

100 →

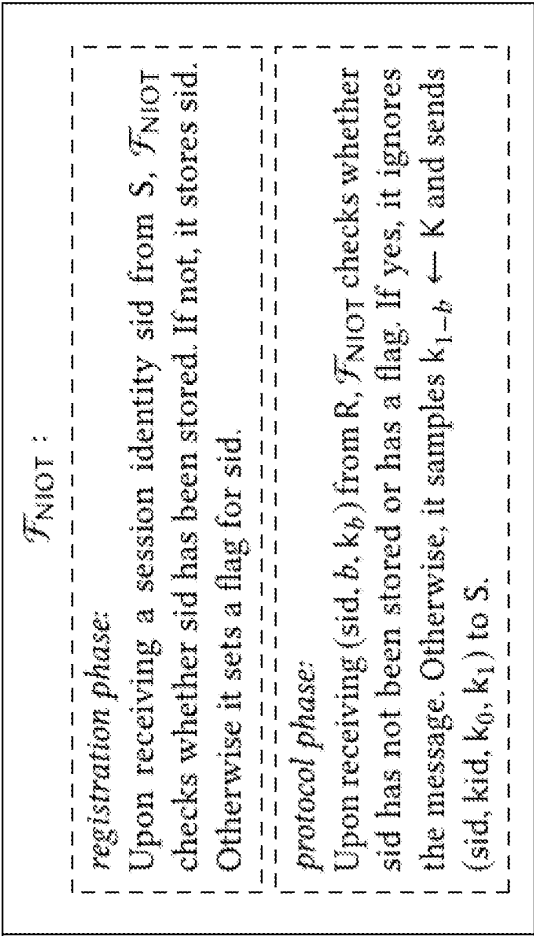


FIG. 1

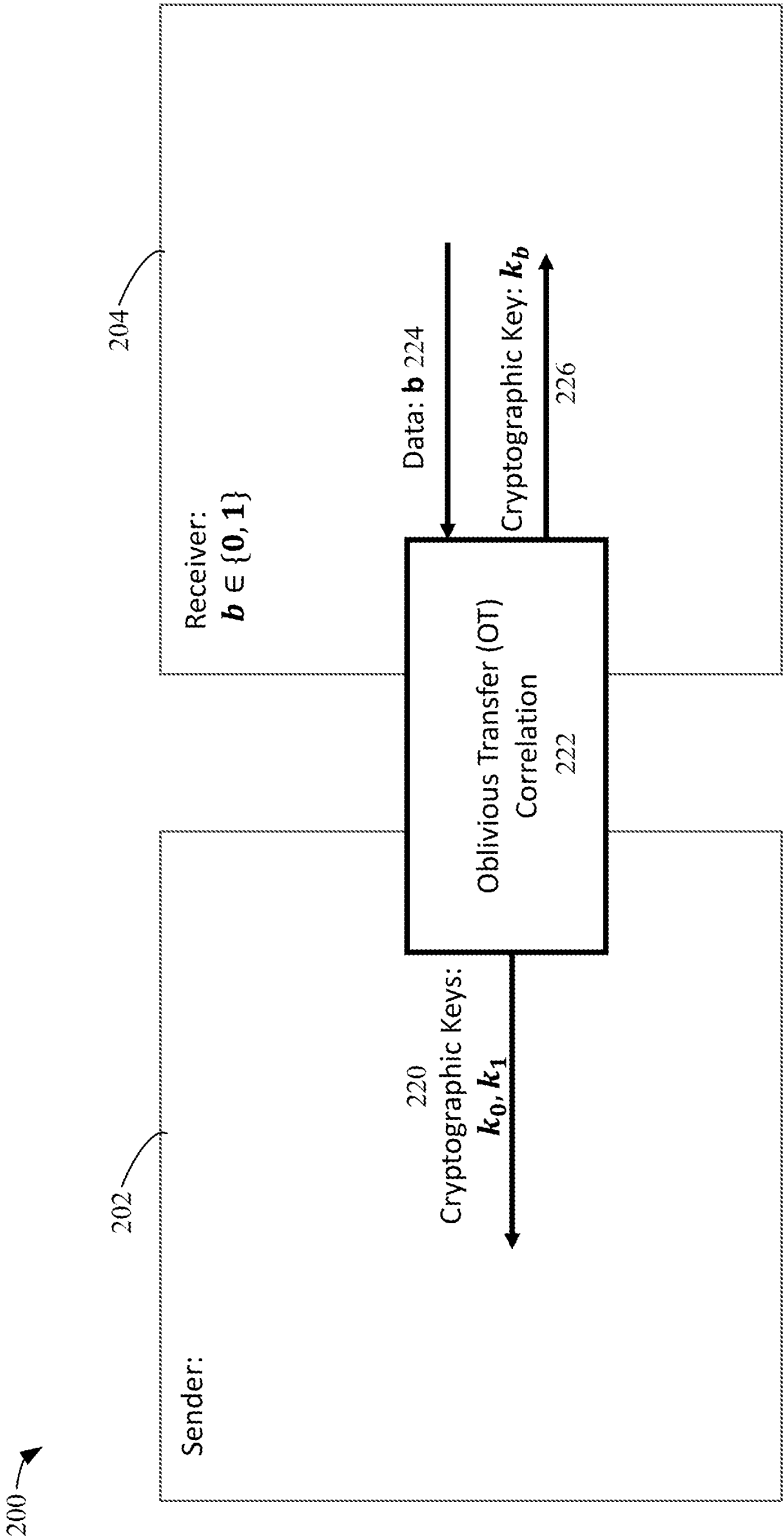


FIG. 2

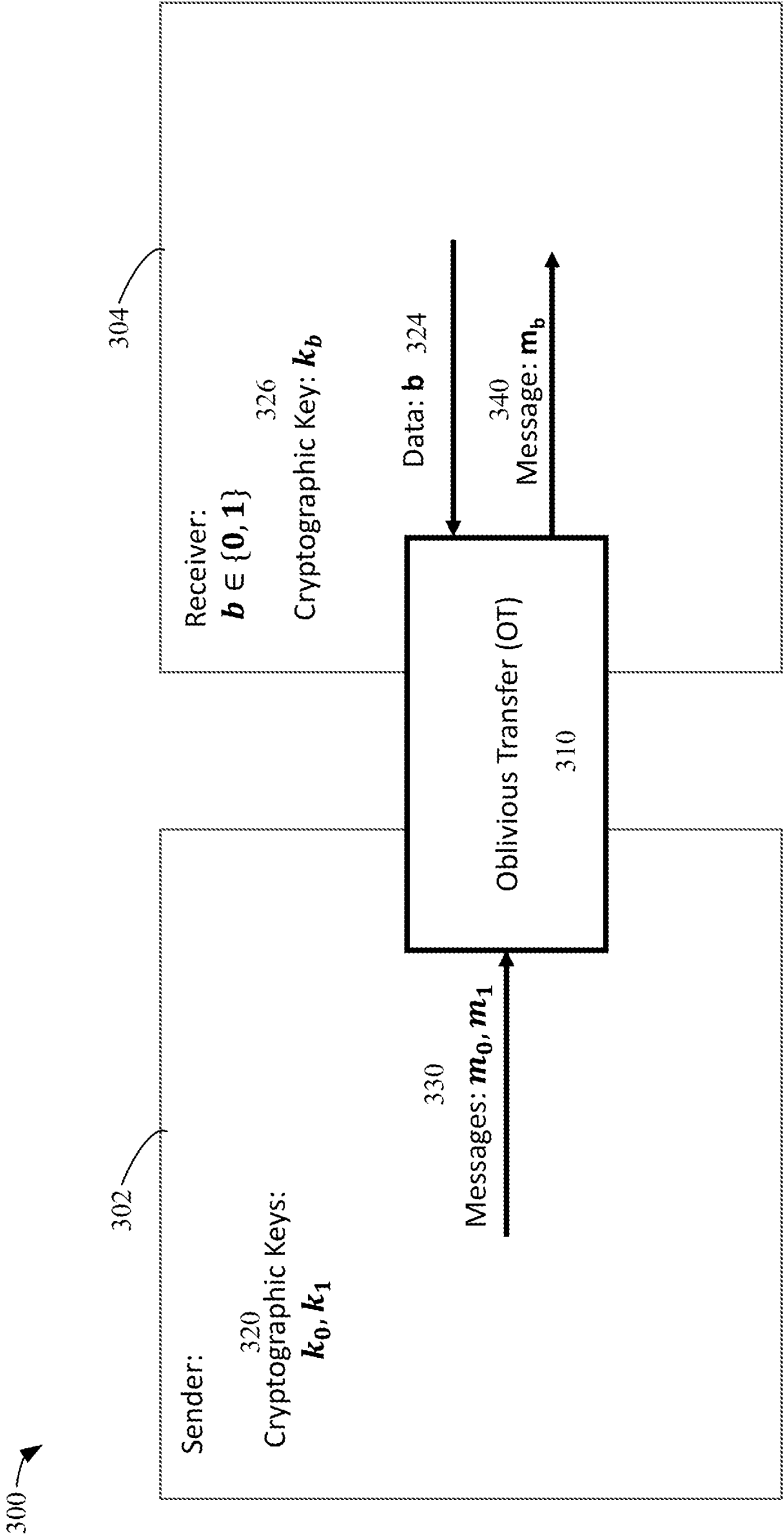


FIG. 3

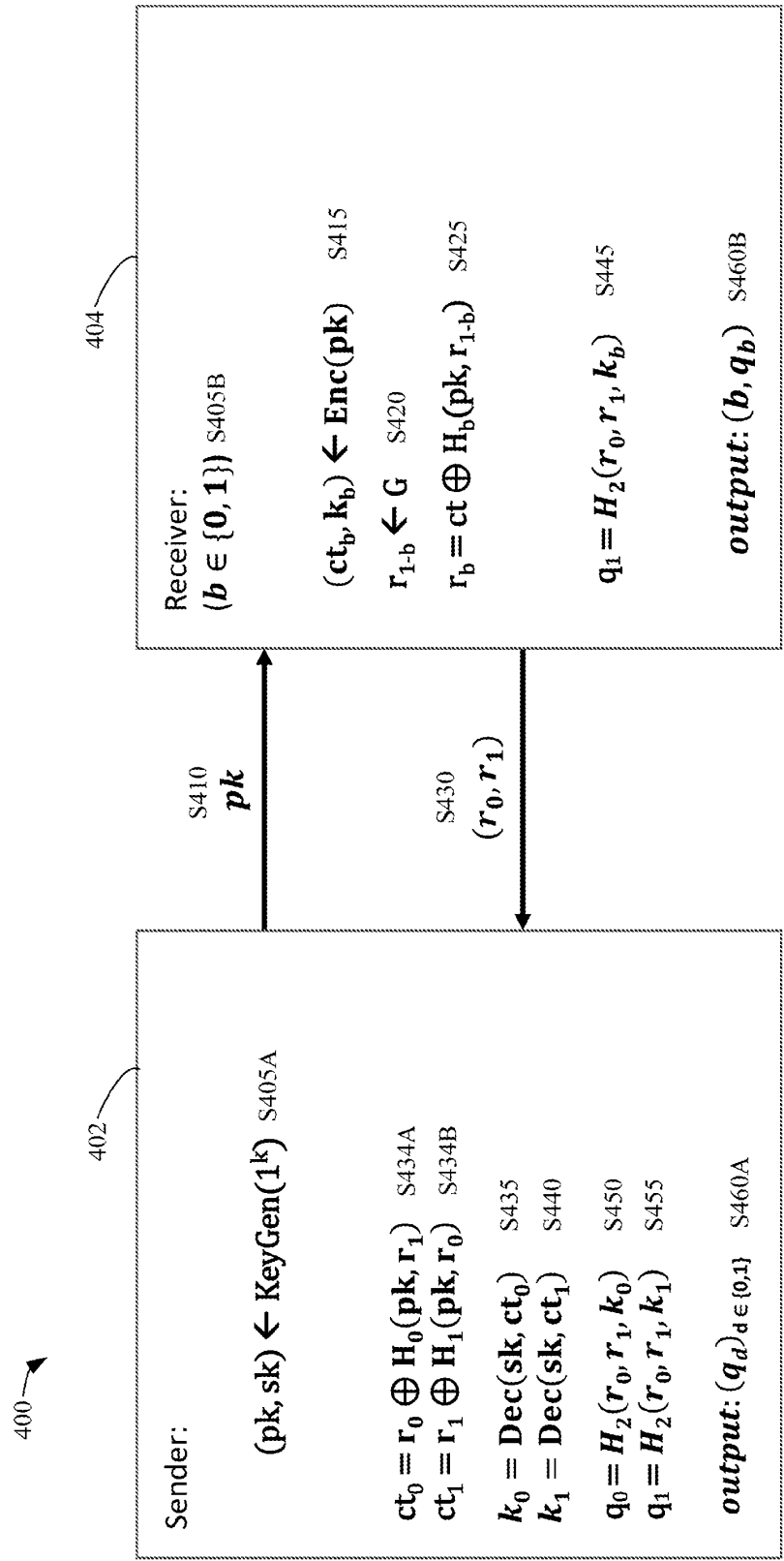


FIG. 4

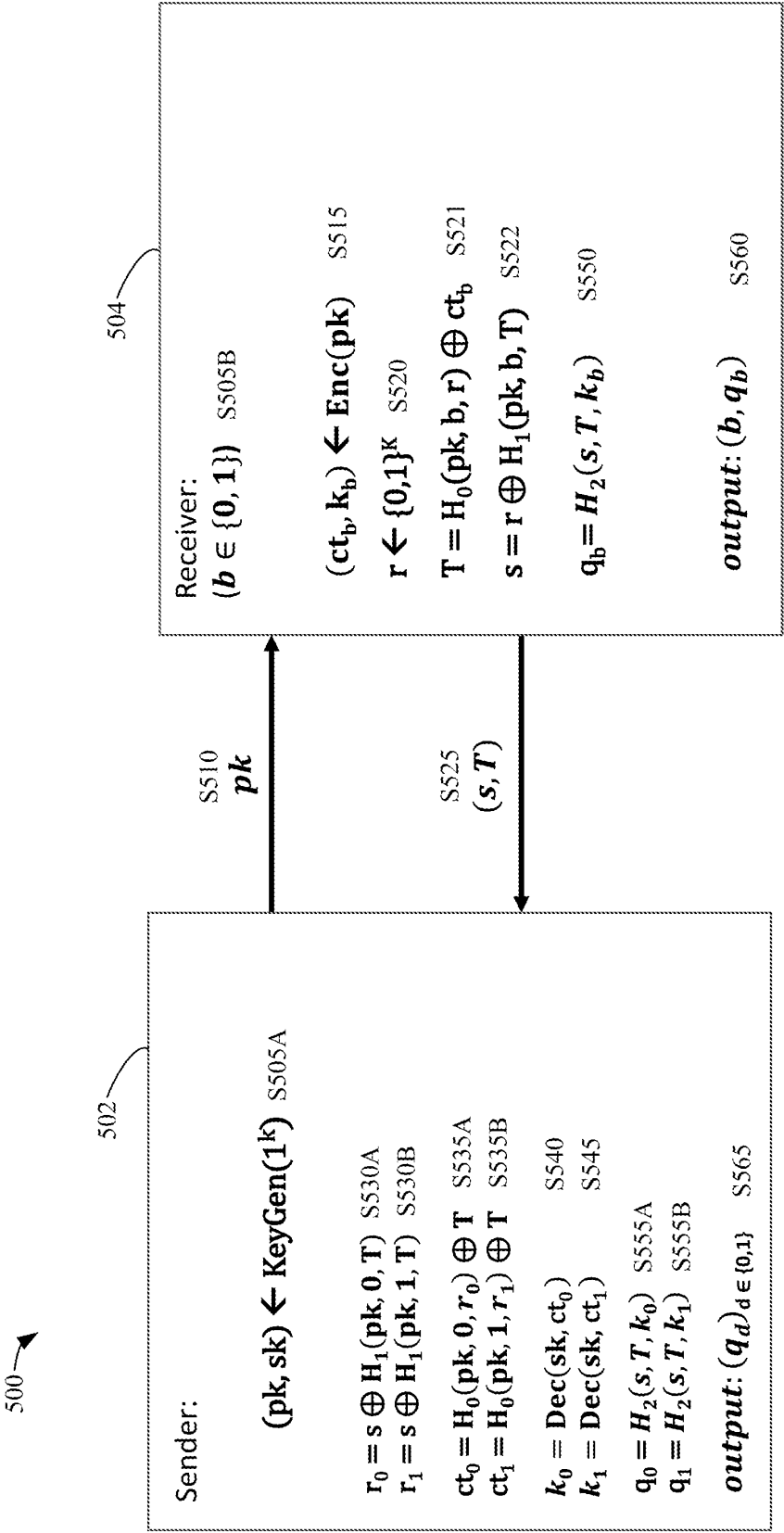


FIG. 5

600

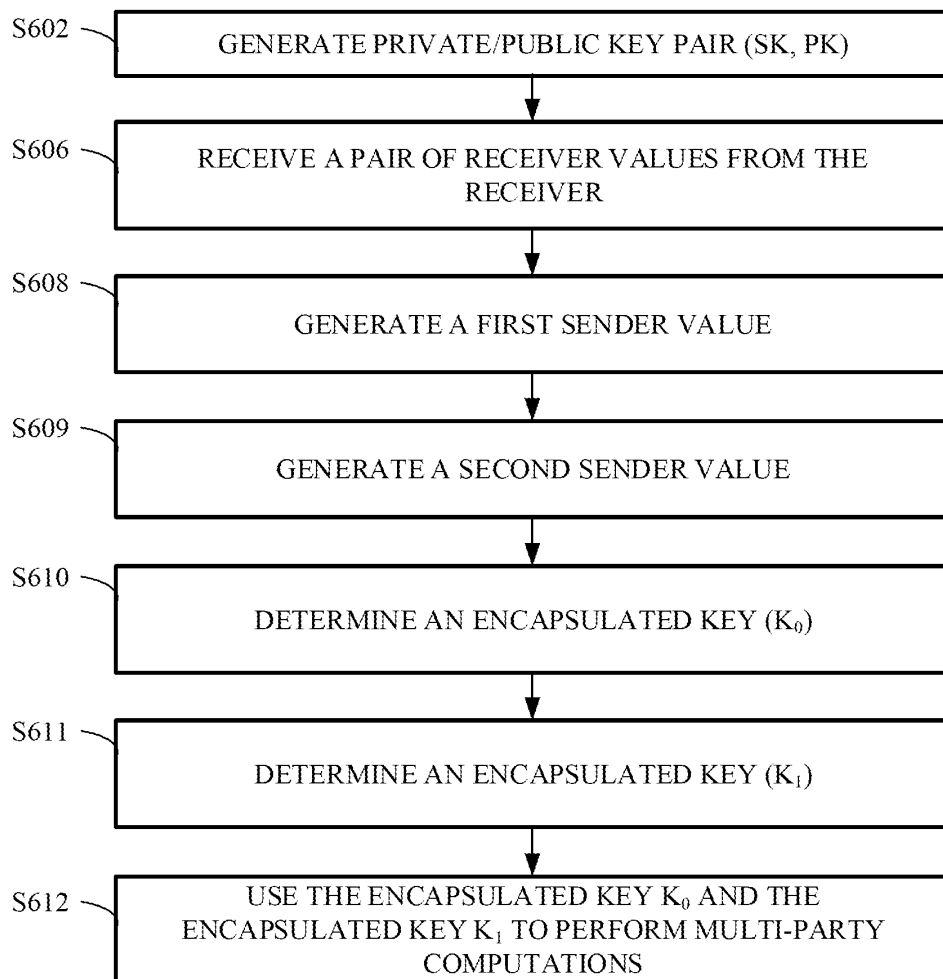


FIG. 6

700

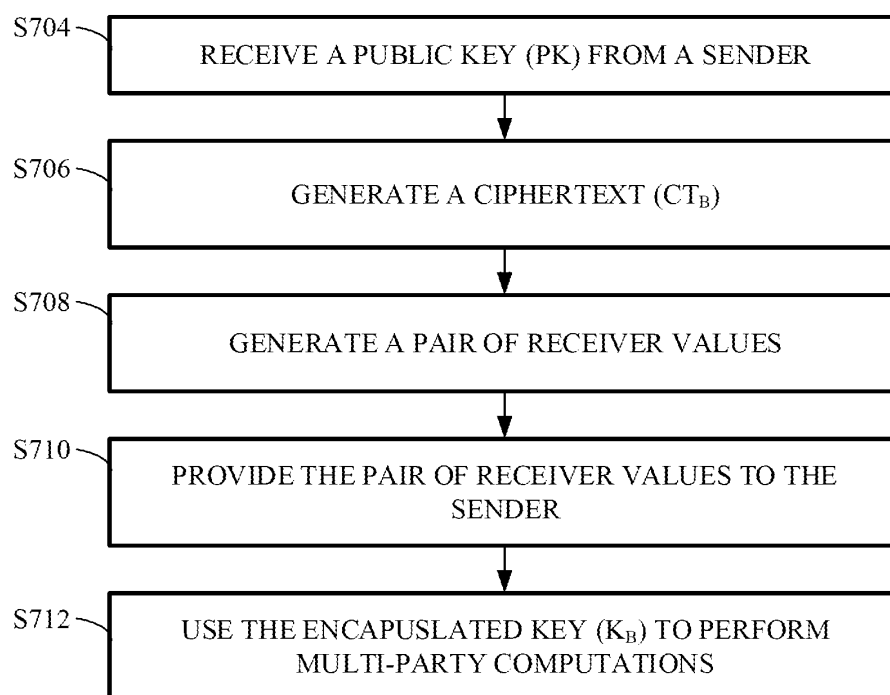


FIG. 7

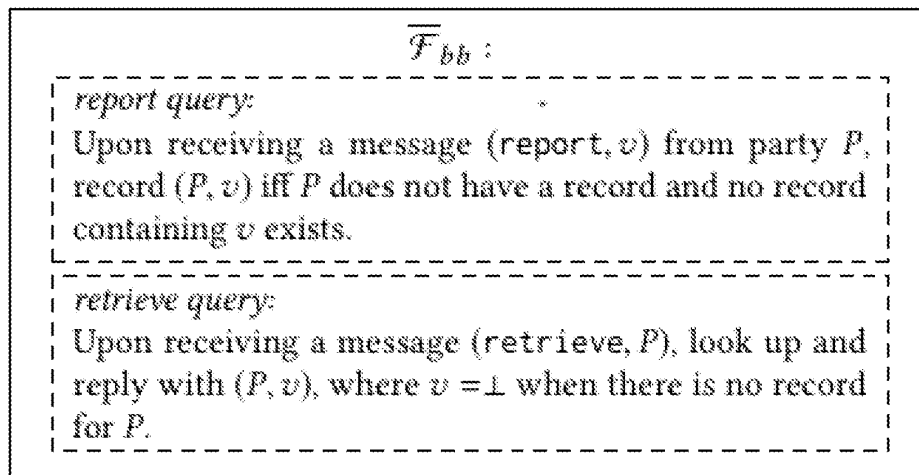


FIG. 8

9/17

900

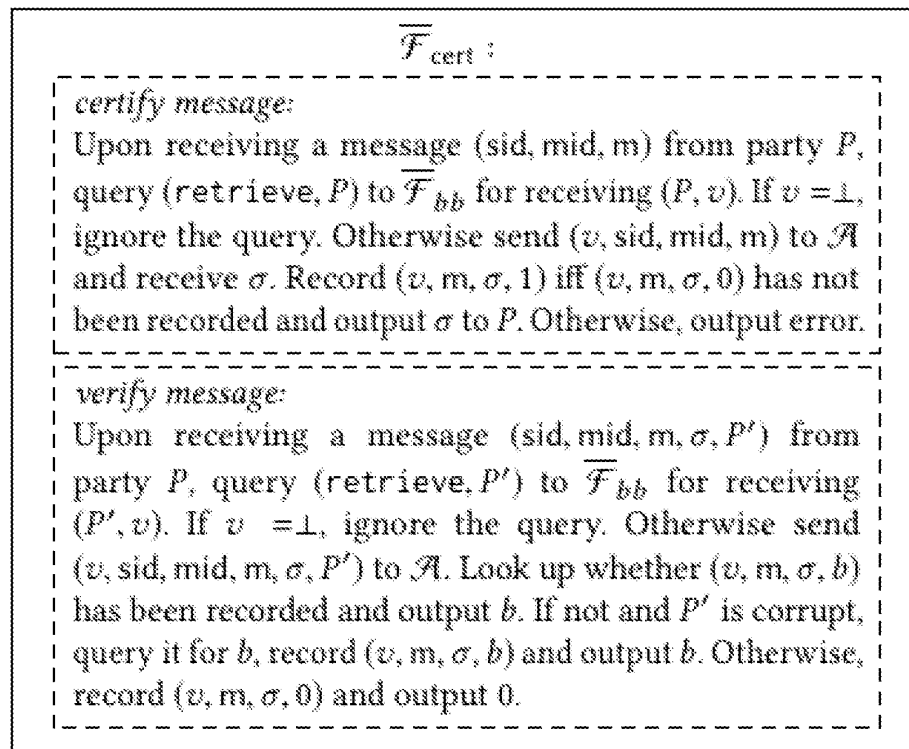


FIG. 9

10/17

1000

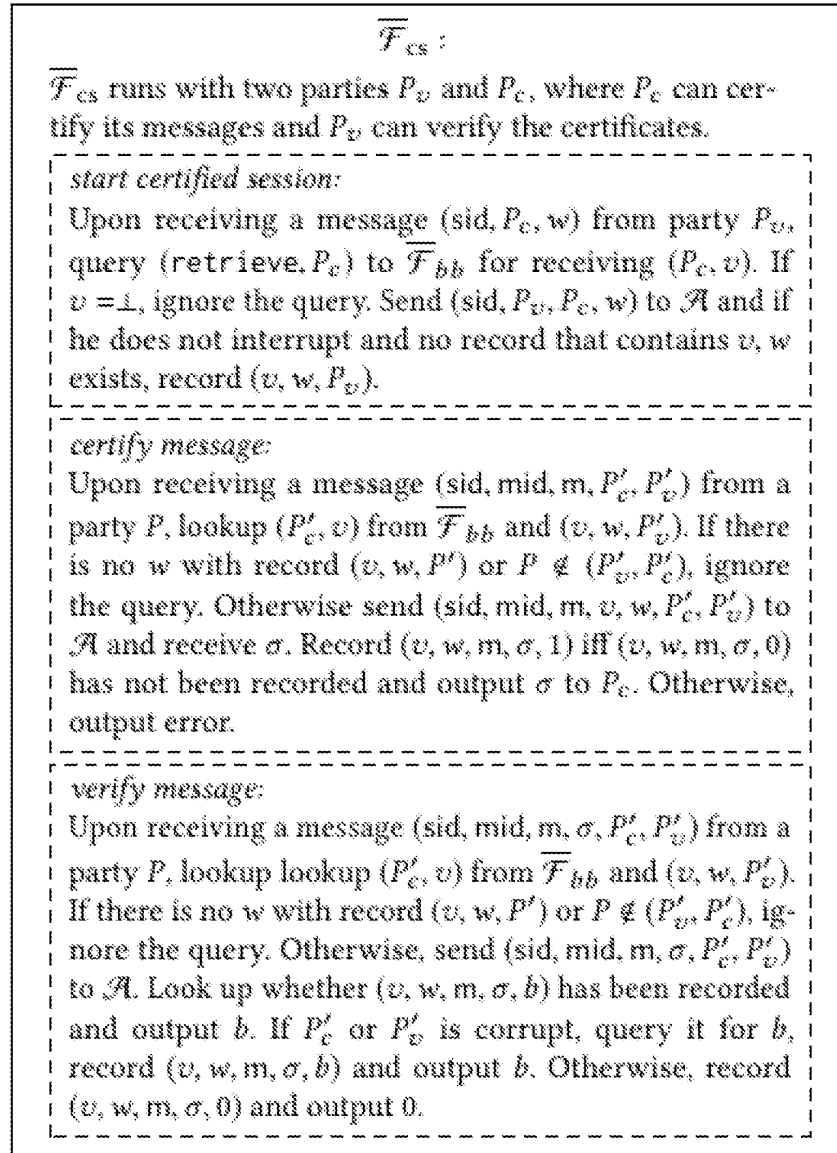


FIG. 10

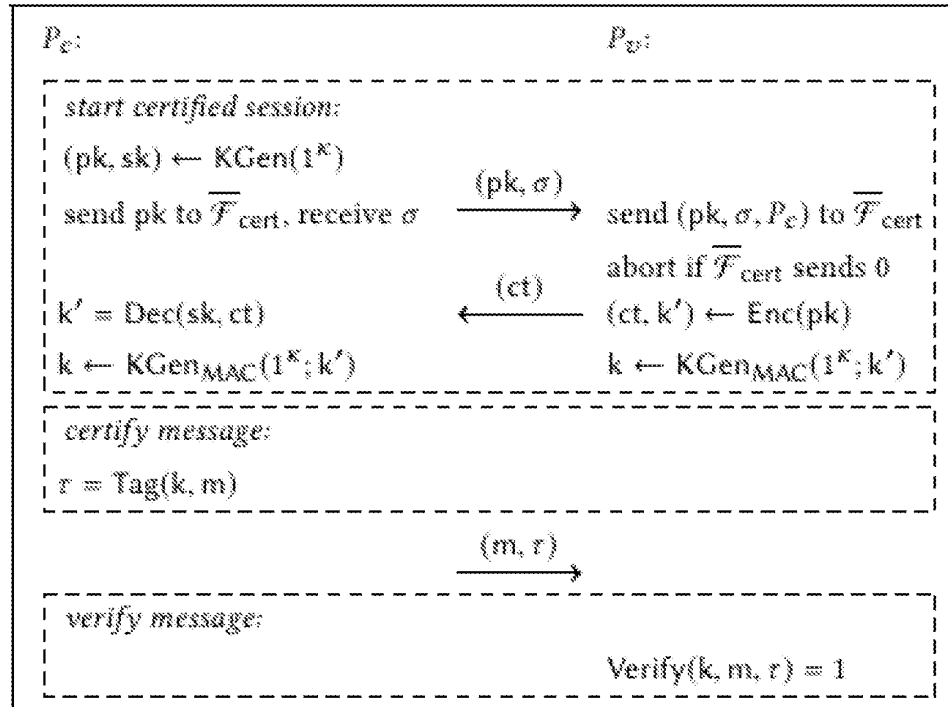


FIG. 11

12/17

1200

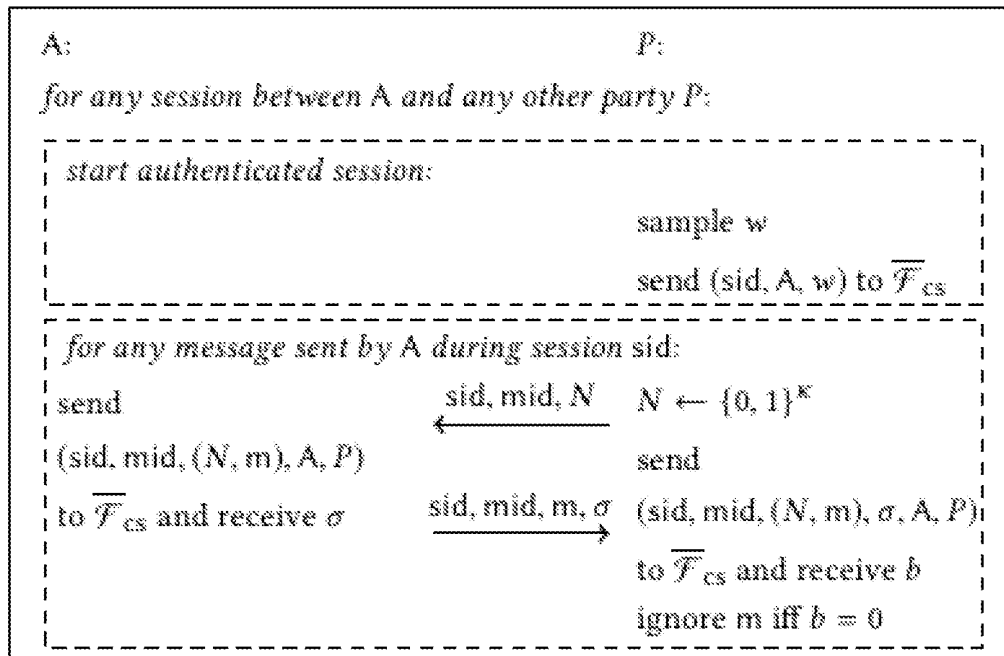


FIG. 12

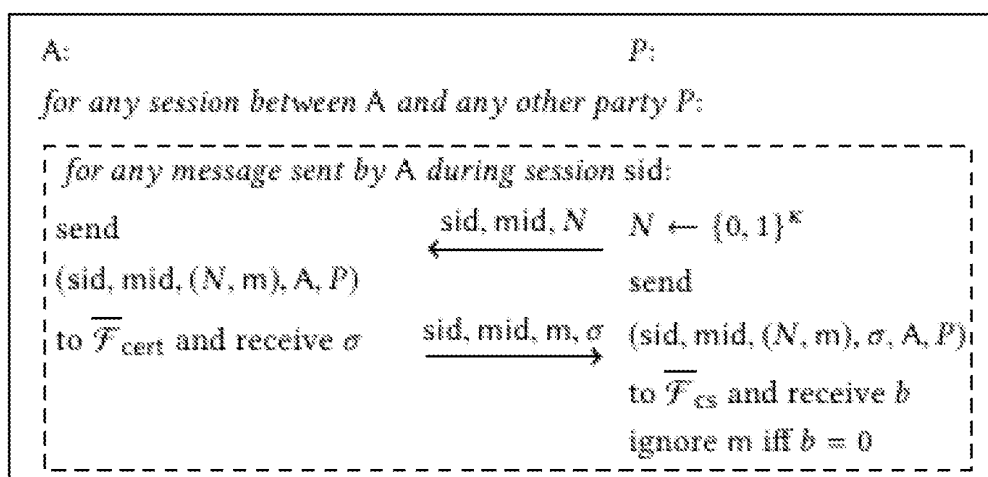


FIG. 13

14/17

1400

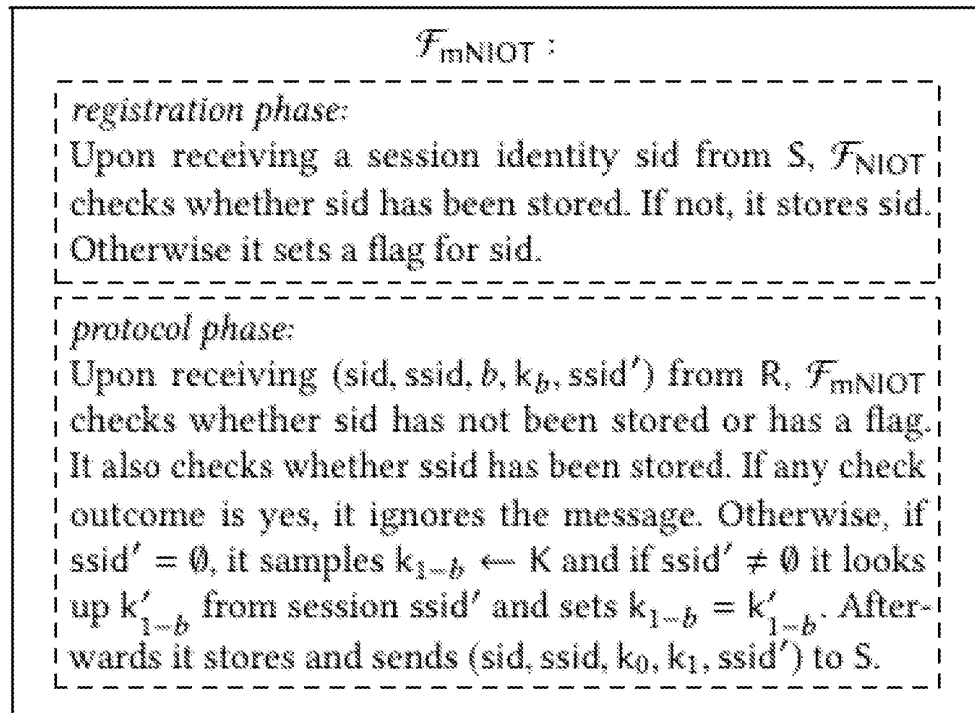


FIG. 14

15/17

1500

Operation	cycles	running time
Mul	584561	0.277 ms
Sub	1228	0.001 ms
Add	1118	0.001 ms
GHash	245569	0.116 ms
Key Generation	232424	0.110 ms
OT _{1,R}	1378214	0.653 ms
OT _{1,S}	1867754	0.885 ms
OT _{2,R}	1195311	0.566 ms
OT _{2,S}	1879205	0.890 ms

FIG. 15

16/17

1600

Operation	cycles	running time
Key Generation	277570659	131.415 ms
RSA Enc	142624	0.068 ms
RSA Dec	3820942	1.810 ms
OT _{1,R}	186457	0.089 ms
OT _{1,S}	7654668	3.625 ms
OT _{2,R}	179813	0.085 ms
OT _{2,S}	7640627	3.618 ms

FIG. 16

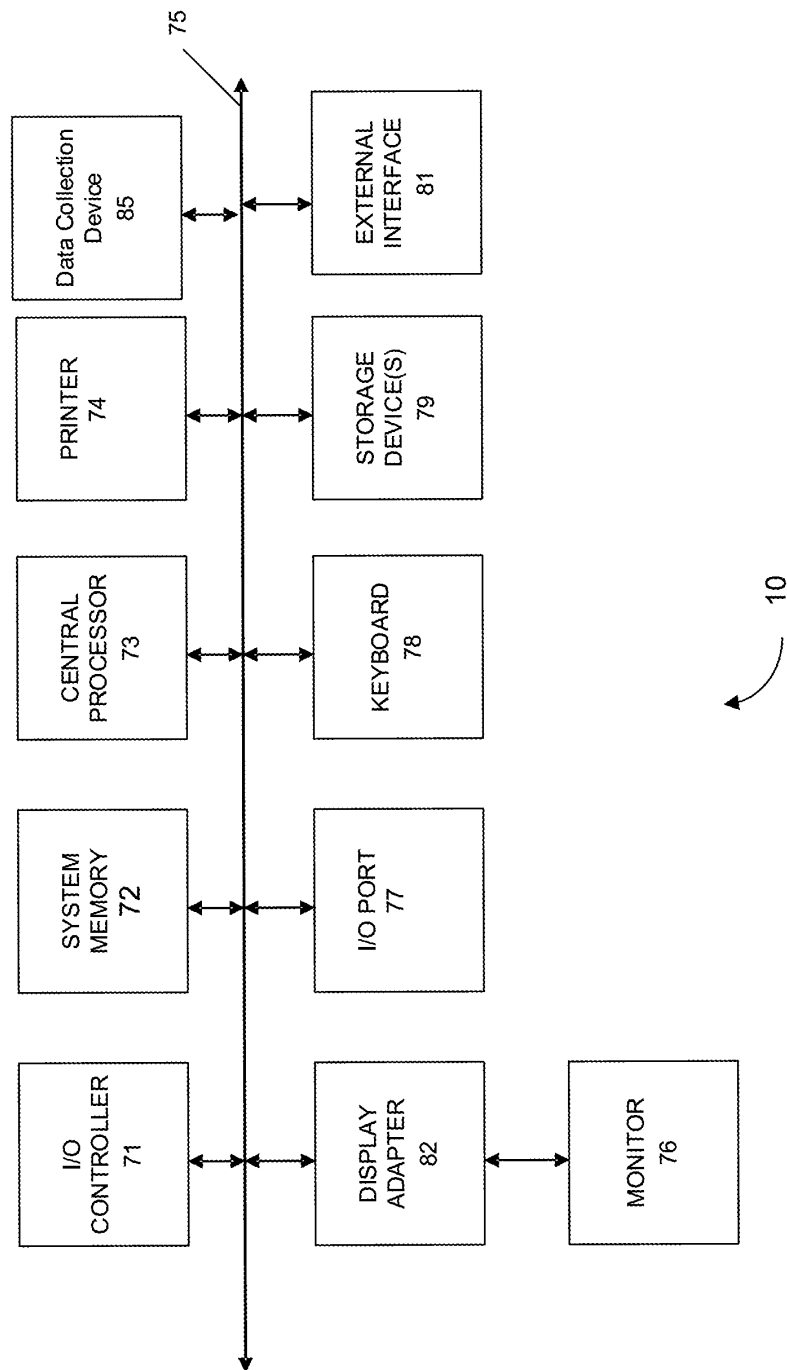


FIG. 17