IN, LCA1: Decentralized Verifiable Computation on Distributed Ledger

Due on Spring 2017

D.Froelicher, J.Troncoso-Pastoriza

Max Premi

March 9, 2018

Algorithm 1 Non-Interactive Range Validation

```
 1: Common Input: $B$ the base point in the EC, $P$ the public key used to encode data, $u, l$ 2 integers and
    commitment $C$.
 2: Prover Input: $\sigma$ the secret integer mapped to a point and $r$ a scalar in the EC such that $C = \sigma \cdot B + Pr$,
    $\sigma \in [0, u^l)$
 3:
 4: Initialization Phase: Each server $i$ in the collective authority computes the following values :
 5: Pick a random $x_i \in \mathbb{Z}_p$
 6: $y_i \leftarrow Bx_i$
 7: $A_{i,j} \leftarrow B(x_i + j)^{-1}$, $\forall j \in \mathbb{Z}_u$ and $i \in \{1, ..., m\}$
 8:
 9: Servers make their signature public as well as the public key $y_i$. When a query is issued by a querier
    $Q$, we now assume that rang is defined in the query and broadcasted by the server, as usual, to the data
    provider. All computations following up to line 22 are done by the DPs.
10:
11: Online Phase: Data provider encodes the signature of the value to check in base $u$ with randomly
    picked $v_j$.
12:
13: Computes value $c = H(B, C, \sum_i y_i)$, where $H()$ is a cryptographic hash function.
14: for $\forall j \in \mathbb{Z}_l$ such that $\sigma = \sum_j \sigma_j u^j$ do
15:     Picks 3 values $s_j, t_j, m_j \in \mathbb{Z}_p$
16:     for $i \in \{0, ...m\}$ (number of servers) do
17:         Picks $v_j \in \mathbb{Z}_p$ and compute $V_{i,j} = A_{i,\sigma_j} v_j$
18:         $a_{i,j} \leftarrow e(V_{i,j}, B)(-s_j) + e(B, B)(t_j)$
19:         $Z_{v_j} \leftarrow t_j - v_j c$
20:     Computes $D = D + B(u^j s_j + Pm_j)$
21:     $Z_{\sigma_j} \leftarrow s_j - \sigma_j c$
22: Finally, computes $m = \sum m_j$ and $Z_r = m - rc$, the final value is $D \leftarrow \sum_j B(u^j s_j + Pm_j)$
23:
24: The DP sends to each server $S_i$ : $D, Z_r, c, C$ and list of values $a_i, Z_v, Z_\sigma$
25: $S_i$ checks that $D = Cc + PZ_r + \sum_j B(u^j Z_{\sigma_j})$ and $a_{i,j} = e(V_{i,j}, y_i)c + e(V_{i,j}, B)(-Z_{\sigma_j}) + e(B, B)(Z_{v_j})$,
    $\forall j \in \mathbb{Z}_l$ , and publish the result.
26:
```