

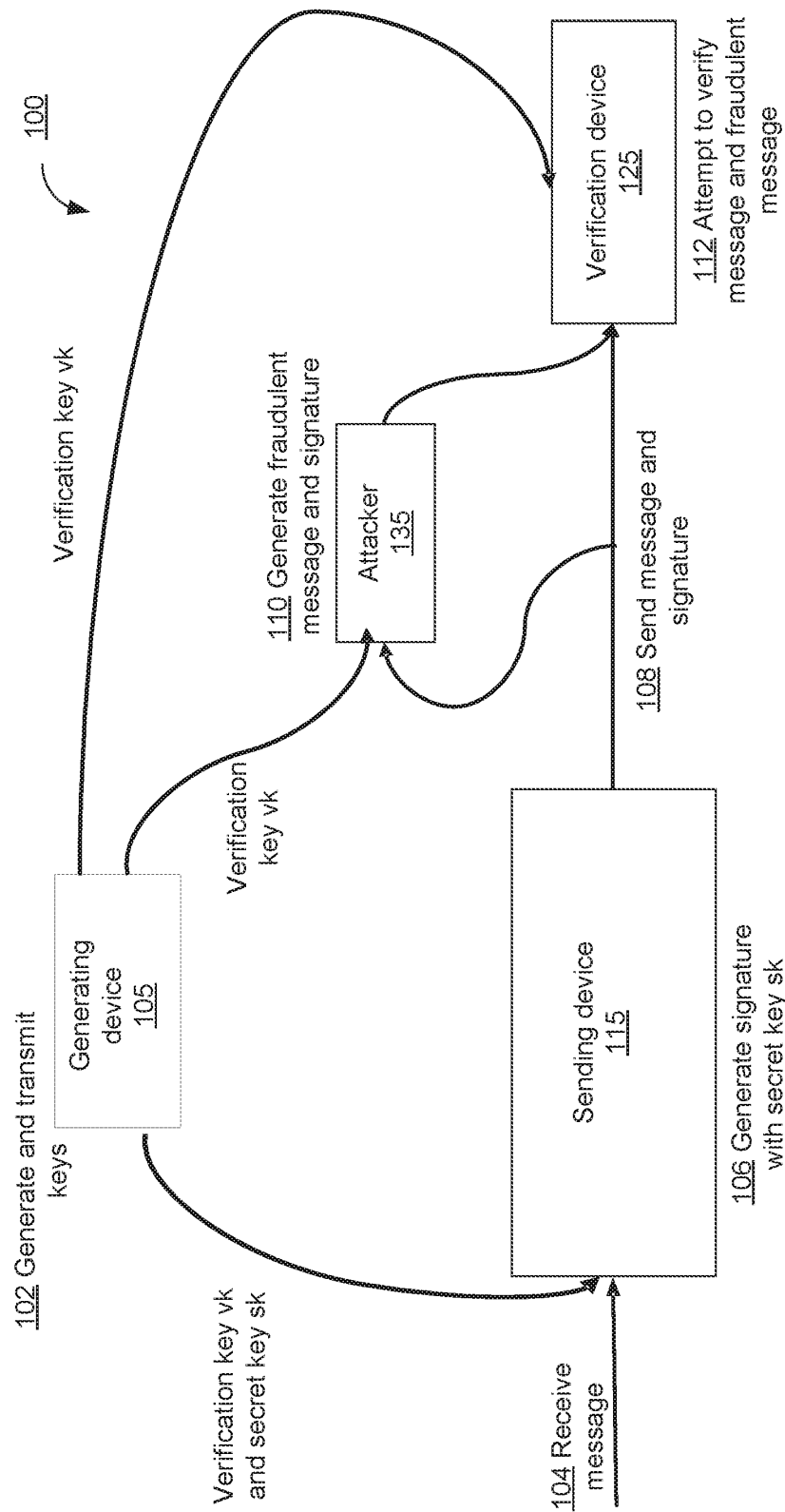


FIG. 1

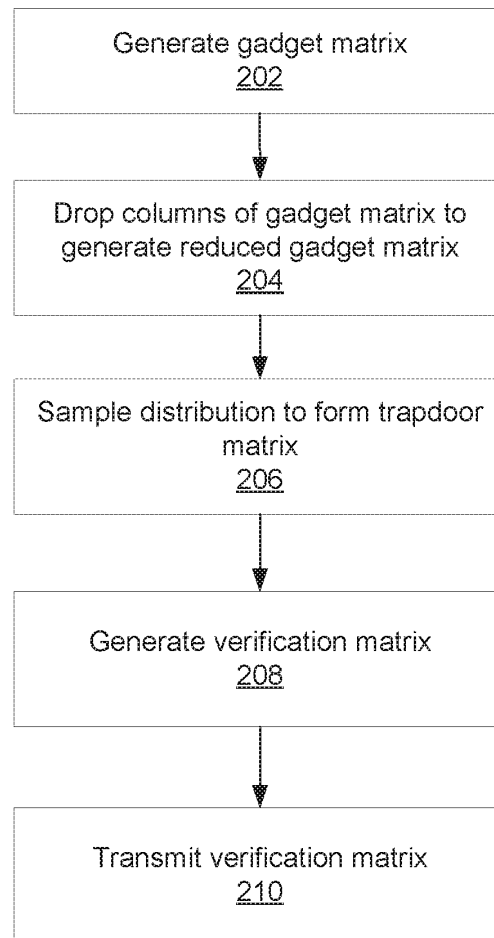


FIG. 2

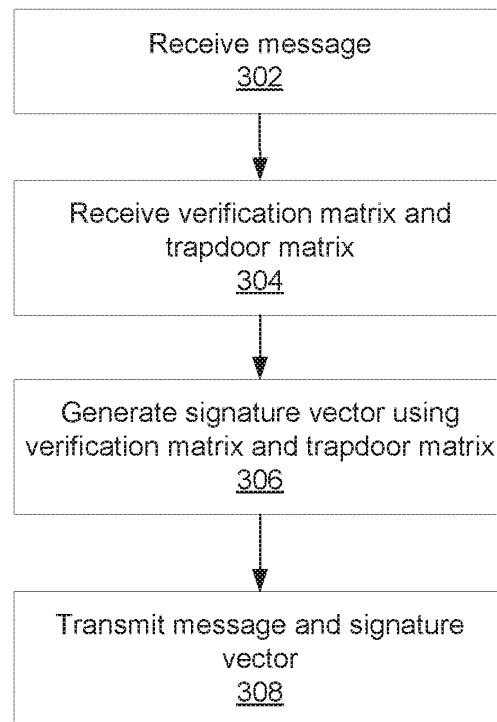


FIG. 3

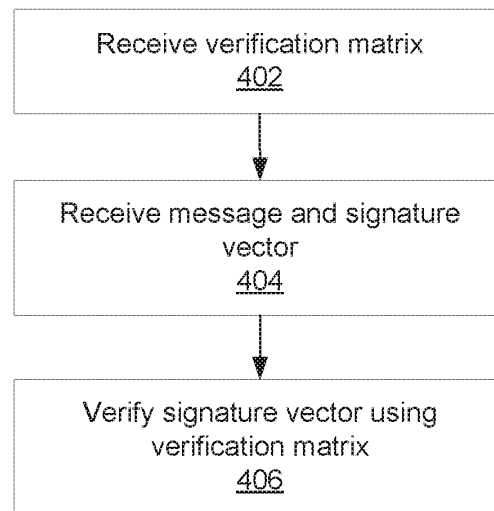


FIG. 4

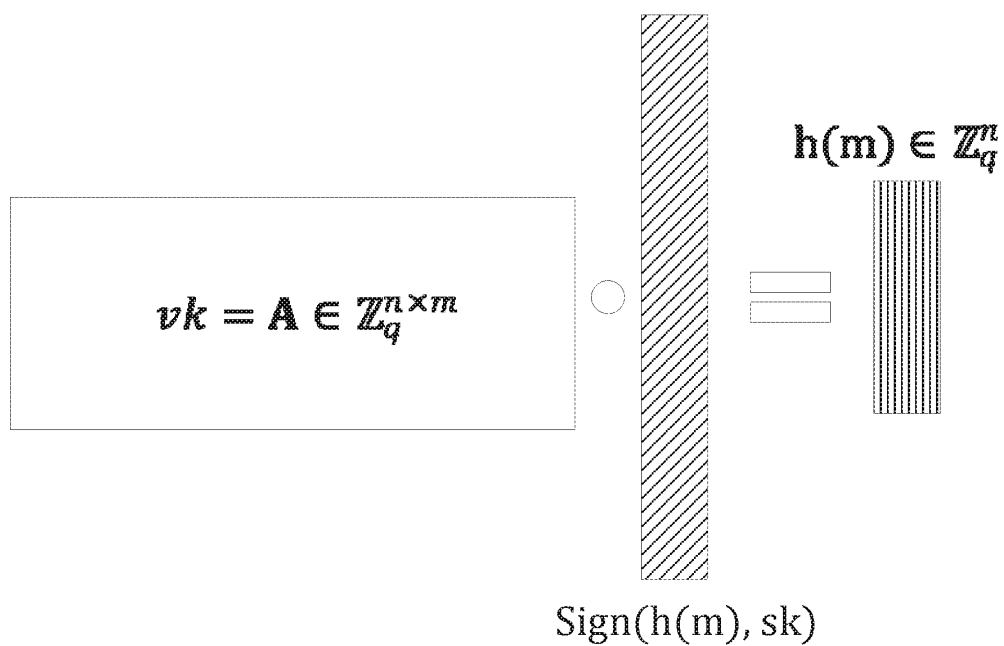


FIG. 5A

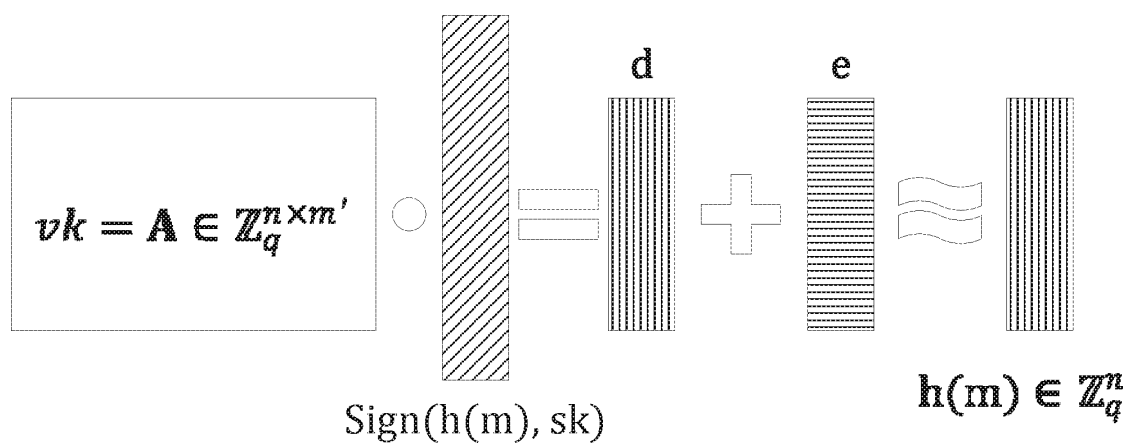


FIG. 5B

Params	Exact	Approx	Approx	Exact	Approx	Approx	Exact	Approx	Approx
n	512	512	512	512	512	512	512	512	512
$\lceil \log_2 q \rceil$	24	24	24	16	16	16	16	16	16
b	2	2	2	2	2	2	4	4	4
l	0	12	15	0	7	9	0	2	4
τ	40	40	40	2.6	2.6	2.6	2.6	2.6	2.6
s	38317.0	29615.3	26726.3	2170.7	1756.3	1618.2	3114.2	2833.3	2505.6
m	13312	7168	5632	9216	5632	4608	5120	4096	3072
$\ x\ _2$	4441737.7	2521387.0	2035008.5	211100.9	133305.5	109339.1	223740.1	183004.9	138145.7
$\ z\ _2$	0	374014.0	2118987.6	0	11897.9	46428.4	0	1402.3	19807.1
PK	37.50	19.50	15.00	17.00	10.00	8.00	9.00	7.00	5.00
Sig	25.68	13.53	10.51	13.16	7.83	6.30	7.62	5.94	4.45
LWE	100.0	100.0	100.0	104.7	104.7	104.7	104.7	104.7	104.7
AISIS	92.3	97.6	93.1	95.6	100.6	99.8	94.8	97.3	99.5

Summary of the concrete parameters. The size of PK and Sig are measured in kB. $\|x\|_2$, $\|z\|_2$ are the upper-bounds of the norms of the preimage and the error term. LWE and AISIS refer to the estimations of security levels for the pseudorandomness of the PK and finding a short approximate preimage.

FIG. 6

Algorithm 1: GSAMP.CUT(v, σ)**Input:** $v \in \mathbb{Z}_q, \sigma \in \mathbb{R}^+$ **Output:** $z \in \mathbb{Z}^{k-l}$

701 Sample $x \in \mathbb{Z}^k$ from $D_{\Lambda_q^\perp(\mathbf{g}^t), \sigma}$
 702 Let z be the last $k - l$ entries of x
 703 return z .

Algorithm 2: APPROX.TRAPGEN(λ)_X**Input:** Security parameter λ **Output:** matrix-approximate trapdoorpair $(\mathbf{A}, \mathbf{R})$.

711 Sample a uniformly random

 $\hat{\mathbf{A}} \leftarrow U(\mathbb{Z}_q^{n \times n})$.712 Let $\bar{\mathbf{A}} := [\mathbf{I}_n, \hat{\mathbf{A}}]$.

713 Sample the approximate trapdoor

 $\mathbf{R} \leftarrow \chi^{2n \times w}$.714 Form $\mathbf{A} := [\bar{\mathbf{A}}|\mathbf{F} - \bar{\mathbf{A}}\mathbf{R}] \in \mathbb{Z}_q^{n \times m}$.
return $(\mathbf{A}, \mathbf{R})$.**Algorithm 3:** APPROX.SAMPLEPRE($\mathbf{A}, \mathbf{R}, \mathbf{u}, s$).**Input:** $(\mathbf{A}, \mathbf{R}, \mathbf{u}, s)$ as in Theorem 4.1.**Output:** An approximate preimage of $\mathbf{u}$
for $\mathbf{A}, \mathbf{y} \in \mathbb{Z}^m$.721 Sample a perturbation $\mathbf{p} \leftarrow D_{\mathbb{Z}^m, \sqrt{\Sigma_p}}$.722 Form $\mathbf{v} = \mathbf{u} - \mathbf{A}\mathbf{p} \in \mathbb{Z}_q^n$.

723 Sample the approximate gadget

preimage $\mathbf{z} \in \mathbb{Z}^{n(k-l)}$ as $\mathbf{z} \leftarrow \text{GSAMP.CUT}(\mathbf{v}, \sigma)$.724 Form $\mathbf{y} := \mathbf{p} + \begin{bmatrix} \mathbf{R} \\ \mathbf{I} \end{bmatrix} \mathbf{z} \in \mathbb{Z}^m$.725 return $\mathbf{y}$.

FIG. 7

Params	Exact	Approx	Approx	Exact	Approx	Approx	Exact	Approx	Approx
n	512	512	512	512	512	512	512	512	512
$\lceil \log_2 q \rceil$	24	24	24	20	20	20	16	16	16
b	2	2	2	2	2	2	2	2	2
l	0	12	15	0	10	12	0	7	9
τ	40	40	40	10	10	10	2.6	2.6	2.6
s	38317.0	29615.3	26726.3	8946.4	6919.8	6416.4	2170.7	1756.3	1618.2
m	13312	7168	5632	11264	6144	5120	9216	5632	4608
$\ x\ _2$	4441737.7	2521387.0	2035008.5	956758.1	545470.5	464022.0	211100.9	133305.5	109339.1
$\ x\ _\infty$	184653	111909	94559	38507	25275	24762	8848	6853	6334
$\ z\ _2$	0	374014.0	2118987.6	0	94916.6	343682.9	0	11897.9	46428.4
$\ z\ _\infty$	0	46895	346439	0	13265	52789	0	1439	7213
PK	37.50	19.50	15.00	26.25	13.75	11.25	17.00	10.00	8.00
Sig	25.68	13.53	10.51	18.87	10.01	8.29	13.16	7.83	6.30
LWE	100.0	100.0	100.0	102.8	102.8	102.8	104.7	104.7	104.7
AISIS	92.3	97.6	93.1	93.4	99.2	96.2	95.6	100.6	99.8
δ	1.00685	1.0643	1.00678	1.00670	1.00631	1.00653	1.00658	1.00621	1.00628
k	174	193	177	180	199	188	186	204	201

Summary of the concrete parameters, with base $b = 2$, aiming at around 100-bit security. The sizes of PK and Sig are measured in kB. τ is the Gaussian width of the secret matrix R . s is the Gaussian width of the preimage. "LWE" refers to the security level of the pseudorandomness of the PK. "AISIS" refers to the security level of breaking approximate ISIS. δ and k are the variables used in the AISIS security estimation.

FIG. 8

Params	Exact	Approx	Approx	Exact	Approx	Approx	Exact	Approx	Approx
n	512	512	512	1024	1024	1024	1024	1024	1024
$\lceil \log_2 q \rceil$	16	16	16	18	18	18	18	18	18
b	4	4	4	8	8	8	4	4	4
l	0	2	4	0	2	3	0	4	5
τ	2.6	2.6	2.6	2.8	2.8	2.8	2.8	2.8	2.8
s	3114.2	2833.3	2505.6	8861.1	7824.8	7227.9	5118.8	4297.8	4015.5
m	5120	4096	3072	8192	6144	5120	11264	7168	6144
$\ x\ _2$	223740.1	183004.9	138145.7	805772.9	604711.5	516446.3	552713.4	369981.2	311153.9
$\ x\ _\infty$	13320	11868	8948	35348	28823	30435	19274	18283	14927
$\ z\ _2$	0	1402.3	19807.1	0	7316.5	54379.8	0	29958.0	115616.4
$\ z\ _\infty$	0	174	2448	0	905	6680	0	3025	12070
PK	9.00	7.00	5.00	15.75	11.25	9.00	22.50	13.50	11.25
Sig	7.62	5.94	4.45	13.70	10.14	8.36	18.74	11.09	9.38
LWE	104.7	104.7	104.7	192.7	192.7	192.7	192.7	192.7	192.7
AISIS	94.8	97.3	99.5	177.6	185.0	187.0	187.9	197.6	195.6
δ	1.00664	1.00645	1.00629	1.0036	1.00347	1.00343	1.00342	1.00326	1.00329
k	183	192	200	462	488	495	498	532	525

Summary of the concrete parameters, with base $b \geq 4$, aiming at around 100-bit and 192-bit security.

FIG. 9

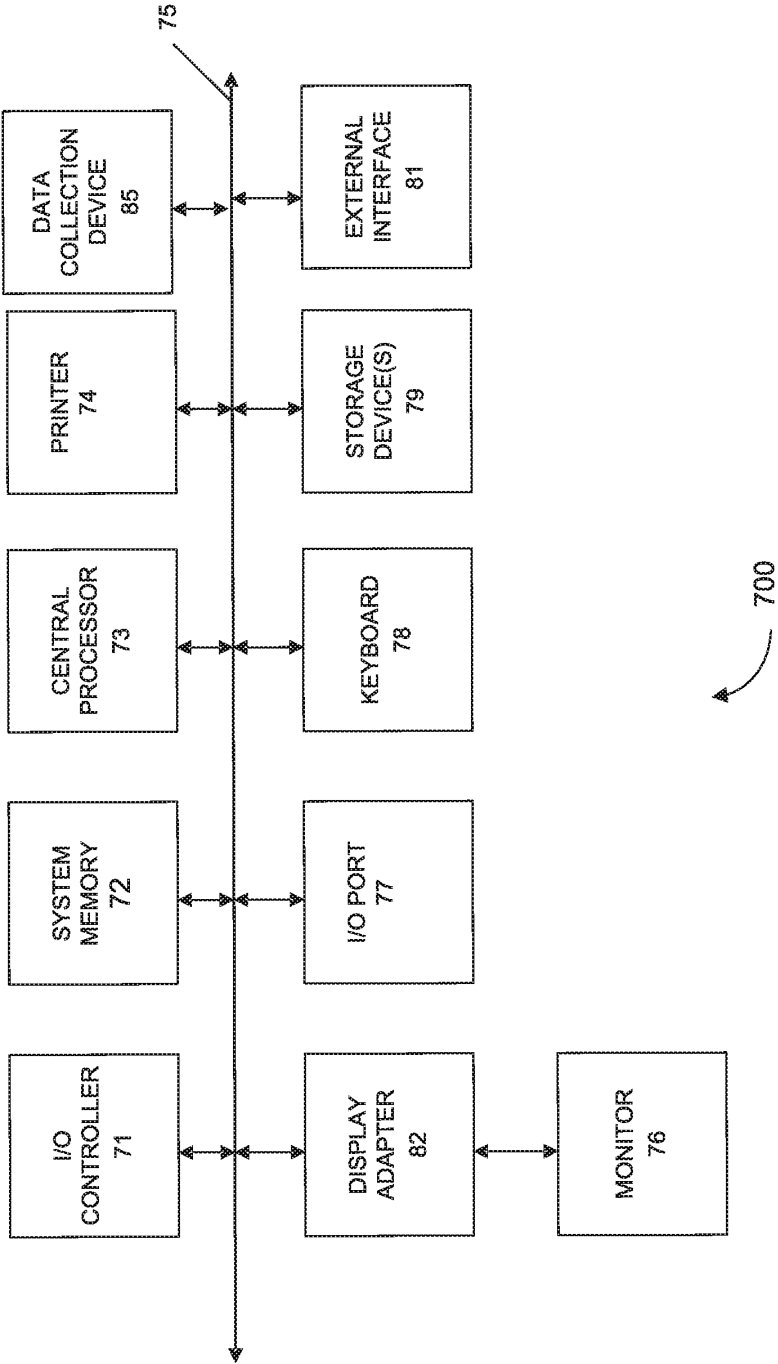


FIG. 10