Figure 1

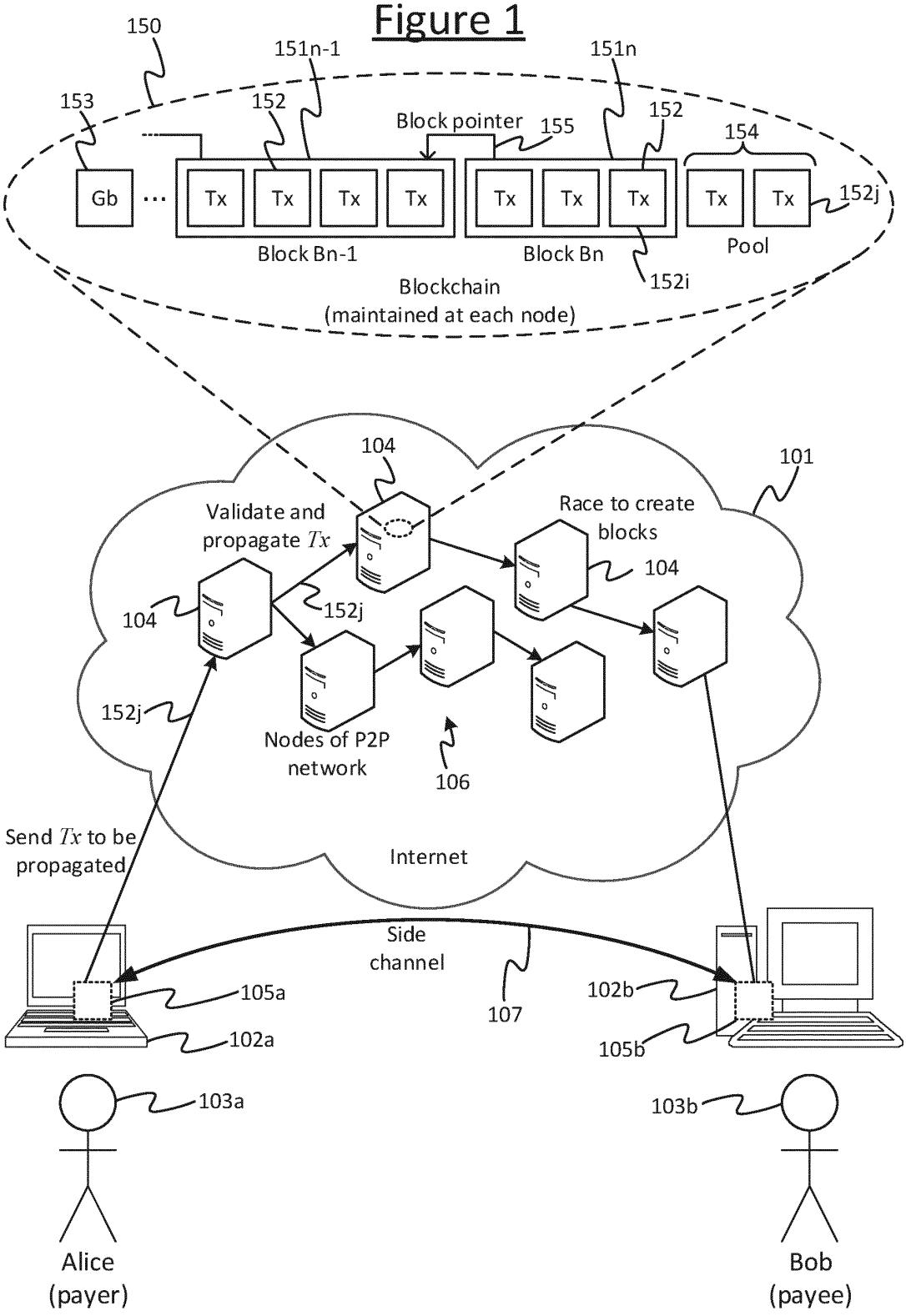
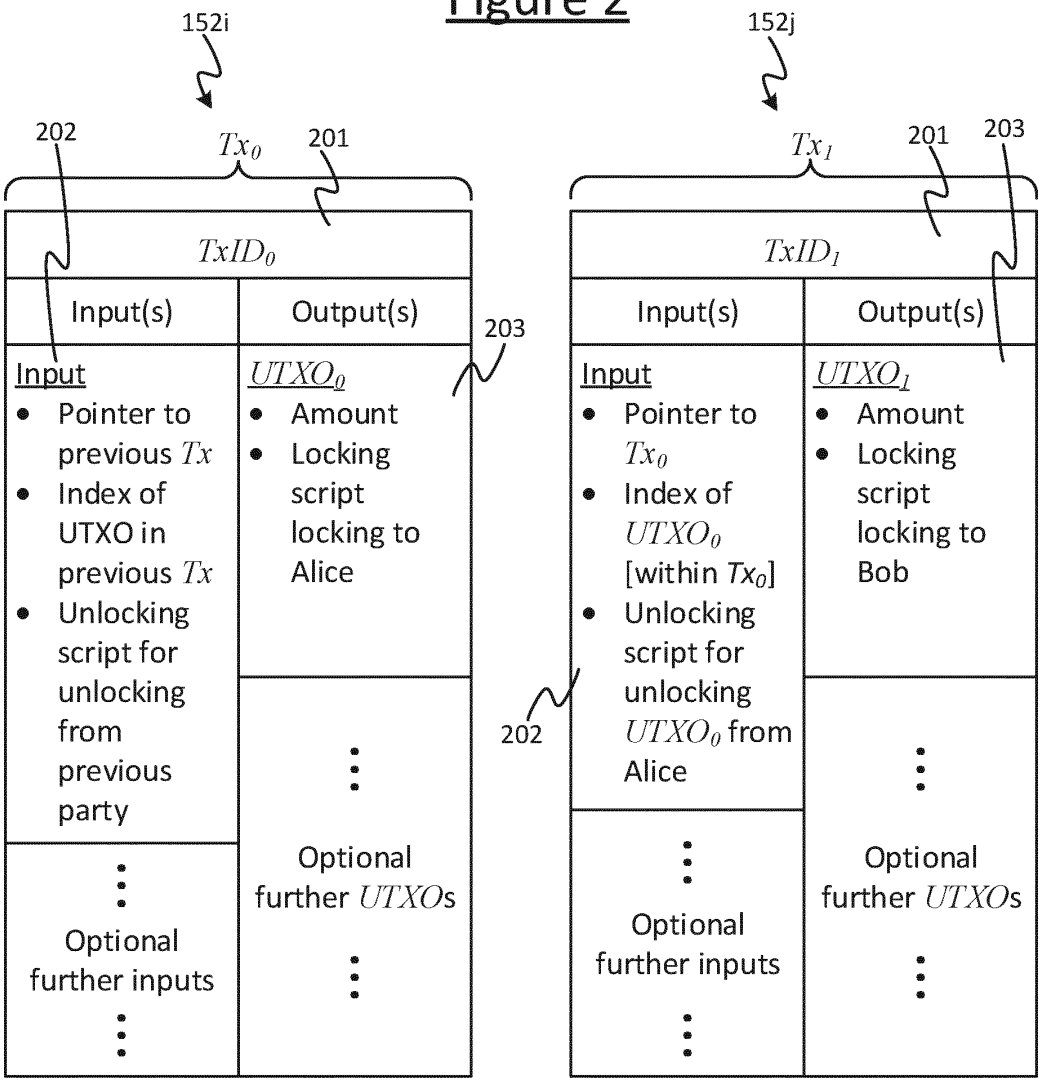

150
151n-1
151n
153
152
Block pointer
155
152
154
Gb
Tx
Tx
Tx
Tx
Tx
Tx
Tx
Tx
Tx
152j
Block Bn-1
Block Bn
Pool
152i
Blockchain
(maintained at each node)
104
101
Validate and
propagate Tx
Race to create
blocks
104
104
152j
152j
Nodes of P2P
network
106
Send Tx to be
propagated
Internet
Side
channel
107
105a
102a
102b
105b
103a
103b
Alice
(payer)
Bob
(payee)

Figure 2



Transaction from Alice to Bob

Validated by running: Locking script from output 203 of Tx_0, together with Alice's unlocking script from input 202 of Tx_1. This checks that Alice's unlocking script in Tx_1 meets the condition(s) defined in the locking script of previous transaction Tx_0.

Figure 3

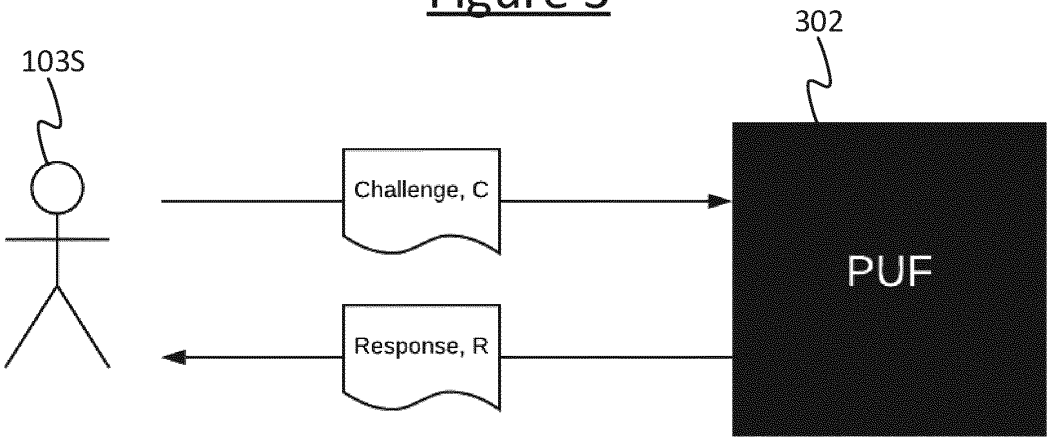


Figure 4

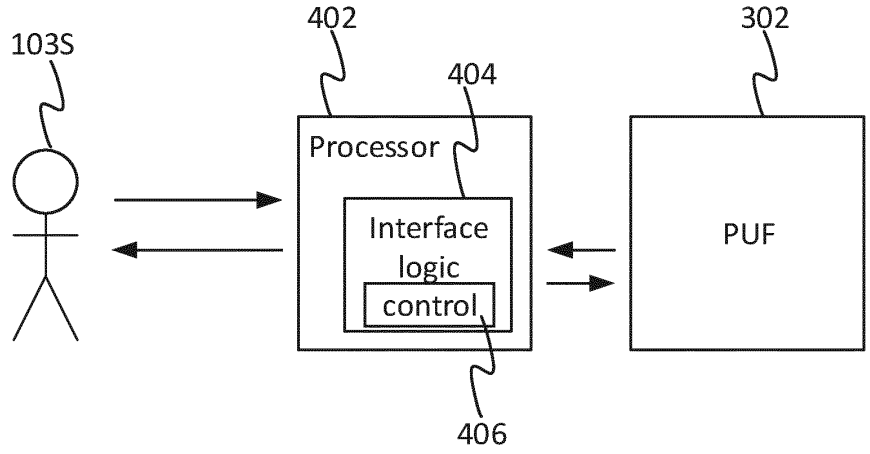


Figure 5A

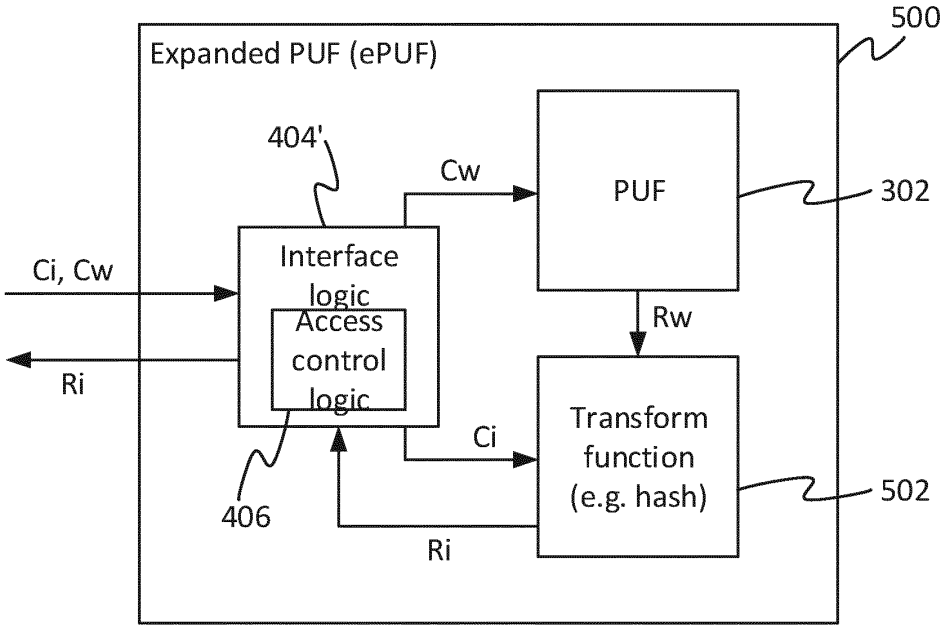


Figure 5B

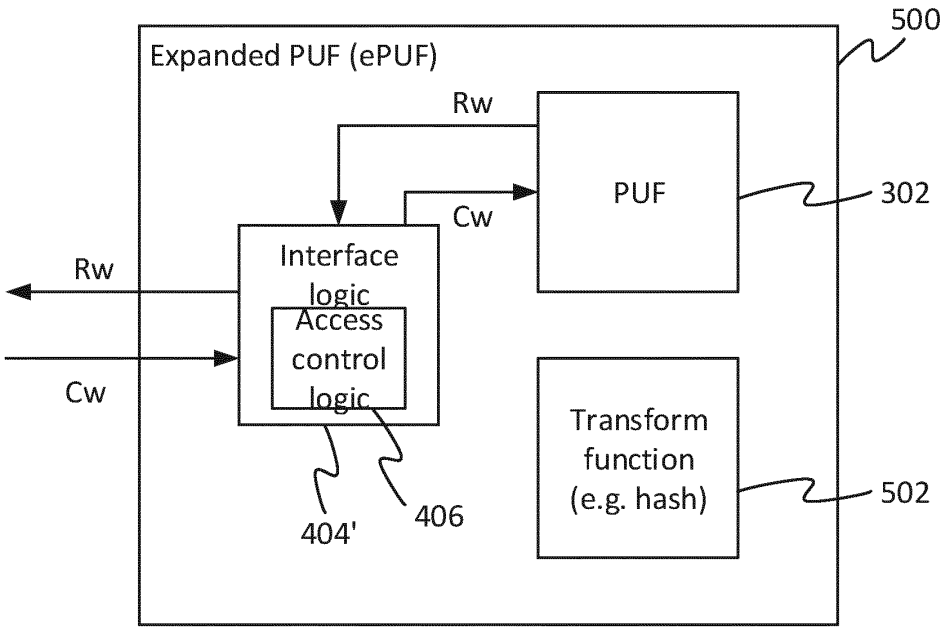


Figure 6

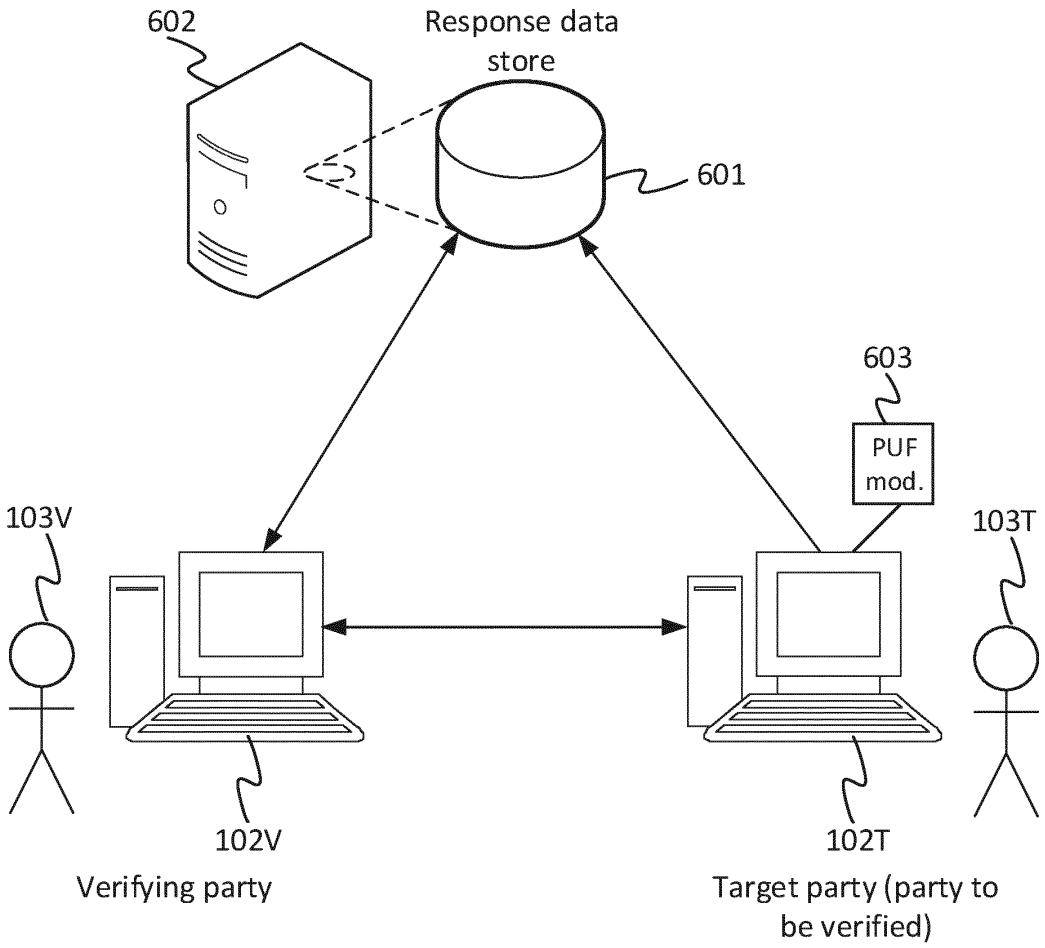

602
Response data store
601
603
PUF mod.
103V
103T
102V
102T
Verifying party
Target party (party to be verified)

Figure 7

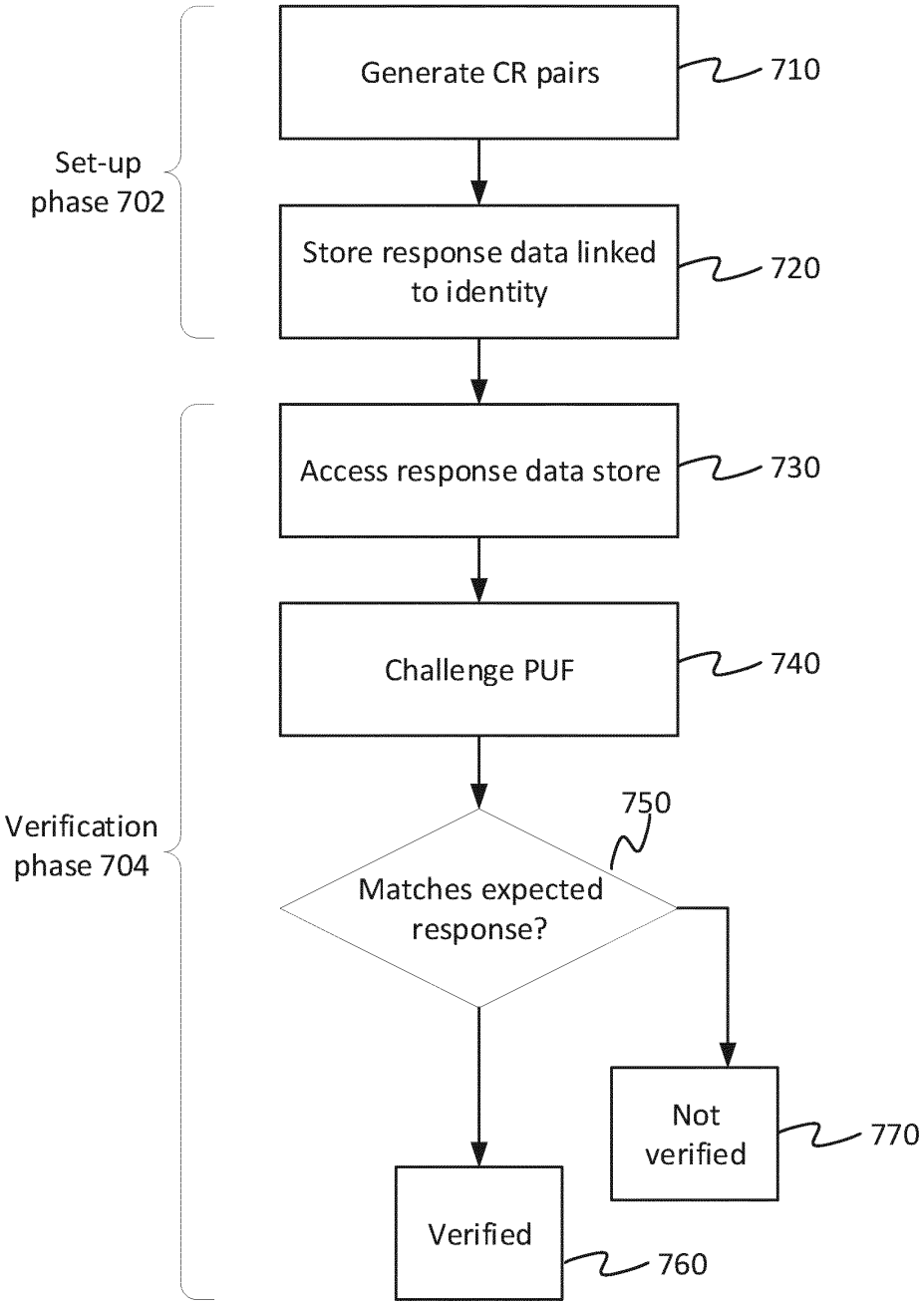

Set-up phase 702
Verification phase 704
Generate CR pairs
710
Store response data linked to identity
720
Access response data store
730
Challenge PUF
740
750
Matches expected response?
Not verified
770
Verified
760

Figure 8A

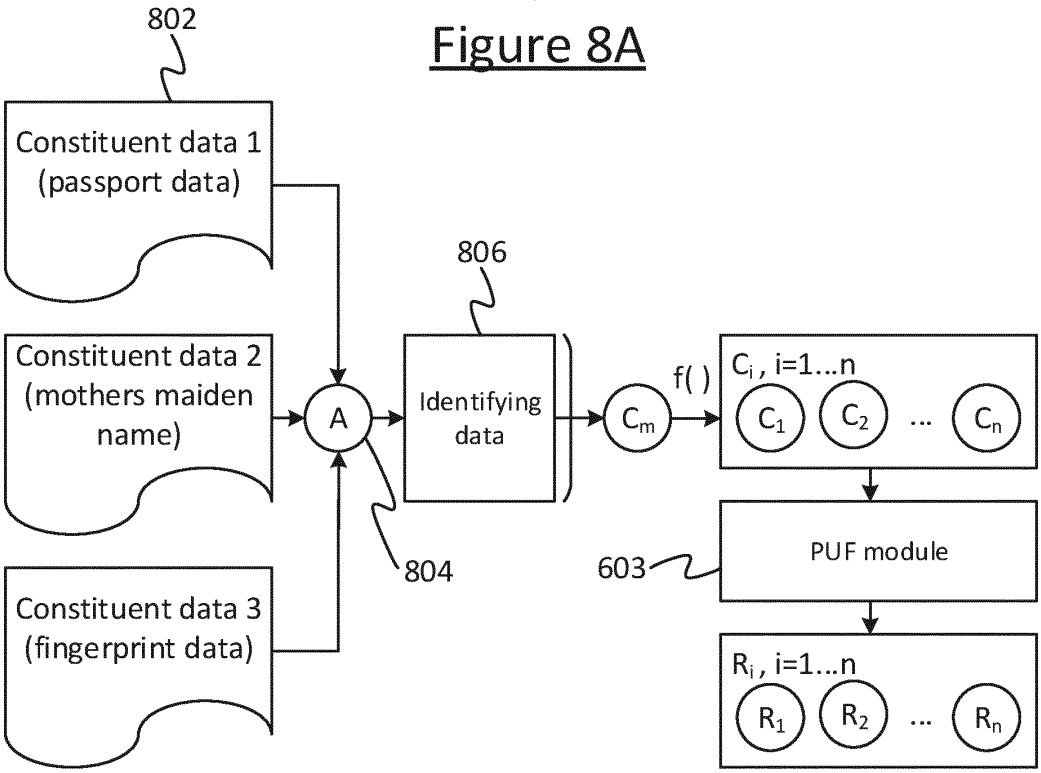


Figure 8B

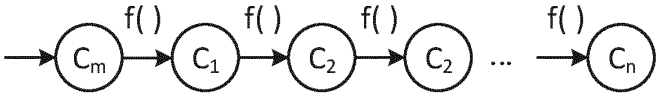


Figure 8C

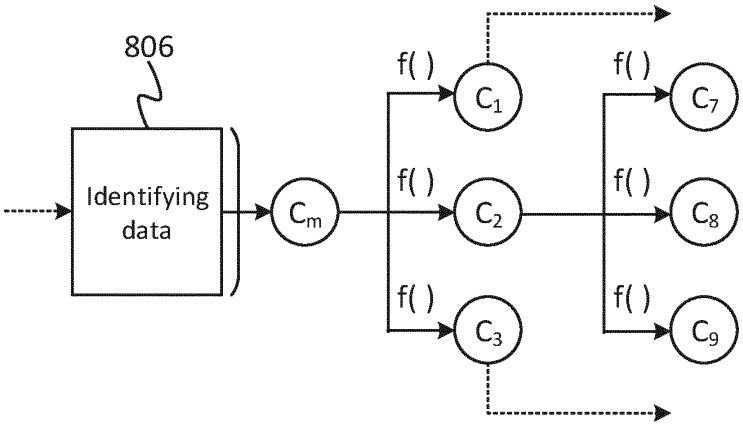


Figure 9

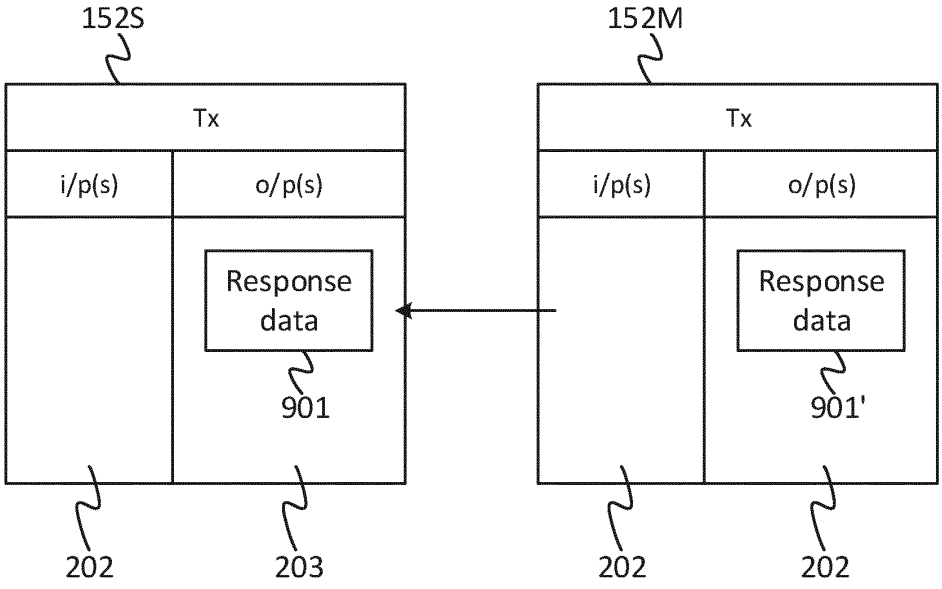
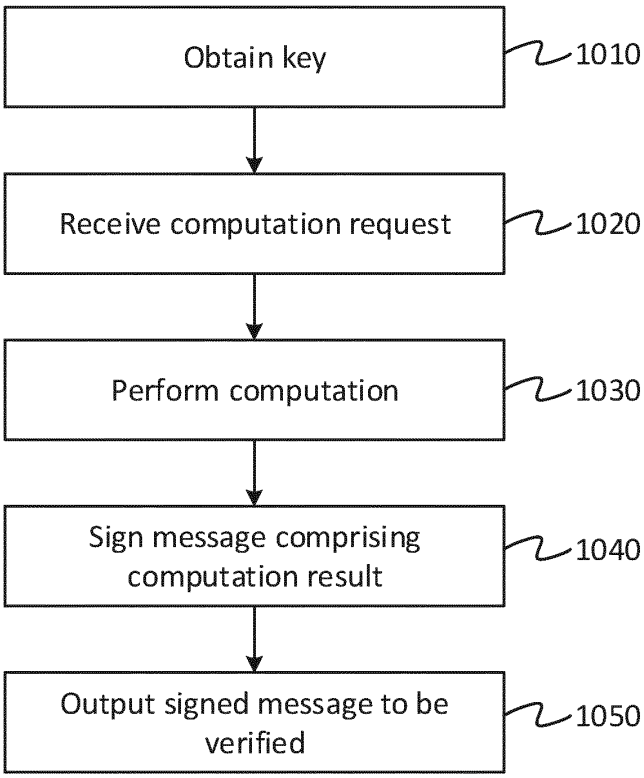

152S
152M
Tx
Tx
i/p(s)
o/p(s)
i/p(s)
o/p(s)
Response data
Response data
901
901'
202
203
202
202

FIGURE 10


Obtain key
1010
Receive computation request
1020
Perform computation
1030
Sign message comprising computation result
1040
Output signed message to be verified
1050