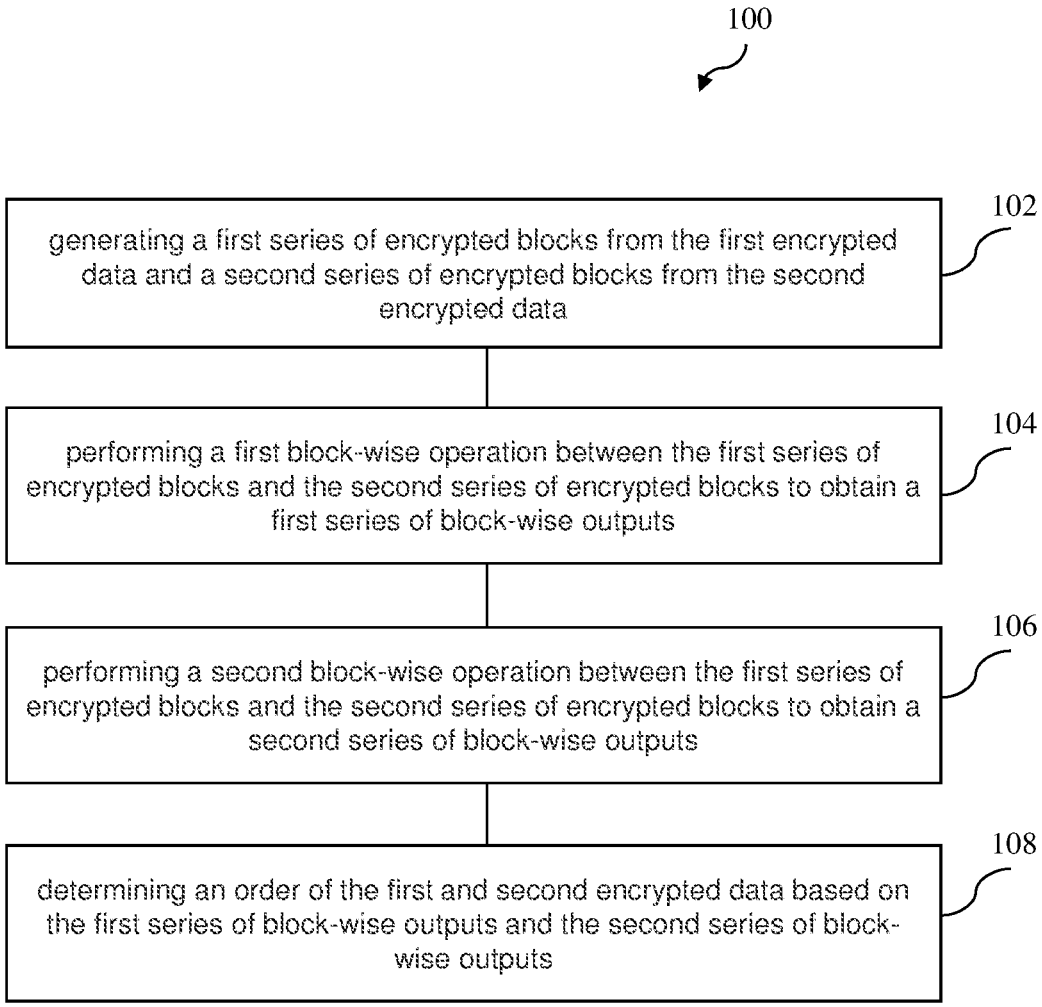

100
generating a first series of encrypted blocks from the first encrypted data and a second series of encrypted blocks from the second encrypted data
102
performing a first block-wise operation between the first series of encrypted blocks and the second series of encrypted blocks to obtain a first series of block-wise outputs
104
performing a second block-wise operation between the first series of encrypted blocks and the second series of encrypted blocks to obtain a second series of block-wise outputs
106
determining an order of the first and second encrypted data based on the first series of block-wise outputs and the second series of block-wise outputs
108

FIG. 1

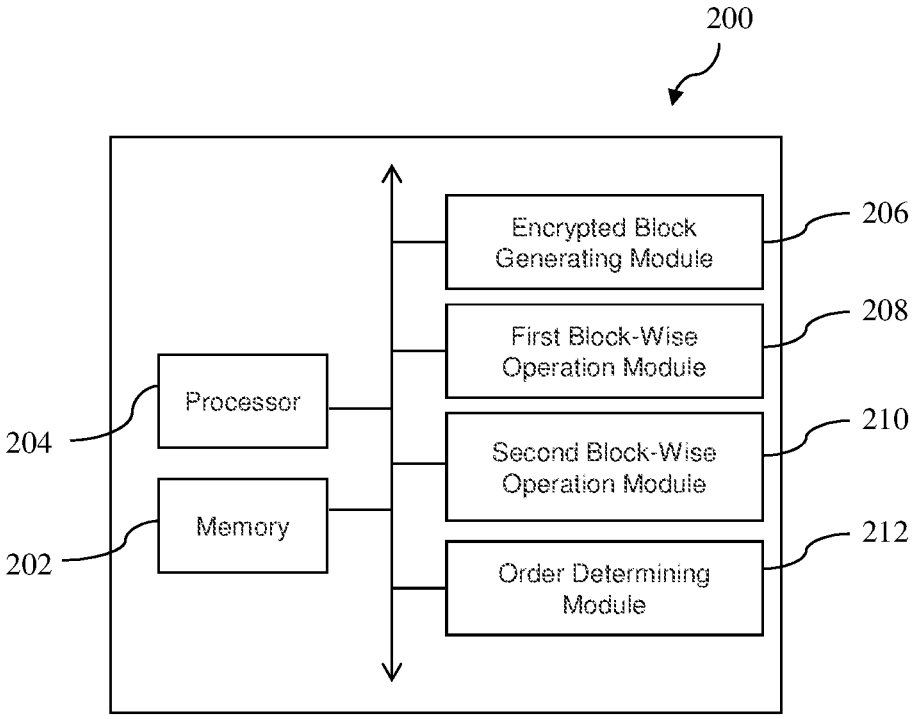

200
Encrypted Block Generating Module
206
First Block-Wise Operation Module
208
Second Block-Wise Operation Module
210
Order Determining Module
212
Processor
204
Memory
202

FIG. 2

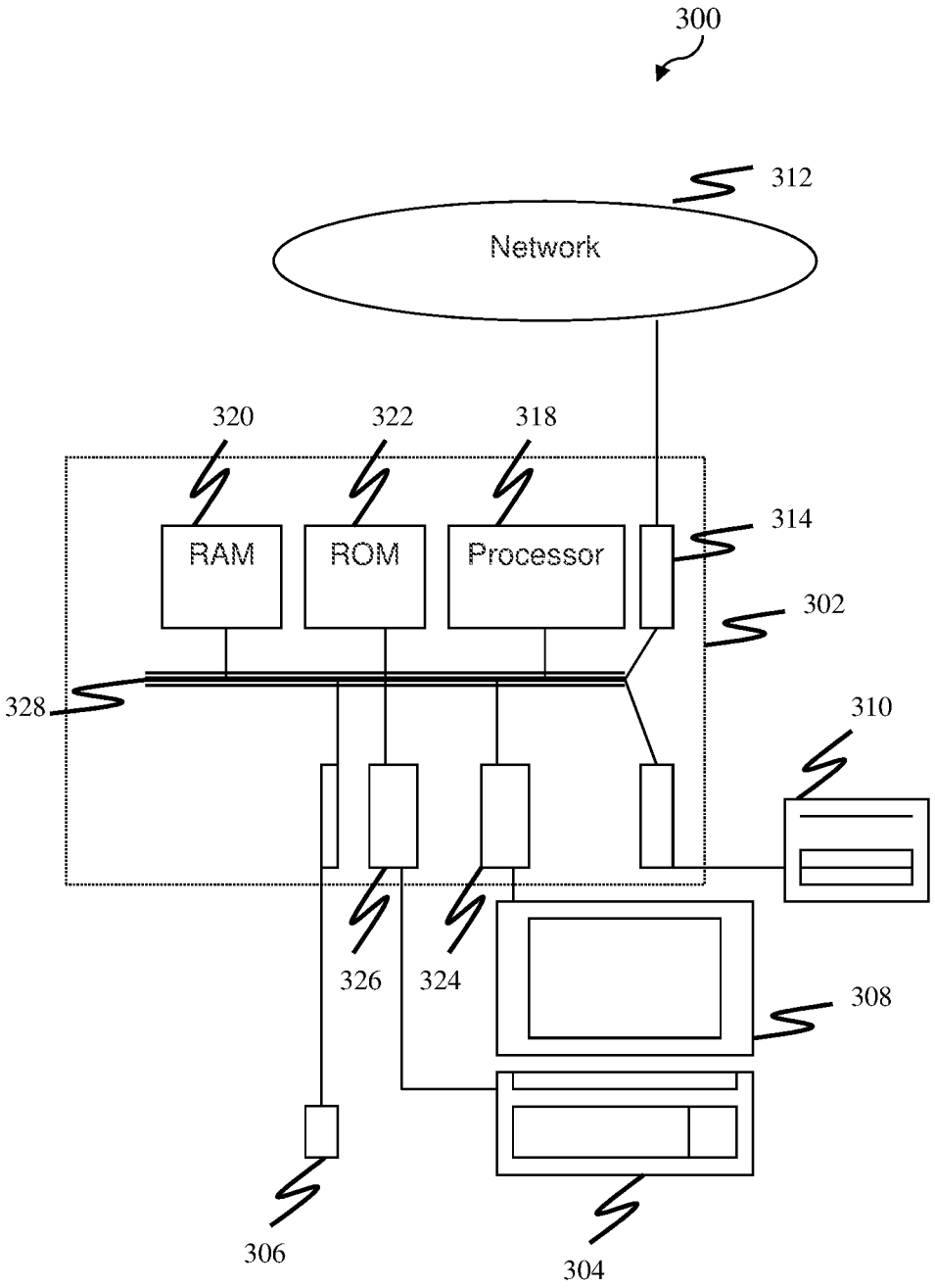

300
312
Network
320
322
318
RAM
ROM
Processor
314
302
328
310
326
324
308
306
304

FIG. 3

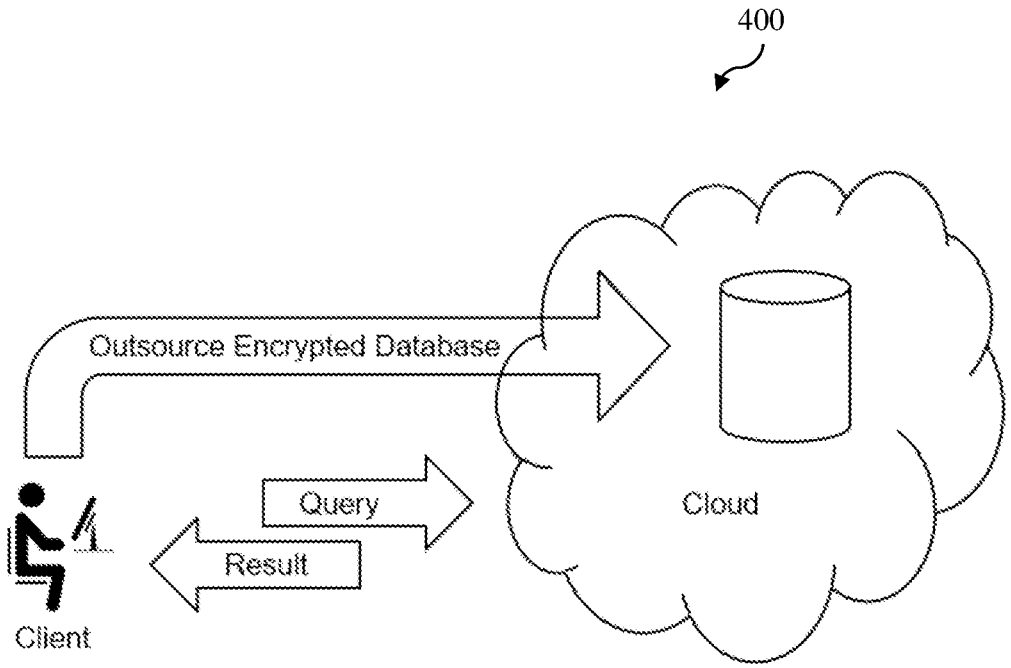

400
Outsource Encrypted Database
Query
Result
Client
Cloud

FIG. 4

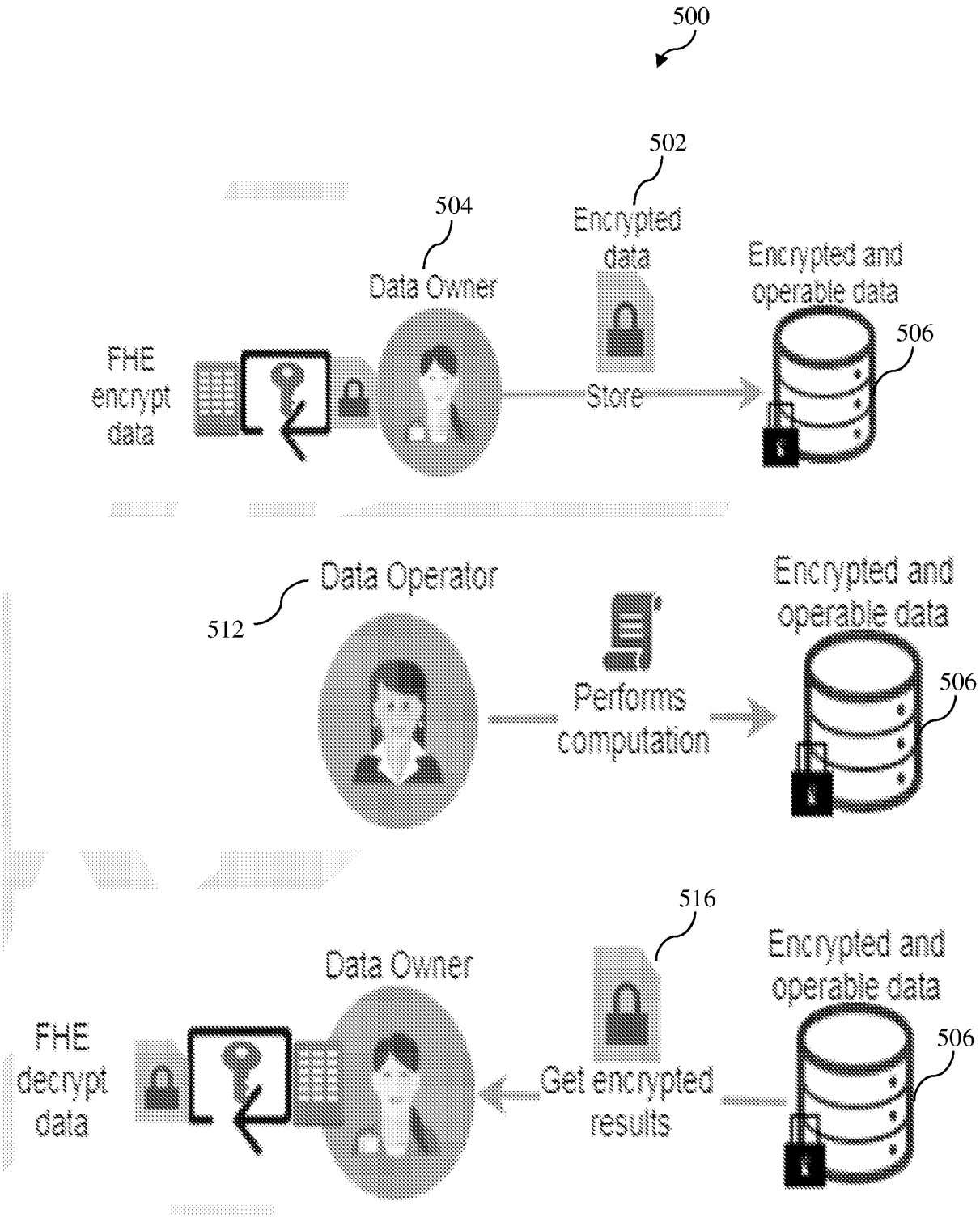

500
502
Encrypted data
504
Data Owner
Encrypted and operable data
506
FHE encrypt data
Store
Data Operator
512
Encrypted and operable data
506
Performs computation
516
Data Owner
Encrypted and operable data
FHE decrypt data
Get encrypted results
506

FIG. 5

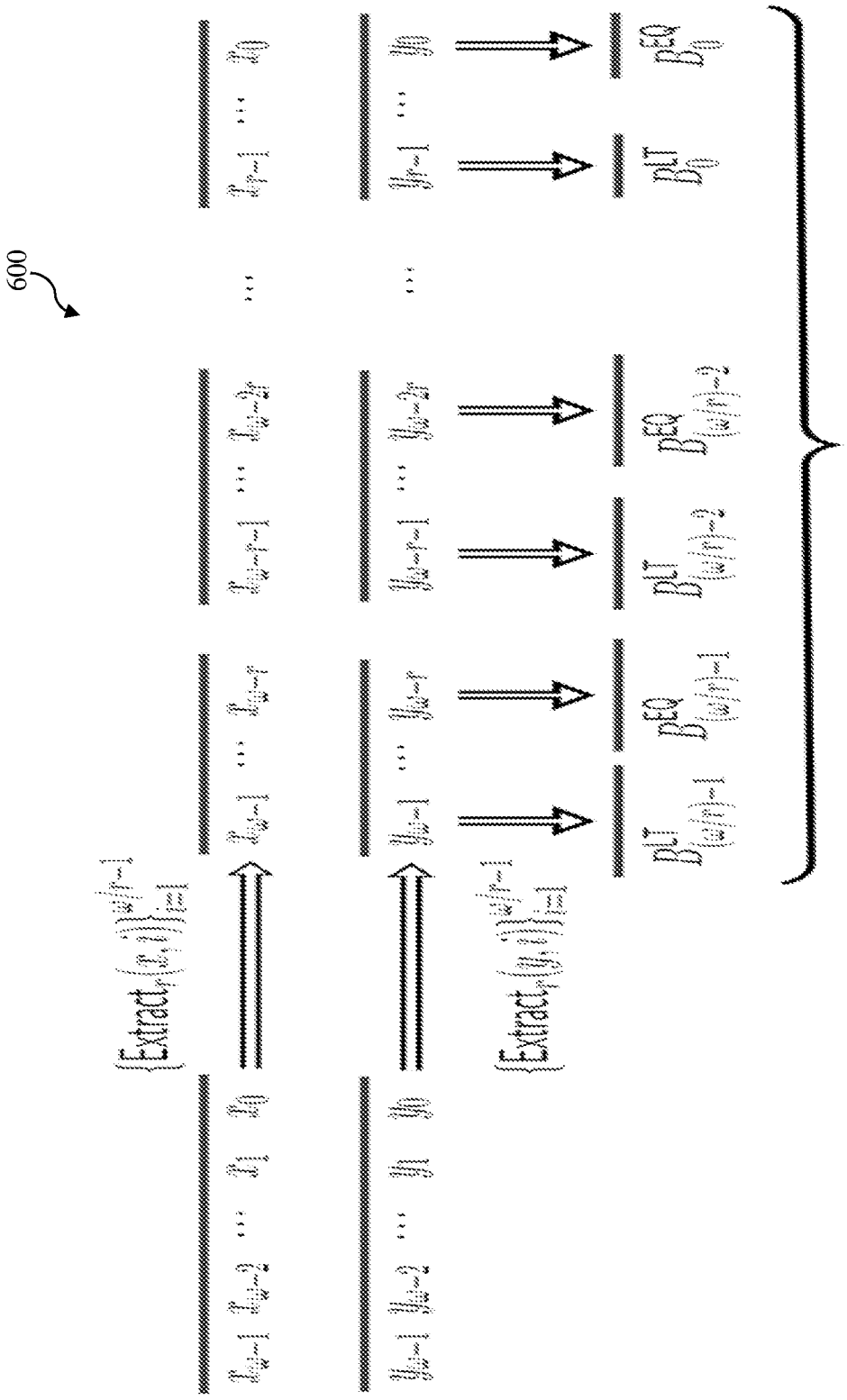

600
$\{\text{Extract}_r(L_i,0)\}_{i=1}^{w/r-1}$
$\{\text{Extract}_r(H_i,0)\}_{i=1}^{w/r-1}$
$L_{w-1}\ L_{w-2}\ \cdots\ L_1\ L_0$
$H_{w-1}\ H_{w-2}\ \cdots\ H_1\ H_0$
$L_{w-1}\ L_{w-2}\ \cdots\ L_{w-r}\ \ L_{r-1}\ \cdots\ L_0$
$H_{w-1}\ H_{w-2}\ \cdots\ H_{w-r}\ \ H_{r-1}\ \cdots\ H_0$
$L_{w-r-1}\ \cdots\ L_{w-2r}\ \ L_{2r-1}\ \cdots\ L_r$
$H_{w-r-1}\ \cdots\ H_{w-2r}\ \ H_{2r-1}\ \cdots\ H_r$
$B_{(w/r)-1}^{LT}\ B_{(w/r)-1}^{EQ}$
$B_{(w/r)-2}^{LT}\ B_{(w/r)-2}^{EQ}$
$B_1^{LT}\ B_1^{EQ}$
$B_0^{LT}\ B_0^{EQ}$
$LT_{(0,1)^w}(x,y) = LT_{2^w}(x,y) = B_{(w/r)-1}^{LT} + \sum_{i=1}^{w/r-2}(B_i^{LT}\cdot\prod_{j=i+1}^{w/r-1}\overline{B_j^{EQ}})$

FIG. 6A

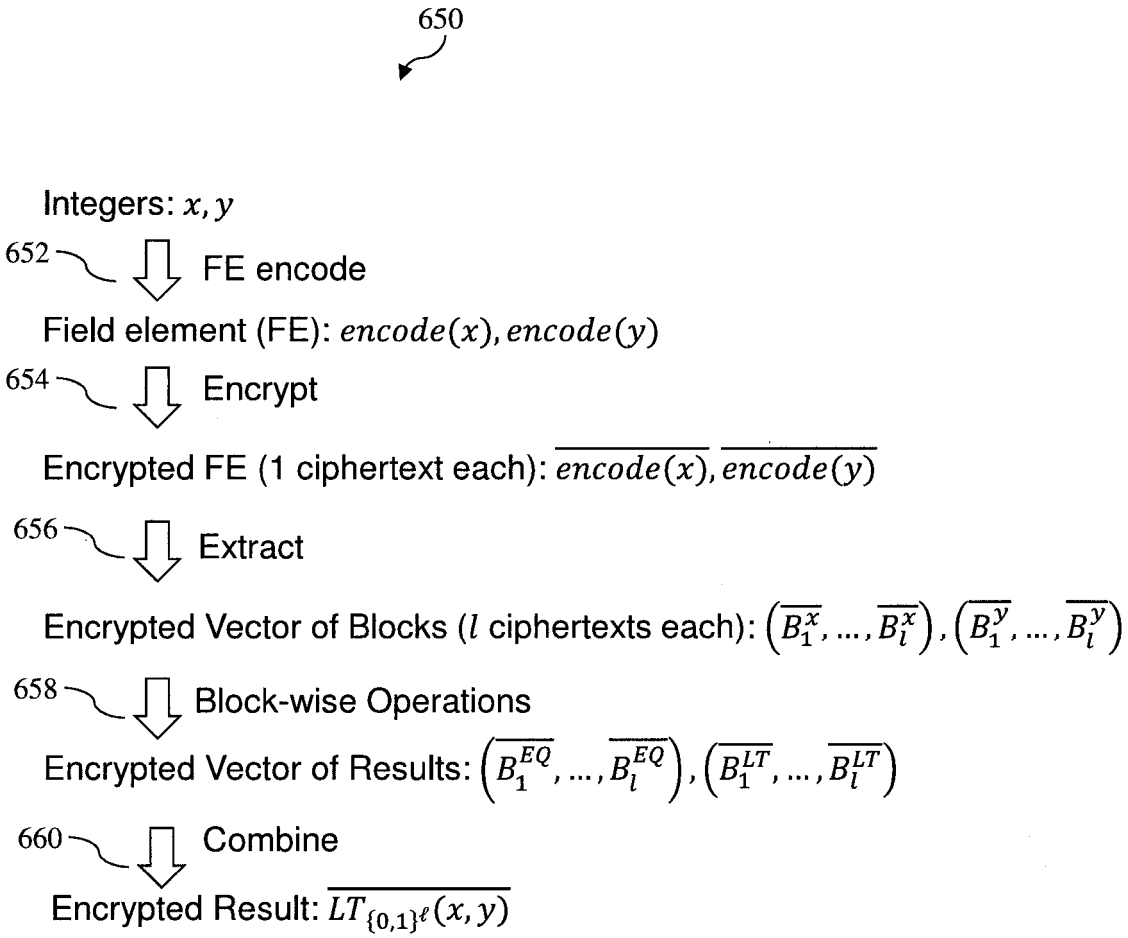

650
Integers: x, y
652
FE encode
Field element (FE): $encode(x), encode(y)$
654
Encrypt
Encrypted FE (1 ciphertext each): $\overline{encode(x)}, \overline{encode(y)}$
656
Extract
Encrypted Vector of Blocks (l ciphertexts each): $\left(\overline{B_1^x}, \ldots, \overline{B_l^x}\right), \left(\overline{B_1^y}, \ldots, \overline{B_l^y}\right)$
658
Block-wise Operations
Encrypted Vector of Results: $\left(\overline{B_1^{EQ}}, \ldots, \overline{B_l^{EQ}}\right), \left(\overline{B_1^{LT}}, \ldots, \overline{B_l^{LT}}\right)$
660
Combine
Encrypted Result: $\overline{LT_{\{0,1\}^\ell}(x, y)}$

FIG. 6B

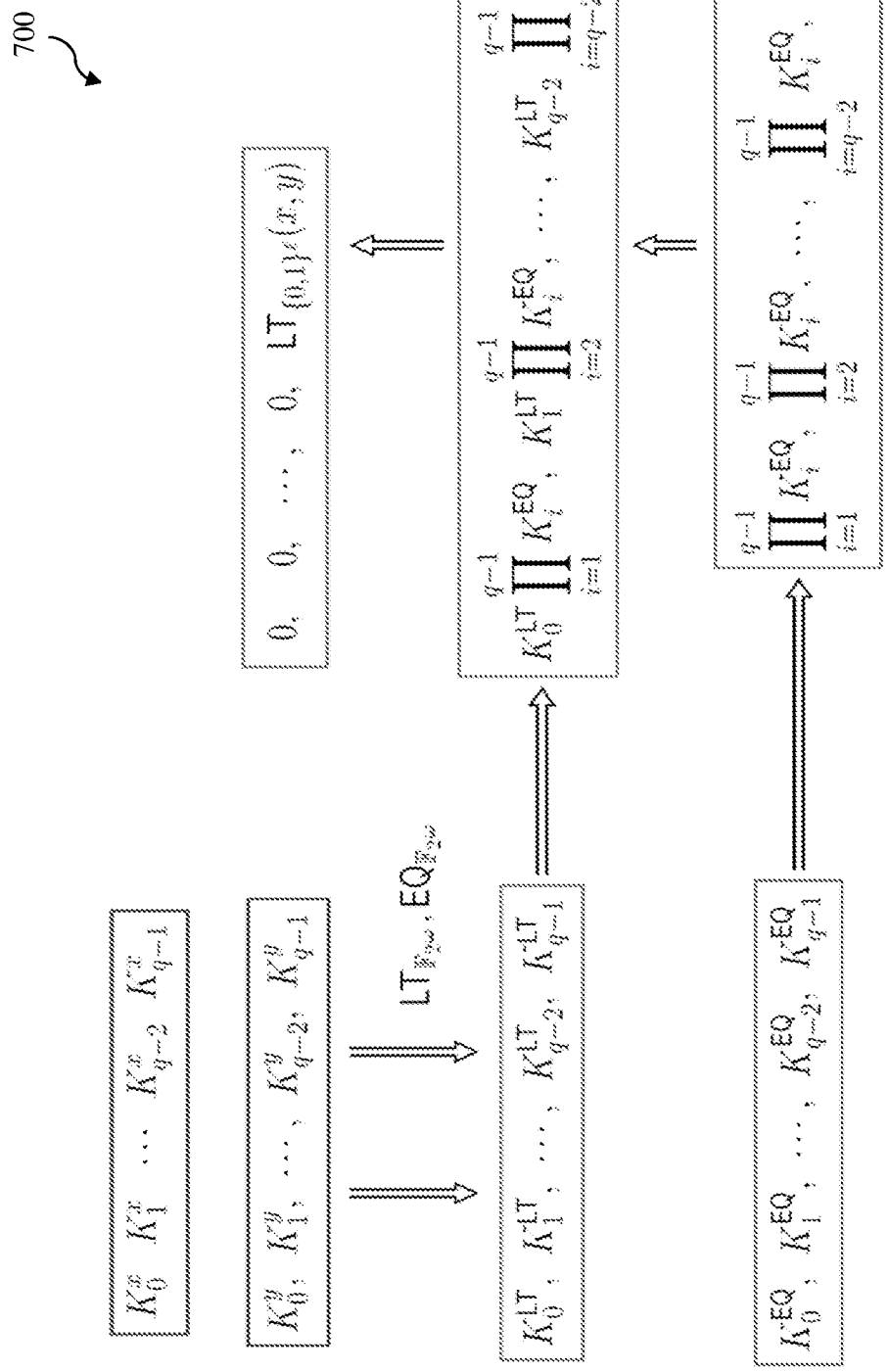

700
$K_0^x,\ K_1^x,\ \cdots,\ K_{q-2}^x,\ K_{q-1}^x$
$K_0^y,\ K_1^y,\ \cdots,\ K_{q-2}^y,\ K_{q-1}^y$
$\mathsf{LT}_{\mathbb{F}_{2^w}}, \mathsf{EQ}_{\mathbb{F}_{2^w}}$
$K_0^{\mathsf{LT}},\ K_1^{\mathsf{LT}},\ \cdots,\ K_{q-2}^{\mathsf{LT}},\ K_{q-1}^{\mathsf{LT}}$
$K_0^{\mathsf{EQ}},\ K_1^{\mathsf{EQ}},\ \cdots,\ K_{q-2}^{\mathsf{EQ}},\ K_{q-1}^{\mathsf{EQ}}$
$\prod_{i=1}^{q-1} K_i^{\mathsf{EQ}},\ \cdots,\ \prod_{i=q-2}^{q-1} K_i^{\mathsf{EQ}},\ 1$
$K_0^{\mathsf{LT}} \prod_{i=1}^{q-1} K_i^{\mathsf{EQ}},\ K_1^{\mathsf{LT}} \prod_{i=2}^{q-1} K_i^{\mathsf{EQ}},\ \cdots,\ K_{q-2}^{\mathsf{LT}} \prod_{i=q-2}^{q-1} K_i^{\mathsf{EQ}},\ K_{q-1}^{\mathsf{LT}}$
$0,\ 0,\ \cdots,\ 0,\ \mathsf{LT}_{\{0,1\}^w}(x,y)$

FIG. 7A

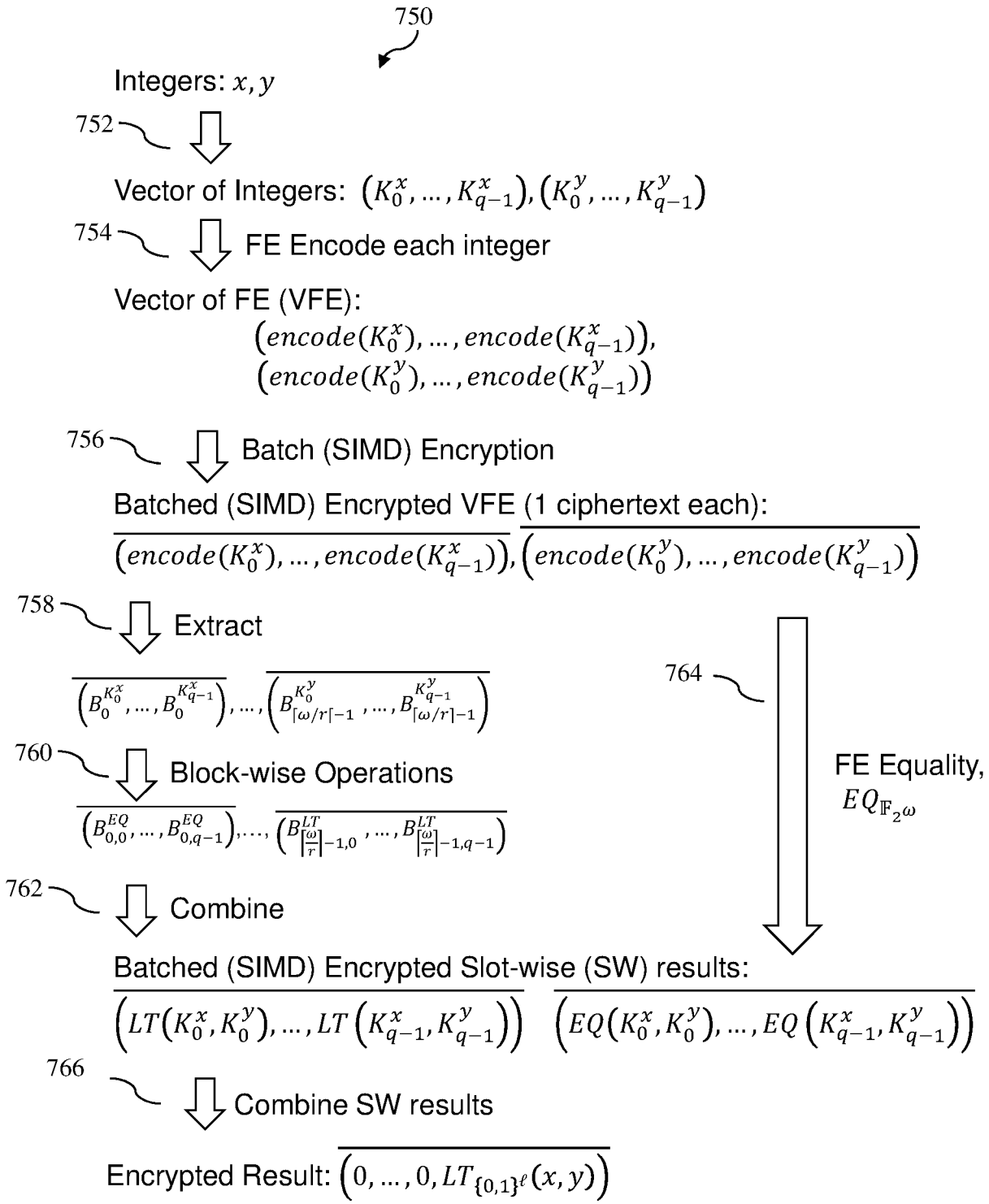

750
Integers: x, y
752
Vector of Integers: $(K_0^x, \ldots, K_{q-1}^x), (K_0^y, \ldots, K_{q-1}^y)$
754
FE Encode each integer
Vector of FE (VFE):
$(encode(K_0^x), \ldots, encode(K_{q-1}^x)),$
$(encode(K_0^y), \ldots, encode(K_{q-1}^y))$
756
Batch (SIMD) Encryption
Batched (SIMD) Encrypted VFE (1 ciphertext each):
$\overline{(encode(K_0^x), \ldots, encode(K_{q-1}^x))}, \overline{(encode(K_0^y), \ldots, encode(K_{q-1}^y))}$
758
Extract
$\overline{(B_0^{K_0^x}, \ldots, B_0^{K_{q-1}^x})}, \ldots, \overline{(B_{\lceil\omega/r\rceil-1}^{K_0^y}, \ldots, B_{\lceil\omega/r\rceil-1}^{K_{q-1}^y})}$
760
Block-wise Operations
$\overline{(B_{0,0}^{EQ}, \ldots, B_{0,q-1}^{EQ})}, \ldots, \overline{(B_{\lceil\frac{\omega}{r}\rceil-1,0}^{LT}, \ldots, B_{\lceil\frac{\omega}{r}\rceil-1,q-1}^{LT})}$
762
Combine
764
FE Equality, $EQ_{\mathbb{F}_2\omega}$
Batched (SIMD) Encrypted Slot-wise (SW) results:
$\overline{(LT(K_0^x, K_0^y), \ldots, LT(K_{q-1}^x, K_{q-1}^y))}$ $\overline{(EQ(K_0^x, K_0^y), \ldots, EQ(K_{q-1}^x, K_{q-1}^y))}$
766
Combine SW results
Encrypted Result: $\overline{(0, \ldots, 0, LT_{\{0,1\}^\ell}(x, y))}$

FIG. 7B

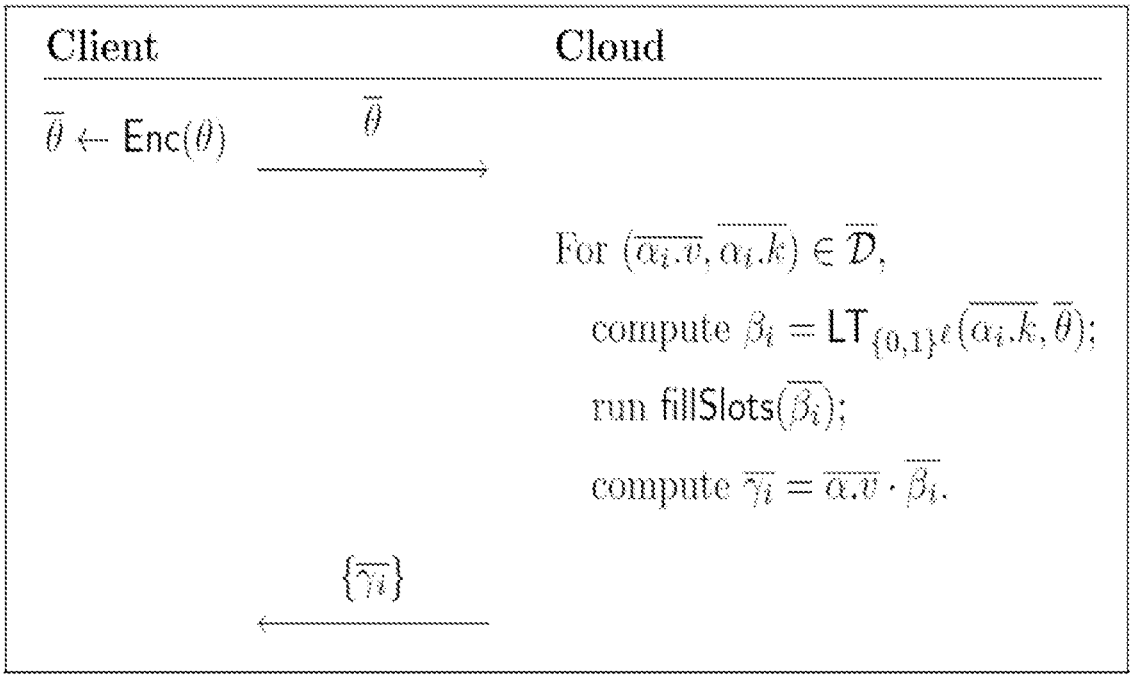

Client
Cloud
$\overline{\theta} \leftarrow \mathsf{Enc}(\theta)$
$\overline{\theta}$
For $(\overline{\alpha_i.v}, \overline{\alpha_i.k}) \in \overline{\mathcal{D}}$,
compute $\overline{\beta_i} = \mathsf{LT}_{\{0,1\}^\ell}(\overline{\alpha_i.k}, \overline{\theta})$;
run $\mathsf{fillSlots}(\overline{\beta_i})$;
compute $\overline{\gamma_i} = \overline{\alpha.v} \cdot \overline{\beta_i}$.
$\{\overline{\gamma_i}\}$

FIG. 8

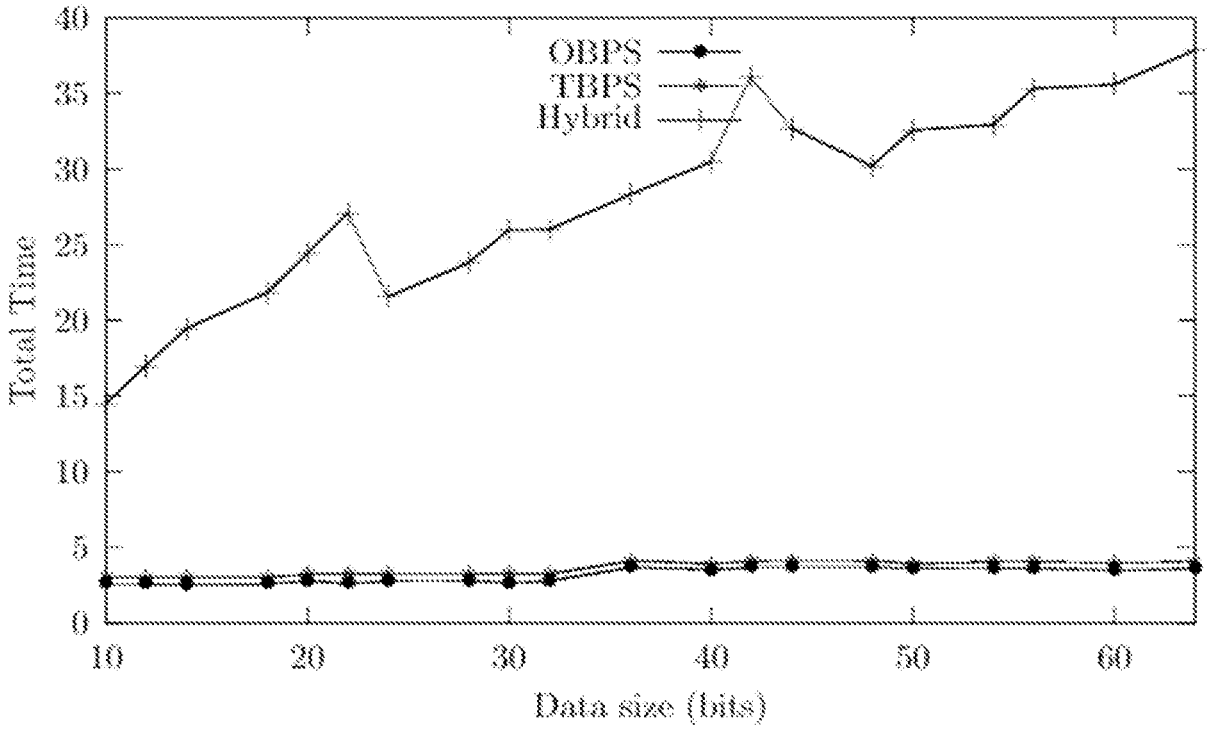

OBPS
TBPS
Hybrid
Total Time
Data size (bits)
0
5
10
15
20
25
30
35
40
10
20
30
40
50
60

FIG. 9A

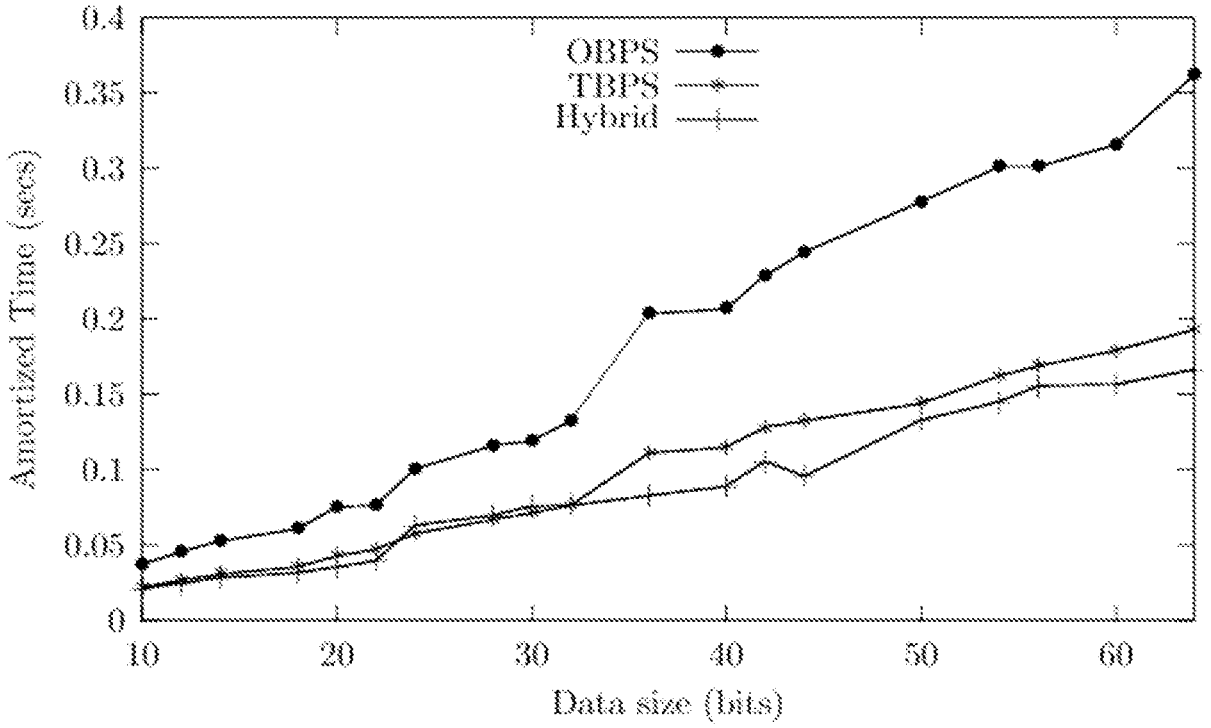

OBPS
TBPS
Hybrid
Amortized Time (secs)
Data size (bits)
0
0.05
0.1
0.15
0.2
0.25
0.3
0.35
0.4
10
20
30
40
50
60

FIG. 9B