IETF Hackathon

Vector Commitment based Proof of Transit

IETF 118

4–5 November 2023

Prague, Czech Republic

I E T F

Hackathon Plan

- We designed and implemented a new **Proof-of-Transit** mechanism
  - **What is Proof-of-Transit:** Proving that a packet has traversed a series of physical or virtual nodes, in a specific order.
  - **Drafts involved:** draft-ietf-sfc-proof-of-transit-08
  - **What we achieved:** Providing a working alternative, but more efficiency and security.

What got done

- **Result:** A working **Proof-of-Transit** solution
  - **New ideas:** It can help audit or monitor routing path.
  - **New code** **(demo inside):** https://github.com/liuchunchi/vcpot-demo
  - **New design:** Built on a newer cryptographic primitive:
    - **KZG polynomial commitment** (a construction to vector commitment)
    - As compared to: **Shamir Secret Sharing** in draft-ietf-sfc-proof-of-transit-08
  - **New results:**
    - **Constant size of transit proof** regardless of routing path length **(24Byte)**
    - **Constant computation time of transit proof** regardless of path length **(1-2ms)**

```
SecretG2-16:
1048486920382426285965681802283223492276724560235541777522005669888140500972024476401051566071576848180774859946645357354131477601829156156054098649123023520207189305993158483342848461876267848481414944240802752136407915380747
5
153733750944850015651842713674479091503727100247900273937331750705074000195494244719369981115284184686798249937160753209520931204688121374302489459471808475515456460745019691399218746870653614662965785200492801517070912257897173385:
[0] Commit polynomial:
1441759610491945124272239752568081377508521942300789486924845445601115222515941848720651081622782636507193633236685384549958568495971260221693542065215337375149433141273485282402470757808281162687156387501694526325534462368515386 8
Setup time cost: 13 ms
Press Enter key to send packets...

Input the real route, e.g., ABCDEFGH: ABCDEFGH
Route: A->B...
Route: B->C...
Route: C->D...
Route: D->E...
Route: E->F...
Route: F->G...
Route: G->H...
Route: H->0...
Demo ends.
Press Enter key to restart this demo...
```

```
[IO-1]
[A] Private data: 1700671788
[A] Parameters received
[A] Generating my proof:
x=1700671788, y=1
proof:
2092280479029362105957565207789329955582167955896253115384623978137706110621539464248826715974944886509193667652361
2984331763375967725888381148364955488794532382523641531496031450175275081235704395213195364857595442696746255939941
[A] Prove time cost: 0.85 ms
[A] Self-verifying A's proof with y=1
[A] Verification result: true
[A] Verification time cost: 1.76 ms
```

```
[IO-2]
[B] Private data: 1575241417
[B] Parameters received
[B] Received and verifying A's proof:
x=1700671788, y=1
proof:
2092280479029362105957565207789329955582167955896253115384623978137706110621539464248826715974944886509193667652361
2984331763375967725888381148364955488794532382523641531496031450175275081235704395213195364857595442696746255939941
[B] Verification result: true
[B] Verification time cost: 1.97 ms
[B] Generating my proof:
x=1575241417, y=2
proof:
2724605663441518536533948589163279403364228774584166217026735197430794847511219247138415747977618361783849358483711583039518195663091078369439729983347530352028859630031975245980028937288694920585615469789867688264254796004896 9
[B] Prove time cost: 0.70 ms
[B] Self-verifying B's proof with y=2
[B] Verification result: true
[B] Verification time cost: 1.76 ms
```

```
[IO-3]
[C] Private data: 863100565
[C] Parameters received
[C] Received and verifying B's proof:
x=1575241417, y=2
proof:
2724605663441518536533948589163279403364228774584166217026735197430794847511219247138415747977618361783849358484371158303951819566309107836943972998334753035202885963003197524598002893728869492058561546978986768826425479604896 9
[C] Verification result: true
[C] Verification time cost: 1.93 ms
[C] Generating my proof:
x=863100565, y=3
proof:
6997215189839018938657732077570719496442187389787692113234183663554412595646348926359906532164345311584299500677829427950373460721271122303372268116289449367627277589115597642492252192359785665461822663861455772773433059120715313
[C] Prove time cost: 0.68 ms
[C] Self-verifying C's proof with y=3
[C] Verification result: true
[C] Verification time cost: 1.75 ms
```

```
[IO-4]
[D] Private data: 119419682
[D] Parameters received
[D] Received and verifying C's proof:
x=863100565, y=3
proof:
6997215189839018938657732077570719496442187389787692113234183663554412595646348926359906532164345311584299500677829427950373460721271122303372268116289449367627277589115597642492252192359785665461822663861455772773433059120715313 1
[D] Verification result: true
[D] Verification time cost: 2.06 ms
[D] Generating my proof:
x=119419682, y=4
proof:
8187797797174210641651610458165025047727083259926870261752194252117150447524773162566788126783237698838251595773 4
7120663127773450142233767817651676393679658093857408057910009477303398552291626817818169944780667726676498199156 5
[D] Verification result: true
[D] Verification time cost: 1.75 ms
[D] Generating my proof:
x=119419682, y=4
proof:
8187797797174210641651610458165025047727083259926870261752194252117150447524773162566788126783237698838251595773 4
7120663127773450142233767817651676393679658093857408057910009477303398552291626817818169944780667726676498199156 5
[D] Prove time cost: 0.70 ms
[D] Self-verifying D's proof with y=4
[D] Verification result: true
[D] Verification time cost: 1.75 ms
```

```
[E] Private data: 905055653
[E] Parameters received
[E] Received and verifying D's proof:
x=119419682, y=4
proof:
8187797797174210641651610458165025047727083259926870261752194252117150447524773162566788126783237698838251595773 4
7120663127773450142233767817651676393679658093857408057910009477303398552291626817818169944780667726676498199156 5
[E] Verification result: true
[E] Verification time cost: 1.98 ms
[E] Generating my proof:
x=905055653, y=5
proof:
1052040618334597843417678343649388164663213066803084155386920612513751150212238166988323138117273424978563316886555 5
3918129096718325469148587886315464931800350699102020364268488520717599828527741132319683736387245367705415226321315
[E] Prove time cost: 0.68 ms
[E] Self-verifying E's proof with y=5
[E] Verification result: true
[E] Verification time cost: 1.76 ms
```

```
[IO-6]
[F] Private data: 396758031
[F] Parameters received
[F] Received and verifying E's proof:
x=905055653, y=5
proof:
1052040618334597843417678343649388164663213066803084155386920612513751150212238166988323138117273424978563316886555 3918129096718325469148587886315464931800350699102020364268488520717599828527741132319683736387245367705415226321315
[F] Verification result: true
[F] Verification time cost: 2.05 ms
[F] Generating my proof:
x=396758031, y=6
proof:
1328106035231795533819748779164933226926407480288036115195485520034630463059602889915715348179821236871192622674179 3384699365796471485062620774393197424264918488497608951397412198123050345870078880429923367033417830646641471899383 8
[F] Prove time cost: 0.68 ms
[F] Self-verifying F's proof with y=6
[F] Verification result: true
[F] Verification time cost: 1.75 ms
```

```
[G] Parameters received
[G] Received and verifying F's proof:
x=396758031, y=6
proof:
1328106035231795533819748779164933226926407480288036115195485520034630463059602889915715348179821236871192622674179 3384699365796471485062620774393197424264918488497608951397412198123050345870078880429923367033417830646641471899383 8
[G] Verification result: true
[G] Verification time cost: 2.07 ms
[G] Generating my proof:
x=1936688334, y=7
proof:
6922561587515006985870769004284574260178837206252935754463374985462588894980867176982128608550404379396158061636 1 8
1036619846060153690944984954778523852892800612833241362651335437147439664878729037613370520147700789022849522044827
[G] Prove time cost: 0.69 ms
[G] Self-verifying G's proof with y=7
[G] Verification result: true
[G] Verification time cost: 1.76 ms
```

```
[H] Parameters received
[H] Received and verifying G's proof:
x=1936688334, y=7
proof:
6922561587515006985870769004284574260178837206252935754463374985462588894980867176982128608550404379396158061636 1 8
1036619846060153690944984954778523852892800612833241362651335437147439664878729037613370520147700789022849522044827
[H] Verification result: true
[H] Verification time cost: 1.95 ms
[H] Generating my proof:
x=446694435, y=8
proof:
3601727386293008956210178662145463960273194641158477679605685770763502349369641213569157539449526646161974115858515 15659112994805274339075437156658812877229859605710295819634369368134691751932052234299815896198162755165832722625118
[H] Prove time cost: 0.69 ms
[H] Self-verifying H's proof with y=8
[H] Verification result: true
[H] Verification time cost: 1.75 ms
```

tmux ⌥⌘2

```
2856819405009716689926244749332931795046842719860443755223376719591522784091660604234690835798379024733720161116525
8725807410643899929289599775530091563027341271396230011821973141982035996003579395723710474258074267746749652340952
6220077728943544278580656961097642058207149266409468653790885771926387774889516849371280797432380733645070368247100
:
SecretG2-16:
1048486920382426285965681802283223492276724560235541777522005669888140500972024476401051566071576848180774485599466
4535735413147760182915615605409864691230235202071893059693158483342848461876267848481414944244002752136407915380747
5
1537337509448500156518427136744790915023721002479002739373317507050740001954944247193699811152841846867982499371607
5320952003120468812137430248945947180847551545646074501969139921874687065361466296578520049280151707091225789717338
5:
[0] Commit polynomial:
9352694998533749161721124393803323045287895655807938584345637446042263222005420624179987775934427249822429776635947
7798646254286527659536013722238834825741200246604475917345200966150600311523101605226959724513891645569968741413341
Setup time cost: 18 ms
Press Enter key to send packets...

Input the real route, e.g., ABCD: ABDC
Route: A->B...
Route: B->D...
Route: D->C...
Route: C->0...
Demo ends.
Press Enter key to restart this demo...
```

```
[A] Private data: 1566549852
[A] Parameters received
[A] Generating my proof:
x=1566549852, y=1
proof:
1615878992070453542821963050455080669543601051719357871359490956434035668368127513238275197153397571612694990176499
3256448342033330894472059817237381721843775597527787963185938097840645087502040313393310509978906032284997021691142
[A] Prove time cost: 0.55 ms
[A] Self-verifying A's proof with y=1
[A] Verification result: true
[A] Verification time cost: 1.76 ms
```

```
[B] Private data: 421893086
[B] Parameters received
[B] Received and verifying A's proof:
x=1566549852, y=1
proof:
1615878992070453542821963050455080669543601051719357871359490956434035668368127513238275197153397571612694990176499
3256448342033330894472059817237381721843775597527787963185938097840645087502040313393310509978906032284997021691142
[B] Verification result: true
[B] Verification time cost: 2.00 ms
[B] Generating my proof:
x=421893086, y=2
proof:
1858794913012773327122825141946275138921201803579776478914139892331968851757717617032732660161084162036765729195684
2464458879949608966368219095247634333521198064936046669919272075509318091205977085358312317492574901155831791032095
[B] Prove time cost: 0.44 ms
[B] Self-verifying B's proof with y=2
[B] Verification result: true
[B] Verification time cost: 1.76 ms
```

```
[C] Private data: 480118022
[C] Parameters received
[C] Received and verifying D's proof:
x=694547063, y=3
proof:
1798790386980613704835371091361098443535807515828614467589868047020495986265361616753935356186287446014696307231583436377712436267535046667515098283096469893533976059055208733624966222590827940011060043565602573816856396040969
[C] Verification result: false
[C] Verification time cost: 1.97 ms
[C] Generating my proof:
x=480118022, y=4
proof:
1128390207434578257822362465720109462058584521416739020608577576382145255662983422336673316790349293194983574998130697052784368934761472157610434146750671547908477883732118661368938561152837318439998175009879848044338832366573565
[C] Prove time cost: 0.45 ms
[C] Self-verifying C's proof with y=4
[C] Verification result: false
[C] Verification time cost: 1.76 ms
```

```
[D] Private data: 694547063
[D] Parameters received
[D] Received and verifying B's proof:
x=421893086, y=2
proof:
1858794913012773327122825141946275138921201803579776478914139892331968851757717617032732660161084162036765729195684
2464458879949608966368219095247634333521198064936046669919272075509318091205977085358312317492574901155831791032095
[D] Verification result: true
[D] Verification time cost: 1.96 ms
[D] Generating my proof:
x=694547063, y=3
proof:
1798790386980613704835371091361098443535807515828614467589868047020495986265361616753935356186287446014696307231583436377712436267535046667515098283096469893533976059055208733624966222590827940011060043565602573816856396040969
[D] Prove time cost: 0.44 ms
[D] Self-verifying D's proof with y=3
[D] Verification result: false
[D] Verification time cost: 1.75 ms
```

What we learned

- **Vector Commitment** is a interesting primitive to commit a routing path and verify actual execution result afterwards.
- **To OPSEC WG:**
  - Proof of Non Transit is hard, and we cannot do that.
  - **We re-distilled better use cases to be presented in SECDISPATCH**
- **To the concluded SFC WG:**
  - We developed a SFC proof of processing solution after you closed, sorry

Wrap Up

Team members:

Peter (Chunchi) Liu

First timers @ IETF/Hackathon:

Peter (Chunchi) Liu

Contacts:

liuchunchi@huawei.com