

DRAWINGS

FIG. 1

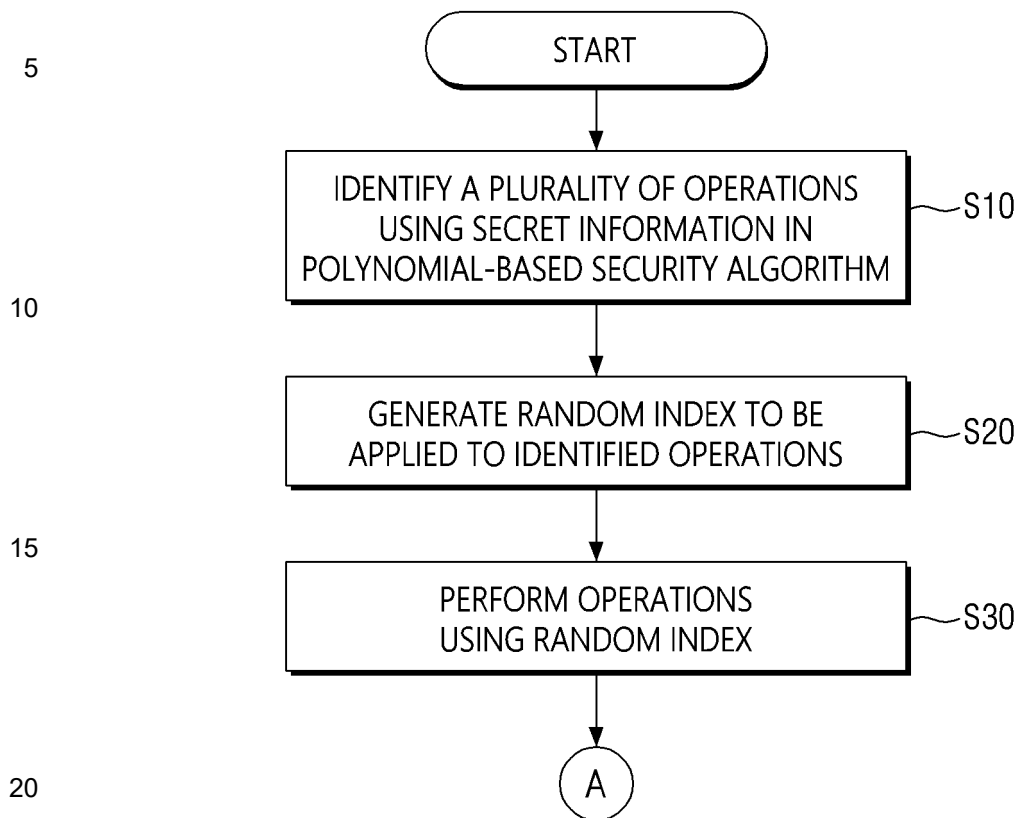


FIG. 2

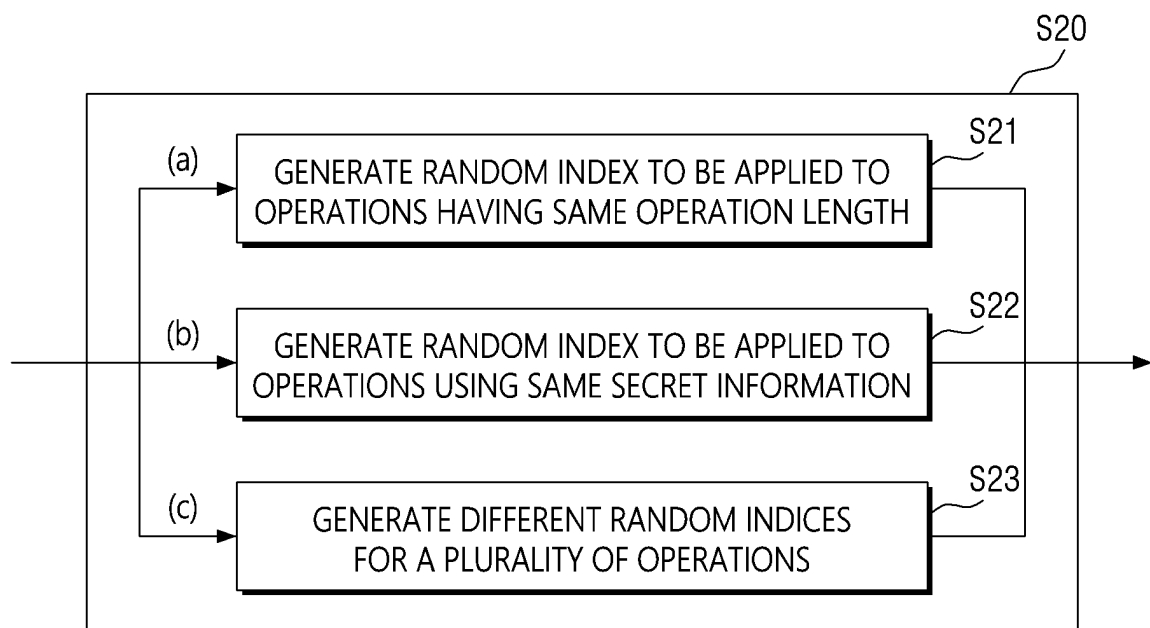


FIG. 3

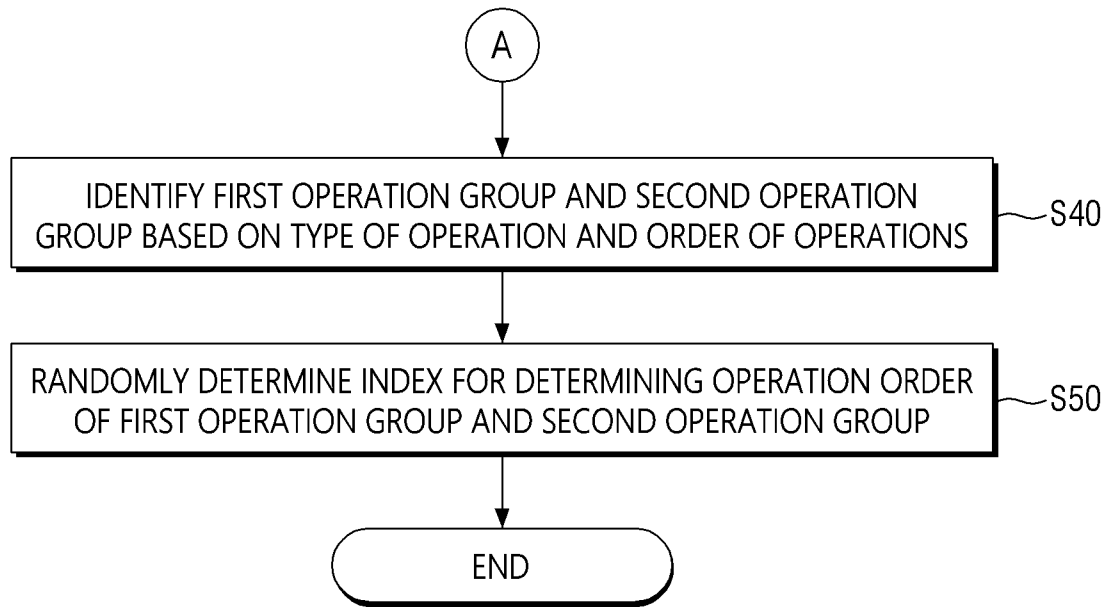


FIG. 4

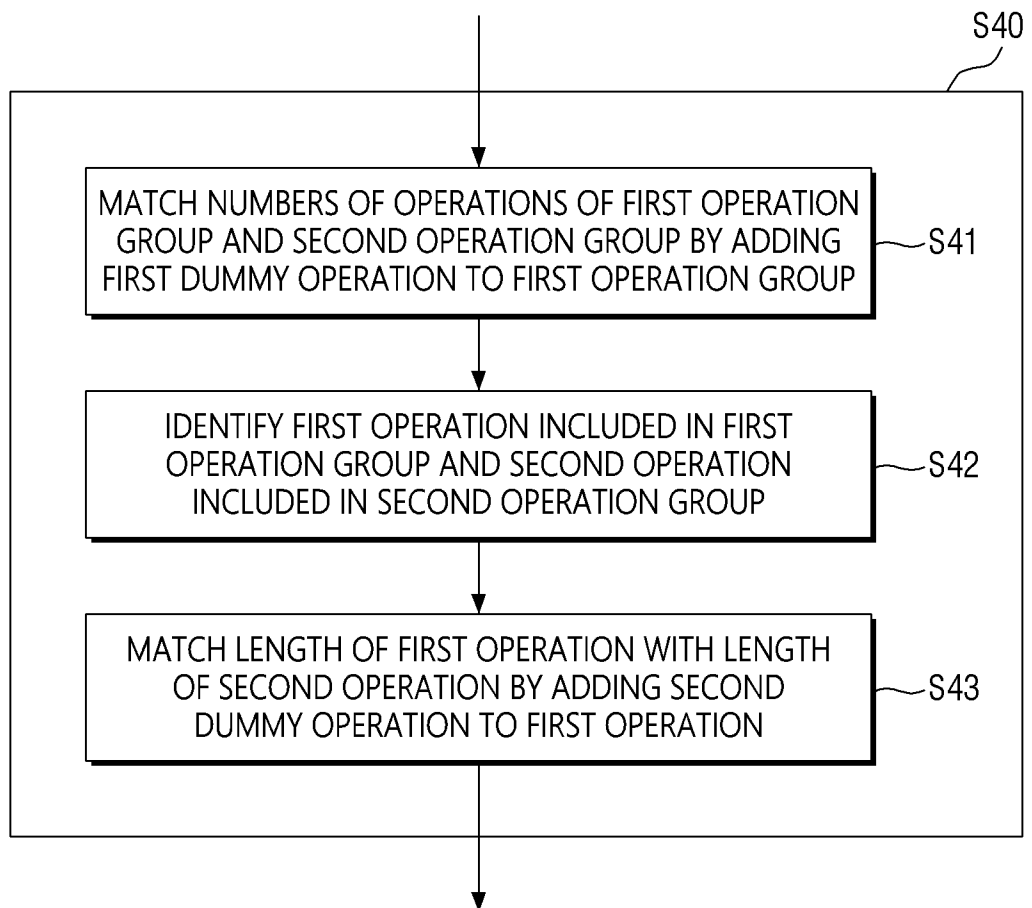


FIG. 5

50

```

5      Key Generation
In      -
Out      $(pk = (\rho, \mathbf{t}_1), sk = (\rho, K, tr, \mathbf{s}_1, \mathbf{s}_2, \mathbf{t}_0))$ 
01       $\zeta \leftarrow \{0, 1\}^{256}$ 
02       $(\rho, \varsigma, K) \in \{0, 1\}^{256 \times 3} := H_1(\zeta)$ 
03       $(\mathbf{s}_1, \mathbf{s}_2) \in S_\eta^l \times S_\eta^k := H_2(\varsigma)$ 
04       $\mathbf{A} \in R_q^{k \times l} := \text{ExpandA}(\rho)$  ▷  $\mathbf{A}$  is generated and stored in NTT representation as  $\hat{\mathbf{A}}$ 
05       $\hat{\mathbf{s}}_1 := \text{NTT}(\mathbf{s}_1)$ 
10     06       $\mathbf{t} := \hat{\mathbf{A}} \cdot \hat{\mathbf{s}}_1$ 
07       $\mathbf{t} := \text{NTT}^{-1}(\mathbf{t})$ 
08       $\mathbf{t} := \mathbf{t} + \mathbf{s}_2$ 
09       $(\mathbf{t}_1, \mathbf{t}_0) := \text{Power2Round}_q(\mathbf{t}, d)$ 
10     10       $tr \in \{0, 1\}^{384} := \text{CRH}(\rho \parallel \mathbf{t}_1)$ 
11     11      return  $(pk = (\rho, \mathbf{t}_1), sk = (\rho, K, tr, \mathbf{s}_1, \mathbf{s}_2, \mathbf{t}_0))$  ▷ Pack( $sk$ ) and return
15

```

FIG. 6

61 OPERATION POSITION	62 TARGET VARIABLE	63 NUMBER OF OPERATION REPETITIONS	NOTE
03. $(s_1, s_2) : H_2(s)$	s_1	$l \times n$	
	s_2	$k \times n$	
05. $\hat{s}_1 := \text{NTT}(s_1)$	s_1	$l \times (n/2)$	
06. $t := \hat{A} \cdot \hat{s}_1$	s_1	$k \times l \times n$	Multiplication
		$k \times n$	Reduction
07. $t := \text{NTT}^{-1}(t)$	s_1	$k \times \{(n/2) + n\}$	
08. $t := t + s_2$	s_2, s_1	$k \times n$	Addition
		$k \times n$	Reduction
09. $(t_1, t_0) := \text{Power2Round}_q(t, d)$	t_0, s_2, s_1	$k \times n$	

FIG. 7

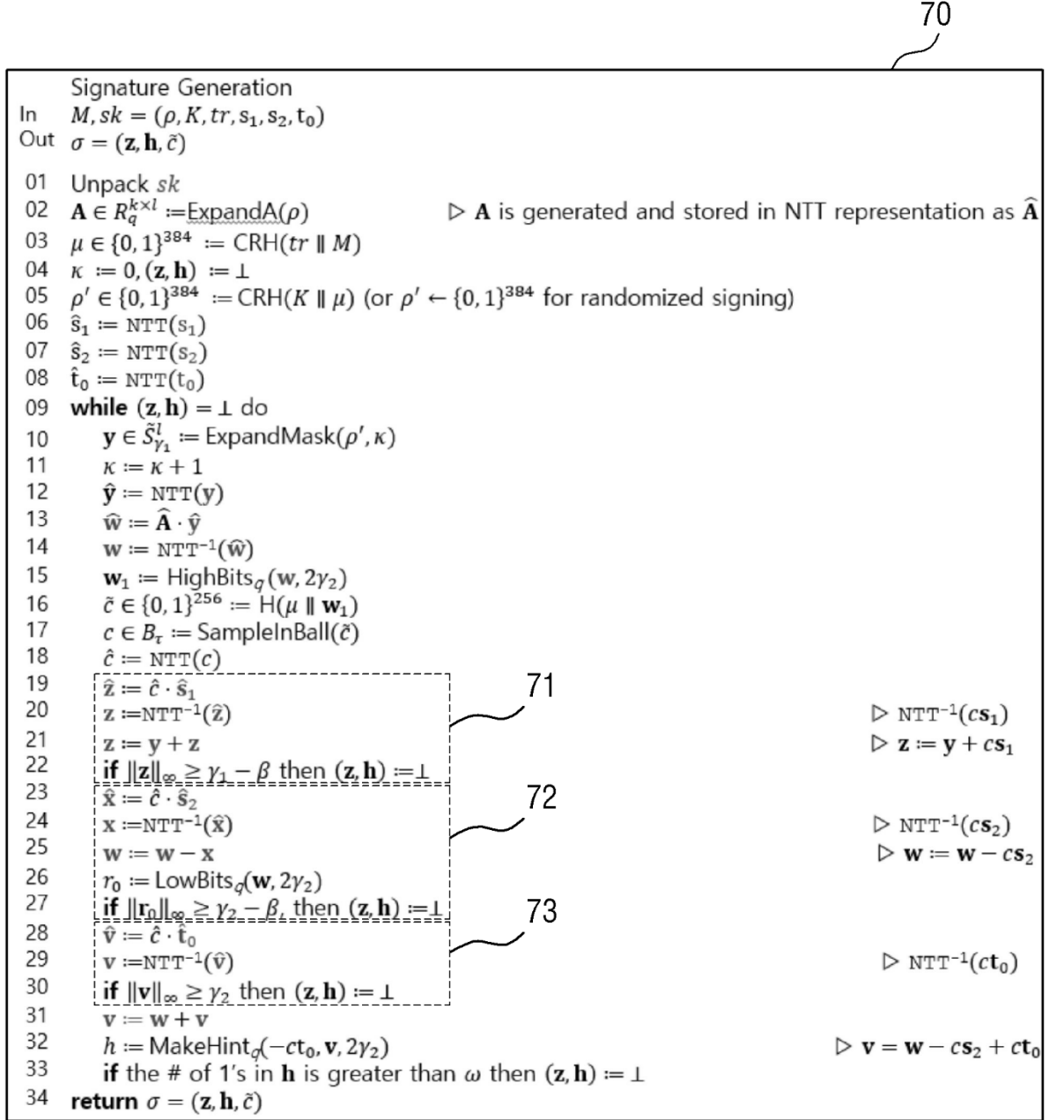


FIG. 8

81 OPERATION POSITION	82 TARGET VARIABLE	83 NUMBER OF OPERATION REPETITIONS	NOTE
06. $\hat{s}_1 := \text{NTT}(s_1)$	s_1	$l \times (n/2)$	
07. $\hat{s}_2 := \text{NTT}(s_2)$	s_2	$k \times (n/2)$	
08. $\hat{t}_0 := \text{NTT}(t_0)$	t_0	$k \times (n/2)$	
10. $y := \text{ExpandMask}(p', k)$	y	$l \times (n/4)$	$l \times (n/2)$ (Dilithium3, Dilithium5)
12. $\hat{y} := \text{NTT}(y)$	y	$l \times (n/2)$	
13. $\hat{w} := \hat{A} \cdot \hat{y}$	y	$k \times l \times n$	Multiplication
		$k \times n$	Reduction
14. $w := \text{NTT}^{-1}(\hat{w})$	y	$k \times \{(n/2) + n\}$	

FIG. 9

OPERATION POSITION	TARGET VARIABLE	NUMBER OF OPERATION REPETITIONS	NOTE
15. $w_1 := \text{HighBits}_q(w, 2r_2)$	y	$k \times n$	Reduction
		$k \times n$	Decompose
19. $\hat{z} := \hat{c} \cdot \hat{s}_1$	s_1	$l \times n$	
20. $z := \text{NTT}^{-1}(\hat{z})$	s_1	$l \times \{(n/2)+n\}$	
21. $z := y + z$	s_1, y	$l \times n$	Addition
		$l \times n$	Reduction
23. $\hat{z} := \hat{c} \cdot \hat{s}_2$	s_2	$k \times n$	
24. $x := \text{NTT}^{-1}(\hat{x})$	s_2	$k \times \{(n/2)+n\}$	
25. $w := w - x$	s_1, s_2	$k \times n$	Subtraction
		$k \times n$	Reduction
28. $\hat{v} := \hat{c} \cdot \hat{t}_0$	t_0	$k \times n$	
29. $v := \text{NTT}^{-1}(\hat{v})$	t_0	$k \times \{(n/2)+n\}$	Inverse NTT
		$k \times n$	Reduction
31. $v := w + v$	t_0, s_2, y	$k \times n$	
32. $h := \text{MakeHint } l(-ct_0, v, 2y_2)$	t_0, s_2, y	$k \times n$	

FIG. 10

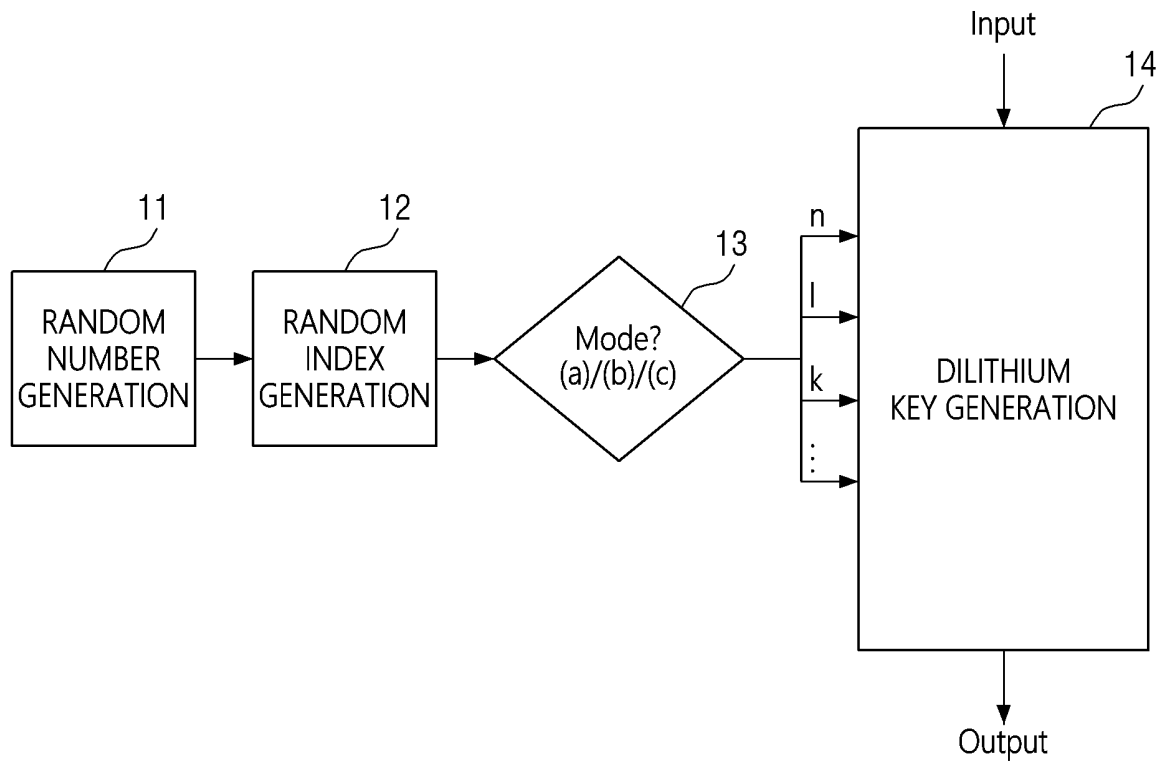


FIG. 12

