

FIG. 1

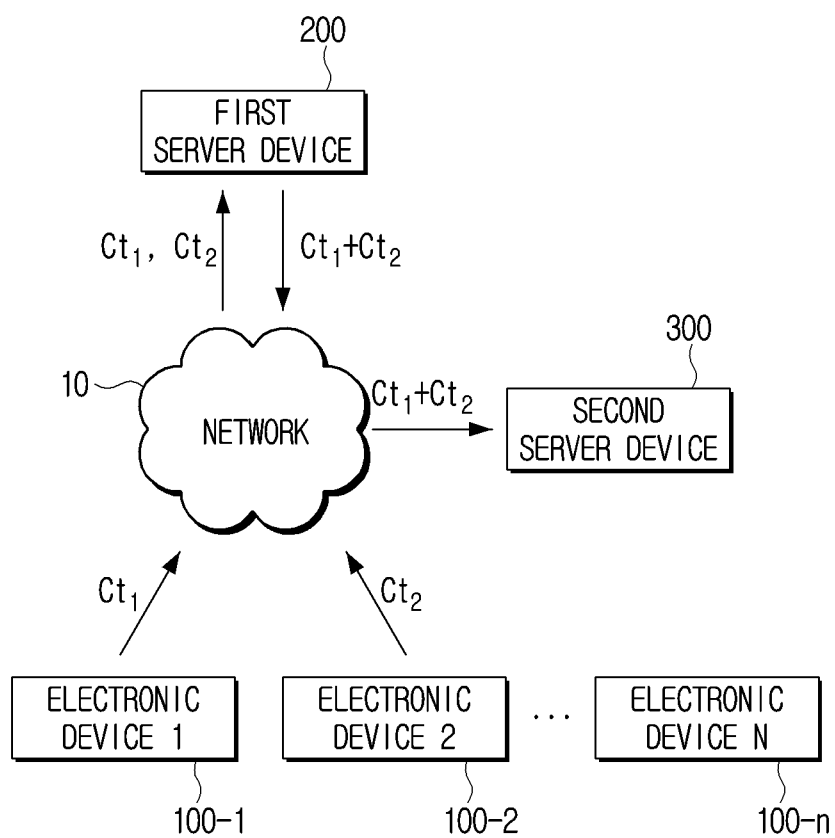


FIG. 2

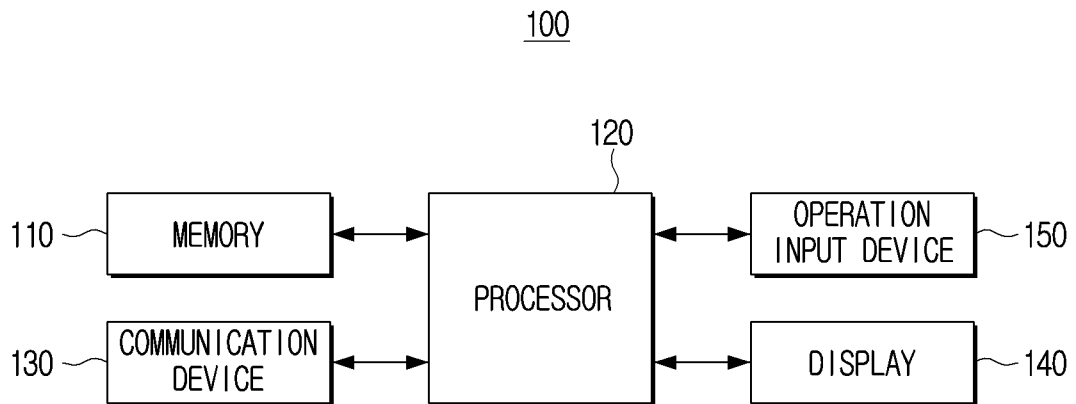


FIG. 3

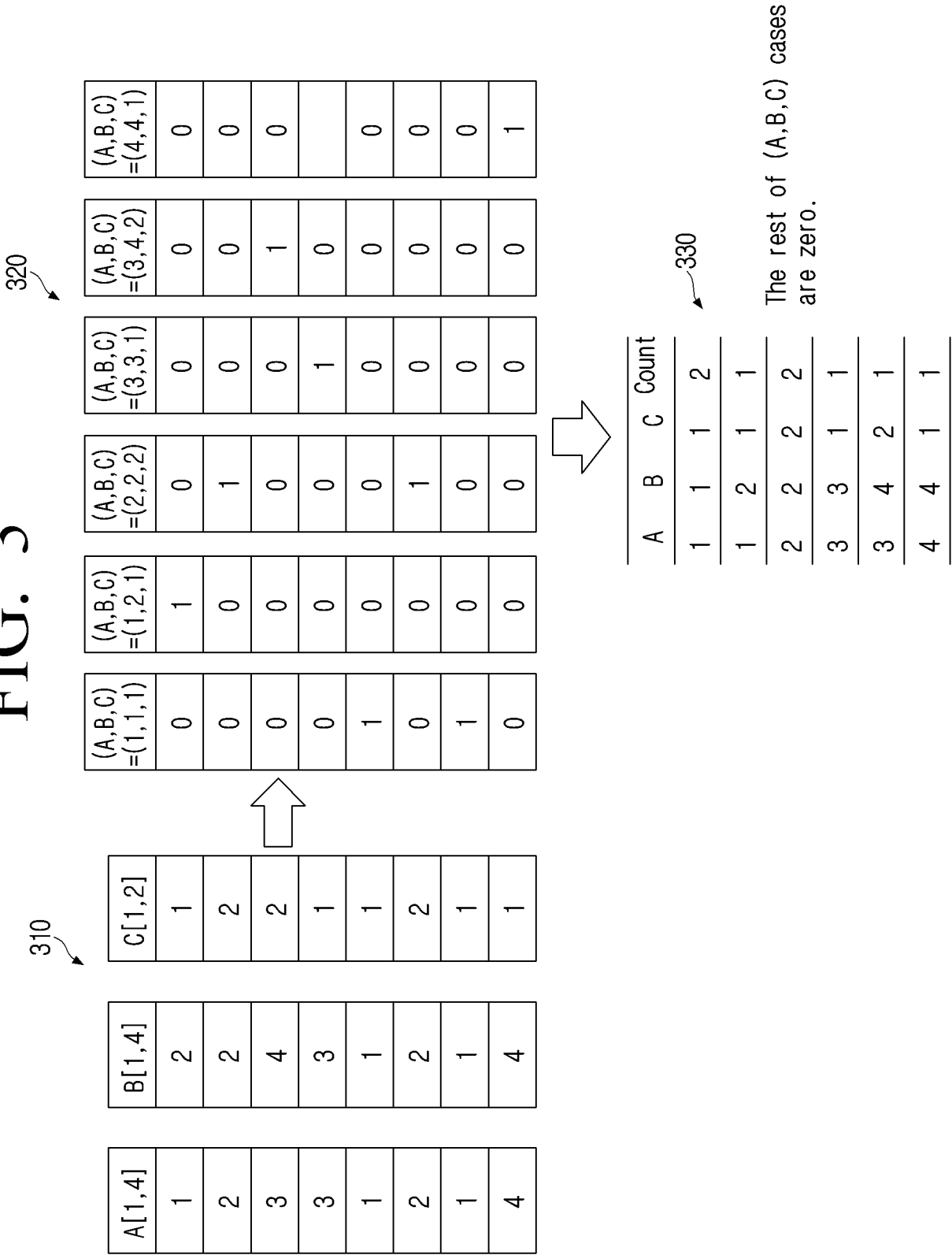


FIG. 4

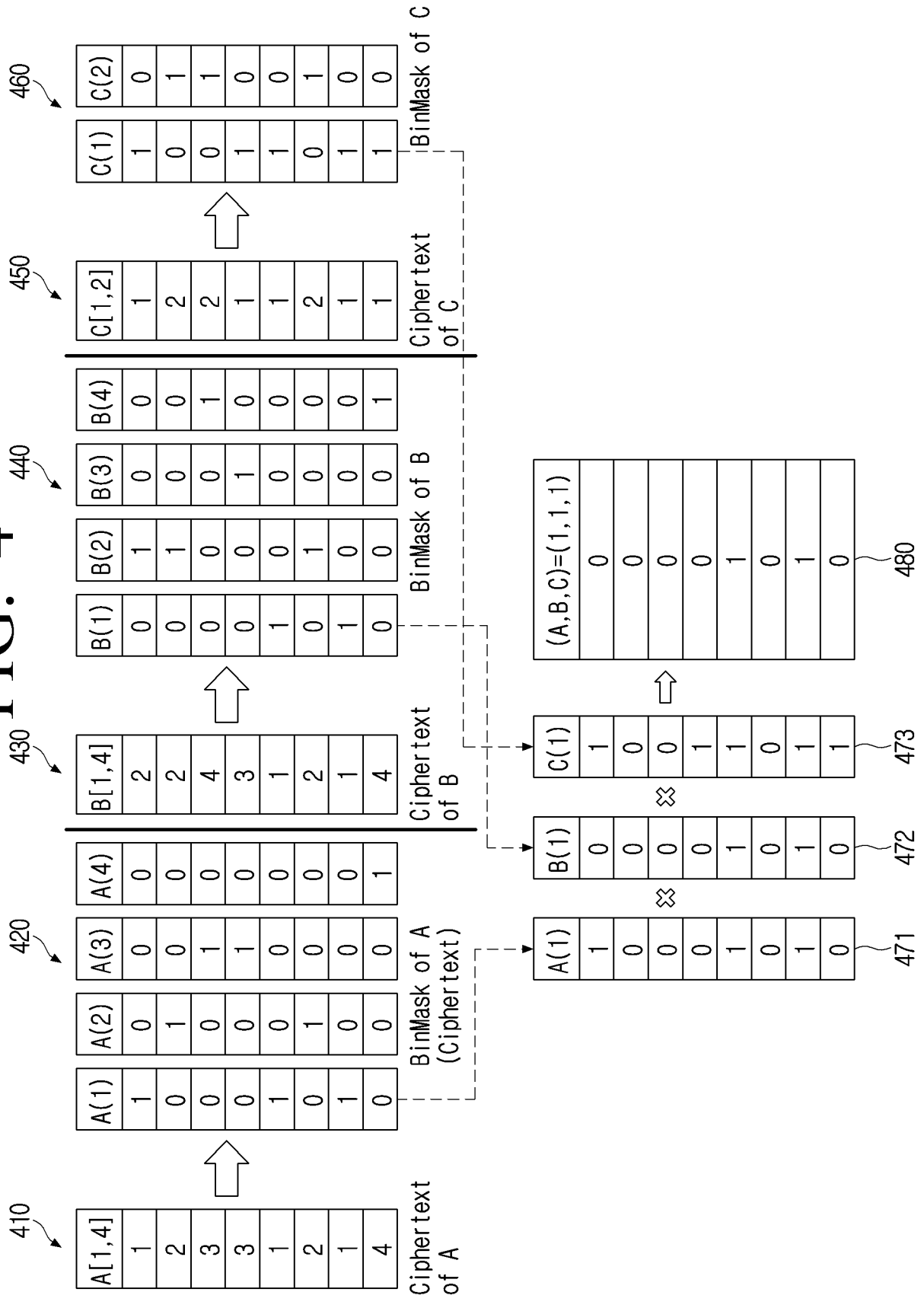


FIG. 5

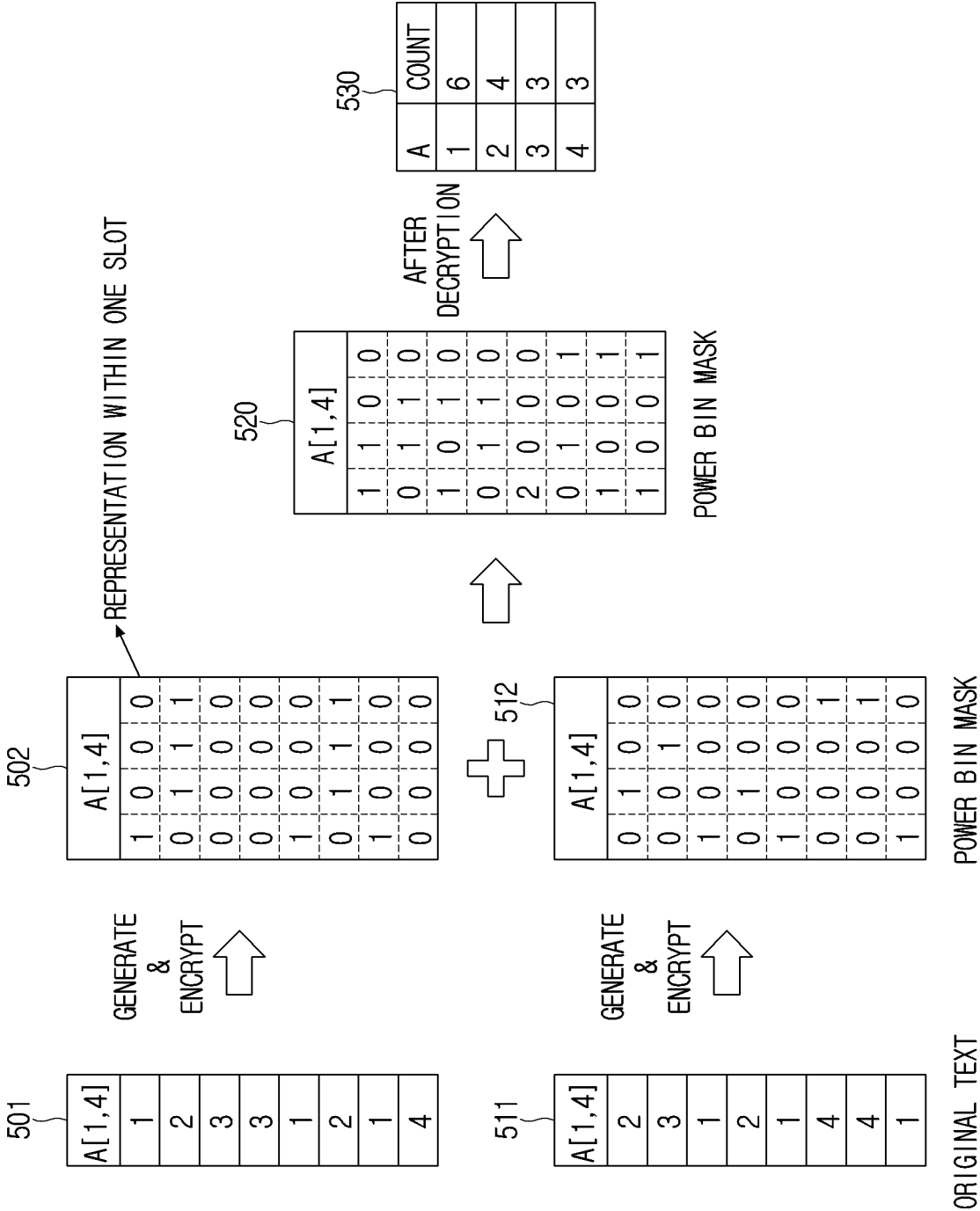


FIG. 6

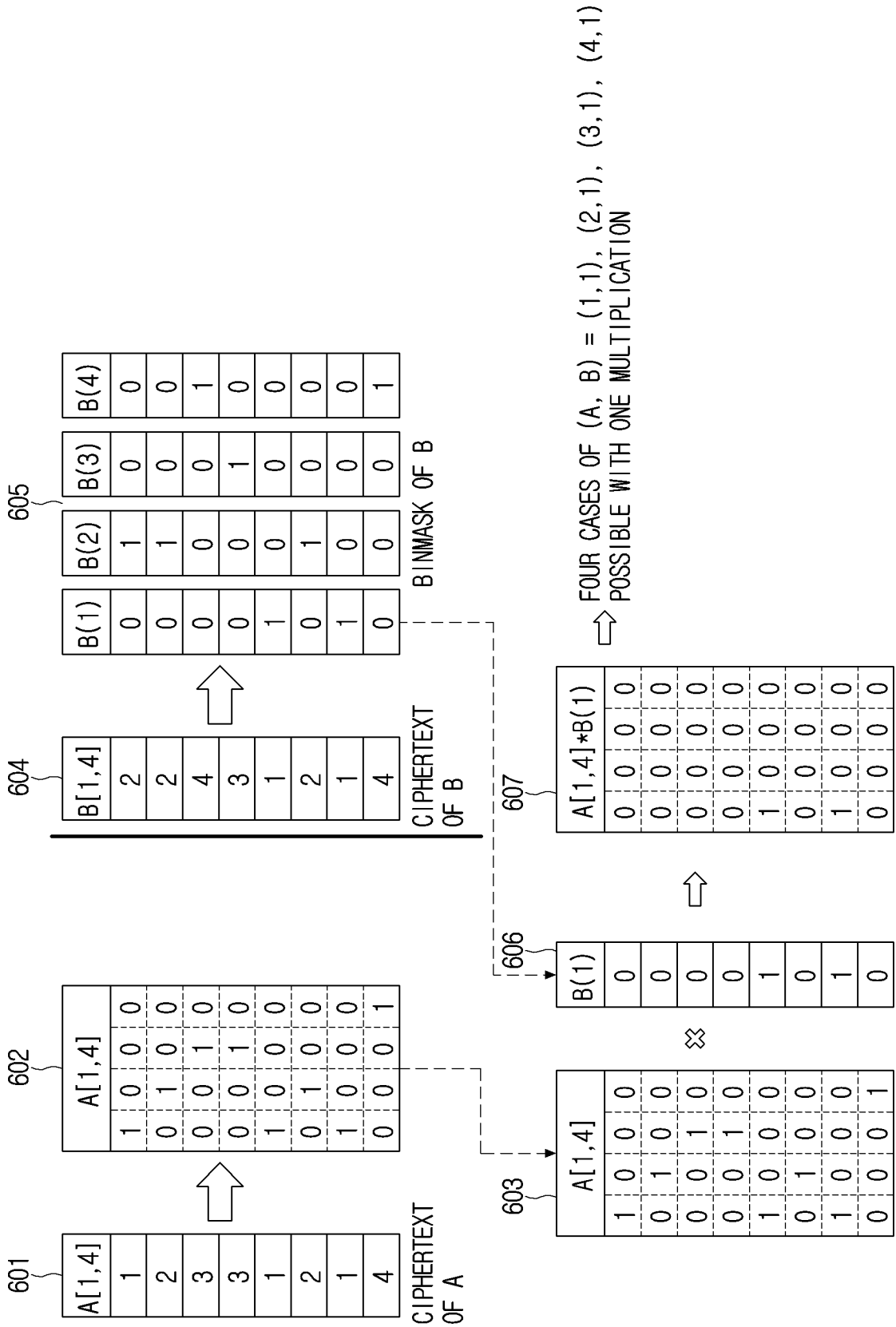


FIG. 7

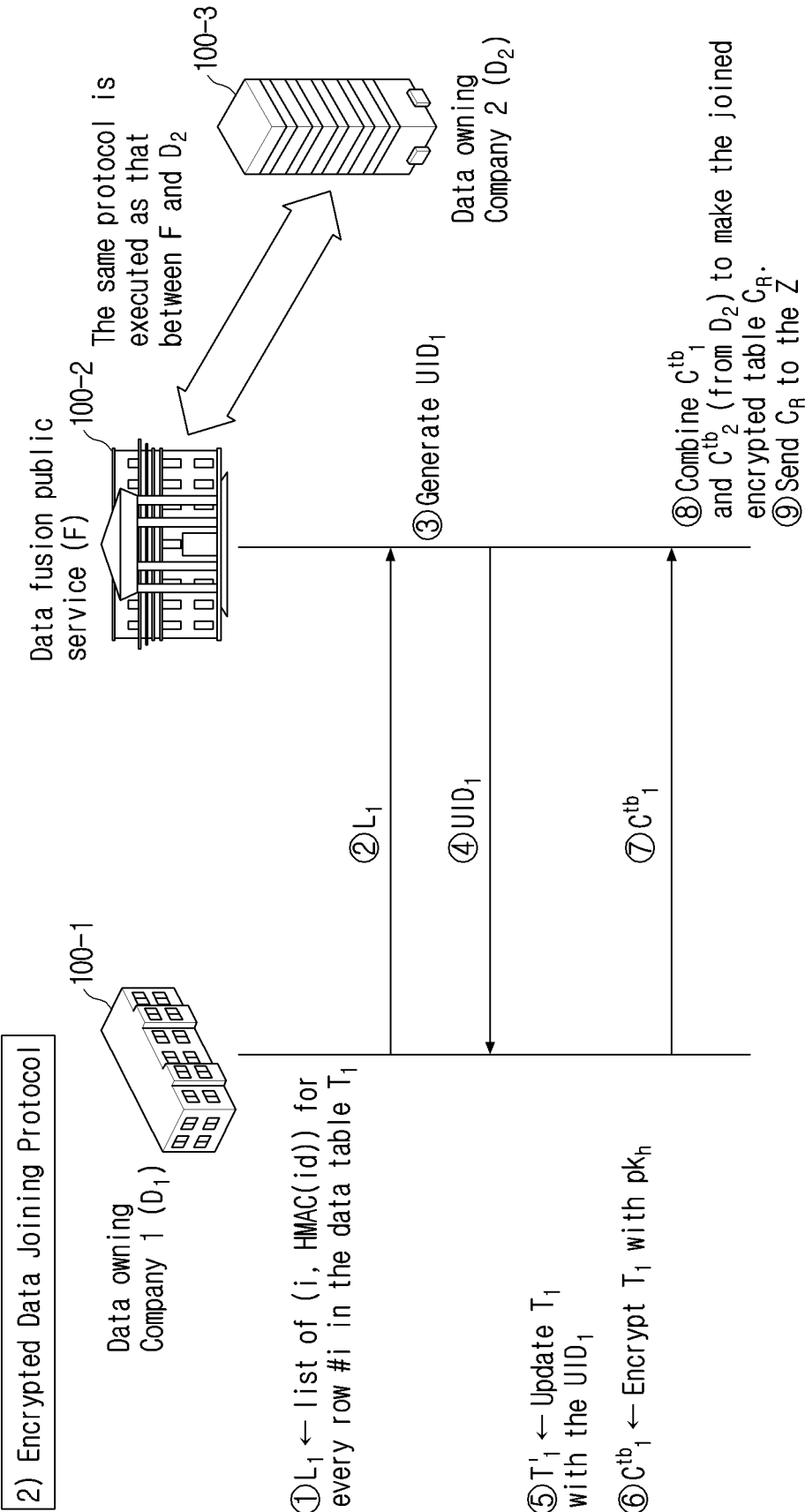


FIG. 8

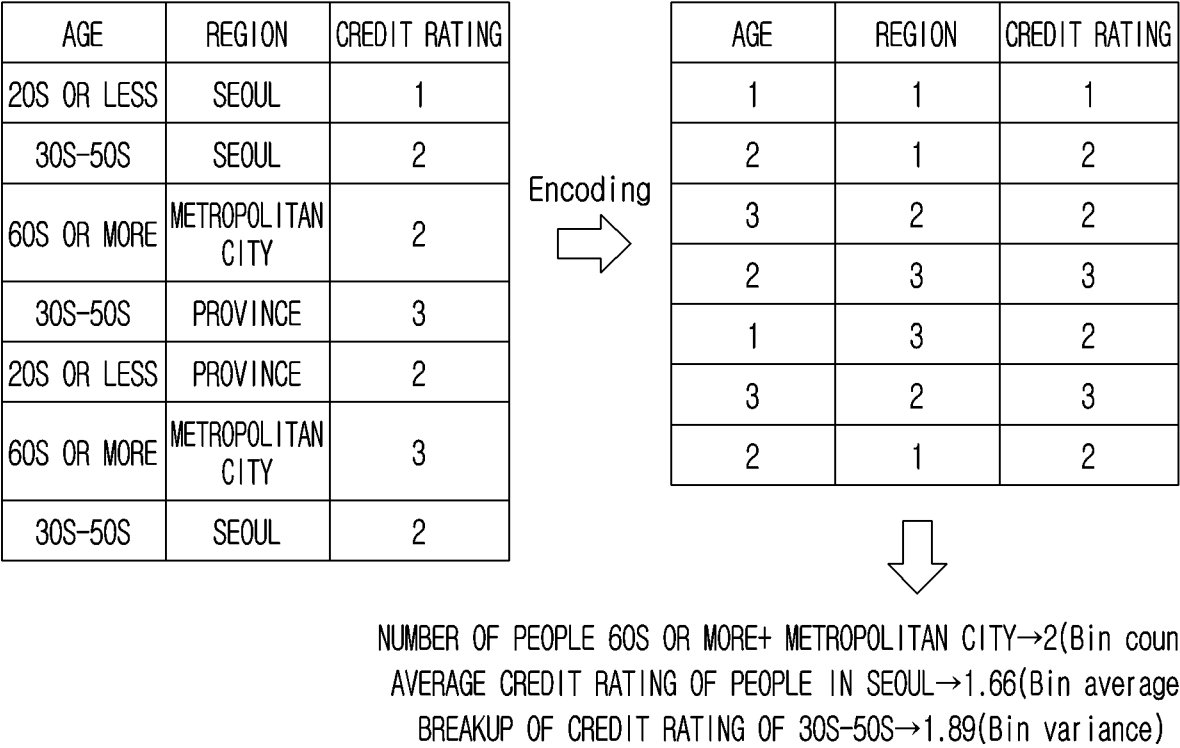


FIG. 9

900

```

1: procedure GENBINMASK(x, v,  $\vec{f}$ ,  $\vec{s}$ )
2:    $n_b \leftarrow \lceil n/M \rceil$ 
3:    $m \leftarrow \text{length}(\vec{f})$ 
4:   for  $i \leftarrow 0, m - 1$  do
5:     for  $j \leftarrow 0, n_b - 1$  do
6:       for  $k \leftarrow 1, s_i$  do
7:          $\text{tmp} \leftarrow 0^M$ 
8:         for  $l \leftarrow 0, M - 1$  do
9:           if  $\bar{x}_j^{(fi)}(l) == k \ \& \ \bar{v}_j^{(fi)}(l) == 1$  then
10:             $\text{tmp}[l] \leftarrow 1$ 
11:           $b_{k,j}^{(fi)} \leftarrow \text{Enc}_{pk}(\text{tmp})$ 
12:   return b

```

FIG. 10

1000
}

```

1: procedure GENBINMASK( $x$ ,  $\bar{f}$ ,  $\bar{s}$ )
2:    $n_b \leftarrow \lceil n/M \rceil$ 
3:    $m \leftarrow \text{length}(\bar{f})$ 
4:   for  $i \leftarrow 0, m - 1$  do
5:     for  $j \leftarrow 0, n_b - 1$  do
6:       for  $k \leftarrow 1, s_i$  do
7:          $\text{tmp} \leftarrow 0^M$ 
8:         for  $l \leftarrow 0, M - 1$  do
9:           if  $\bar{x}_j^{(fi)}(l) == k$  then
10:             $\text{tmp}[l] \leftarrow 1$ 
11:           $b_{k,j}^{(fi)} \leftarrow \text{Enc}_{pk}(\text{tmp})$ 
12:   return  $b$ 

```

FIG. 11

1100

```

1: procedure DISCRETEEQUALZERO(x,  $\mu$ , K)
2:    $d \leftarrow \lceil \log_2 \mu \rceil$ 
3:    $y \leftarrow \text{Mult}_{\text{evk}}(x, 1/2^d)$ 
4:
5:   declare pows[K + 1] ▷ array of ciphertexts
6:    $\text{pows}[0] \leftarrow \text{Enc}_{\text{pk}}((1^M)^T)$ 
7:    $\text{pows}[1] \leftarrow y$ 
8:   for  $i \leftarrow 2, K$  do
9:      $\text{pows}[i] \leftarrow \text{Mult}_{\text{evk}}(\text{pows}[\lceil i/2 \rceil], \text{pows}[\lceil i/2 \rceil])$ 
10:   $s \leftarrow \text{Enc}_{\text{pk}}((0^M)^T)$ 
11:   $c \leftarrow \text{Enc}_{\text{pk}}((0^M)^T)$ 
12:  for  $i \leftarrow 0, K$  do
13:     $s \leftarrow \text{Add}(s, \text{mult}_{\text{evk}}(a_i, \text{pow}[i]))$ 
14:     $c \leftarrow \text{Add}(s, \text{mult}_{\text{evk}}(b_i, \text{pow}[i]))$ 
15:  ▷  $s \approx \text{sinc}(x/2^d)$ ,  $c \approx \cos(\pi x/2^d)$ 
16:
17:   $s \leftarrow \text{Mult}_{\text{evk}}(s, c)$ 
18:  for  $i \leftarrow 0, d$  do
19:     $c \leftarrow \text{Mult}_{\text{evk}}(c, c)$ 
20:     $c \leftarrow \text{Mult}_{\text{evk}}(c, 2)$ 
21:     $c \leftarrow \text{Sub}(c, 1)$ 
22:     $s \leftarrow \text{Mult}_{\text{evk}}(s, c)$ 
23:  return s

```

FIG. 12

1200
}

```

1: procedure GENBINMASK(X, V,  $\vec{f}$ ,  $\vec{s}$ )
2:    $n_b \leftarrow \lceil n/M \rceil$ 
3:    $m \leftarrow \text{length}(\vec{f})$ 
4:   for  $i \leftarrow 0, m - 1$  do
5:     for  $j \leftarrow 0, n_b - 1$  do
6:       for  $k \leftarrow 1, s_i$  do
7:          $\text{tmp} \leftarrow \text{Sub}(X_j^{(fi)}, k)$ 
8:          $\text{tmp} \leftarrow \text{DiscreteEqualZero}(\text{tmp}, s_i, K)$ 
9:         if v-bit table exists, then
10:           $\text{tmp} \leftarrow \text{Mult}_{\text{evk}}(\text{tmp}, V_j^{(fi)})$ 
11:         $b_{k,j}^{(fi)} \leftarrow \text{tmp}$ 
12:   return b

```

FIG. 13

1300

```

1: procedure BINCOUNT( $b, \bar{f}, \bar{c}$ )
2:    $n_b \leftarrow \lceil n/M \rceil$ 
3:    $m \leftarrow \text{length}(\bar{f})$ 
4:    $\text{sum} \leftarrow \text{Enc}_{\text{pk}}((O^M)^T)$ 
5:   for  $i \leftarrow 0, n_b - 1$  do
6:      $\text{tmp} \leftarrow b_{\text{co},i}^{(\text{fo})}$ 
7:     for  $j \leftarrow 1, m - 1$  do
8:        $\text{tmp} \leftarrow \text{Mult}_{\text{evk}}(\text{tmp}, b_{\text{cj},i}^{(\text{fj})})$ 
9:      $\text{sum} \leftarrow \text{Add}(\text{sum}, \text{tmp})$ 
10:  for  $i \leftarrow 0, \log_2(M) - 1$  do
11:     $\text{sum} \leftarrow \text{Add}(\text{sum}, \text{Rot}_{\text{evk}}(\text{sum}, 2^i))$ 
12:  return sum

```

FIG. 14

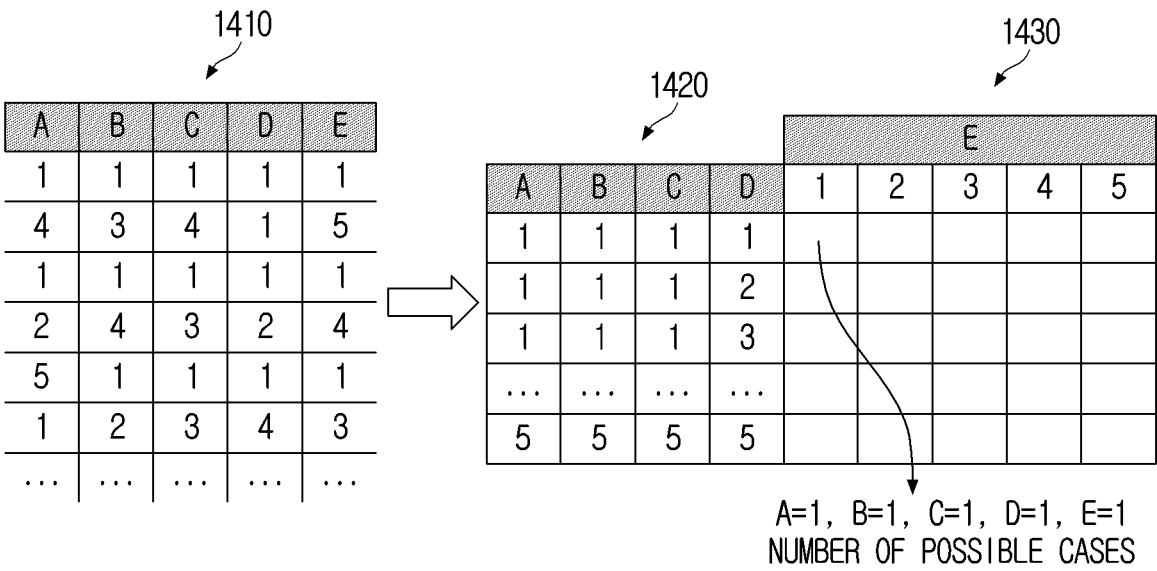


FIG. 15

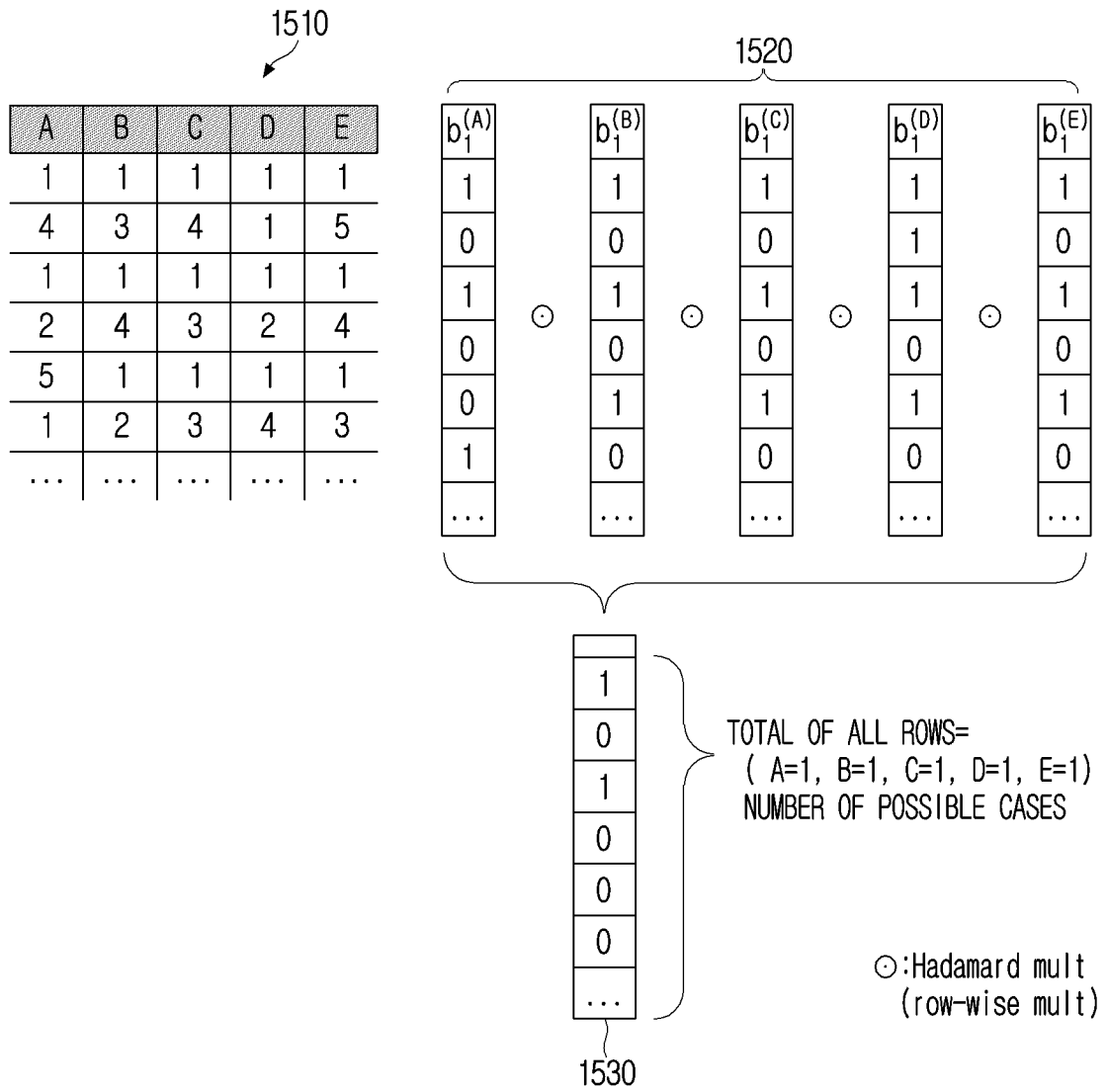


FIG. 16

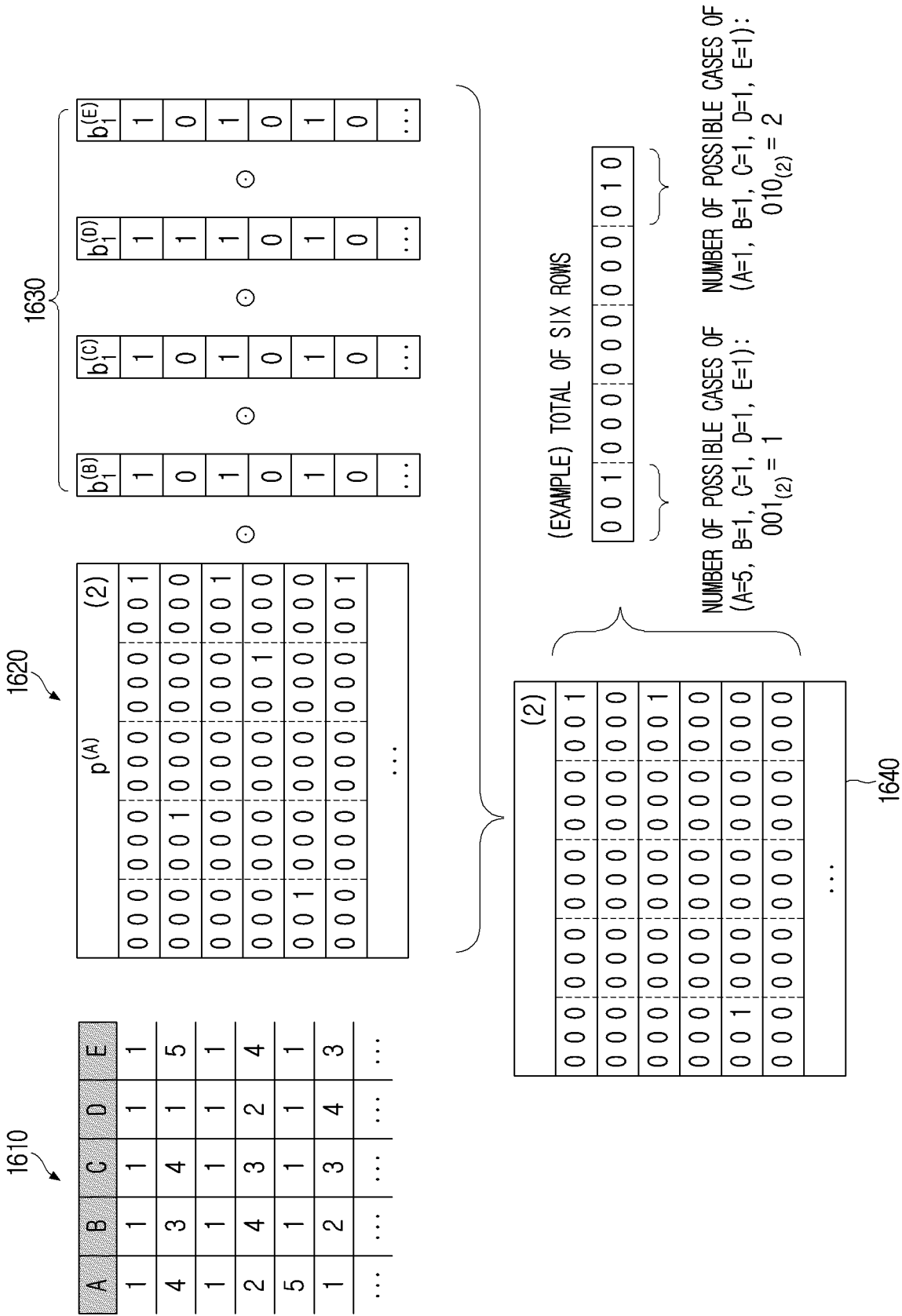


FIG. 17

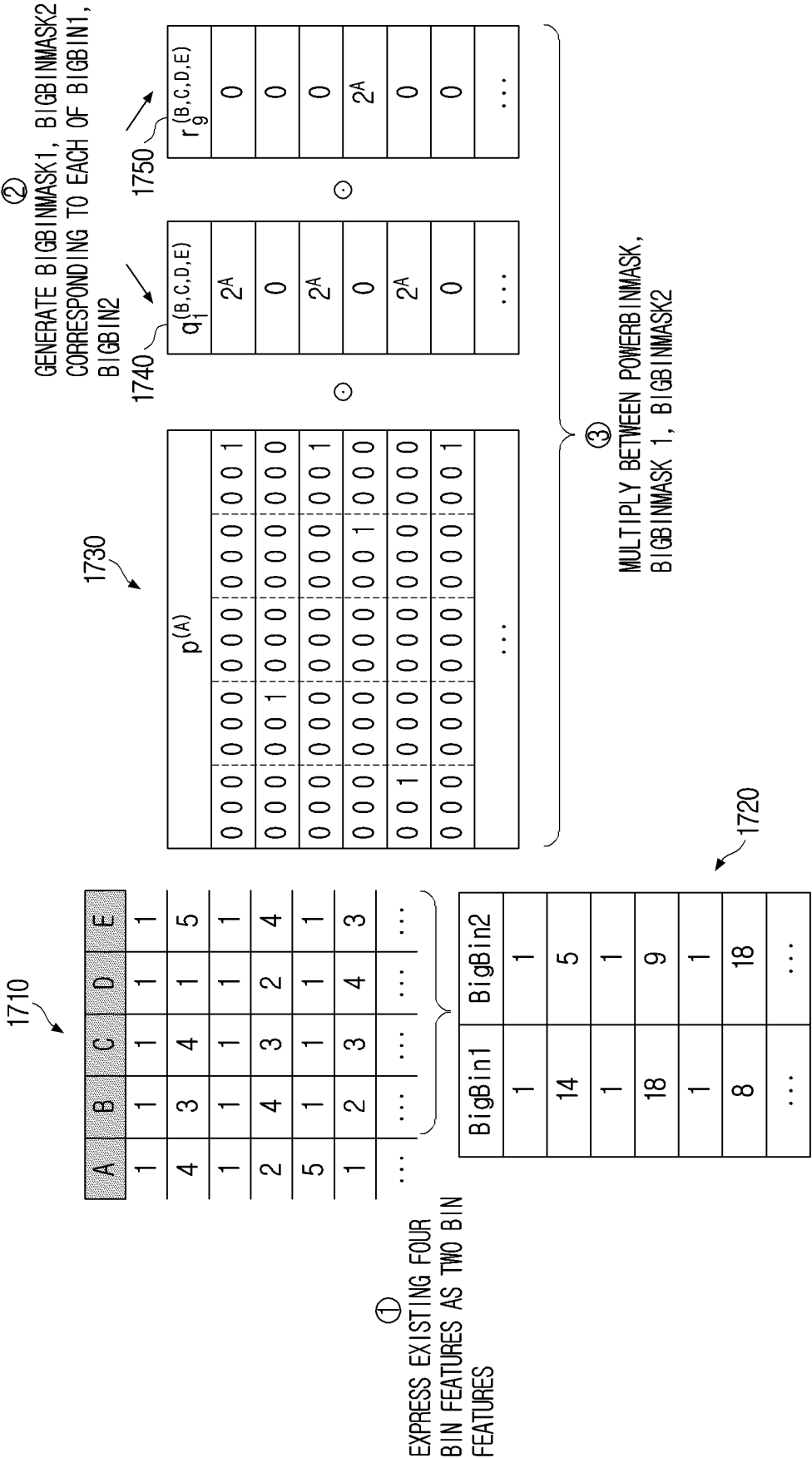


FIG. 18

1800
}

```

1: procedure GENPOWERBINMASK( $x$ ,  $v$ ,  $fo$ )
2:    $n_b \leftarrow \lceil n/M \rceil$ 
3:   for  $i \leftarrow 0, n_b - 1$  do
4:      $\bar{p} \leftarrow (0^M)^T$ 
5:     for  $j \leftarrow 0, M - 1$  do
6:       if  $\bar{v}^{(fo)}(i * M + j) == 1$  then
7:          $\bar{p}(j) \leftarrow \text{Pow}(2, \Delta \cdot (\bar{x}^{(fo)}(i * M + j) - 1) + \delta)$ 
8:      $p_i \leftarrow \text{Enc}_{sk}(\bar{p})$ 
9:   return  $p$ 

```

FIG. 19

1900

```

1: procedure GENBIGBINMASK(x, v, (f1, ..., fm-1), (s1, ..., sm-1))
2:   nb ← ⌈n/M⌉
3:   Q ← ⌈√∏i=1m-1 (si)⌉
4:   for i ← 0, nb - 1 do
5:      $\vec{q}^{(1)}, \dots, \vec{q}^{(Q)} \leftarrow (O^M)^T$ 
6:      $\vec{r}^{(1)}, \dots, \vec{r}^{(Q)} \leftarrow (O^M)^T$ 
7:     for j ← 0, M - 1 do
8:       if  $\vec{v}_i^{(f1)}(j) == 1$  for l = 0, 1, ..., m - 1 then
9:         ▷ if every valid bits are one,
10:            tmp ← 0
11:            for l ← 0, m - 1 do
12:              tmp ← sl * tmp + ( $\vec{x}_i^{(f1)}(j) - 1$ )
13:            q' ← ⌊tmp/Q⌋ + 1
14:            r' ← tmp%Q + 1
15:             $\vec{q}^{(q')}(j) \leftarrow 2^j$ 
16:             $\vec{r}^{(r')}(j) \leftarrow 2^j$ 
17:          for j ← 1, Q do
18:            qi(j) ← Encpk( $\vec{q}^{(j)}$ )
19:            ri(j) ← Encpk( $\vec{r}^{(j)}$ )
20:  return q(i), r(i) (i = 1, 2...Q)

```

FIG. 20

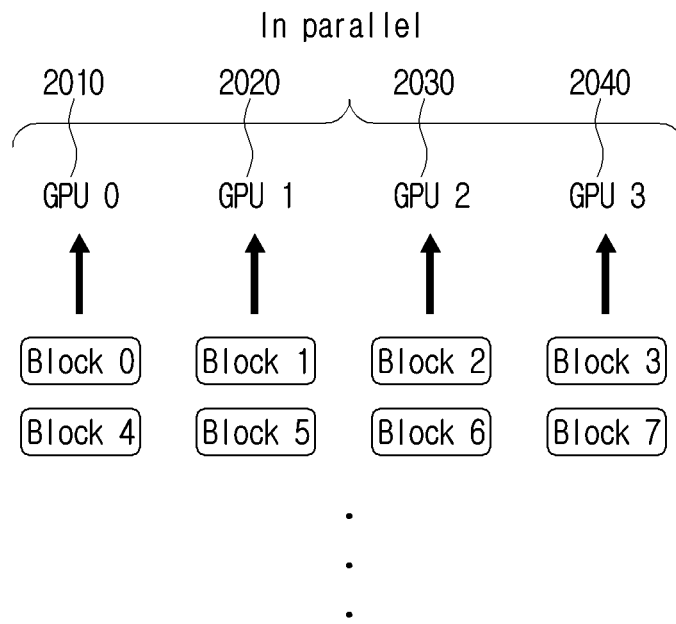


FIG. 21

2100

```

1: procedure MULTPERGPU(p, q, r, curr_gpu_idx, Ng)
2:   l = current_gpu_idx
3:   while l < ⌈n/M⌉ do
4:     a ← 0
5:     while a < Q do
6:       for i ← 1, c do
7:         ql(a+i) ← Multevk(pl, ql(a+i))
8:         b ← 0
9:         while b < Q do
10:          for j ← 1, c do
11:            tmp ← Multevk(ql(a+i), rl(b+j))
12:            if l == current_gpu_idx then
13:              rescurrent_gpu_idx(a+i, b+j) ← tmp
14:            else
15:              rescurrent_gpu_idx(a+i, b+j) ← Add(tmp, rescurrent_gpu_idx(a+i, b+j))
16:          b ← b + c
17:        a ← a + c
18:      l ← l + Ng
19:    return {rescurrent_gpu_idx(i,j) | i, j = 1, 2, ..., Q}
20:
21: procedure LARGE BINCOUNTMULT(p, q, r, Ng)
22:   mres ← {}
23:   for curr_gqu_idx ← 0, Ng - 1 do ▷ in parallel
24:     mres ← mres ∪ MULTPERGPU(p, q, r, curr_gpu_idx, Ng)
25:   return mres = {resk(i,j) | k = 0, 1, ..., Ng - 1, i, j = 1, 2, ..., Q}

```

FIG. 22

2200

```

1: procedure LARGEBINCOUNTDEC(mres)
2:   arr ← zeros((Q2, s0))    ▷ an (Q2 * s0)-size array filled with zeros
3:   for i ← 1, Q do
4:     for j ← 1, Q do
5:       for k ← 0, Ng - 1 do
6:          $\overrightarrow{\text{res}} \leftarrow \text{Dec}_{\text{sk}}(\text{res}_k^{(i,j)})$ 
7:         for s ← 0, M - 1 do
8:           tmp ←  $\overrightarrow{\text{res}}(s)$ 
9:           tmp ← tmp / (2 ·  $\wedge$  +  $\delta$ )
10:        for l ← 1, s0 do
11:          cnt ← tmp % (1 <<  $\Delta$ )
12:          arr[Q * (i-1) + (j-1)][l-1] += cnt
13:          tmp ← tmp / (1 <<  $\Delta$ )
14:   return arr

```

FIG. 23

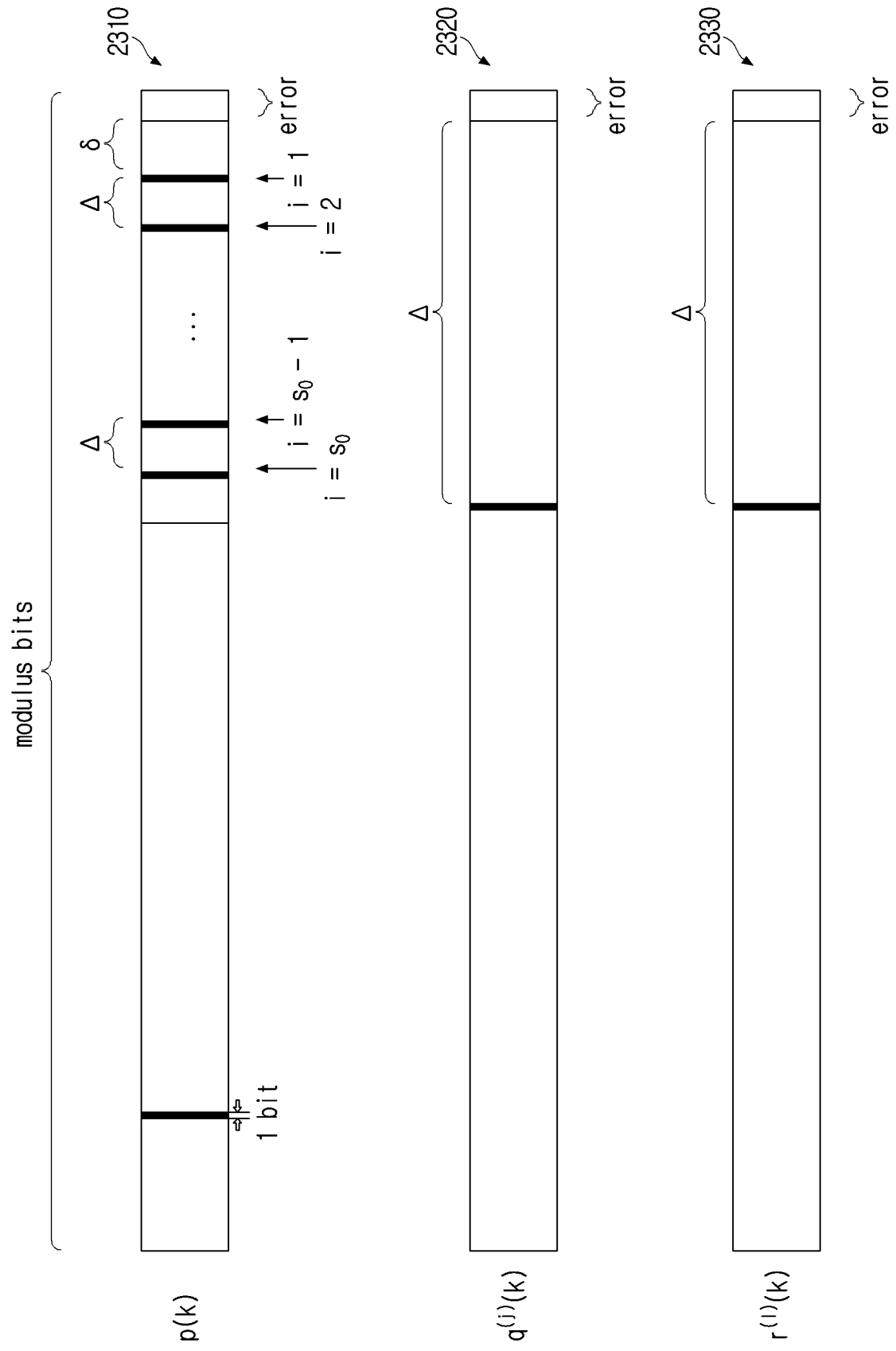


FIG. 24

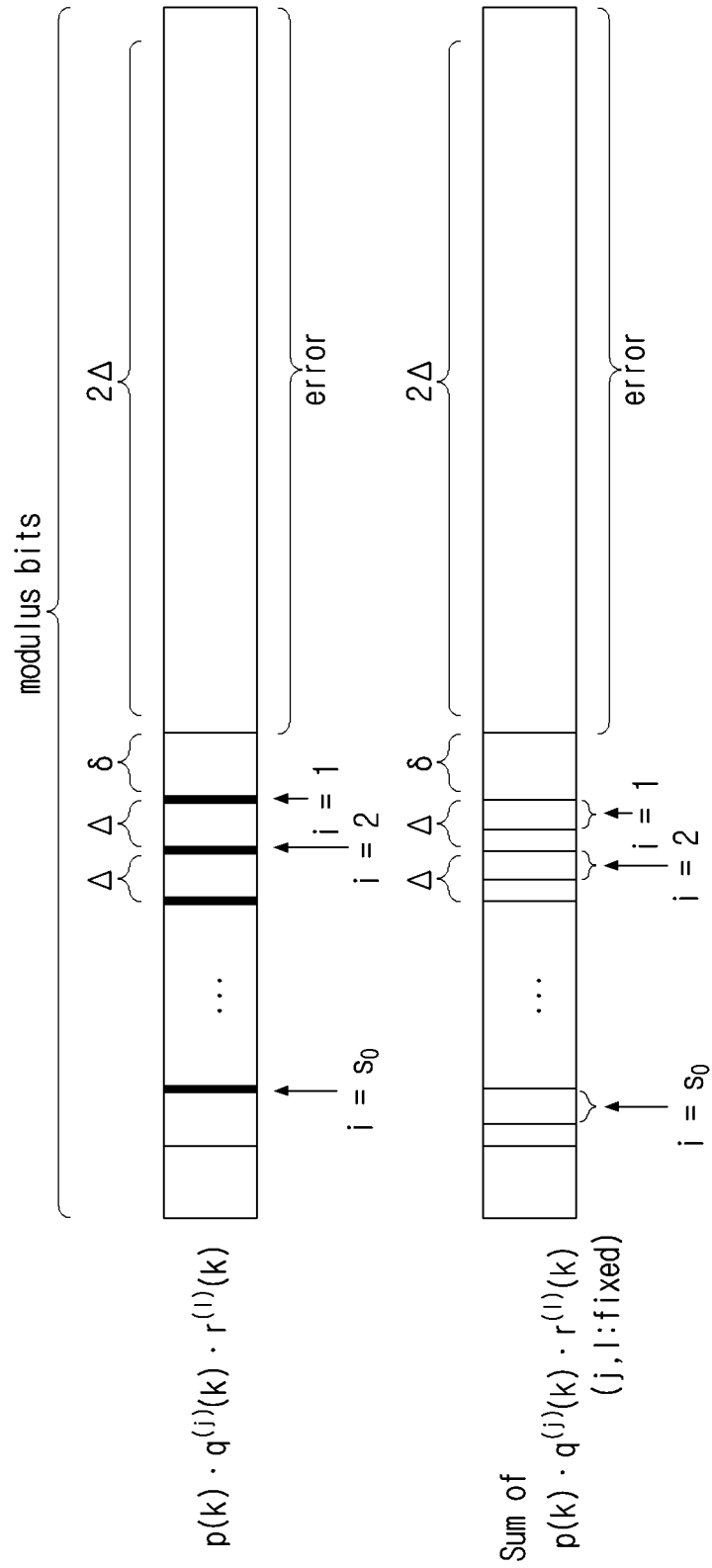


FIG. 25

2500
{

Algorithm 1 $\text{COMP}(\mathbf{x}_1, \mathbf{x}_2, \text{iter})$

Require: $\mathbf{x}_1(k), \mathbf{x}_2(k) \in [0, 1]$ for every $k \in [0, M - 1]$ **Ensure:** $\mathbf{y}$ where $\mathbf{y}(k)$ is an approximation of 1 if $\mathbf{x}_1(k) > \mathbf{x}_2(k)$,
0 if $\mathbf{x}_1(k) < \mathbf{x}_2(k)$, and $1/2$ otherwise ($k \in [0, M - 1]$).0: **procedure** $\text{COMP}(\mathbf{x}_1, \mathbf{x}_2, \text{iter})$ 1: $\mathbf{x} \leftarrow \mathbf{x}_1 - \mathbf{x}_2, i \leftarrow 0$ 2: **while** $i < \text{iter}$ **do**3: $\mathbf{x} \leftarrow f(\mathbf{x}), i \leftarrow i + 1$ 4: **return** $(\mathbf{x} + 1)/2$

FIG. 26

2600
}**Algorithm 7** Computing the mean of a column

```

0: procedure MEAN( $\mathbf{x}, \mathbf{v}$ )
1:  $\text{sum} \leftarrow \text{Enc}(0)$ 
2:  $\mathbf{n} \leftarrow \text{Enc}(0)$ 
3: for  $i = 0$  to  $N_B - 1$  do
4:    $\text{sum} \leftarrow \text{Add}(\text{sum}, \text{Mult}(\mathbf{x}_i, \mathbf{v}_i))$ 
5:    $\mathbf{n} \leftarrow \text{Add}(\mathbf{n}, \mathbf{v}_i)$ 
6: for  $i = 0$  to  $\log_2 M - 1$  do
7:    $\text{sum} \leftarrow \text{Add}(\text{sum}, \text{Rot}(\text{sum}, 2^i))$ 
8:    $\mathbf{n} \leftarrow \text{Add}(\mathbf{n}, \text{Rot}(\mathbf{n}, 2^i))$ 
9:  $\text{invn} \leftarrow \text{INVNTHSQRT}(\mathbf{n}, \text{Enc}(\mathbf{1}^M), 1, 25)$ 
10:  $\text{mean} \leftarrow \text{Mult}(\text{invn}, \text{sum})$ 
11: return  $\text{mean}$ 

```

FIG. 27

2700

Algorithm 8 Computing variance of a column

```

0: procedure VAR( $\mathbf{x}, \mathbf{v}$ )
1:  $\mathbf{sum} \leftarrow \text{Enc}(0)$ 
2:  $\mathbf{n} \leftarrow \text{Enc}(0)$ 
2:    $\mathbf{mean} \leftarrow \text{mean}(\mathbf{x}, \mathbf{v})$ 
3: for  $i = 0$  to  $N_B - 1$  do
4:    $\mathbf{tmp} \leftarrow \text{Sub}(\mathbf{x}, \mathbf{mean})$ 
5:    $\mathbf{tmp} \leftarrow \text{Mult}(\mathbf{tmp}, \mathbf{tmp})$ 
6:    $\mathbf{sum} \leftarrow \text{Add}(\mathbf{sum}, \text{Mult}(\mathbf{tmp}, \mathbf{v}))$ 
7:    $\mathbf{n} \leftarrow \text{Add}(\mathbf{n}, \mathbf{v}_i)$ 
8: for  $i = 0$  to  $\log_2 M - 1$  do
9:    $\mathbf{sum} \leftarrow \text{Add}(\mathbf{sum}, \text{Rot}(\mathbf{sum}, 2^i))$ 
10:   $\mathbf{n} \leftarrow \text{Add}(\mathbf{n}, \text{Rot}(\mathbf{n}, 2^i))$ 
11:  $\mathbf{invn} \leftarrow \text{INVNTHSQRT}(\mathbf{n}, \text{Enc}(1^M), 1, 25)$ 
12:  $\mathbf{var} \leftarrow \text{Mult}(\mathbf{invn}, \mathbf{sum})$ 
13: return  $\mathbf{var}$ 

```

FIG. 28

2800

Algorithm 9 Computing correlation of a column

```

0: procedure CORR( $\mathbf{x}, \mathbf{y}, \mathbf{v}$ )
1:  $\text{sum} \leftarrow \text{Enc}(0)$ 
2:  $\text{mean1} \leftarrow \text{mean}(\mathbf{x}, \mathbf{v}), \text{mean2} \leftarrow \text{mean}(\mathbf{y}, \mathbf{v})$ 
3:  $\text{var1} \leftarrow \text{var}(\mathbf{x}, \mathbf{v}), \text{var2} \leftarrow \text{var}(\mathbf{y}, \mathbf{v})$ 
4:  $\text{invstdev1} \leftarrow \text{INVNTHSQRT}(\text{var1}, \text{Enc}(1), 2, 21)$ 
5:  $\text{invstdev2} \leftarrow \text{INVNTHSQRT}(\text{var2}, \text{Enc}(1), 2, 21)$ 
6: for  $i = 0$  to  $N_B - 1$  do
7:    $\text{tmp1} \leftarrow \text{Sub}(\mathbf{x}, \text{mean1}), \text{tmp2} \leftarrow \text{Sub}(\mathbf{y}, \text{mean2})$ 
8:    $\text{tmp} \leftarrow \text{Mult}(\text{tmp1}, \text{tmp2})$ 
9:    $\text{sum} \leftarrow \text{Add}(\text{sum}, \text{Mult}(\text{tmp}, \mathbf{v}))$ 
10: for  $i = 0$  to  $\log_2 M - 1$  do
11:    $\text{sum} \leftarrow \text{Add}(\text{sum}, \text{Rot}(\text{sum}, 2^i))$ 
12:  $\text{corr} \leftarrow \text{Mult}(\text{sum}, \text{Mult}(\text{invstdev1}, \text{invstdev2}))$ 
13: return  $\text{corr}$ 

```

FIG. 29

2900

Algorithm 10 Computing the maximum in a block

```

0: procedure APPROXMAXSLOT(x)
1: max  $\leftarrow$  x
2: for  $i = \log_2 M - 1$  to 0 do
3:   y  $\leftarrow$  Rot(max,  $2^i$ )
4:   z  $\leftarrow$  COMP(max, y)
5:   max  $\leftarrow$  Mult(max, z)
6:   max  $\leftarrow$  Add(max, Rot(max,  $2^i$ ))
7: return max

```

FIG. 30

3000
}

Algorithm 11 Computing the maximum in a whole column of multiple blocks

```

0: procedure APPROXMAX( $\mathbf{x}$ )
1:  $\mathbf{max} \leftarrow \text{APPROXMAXSLOT}(\mathbf{x}_0)$ 
2: for  $i = 1$  to  $N_B - 1$  do
3:    $\mathbf{y} \leftarrow \text{APPROXMAXSLOT}(\mathbf{x}_i)$ 
4:    $\mathbf{z} \leftarrow \text{COMP}(\mathbf{max}, \mathbf{y})$ 
5:    $\mathbf{w} \leftarrow \text{Sub}(\mathbf{1}^M, \mathbf{z})$ 
6:    $\mathbf{max} \leftarrow \text{Mult}(\mathbf{max}, \mathbf{z}), \mathbf{y} \leftarrow \text{Mult}(\mathbf{y}, \mathbf{w})$ 
7:    $\mathbf{max} \leftarrow \text{Add}(\mathbf{max}, \mathbf{y})$ 
8: return  $\mathbf{max}$ 

```

FIG. 31

3100

Algorithm 12 k-percentile function for ordinal variables

```

0: procedure PERCENTILE( $B, \mathbf{v}^{(f_0)}, S_{f_0}, k$ )
1:  $\mathbf{c}_1 \leftarrow \text{Enc}(\mathbf{0}^M)$ 
2: for  $i \leftarrow 1, S_{f_0}$  do
3:    $\mathbf{c}_{\text{tmp}} \leftarrow \mathbf{b}_{i,0}^{(f_0)}$ 
4:   for  $j \leftarrow 1, N_B - 1$  do
5:      $\text{Add}(\mathbf{c}_{\text{tmp}}, \mathbf{b}_{i,j}^{(f_0)}, \mathbf{c}_{\text{tmp}})$ 
6:   for  $j \leftarrow 0, \log_2(M) - 1$  do
7:      $\mathbf{c}_{\text{tmp}} \leftarrow \text{Add}(\mathbf{c}_{\text{tmp}}, \text{Rot}(\mathbf{c}_{\text{tmp}}, 2^j))$ 
8:    $\vec{m} \leftarrow \mathbf{0}^M$ 
9:   for  $j \leftarrow i - 1, S_{f_0} - 1$  do
10:     $\vec{m}(j) \leftarrow 1$ 
11:    $\mathbf{c}_1 \leftarrow \text{Add}(\mathbf{c}_1, \text{Mult}_{evk}(\mathbf{c}_{\text{tmp}}, \vec{m}))$ 
12:  $\mathbf{c}_2 \leftarrow \mathbf{v}_0^{(f_0)}$ 
13: for  $i \leftarrow 1, N_B - 1$  do
14:    $\text{Add}(\mathbf{c}_2, \mathbf{v}_i^{(f_0)}, \mathbf{c}_2)$ 
15: for  $i \leftarrow 0, \log_2(M) - 1$  do
16:    $\mathbf{c}_2 \leftarrow \text{Add}(\mathbf{c}_2, \text{Rot}(\mathbf{c}_2, 2^j))$ 
17:  $\mathbf{c}_2 \leftarrow \text{INVNTHSQRT}(\mathbf{c}_2, \text{Enc}(\mathbf{1}^M), 1, 25)$ 
18:  $\mathbf{c}_1 \leftarrow \text{Mult}(\mathbf{c}_1, \mathbf{c}_2)$ 
19:  $\mathbf{c}_1 \leftarrow \text{APPROXSIGN}(\text{Sub}(\mathbf{c}_1, \frac{k}{100}))$ 
     $\triangleright$  operate  $f(x) = -0.5(x - 0.5)^2 + 1.125$ 
20:  $\mathbf{c}_1 \leftarrow \text{Square}_{evk}(\text{Sub}(\mathbf{c}_1, 0.5))$ 
21:  $\mathbf{c}_1 \leftarrow \text{Add}(\text{Mult}(\mathbf{c}_1, -0.5), 1.125)$ 
     $\triangleright$  find  $l$  s.t.  $l$ -th to  $S_{f_0}$ -th slots have 1 as value
22: for  $j \leftarrow 0, \log_2(M) - 1$  do
23:    $\mathbf{c}_1 \leftarrow \text{Add}(\mathbf{c}_1, \text{Rot}(\mathbf{c}_1, 2^j))$ 
24:  $\mathbf{c}_1 \leftarrow \text{Negate}(\mathbf{c}_1)$ 
25:  $\mathbf{c}_1 \leftarrow \text{Add}(\mathbf{c}_1, S_{f_0} + 1)$ 
26: return  $\mathbf{c}_1$ 

```

FIG. 32

