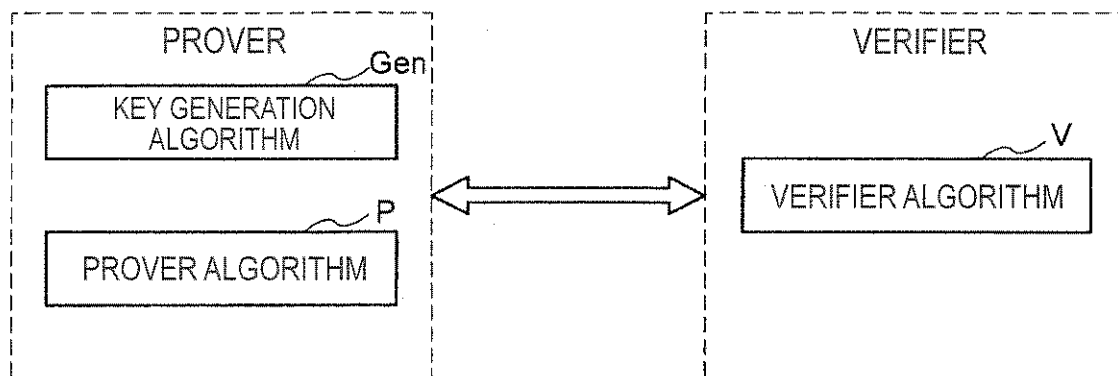


1/20
FIG. 1PUBLIC KEY AUTHENTICATION SCHEME

2/20
FIG. 2

N-PASS PUBLIC KEY AUTHENTICATION SCHEME

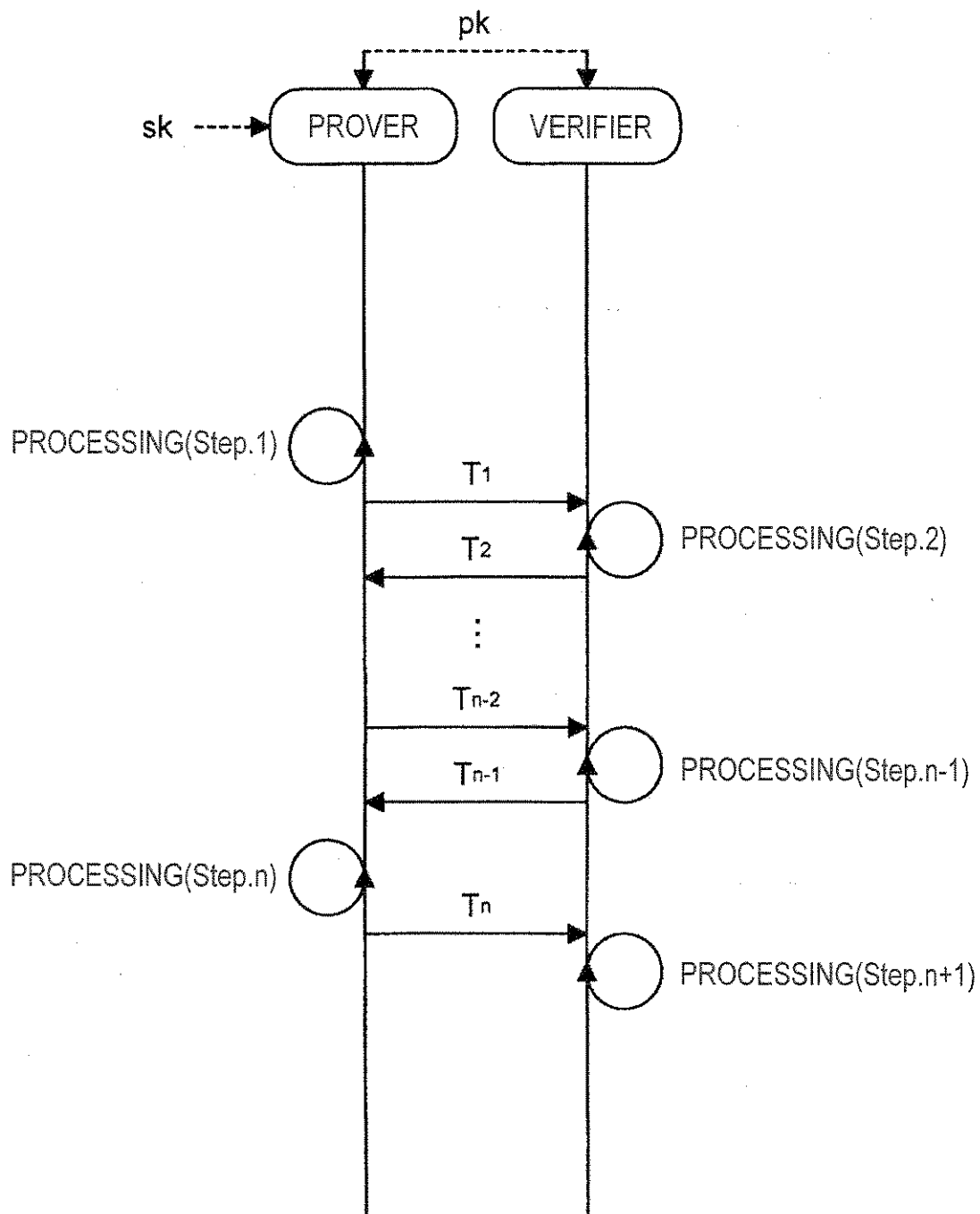


FIG. 3

SSH10a PUBLIC KEY AUTHENTICATION SCHEME

$pk = (F, y)$

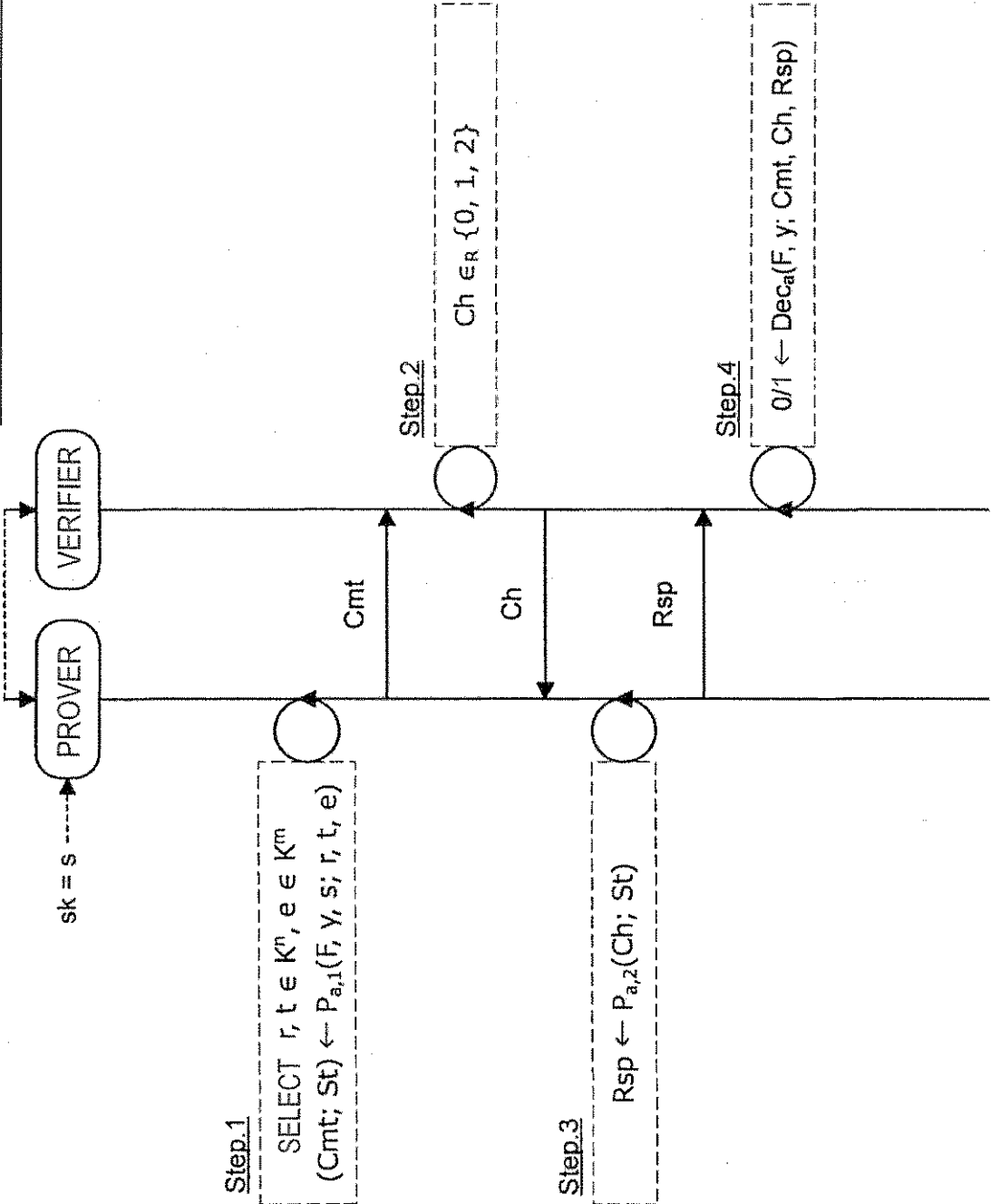
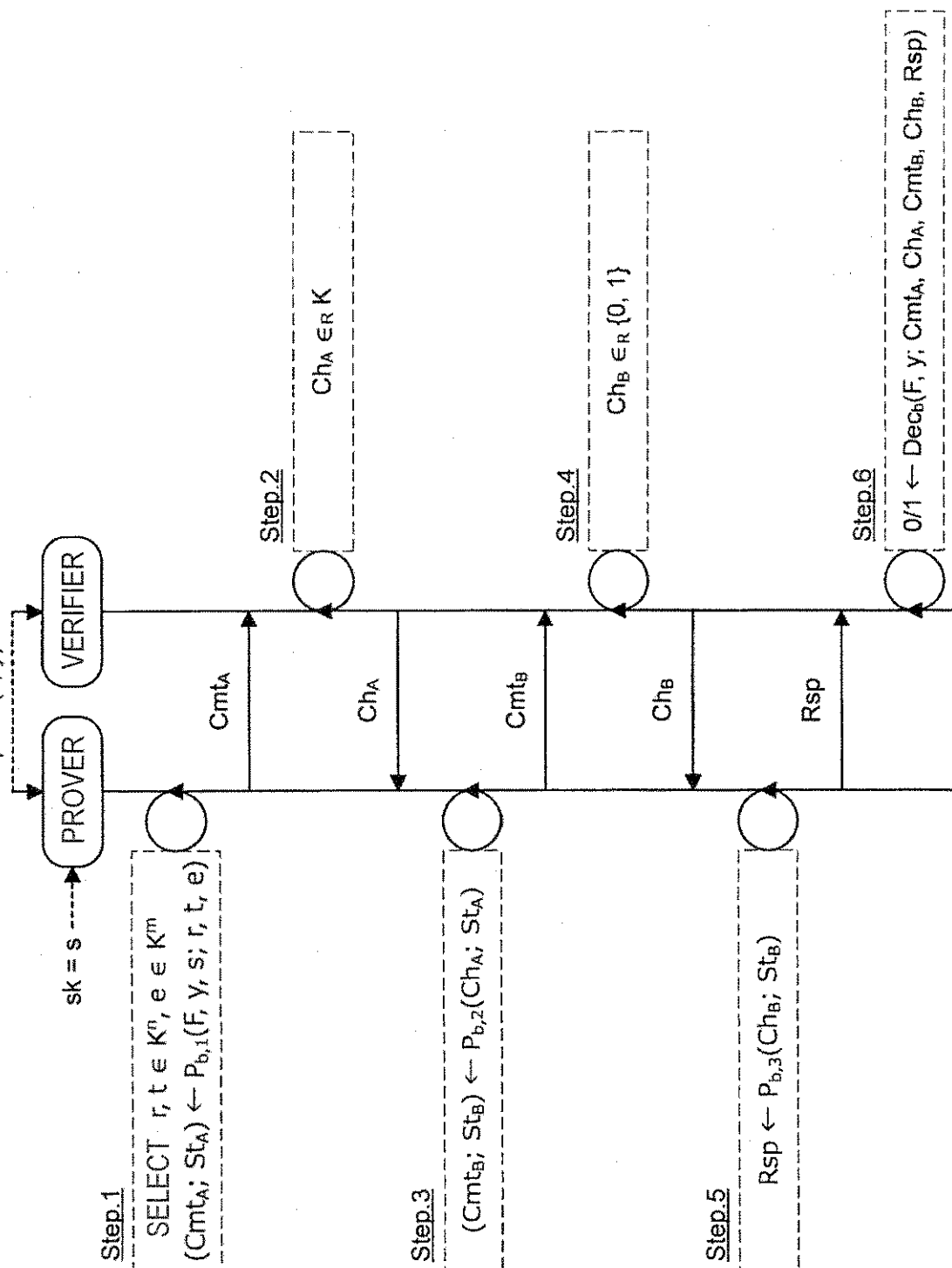


FIG. 4
SSH10b PUBLIC KEY AUTHENTICATION SCHEME



5/20

FIG. 5

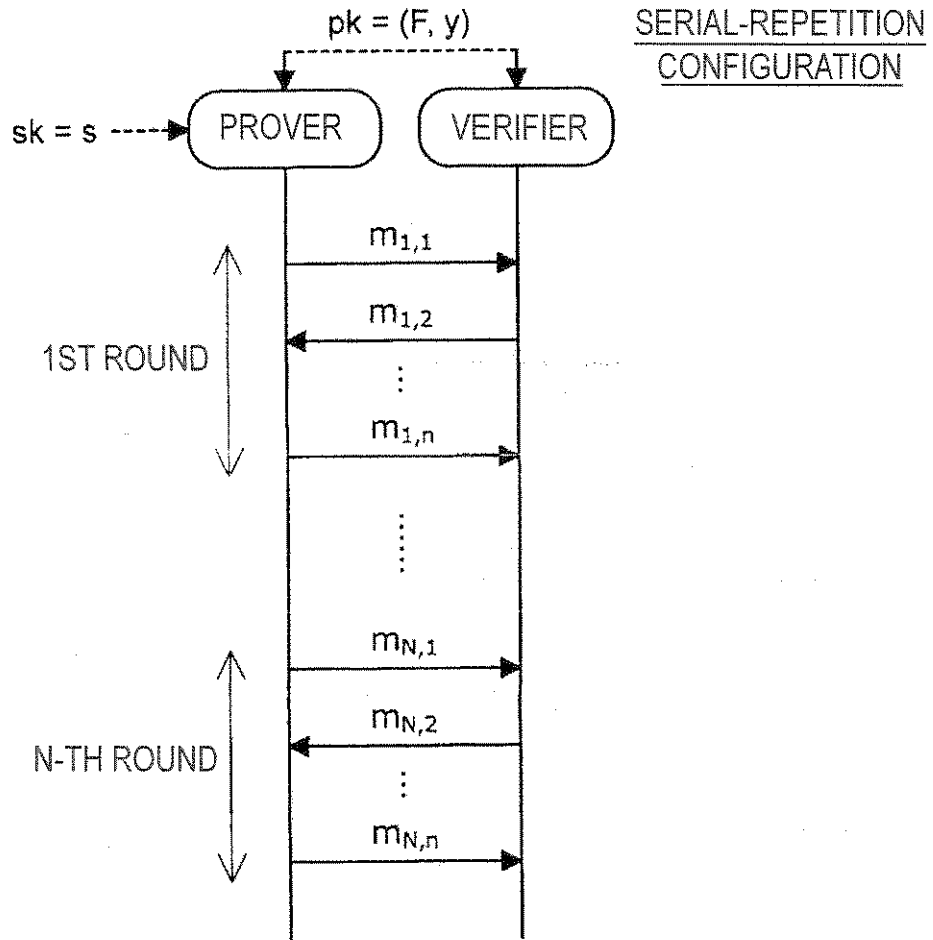


FIG. 6

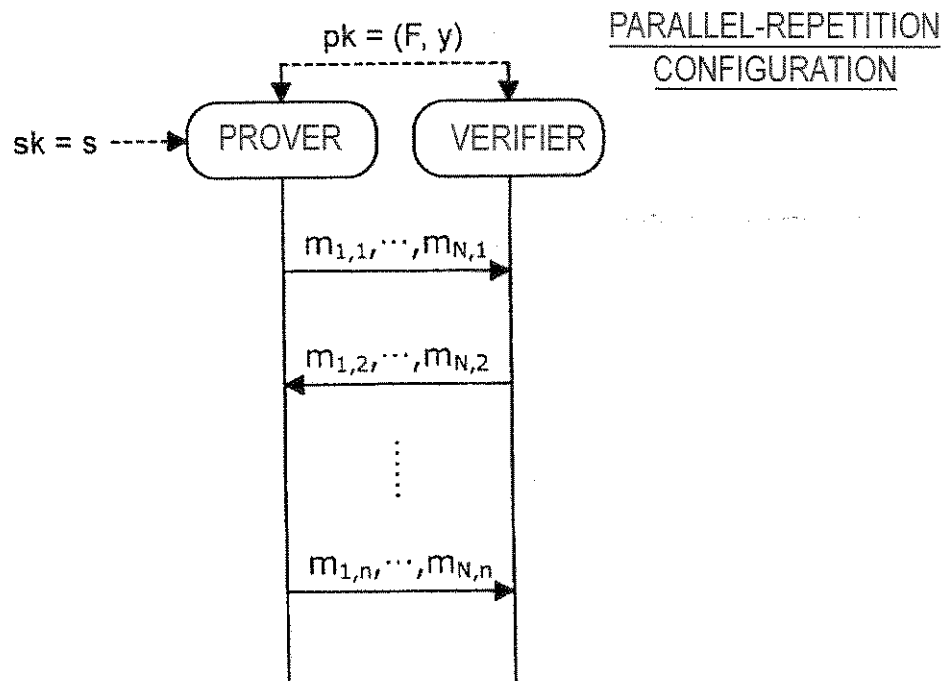


FIG. 7

FALSIFICATION ALGORITHM FOR SSH10a
PUBLIC KEY AUTHENTICATION SCHEME

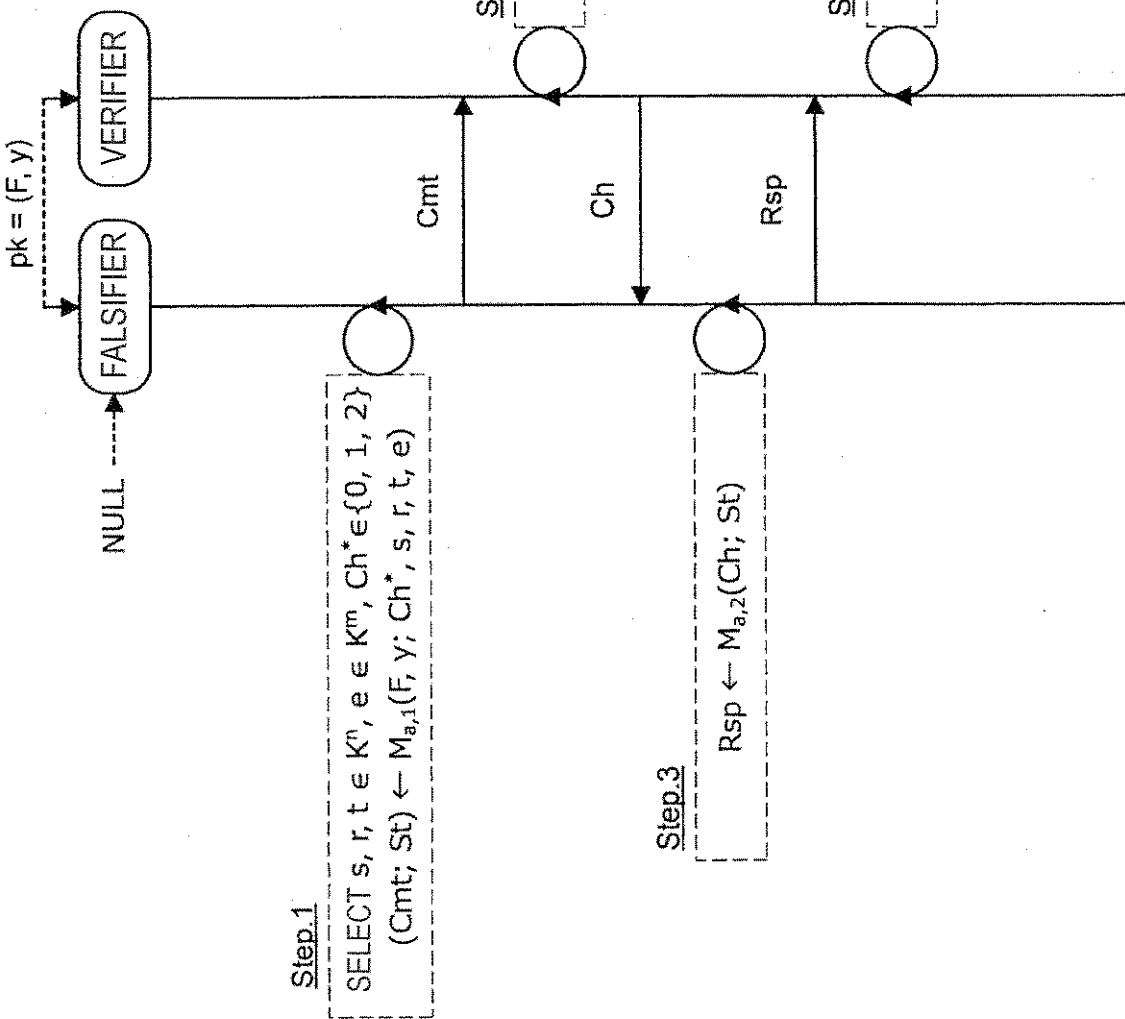


FIG. 8
FALSIFICATION ALGORITHM FOR SSH10b
PUBLIC KEY AUTHENTICATION SCHEME

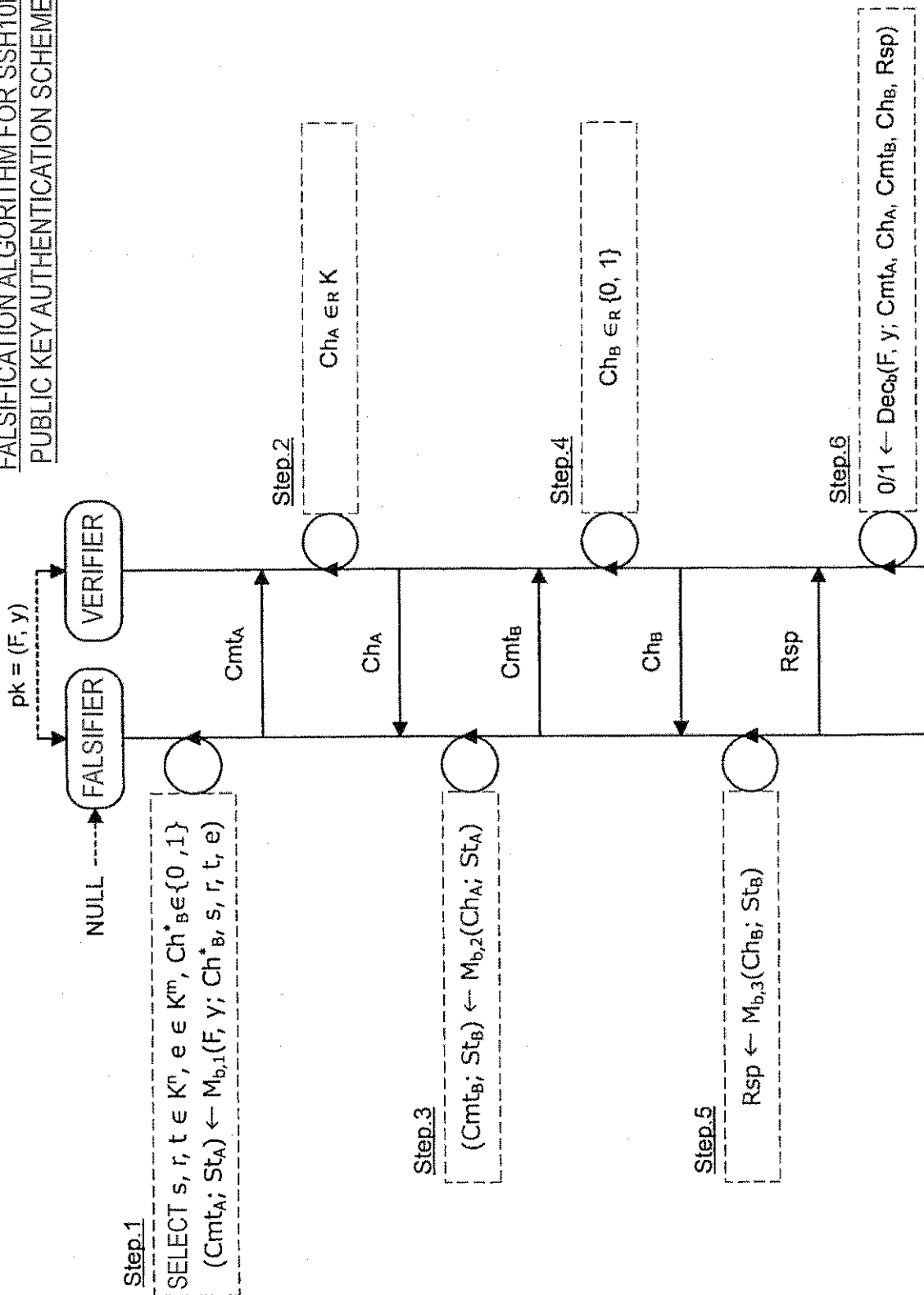


FIG. 9

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

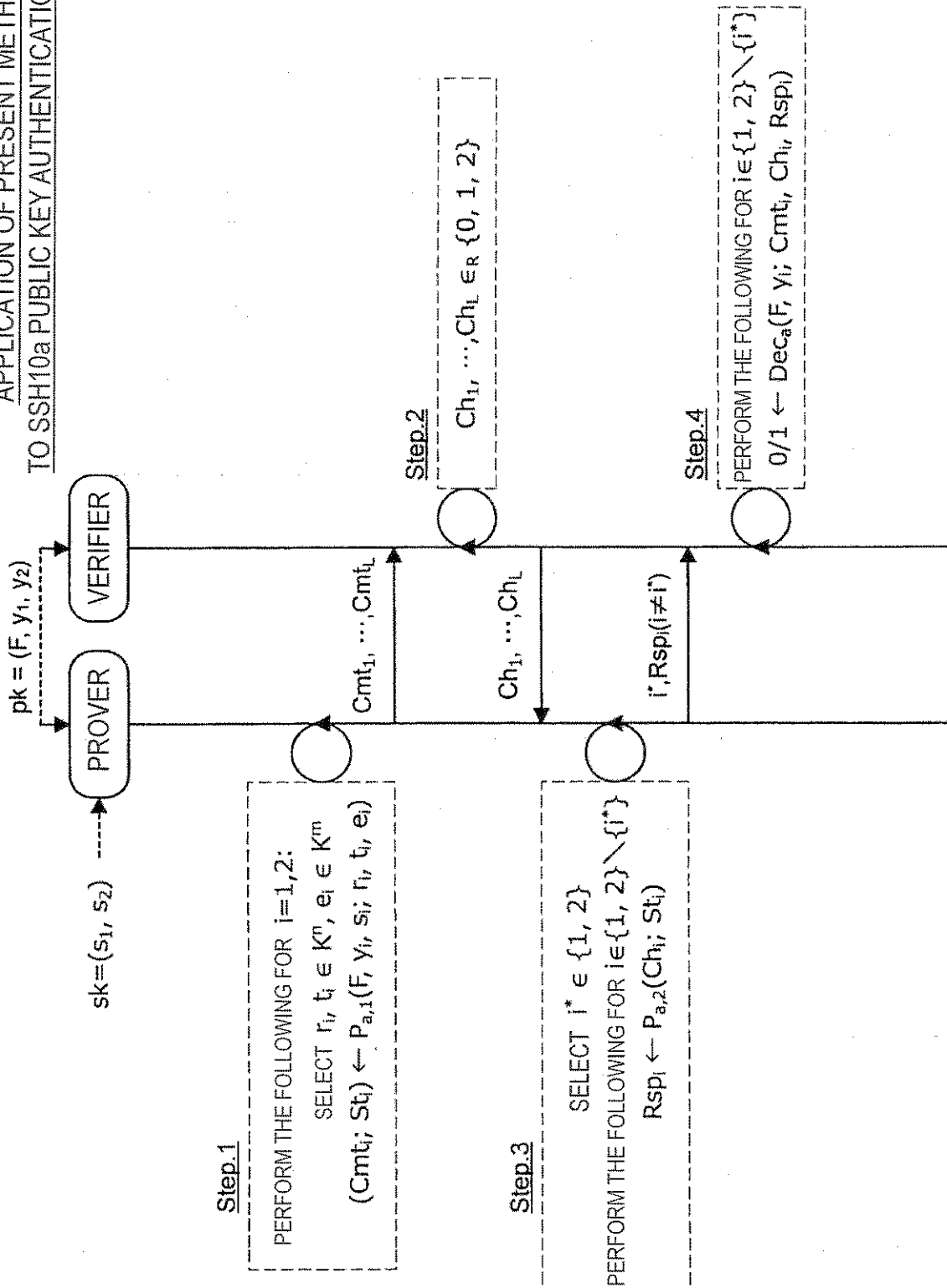
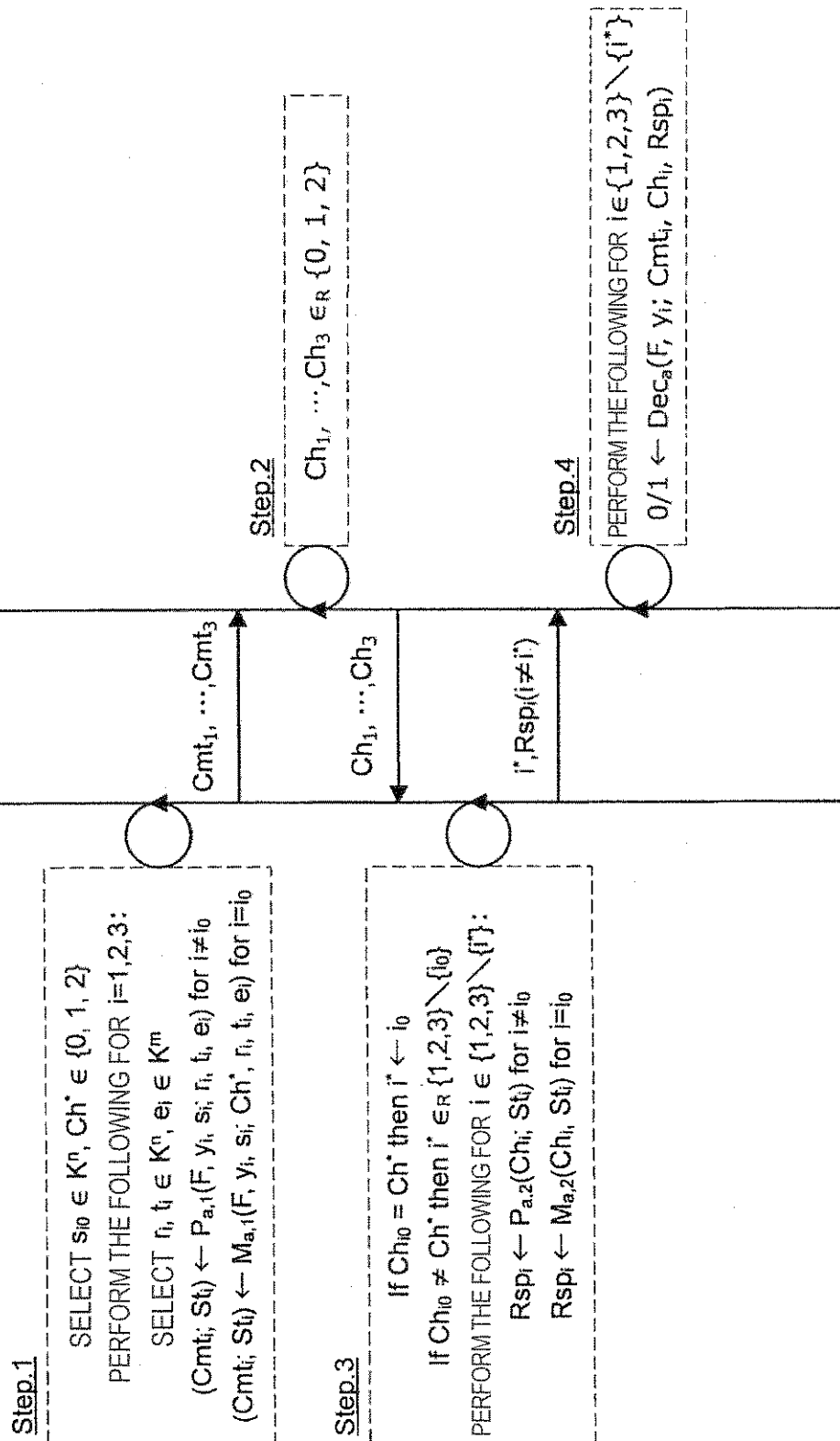


FIG. 10

pk = (F, y₁, y₂, y₃)
 APPLICATION OF PRESENT METHOD #1
 TO SSH10a PUBLIC KEY AUTHENTICATION
 SCHEME (MODIFIED EXAMPLE 1)



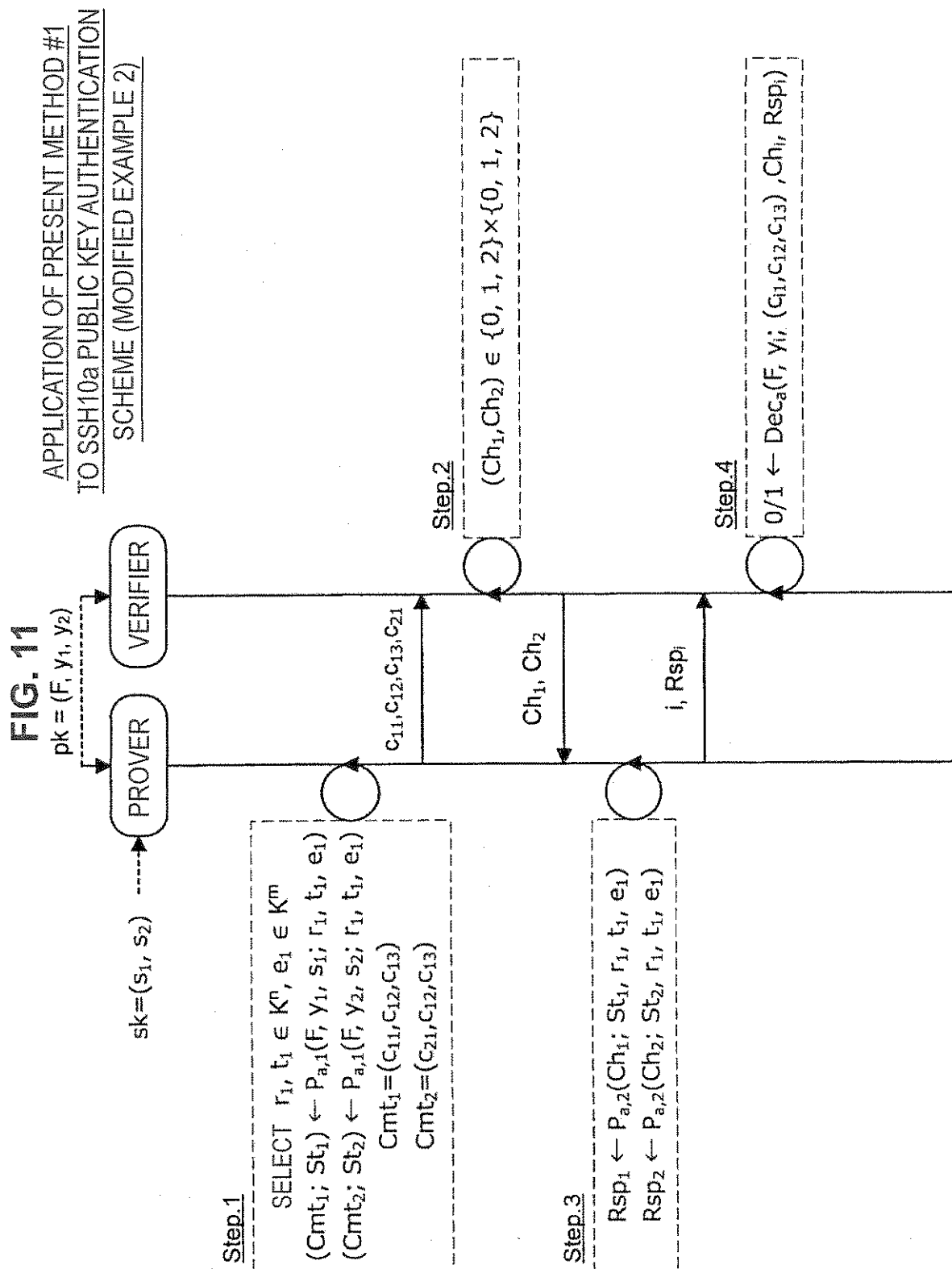


FIG. 12

APPLICATION OF PRESENT METHOD #1
TO SSH10a PUBLIC KEY AUTHENTICATION
SCHEME (MODIFIED EXAMPLE 3)

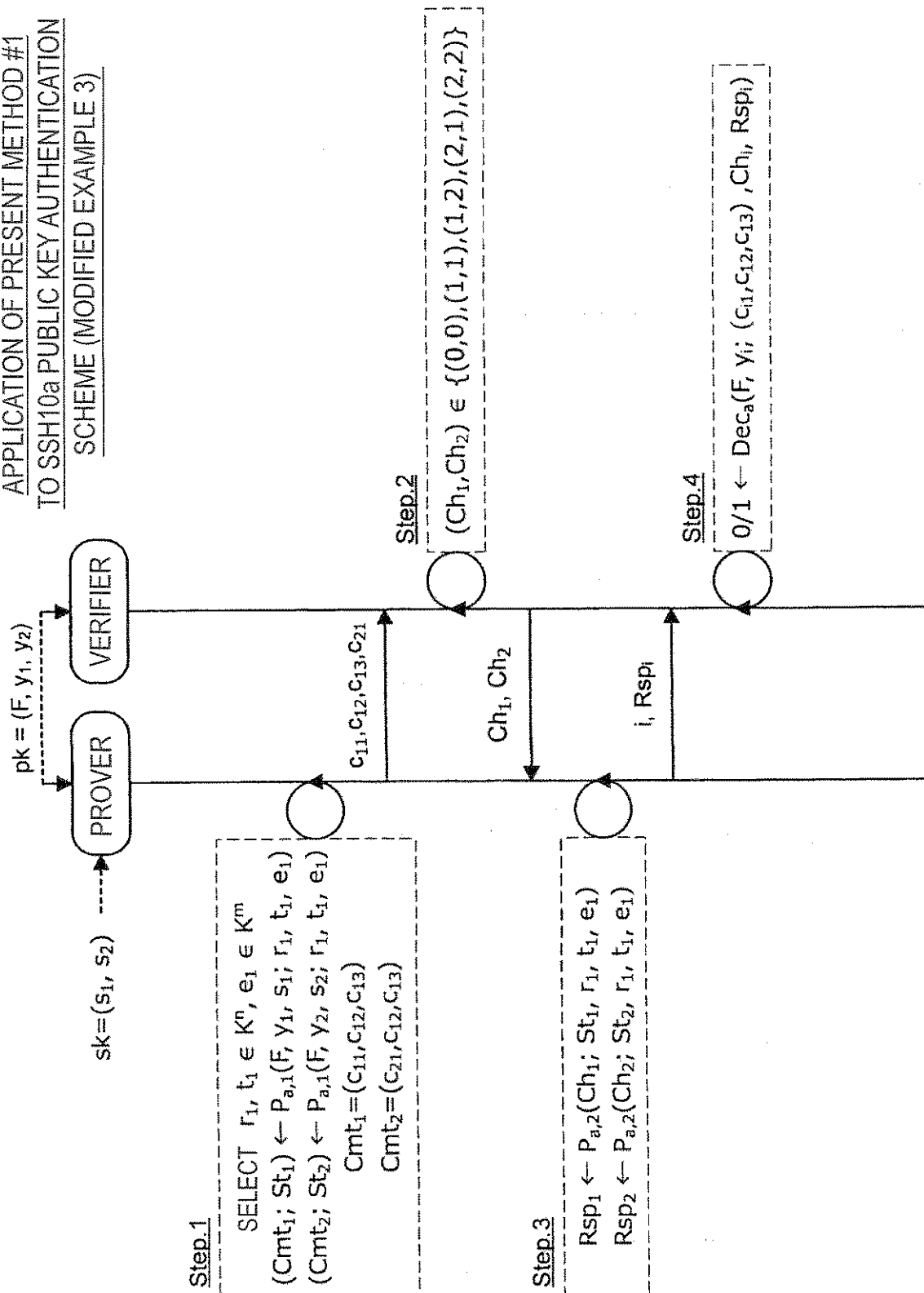
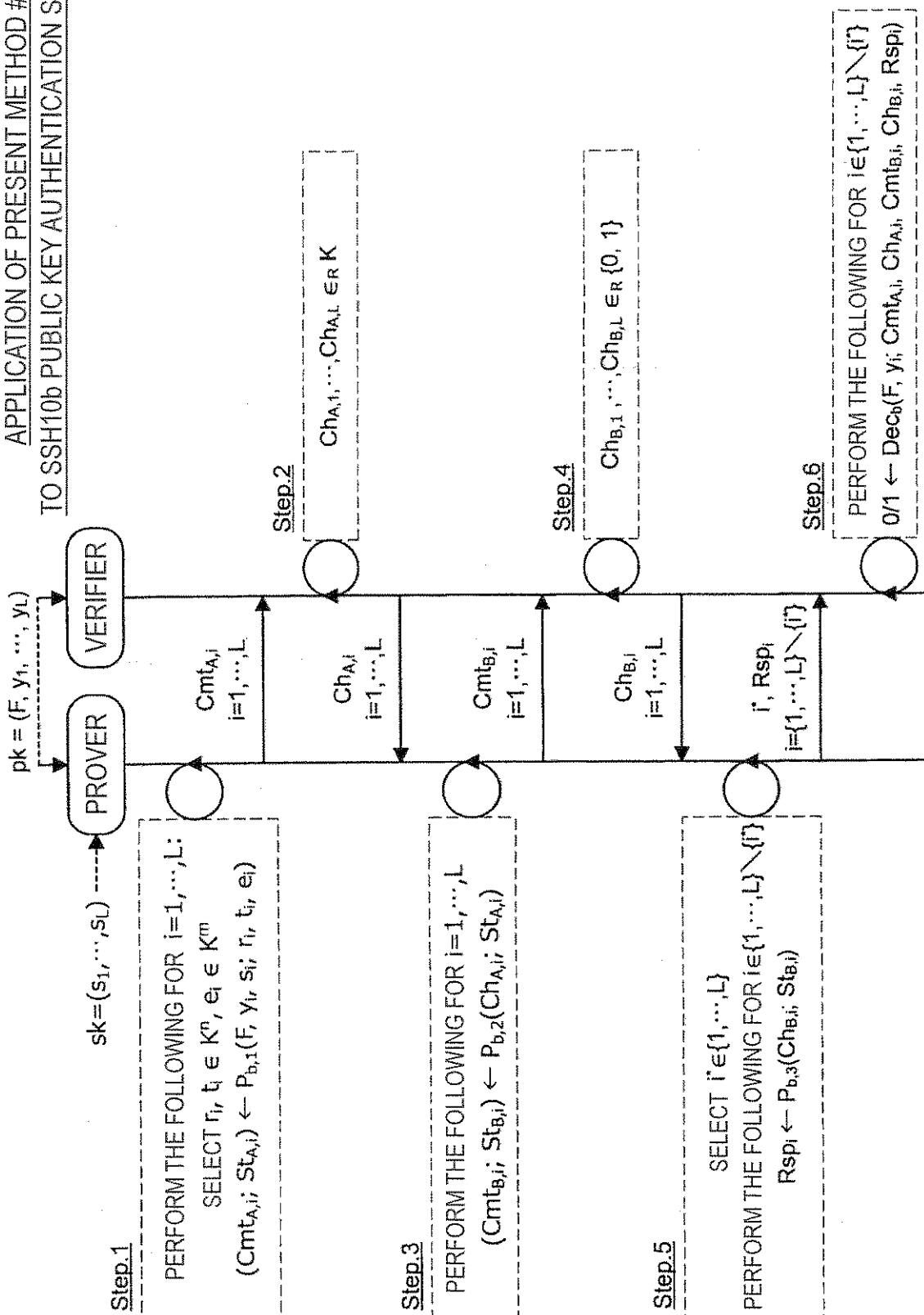


FIG. 13

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



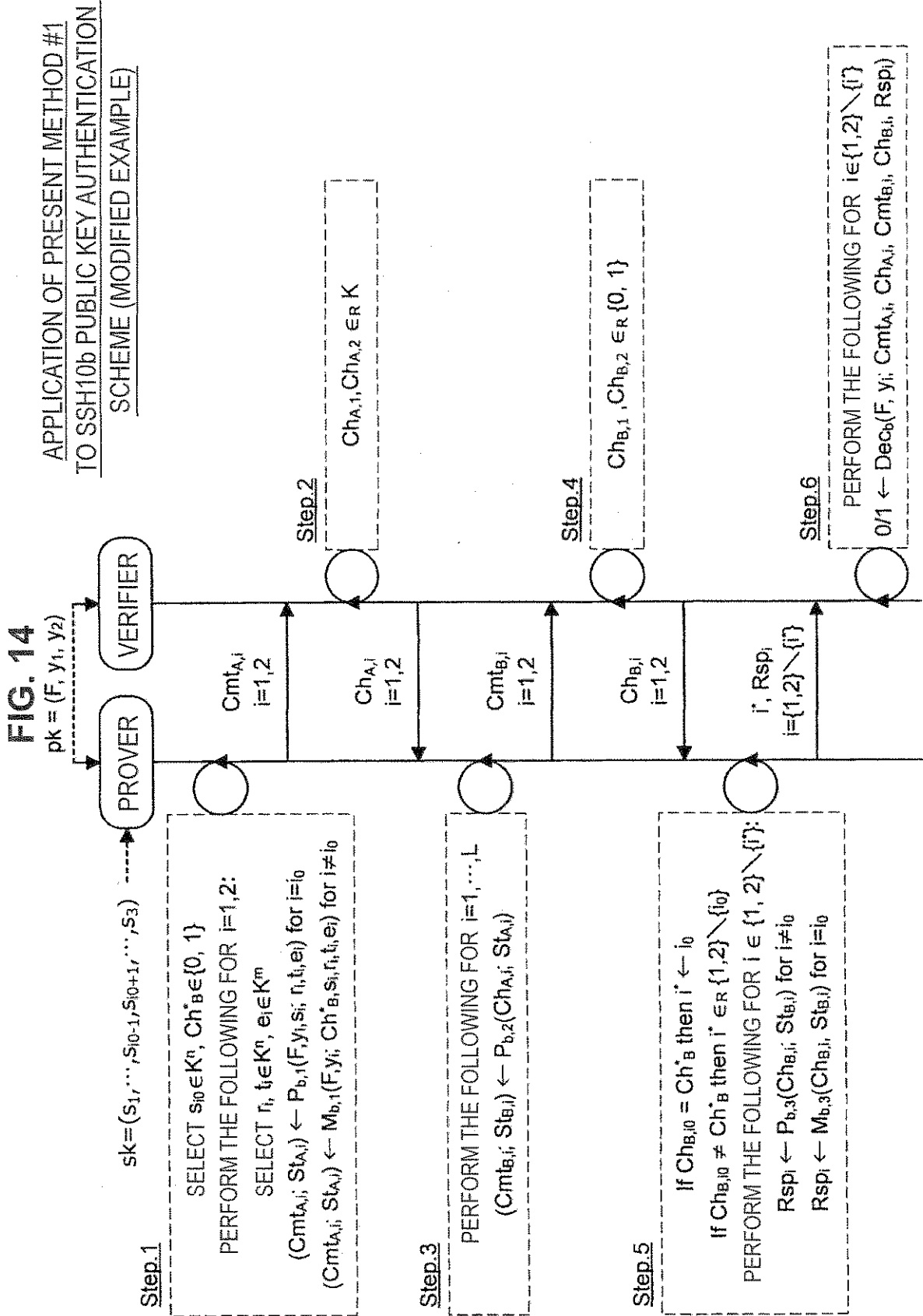


FIG. 15

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

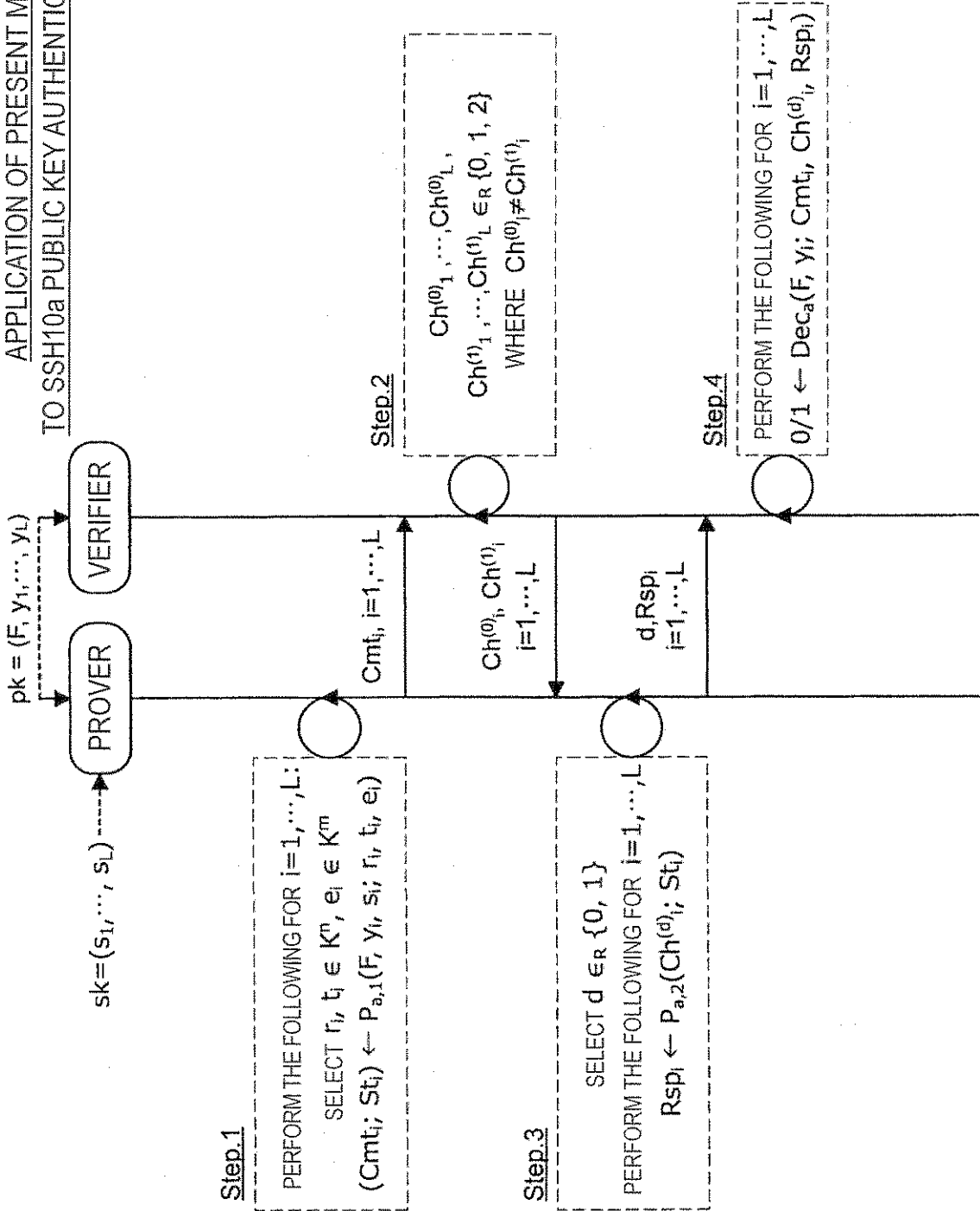


FIG. 16

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

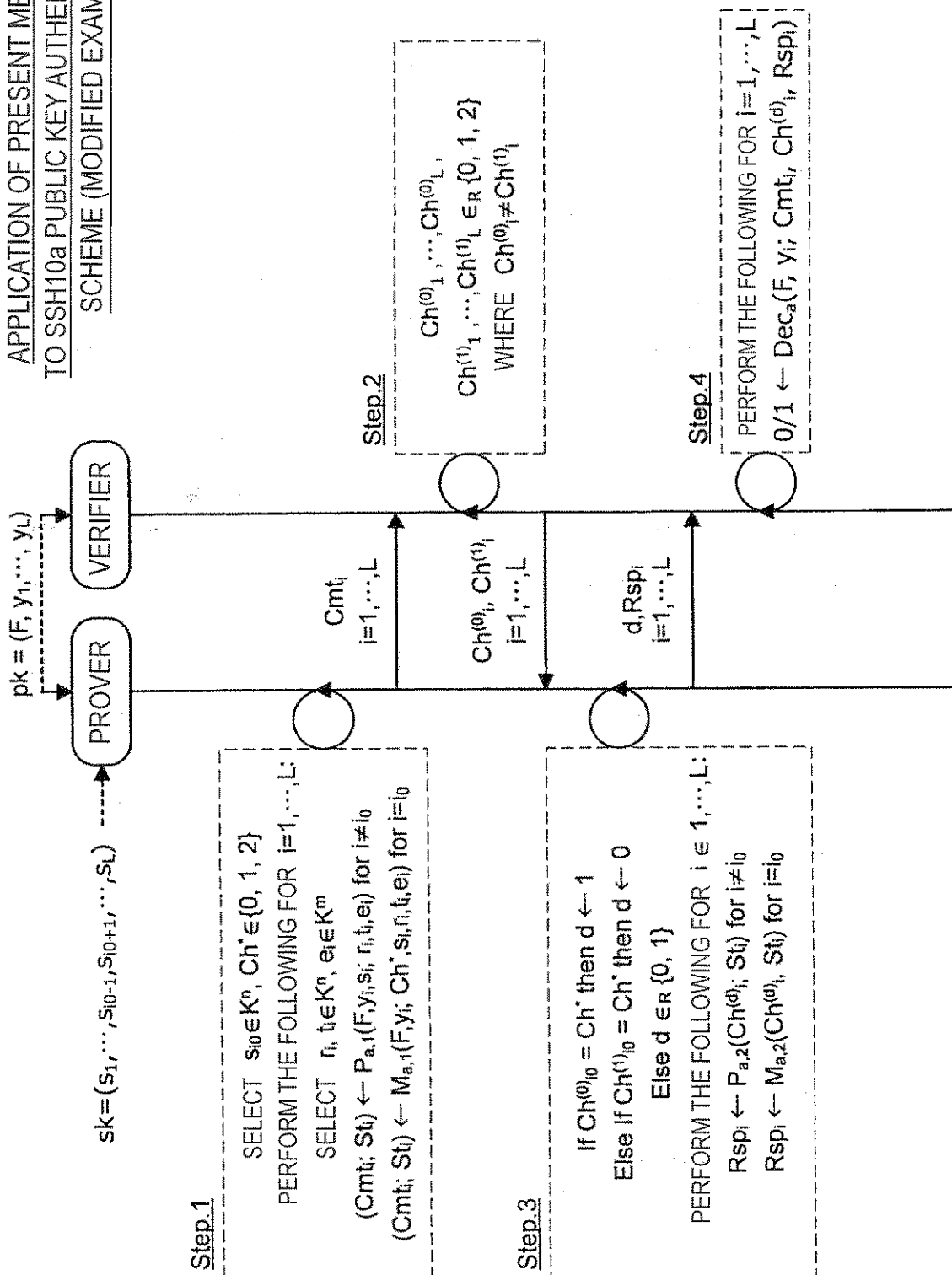


FIG. 17

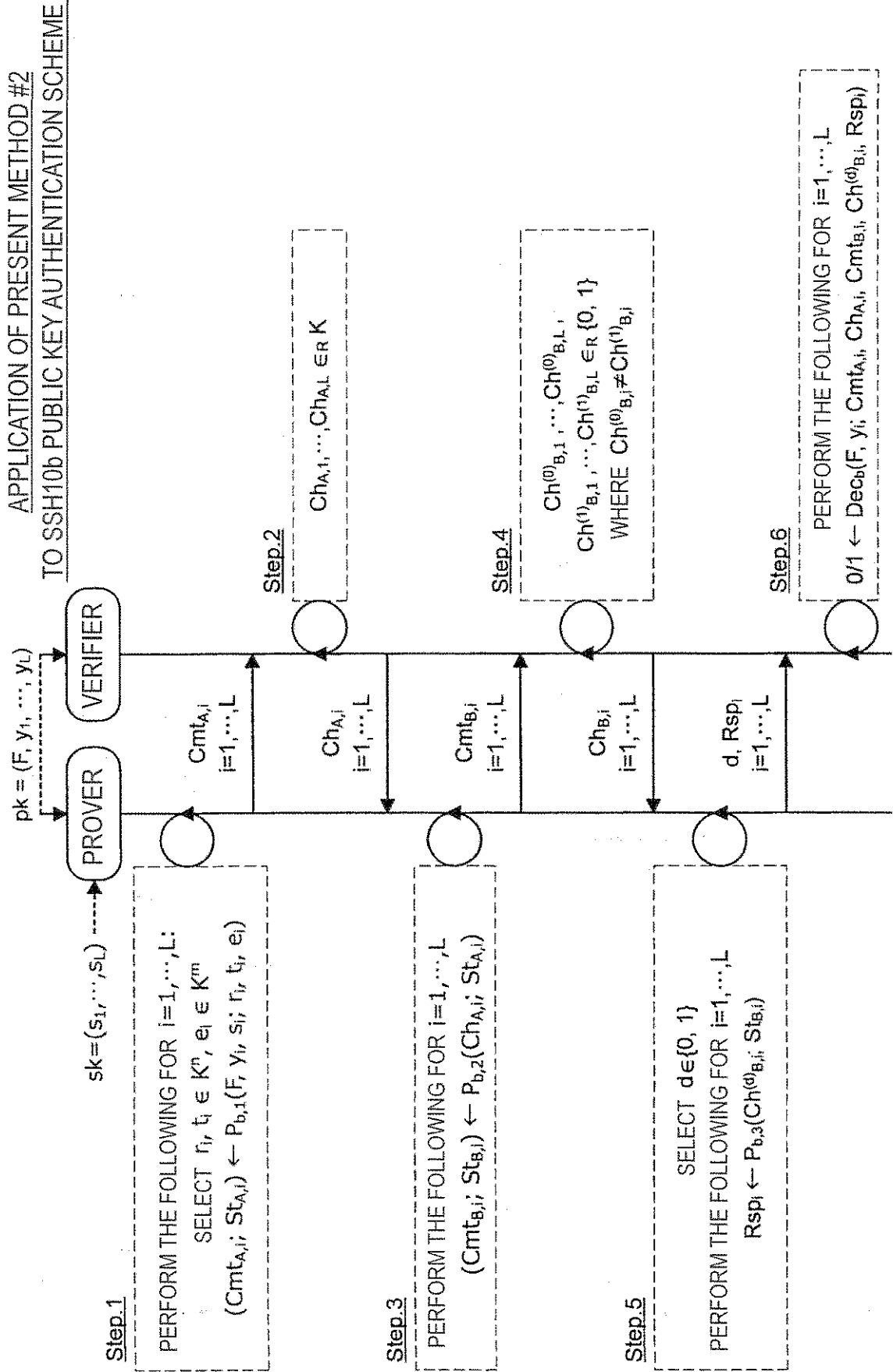
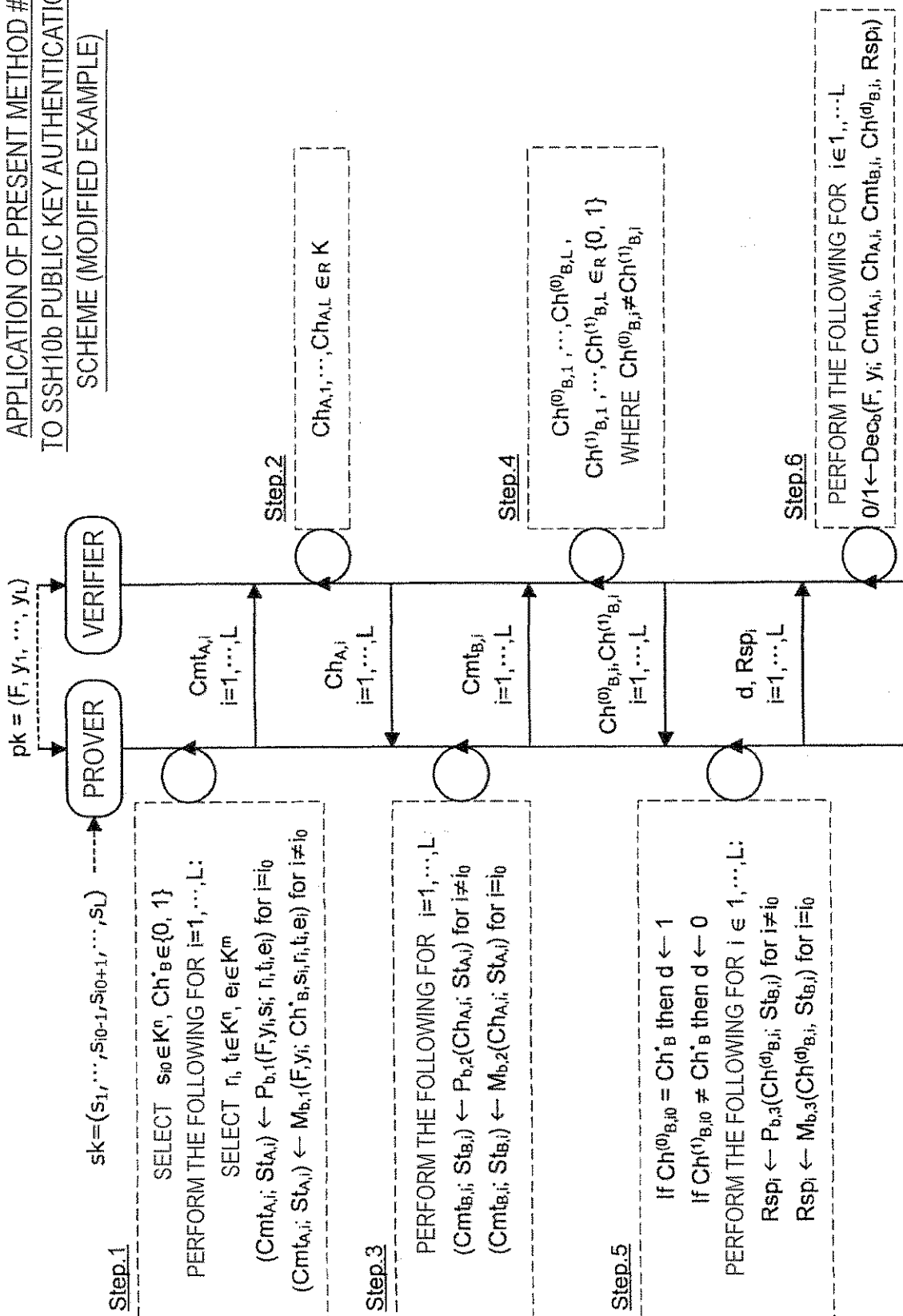
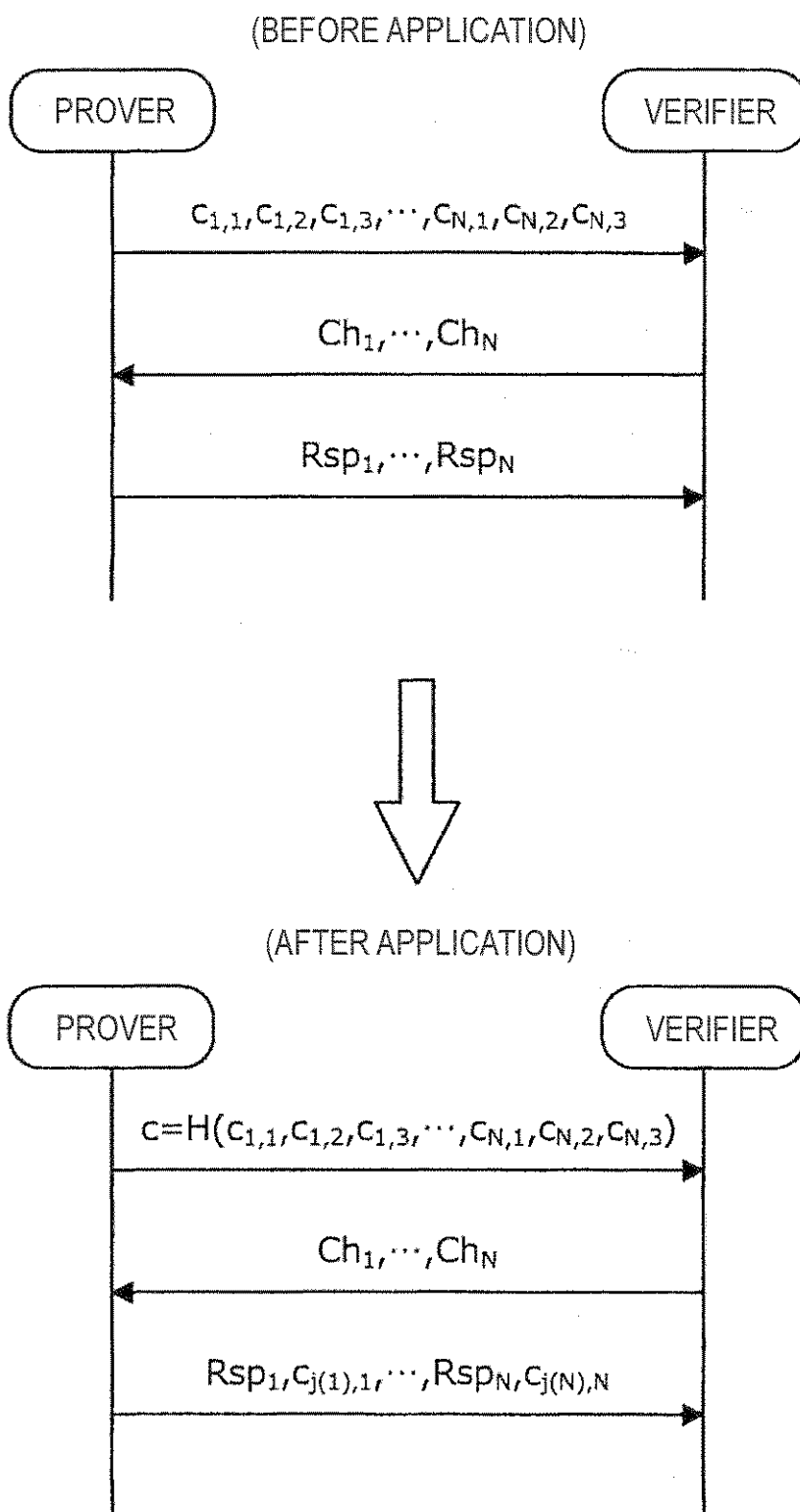


FIG. 18

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)

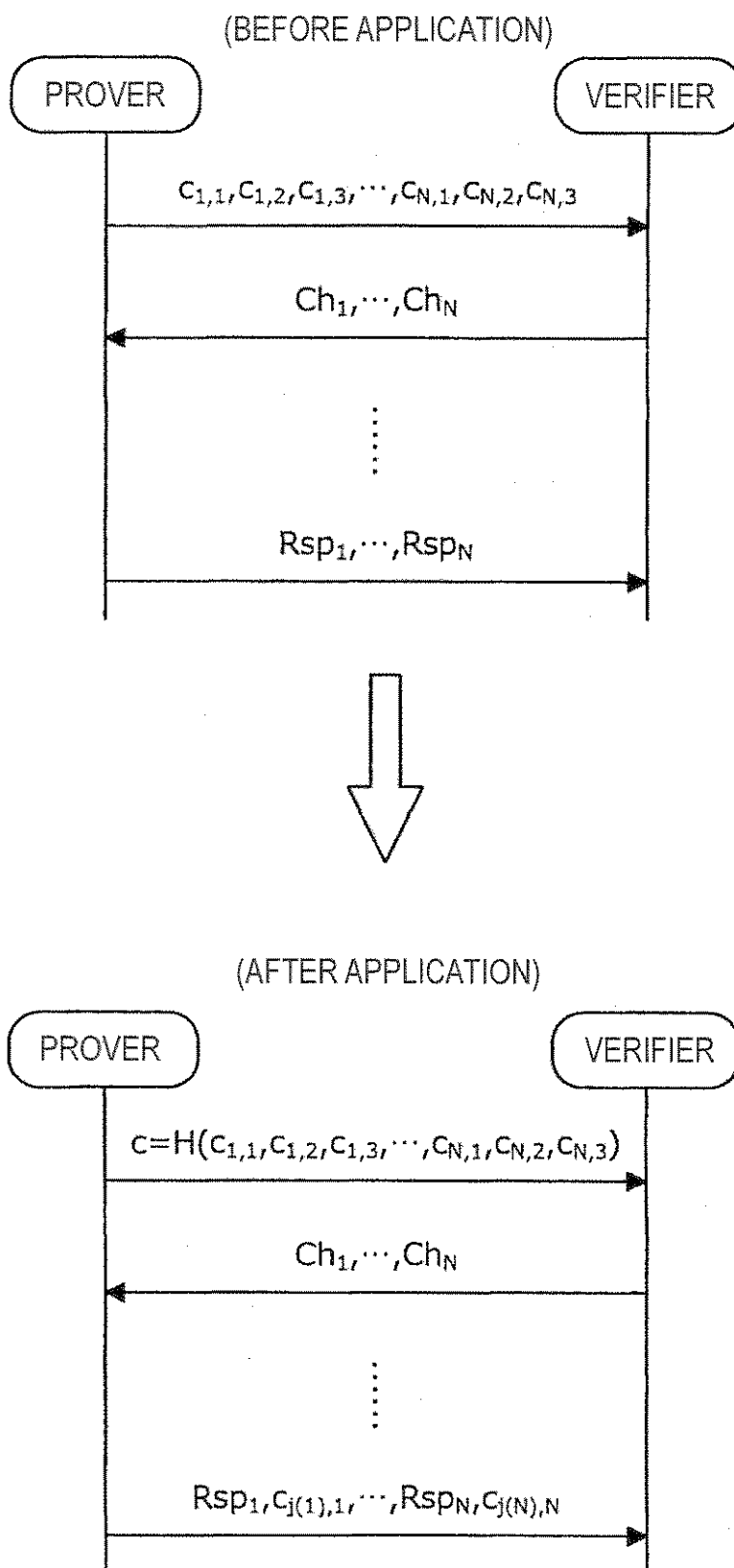


FIG. 21

