

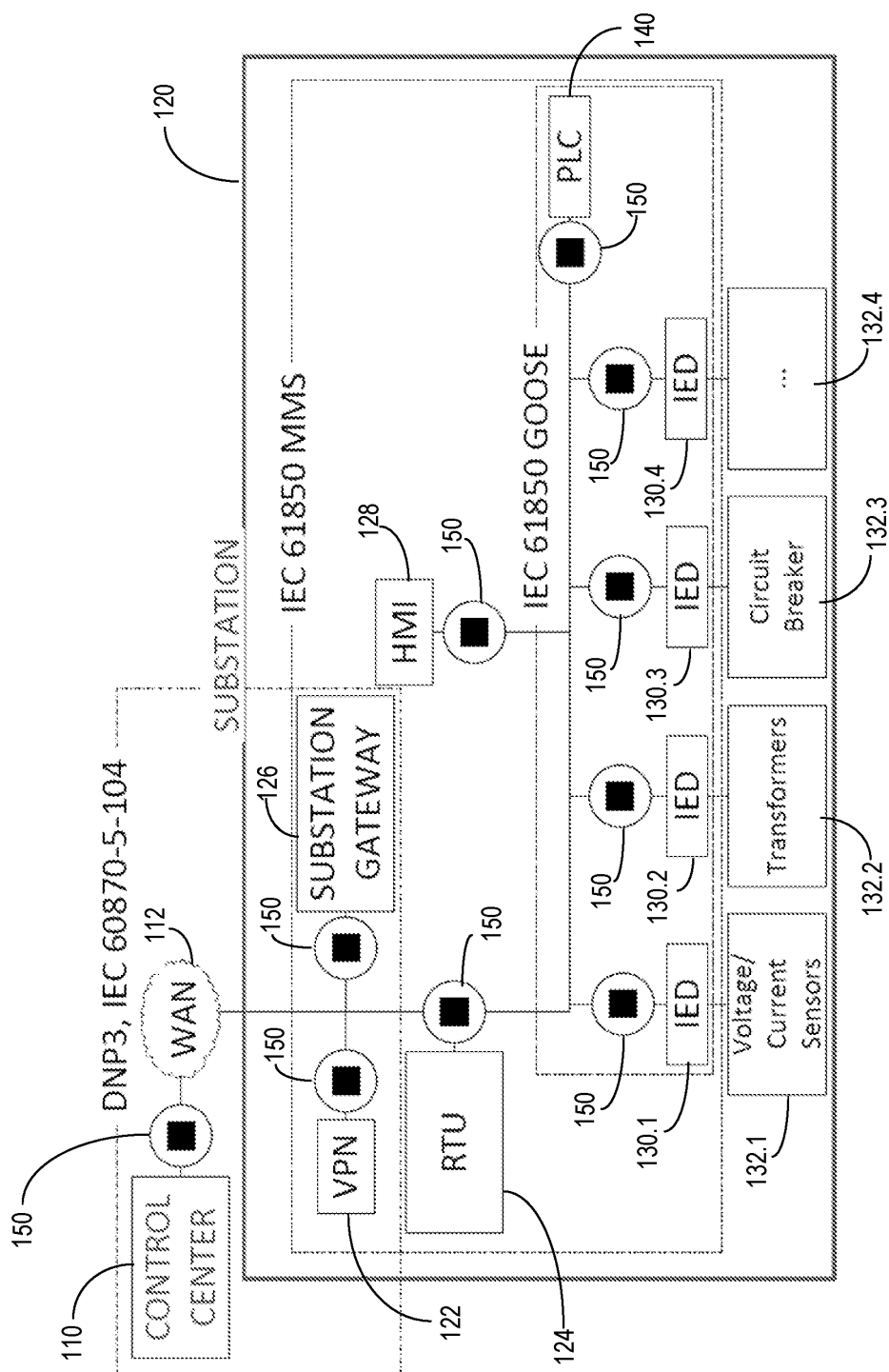


Figure 1

2/9

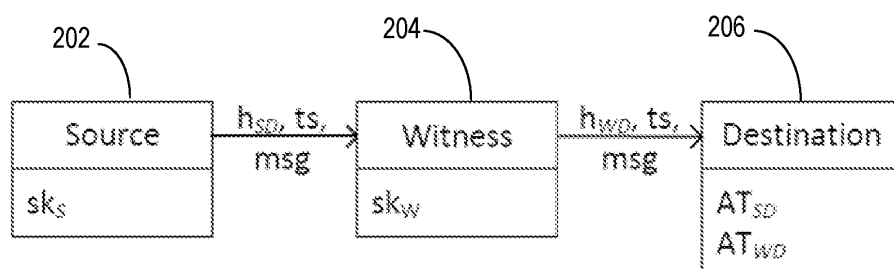


Figure 2A

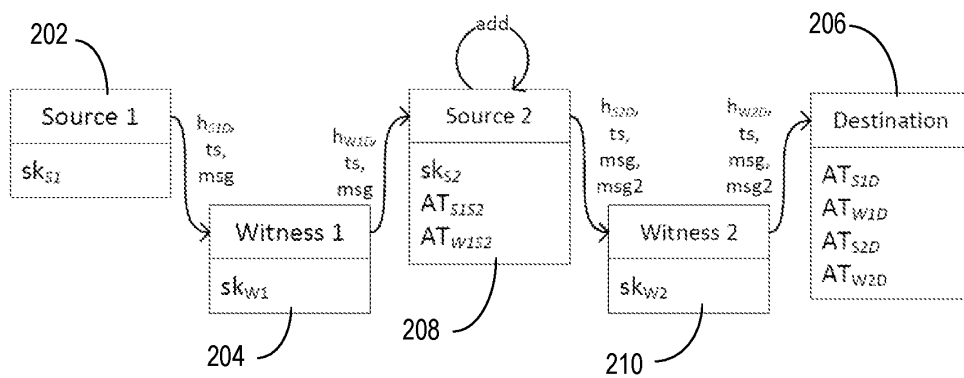


Figure 2B

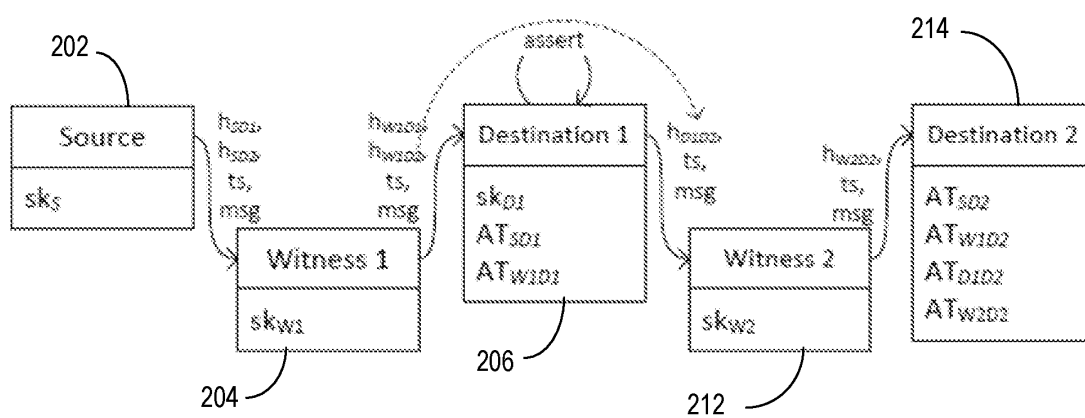


Figure 2C

Algorithm IV.1: Provenance Verification

Data: h , ts , $messages$, $numberOfNodesOnThePath$
Result: accept/reject

```

1  $h'_0 = \text{hash}(AT_{source}, ts, messages[0])$ 
2  $c = 1$ 
3  $sourceCounter = 0$ 
4 while  $c++ \leq numberOfNodesOnThePath$  do
5     if  $Witness_c$  is another source then
6          $sourceCounter++$ 
7          $h'_c = \text{hash}(h'_{c-1}, AT_c, ts, messages[0 : sourceCounter])$ 
8 if  $h'_c = h$  then
9     accept
10 else
11     reject

```

Figure 3

Notation	Description
sk_i	A secret key that belongs to a node i , $i \in \{0, 1, \dots, n\}$ where $i = 0$ refers to the source and n is the destination.
$\mathcal{K}$	The security parameter
AT	The authentication token. It is subscripted to denote its "from" and "to" (s.a., AT_{SD} to denote it is the authentication token that servers between the source, S , and the destination D).
h	The Cryptographic evidence every node prepares when they initiate, witness or extend a message. h_i is the cryptographic evidence for the i^{th} node on the path of the message. To denote a cryptographic evidence's "from" and "to", we use the same notation with AT , where h_{SD} means the cryptographic evidence from S to D .
S, W, D	The source, witness and destination node IDs, respectively.
ts, msg	A timestamp, a message.
MSG	A set of messages. When a message is initiate by a source, if it is extended by any downstream node, the new message is added to this set.
$\mathcal{A}$	The blackbox PPT adversary.
$\mathcal{HC}$	The hash challenger.
$\mathcal{C}$	The challenger in the proof that plays the role of the destination node and the honest nodes. It uses the output of $\mathcal{A}$ to win against $\mathcal{HC}$, which means to break the security assumption.
$\mathcal{B}$	$\mathcal{B}$ plays the role of $\mathcal{C}$ against $\mathcal{A}$ and acts as the adversary to $\mathcal{HC}$.
$\mathcal{HN}, \mathcal{MN}$	The sets of honest nodes and the malicious nodes

Figure 4

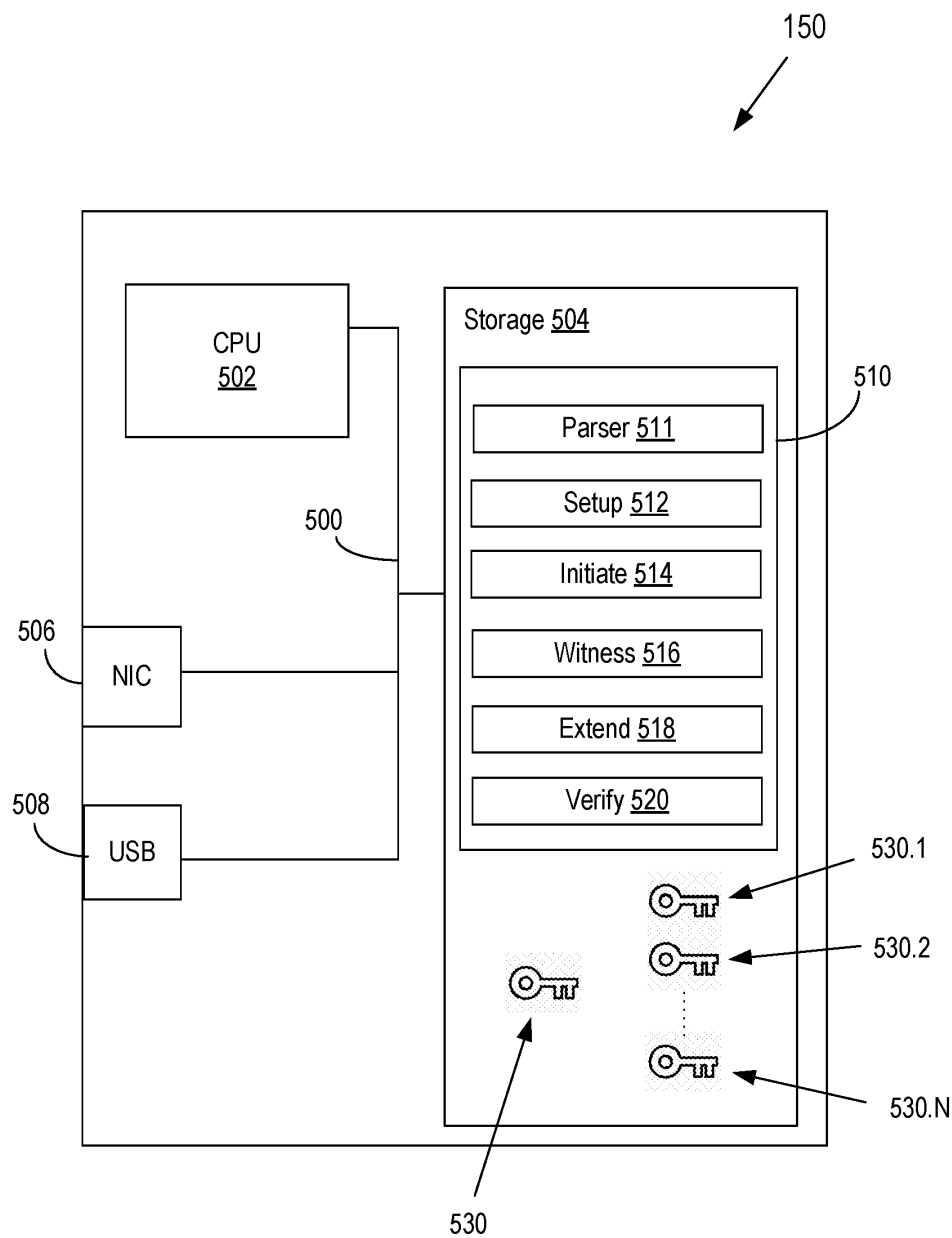


Figure 5

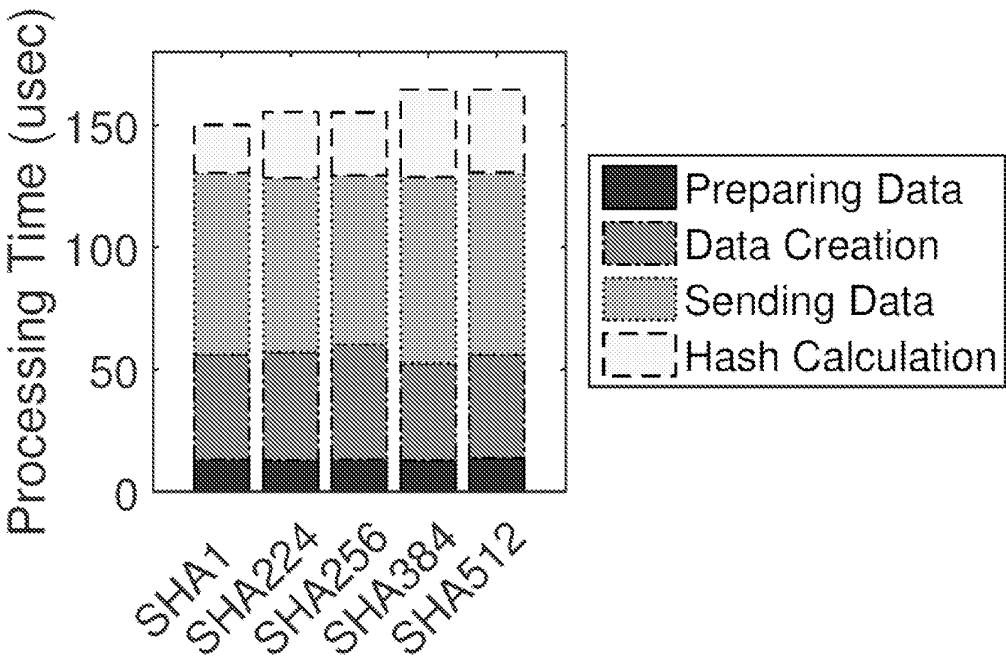


Figure 6A

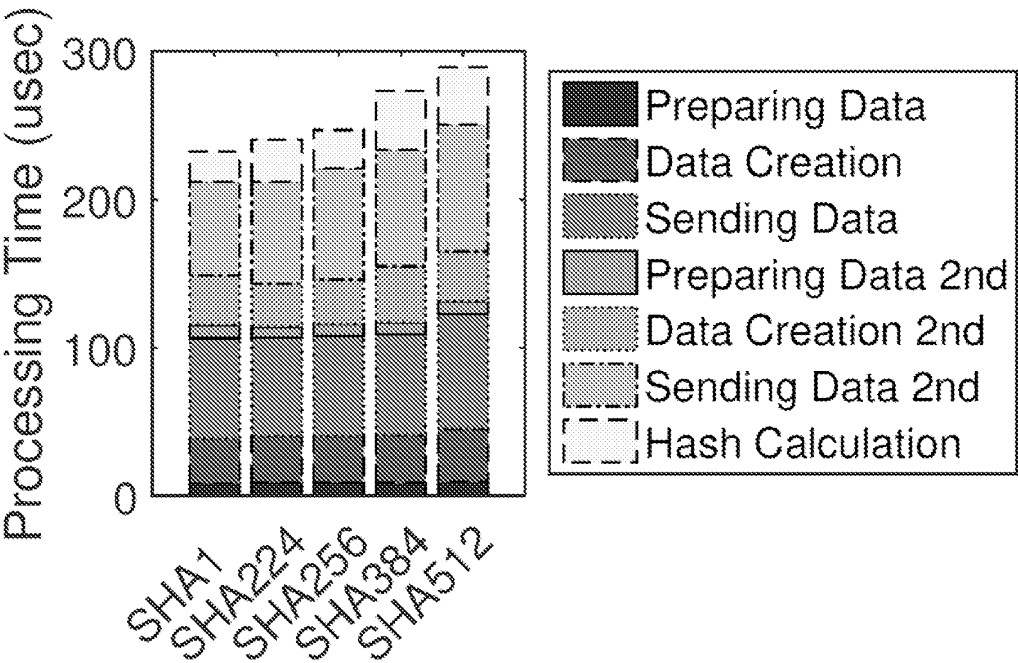


Figure 6B

7/9

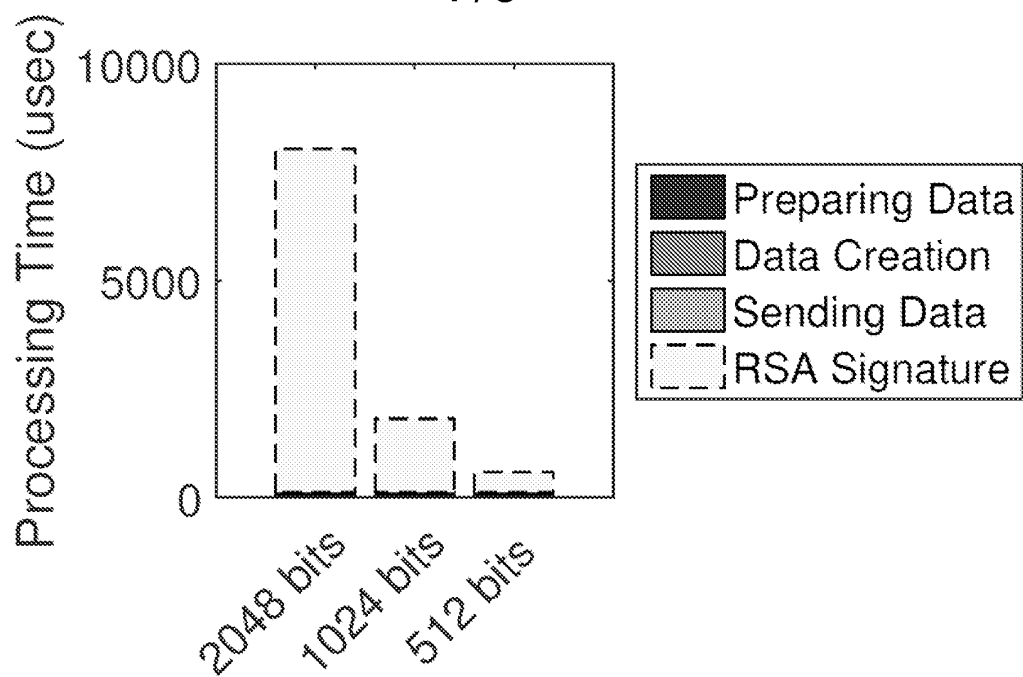


Figure 6C

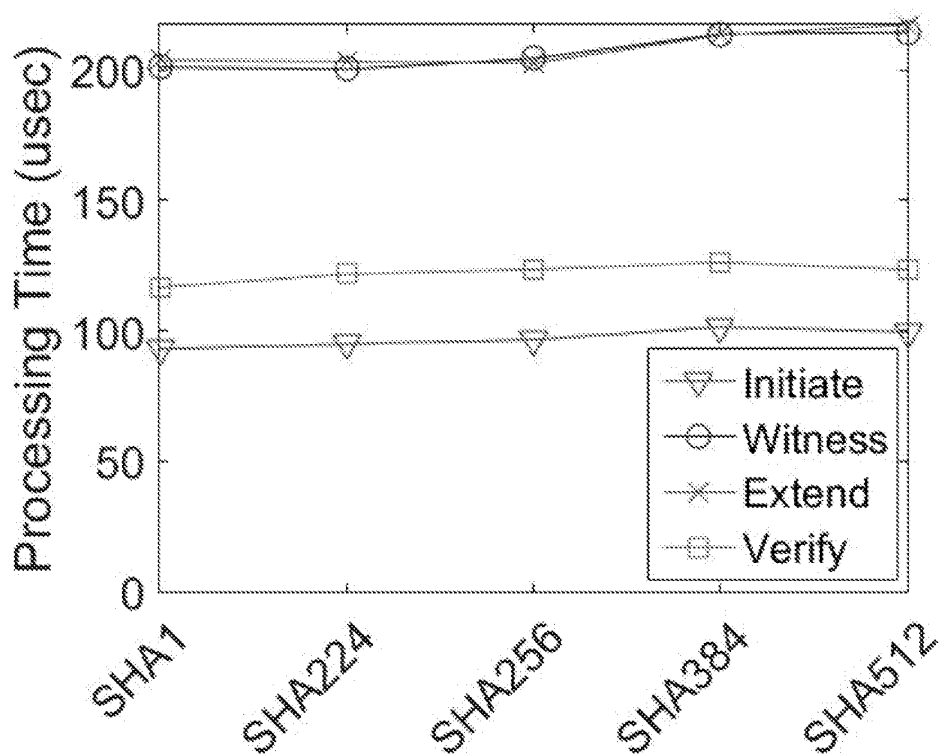


Figure 6D

8/9

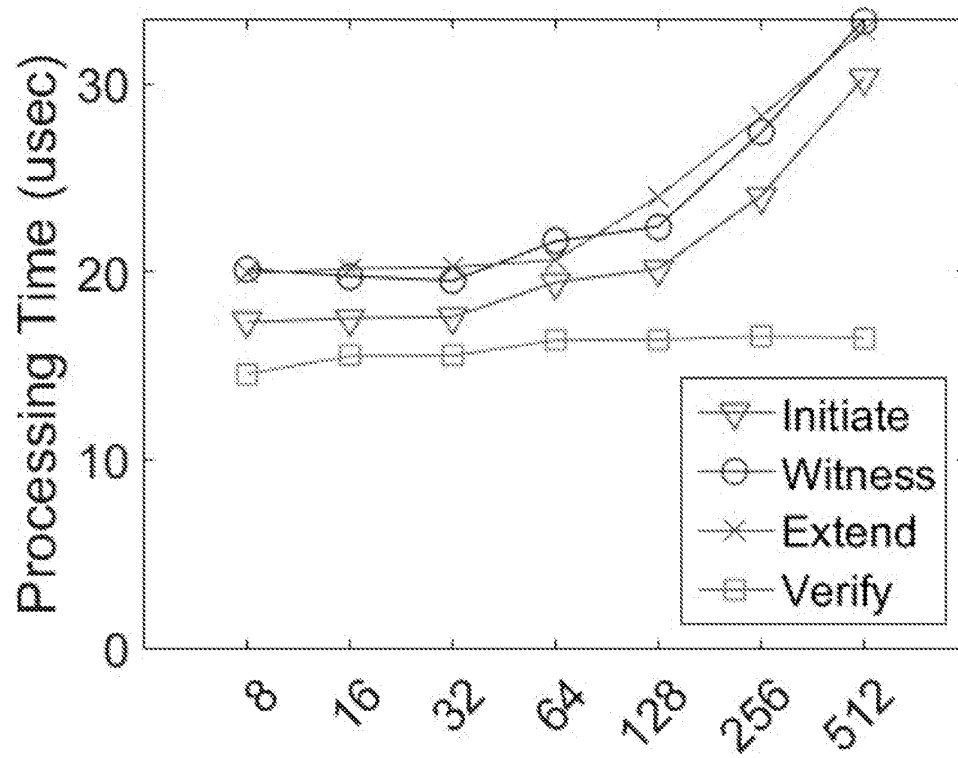


Figure 6E

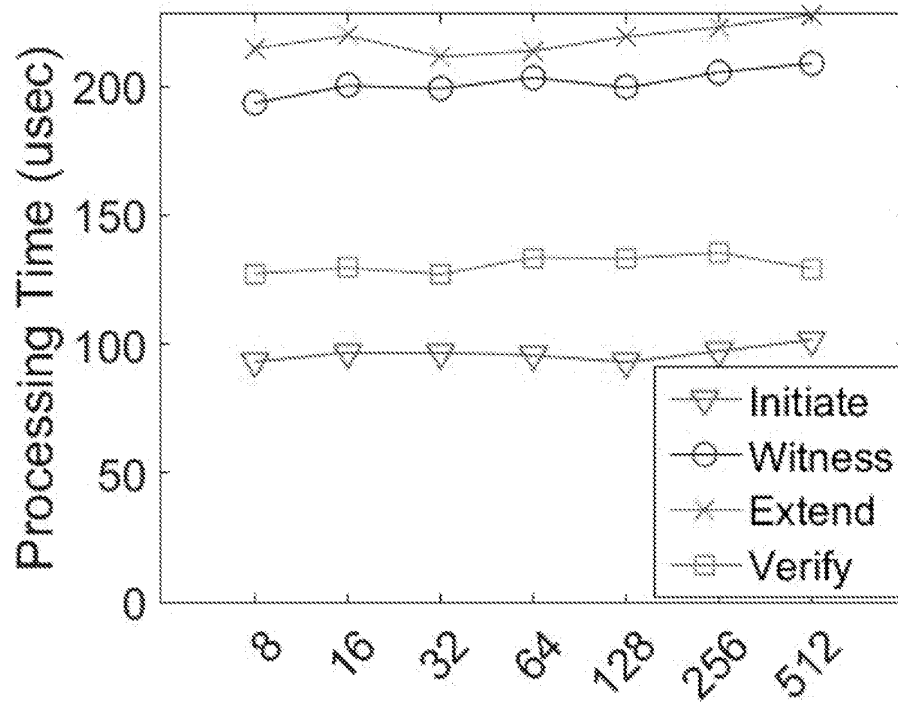


Figure 6F

9/9

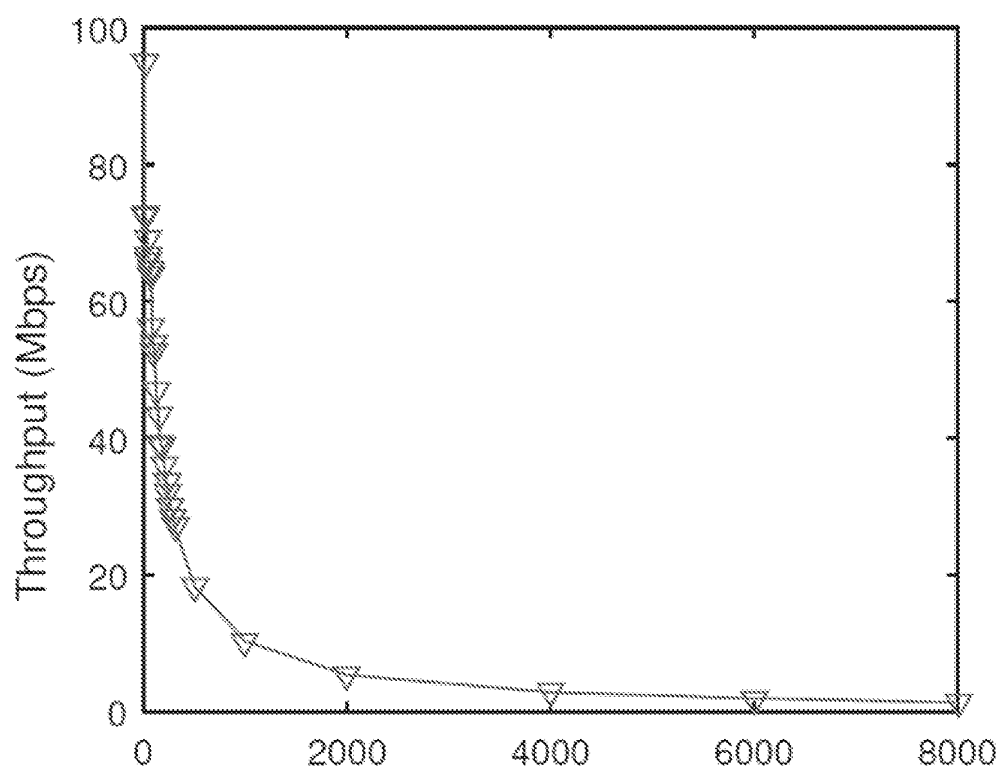


Figure 6G