

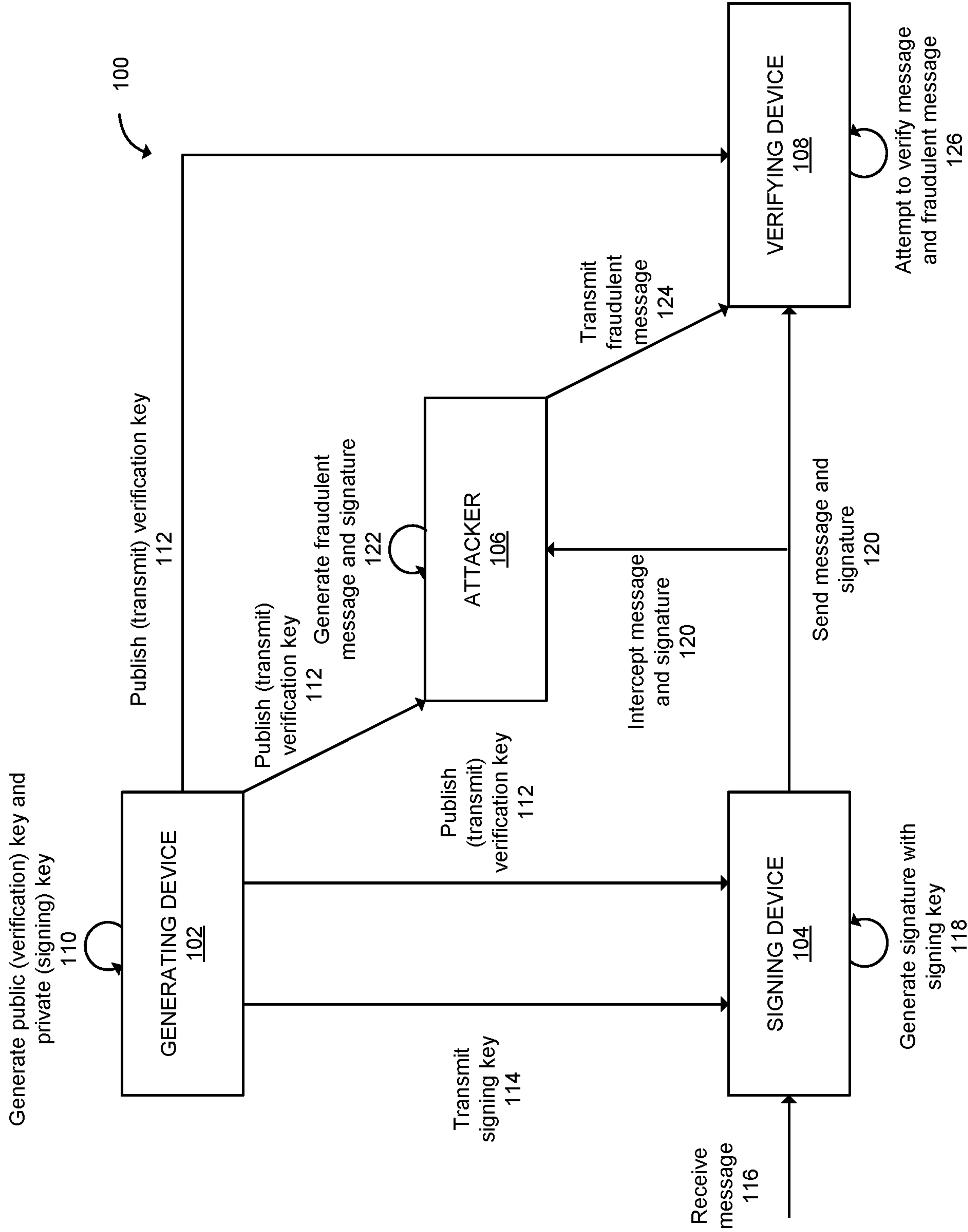
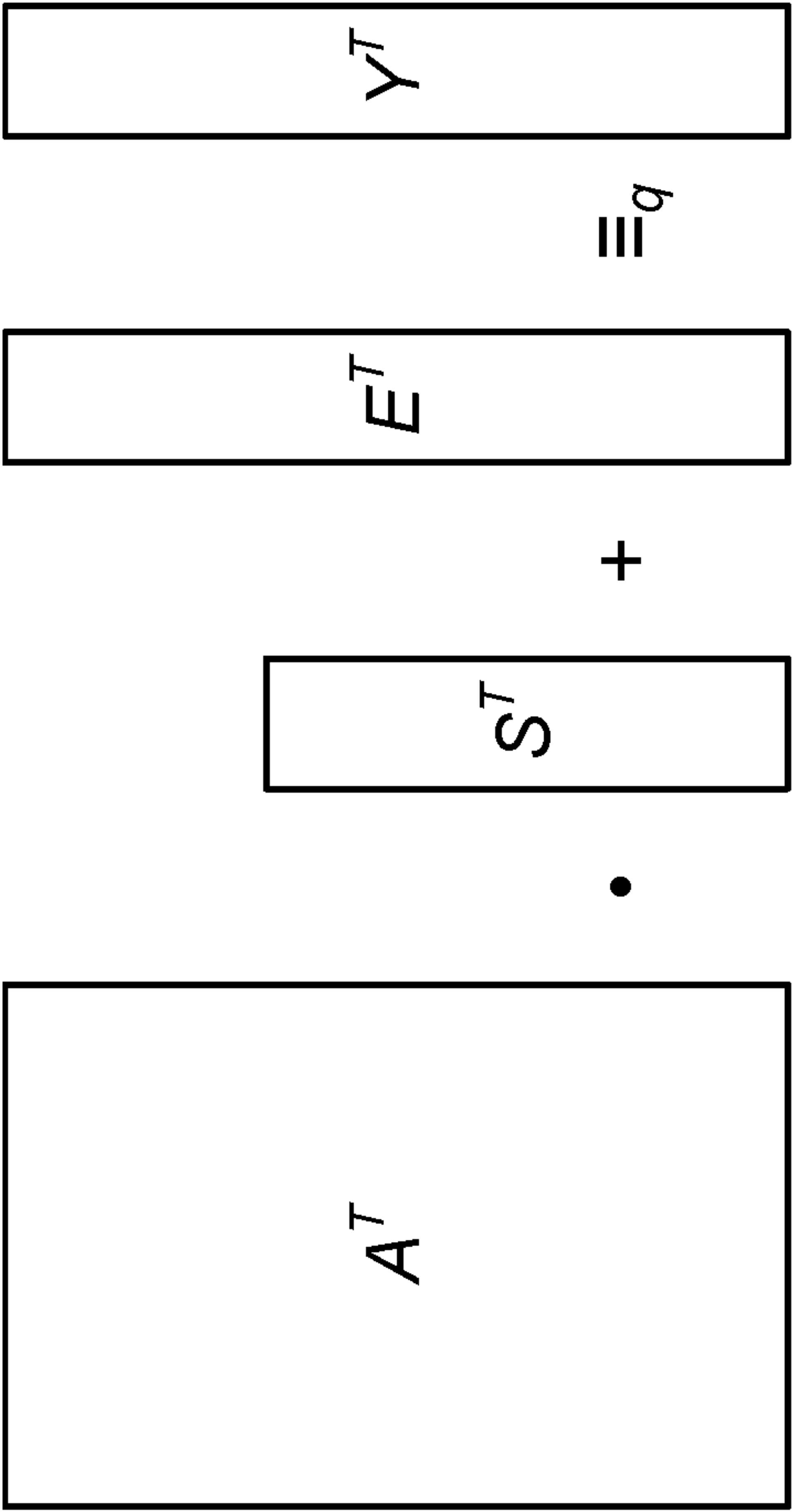


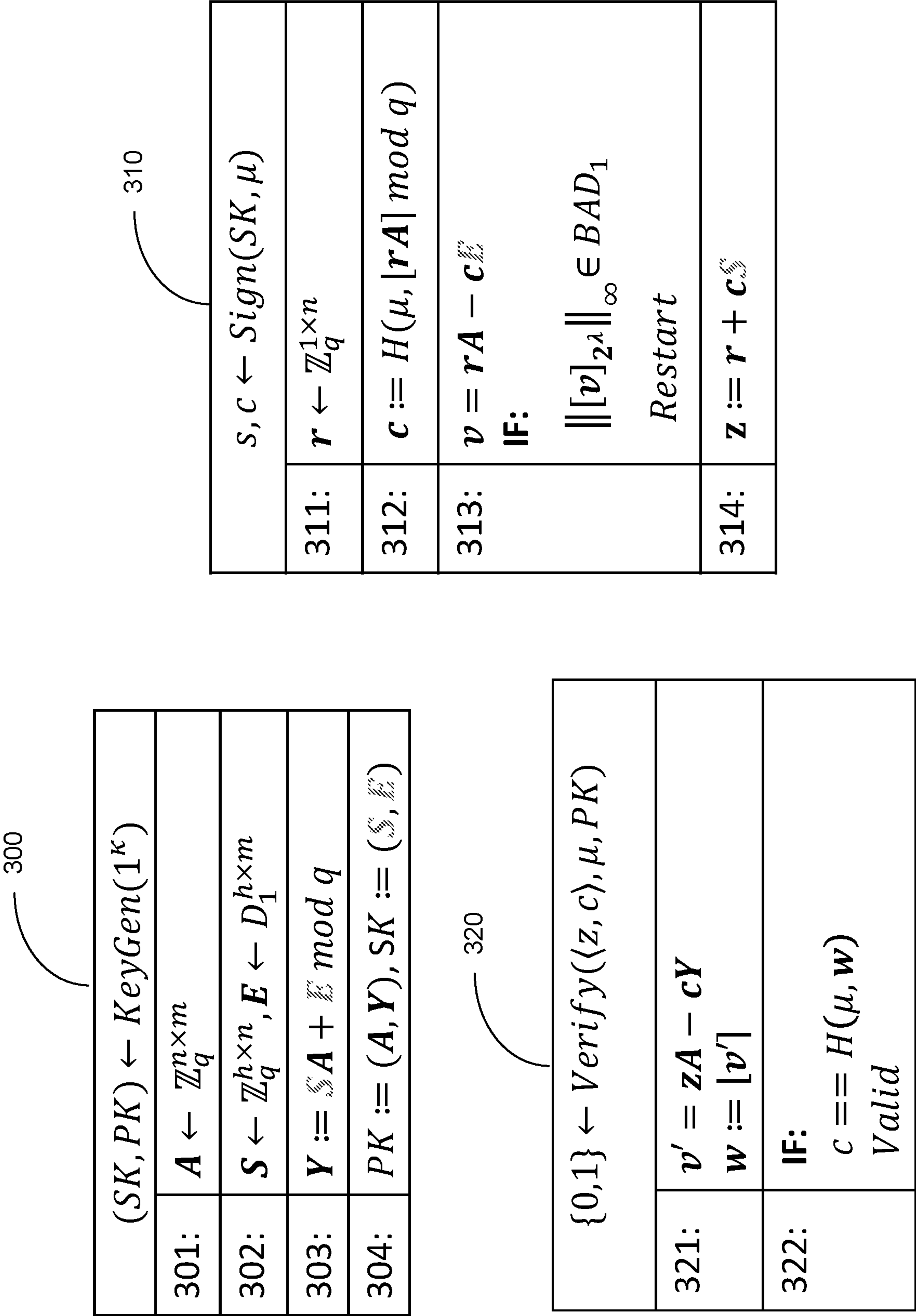
FIG. 1

LWE Problem



SEARCH: Given (A, Y) find S or E
DECISION: Given (A, Y) , decide if LWE sample or Random

FIG. 2



321:

322:

$\{0,1\} \leftarrow \text{Verify}(\langle z, c \rangle, \mu, PK)$

$v' = zA - cY$
 $w := \lfloor v' \rfloor$

IF:
 $c == H(\mu, w)$
Valid

FIG. 3

4/8

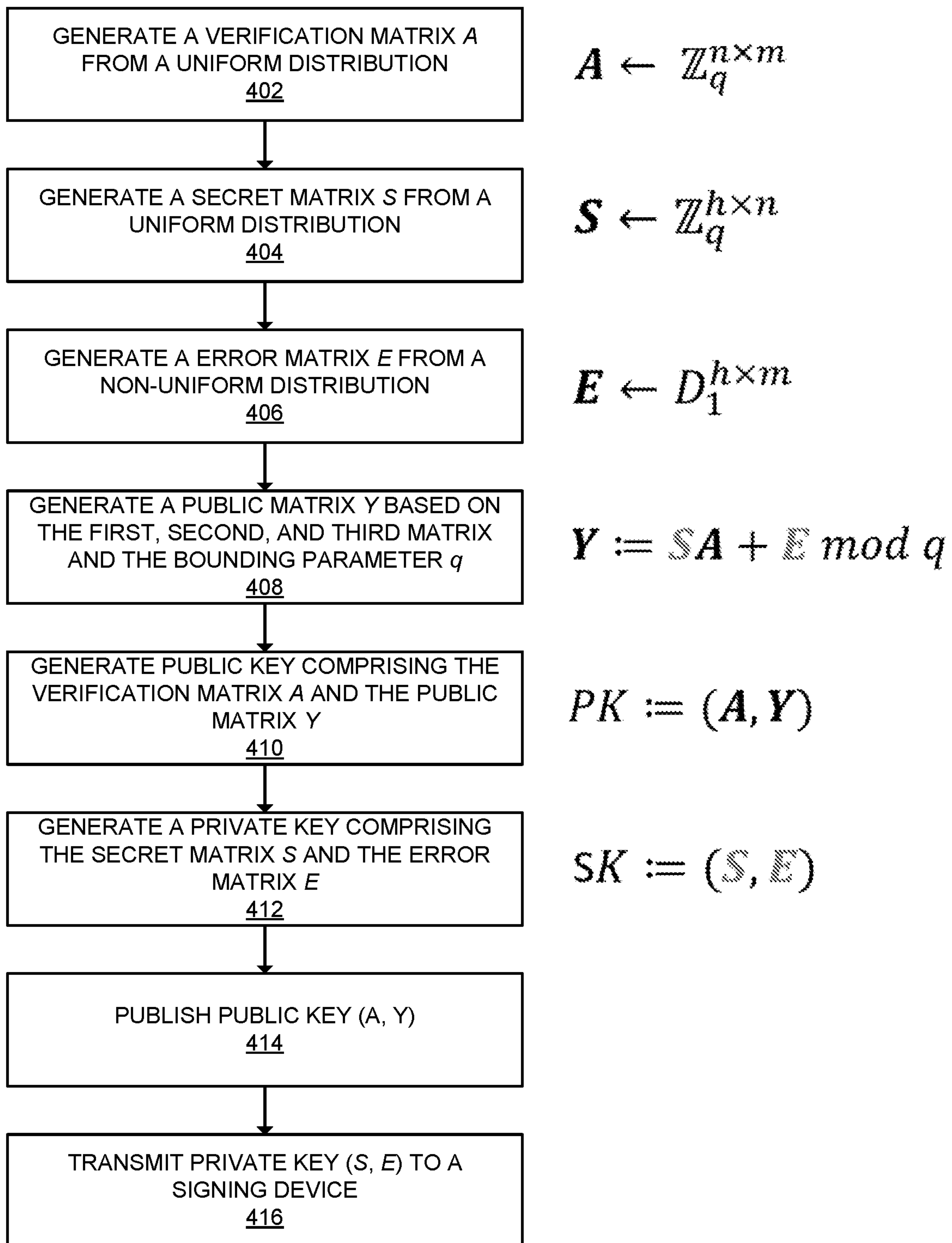


FIG. 4

5/8

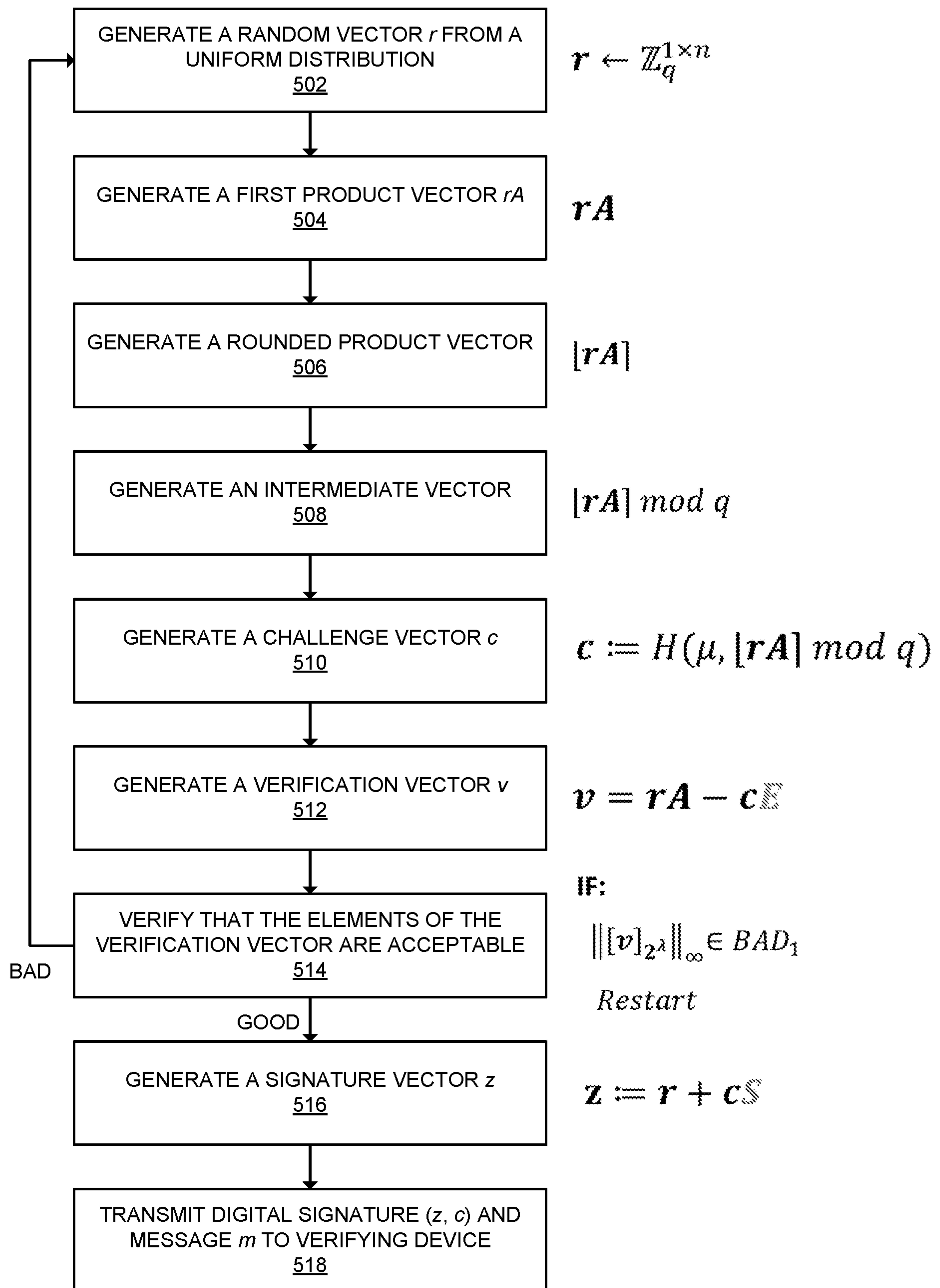


FIG. 5

6/8

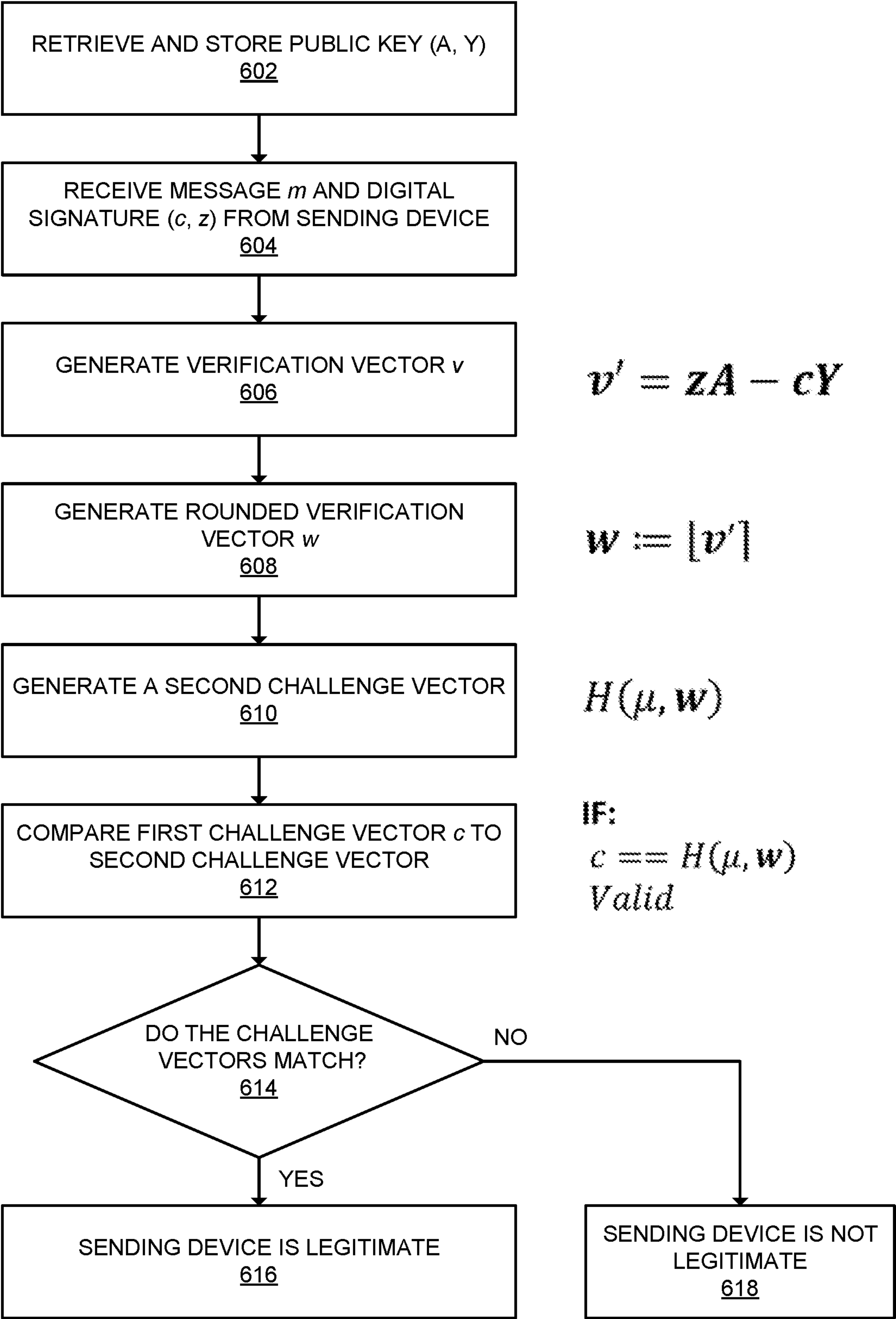


FIG. 6

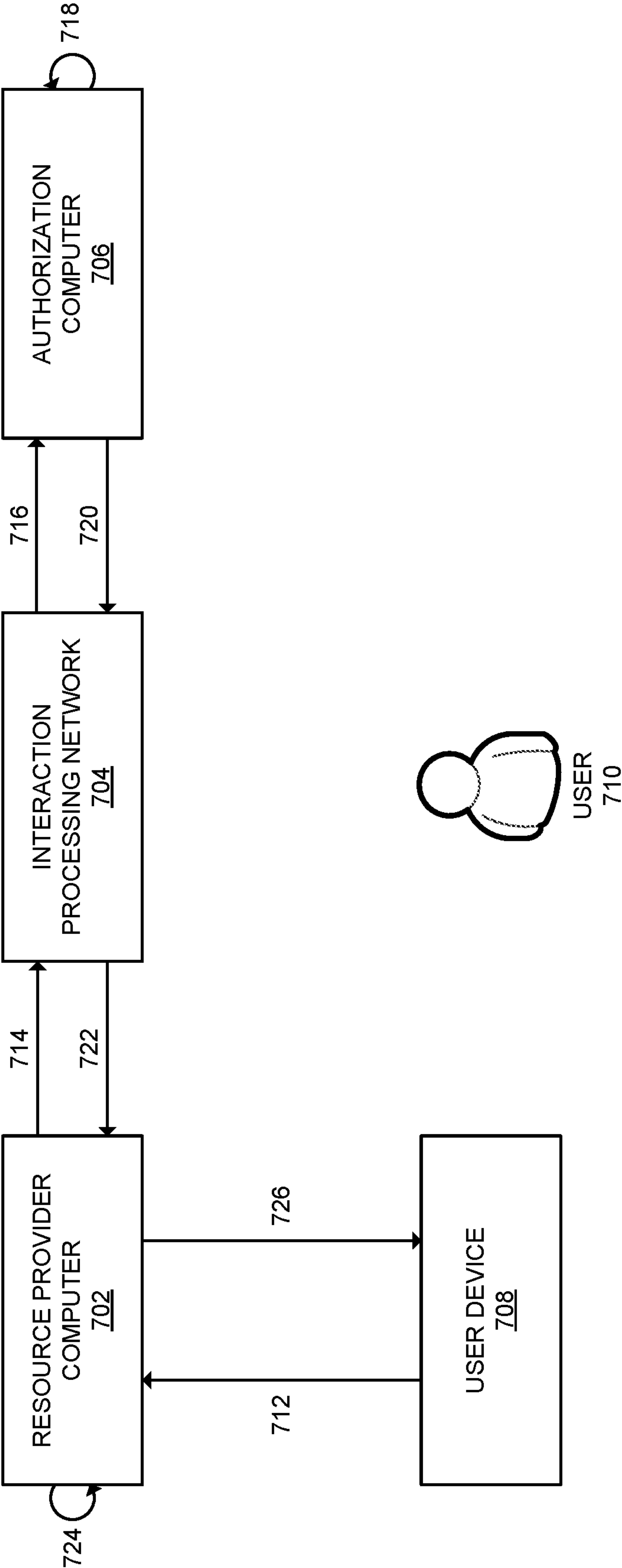


FIG. 7

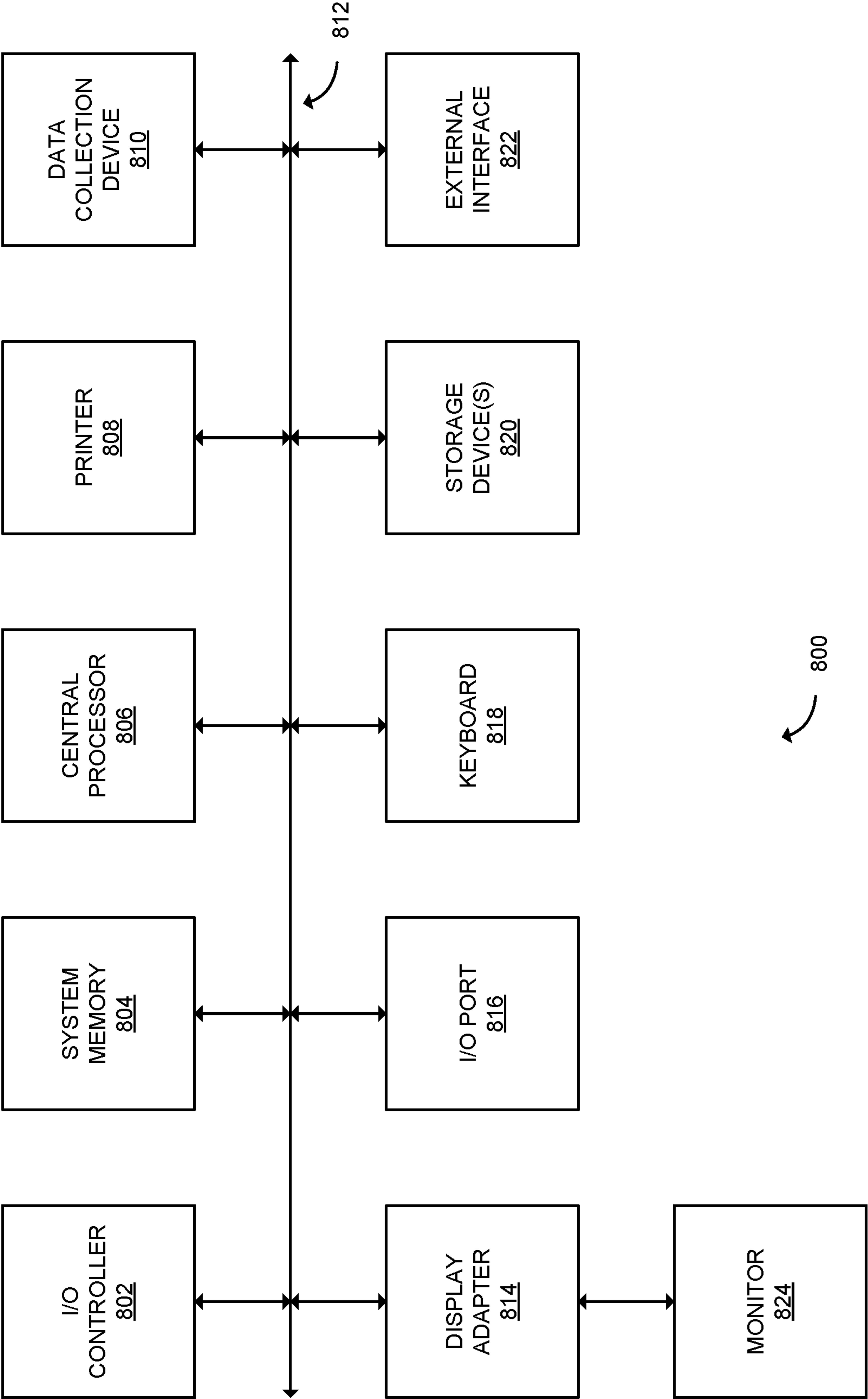


FIG. 8