DRAWINGS

FIG. 1

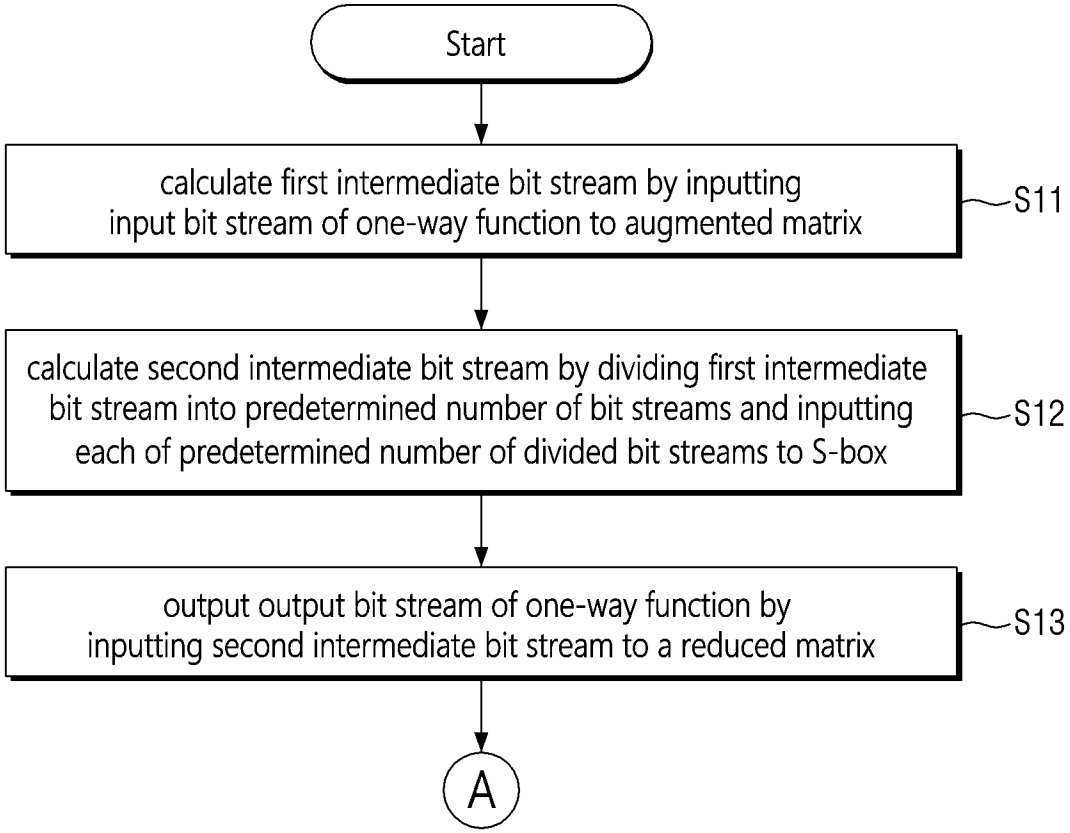


FIG. 2

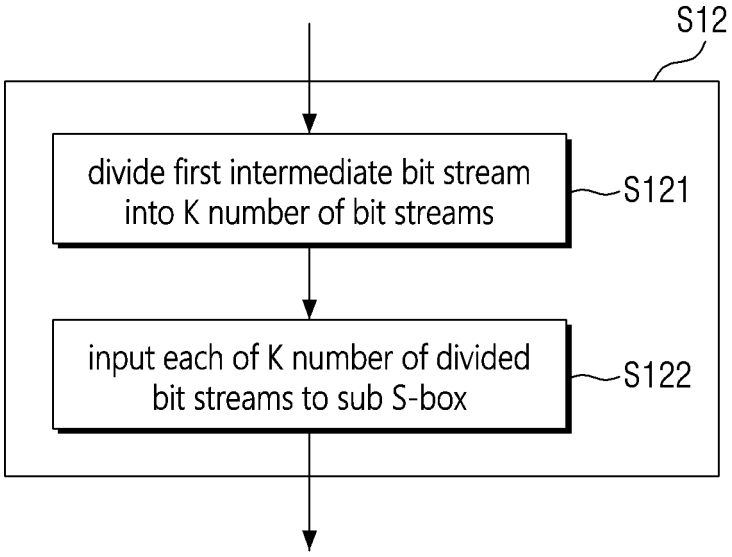

S12
divide first intermediate bit stream into K number of bit streams
S121
input each of K number of divided bit streams to sub S-box
S122

FIG. 3

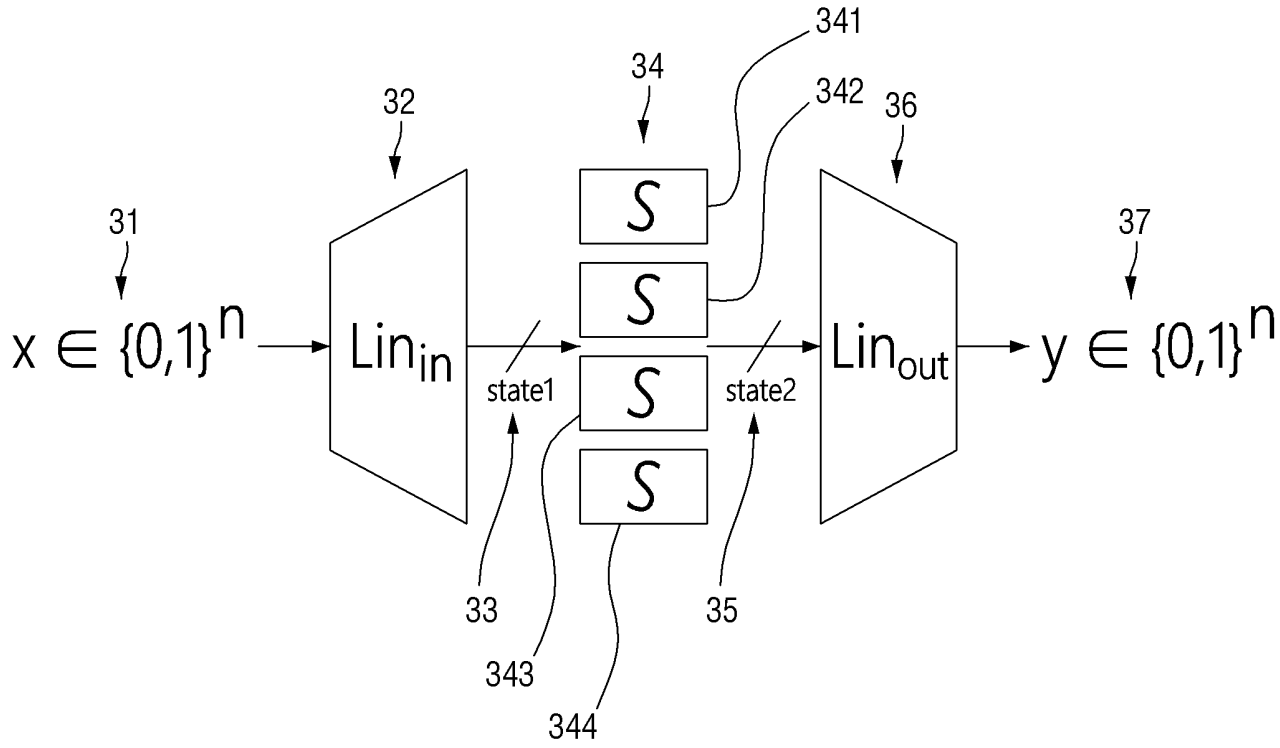

341
34
342
32
36
31
37
S
S
S
S
$x \in \{0,1\}^n$
Lin_{in}
state1
state2
Lin_{out}
$y \in \{0,1\}^n$
33
35
343
344

FIG. 4

31 $\mathbf{x} \in \{0,1\}^{\mathbf{n}}$

33 $\mathbf{state}_1 = \mathbf{Lin}_{\mathbf{in}} \cdot \mathbf{x} \in \{0,1\}^{\mathbf{m}}$

331 $\mathbf{state}_1 = (u_1, \cdots, u_{m/\ell}) \in \{0,1\}^{\ell \cdot (\frac{\mathbf{m}}{\ell})}, \quad u_i \in \{0,1\}^{\ell}$

35 $\mathbf{state}_2 = (v_1, \cdots, v_{m/\ell}) \in \{0,1\}^{\mathbf{m}}, \quad v_i = S(u_i) \in \{0,1\}^{\ell}$

37 $\mathbf{y} = \mathbf{Lin}_{\mathbf{out}} \cdot \mathbf{state}_2 \in \{0,1\}^{\mathbf{n}}$

FIG. 5

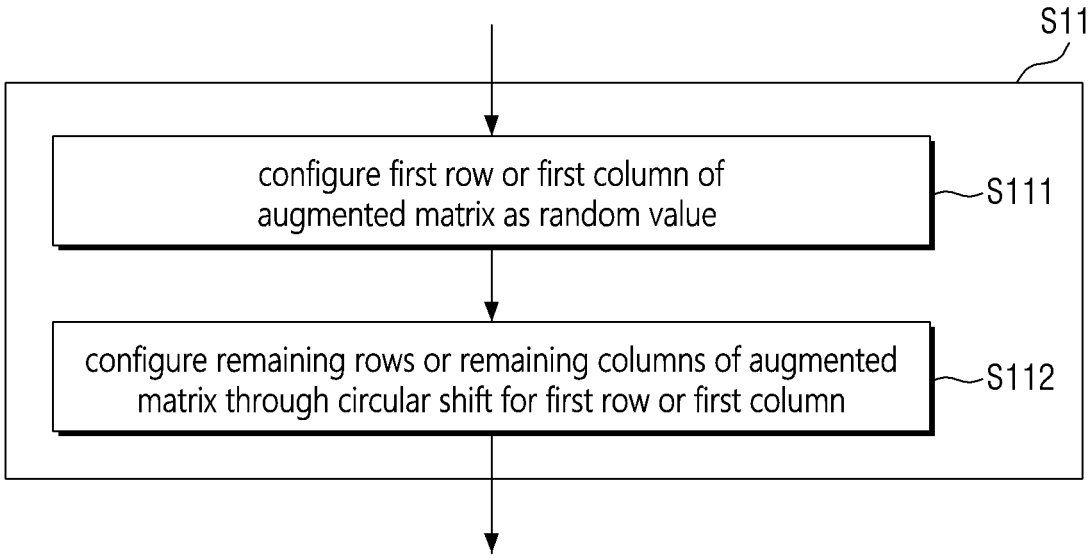

S11
configure first row or first column of augmented matrix as random value
S111
configure remaining rows or remaining columns of augmented matrix through circular shift for first row or first column
S112

FIG. 6

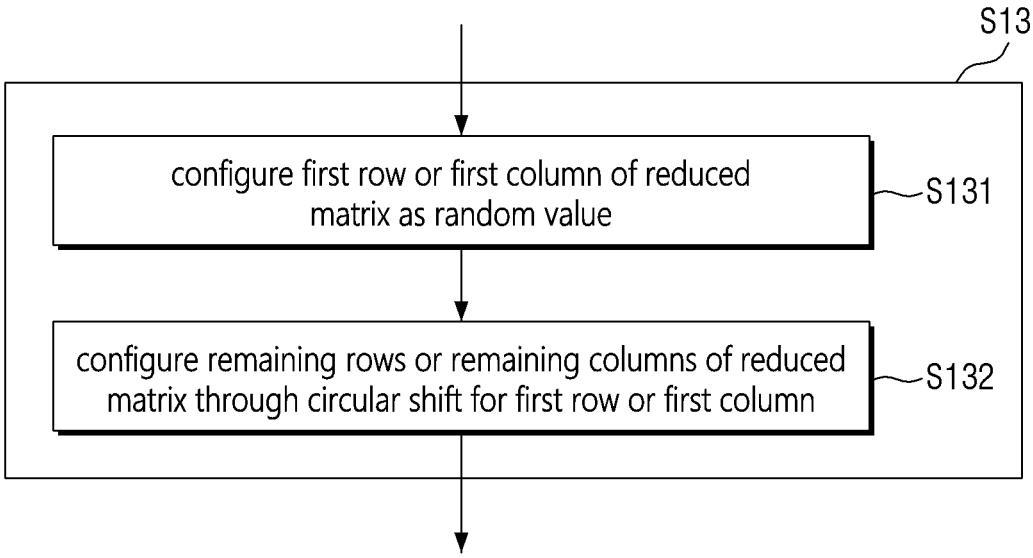

S13
configure first row or first column of reduced matrix as random value
S131
configure remaining rows or remaining columns of reduced matrix through circular shift for first row or first column
S132

FIG. 7

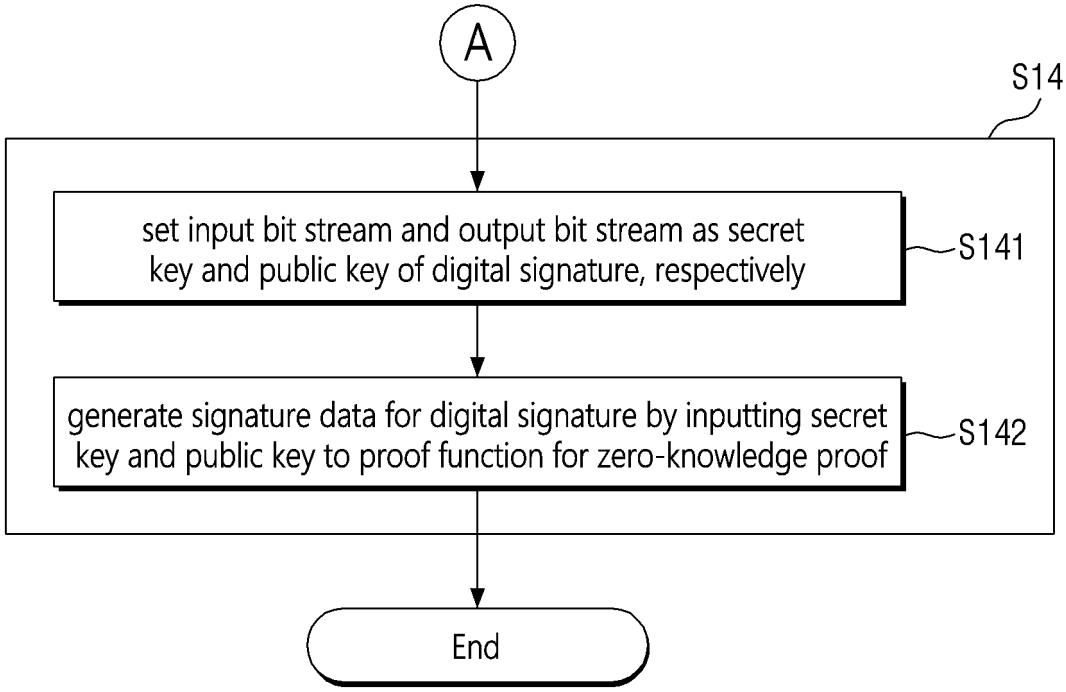

A
S14
set input bit stream and output bit stream as secret key and public key of digital signature, respectively
S141
generate signature data for digital signature by inputting secret key and public key to proof function for zero-knowledge proof
S142
End

FIG. 8

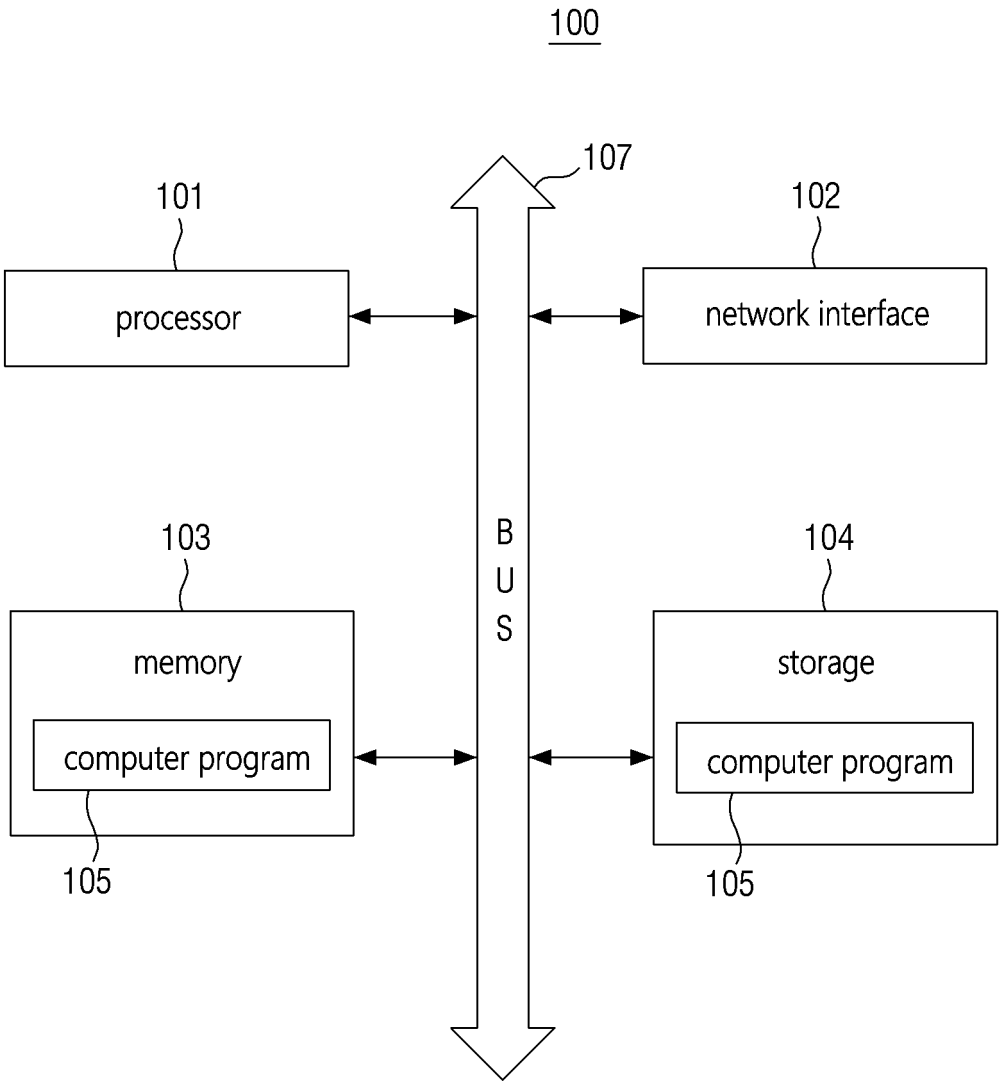
81 $\mathbf{L} = \{(\mathbf{y}, \mathbf{x})' : \mathbf{x} \leftarrow \{0,1\}^{\mathbf{n}}, \mathbf{y} = \mathbf{F}(\mathbf{x})\}$

82 $\mathbf{KeyGen}(\mathbf{1}^{\lambda}) \rightarrow (\boldsymbol{pk}, \boldsymbol{sk}), \quad \mathbf{pk} = \mathbf{y} = \mathbf{F}(\mathbf{x}), \ \mathbf{sk} = \mathbf{x}$

83 $\mathbf{Sign}(\mathbf{sk}, \mathbf{m}) \rightarrow \boldsymbol{\sigma}, \quad \boldsymbol{\sigma} = \boldsymbol{\pi} \leftarrow \mathbf{ZK.Prove}(\boldsymbol{pk}, \boldsymbol{sk}); \boldsymbol{m})$

84 $\mathbf{Verify}(\mathbf{pk}, \boldsymbol{\sigma}) \rightarrow 0 \ \mathbf{or} \ 1, \quad 0 \ \mathbf{or} \ 1 \leftarrow \mathbf{ZK.Verify}(\mathbf{pk}, \boldsymbol{\pi})$

FIG. 9


100
107
101
processor
102
network interface
103
memory
computer program
105
B
U
S
104
storage
computer program
105