]];
    FiatShamirAdd["Rd."<>ciStr,compressPoint[R_d],entropyParameters["group"]];
    FiatShamirAdd["LW."<>ciStr,compressPoint[L_W],entropyParameters["group"]];
    FiatShamirAdd["RW."<>ciStr,compressPoint[R_W],entropyParameters["group"]];
];
Print[Grid[{
    {Style["Name",Bold],Style["Knowledge",Bold],Style["Value",Bold]},
    {"(1) L_{h,b,c,d} := L_{2,{h,b,c,d}}."<>ciStr<>" :=\n(2) <a_lo,G_hi> + <b_hi,{H,B,C,D}_lo> + <a_lo,b
    {"(1) R_{h,b,c,d} := R_{2,{h,b,c,d}}."<>ciStr<>" :=\n(2) <a_hi,G_lo> + <b_lo,{H,B,C,D}_hi> + <a_hi,b
    {"(1) L_W := L_{2,W}."<>ciStr<>" :=\n(2) <a_{lo,W},G_hi> + <b_{hi,W},H_lo> + <a_{lo,W},b_{hi,W}>g'","1: P,V\
    {"(1) R_W := R_{2,W}."<>ciStr<>" :=\n(2) <a_{hi,W},G_lo> + <b_{lo,W},H_hi> + <a_{hi,W},b_{lo,W}>g'","1: P,V\r
}, Alignment→{{Left,Left,Left}},Frame→All]];
(*Challenge u_IP*)
If[interactive,
```

```
(*Random challenge from interactive verifier*)
    u_IP = WaitForRandomChallenge["u."<>ciStr];
(*Else*),
(*Fiat-Shamir*)
    u_IP = FiatShamirGet["u."<>ciStr,q,entropyParameters["scalar"]];
    TellVerifier[{"u."<>ciStr→u_IP,"_cost"→"scalar"}];
];
AppendTo[u_2,u_IP];
u^-1 = modinvq[u_IP];
G_next→ = u^-1*G_lo→+u_IP*G_hi→;
AppendTo[G_2→,G_next→];
H_next→ = u_IP*H_lo→+u^-1*H_hi→;
AppendTo[H_2→,H_next→];
B_next→ = u_IP*B_lo→+u^-1*B_hi→;
AppendTo[B_2→,B_next→];
C_next→ = u_IP*C_lo→+u^-1*C_hi→;
AppendTo[C_2→,C_next→];
D_next→ = u_IP*D_lo→+u^-1*D_hi→;
AppendTo[D_2→,D_next→];
P_next,h = P_h + u_IP^2*L_h + u^-1^2*R_h;
AppendTo[P_2,h,P_next,h];
P_next,b = P_b + u_IP^2*L_b + u^-1^2*R_b;
AppendTo[P_2,b,P_next,b];
P_next,c = P_c + u_IP^2*L_c + u^-1^2*R_c;
AppendTo[P_2,c,P_next,c];
P_next,d = P_d + u_IP^2*L_d + u^-1^2*R_d;
AppendTo[P_2,d,P_next,d];
P_next,W = P_W + u_IP^2*L_W + u^-1^2*R_W;
AppendTo[P_2,W,P_next,W];
a_next→ = modq[u_IP*a_lo→ + u^-1*a_hi→];
AppendTo[a_2→,a_next→];
b_next→ = modq[u^-1*b_lo→ + u_IP*b_hi→];
AppendTo[b_2→,b_next→];
a_next,W→ = modq[u_IP*a_lo,W→ + u^-1*a_hi,W→];
AppendTo[a_2,W→,a_next,W→];
b_next,W→ = modq[u^-1*b_lo,W→ + u_IP*b_hi,W→];
AppendTo[b_2,W→,b_next,W→];
Print[Grid[{
    {Style["Fold G→, H→, B→, C→, P→, a→ and b→ based on challenge u_IP"], SpanFromLeft, SpanFromL
    {Style["Name",Bold],Style["Knowledge",Bold],Style["Value",Bold]},
    {"u_IP = u_2."<>ciStr,"P,V",u_IP},
    {"G_next→ := u_IP^-1G_lo→ + u_IPG_hi→","P,V",G_next→},
    {"H_next→ := u_IPH_lo→ + u_IP^-1H_hi→","P,V",H_next→},
    {"B_next→ := u_IPB_lo→ + u_IP^-1B_hi→","P,V",B_next→},
    {"C_next→ := u_IPC_lo→ + u_IP^-1C_hi→","P,V",C_next→},
```

```
        {"D_next := u_IP D_lo + u_IP^-1 D_hi","P,V",D_next},
        {"P_next,{h,b,c,d,W} := P_{h,b,c,d,W} + u_IP^2 L_{h,b,c,d,W} + u_IP^-2 R_{h,b,c,d,W}","P,V",{P_next,h,P_next,b,P_next,c,P
        {"a_next = u_IP a_lo + u_IP^-1 a_hi","P",a_next},
        {"b_next = u_IP^-1 b_lo + u_IP b_hi","P",b_next},
        {"a_next,W = u_IP a_lo,W + u_IP^-1 a_hi,W","P",a_next,W},
        {"b_next,W = u_IP^-1 b_lo,W + u_IP b_hi,W","P",b_next,W},
        {"P_next,{h,b,c,d} ?= \n<a_next,G_next> + <b_next,{H,B,C,D}_next> + <a_next,b_next>g'","P",{P_next,h == a_nex
        {"P_next,W ?= \n<a_next,W,G_next> + <b_next,W,H_next> + <a_next,W,b_next,W>g'","P",P_next,W == a_next,W.G_next +
    }, Alignment→{{Left,Left,Left}},Frame→All]];
    (*Update variables for next iteration*)
    AppendTo[n_2,halfN];
    k = k - 1;
    AppendTo[k_2,k];
    currentIteration += 1;
]

(*Last, single-valued iteration*)
ciStr = IntegerString[k_2[[currentIteration]]];
n_0 = n_2[[currentIteration]];
k_0 = k_2[[currentIteration]];
G = G_2[[currentIteration]];
H = H_2[[currentIteration]];
B = B_2[[currentIteration]];
C = C_2[[currentIteration]];
D = D_2[[currentIteration]];
a_IP = a_2[[currentIteration]];
b_IP = b_2[[currentIteration]];
a_W = a_2,W[[currentIteration]];
b_W = b_2,W[[currentIteration]];
P_h = P_2,h[[currentIteration]];
P_b = P_2,b[[currentIteration]];
P_c = P_2,c[[currentIteration]];
P_d = P_2,d[[currentIteration]];
P_W = P_2,W[[currentIteration]];
a_0 = a_IP[[1]];
b_0 = b_IP[[1]];
a_0,W = a_W[[1]];
b_0,W = b_W[[1]];
G_0 = G[[1]];
H_0 = H[[1]];
B_0 = B[[1]];
C_0 = C[[1]];
D_0 = D[[1]];
P_0,h = P_h;
P_0,b = P_b;
P_0,c = P_c;
P_0,d = P_d;
```

```
P_{0,W} = P_W;

TellVerifier[{"a0"→a_0,"b0"→b_0,"_cost"→"scalar"}];
If[!interactive,
    FiatShamirAdd["a0",a_0,entropyParameters["scalar"]];
    FiatShamirAdd["b0",b_0,entropyParameters["scalar"]];
];
c_0 = modq[a_0*b_0];

TellVerifier[{"a0W"→a_{0,W},"b0W"→b_{0,W},"_cost"→"scalar"}];
If[!interactive,
    FiatShamirAdd["a0W",a_{0,W},entropyParameters["scalar"]];
    FiatShamirAdd["b0W",b_{0,W},entropyParameters["scalar"]];
];
c_{0,W} = modq[a_{0,W}*b_{0,W}];

Print[Grid[{
    {Style["Iteration "<>ciStr<>" (Counting from "<>IntegerString[k_2[[1]]]<>" to 0)"], SpanFrom
    {Style["Name",Bold],Style["Semantics"],Style["Knowledge",Bold],Style["Value",Bold]},
    {"n_0 := n_2."<>ciStr<>"[1] ?= 1","Halving Complete?","P,V",n_0==1},
    {"k_0 := k_2."<>ciStr<>"[1] ?= 0","Halving Complete?","P,V",k_0==0},
    {"G_0 := G_2→."<>ciStr<>"[1]","","P,V",G_0},
    {"H_0 := H_2→."<>ciStr<>"[1]","","P,V",H_0},
    {"B_0 := B_2→."<>ciStr<>"[1]","","P,V",B_0},
    {"C_0 := C_2→."<>ciStr<>"[1]","","P,V",C_0},
    {"D_0 := D_2→."<>ciStr<>"[1]","","P,V",D_0},
    {"a_0 := a_2→."<>ciStr<>"[1]","","P,V",a_0},
    {"b_0 := b_2→."<>ciStr<>"[1]","","P,V",b_0},
    {"a_{0,W} := a_{2,W}→."<>ciStr<>"[1]","","P,V",a_{0,W}},
    {"b_{0,W} := b_{2,W}→."<>ciStr<>"[1]","","P,V",b_{0,W}},
    {"P_{0,{h,b,c,W}} := P_{2,{h,b,c,W}}."<>ciStr,"","P,V",{P_{0,h},P_{0,b},P_{0,c},P_{0,W}}},
    {"c_0 := a_0b_0","","P,V",c_0},
    {"c_{0,W} := a_{0,W}b_{0,W}","","P,V",c_{0,W}},
    {"P_{0,{h,b,c,d,W}} ?= P´_{h,b,c,d,W}} + <u_2^2,L_{2,{h,b,c,d,W}}> + <u_2^-2,R_{2,{h,b,c,d,W}}>","Sanity Check\nfor P_0","P,
    {"P_{0,{h,b,c,d}} ?= G_0a_0 + {H,B,C,D}_0b_0 + c_0g´","Verifier's Check","P,V",{P_{0,h}==G_0*a_0+H_0*b_0+g´*c_0,
    {"P_{0,W} ?= G_0a_{0,W} + H_0b_{0,W} + c_{0,W}g´","Verifier's Check","P,V",P_{0,W}==G_0*a_{0,W}+H_0*b_{0,W}+g´*c_{0,W}}
}, Alignment→{{Left,Left,Left,Left}},Frame→All]]

Print["Inner product protocol finished!"]
Print[CommunicationCostGrid[]]
If[!interactive,Print[FiatShamirGrid[]]];
ProofFinished[];
StateMachineSave["inner_product_halving"];
```

Iteration 2 (Counting from 2 to 0)			
Name	**Semantics**	**Knowledge**	**Value**

$k := k_2.2$	Current Iteration (counting down)	P,V	2
$n_2.2 = 2^k$	Current Length of Vectors	P,V	4
$\vec{G} := \vec{G_2}.2$		P,V (implicit)	{ecPnt[101 548 470 124 358 210 188 072 679 - 181 678 188 450 387 789 916 654 - 718 462 374 321 277 161 805 765 - 354, 70 108 350 633 035 199 759 065 376 - 354 370 719 210 357 510 544 392 - 766 796 027 711 414 587 086 150 - 112], ecPnt[81 881 281 191 882 355 160 881 140 - 819 926 411 859 223 579 216 161 - 786 219 247 020 789 084 841 886 - 435, 40 551 526 063 420 644 421 580 965 - 386 725 729 859 544 147 053 123 - 598 525 382 531 556 934 666 119 - 757], ecPnt[27 427 957 168 767 222 510 921 650 - 620 077 570 798 709 753 797 557 - 336 240 233 137 618 475 833 226 - 690, 42 650 441 509 520 284 448 005 737 - 515 710 331 630 163 209 846 762 - 957 134 645 512 392 724 356 208 - 176], ecPnt[∞, ∞]}
$\vec{H} := \vec{H_2}.2$		P,V (implicit)	{ecPnt[78 567 409 798 129 814 866 150 056 - 060 307 810 399 673 849 671 094 - 211 427 553 792 618 009 791 659 - 223, 50 464 327 830 870 926 983 164 620 - 566 499 054 037 449 550 745 776 - 160 850 919 973 618 220 747 519 - 859], ecPnt[16 230 325 873 944 567 770 651 181 - 130 303 324 912 121 224 490 802 - 407 282 022 789 649 993 284 143 - 768, 13 743 595 330 208 364 632 961 058 - 787 086 372 972 527 668 621 267 - 658 729 713 274 917 516 765 878 - 025], ecPnt[73 955 863 155 933 535 982 859 074 - 509 836 995 565 814 682 227 118 - 115 222 970 062 094 871 722 157 - 004, 12 661 142 626 516 128 143 965 107 - 877 524 977 948 748 772 063 737 - 046 982 621 034 957 911 954 836 - 350], ecPnt[∞, ∞]}

$\vec{B} := \overrightarrow{B_2}.2$		P,V (implicit)	{ecPnt[59 043 719 839 056 093 060 455 647 - 773 031 110 426 513 415 445 959 - 592 906 283 022 536 109 982 690 - 406, 15 581 121 562 794 375 473 593 189 - 690 062 526 490 521 359 132 176 - 103 829 752 471 918 632 370 295 - 336], ecPnt[112 521 091 029 611 710 525 094 888 - 851 919 040 284 401 236 803 289 - 858 290 779 025 976 942 166 966 - 892, 71 802 849 234 922 876 881 679 460 - 540 584 158 214 170 652 826 348 - 764 564 492 847 489 002 175 595 - 813], ecPnt[35 174 235 482 391 906 576 550 590 - 433 357 833 240 355 046 807 245 - 255 381 964 494 894 476 083 182 - 660, 55 925 870 782 800 122 155 770 079 - 253 820 122 879 523 420 329 479 - 534 761 202 990 107 031 888 939 - 945], ecPnt[∞, ∞]}
$\vec{C} := \overrightarrow{C_2}.2$		P,V (implicit)	{ecPnt[82 677 993 194 665 902 474 541 122 - 728 628 239 106 974 633 730 721 - 916 315 448 799 654 380 724 509 - 062, 82 899 414 855 368 741 404 724 030 - 068 539 514 612 899 114 324 925 - 700 999 638 050 403 382 505 421 - 116], ecPnt[45 422 098 385 527 520 105 729 242 - 155 385 912 239 396 352 275 187 - 691 869 915 510 620 991 934 660 - 246, 42 981 417 682 506 542 040 834 084 - 511 832 054 752 082 115 267 275 - 737 379 170 623 738 544 398 871 - 700], ecPnt[79 731 591 686 381 398 751 792 815 - 416 125 448 258 844 377 845 199 - 135 938 472 730 072 263 316 128 - 928, 14 986 293 206 980 309 680 514 267 - 840 081 157 662 963 426 467 477 - 088 209 824 552 014 914 871 589 - 040], ecPnt[∞, ∞]}

$\vec{D} := \overrightarrow{D_2}.2$		P,V (implicit)	{ecPnt[97 038 873 997 667 556 164 890 627 - 159 143 816 584 036 737 601 412 - 047 181 786 115 325 137 586 601 - 893, 28 632 182 194 222 295 567 409 644 - 033 114 434 203 763 962 660 717 - 808 858 714 880 991 421 895 676 - 479], ecPnt[114 943 785 603 625 565 834 113 287 - 895 479 632 817 105 457 530 959 - 156 178 552 924 525 977 788 156 - 149, 75 005 268 061 152 234 748 488 293 - 094 956 398 629 562 793 675 286 - 378 681 571 354 303 324 894 122 - 899], ecPnt[34 283 013 894 072 667 721 275 831 - 653 793 797 981 117 913 068 563 - 331 324 282 032 073 934 983 384 - 369, 16 444 072 431 226 081 049 726 942 - 532 624 576 021 955 849 773 018 - 079 843 576 838 182 070 874 161 - 038], ecPnt[∞, ∞]}
$\vec{a} := \overrightarrow{a_2}.2$		P	{61 442 343 775 113 140 880 034 650 - 887 022 378 965 571 424 979 173 001 - 973 397 458 542 222 999 566 892, 112 164 513 297 470 756 571 473 984 - 141 438 273 936 195 334 402 062 428 - 015 459 026 081 712 107 932 702, 100 474 102 720 414 684 705 898 037 - 977 251 389 482 922 603 087 723 310 - 707 681 533 634 105 023 940 360, 0}
$\vec{b} := \overrightarrow{b_2}.2$		P	{62 425 708 243 501 832 904 842 395 - 569 180 717 767 201 166 970 569 719 - 744 186 579 509 066 013 239 789, 108 894 093 373 790 087 805 981 249 - 637 450 006 012 557 717 717 172 910 - 157 161 661 185 273 450 166 896, 80 085 874 135 138 745 719 381 189 - 911 405 897 849 137 938 574 627 947 - 766 879 149 979 384 405 495 240, 0}
$\vec{a_w} := \overrightarrow{a_{2,w}}.2$		P	{48 564 477 212 184 250 415 170 747 - 693 694 481 439 232 973 935 076 016 - 590 509 497 532 087 603 698 870, 8 819 342 647 412 475 122 593 262 - 319 876 611 403 831 739 595 798 027 - 640 620 830 864 043 632 355 299, 115 268 474 747 795 881 775 546 216 - 783 739 194 713 511 413 966 655 407 - 981 146 926 754 407 903 409 076, 0}

$\overrightarrow{b_W}$:= $\overrightarrow{b_{2,W}}$.2		P	{73 357 405 155 266 425 915 543 821 - 545 319 812 280 870 144 848 159 677 - 532 949 644 361 748 894 556 594, 26 473 080 131 638 368 664 311 419 - 668 052 580 406 527 293 561 077 903 - 757 204 398 370 221 010 052 161, 8 085 424 818 135 938 036 088 244 - 802 558 875 166 648 813 733 660 931 - 210 189 856 208 497 918 675 798, 0}
$P_{\{h,b,c,d,W\}}$:= $P_{2,\{h,b,c,d,W\}}$.2		P,V (implicit)	{ecPnt[42 427 373 215 793 781 659 408 924 - 843 768 227 225 882 770 225 375 - 757 126 397 503 527 068 891 674 - 844, 25 721 469 407 782 422 059 186 990 - 187 869 888 211 409 564 752 656 - 079 140 365 100 434 148 494 723 - 328], ecPnt[53 093 155 971 198 350 375 134 075 - 441 510 772 569 193 709 629 578 - 094 931 141 813 154 602 240 565 - 106, 55 938 320 630 024 527 613 951 665 - 036 283 624 008 160 716 735 992 - 177 830 942 127 603 092 847 901 - 156], ecPnt[87 623 278 363 384 013 501 616 299 - 287 548 132 476 250 177 902 650 - 041 648 463 953 140 336 403 353 - 190, 41 060 481 386 143 080 378 375 521 - 196 934 627 853 309 131 610 093 - 864 338 133 773 149 938 053 272 - 351], ecPnt[81 848 919 976 003 370 114 473 563 - 771 257 237 692 448 808 430 626 - 166 945 431 568 046 554 818 008 - 682, 2 643 826 270 596 107 626 712 310 - 049 127 795 608 650 776 351 598 - 726 801 898 843 301 631 070 212 - 794], ecPnt[98 991 610 698 448 567 601 040 979 - 656 886 525 408 488 940 163 120 - 548 218 252 896 669 433 046 079 - 564, 52 231 224 843 856 607 266 205 397 - 725 579 670 752 662 648 688 237 - 226 846 639 049 801 479 304 835 - 028]}

Name	**Knowledge**	**Value**
(1) $L_{\{h,b,c,d\}}$:= $L_{2,\{h,b,c,d\}}$.2 := (2) $\langle\overrightarrow{a_{lo}},\overrightarrow{G_{hi}}\rangle$ + $\langle\overrightarrow{b_{hi}},\overrightarrow{\{H, B, C, D\}_{lo}}\rangle$ + $\langle\overrightarrow{a_{lo}},\overrightarrow{b_{hi}}\rangle g'$	1: P,V 2: P	{ecPnt[51 937 848 323 061 722 610 475 181 980 830 - 591 914 660 958 406 428 433 789 558 240 107 - 198 247 801 268, 106 560 155 938 380 029 201 930 354 580 040 - 167 551 432 141 775 760 085 148 764 943 146 - 178 634 187 408], ecPnt[79 863 622 949 771 475 243 779 360 474 452 - 590 639 328 325 896 457 338 087 659 196 341 -

(1) $R_{\{h,b,c,d\}}$:= $R_{2,\{h,b,c,d\}}$.2 := (2) $\langle \overrightarrow{a_{hi}}, \overrightarrow{G_{lo}} \rangle$ + $\langle \overrightarrow{b_{lo}}, \overrightarrow{\{H, B, C, D\}_{hi}} \rangle$ + $\langle \overrightarrow{a_{hi}}, \overrightarrow{b_{lo}} \rangle g'$	1: P,V 2: P	{ecPnt[13 573 483 833 446 195 039 386 191 823 126 - 470 200 557 258 027 456 445 688 282 344 784 - 336 103 649 212, 92 052 865 363 241 580 056 892 319 302 489 - 258 396 224 827 868 501 036 283 611 297 590 - 954 929 380 563], ecPnt[87 157 328 238 784 876 368 170 585 205 145 - 864 149 517 917 546 640 676 011 828 505 926 - 229 337 545 559, 49 329 002 166 834 480 429 318 163 327 266 - 459 724 785 883 670 773 200 913 837 835 518 - 032 372 564 965], ecPnt[71 520 343 767 673 936 517 024 801 860 388 - 366 635 511 719 271 546 226 054 794 719 093 - 802 183 956 346, 9 553 873 364 145 156 327 236 306 452 545 - 122 960 621 391 111 899 159 271 714 122 464 - 263 182 680 439], ecPnt[46 035 612 930 752 939 628 947 962 040 107 - 160 554 358 813 179 886 532 133 542 862 333 - 459 924 699 781, 45 447 377 390 389 063 397 803 533 683 113 - 774 914 322 866 417 884 852 592 242 983 262 - 329 077 405 730]}
(1) L_W := $L_{2,W}$.2 := (2) $\langle \overrightarrow{a_{lo,W}}, \overrightarrow{G_{hi}} \rangle$ + $\langle \overrightarrow{b_{hi,W}}, \overrightarrow{H_{lo}} \rangle$ + $\langle \overrightarrow{a_{lo,W}}, \overrightarrow{b_{hi,W}} \rangle g'$	1: P,V 2: P	ecPnt[72 556 481 017 632 433 693 661 511 017 633 298 - 756 512 321 178 079 509 482 506 125 039 316 - 340 588 923, 58 628 123 834 064 766 575 081 733 647 402 276 - 204 937 487 939 674 442 001 533 559 083 399 - 118 278 801]
(1) R_W := $R_{2,W}$.2 := (2) $\langle \overrightarrow{a_{hi,W}}, \overrightarrow{G_{lo}} \rangle$ + $\langle \overrightarrow{b_{lo,W}}, \overrightarrow{H_{hi}} \rangle$ + $\langle \overrightarrow{a_{hi,W}}, \overrightarrow{b_{lo,W}} \rangle g'$	1: P,V 2: P	ecPnt[78 477 488 904 028 436 481 347 412 600 613 206 - 616 914 628 278 154 149 166 226 514 663 489 - 162 792 819, 6 247 703 021 684 575 120 229 172 459 504 646 - 297 671 321 951 456 904 911 106 626 166 428 - 084 591 726]

Waiting to receive u.2 from InteractiveVerifier ...

Fold $\vec{G}$, $\vec{H}$, $\vec{B}$, $\vec{C}$, $\vec{P}$, $\vec{a}$ and $\vec{b}$ based on challenge u_{IP}		
Name	**Knowledge**	**Value**
u_{IP} = u_2.2	P,V	49 778 263 016 596 358 861 024 029 034 781 411 - 586 030 758 570 633 068 967 576 917 901 438 - 334 298 455

$\overrightarrow{G_{next}} := u_{IP}^{-1}\overrightarrow{G_{lo}} + u_{IP}\overrightarrow{G_{hi}}$	P,V	{ecPnt[7 197 114 176 193 752 980 303 643 403 695 - 828 532 990 120 997 512 485 136 578 092 011 - 866 184 268 691, 60 730 773 379 641 461 649 895 581 236 702 - 273 487 306 200 766 726 745 877 010 587 530 - 816 841 971 454], ecPnt[25 740 309 652 130 294 792 014 274 623 822 - 906 233 778 698 385 632 087 797 179 590 756 - 586 611 447 326, 7 559 288 557 352 841 504 839 453 446 974 - 796 689 854 239 679 145 566 894 672 072 255 - 236 025 649 192]}
$\overrightarrow{H_{next}} := u_{IP}\overrightarrow{H_{lo}} + u_{IP}^{-1}\overrightarrow{H_{hi}}$	P,V	{ecPnt[9 923 669 315 589 724 236 175 802 580 426 - 592 379 857 281 435 169 619 817 581 664 784 - 806 305 050 600, 69 301 315 300 106 900 630 344 329 105 588 - 533 710 615 432 967 412 701 440 587 206 110 - 103 239 979 056], ecPnt[69 958 554 280 672 469 733 643 275 419 680 - 116 457 375 050 330 391 348 300 638 192 607 - 697 674 499 972, 70 322 526 074 710 939 661 538 785 781 005 - 409 111 808 935 480 016 459 677 331 324 303 - 468 832 670 948]}
$\overrightarrow{B_{next}} := u_{IP}\overrightarrow{B_{lo}} + u_{IP}^{-1}\overrightarrow{B_{hi}}$	P,V	{ecPnt[103 181 688 540 283 550 900 115 377 074 572 - 906 022 092 269 214 954 726 718 790 501 569 - 337 390 653 136, 88 587 317 905 811 582 887 852 333 128 737 - 362 967 001 668 115 722 517 496 378 551 323 - 743 472 873 003], ecPnt[78 043 950 849 939 684 905 494 886 280 107 - 655 203 568 705 298 939 663 195 960 427 464 - 870 794 481 036, 63 028 727 487 347 507 861 088 825 955 612 - 637 572 326 719 118 902 670 929 364 859 450 - 357 002 591 244]}
$\overrightarrow{C_{next}} := u_{IP}\overrightarrow{C_{lo}} + u_{IP}^{-1}\overrightarrow{C_{hi}}$	P,V	{ecPnt[77 648 398 834 955 981 434 915 225 171 372 - 670 033 920 110 798 382 972 995 557 496 536 - 072 160 616 152, 114 993 206 617 194 884 582 252 467 178 870 - 559 035 021 674 392 919 932 899 922 134 085 - 890 650 235 761], ecPnt[4 016 477 553 053 980 634 592 868 942 935 - 513 988 297 652 249 720 374 332 911 319 787 - 059 969 395 864, 107 780 355 073 054 246 547 274 550 757 710 - 943 490 511 352 511 246 624 914 557 077 087 - 278 354 014 724]}

$\overrightarrow{D_{next}} := u_{IP}\overrightarrow{D_{lo}} + u_{IP}^{-1}\overrightarrow{D_{hi}}$	P,V	{ecPnt[9 204 564 868 782 270 412 870 134 496 961 - 531 211 545 298 619 676 831 565 162 531 509 - 980 471 661 504, 110 656 730 936 786 158 948 279 040 537 731 - 806 719 194 876 348 740 960 648 492 508 893 - 706 752 655 534], ecPnt[57 318 399 460 579 651 382 855 744 160 054 - 965 144 349 045 280 754 541 796 339 058 133 - 751 450 351 507, 9 752 431 091 061 141 156 954 293 420 600 - 431 415 368 763 923 621 403 283 475 976 022 - 665 295 425 015]}
$P_{next,\{h,b,c,d,W\}} := P_{\{h,b,c,d,W\}} + u_{IP}^{2}L_{\{h,b,c,d,W\}} + u_{IP}^{-2}R_{\{h,b,c,d,W\}}$	P,V	{ecPnt[86 549 293 700 705 576 310 670 778 784 597 - 836 333 741 541 083 996 755 111 959 480 234 - 696 972 978 414, 20 933 742 971 864 474 163 704 352 952 168 - 549 433 873 232 361 691 192 046 047 306 574 - 101 250 855 678], ecPnt[5 329 237 281 080 061 557 087 386 541 512 - 094 989 216 765 361 219 651 754 727 494 075 - 651 069 853 882, 25 505 779 482 843 203 644 899 024 985 738 - 424 791 777 493 582 803 862 991 865 292 667 - 174 203 131 274], ecPnt[101 669 631 185 013 308 541 174 320 487 441 - 264 026 981 613 007 202 453 793 298 531 133 - 729 240 553 633, 82 960 685 798 015 610 060 110 994 730 438 - 408 801 163 464 994 126 881 961 038 986 643 - 726 868 054 985], ecPnt[80 930 121 240 166 102 505 541 582 335 909 - 769 099 418 550 745 921 470 989 327 339 028 - 870 473 478 673, 73 213 433 432 881 882 608 741 265 907 352 - 624 933 247 540 024 738 086 475 996 367 177 - 305 424 525 869], ecPnt[77 655 419 294 702 414 646 521 152 577 006 - 451 504 570 431 019 614 816 380 532 870 948 - 964 923 887 672, 68 497 091 790 293 927 373 067 739 936 022 - 331 983 241 210 497 850 650 557 960 541 940 - 114 992 397 821]}
$\overrightarrow{a_{next}} = u_{IP}\overrightarrow{a_{lo}} + u_{IP}^{-1}\overrightarrow{a_{hi}}$	P	{38 826 934 934 266 278 564 376 991 932 224 879 - 921 467 884 016 384 437 669 174 859 001 433 - 652 826 451, 14 950 440 508 257 192 435 052 892 282 924 338 - 455 941 822 798 411 013 554 535 366 510 172 - 265 708 252}

$\overrightarrow{b_{next}} = u_{IP}^{-1}\overrightarrow{b_{lo}} + u_{IP}\overrightarrow{b_{hi}}$	P	{59 997 829 551 751 729 144 732 031 187 108 785 - 825 000 434 286 957 416 101 173 056 956 235 - 494 774 978, 34 806 094 471 593 118 319 815 582 709 700 137 - 835 049 304 731 731 998 692 617 281 333 970 - 707 499 188}
$\overrightarrow{a_{next,W}} = u_{IP}\overrightarrow{a_{lo,W}} + u_{IP}^{-1}\overrightarrow{a_{hi,W}}$	P	{21 636 613 409 272 720 301 495 908 564 816 535 - 377 739 717 154 564 729 269 573 025 062 875 - 800 622 490, 63 694 636 969 989 547 141 670 523 040 843 444 - 911 499 086 548 713 728 140 695 990 018 264 - 233 587 777}
$\overrightarrow{b_{next,W}} = u_{IP}^{-1}\overrightarrow{b_{lo,W}} + u_{IP}\overrightarrow{b_{hi,W}}$	P	{2 947 963 732 633 331 054 907 160 418 259 914 - 054 475 788 531 314 040 482 397 781 918 326 - 889 928 834, 59 196 493 273 039 883 537 911 480 529 904 968 - 370 093 255 244 710 882 573 057 833 282 435 - 404 050 859}
$P_{next,\{h,b,c,d\}} \stackrel{?}{=} \langle\overrightarrow{a_{next}}, \overrightarrow{G_{next}}\rangle + \langle\overrightarrow{b_{next}}, \overrightarrow{\{H, B, C, D\}_{next}}\rangle + \langle\overrightarrow{a_{next}}, \overrightarrow{b_{next}}\rangle g'$	P	{True, True, True, True}
$P_{next,W} \stackrel{?}{=} \langle\overrightarrow{a_{next,W}}, \overrightarrow{G_{next}}\rangle + \langle\overrightarrow{b_{next,W}}, \overrightarrow{H_{next}}\rangle + \langle\overrightarrow{a_{next,W}}, \overrightarrow{b_{next,W}}\rangle g'$	P	True

Iteration 1 (Counting from 2 to 0)

Name	**Semantics**	**Knowledge**	**Value**
$k := k_2.1$	Current Iteration (counting down)	P,V	1
$n_2.1 = 2^k$	Current Length of Vectors	P,V	2
$\vec{G} := \overrightarrow{G_2}.1$		P,V (implicit)	{ecPnt[7 197 114 176 193 752 980 303 643 - 403 695 828 532 990 120 997 512 - 485 136 578 092 011 866 184 268 - 691, 60 730 773 379 641 461 649 895 581 - 236 702 273 487 306 200 766 726 - 745 877 010 587 530 816 841 971 - 454], ecPnt[25 740 309 652 130 294 792 014 274 - 623 822 906 233 778 698 385 632 - 087 797 179 590 756 586 611 447 - 326, 7 559 288 557 352 841 504 839 453 - 446 974 796 689 854 239 679 145 - 566 894 672 072 255 236 025 649 - 192]}

$\vec{H}$:= $\overrightarrow{H_2}$.1		P,V (implicit)	{ecPnt[9 923 669 315 589 724 236 175 802 - 580 426 592 379 857 281 435 169 - 619 817 581 664 784 806 305 050 - 600, 69 301 315 300 106 900 630 344 329 - 105 588 533 710 615 432 967 412 - 701 440 587 206 110 103 239 979 - 056], ecPnt[69 958 554 280 672 469 733 643 275 - 419 680 116 457 375 050 330 391 - 348 300 638 192 607 697 674 499 - 972, 70 322 526 074 710 939 661 538 785 - 781 005 409 111 808 935 480 016 - 459 677 331 324 303 468 832 670 - 948]}
$\vec{B}$:= $\overrightarrow{B_2}$.1		P,V (implicit)	{ecPnt[103 181 688 540 283 550 900 115 377 - 074 572 906 022 092 269 214 954 - 726 718 790 501 569 337 390 653 - 136, 88 587 317 905 811 582 887 852 333 - 128 737 362 967 001 668 115 722 - 517 496 378 551 323 743 472 873 - 003], ecPnt[78 043 950 849 939 684 905 494 886 - 280 107 655 203 568 705 298 939 - 663 195 960 427 464 870 794 481 - 036, 63 028 727 487 347 507 861 088 825 - 955 612 637 572 326 719 118 902 - 670 929 364 859 450 357 002 591 - 244]}
$\vec{C}$:= $\overrightarrow{C_2}$.1		P,V (implicit)	{ecPnt[77 648 398 834 955 981 434 915 225 - 171 372 670 033 920 110 798 382 - 972 995 557 496 536 072 160 616 - 152, 114 993 206 617 194 884 582 252 467 - 178 870 559 035 021 674 392 919 - 932 899 922 134 085 890 650 235 - 761], ecPnt[4 016 477 553 053 980 634 592 868 - 942 935 513 988 297 652 249 720 - 374 332 911 319 787 059 969 395 - 864, 107 780 355 073 054 246 547 274 550 - 757 710 943 490 511 352 511 246 - 624 914 557 077 087 278 354 014 - 724]}

$\vec{D} := \overrightarrow{D_2}.1$		P,V (implicit)	{ecPnt[9 204 564 868 782 270 412 870 134 - 496 961 531 211 545 298 619 676 - 831 565 162 531 509 980 471 661 - 504, 110 656 730 936 786 158 948 279 040 - 537 731 806 719 194 876 348 740 - 960 648 492 508 893 706 752 655 - 534], ecPnt[57 318 399 460 579 651 382 855 744 - 160 054 965 144 349 045 280 754 - 541 796 339 058 133 751 450 351 - 507, 9 752 431 091 061 141 156 954 293 - 420 600 431 415 368 763 923 621 - 403 283 475 976 022 665 295 425 - 015]}
$\vec{a} := \overrightarrow{a_2}.1$		P	{38 826 934 934 266 278 564 376 991 - 932 224 879 921 467 884 016 384 437 - 669 174 859 001 433 652 826 451, 14 950 440 508 257 192 435 052 892 - 282 924 338 455 941 822 798 411 013 - 554 535 366 510 172 265 708 252}
$\vec{b} := \overrightarrow{b_2}.1$		P	{59 997 829 551 751 729 144 732 031 - 187 108 785 825 000 434 286 957 416 - 101 173 056 956 235 494 774 978, 34 806 094 471 593 118 319 815 582 - 709 700 137 835 049 304 731 731 998 - 692 617 281 333 970 707 499 188}
$\overrightarrow{a_w} := \overrightarrow{a_{2,w}}.1$		P	{21 636 613 409 272 720 301 495 908 - 564 816 535 377 739 717 154 564 729 - 269 573 025 062 875 800 622 490, 63 694 636 969 989 547 141 670 523 - 040 843 444 911 499 086 548 713 728 - 140 695 990 018 264 233 587 777}
$\overrightarrow{b_w} := \overrightarrow{b_{2,w}}.1$		P	{2 947 963 732 633 331 054 907 160 - 418 259 914 054 475 788 531 314 040 - 482 397 781 918 326 889 928 834, 59 196 493 273 039 883 537 911 480 - 529 904 968 370 093 255 244 710 882 - 573 057 833 282 435 404 050 859}

$P_{\{h,b,c,d,W\}} := P_{2,\{h,b,c,d,W\}}.1$		P,V (implicit)	{ecPnt[86 549 293 700 705 576 310 670 778 - 784 597 836 333 741 541 083 996 - 755 111 959 480 234 696 972 978 - 414, 20 933 742 971 864 474 163 704 352 - 952 168 549 433 873 232 361 691 - 192 046 047 306 574 101 250 855 - 678], ecPnt[5 329 237 281 080 061 557 087 386 - 541 512 094 989 216 765 361 219 - 651 754 727 494 075 651 069 853 - 882, 25 505 779 482 843 203 644 899 024 - 985 738 424 791 777 493 582 803 - 862 991 865 292 667 174 203 131 - 274], ecPnt[101 669 631 185 013 308 541 174 320 - 487 441 264 026 981 613 007 202 - 453 793 298 531 133 729 240 553 - 633, 82 960 685 798 015 610 060 110 994 - 730 438 408 801 163 464 994 126 - 881 961 038 986 643 726 868 054 - 985], ecPnt[80 930 121 240 166 102 505 541 582 - 335 909 769 099 418 550 745 921 - 470 989 327 339 028 870 473 478 - 673, 73 213 433 432 881 882 608 741 265 - 907 352 624 933 247 540 024 738 - 086 475 996 367 177 305 424 525 - 869], ecPnt[77 655 419 294 702 414 646 521 152 - 577 006 451 504 570 431 019 614 - 816 380 532 870 948 964 923 887 - 672, 68 497 091 790 293 927 373 067 739 - 936 022 331 983 241 210 497 850 - 650 557 960 541 940 114 992 397 - 821]}

Name	Knowledge	Value
(1) $L_{\{h,b,c,d\}} := L_{2,\{h,b,c,d\}}.1 :=$ (2) $<\overrightarrow{a_{lo}},\overrightarrow{G_{hi}}> +$ $<\overrightarrow{b_{hi}},\overrightarrow{\{H, B, C, D\}_{lo}}> + <\overrightarrow{a_{lo}},\overrightarrow{b_{hi}}>g'$	1: P,V 2: P	{ecPnt[75 675 059 526 275 504 068 918 777 111 604 - 858 788 471 629 915 134 420 171 265 812 896 - 626 119 066 391, 18 197 204 939 082 113 188 285 923 802 867 - 554 462 472 120 668 263 296 596 875 421 190 - 375 977 857 454], ecPnt[12 416 377 022 545 922 744 939 982 468 289 - 996 520 934 072 056 023 744 431 017 501 656 - 184 389 730 319, 81 051 326 905 139 913 890 607 962 198 725 - 137 410 169 439 643 088 588 490 840 272 138 - 742 545 929 540], ecPnt[98 853 291 129 251 635 680 053 212 406 582 - 180 789 552 600 828 913 507 523 250 568 084 - 217 954 820 657, 87 281 355 932 318 972 300 122 755 145 147 - 993 995 828 597 934 957 482 135 707 810 979 -

(1) $R_{\{h,b,c,d\}}$:= $R_{2,\{h,b,c,d\}}$.1 := (2) $\langle \overrightarrow{a_{hi}}, \overrightarrow{G_{lo}} \rangle$ + $\langle \overrightarrow{b_{lo}}, \overrightarrow{\{H, B, C, D\}_{hi}} \rangle$ + $\langle \overrightarrow{a_{hi}}, \overrightarrow{b_{lo}} \rangle g'$	1: P,V 2: P	{ecPnt[30 549 668 247 877 315 168 586 354 189 454 - 040 046 905 352 468 501 612 133 078 991 262 - 937 458 834 121, 8 064 041 257 520 572 495 742 525 983 644 - 270 490 558 397 227 754 385 810 941 773 435 - 446 589 877 912], ecPnt[17 271 082 237 114 661 662 782 139 528 333 - 954 135 060 936 698 181 697 107 019 792 539 - 131 982 397 059, 100 485 113 882 867 413 113 226 576 224 258 - 467 945 632 855 040 297 438 669 404 557 630 - 187 333 726 261], ecPnt[77 039 539 825 354 912 829 621 507 432 128 - 099 080 227 116 487 899 322 574 405 235 729 - 421 193 756 314, 19 810 300 289 411 477 639 048 480 556 880 - 870 950 820 614 431 045 845 021 683 132 249 - 865 903 583 930], ecPnt[93 268 138 165 182 546 384 818 285 702 418 - 187 945 928 666 090 817 865 643 211 434 544 - 562 242 435 789, 111 279 597 227 286 293 277 376 134 144 323 - 743 374 311 220 963 861 626 278 010 175 736 - 815 569 060 927]}
(1) L_W := $L_{2,W}$.1 := (2) $\langle \overrightarrow{a_{lo,W}}, \overrightarrow{G_{hi}} \rangle$ + $\langle \overrightarrow{b_{hi,W}}, \overrightarrow{H_{lo}} \rangle$ + $\langle \overrightarrow{a_{lo,W}}, \overrightarrow{b_{hi,W}} \rangle g'$	1: P,V 2: P	ecPnt[14 388 906 438 534 551 094 002 496 836 880 047 - 677 016 190 339 915 135 357 923 304 609 889 - 922 238 095, 25 350 077 021 118 276 994 302 587 444 563 735 - 933 315 591 300 912 219 383 404 434 462 160 - 307 924 273]
(1) R_W := $R_{2,W}$.1 := (2) $\langle \overrightarrow{a_{hi,W}}, \overrightarrow{G_{lo}} \rangle$ + $\langle \overrightarrow{b_{lo,W}}, \overrightarrow{H_{hi}} \rangle$ + $\langle \overrightarrow{a_{hi,W}}, \overrightarrow{b_{lo,W}} \rangle g'$	1: P,V 2: P	ecPnt[101 171 956 531 732 571 746 440 210 062 672 - 013 112 905 510 995 303 776 665 016 931 002 - 977 742 739 679, 95 465 264 805 104 010 998 282 450 451 339 127 - 840 467 517 182 363 902 674 875 441 902 949 - 420 100 229]

Waiting to receive u.1 from InteractiveVerifier ...

Fold $\vec{G}$, $\vec{H}$, $\vec{B}$, $\vec{C}$, $\vec{P}$, $\vec{a}$ and $\vec{b}$ based on challenge u_{IP}		
Name	**Knowledge**	**Value**
u_{IP} = u_2.1	P,V	60 107 283 168 128 902 360 549 399 981 388 134 - 586 079 393 627 328 093 194 820 115 310 250 - 308 340 078
$\overrightarrow{G_{next}}$:= $u_{IP}^{-1}\overrightarrow{G_{lo}}$ + $u_{IP}\overrightarrow{G_{hi}}$	P,V	{ecPnt[106 047 928 382 399 298 606 307 270 553 659 - 199 565 771 566 643 562 941 779 995 199 351 - 454 640 836 231, 93 720 323 795 988 478 677 394 413 863 093 - 059 165 226 732 196 254 855 469 832 899 039 - 748 827 794 813]}

$\overrightarrow{H_{next}} := u_{IP}\overrightarrow{H_{lo}} + u_{IP}^{-1}\overrightarrow{H_{hi}}$	P,V	{ecPnt[65 798 702 696 880 764 213 759 080 205 885 - 559 823 919 736 555 092 196 315 458 956 414 - 043 528 990 417, 113 060 727 953 871 578 706 455 950 897 122 - 407 255 435 350 435 014 258 540 357 290 902 - 460 111 718 764]}
$\overrightarrow{B_{next}} := u_{IP}\overrightarrow{B_{lo}} + u_{IP}^{-1}\overrightarrow{B_{hi}}$	P,V	{ecPnt[51 263 962 075 200 262 089 977 527 991 489 - 154 090 256 876 495 239 263 853 673 968 662 - 269 867 159 880, 59 304 354 354 125 370 257 888 899 770 035 - 709 731 793 990 653 314 774 277 689 815 845 - 108 336 596 654]}
$\overrightarrow{C_{next}} := u_{IP}\overrightarrow{C_{lo}} + u_{IP}^{-1}\overrightarrow{C_{hi}}$	P,V	{ecPnt[3 063 446 378 215 682 504 529 818 388 742 - 295 906 691 774 205 907 395 646 281 960 170 - 478 485 277 782, 41 711 340 372 428 252 715 592 184 575 370 - 511 221 524 887 064 978 818 572 894 341 476 - 773 483 215 453]}
$\overrightarrow{D_{next}} := u_{IP}\overrightarrow{D_{lo}} + u_{IP}^{-1}\overrightarrow{D_{hi}}$	P,V	{ecPnt[24 816 052 915 344 061 723 394 546 168 913 - 174 577 843 710 948 969 225 602 687 365 265 - 051 637 040 815, 67 401 455 371 277 781 651 260 916 671 100 - 331 294 882 258 933 658 861 019 459 735 037 - 385 044 630 090]}

$P_{next,\{h,b,c,d,W\}} := P_{\{h,b,c,d,W\}} + u_{IP}^{2} L_{\{h,b,c,d,W\}} + u_{IP}^{-2} R_{\{h,b,c,d,W\}}$	P,V	{ecPnt[89 558 932 688 492 177 722 272 018 113 494 - 238 314 242 283 658 549 690 867 267 807 775 - 428 511 718 321, 82 308 534 977 355 512 322 370 152 675 903 - 609 108 741 121 212 616 595 116 137 887 645 - 130 578 579 276], ecPnt[2 535 106 563 306 329 634 217 460 360 590 - 660 394 532 660 318 333 598 601 313 805 246 - 253 811 670 167, 37 905 362 638 224 769 609 916 560 569 773 - 911 176 947 719 296 274 603 389 536 502 708 - 617 675 361 051], ecPnt[112 719 119 487 721 161 889 159 211 082 551 - 290 789 635 633 197 790 401 234 517 080 402 - 764 506 322 042, 59 038 507 861 533 321 775 922 462 484 860 - 668 668 411 724 675 754 721 170 660 930 498 - 202 940 497 565], ecPnt[105 479 895 284 880 952 363 906 946 754 971 - 019 937 646 107 950 192 208 454 804 756 816 - 712 996 878 277, 88 367 073 377 840 609 503 965 989 028 276 - 026 025 955 631 419 100 797 652 975 414 156 - 539 639 740 891], ecPnt[66 576 517 566 997 309 876 776 372 876 836 - 199 019 185 475 935 761 406 744 525 505 228 - 996 757 486 023, 90 324 928 969 768 165 511 842 292 293 833 - 554 044 922 227 263 120 569 797 649 525 696 - 262 179 099 046]}
$\overrightarrow{a_{next}} = u_{IP}\overrightarrow{a_{lo}} + u_{IP}^{-1}\overrightarrow{a_{hi}}$	P	{108 423 123 045 658 025 157 618 639 588 976 - 361 816 248 958 028 757 952 488 070 957 825 - 485 293 867 099}
$\overrightarrow{b_{next}} = u_{IP}^{-1}\overrightarrow{b_{lo}} + u_{IP}\overrightarrow{b_{hi}}$	P	{42 898 793 650 488 454 998 791 851 268 901 023 - 693 781 135 981 625 855 329 285 685 978 384 - 189 744 313}
$\overrightarrow{a_{next,W}} = u_{IP}\overrightarrow{a_{lo,W}} + u_{IP}^{-1}\overrightarrow{a_{hi,W}}$	P	{1 375 560 257 280 688 522 612 389 858 362 182 - 280 930 062 576 340 977 657 137 703 999 687 - 345 468 197}
$\overrightarrow{b_{next,W}} = u_{IP}^{-1}\overrightarrow{b_{lo,W}} + u_{IP}\overrightarrow{b_{hi,W}}$	P	{77 752 142 049 699 130 174 929 194 338 535 297 - 301 448 986 784 213 237 165 185 139 643 741 - 664 012 763}
$P_{next,\{h,b,c,d\}} \stackrel{?}{=} <\overrightarrow{a_{next}},\overrightarrow{G_{next}}> + <\overrightarrow{b_{next}},\overrightarrow{\{H, B, C, D\}_{next}}> + <\overrightarrow{a_{next}},\overrightarrow{b_{next}}>g'$	P	{True, True, True, True}
$P_{next,W} \stackrel{?}{=} <\overrightarrow{a_{next,W}},\overrightarrow{G_{next}}> + <\overrightarrow{b_{next,W}},\overrightarrow{H_{next}}> + <\overrightarrow{a_{next,W}},\overrightarrow{b_{next,W}}>g'$	P	True

Iteration 0 (Counting from 2 to 0)			
Name	Semantics	**Knowledge**	**Value**

$n_0 := n_2.0[1] \stackrel{?}{=} 1$	Halving Complete?	P,V	True
$k_0 := k_2.0[1] \stackrel{?}{=} 0$	Halving Complete?	P,V	True
$G_0 := \overrightarrow{G_2}.0[1]$		P,V	ecPnt[106 047 928 382 399 298 606 307 - 270 553 659 199 565 771 566 643 - 562 941 779 995 199 351 454 640 - 836 231, 93 720 323 795 988 478 677 394 413 - 863 093 059 165 226 732 196 254 - 855 469 832 899 039 748 827 794 - 813]
$H_0 := \overrightarrow{H_2}.0[1]$		P,V	ecPnt[65 798 702 696 880 764 213 759 080 - 205 885 559 823 919 736 555 092 - 196 315 458 956 414 043 528 990 - 417, 113 060 727 953 871 578 706 455 - 950 897 122 407 255 435 350 435 - 014 258 540 357 290 902 460 111 - 718 764]
$B_0 := \overrightarrow{B_2}.0[1]$		P,V	ecPnt[51 263 962 075 200 262 089 977 527 - 991 489 154 090 256 876 495 239 - 263 853 673 968 662 269 867 159 - 880, 59 304 354 354 125 370 257 888 899 - 770 035 709 731 793 990 653 314 - 774 277 689 815 845 108 336 596 - 654]
$C_0 := \overrightarrow{C_2}.0[1]$		P,V	ecPnt[3 063 446 378 215 682 504 529 818 - 388 742 295 906 691 774 205 907 - 395 646 281 960 170 478 485 277 - 782, 41 711 340 372 428 252 715 592 184 - 575 370 511 221 524 887 064 978 - 818 572 894 341 476 773 483 215 - 453]
$D_0 := \overrightarrow{D_2}.0[1]$		P,V	ecPnt[24 816 052 915 344 061 723 394 546 - 168 913 174 577 843 710 948 969 - 225 602 687 365 265 051 637 040 - 815, 67 401 455 371 277 781 651 260 916 - 671 100 331 294 882 258 933 658 - 861 019 459 735 037 385 044 630 - 090]
$a_0 := \overrightarrow{a_2}.0[1]$		P,V	108 423 123 045 658 025 157 618 639 - 588 976 361 816 248 958 028 757 - 952 488 070 957 825 485 293 867 099

$b_0 := \overrightarrow{b_2}.0[1]$		P,V	42 898 793 650 488 454 998 791 851 - 268 901 023 693 781 135 981 625 - 855 329 285 685 978 384 189 744 313
$a_{0,W} := \overrightarrow{a_{2,W}}.0[1]$		P,V	1 375 560 257 280 688 522 612 389 - 858 362 182 280 930 062 576 340 - 977 657 137 703 999 687 345 468 197
$b_{0,W} := \overrightarrow{b_{2,W}}.0[1]$		P,V	77 752 142 049 699 130 174 929 194 - 338 535 297 301 448 986 784 213 - 237 165 185 139 643 741 664 012 763
$P_{0,\{h,b,c,W\}} := P_{2,\{h,b,c,W\}}.0$		P,V	{ecPnt[89 558 932 688 492 177 722 272 - 018 113 494 238 314 242 283 658 - 549 690 867 267 807 775 428 511 - 718 321, 82 308 534 977 355 512 322 370 - 152 675 903 609 108 741 121 212 - 616 595 116 137 887 645 130 578 - 579 276], ecPnt[2 535 106 563 306 329 634 217 460 - 360 590 660 394 532 660 318 333 - 598 601 313 805 246 253 811 670 - 167, 37 905 362 638 224 769 609 916 - 560 569 773 911 176 947 719 296 - 274 603 389 536 502 708 617 675 - 361 051], ecPnt[112 719 119 487 721 161 889 159 - 211 082 551 290 789 635 633 197 - 790 401 234 517 080 402 764 506 - 322 042, 59 038 507 861 533 321 775 922 - 462 484 860 668 668 411 724 675 - 754 721 170 660 930 498 202 940 - 497 565], ecPnt[66 576 517 566 997 309 876 776 - 372 876 836 199 019 185 475 935 - 761 406 744 525 505 228 996 757 - 486 023, 90 324 928 969 768 165 511 842 - 292 293 833 554 044 922 227 263 - 120 569 797 649 525 696 262 179 - 099 046]}
$c_0 := a_0 b_0$		P,V	50 802 272 133 873 189 188 778 463 - 155 973 251 716 683 768 205 680 - 082 583 600 857 092 767 270 065 867
$c_{0,W} := a_{0,W} b_{0,W}$		P,V	70 417 494 905 687 723 108 590 833 - 688 312 608 761 422 205 629 541 - 919 203 657 017 687 229 748 318 131
$P_{0,\{h,b,c,d,W\}} \overset{?}{=} P_{\{h,b,c,d,W\}} + \langle u_2^2, L_{2,\{h,b,c,d,W\}} \rangle + \langle u_2^{-2}, R_{2,\{h,b,c,d,W\}} \rangle$	Sanity Check for P_0	P,V	{True, True, True, True, True}

$P_{0,\{h,b,c,d\}} \stackrel{?}{=} G_0 a_0 + \{H,B,C,D\}_0 b_0 + c_0 g'$	Verifier's Check	P,V	{True, True, True, True}
$P_{0,W} \stackrel{?}{=} G_0 a_{0,W} + H_0 b_{0,W} + c_{0,W} g'$	Verifier's Check	P,V	True

Inner product protocol finished!

Total Communication Cost			
Type	**Count**	**Names**	**Bits**
group	34	V, W, AW, SW, AL, SL, SRh, SRb, SRc, SRd, T3, T5, T1W, T2W, Lh.2, Rh.2, Lb.2, Rb.2, Lc.2, Rc.2, Ld.2, Rd.2, LW.2, RW.2, Lh.1, Rh.1, Lb.1, Rb.1, Lc.1, Rc.1, Ld.1, Rd.1, LW.1, RW.1	8738
scalar	21	r, u, y, z, w, x, taux, muh, mub, muc, mud, t, tauxW, muW, tW, u.2, u.1, a0, b0, a0W, b0W	5376
total	55		14114

Creating proof finished.

Verification and Inspection

In[448]:=

```
If[fiatShamirSingleKernel,
Print["Can't react to results and requests without multi-kernel or multi-machine setup"];
(*Else*),
WaitForVariables[{
    "_verification_result_",
    "_inspection_request_",
    "_inspection_result_"
}];
];
```

Waiting to receive _verification_result_, _inspection_request_, _inspection_result_ ...

Received verification result from InteractiveVerifier@Alice-Shuffle-Ver: Verification succeeded!

Received inspection request from InteractiveVerifier@Alice-Shuffle-Ver. Revealing secrets of Pedersen commitments V, W, A_W, S_W, A_L, S_L, $S_{R,h}$, $S_{R,b}$, $S_{R,c}$, $S_{R,d}$, T_3, T_5, $T_{1,W}$ and $T_{2,W}$

Received inspection result from InteractiveVerifier@Alice-Shuffle-Ver: Inspection succeeded!

Message Processing: Event Loop

Not needed if notebook is executed correctly. Helpful for debugging and introducing new features. Wait for inspection requests and receive verification and inspection results after proof has been finished. Abort after all expected messages have been received.

In[ ]:=

```
StateMachineRestore["inner_product_halving"];
ProcessIncomingMessages[router, {""}];
```