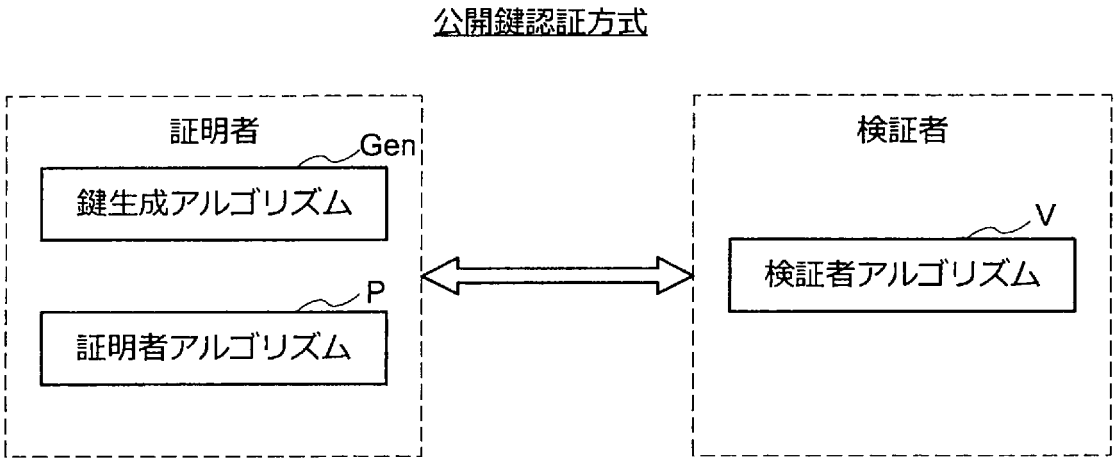
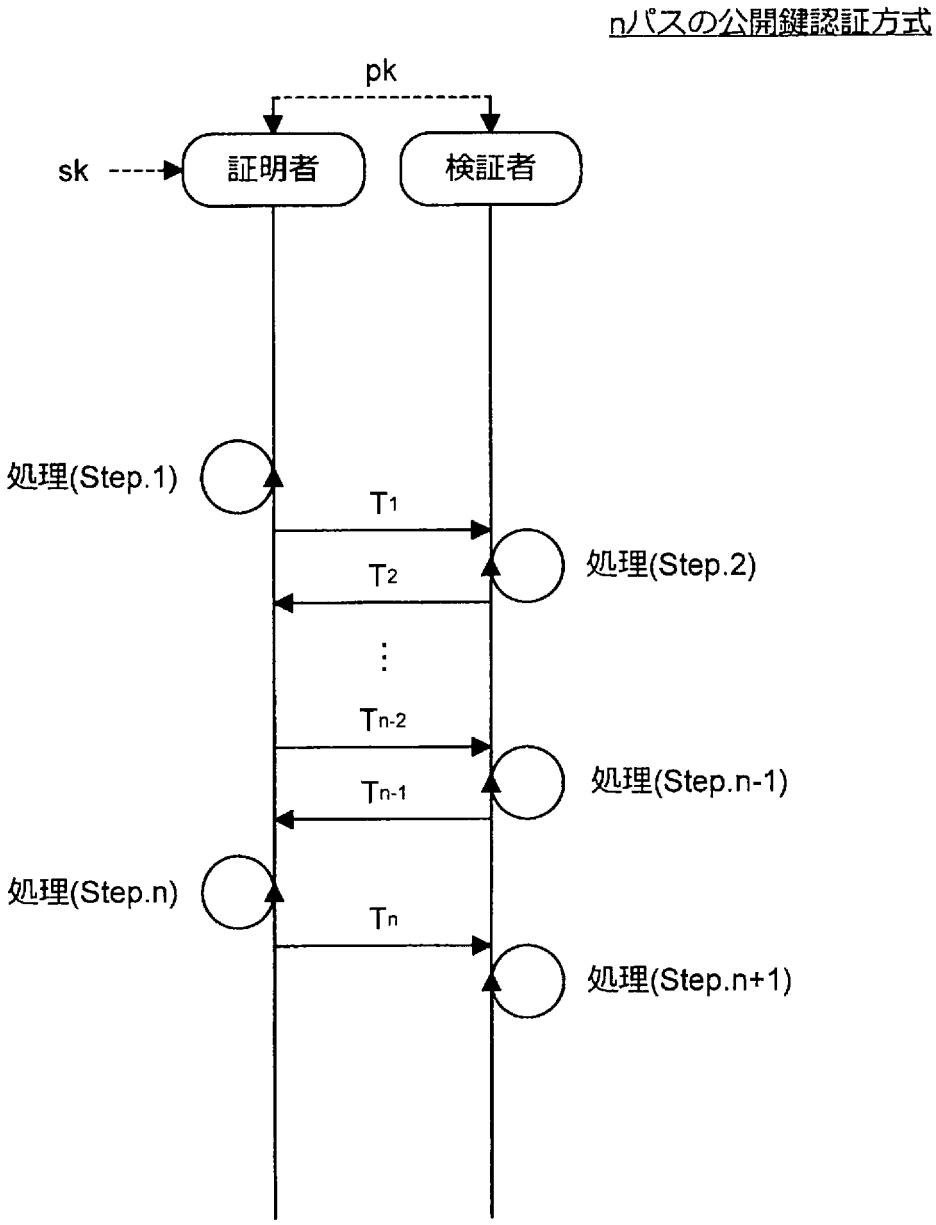
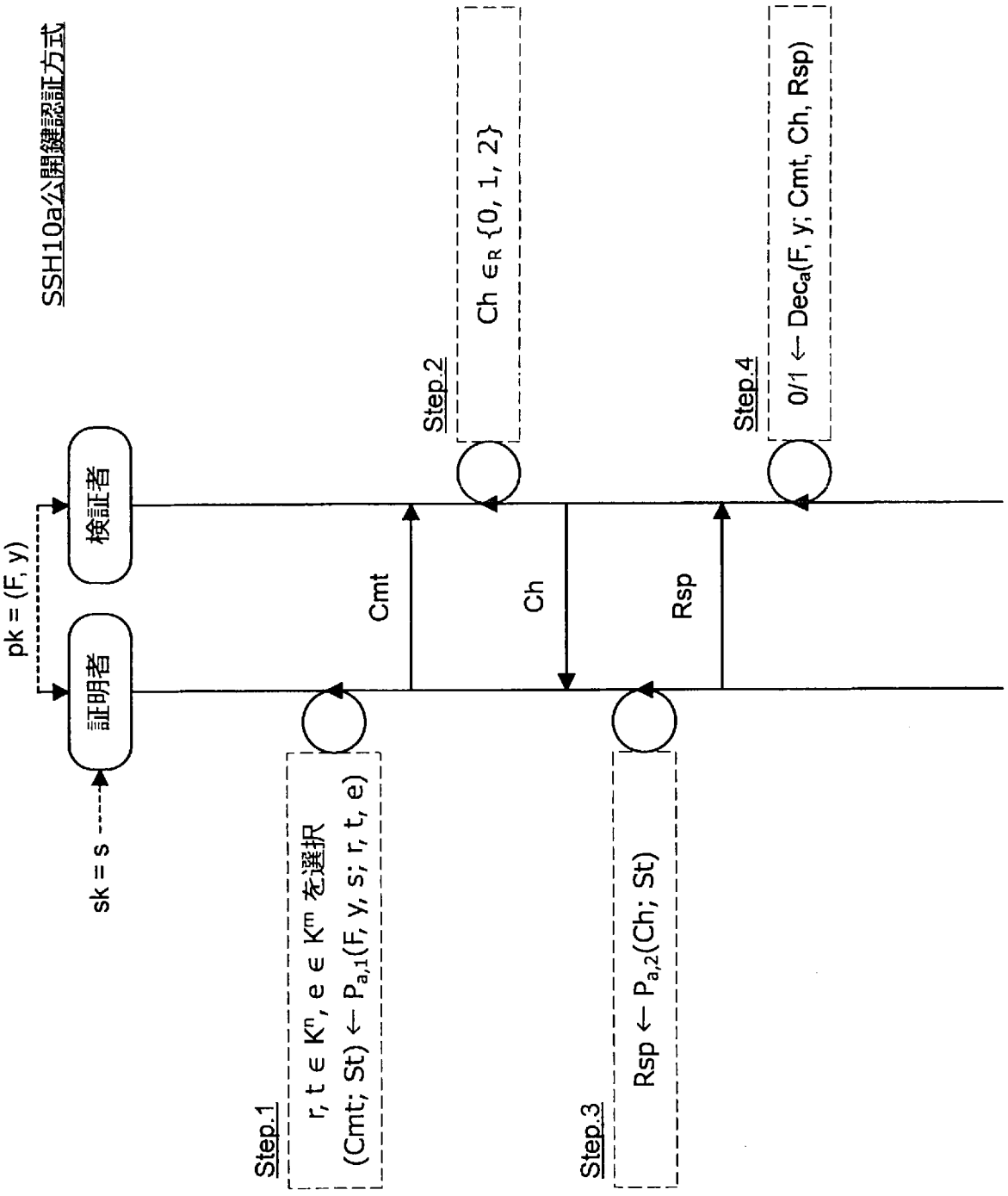
[図1]


公開鍵認証方式
証明者
Gen
鍵生成アルゴリズム
P
証明者アルゴリズム
検証者
V
検証者アルゴリズム

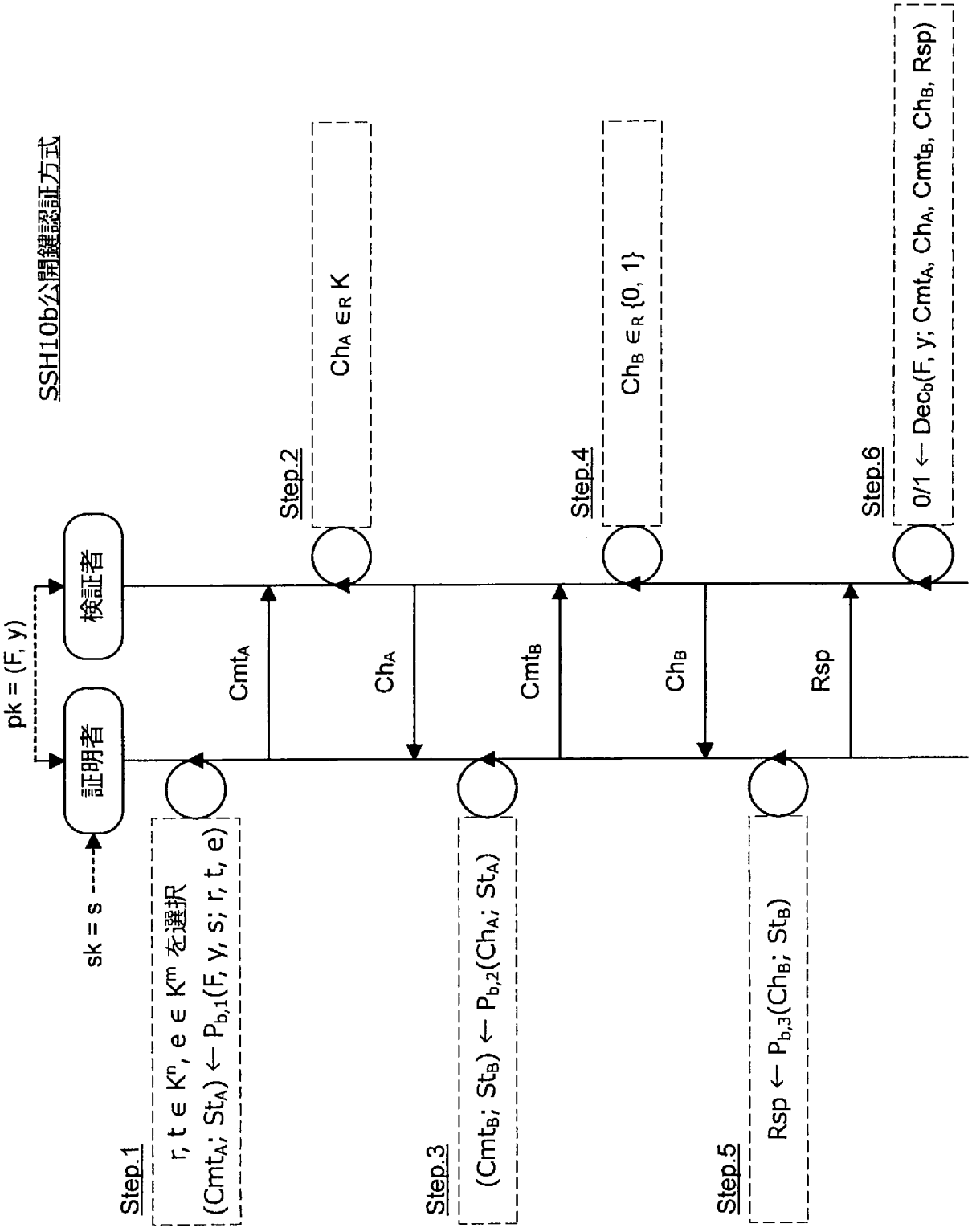
[図2]


nパスの公開鍵認証方式
pk
sk
証明者
検証者
処理(Step.1)
T1
T2
処理(Step.2)
Tn-2
Tn-1
処理(Step.n-1)
処理(Step.n)
Tn
処理(Step.n+1)

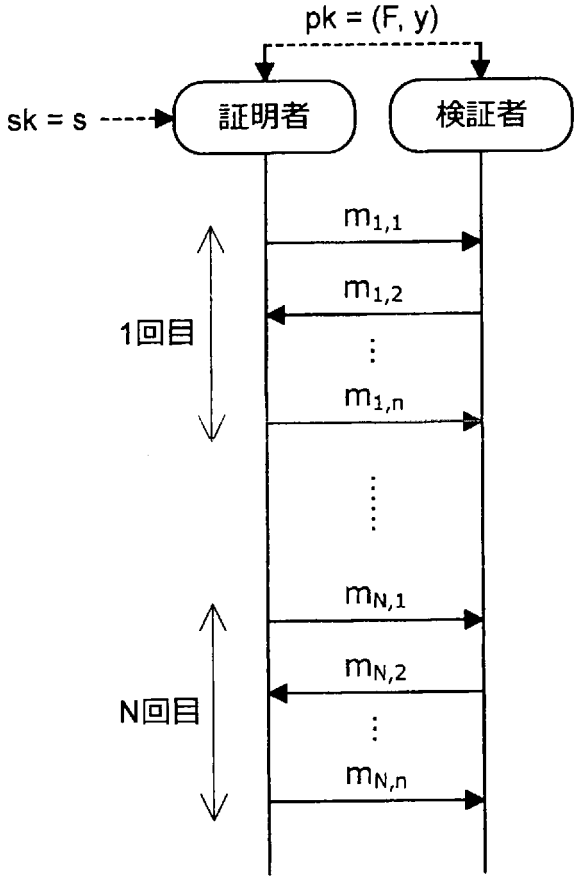
[図3]


SSH10a公開鍵認証方式
検証者
証明者
pk = (F, y)
sk = s
Step.1
r, t ∈ K^n, e ∈ K^m を選択
(Cmt; St) ← P_a,1(F, y, s; r, t, e)
Cmt
Step.2
Ch ∈_R {0, 1, 2}
Ch
Step.3
Rsp ← P_a,2(Ch; St)
Rsp
Step.4
0/1 ← Dec_a(F, y; Cmt, Ch, Rsp)

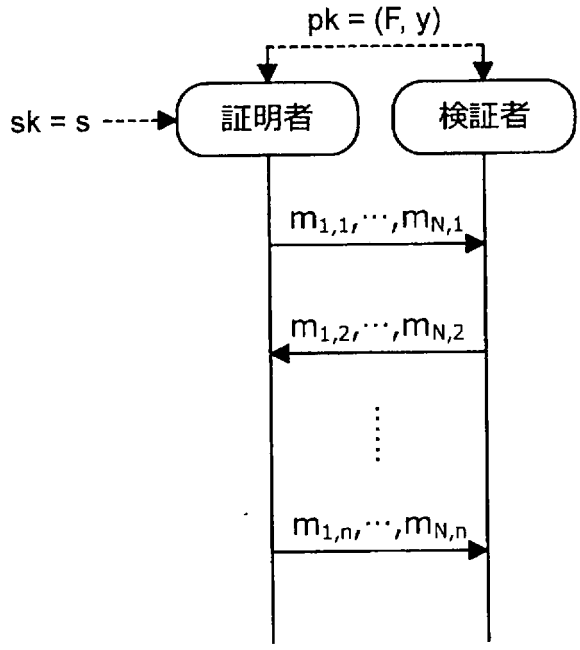
[図4]


SSH10b公開鍵認証方式
証明者
検証者
pk = (F, y)
sk = s
Step.1
r, t ∈ K^n, e ∈ K^m を選択
(Cmt_A; St_A) ← P_b,1(F, y, s; r, t, e)
Cmt_A
Step.2
Ch_A ∈_R K
Ch_A
Step.3
(Cmt_B; St_B) ← P_b,2(Ch_A; St_A)
Cmt_B
Step.4
Ch_B ∈_R {0, 1}
Ch_B
Step.5
Rsp ← P_b,3(Ch_B; St_B)
Rsp
Step.6
0/1 ← Dec_b(F, y; Cmt_A, Ch_A, Cmt_B, Ch_B, Rsp)

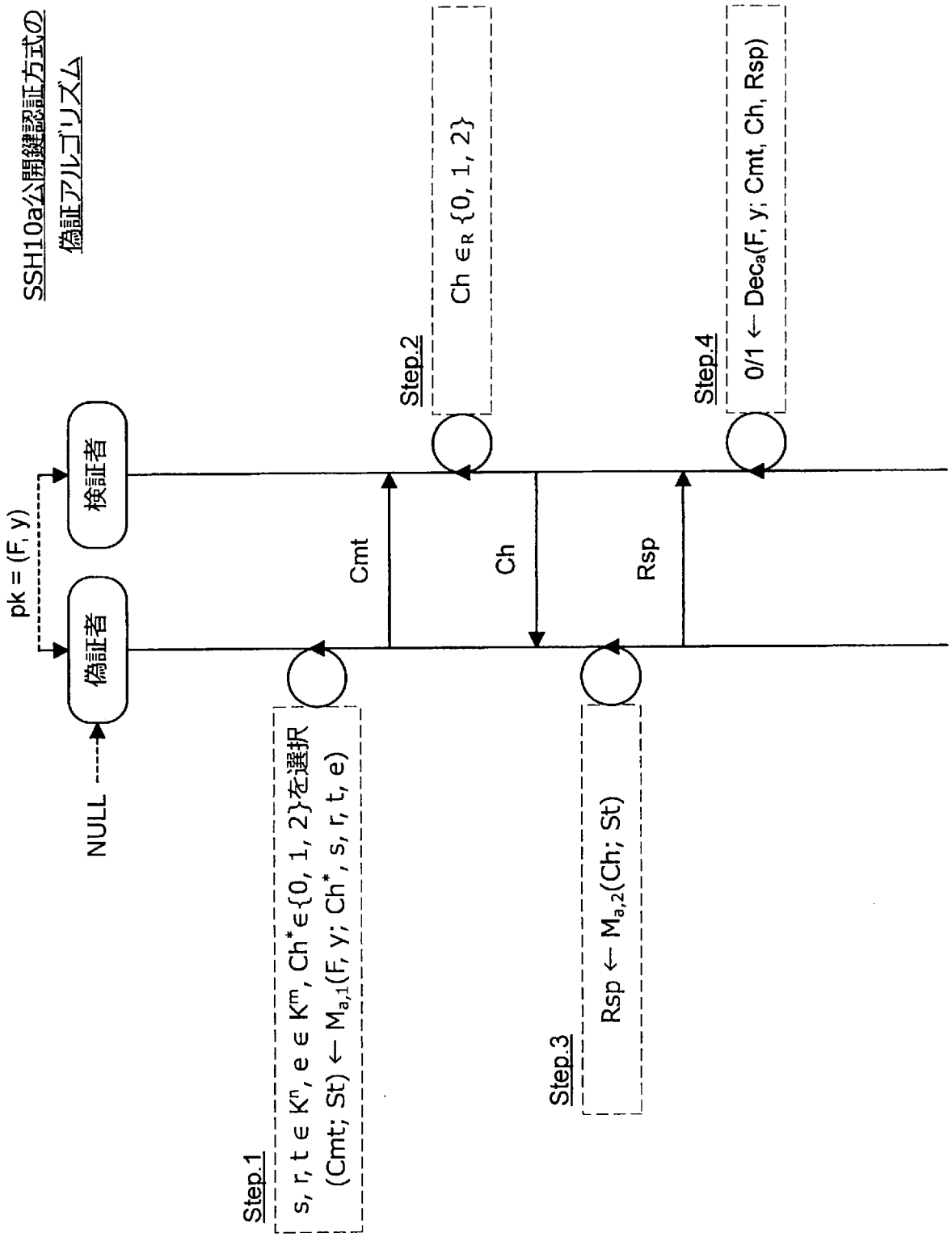
[図5]


pk = (F, y)
直列的繰り返し構成
sk = s
証明者
検証者
$m_{1,1}$
$m_{1,2}$
1回目
$m_{1,n}$
$m_{N,1}$
$m_{N,2}$
N回目
$m_{N,n}$

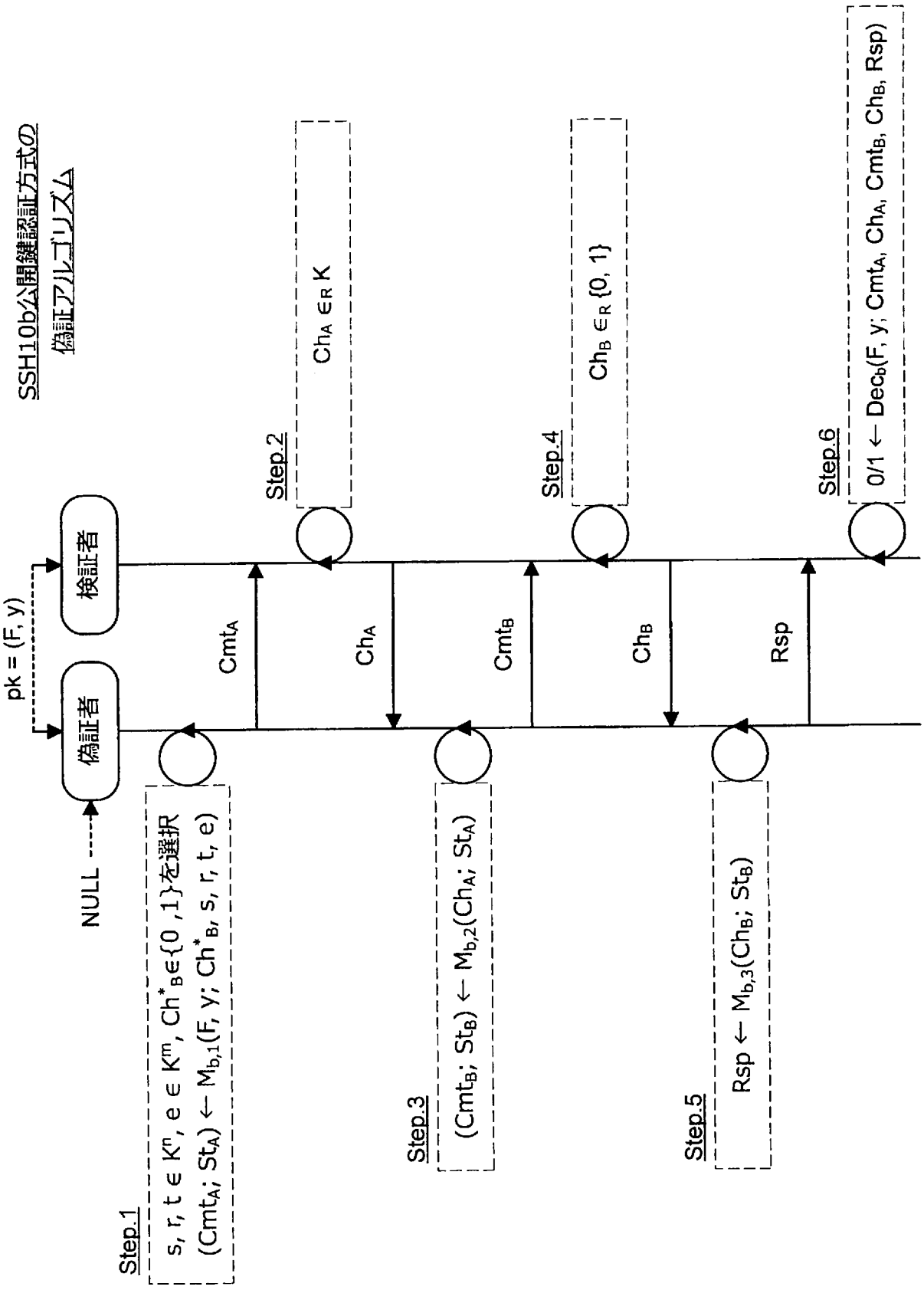
[図6]


pk = (F, y)
並列的繰り返し構成
sk = s
証明者
検証者
$m_{1,1},\cdots,m_{N,1}$
$m_{1,2},\cdots,m_{N,2}$
$m_{1,n},\cdots,m_{N,n}$

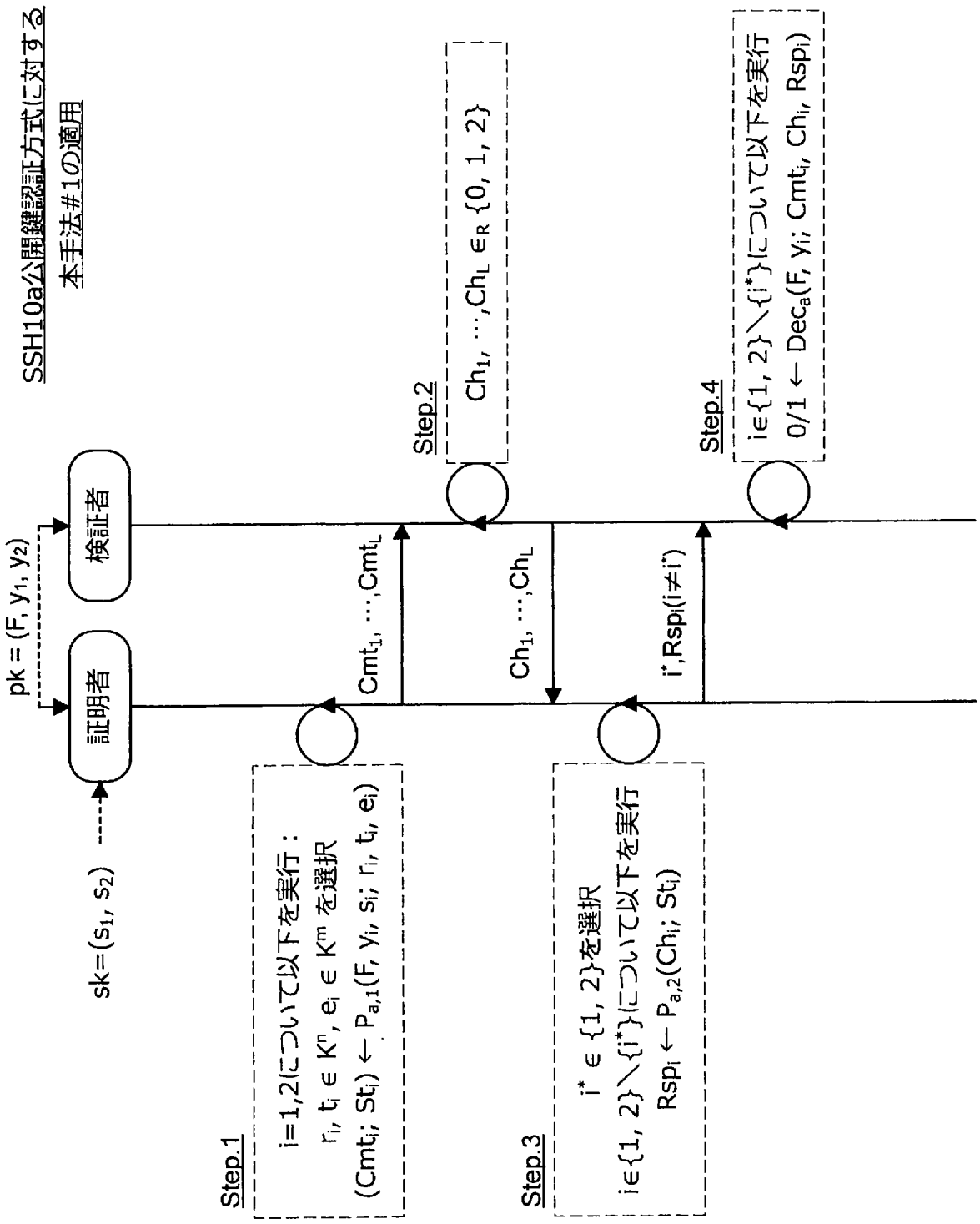
[図7]


SSH10a公開鍵認証方式の
偽証アルゴリズム
検証者
偽証者
pk = (F, y)
NULL
Step.1
s, r, t ∈ K^n, e ∈ K^m, Ch*∈{0, 1, 2}を選択
(Cmt; St) ← M_a,1(F, y; Ch*, s, r, t, e)
Cmt
Step.2
Ch ∈_R {0, 1, 2}
Ch
Step.3
Rsp ← M_a,2(Ch; St)
Rsp
Step.4
0/1 ← Dec_a(F, y; Cmt, Ch, Rsp)

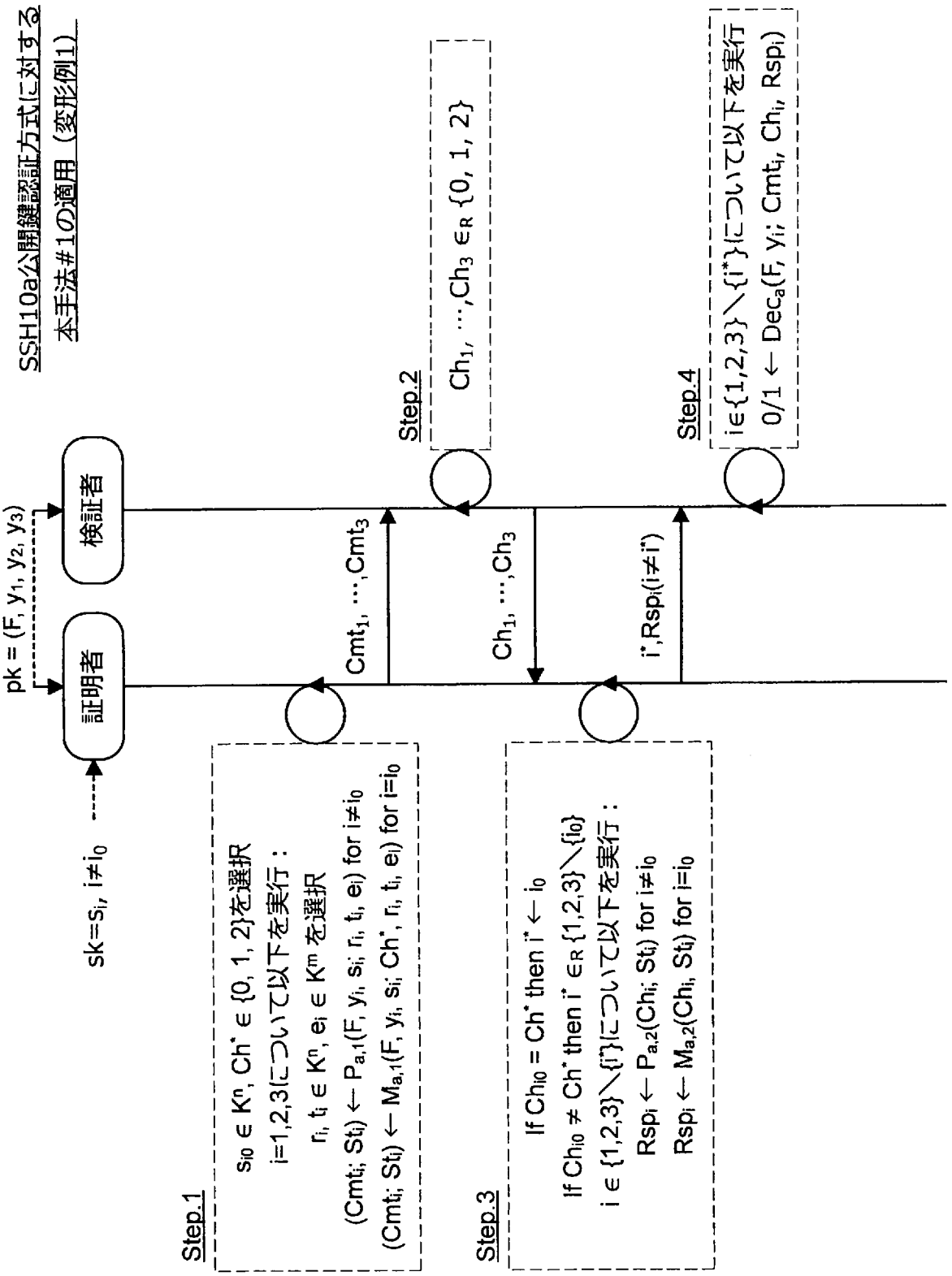
[図8]


SSH10b公開鍵認証方式の
偽証アルゴリズム
検証者
偽証者
pk = (F, y)
NULL
Step.1
s, r, t ∈ K^n, e ∈ K^m, Ch*_B∈{0 ,1}を選択
(Cmt_A; St_A) ← M_b,1(F, y; Ch*_B, s, r, t, e)
Cmt_A
Step.2
Ch_A ∈_R K
Ch_A
Step.3
(Cmt_B; St_B) ← M_b,2(Ch_A; St_A)
Cmt_B
Step.4
Ch_B ∈_R {0, 1}
Ch_B
Step.5
Rsp ← M_b,3(Ch_B; St_B)
Rsp
Step.6
0/1 ← Dec_b(F, y; Cmt_A, Ch_A, Cmt_B, Ch_B, Rsp)

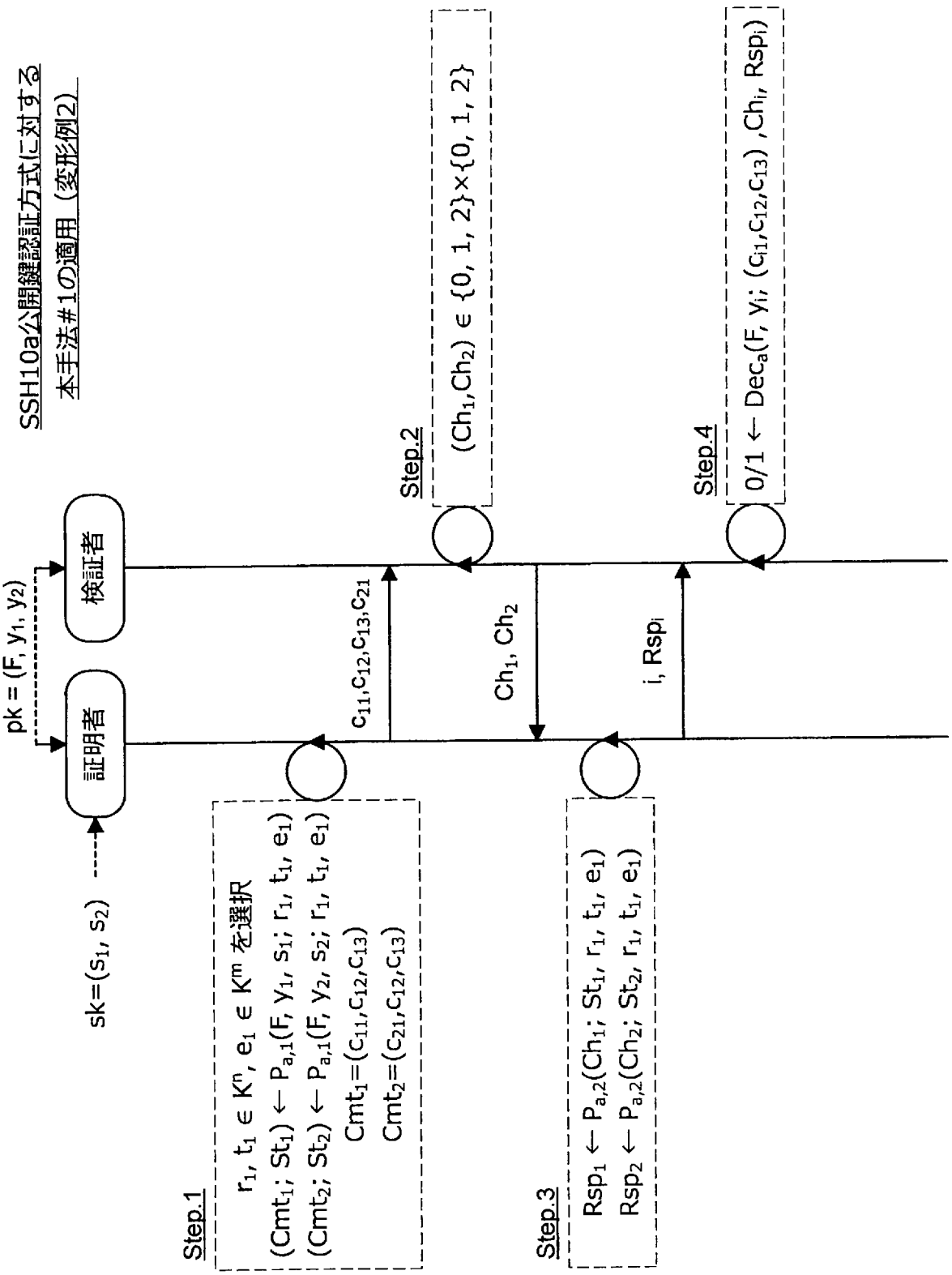
[図9]


SSH10a公開鍵認証方式に対する
本手法#1の適用
証明者
検証者
pk = (F, y1, y2)
sk=(s1, s2)
Step.1
i=1,2について以下を実行：
ri, ti ∈ Km, ei ∈ Km を選択
(Cmti; Sti) ← Pa,1(F, yi, si; ri, ti, ei)
Cmt1, …,CmtL
Step.2
Ch1, …,ChL ∈R {0, 1, 2}
Ch1, …,ChL
Step.3
i* ∈ {1, 2}を選択
i∈{1, 2}\{i*}について以下を実行
Rspi ← Pa,2(Chi; Sti)
i*,Rspi(i≠i*)
Step.4
i∈{1, 2}\{i*}について以下を実行
0/1 ← Deca(F, yi; Cmti, Chi, Rspi)

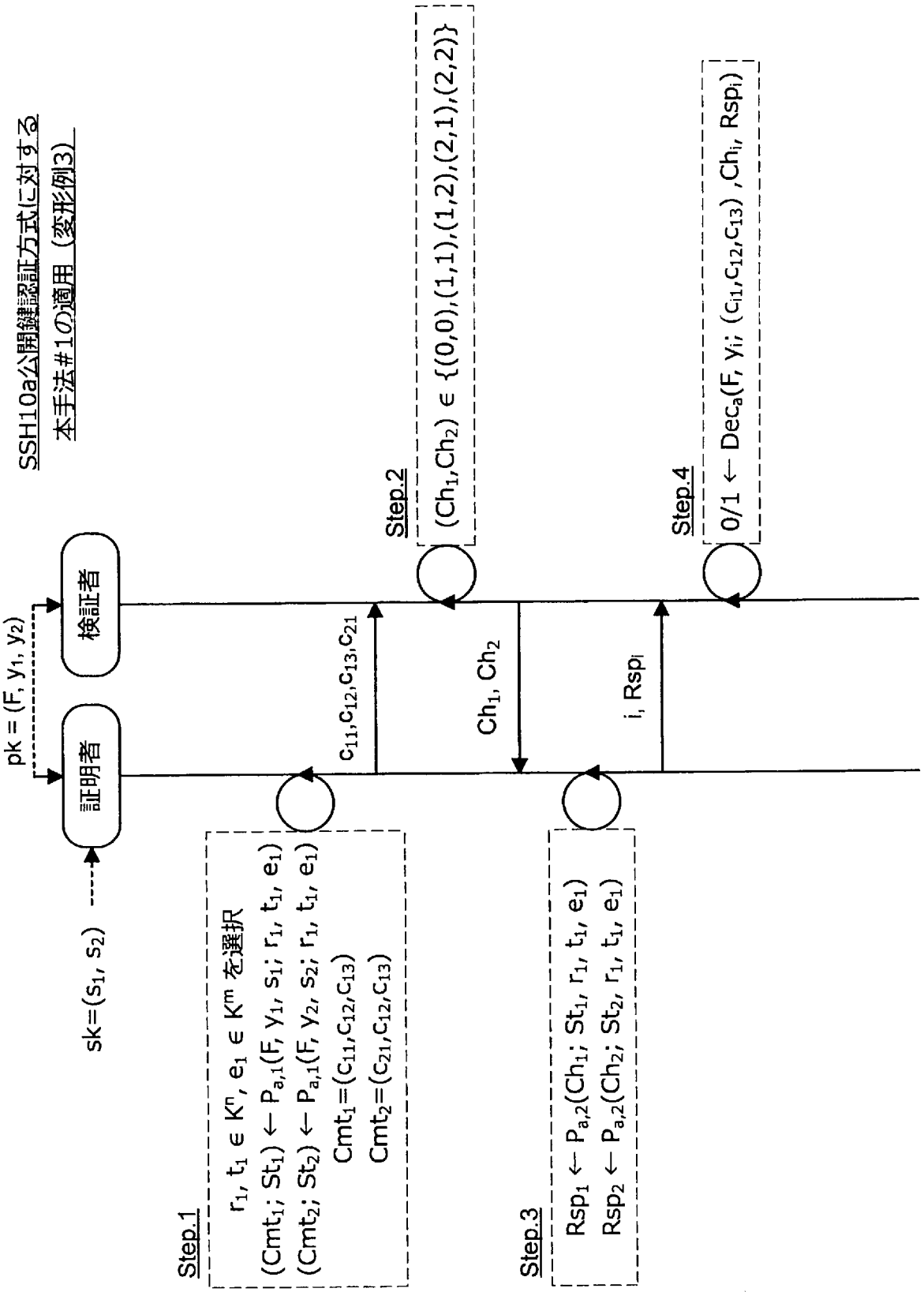
[図10]


SSH10a公開鍵認証方式に対する
本手法#1の適用（変形例1）
pk = (F, y1, y2, y3)
sk=si, i≠i0
証明者
検証者
Step.1
si0 ∈ K^n, Ch* ∈ {0, 1, 2}を選択
i=1,2,3について以下を実行：
ri, ti ∈ K^n, ei ∈ K^m を選択
(Cmti; Sti) ← Pa,1(F, yi, si; ri, ti, ei) for i≠i0
(Cmti; Sti) ← Ma,1(F, yi, si; Ch*, ri, ti, ei) for i=i0
Cmt1, ⋯,Cmt3
Step.2
Ch1, ⋯,Ch3 ∈R {0, 1, 2}
Ch1, ⋯,Ch3
Step.3
If Chi0 = Ch* then i* ← i0
If Chi0 ≠ Ch* then i* ∈R {1,2,3}＼{i0}
i ∈ {1,2,3}＼{i*}について以下を実行：
Rspi ← Pa,2(Chi; Sti) for i≠i0
Rspi ← Ma,2(Chi, Sti) for i=i0
i*,Rspi(i≠i*)
Step.4
i∈{1,2,3}＼{i*}について以下を実行
0/1 ← Deca(F, yi; Cmti, Chi, Rspi)

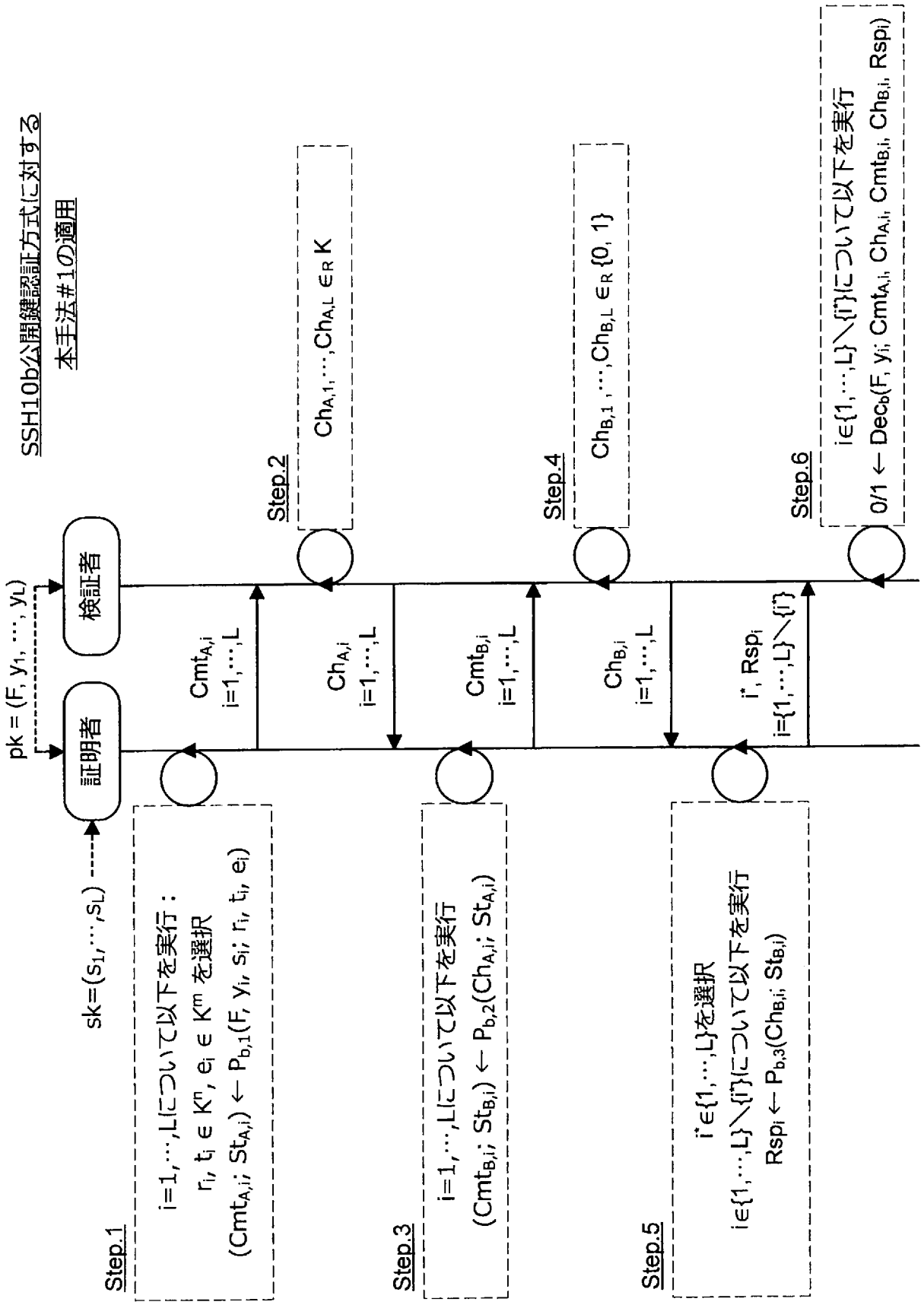
[図11]


SSH10a公開鍵認証方式に対する
本手法#1の適用（変形例2）
検証者
証明者
pk = (F, y1, y2)
sk=(s1, s2)
Step.1
r1, t1 ∈ Kn, e1 ∈ Km を選択
(Cmt1; St1) ← Pa,1(F, y1, s1; r1, t1, e1)
(Cmt2; St2) ← Pa,1(F, y2, s2; r1, t1, e1)
Cmt1=(c11,c12,c13)
Cmt2=(c21,c12,c13)
c11,c12,c13,c21
Step.2
(Ch1,Ch2) ∈ {0, 1, 2}×{0, 1, 2}
Ch1, Ch2
Step.3
Rsp1 ← Pa,2(Ch1; St1, r1, t1, e1)
Rsp2 ← Pa,2(Ch2; St2, r1, t1, e1)
i, Rspi
Step.4
0/1 ← Deca(F, yi; (ci1,ci2,ci3) ,Chi, Rspi)

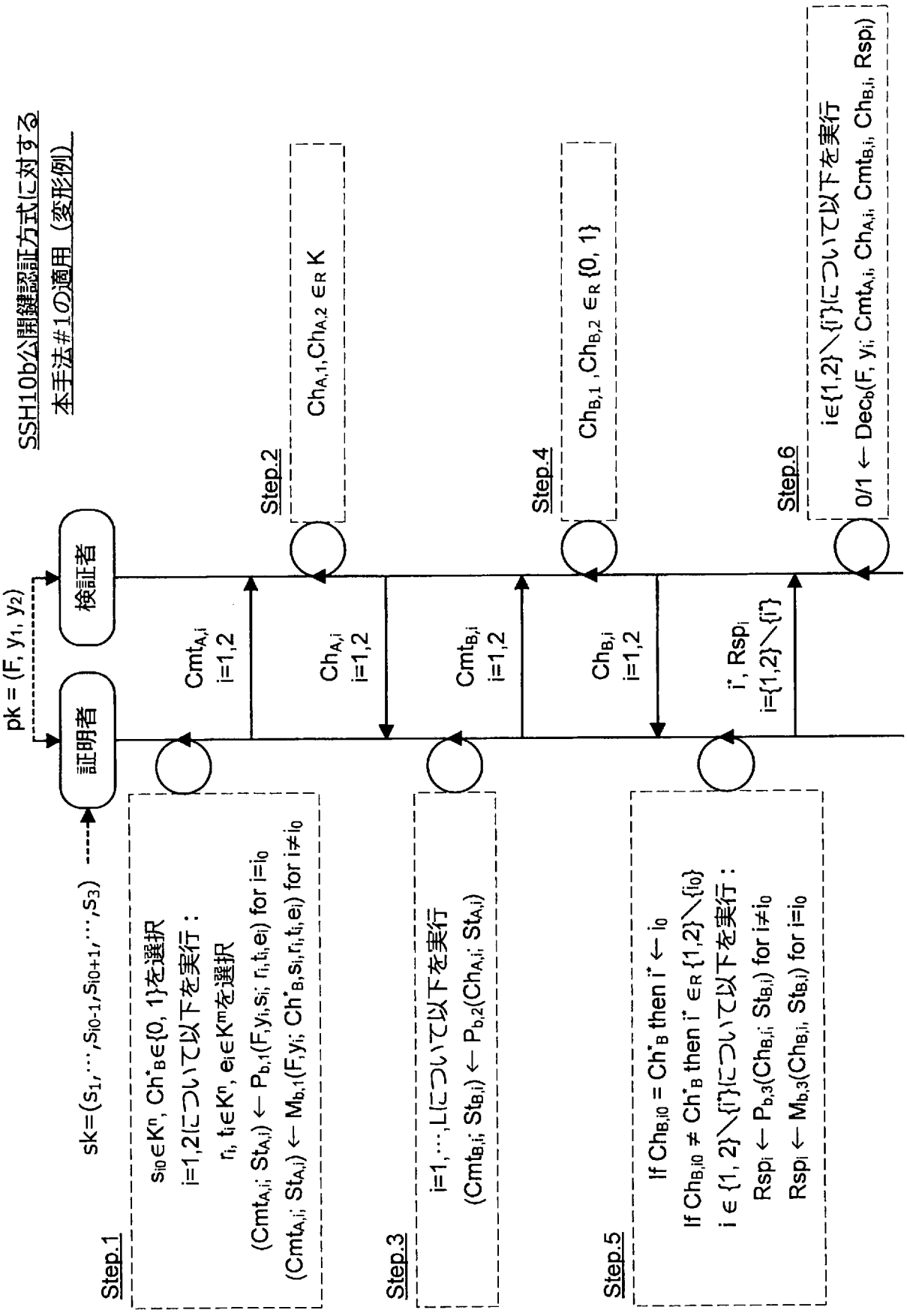
[図12]


SSH10a公開鍵認証方式に対する
本手法#1の適用（変形例3）
証明者
検証者
pk = (F, y1, y2)
sk=(s1, s2)
Step.1
r1, t1 ∈ Kn, e1 ∈ Km を選択
(Cmt1; St1) ← Pa,1(F, y1, s1; r1, t1, e1)
(Cmt2; St2) ← Pa,1(F, y2, s2; r1, t1, e1)
Cmt1=(c11,c12,c13)
Cmt2=(c21,c12,c13)
c11,c12,c13,c21
Step.2
(Ch1,Ch2) ∈ {(0,0),(1,1),(1,2),(2,1),(2,2)}
Ch1, Ch2
Step.3
Rsp1 ← Pa,2(Ch1; St1, r1, t1, e1)
Rsp2 ← Pa,2(Ch2; St2, r1, t1, e1)
i, Rspi
Step.4
0/1 ← Deca(F, yi; (ci1,c12,c13) ,Chi, Rspi)

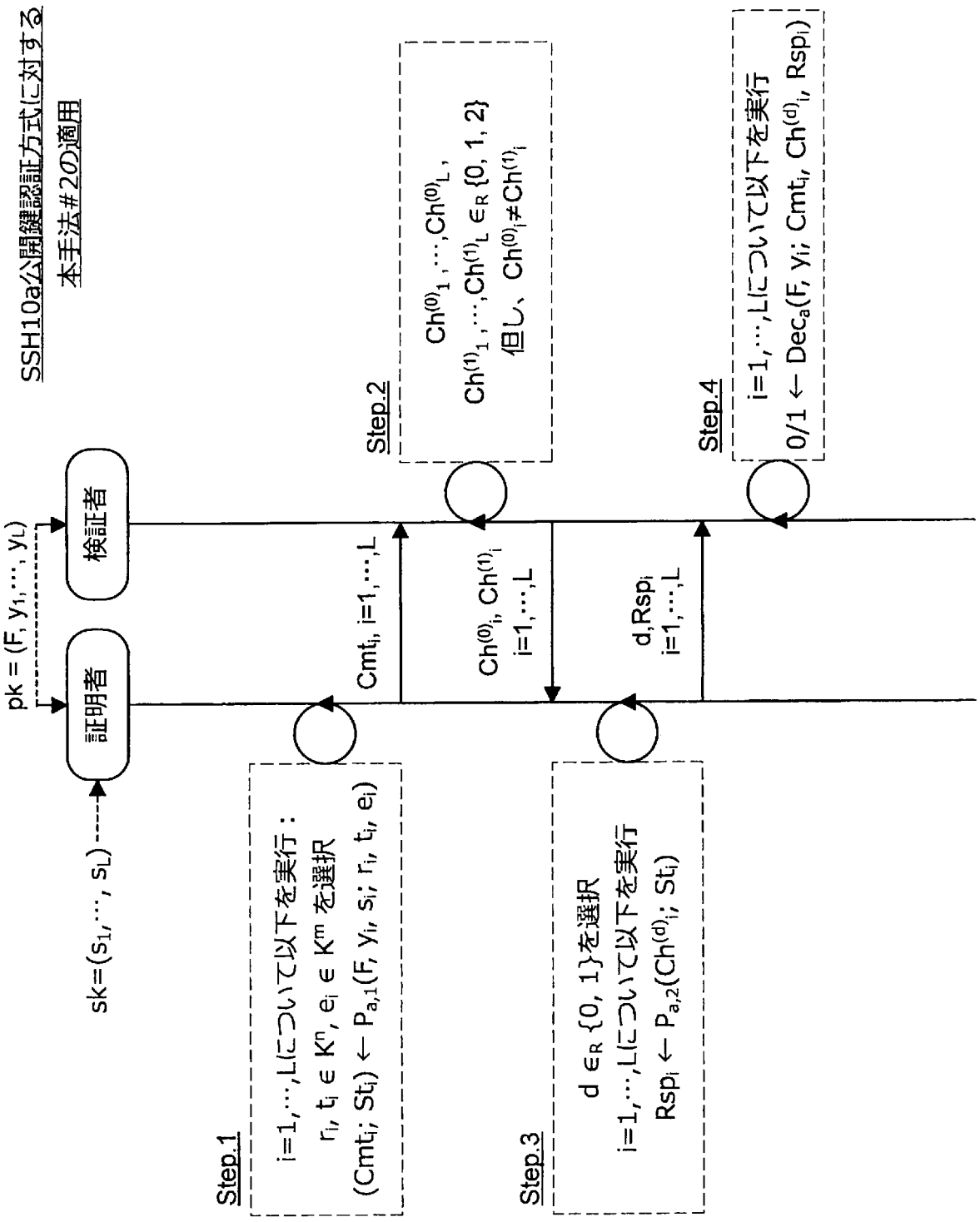
[図13]


SSH10b公開鍵認証方式に対する
本手法#1の適用
証明者
検証者
pk = (F, y1, ⋯, yL)
sk=(s1,⋯,sL)
Step.1
i=1,⋯,Lについて以下を実行：
ri, ti ∈ Kn, ei ∈ Km を選択
(Cmt_A,i; St_A,i) ← P_b,1(F, yi, si; ri, ti, ei)
Cmt_A,i
i=1,⋯,L
Step.2
Ch_A,1,⋯,Ch_A,L ∈R K
Ch_A,i
i=1,⋯,L
Step.3
i=1,⋯,Lについて以下を実行
(Cmt_B,i; St_B,i) ← P_b,2(Ch_A,i; St_A,i)
Cmt_B,i
i=1,⋯,L
Step.4
Ch_B,1,⋯,Ch_B,L ∈R {0, 1}
Ch_B,i
i=1,⋯,L
Step.5
i*∈{1,⋯,L}を選択
i∈{1,⋯,L}\{i*}について以下を実行
Rspi ← P_b,3(Ch_B,i; St_B,i)
i*, Rspi
i={1,⋯,L}\{i*}
Step.6
i∈{1,⋯,L}\{i*}について以下を実行
0/1 ← Dec_b(F, yi; Cmt_A,i, Ch_A,i, Cmt_B,i, Ch_B,i, Rspi)

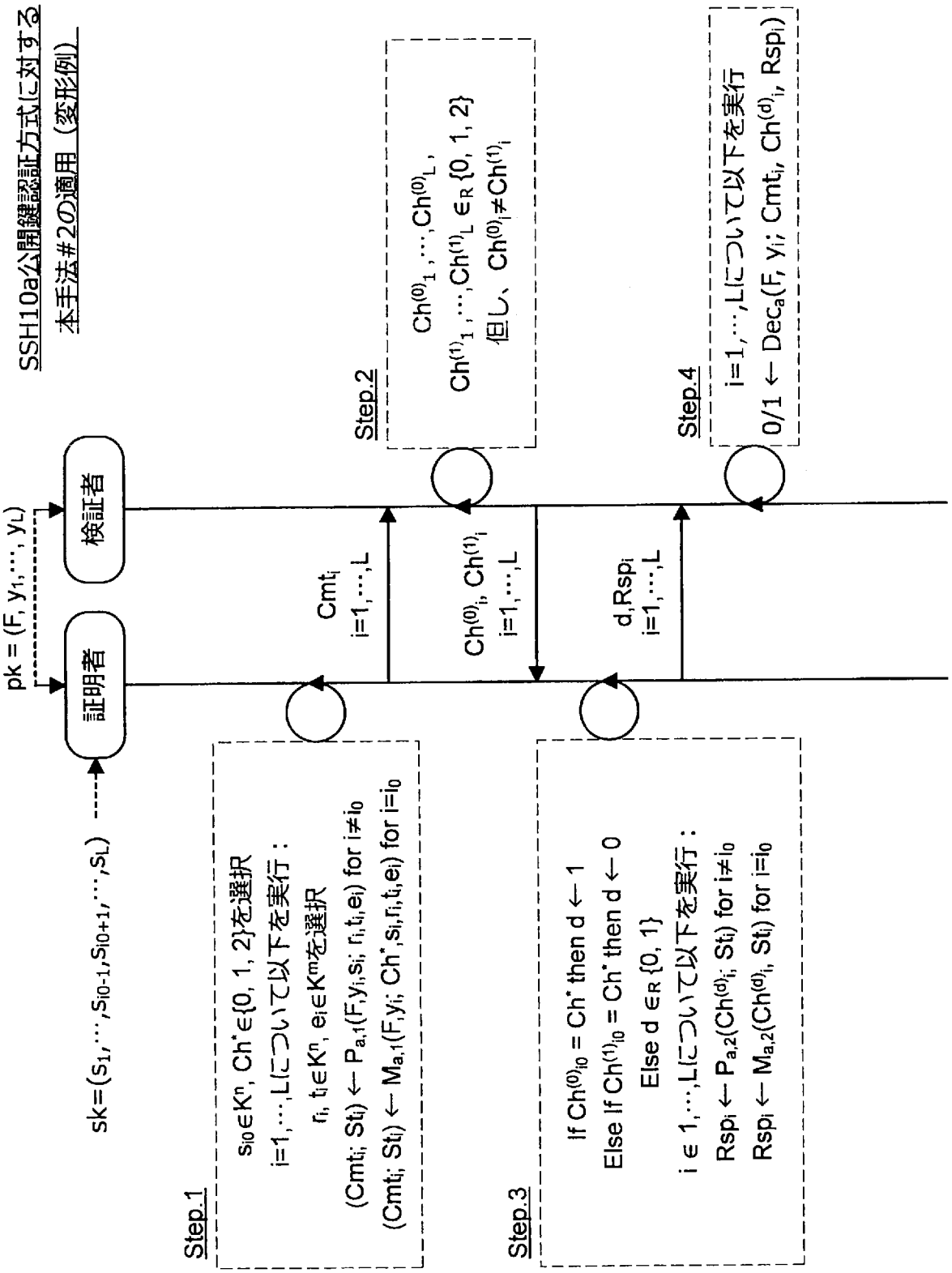
[図14]


SSH10b公開鍵認証方式に対する
本手法#1の適用（変形例）
証明者
検証者
pk = (F, y1, y2)
sk=(s1,…,si0-1,si0+1,…,s3)
Step.1
si0∈Kn, Ch*B∈{0, 1}を選択
i=1,2について以下を実行：
ri, ti∈Kn, ei∈Km を選択
(Cmt*A,i; St*A,i) ← Pb,1(F,yi,si; ri,ti,ei) for i=i0
(Cmt*A,i; St*A,i) ← Mb,1(F,yi; Ch*B,si,ri,ti,ei) for i≠i0
Cmt*A,i
i=1,2
Step.2
Ch*A,1,Ch*A,2 ∈R K
Ch*A,i
i=1,2
Step.3
i=1,…,Lについて以下を実行
(Cmt*B,i; St*B,i) ← Pb,2(Ch*A,i; St*A,i)
Cmt*B,i
i=1,2
Step.4
Ch*B,1 ,Ch*B,2 ∈R {0, 1}
Ch*B,i
i=1,2
Step.5
If Ch*B,i0 = Ch*B then i* ← i0
If Ch*B,i0 ≠ Ch*B then i* ∈R {1,2}＼{i0}
i ∈ {1, 2}＼{i*}について以下を実行：
Rspi ← Pb,3(Ch*B,i; St*B,i) for i≠i0
Rspi ← Mb,3(Ch*B,i; St*B,i) for i=i0
i*, Rspi
i={1,2}＼{i*}
Step.6
i∈{1,2}＼{i*}について以下を実行
0/1 ← Decb(F, yi; Cmt*A,i, Ch*A,i, Cmt*B,i, Ch*B,i, Rspi)

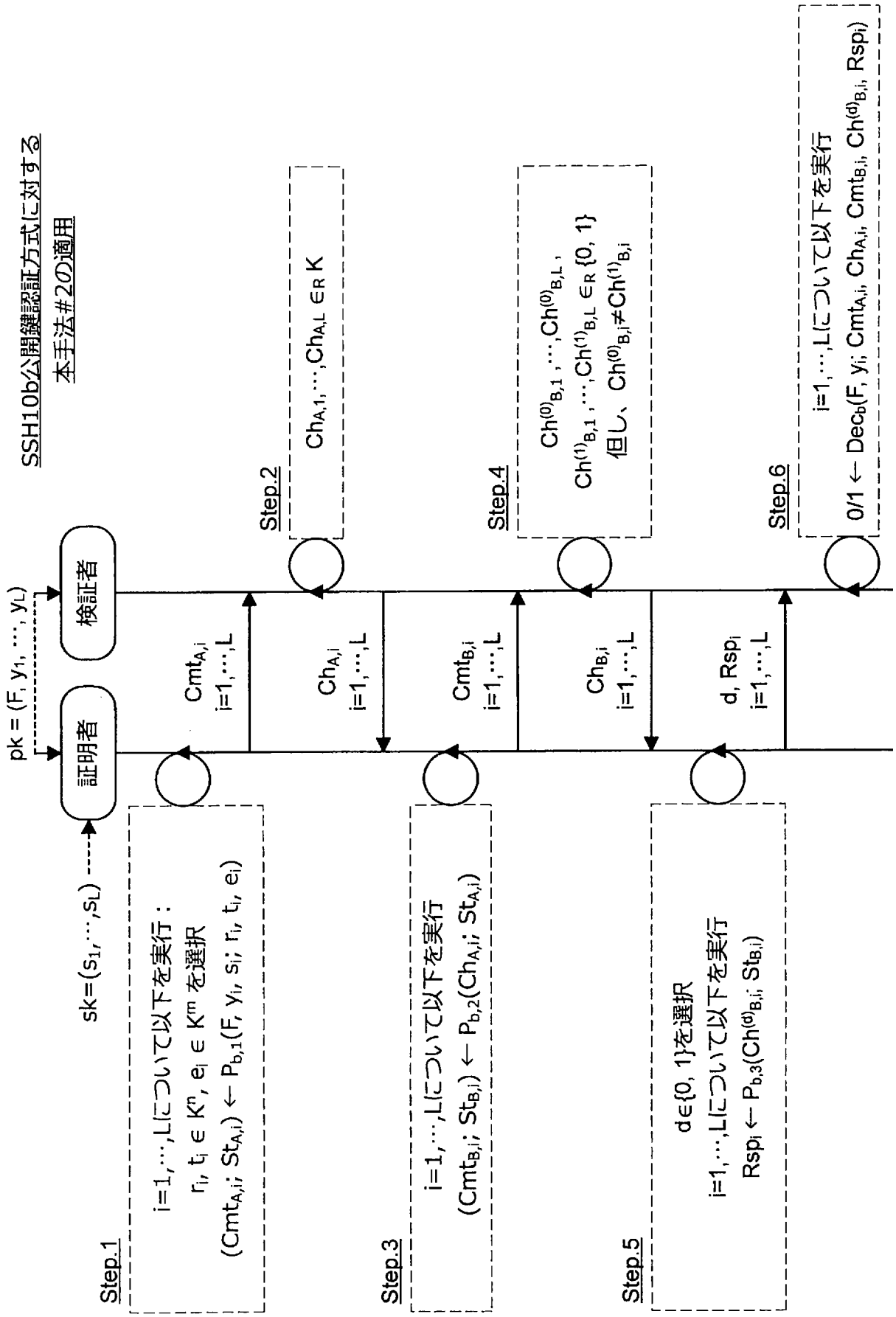
[図15]


SSH10a公開鍵認証方式に対する
本手法#2の適用
pk = (F, y1,…, yL)
sk=(s1,…, sL)
証明者
検証者
Step.1
i=1,…,Lについて以下を実行：
ri, ti ∈ Kn, ei ∈ Km を選択
(Cmti; Sti) ← Pa,1(F, yi, si; ri, ti, ei)
Cmti, i=1,…,L
Step.2
Ch(0)1,…,Ch(0)L,
Ch(1)1,…,Ch(1)L ∈R {0, 1, 2}
但し、Ch(0)i≠Ch(1)i
Ch(0)i, Ch(1)i
i=1,…,L
Step.3
d ∈R {0, 1}を選択
i=1,…,Lについて以下を実行
Rspi ← Pa,2(Ch(d)i; Sti)
d,Rspi
i=1,…,L
Step.4
i=1,…,Lについて以下を実行
0/1 ← Deca(F, yi; Cmti, Ch(d)i, Rspi)

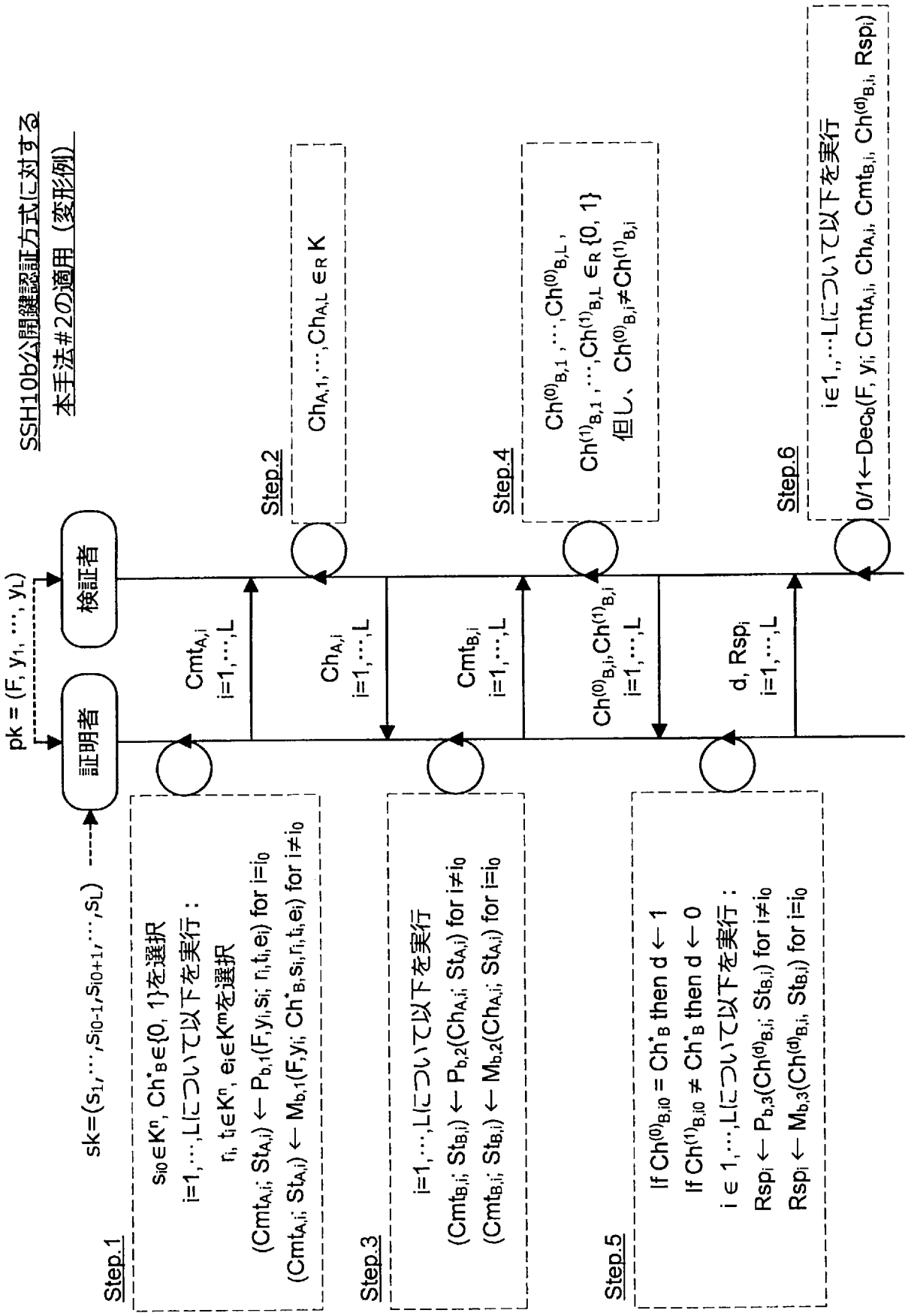
[図16]


SSH10a公開鍵認証方式に対する
本手法#2の適用（変形例）
証明者
検証者
pk = (F, y1,…, yL)
sk=(s1,…,si0-1,si0+1,…,sL)
Step.1
si0∈Kn, Ch*∈{0, 1, 2}を選択
i=1,…,Lについて以下を実行：
ri, ti∈Kn, ei∈Km を選択
(Cmti; Sti) ← Pa,1(F,yi,si; ri,ti,ei) for i≠i0
(Cmti; Sti) ← Ma,1(F,yi; Ch*,si,ri,ti,ei) for i=i0
Cmti
i=1,…,L
Step.2
Ch(0)1,…,Ch(0)L,
Ch(1)1,…,Ch(1)L ∈R {0, 1, 2}
但し、Ch(0)i≠Ch(1)i
Ch(0)i, Ch(1)i
i=1,…,L
Step.3
If Ch(0)i0 = Ch* then d ← 1
Else If Ch(1)i0 = Ch* then d ← 0
Else d ∈R {0, 1}
i ∈ 1,…,Lについて以下を実行：
Rspi ← Pa,2(Ch(d)i; Sti) for i≠i0
Rspi ← Ma,2(Ch(d)i, Sti) for i=i0
d,Rspi
i=1,…,L
Step.4
i=1,…,Lについて以下を実行
0/1 ← Deca(F, yi; Cmti, Ch(d)i, Rspi)

[図17]

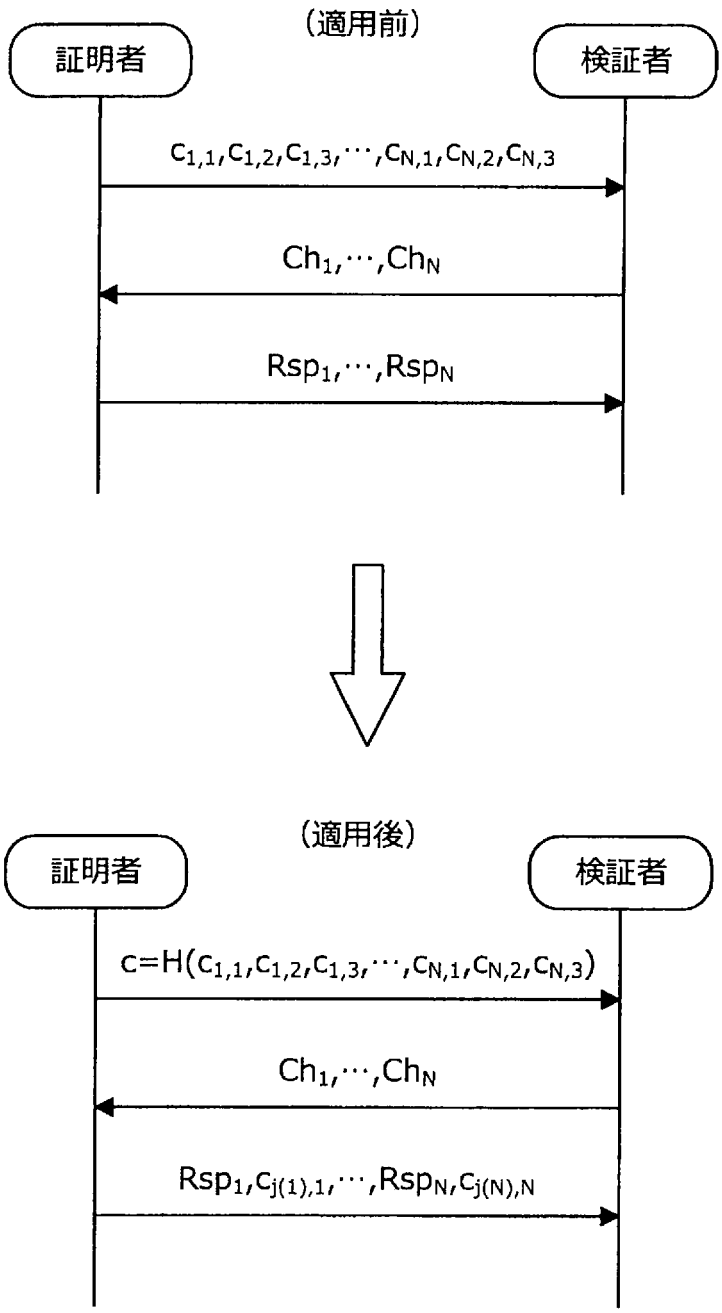

SSH10b公開鍵認証方式に対する
本手法#2の適用
pk = (F, y1, ⋯, yL)
sk=(s1,⋯,sL)
証明者
検証者
Step.1
i=1,⋯,Lについて以下を実行：
ri, ti ∈ Km, ei ∈ Km を選択
(CmtA,i; StA,i) ← Pb,1(F, yi, si; ri, ti, ei)
CmtA,i
i=1,⋯,L
Step.2
ChA,1,⋯,ChA,L ∈R K
ChA,i
i=1,⋯,L
Step.3
i=1,⋯,Lについて以下を実行
(CmtB,i; StB,i) ← Pb,2(ChA,i; StA,i)
CmtB,i
i=1,⋯,L
Step.4
Ch(0)B,1 ,⋯,Ch(0)B,L ,
Ch(1)B,1 ,⋯,Ch(1)B,L ∈R {0, 1}
但し、Ch(0)B,i≠Ch(1)B,i
ChB,i
i=1,⋯,L
Step.5
d∈{0, 1}を選択
i=1,⋯,Lについて以下を実行
Rspi ← Pb,3(Ch(d)B,i; StB,i)
d, Rspi
i=1,⋯,L
Step.6
i=1,⋯,Lについて以下を実行
0/1 ← Decb(F, yi; CmtA,i, ChA,i, CmtB,i, Ch(d)B,i, Rspi)

[図18]


SSH10b公開鍵認証方式に対する
本手法#2の適用（変形例）
pk = (F, y1, ⋯, yL)
sk=(s1,⋯,si0-1,si0+1,⋯,sL)
証明者
検証者
Step.1
si0∈Kn, Ch*B∈{0, 1}を選択
i=1,⋯,Lについて以下を実行：
ri, ti∈Kn, ei∈Kmを選択
(CmtA,i; StA,i) ← Pb,1(F,yi,si; ri,ti,ei) for i=i0
(CmtA,i; StA,i) ← Mb,1(F,yi; Ch*B,si,ri,ti,ei) for i≠i0
CmtA,i
i=1,⋯,L
Step.2
ChA,1,⋯,ChA,L ∈R K
ChA,i
i=1,⋯,L
Step.3
i=1,⋯,Lについて以下を実行
(CmtB,i; StB,i) ← Pb,2(ChA,i; StA,i) for i≠i0
(CmtB,i; StB,i) ← Mb,2(ChA,i; StA,i) for i=i0
CmtB,i
i=1,⋯,L
Step.4
Ch(0)B,1 ,⋯,Ch(0)B,L ,
Ch(1)B,1 ,⋯,Ch(1)B,L ∈R {0, 1}
但し、Ch(0)B,i≠Ch(1)B,i
Ch(0)B,i,Ch(1)B,i
i=1,⋯,L
Step.5
If Ch(0)B,i0 = Ch*B then d ← 1
If Ch(1)B,i0 ≠ Ch*B then d ← 0
i ∈ 1,⋯,Lについて以下を実行：
Rspi ← Pb,3(Ch(d)B,i; StB,i) for i≠i0
Rspi ← Mb,3(Ch(d)B,i; StB,i) for i=i0
d, Rspi
i=1,⋯,L
Step.6
i∈1,,⋯Lについて以下を実行
0/1←Decb(F, yi; Cmtb,i, Cha,i, Cmtb,i, Ch(d)b,i, Rspi)

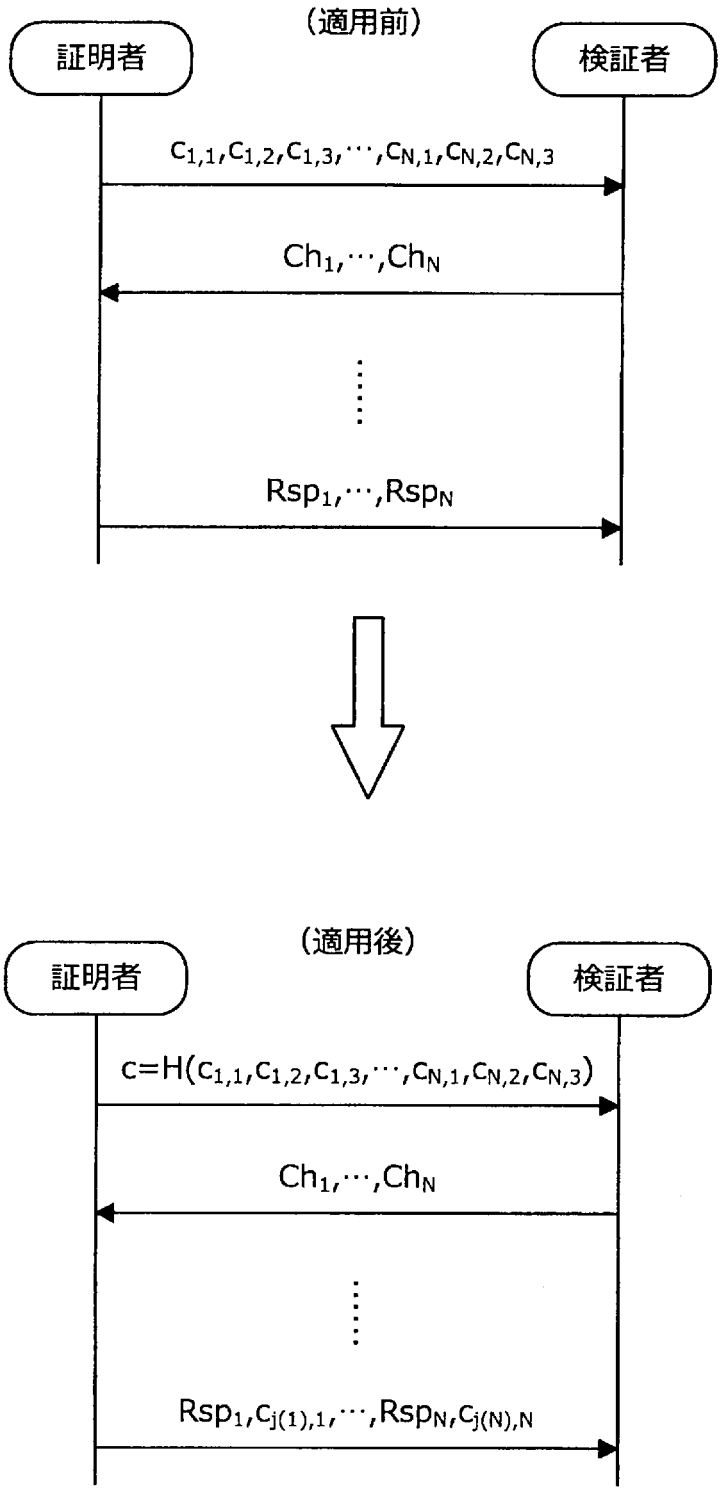
[図19]

通信量の削減方法（SSH10aの場合）

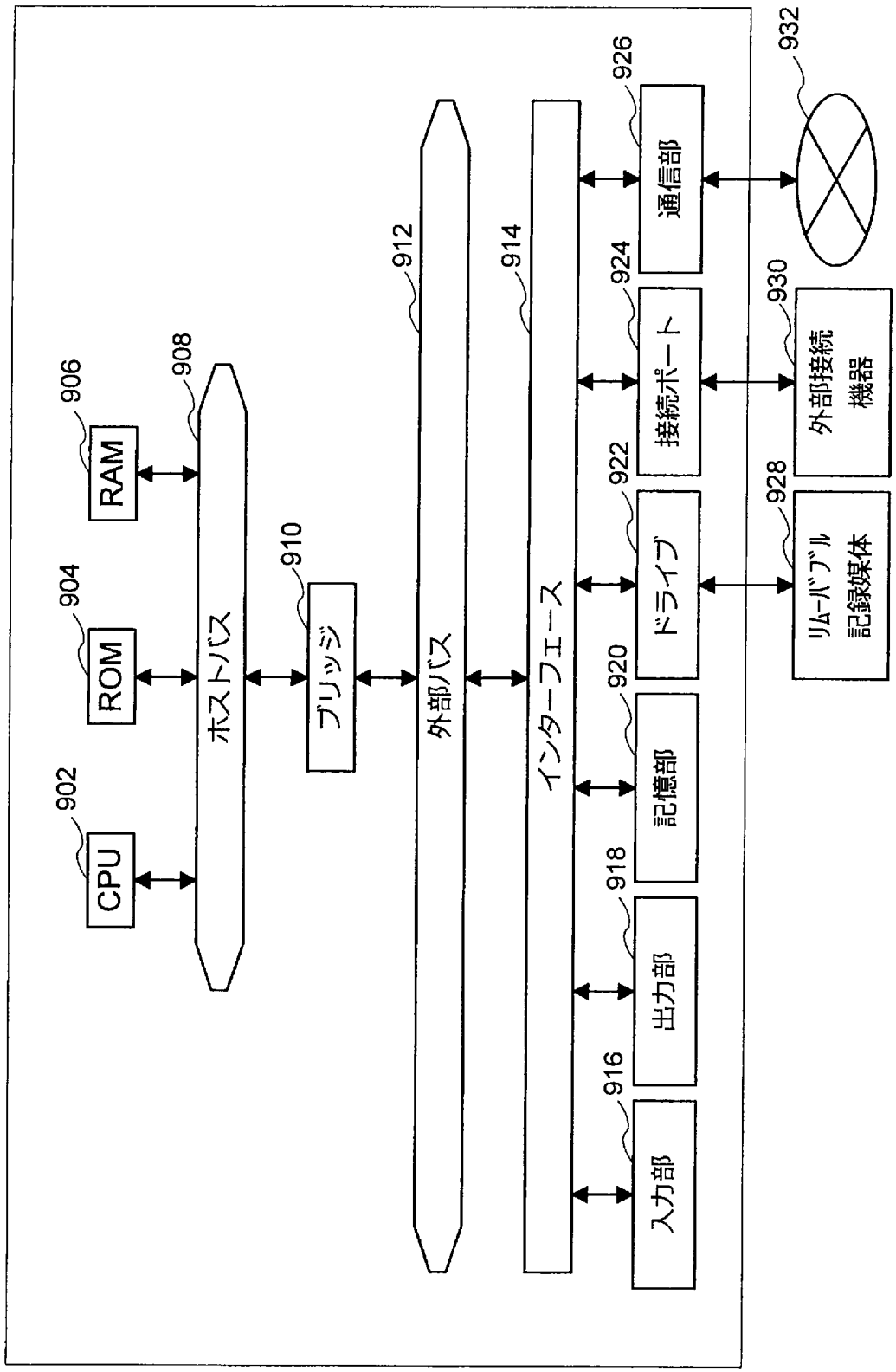


[図20]

通信量の削減方法（SSH10bの場合）



[図21]


902
CPU
904
ROM
906
RAM
908
ホストバス
910
ブリッジ
912
外部バス
914
インターフェース
916
入力部
918
出力部
920
記憶部
922
ドライブ
924
接続ポート
926
通信部
928
リムーバブル記録媒体
930
外部接続機器
932