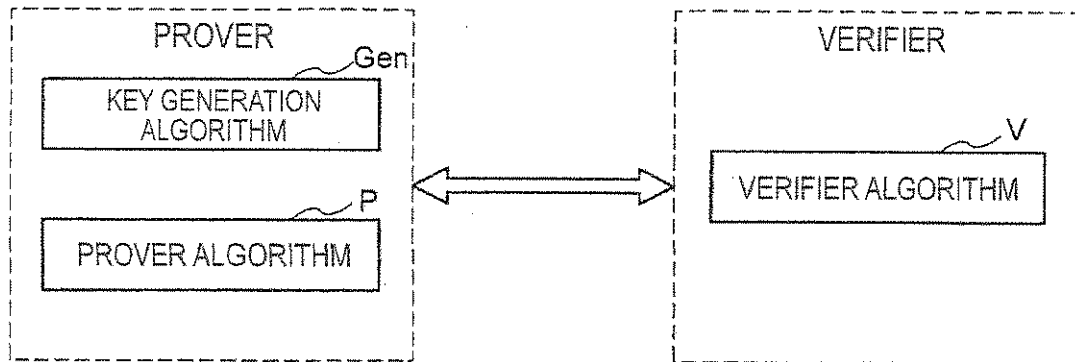


1/20
FIG. 1

PUBLIC KEY AUTHENTICATION SCHEME



2/20
FIG. 2

N-PASS PUBLIC KEY AUTHENTICATION SCHEME

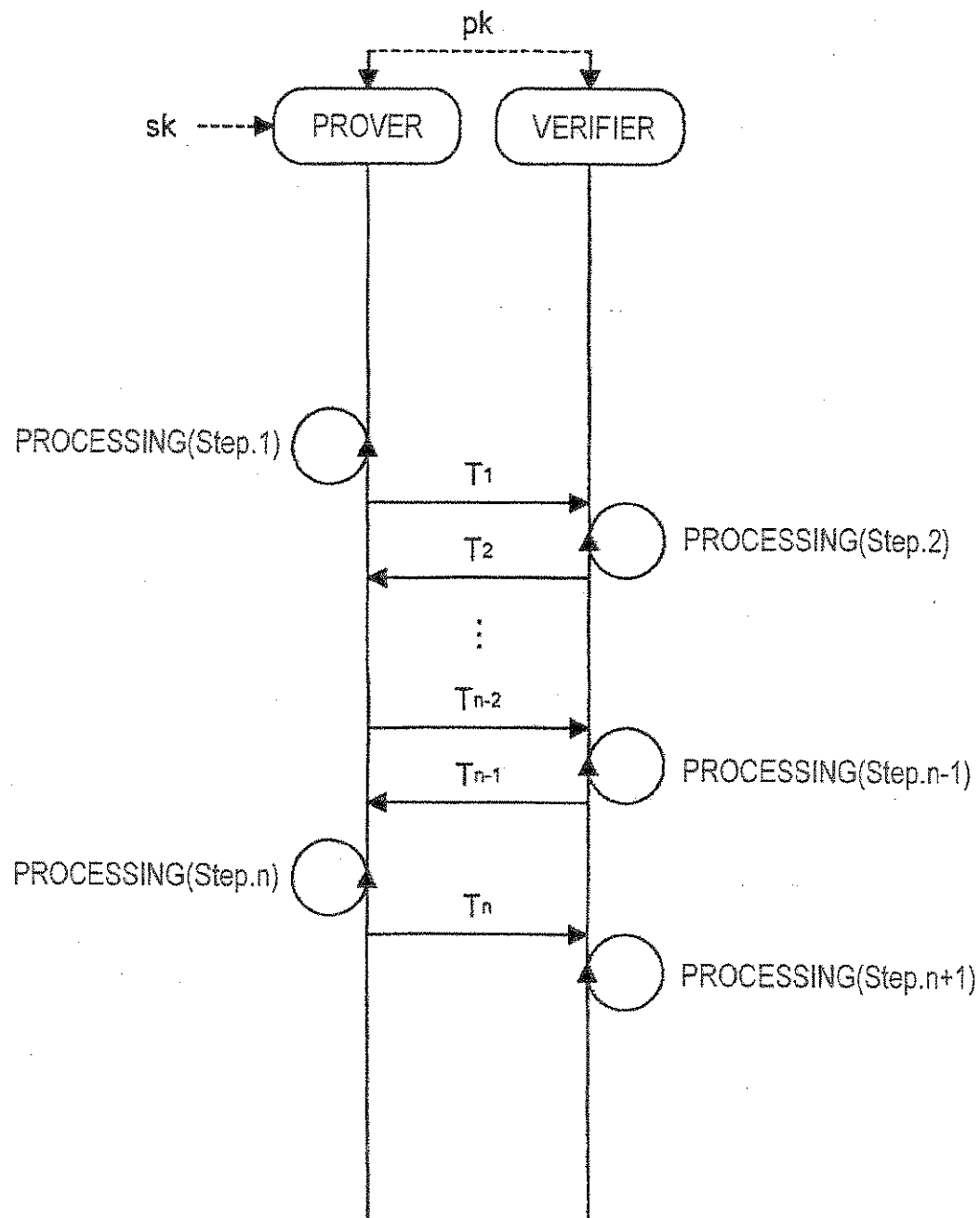
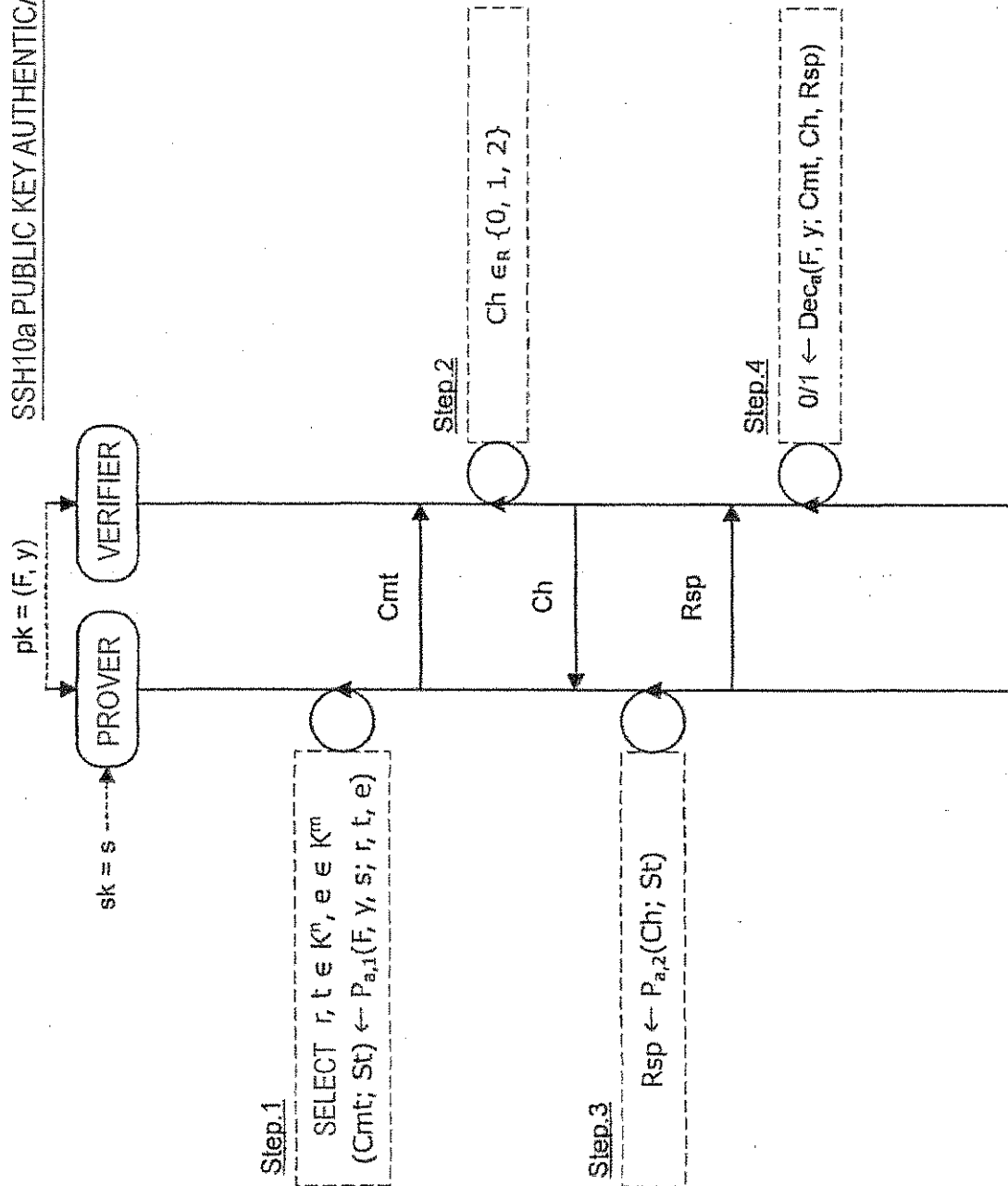
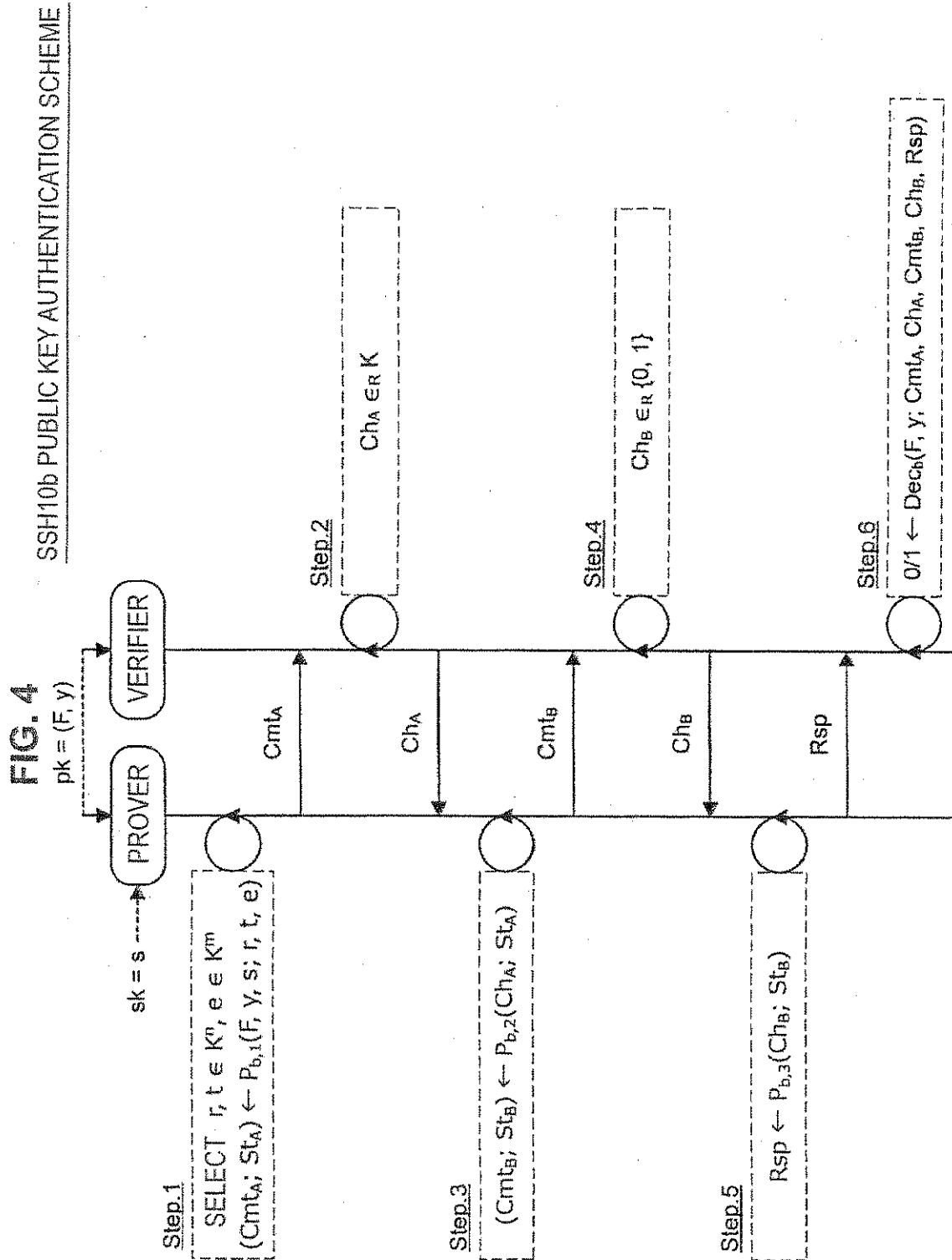


FIG. 3

SSH10a PUBLIC KEY AUTHENTICATION SCHEME





5/20
FIG. 5

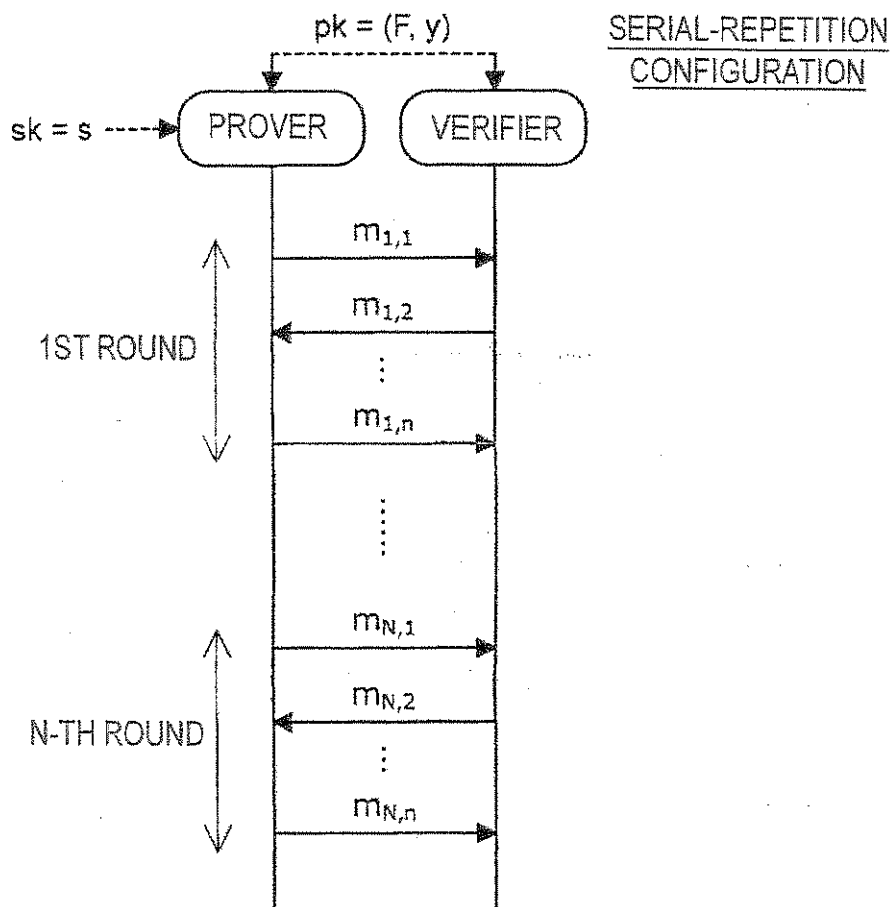


FIG. 6

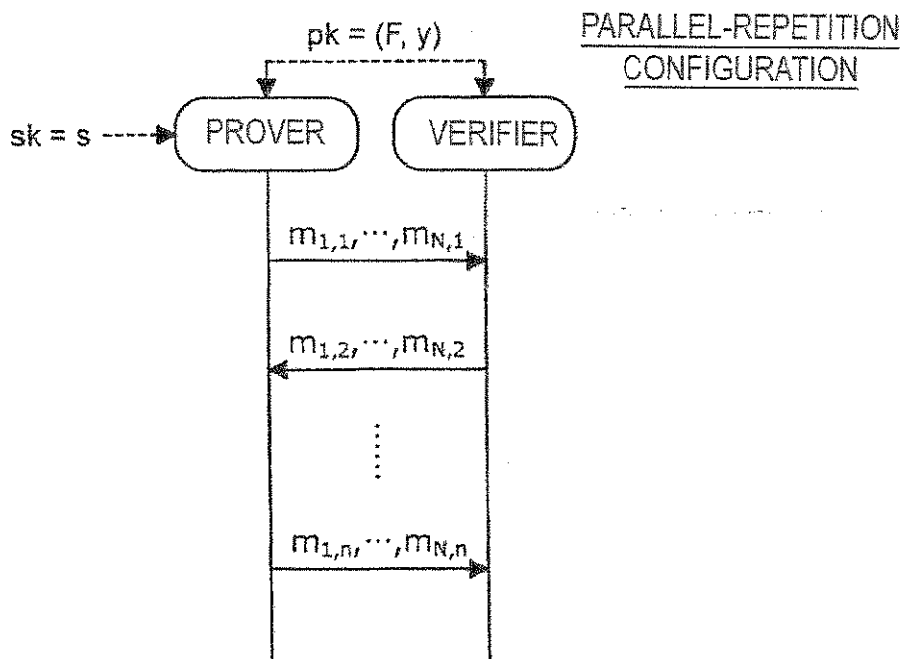
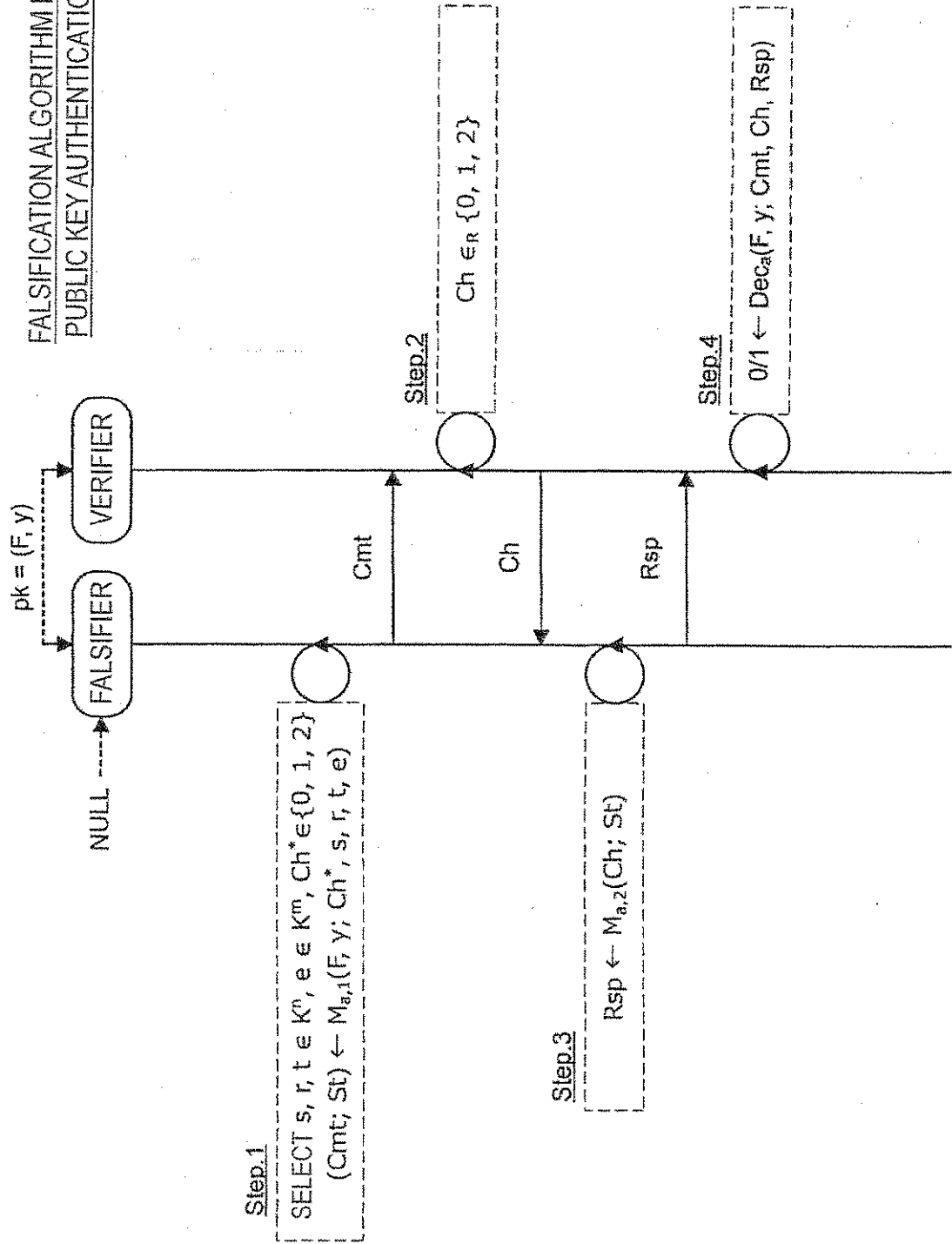


FIG. 7

FALSIFICATION ALGORITHM FOR SSH10a
PUBLIC KEY AUTHENTICATION SCHEME



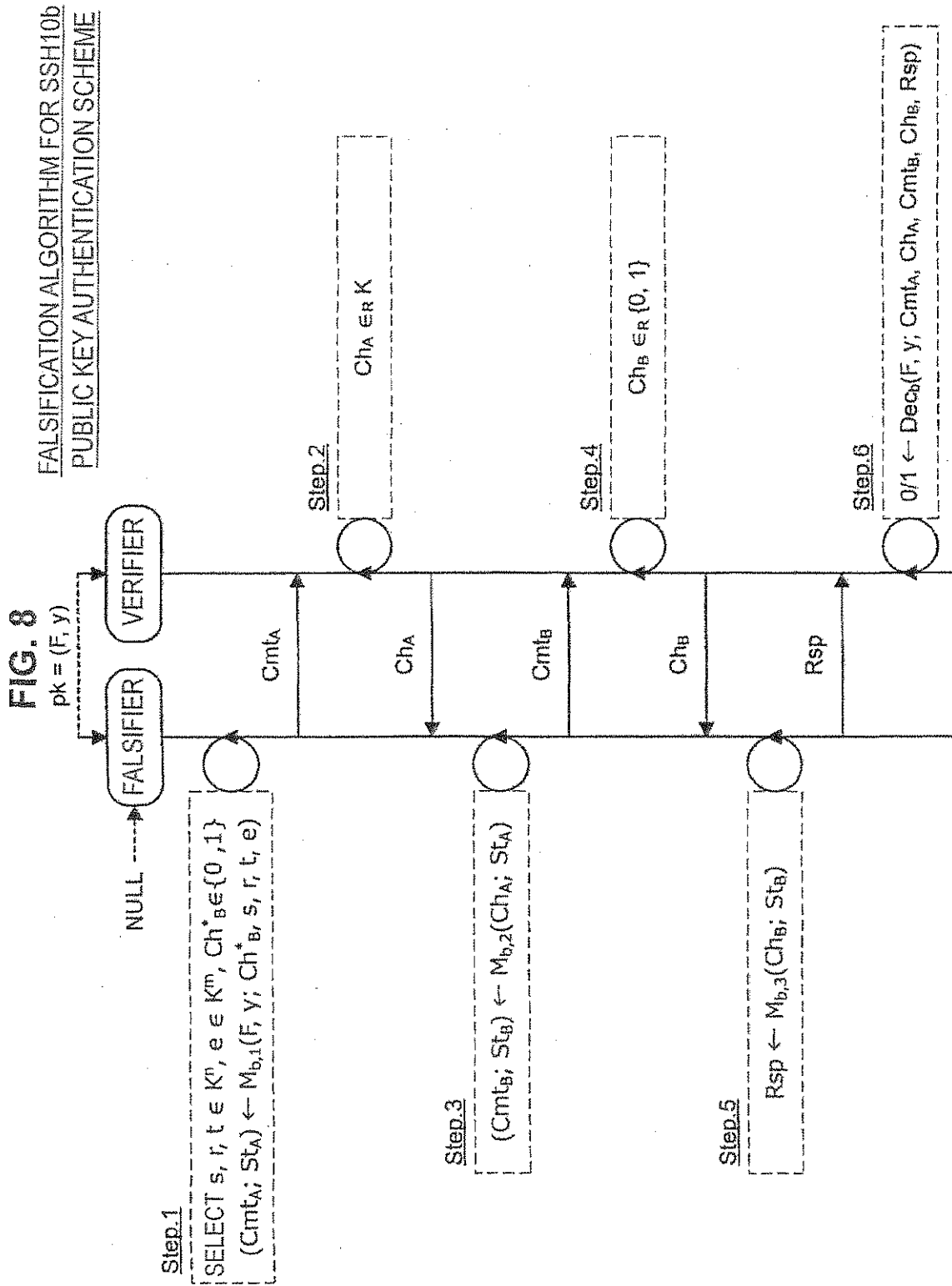
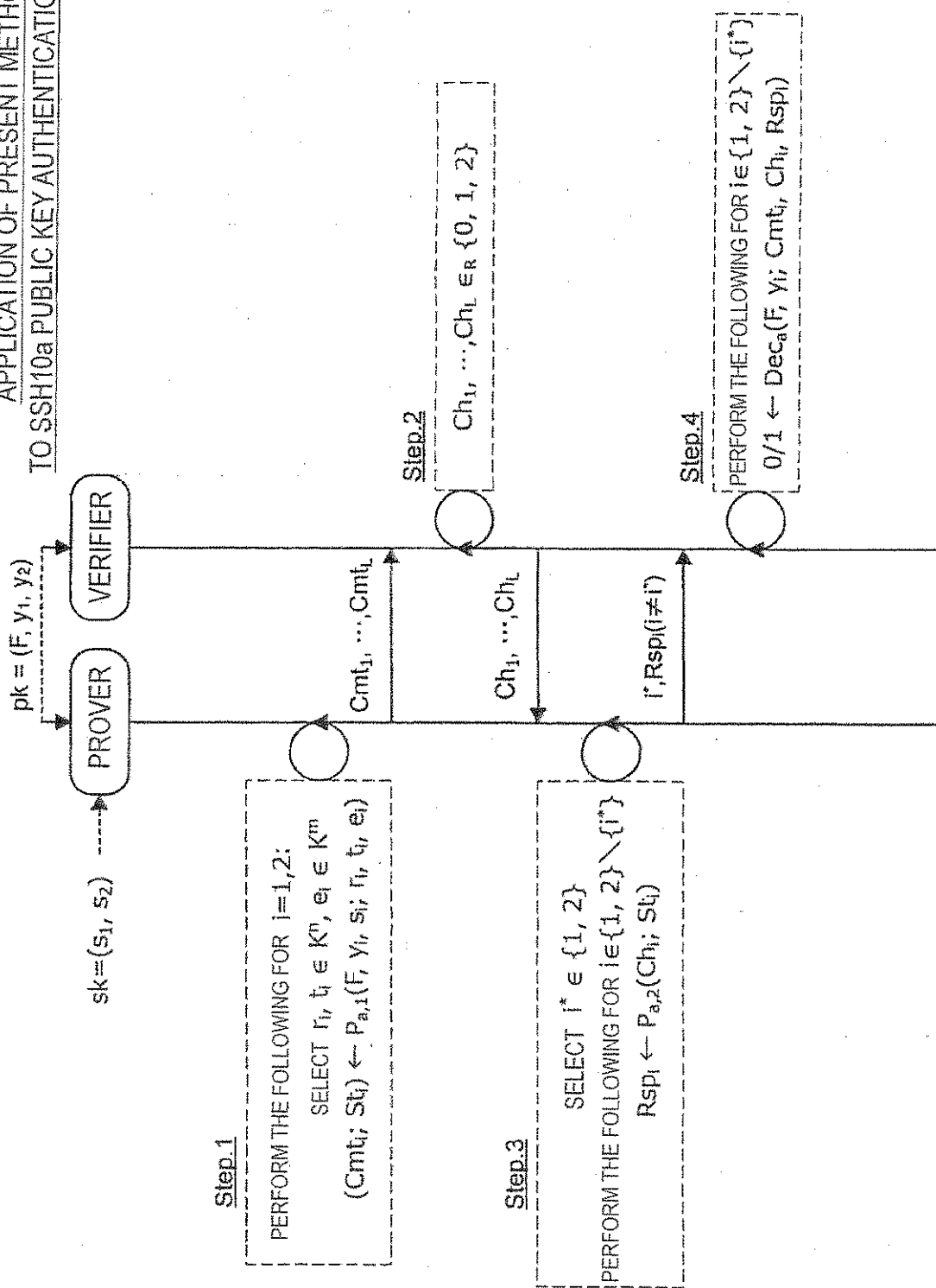


FIG. 9

APPLICATION OF PRESENT METHOD #1
TO SSH10a PUBLIC KEY AUTHENTICATION SCHEME



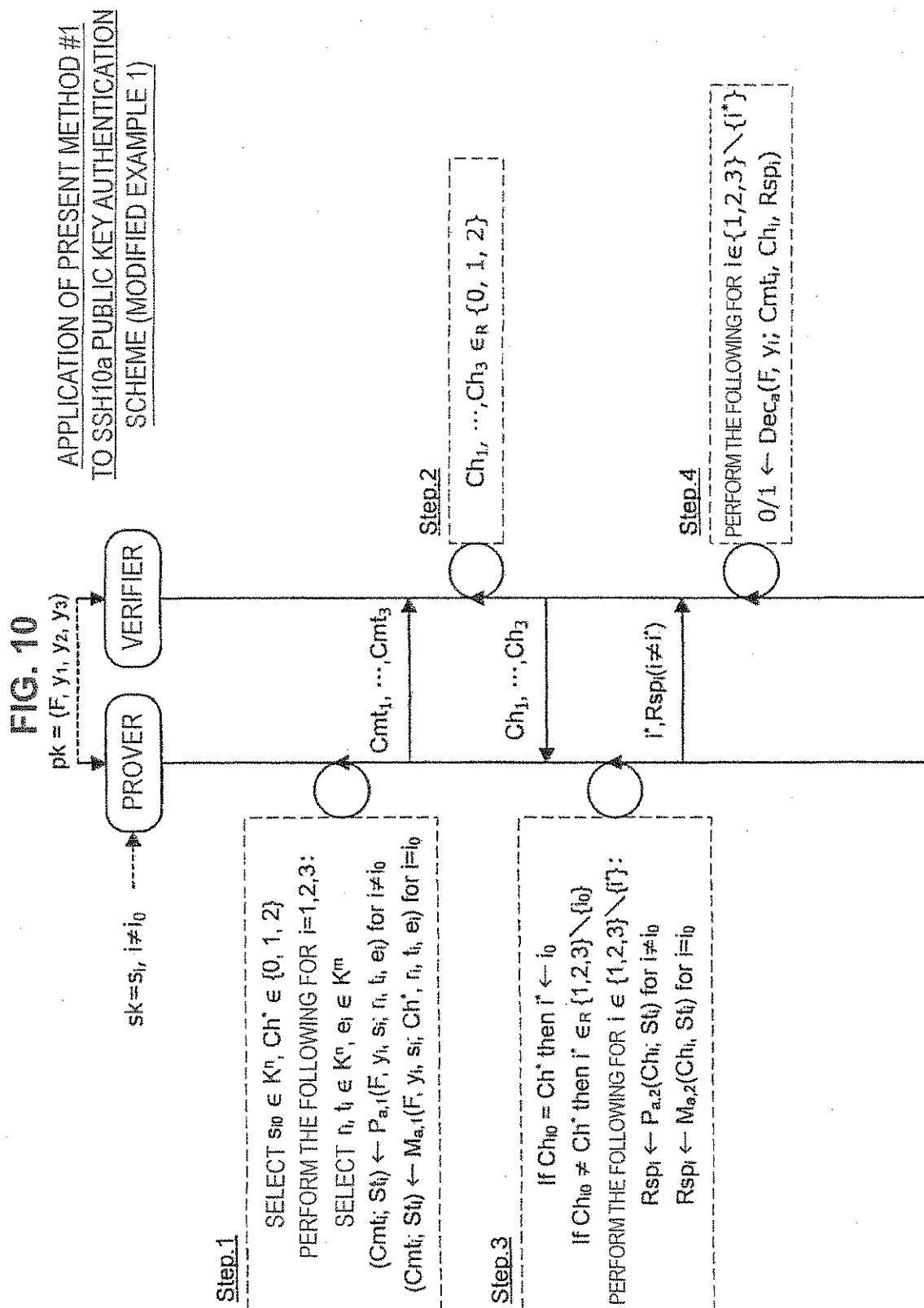
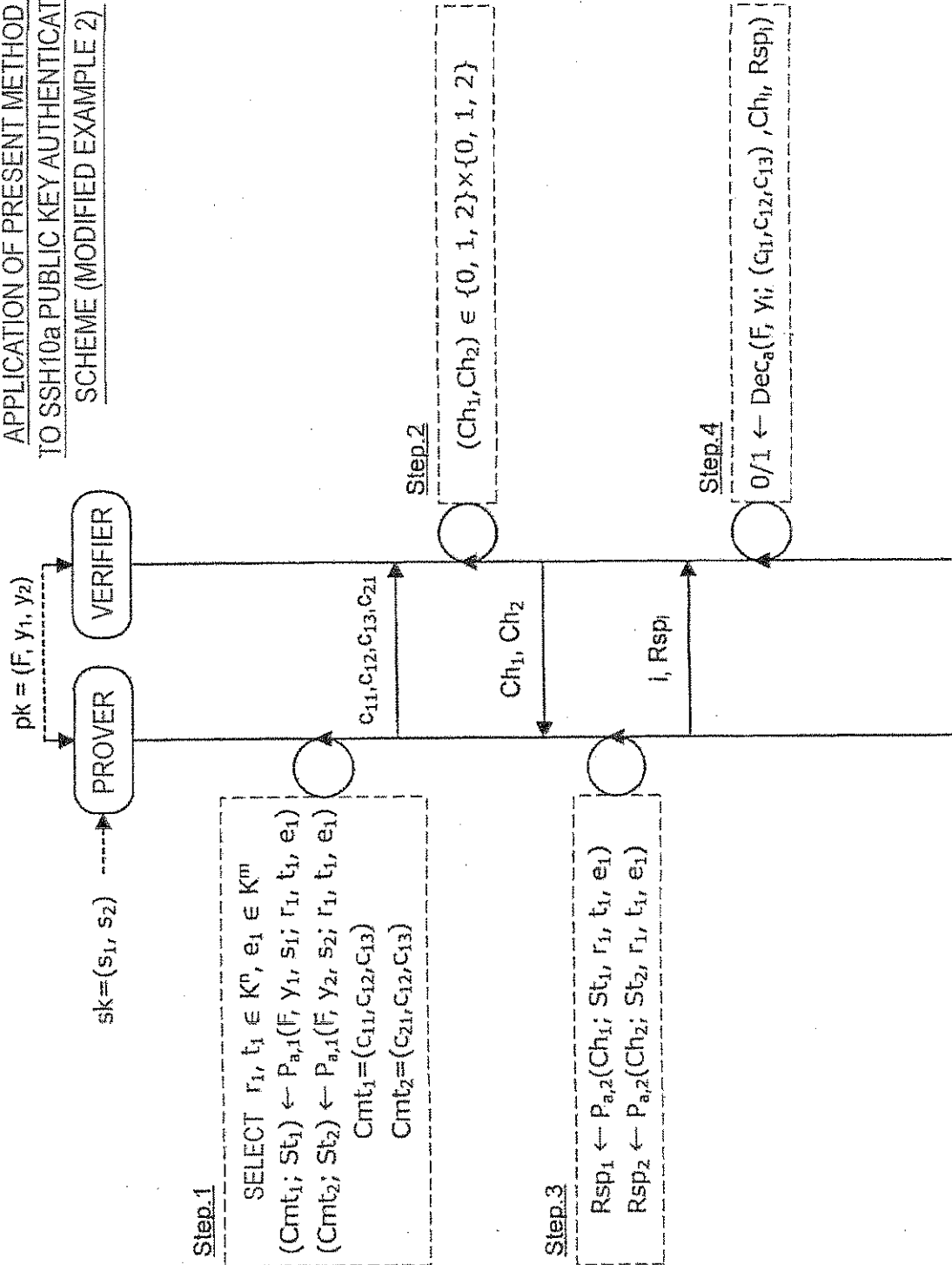


FIG. 11
 APPLICATION OF PRESENT METHOD #1
 TO SSH10a PUBLIC KEY AUTHENTICATION
 SCHEME (MODIFIED EXAMPLE 2)



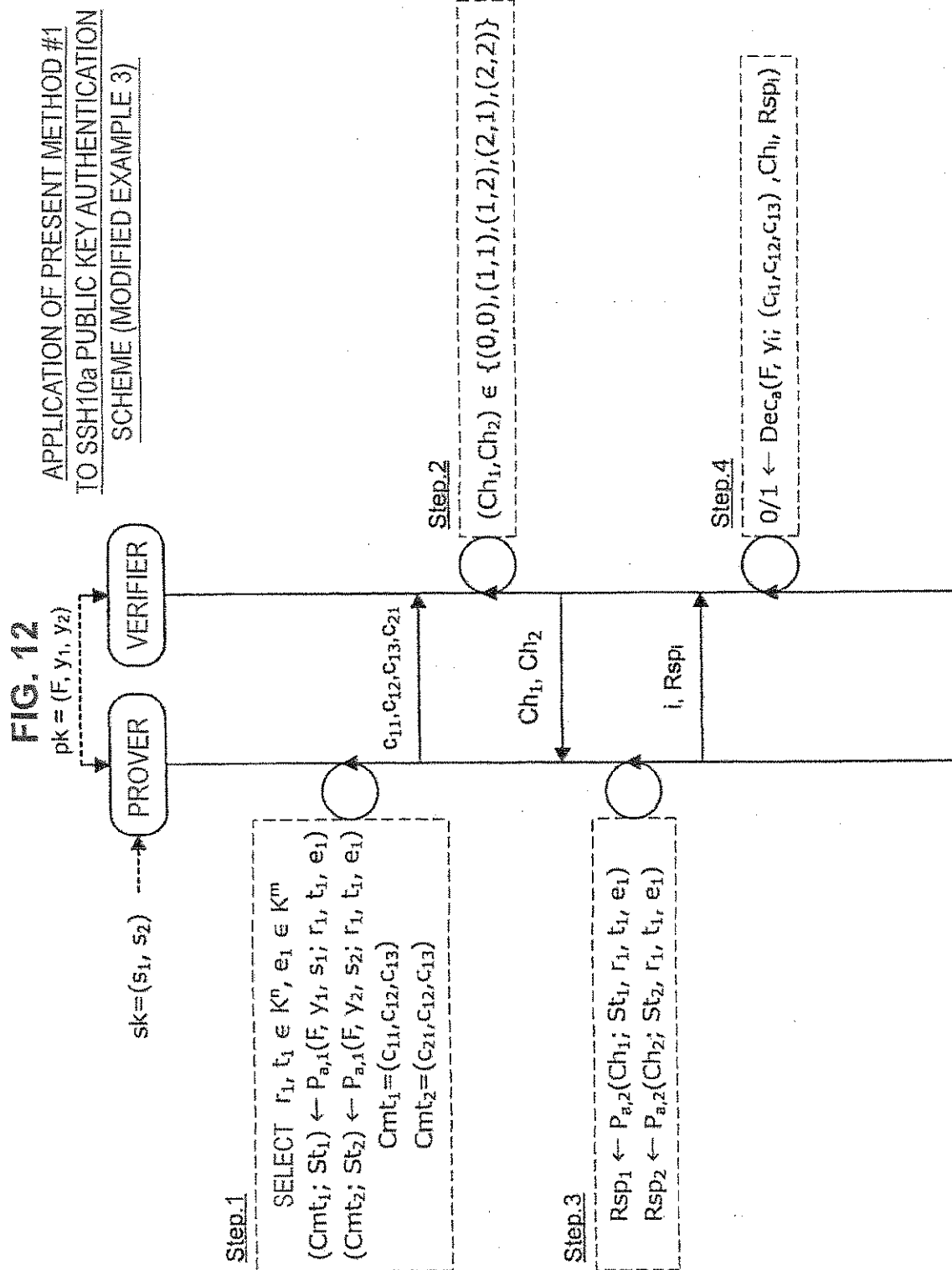
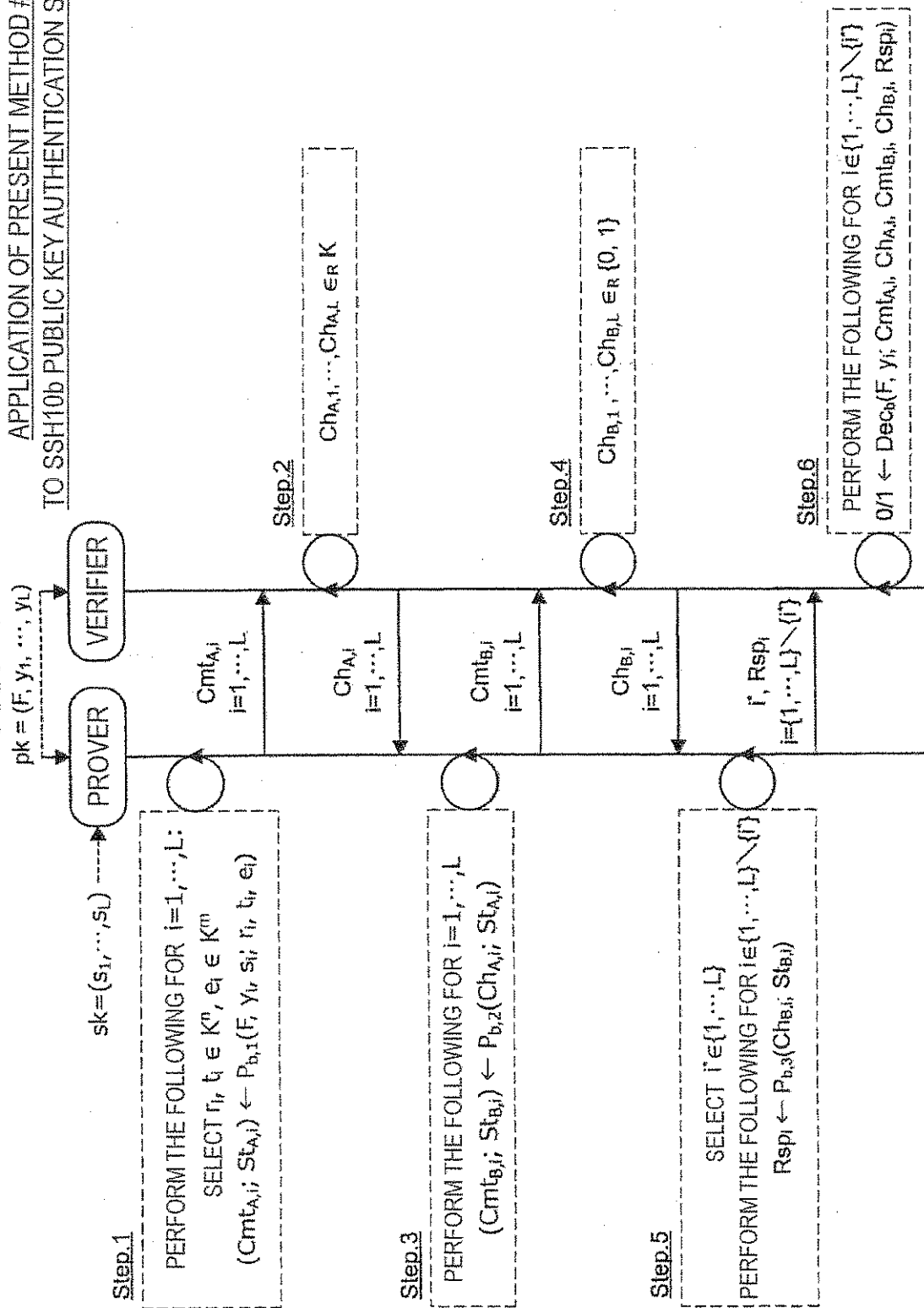


FIG. 13

APPLICATION OF PRESENT METHOD #1
TO SSH10b PUBLIC KEY AUTHENTICATION SCHEME



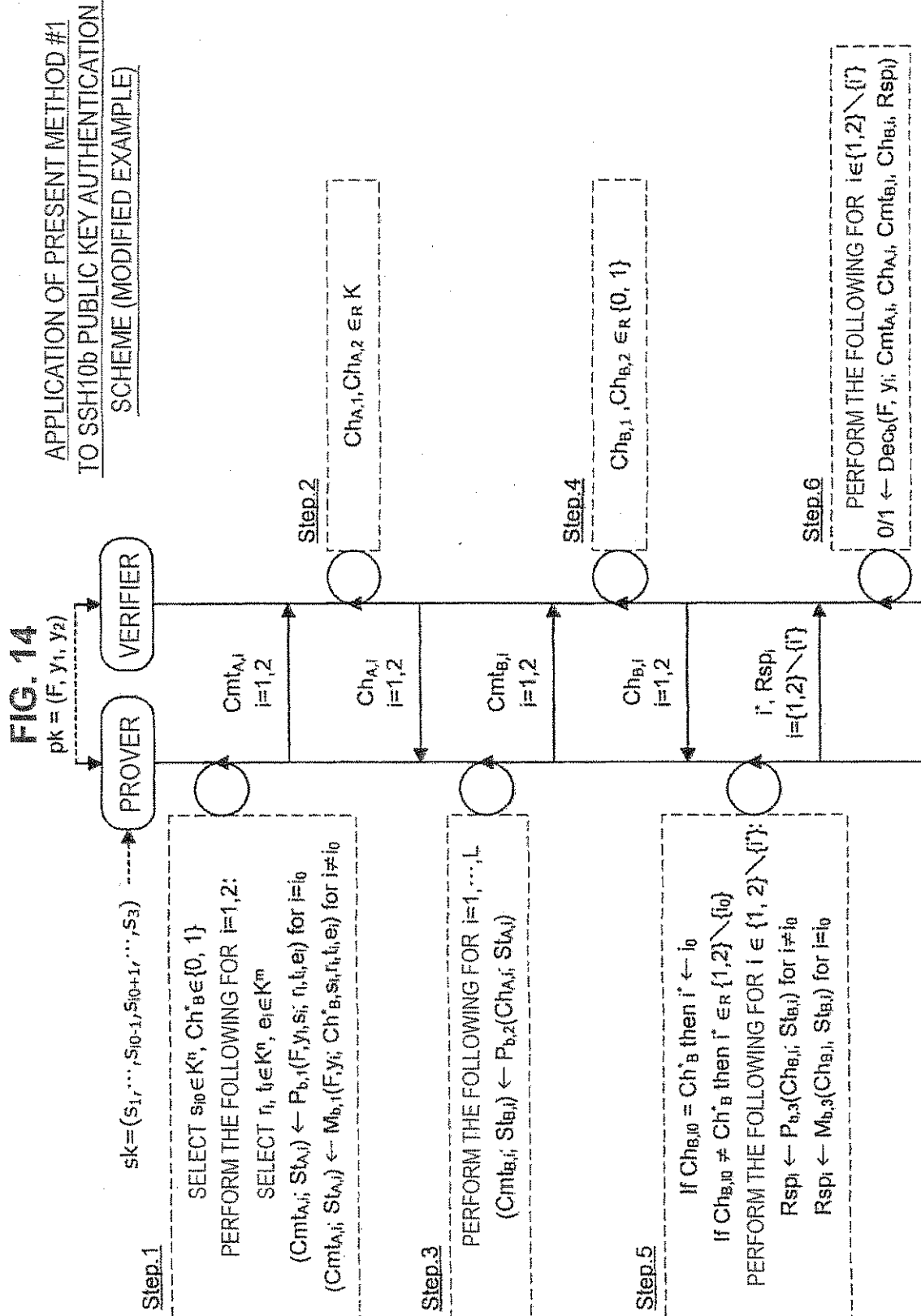


FIG. 15

APPLICATION OF PRESENT METHOD #2
TO SSH10a PUBLIC KEY AUTHENTICATION SCHEME

$pk = (F, y_1, \dots, y_L)$

PROVER

VERIFIER

$sk = (s_1, \dots, s_L)$

Step.1

PERFORM THE FOLLOWING FOR $i=1, \dots, L$:
SELECT $r_i, t_i \in K^m, e_i \in K^m$
($Cmt_i; St_i$) $\leftarrow P_{a,1}(F, y_i, s_i; r_i, t_i, e_i)$

Step.3

SELECT $d \in_R \{0, 1\}$
PERFORM THE FOLLOWING FOR $i=1, \dots, L$
 $Rsp_i \leftarrow P_{a,2}(Ch^{(d)}; St_i)$

Step.2

$Ch^{(0)}_1, \dots, Ch^{(0)}_L,$
 $Ch^{(1)}_1, \dots, Ch^{(1)}_L \in_R \{0, 1, 2\}$
WHERE $Ch^{(0)}_i \neq Ch^{(1)}_i$

Step.4

PERFORM THE FOLLOWING FOR $i=1, \dots, L$
 $0/1 \leftarrow Dec_a(F, y_i; Cmt_i, Ch^{(0)}_i, Rsp_i)$

$Cmt_i, i=1, \dots, L$

$Ch^{(0)}_i, Ch^{(1)}_i$
 $i=1, \dots, L$

d, Rsp_i
 $i=1, \dots, L$

FIG. 16

APPLICATION OF PRESENT METHOD #2
TO SSH10a PUBLIC KEY AUTHENTICATION
SCHEME (MODIFIED EXAMPLE)

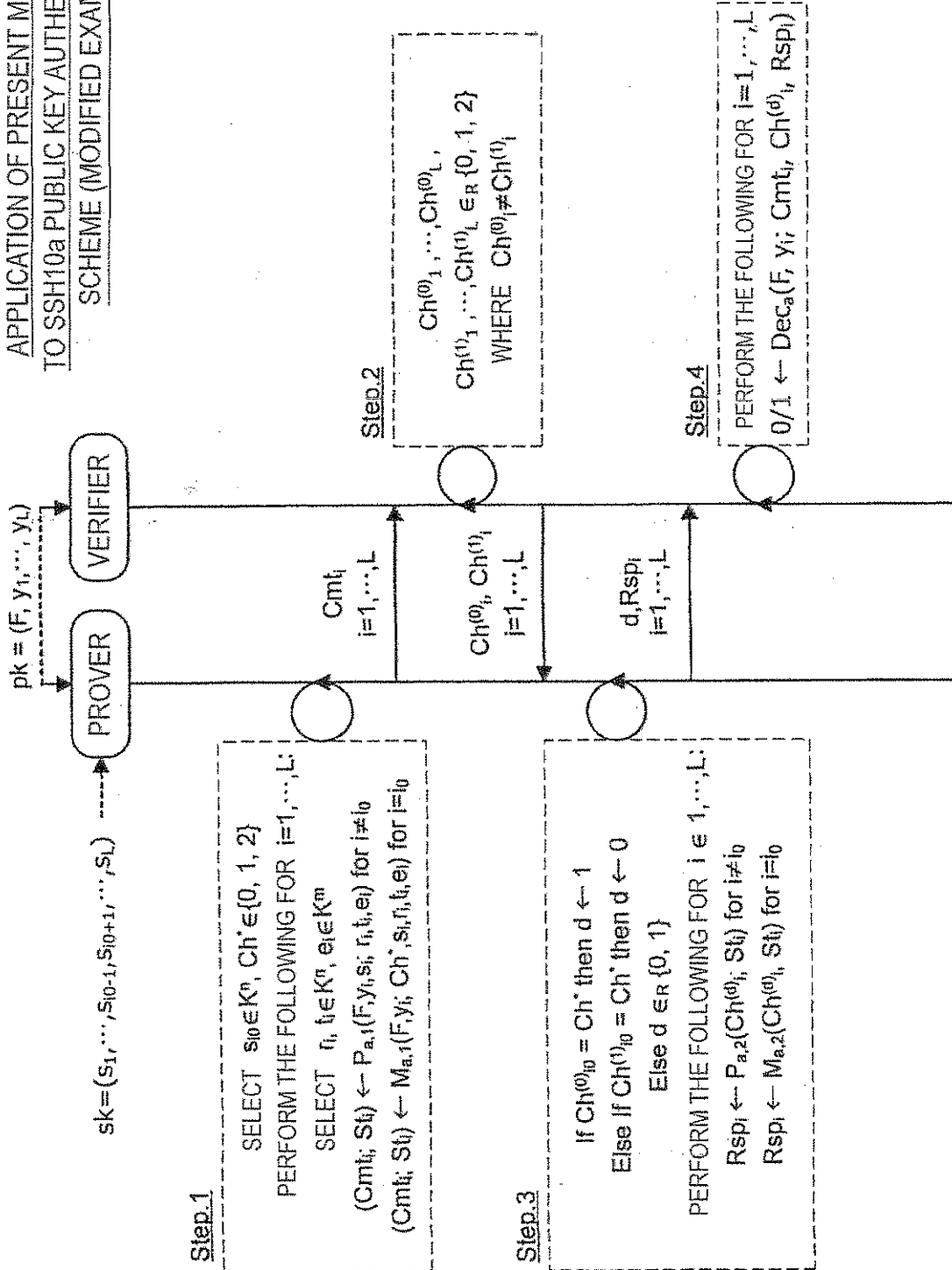


FIG. 17

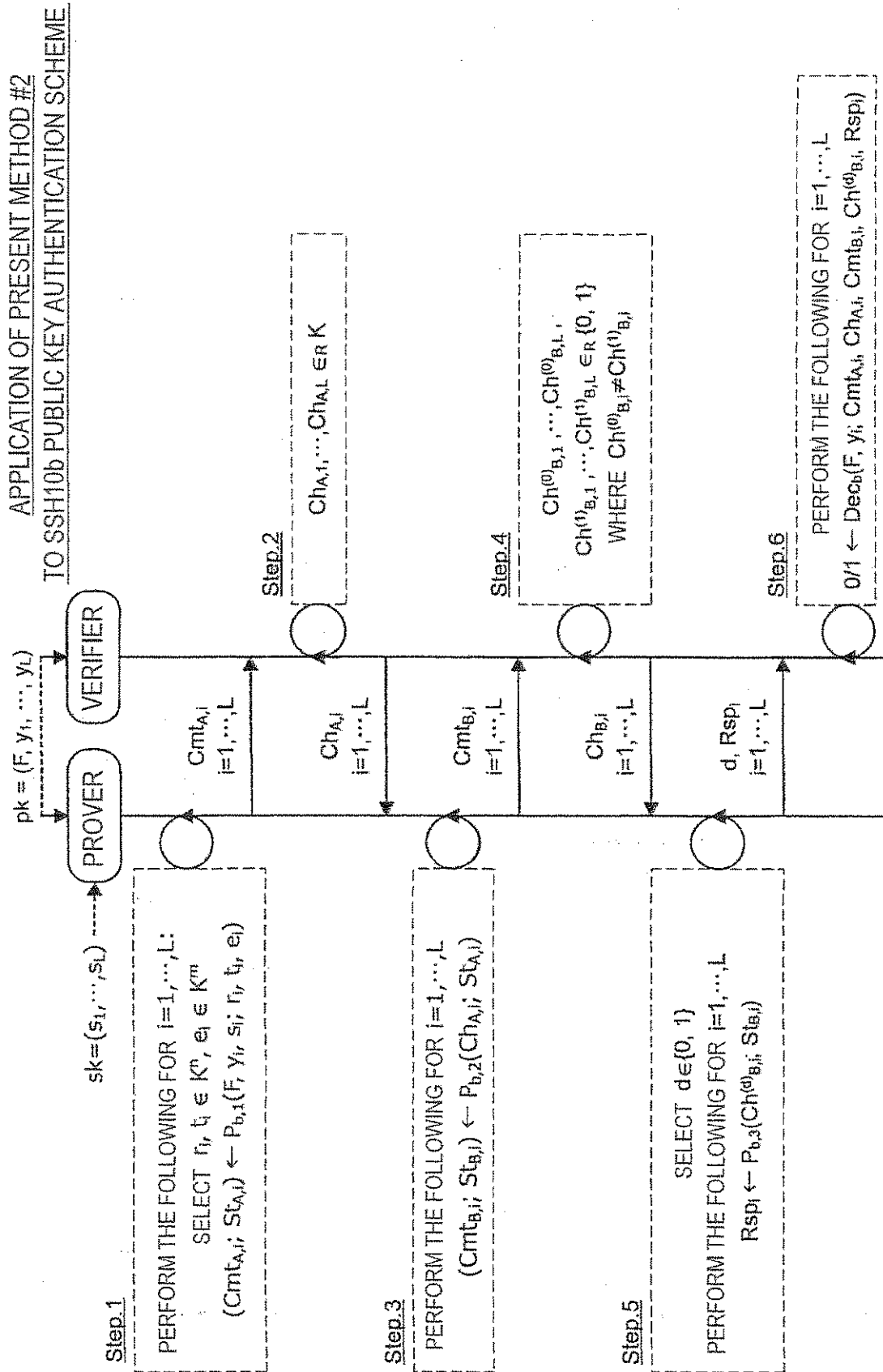
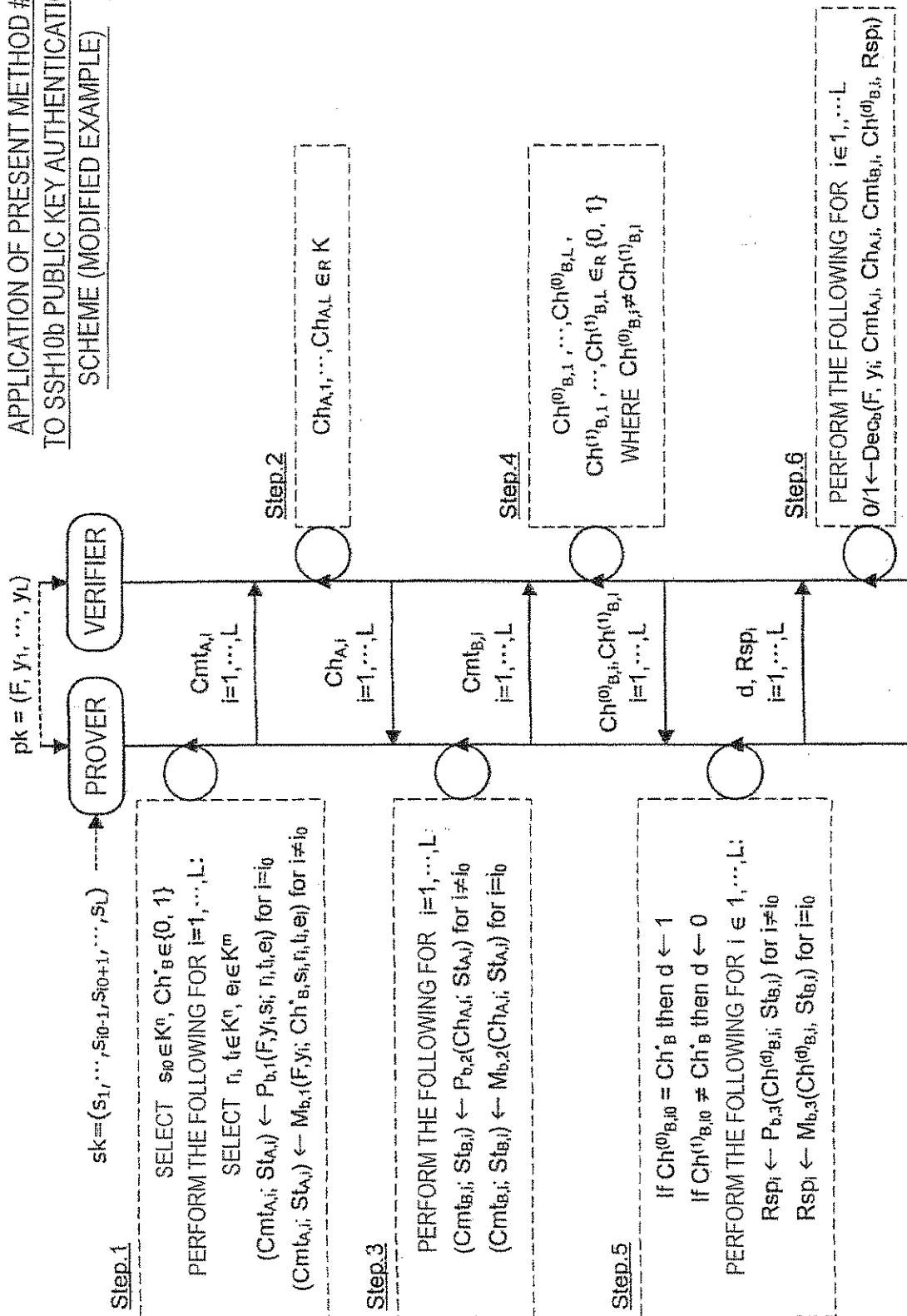
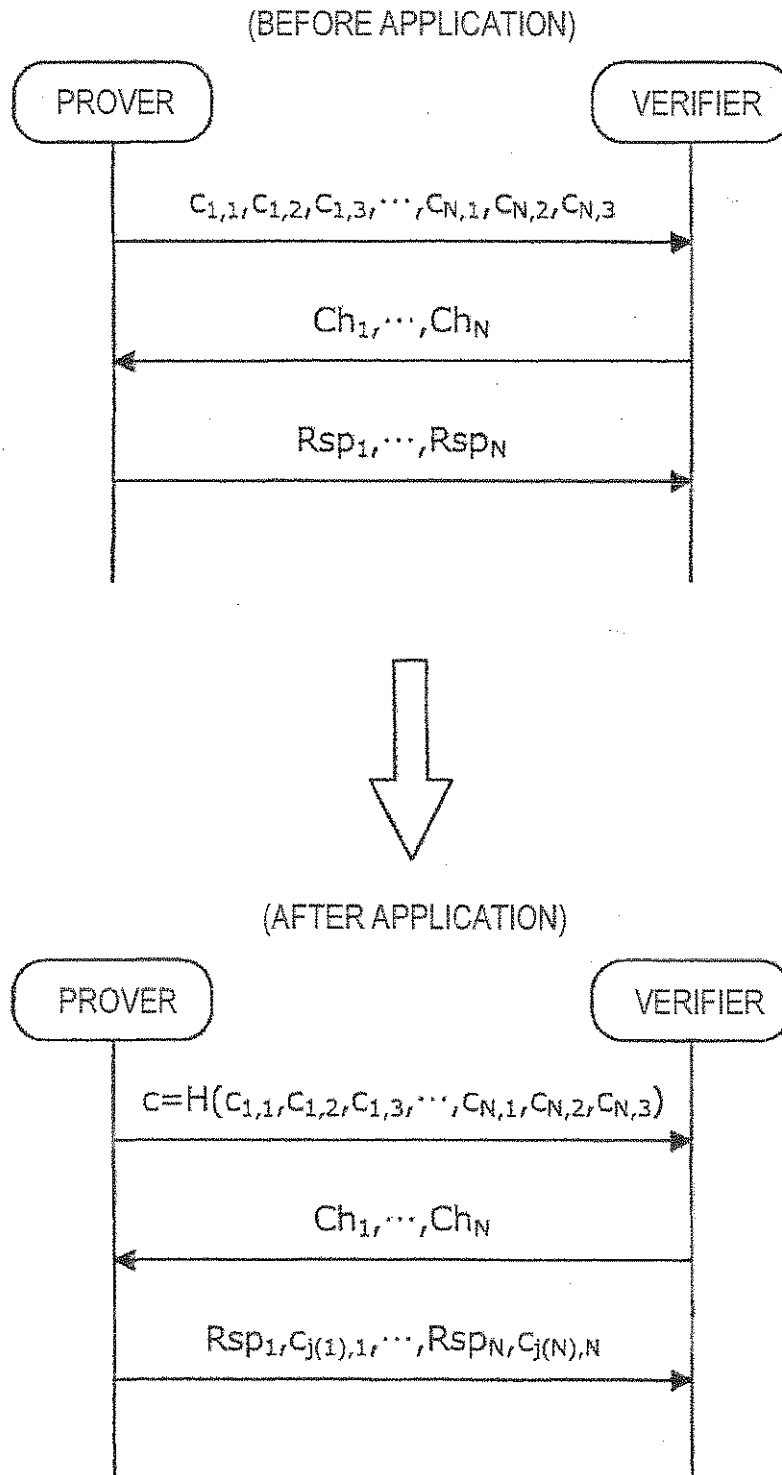


FIG. 18

APPLICATION OF PRESENT METHOD #2
TO SSH10b PUBLIC KEY AUTHENTICATION
SCHEME (MODIFIED EXAMPLE)



18/20
FIG. 19METHOD OF REDUCING COMMUNICATION AMOUNT (CASE OF SSH10a)

19/20
FIG. 20

METHOD OF REDUCING COMMUNICATION AMOUNT (CASE OF SSH10b)

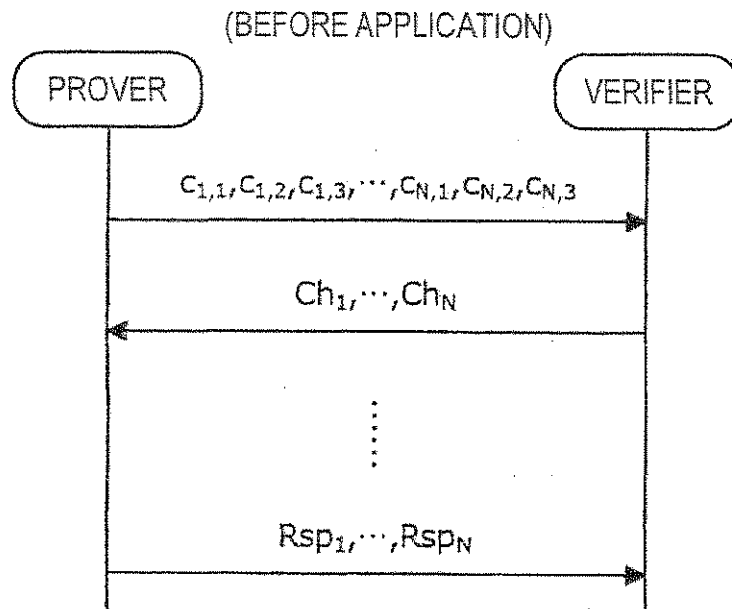
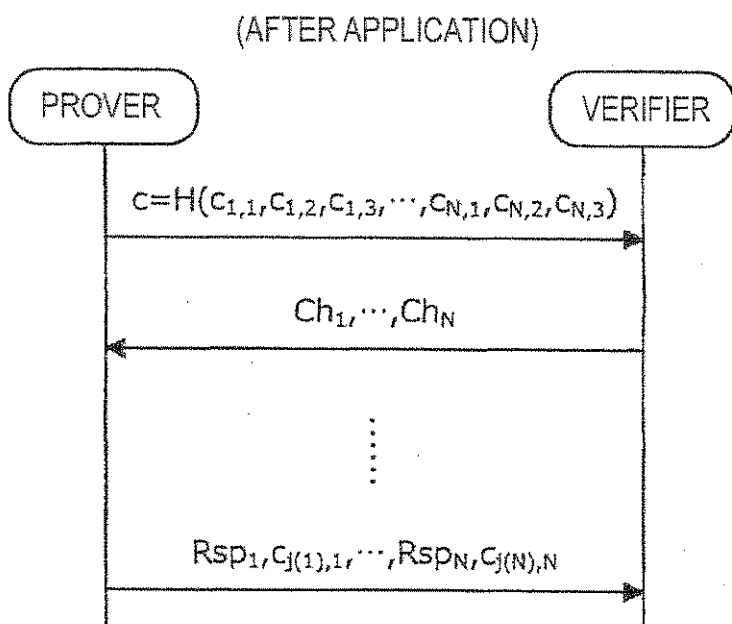


FIG. 21

