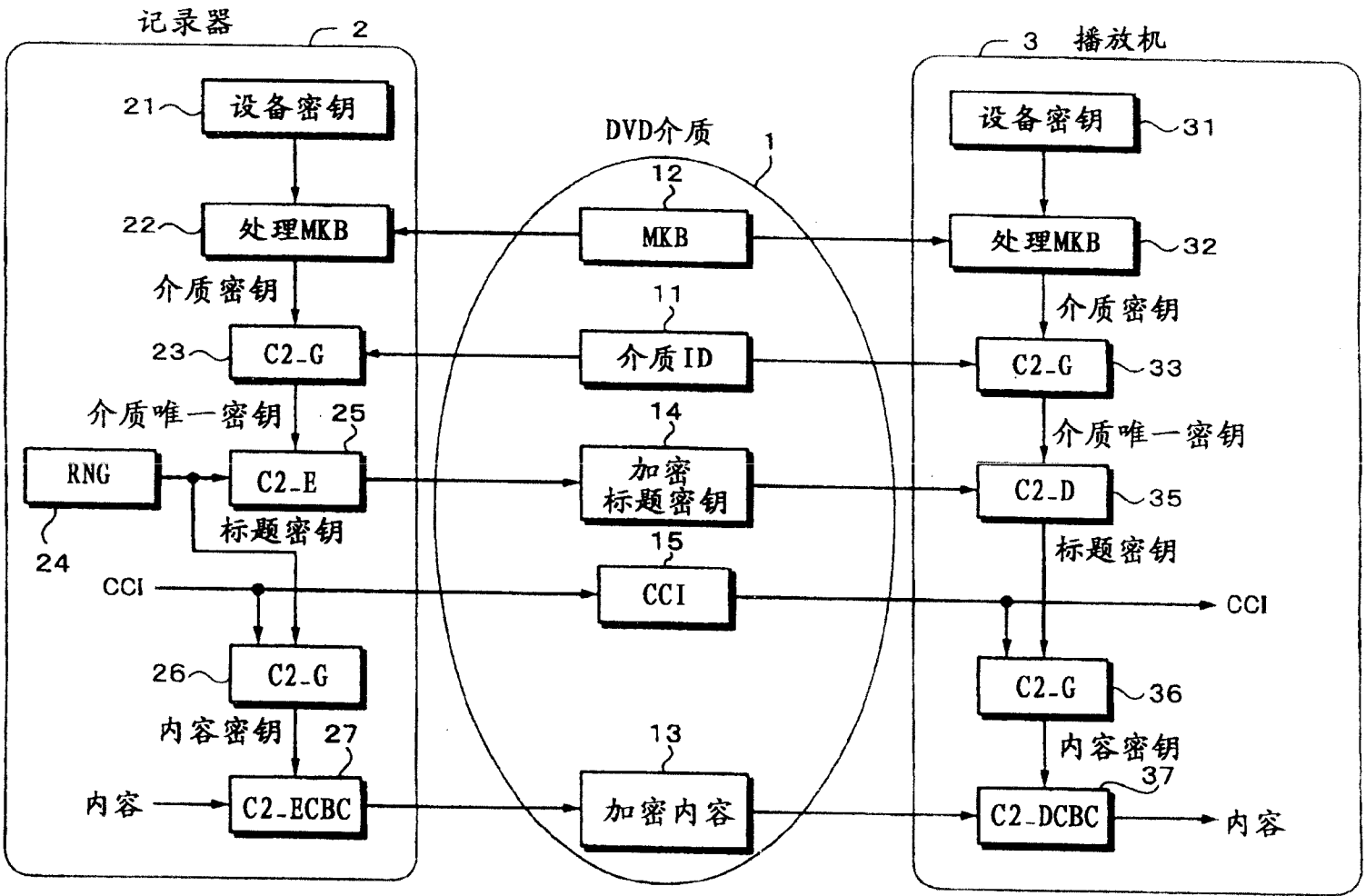
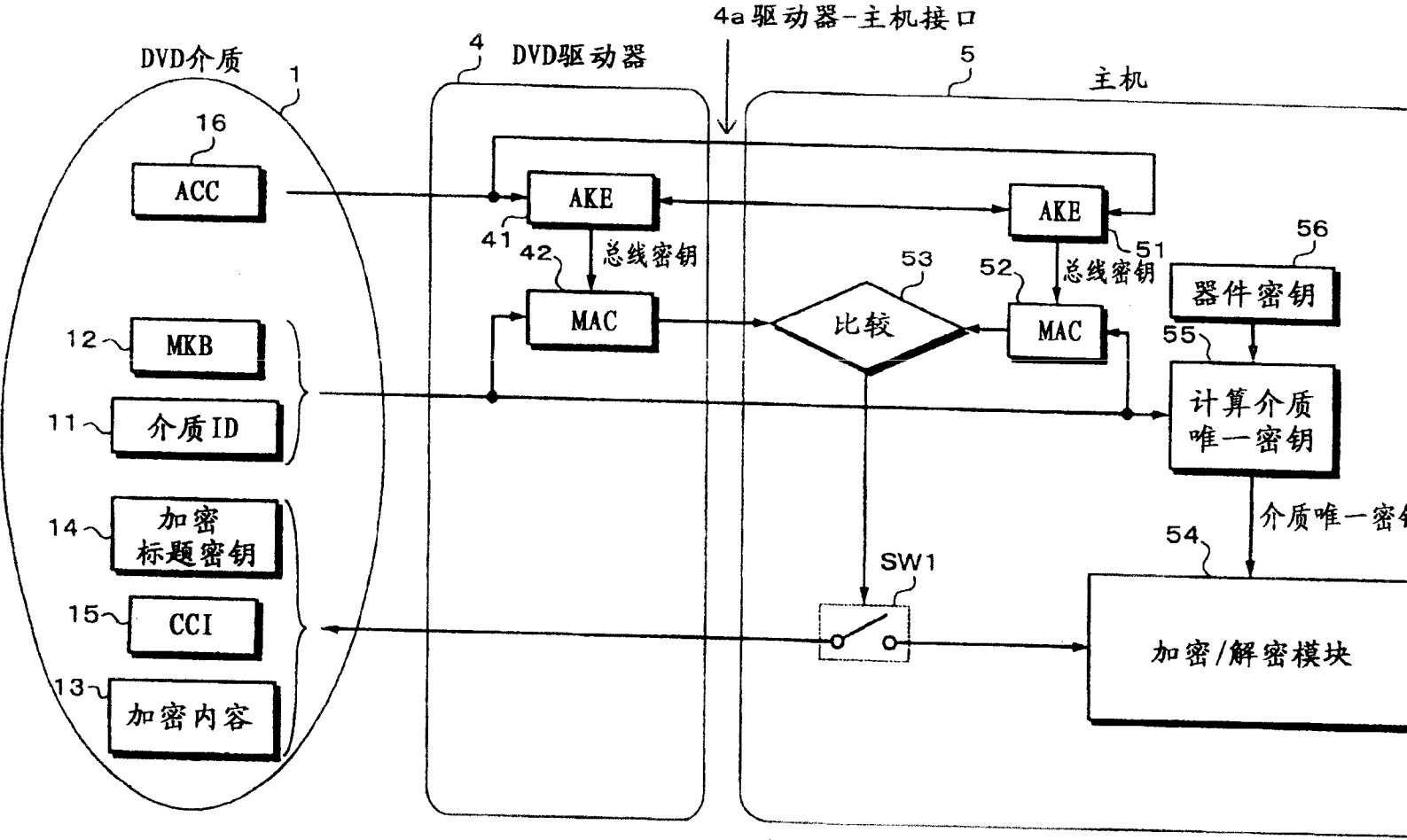
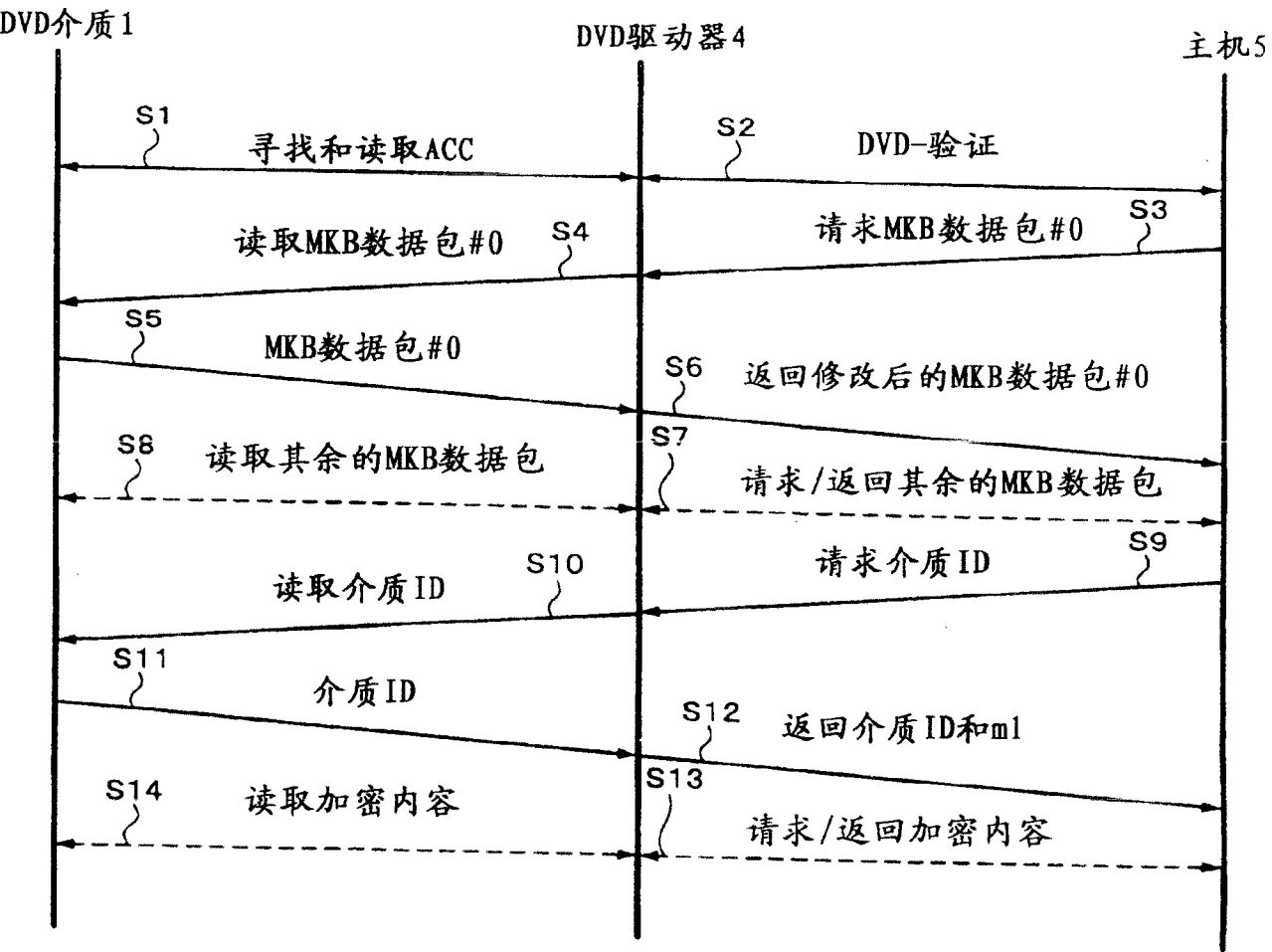
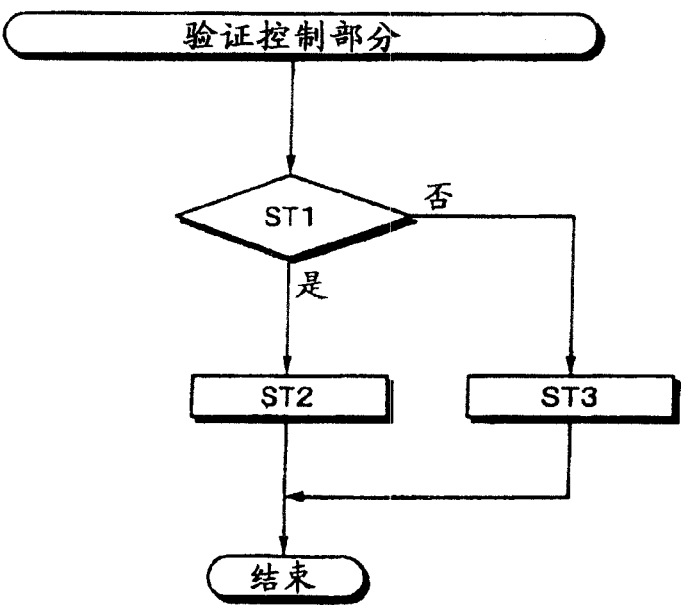
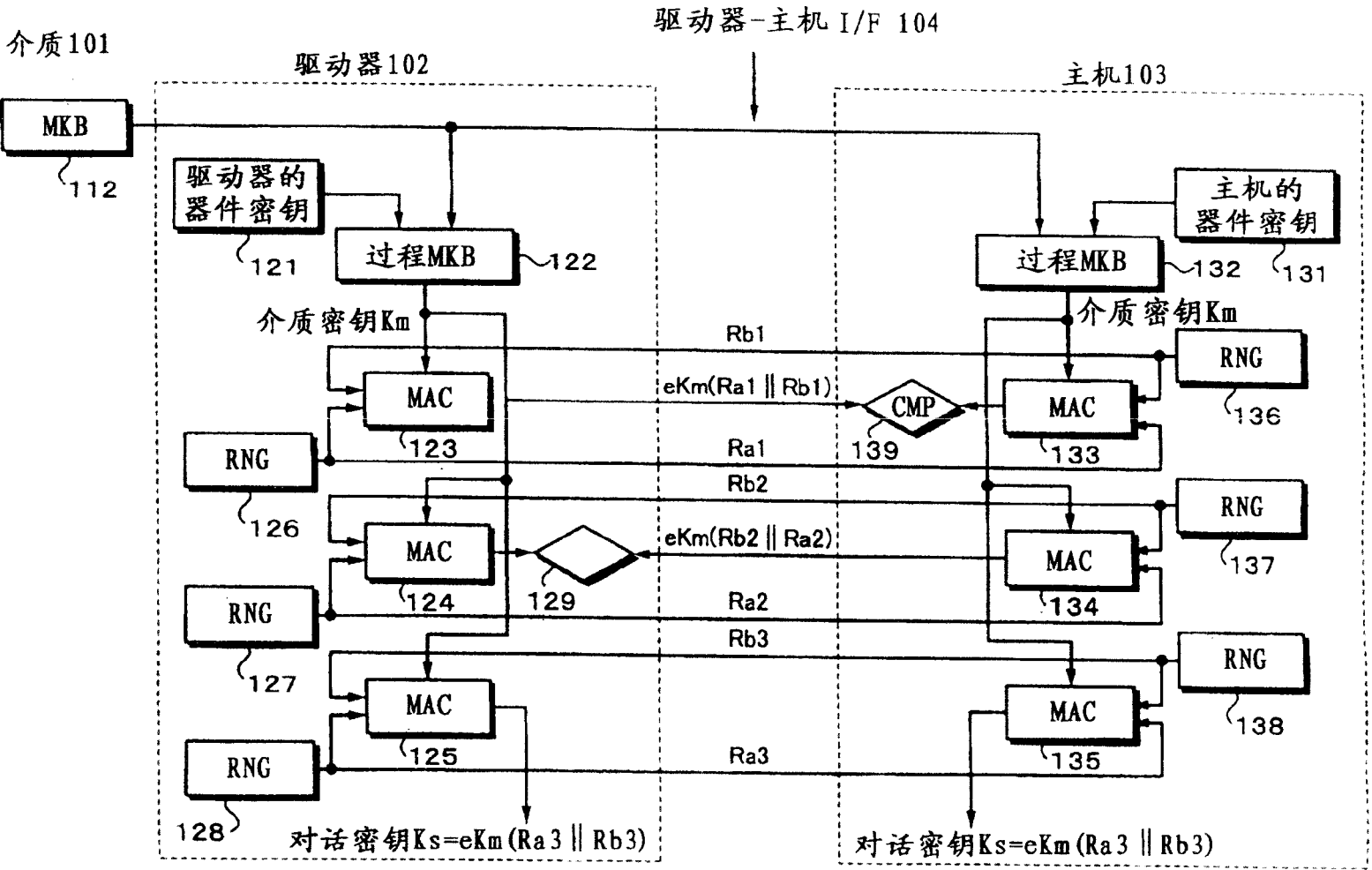

记录器
2
3 播放机
DVD介质
1
21
设备密钥
22
处理MKB
介质密钥
23
C2_G
介质唯一密钥
25
RNG
C2_E
24
标题密钥
CCI
26
C2_G
内容密钥
27
内容
C2_ECBC
12
MKB
11
介质ID
14
加密
标题密钥
15
CCI
13
加密内容
设备密钥
31
处理MKB
32
介质密钥
C2_G
33
介质唯一密钥
C2_D
35
标题密钥
CCI
C2_G
36
内容密钥
37
C2_DCBC
内容

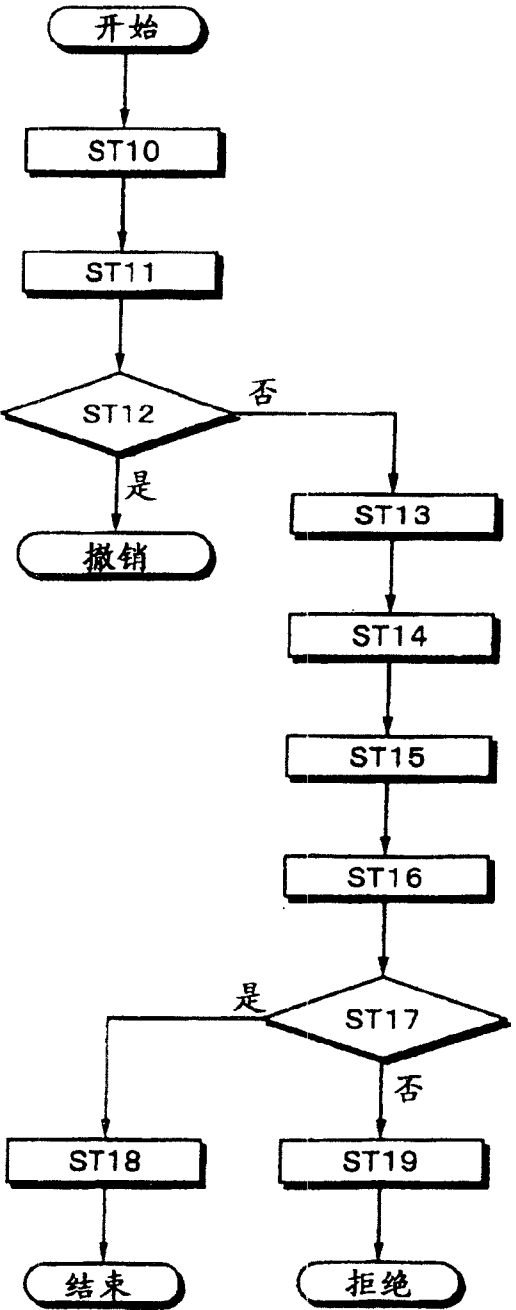

4a 驱动器-主机接口
DVD介质
1
4
DVD驱动器
5
主机
16
ACC
AKE
AKE
41
42
总线密钥
51
总线密钥
53
52
56
器件密钥
MAC
比较
MAC
55
12
MKB
计算介质
唯一密钥
11
介质ID
介质唯一密
14
加密
标题密钥
54
SW1
15
CCI
加密/解密模块
13
加密内容


DVD介质1
DVD驱动器4
主机5
S1
寻找和读取ACC
S2
DVD-验证
读取MKB数据包#0
S4
请求MKB数据包#0
S3
S5
MKB数据包#0
S6
返回修改后的MKB数据包#0
S8
读取其余的MKB数据包
S7
请求/返回其余的MKB数据包
读取介质ID
S10
请求介质ID
S9
S11
介质ID
S12
返回介质ID和m1
S14
读取加密内容
S13
请求/返回加密内容

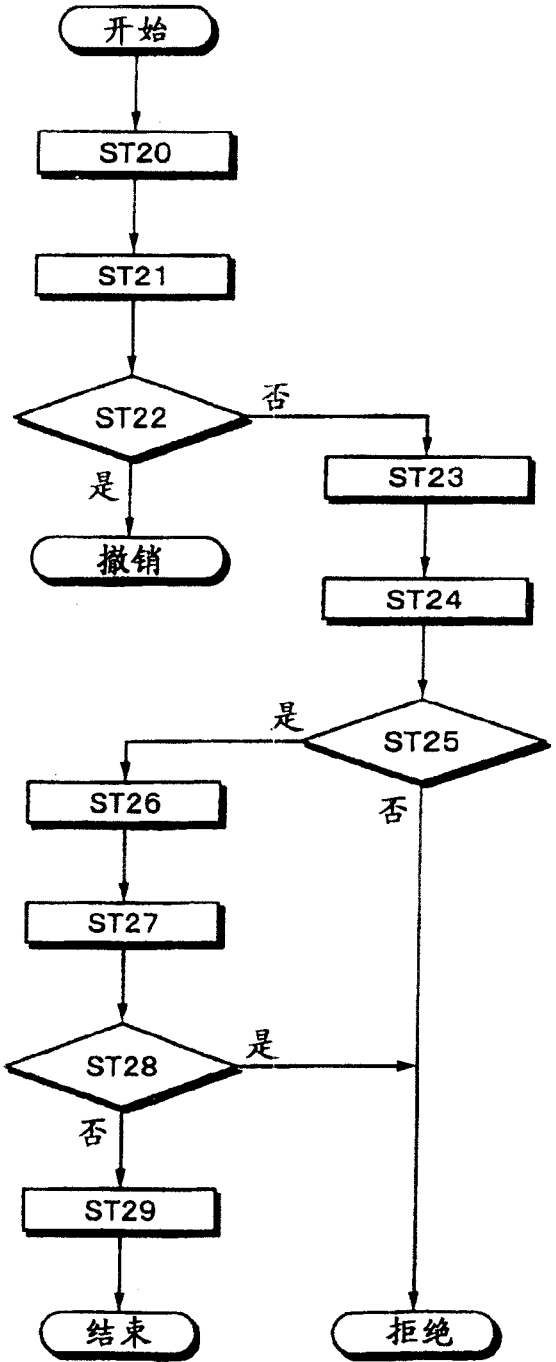

验证控制部分
ST1
否
是
ST2
ST3
结束

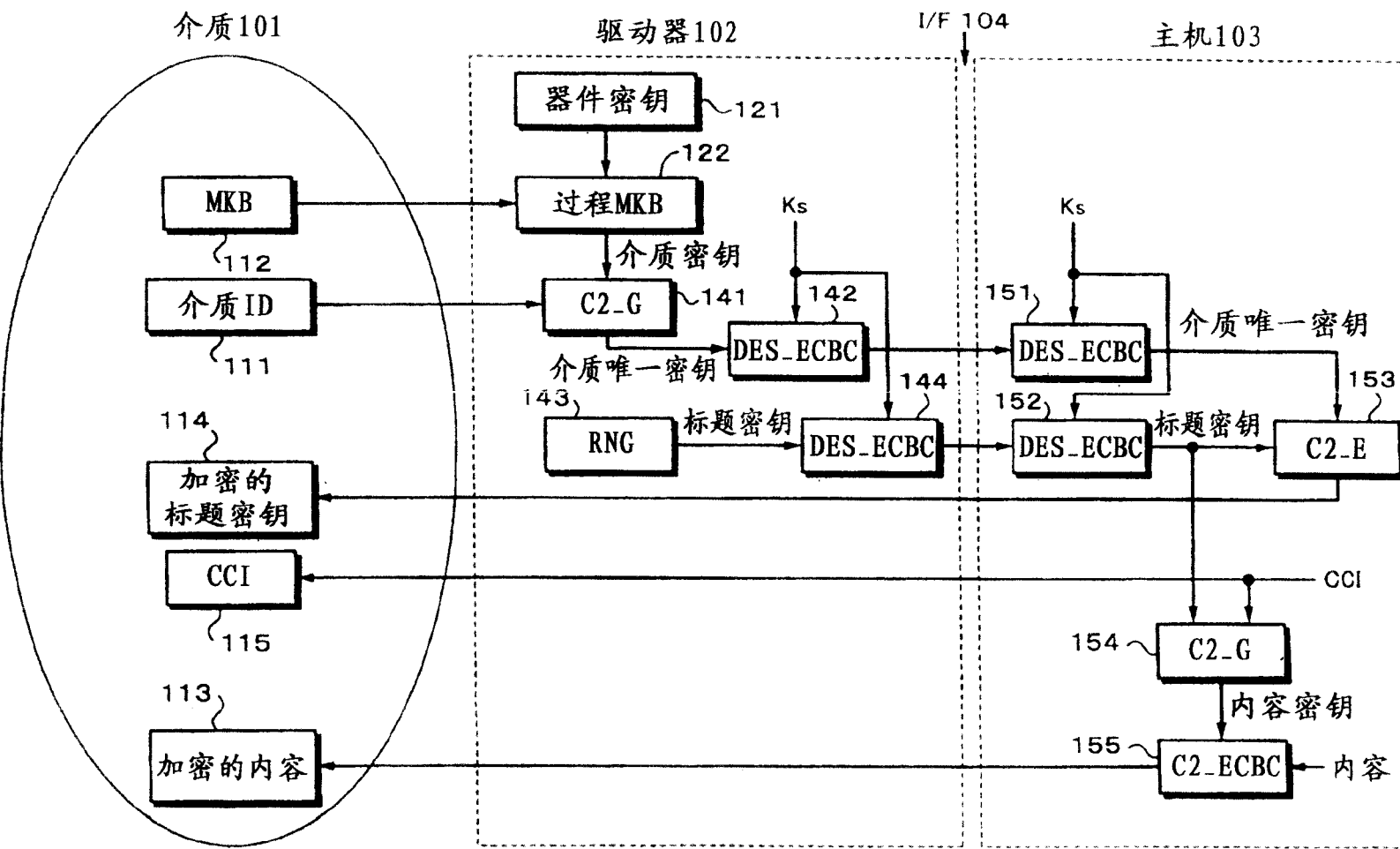

介质101
驱动器-主机 I/F 104
驱动器102
主机103
MKB
112
驱动器的器件密钥
121
过程MKB
122
介质密钥Km
MAC
123
RNG
126
MAC
124
129
RNG
127
MAC
125
RNG
128
对话密钥Ks=eKm(Ra3 || Rb3)
Rb1
eKm(Ra1 || Rb1)
Ra1
Rb2
eKm(Rb2 || Ra2)
Ra2
Rb3
Ra3
CMP
139
主机的器件密钥
131
过程MKB
132
介质密钥Km
MAC
133
RNG
136
MAC
134
RNG
137
MAC
135
RNG
138
对话密钥Ks=eKm(Ra3 || Rb3)

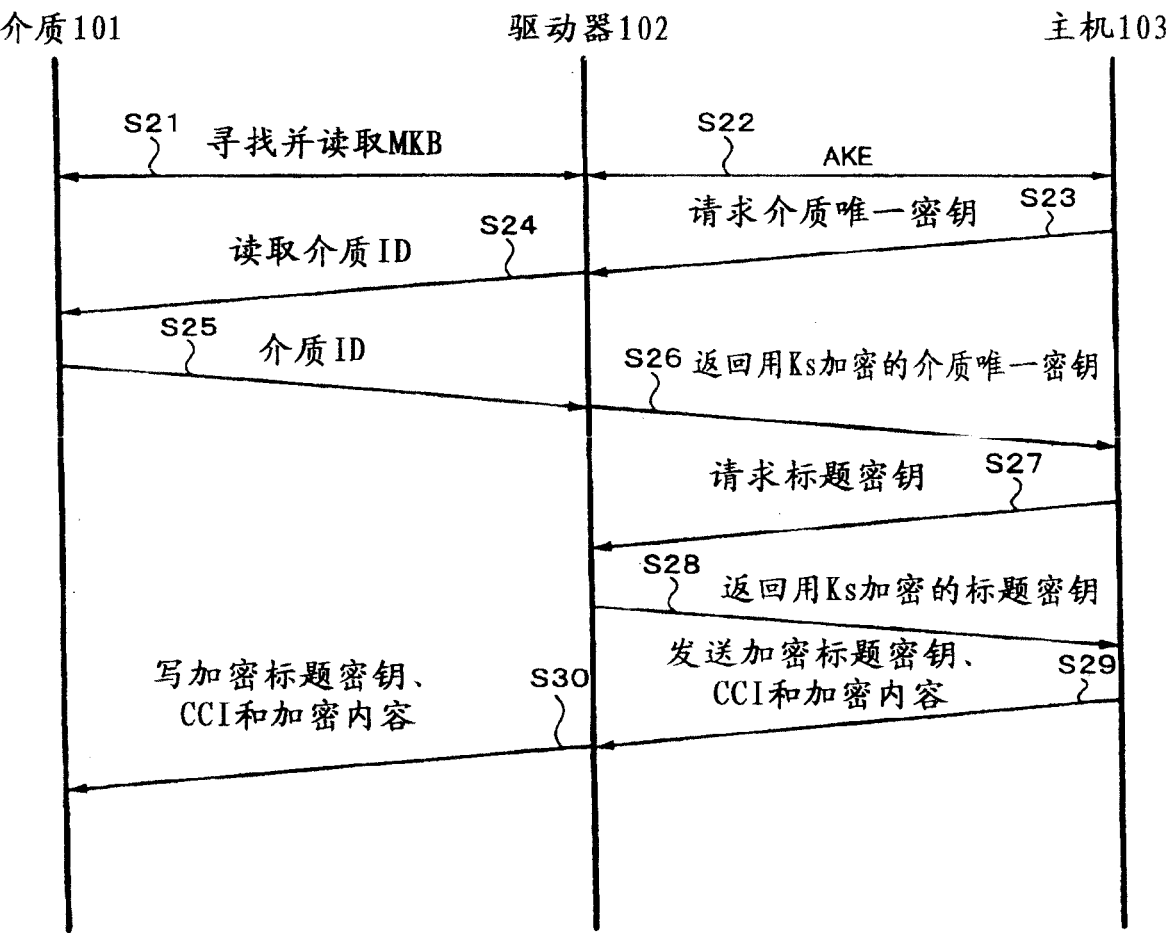
驱动器102

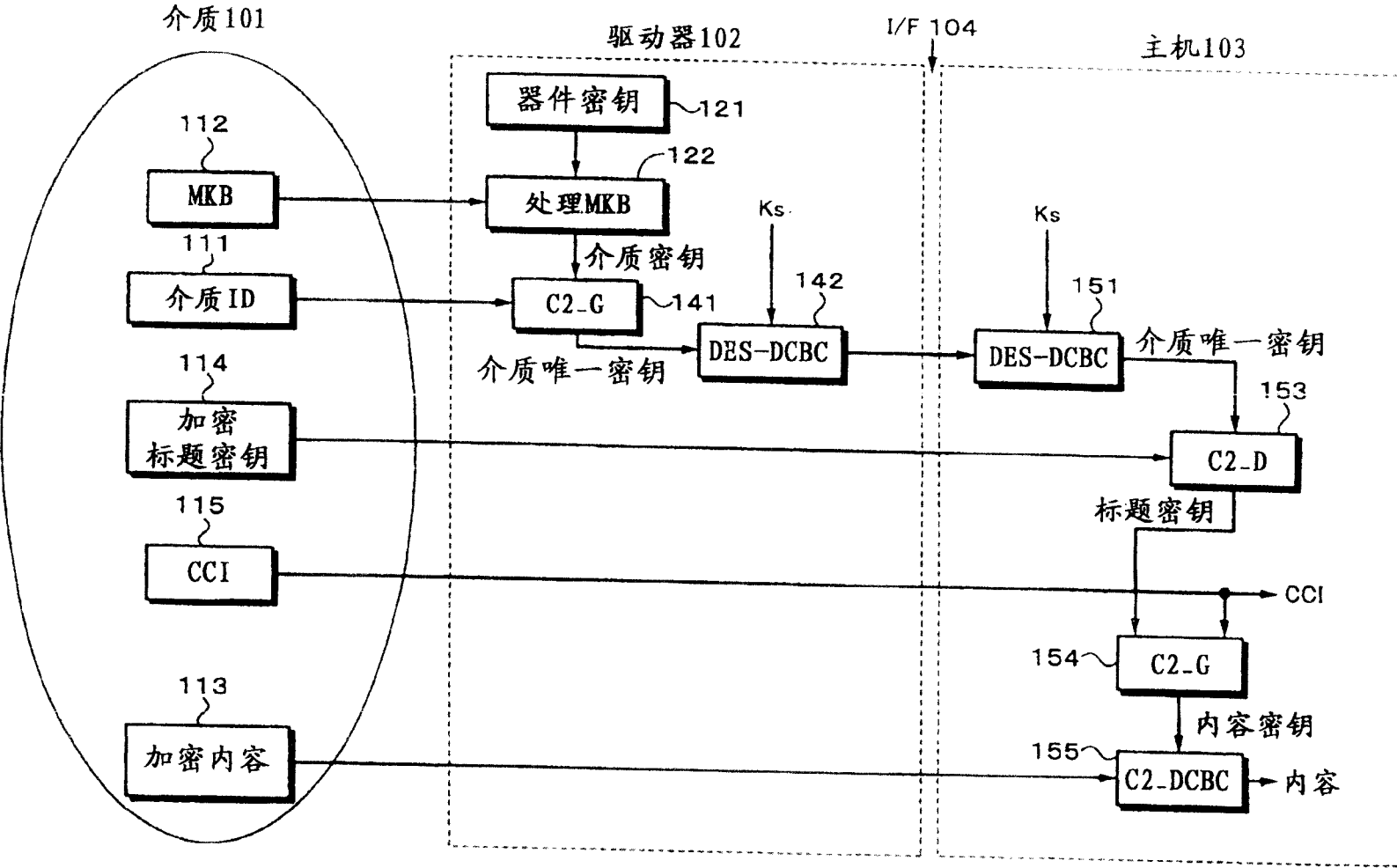

开始
ST10
ST11
ST12
否
是
撤销
ST13
ST14
ST15
ST16
是
ST17
否
ST18
ST19
结束
拒绝

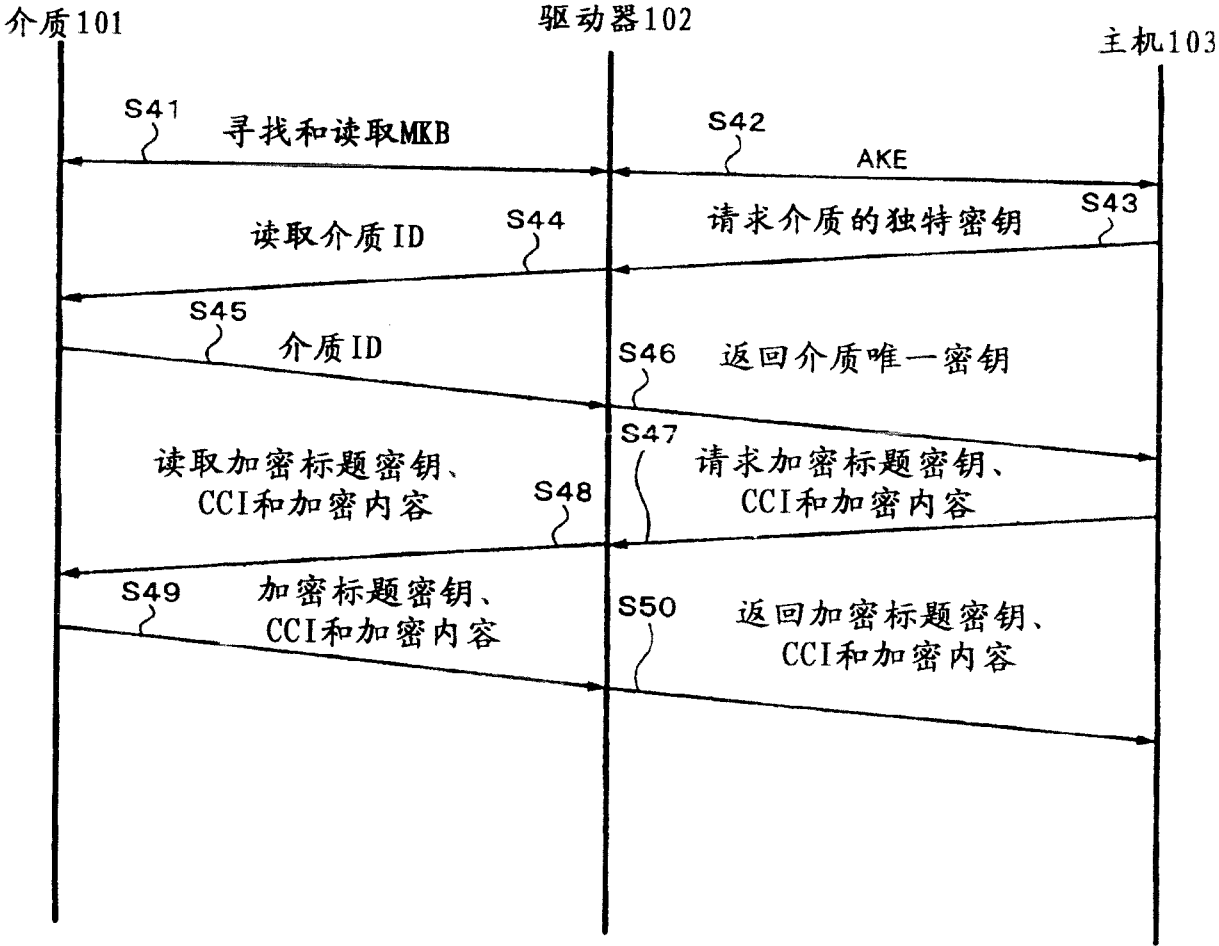
主机103

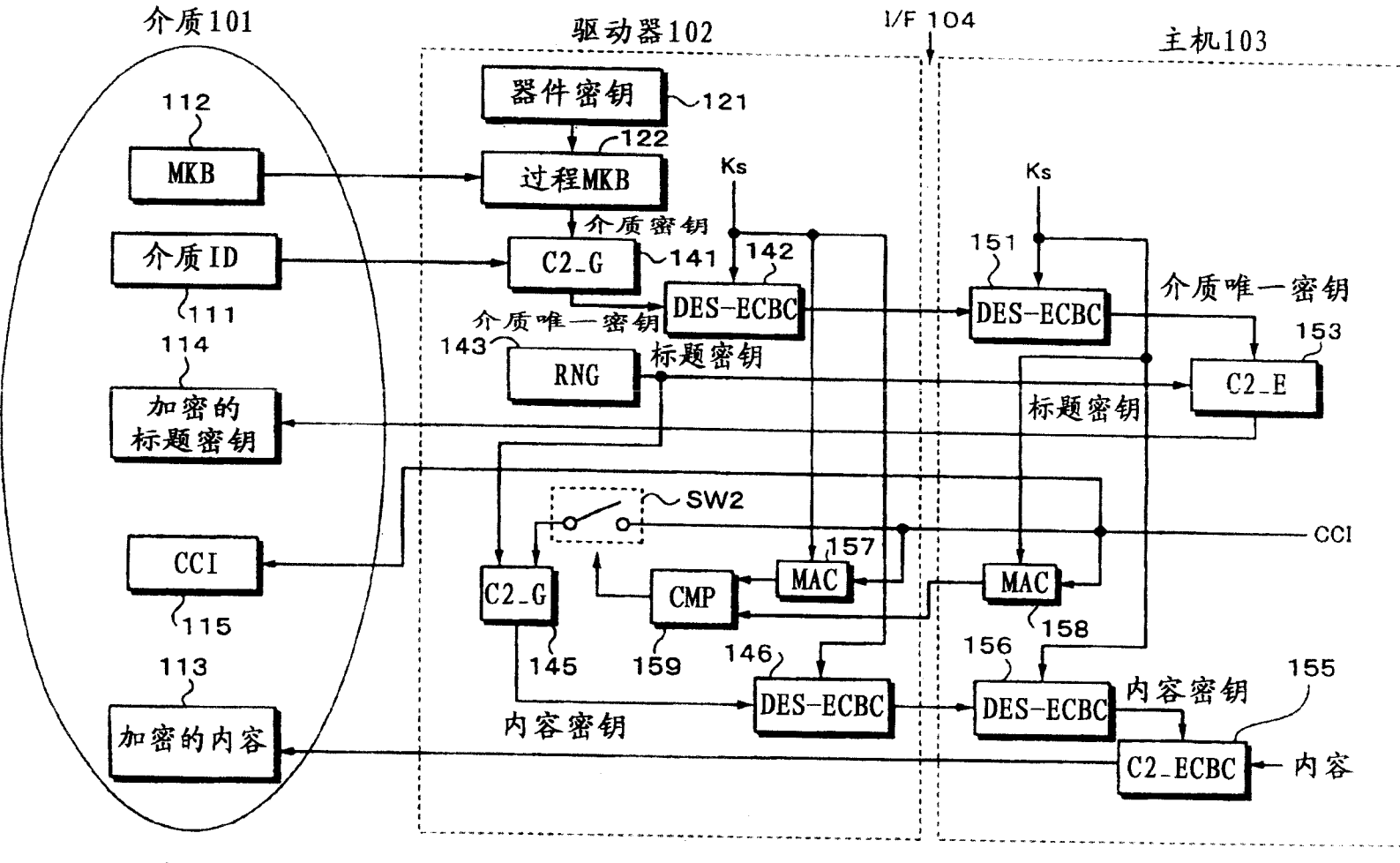

开始
ST20
ST21
ST22
否
是
撤销
ST23
ST24
是
ST25
否
ST26
ST27
ST28
是
否
ST29
结束
拒绝


介质101
驱动器102
I/F 104
主机103
器件密钥
121
122
MKB
过程MKB
Ks
Ks
介质密钥
112
介质ID
C2_G
141
142
151
介质唯一密钥
111
DES_ECBC
DES_ECBC
介质唯一密钥
153
143
144
152
RNG
标题密钥
DES_ECBC
DES_ECBC
标题密钥
C2_E
114
加密的
标题密钥
CCI
CCI
115
154
C2_G
113
内容密钥
加密的内容
155
C2_ECBC
内容


介质101
驱动器102
主机103
S21
寻找并读取MKB
S22
AKE
请求介质唯一密钥
S23
S24
读取介质ID
S25
介质ID
S26 返回用Ks加密的介质唯一密钥
请求标题密钥
S27
S28
返回用Ks加密的标题密钥
发送加密标题密钥、
CCI和加密内容
S29
写加密标题密钥、
CCI和加密内容
S30


介质101
驱动器102
I/F 104
主机103
器件密钥
121
112
MKB
122
处理MKB
Ks
Ks
介质密钥
111
介质ID
C2_G
141
142
151
介质唯一密钥
DES-DCBC
DES-DCBC
介质唯一密钥
153
114
加密
标题密钥
C2_D
标题密钥
115
CCI
CCI
154
C2_G
内容密钥
113
155
加密内容
C2_DCBC
内容


介质101
驱动器102
主机103
S41
寻找和读取MKB
S42
AKE
S43
请求介质的独特密钥
S44
读取介质ID
S45
介质ID
S46
返回介质唯一密钥
S47
请求加密标题密钥、
CCI和加密内容
S48
读取加密标题密钥、
CCI和加密内容
S49
加密标题密钥、
CCI和加密内容
S50
返回加密标题密钥、
CCI和加密内容


介质101
驱动器102
I/F 104
主机103
器件密钥
121
122
MKB
过程MKB
Ks
介质密钥
介质ID
C2_G
141
142
DES-ECBC
介质唯一密钥
111
介质唯一密钥
143
RNG
标题密钥
114
加密的
标题密钥
SW2
CCI
115
C2_G
CMP
MAC
157
158
145
159
146
156
113
内容密钥
DES-ECBC
155
加密的内容
C2_ECBC
内容
151
153
C2_E

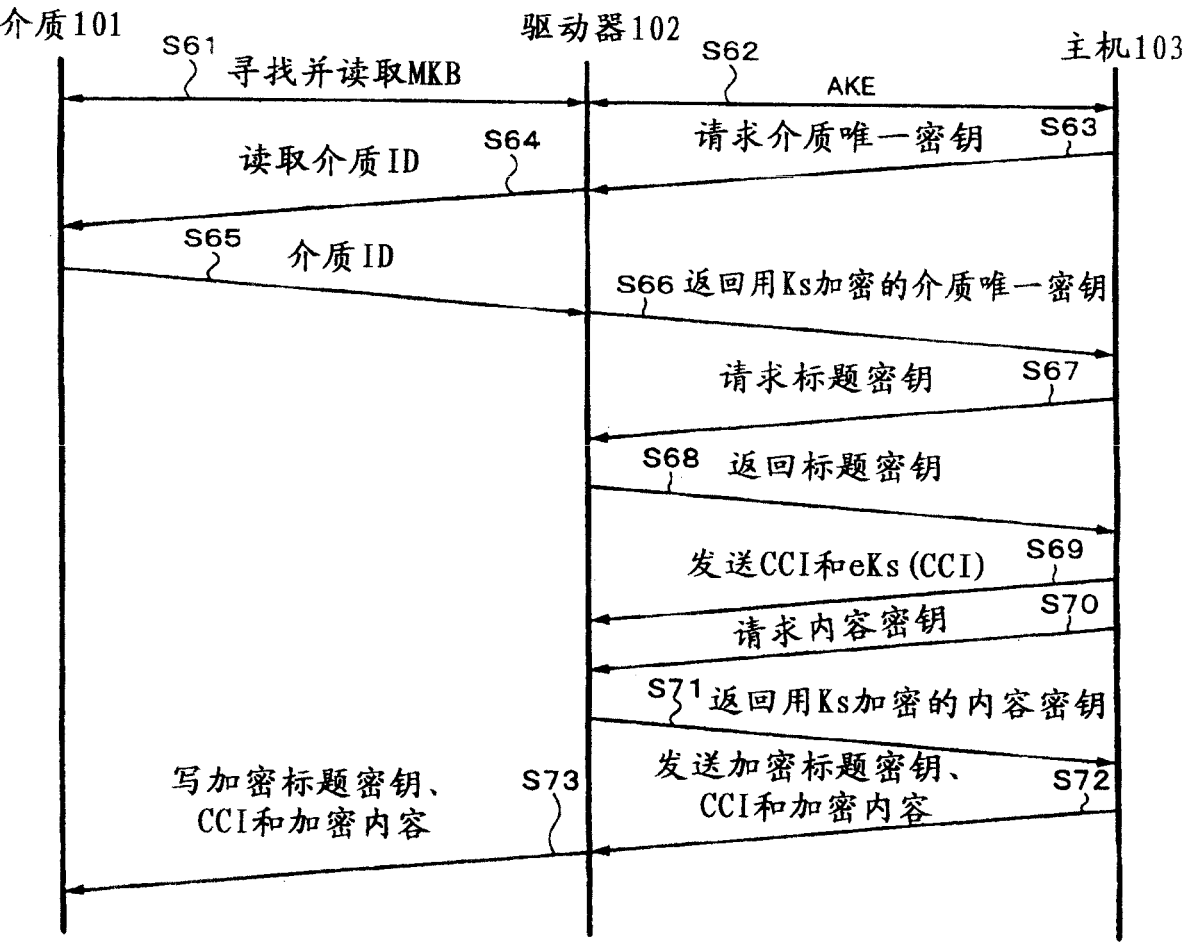

介质101
驱动器102
主机103
S61
寻找并读取MKB
S62
AKE
请求介质唯一密钥
S63
读取介质ID
S64
S65
介质ID
S66 返回用Ks加密的介质唯一密钥
请求标题密钥
S67
S68
返回标题密钥
发送CCI和eKs(CCI)
S69
请求内容密钥
S70
S71
返回用Ks加密的内容密钥
写加密标题密钥、
CCI和加密内容
S73
发送加密标题密钥、
CCI和加密内容
S72

图1

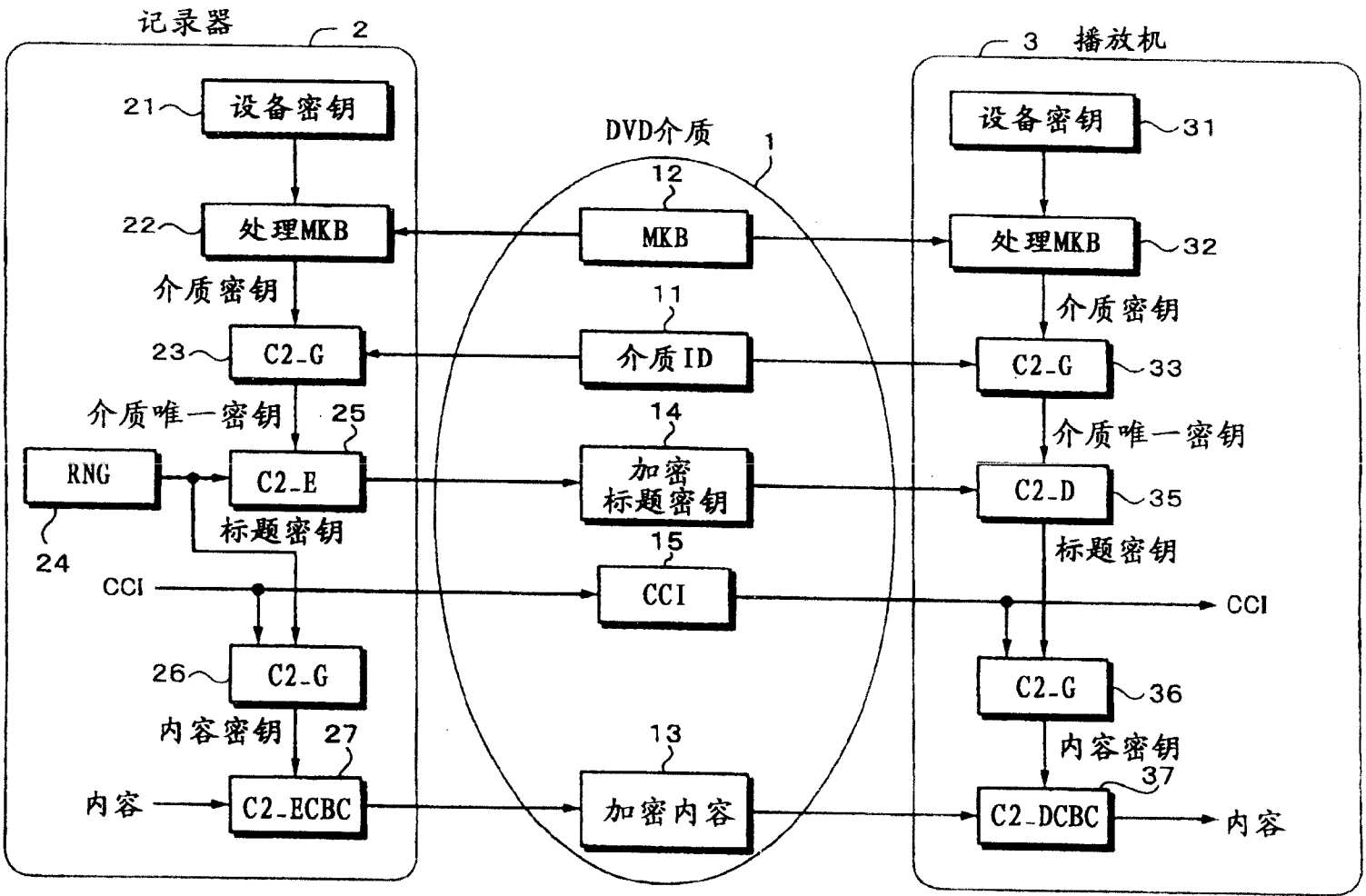

记录器
2
3 播放机
DVD介质
1
21
设备密钥
22
处理MKB
介质密钥
23
C2_G
介质唯一密钥
25
RNG
C2_E
标题密钥
24
CCI
26
C2_G
内容密钥
27
内容
C2_ECBC
12
MKB
11
介质ID
14
加密
标题密钥
15
CCI
13
加密内容
设备密钥
31
处理MKB
32
介质密钥
C2_G
33
介质唯一密钥
C2_D
35
标题密钥
CCI
C2_G
36
内容密钥
37
C2_DCBC
内容

图2

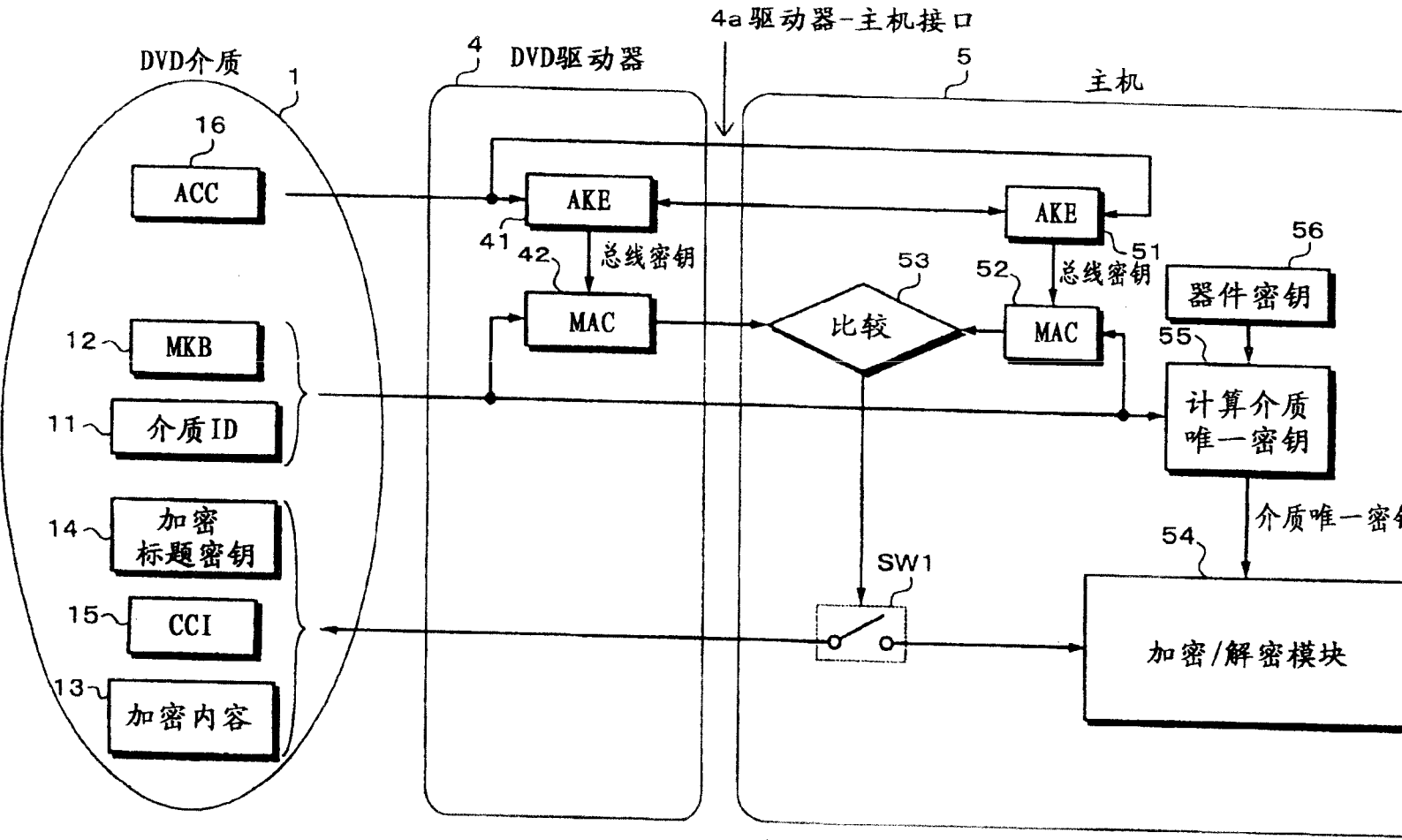

4a 驱动器-主机接口
DVD介质
1
4
DVD驱动器
5
主机
16
ACC
AKE
AKE
41
42
总线密钥
51
总线密钥
53
52
56
器件密钥
MAC
比较
MAC
55
12
MKB
11
介质ID
计算介质唯一密钥
介质唯一密钥
14
加密标题密钥
54
SW1
15
CCI
加密/解密模块
13
加密内容

图 3

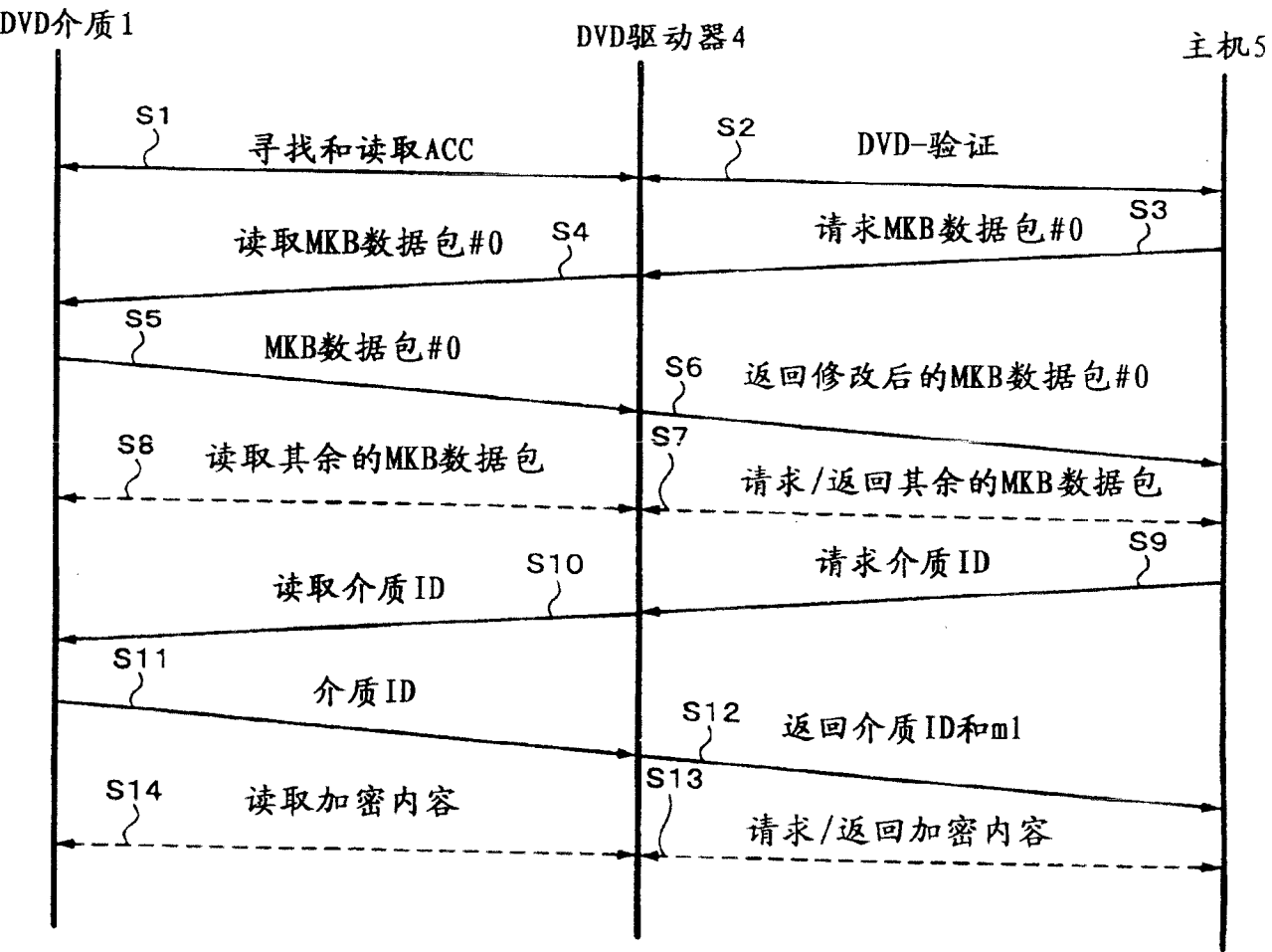

DVD介质1
DVD驱动器4
主机5
S1
寻找和读取ACC
S2
DVD-验证
S3
请求MKB数据包#0
S4
读取MKB数据包#0
S5
MKB数据包#0
S6
返回修改后的MKB数据包#0
S7
请求/返回其余的MKB数据包
S8
读取其余的MKB数据包
S9
请求介质ID
S10
读取介质ID
S11
介质ID
S12
返回介质ID和m1
S13
请求/返回加密内容
S14
读取加密内容

图4

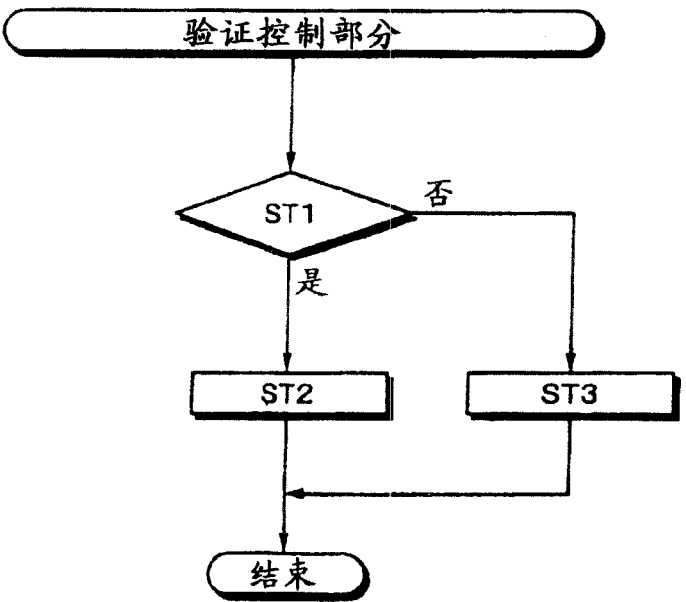


图5

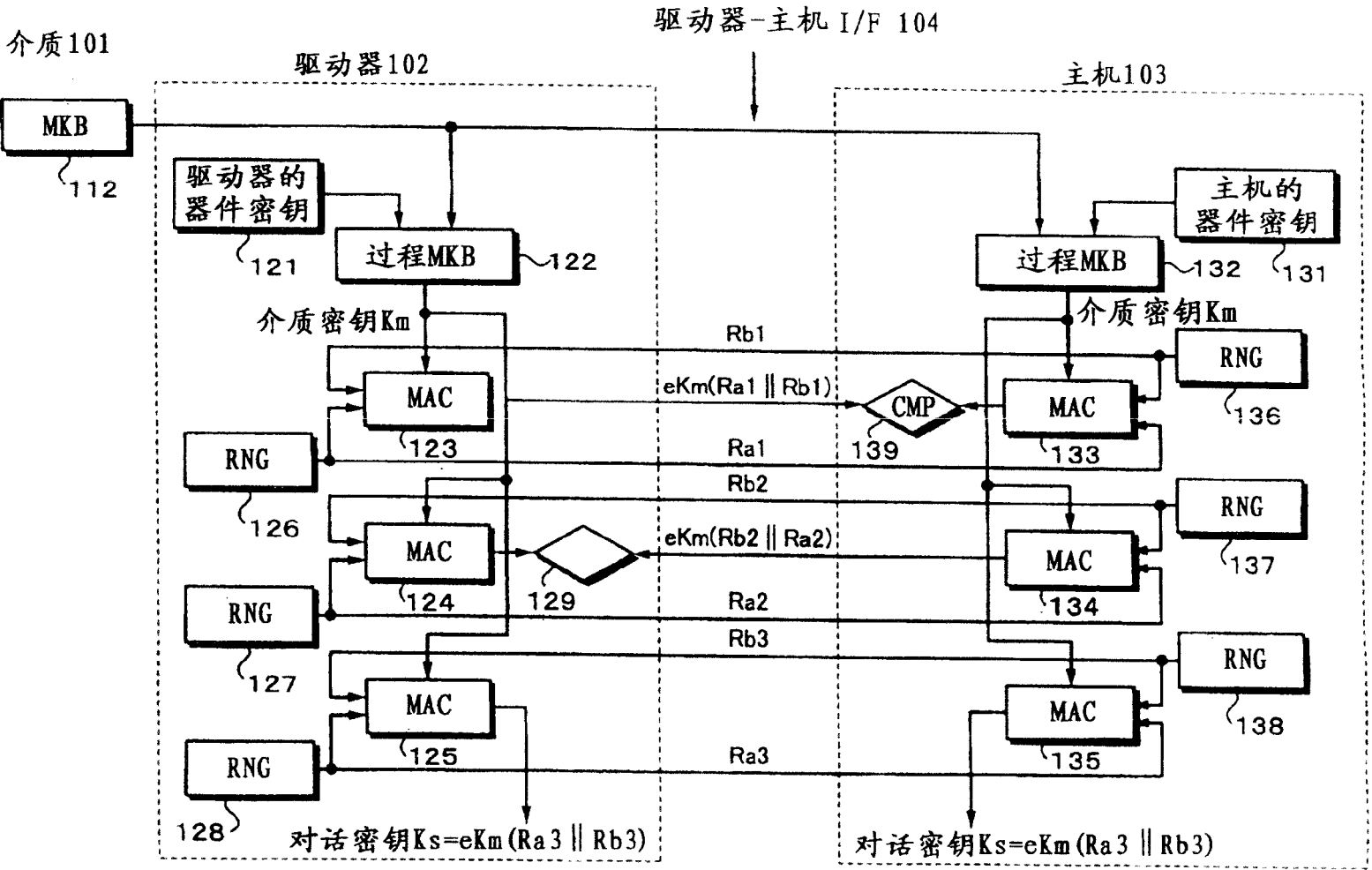

介质101
驱动器-主机 I/F 104
驱动器102
主机103
MKB
112
驱动器的器件密钥
121
过程MKB
122
介质密钥Km
主机的器件密钥
131
过程MKB
132
介质密钥Km
Rb1
eKm(Ra1 || Rb1)
MAC
123
CMP
139
MAC
133
RNG
136
RNG
126
Ra1
Rb2
eKm(Rb2 || Ra2)
MAC
124
129
MAC
134
RNG
137
RNG
127
Ra2
Rb3
MAC
125
MAC
135
RNG
138
RNG
128
Ra3
对话密钥Ks=eKm(Ra3 || Rb3)
对话密钥Ks=eKm(Ra3 || Rb3)

图6

驱动器102

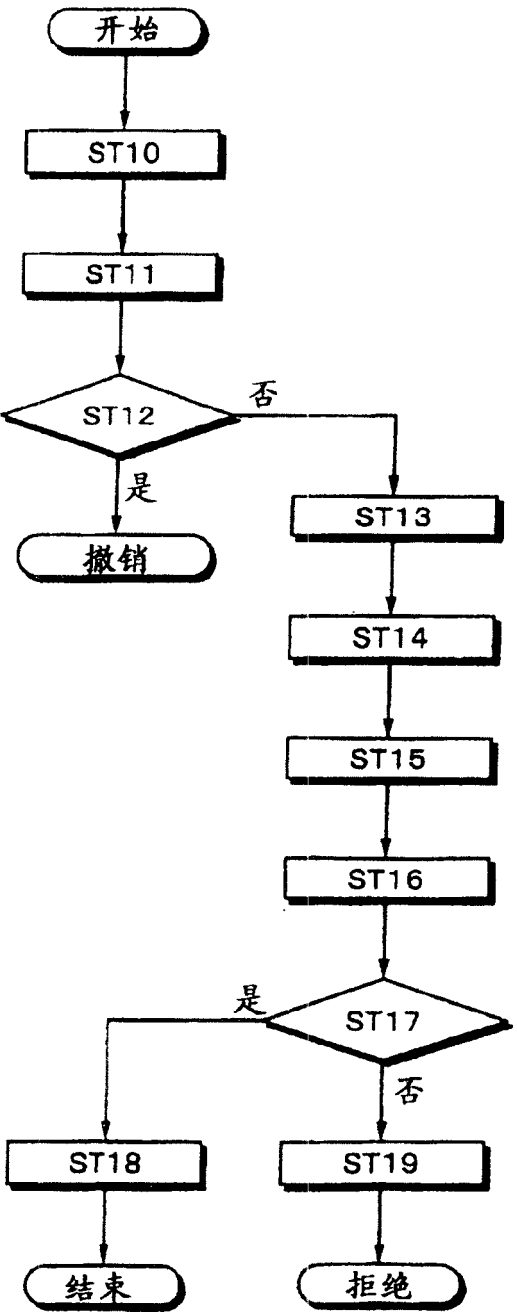

开始
ST10
ST11
ST12
否
是
撤销
ST13
ST14
ST15
ST16
是
ST17
否
ST18
ST19
结束
拒绝

图7

主机103

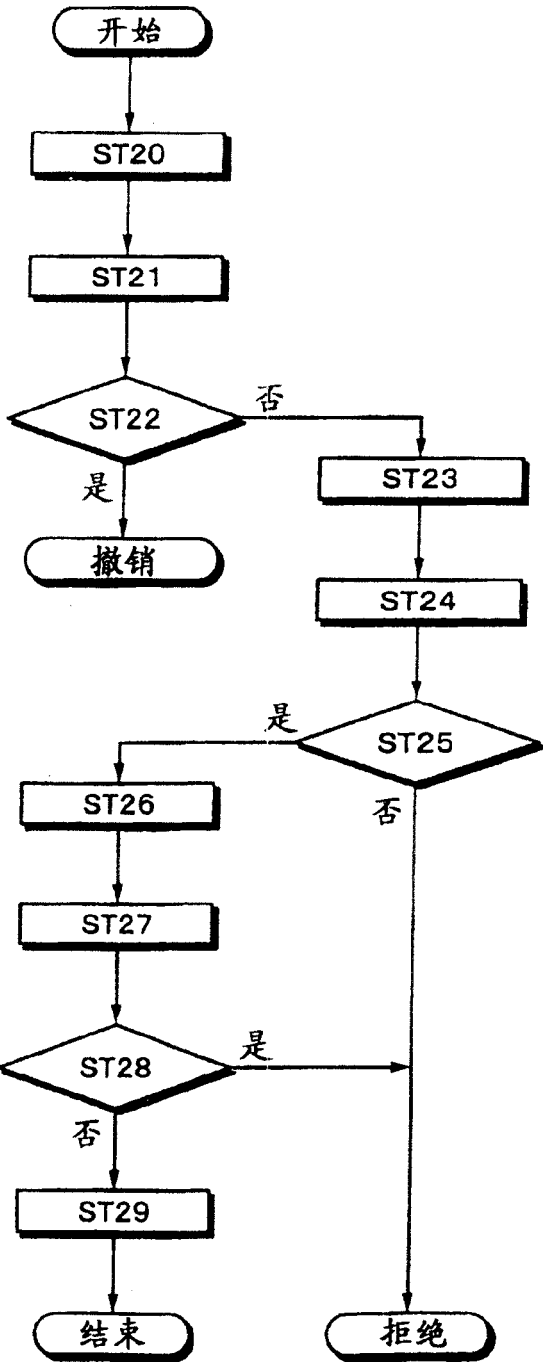

开始
ST20
ST21
ST22
否
是
撤销
ST23
ST24
ST25
是
否
ST26
ST27
ST28
是
否
ST29
结束
拒绝

图8

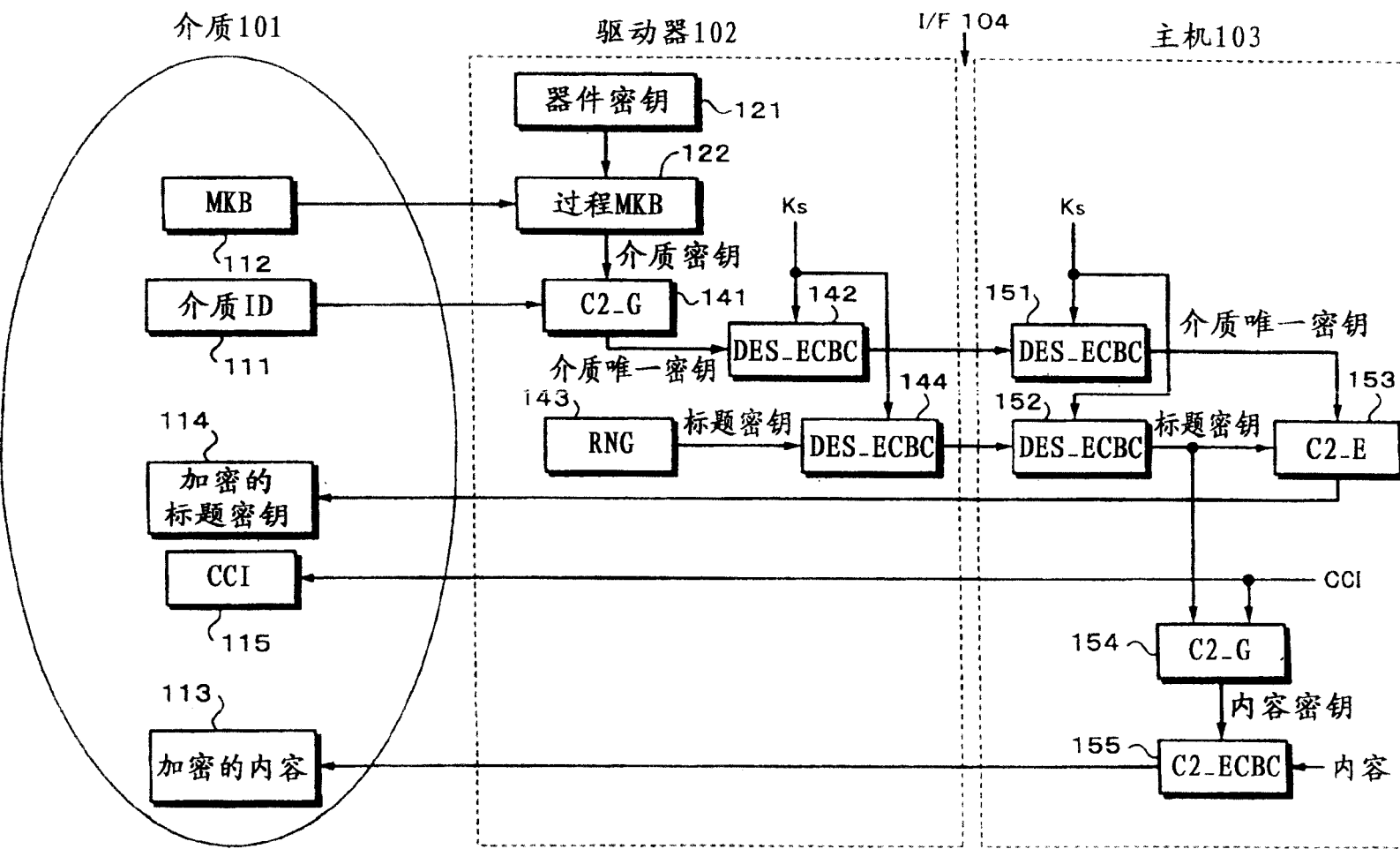

介质101
驱动器102
I/F 104
主机103
器件密钥
121
122
MKB
过程MKB
Ks
Ks
介质密钥
112
介质ID
C2_G
141
142
151
介质唯一密钥
111
DES_ECBC
DES_ECBC
介质唯一密钥
153
143
144
152
114
RNG
标题密钥
DES_ECBC
DES_ECBC
标题密钥
C2_E
加密的
标题密钥
CCI
CCI
115
154
C2_G
113
内容密钥
加密的内容
155
C2_ECBC
内容

图9

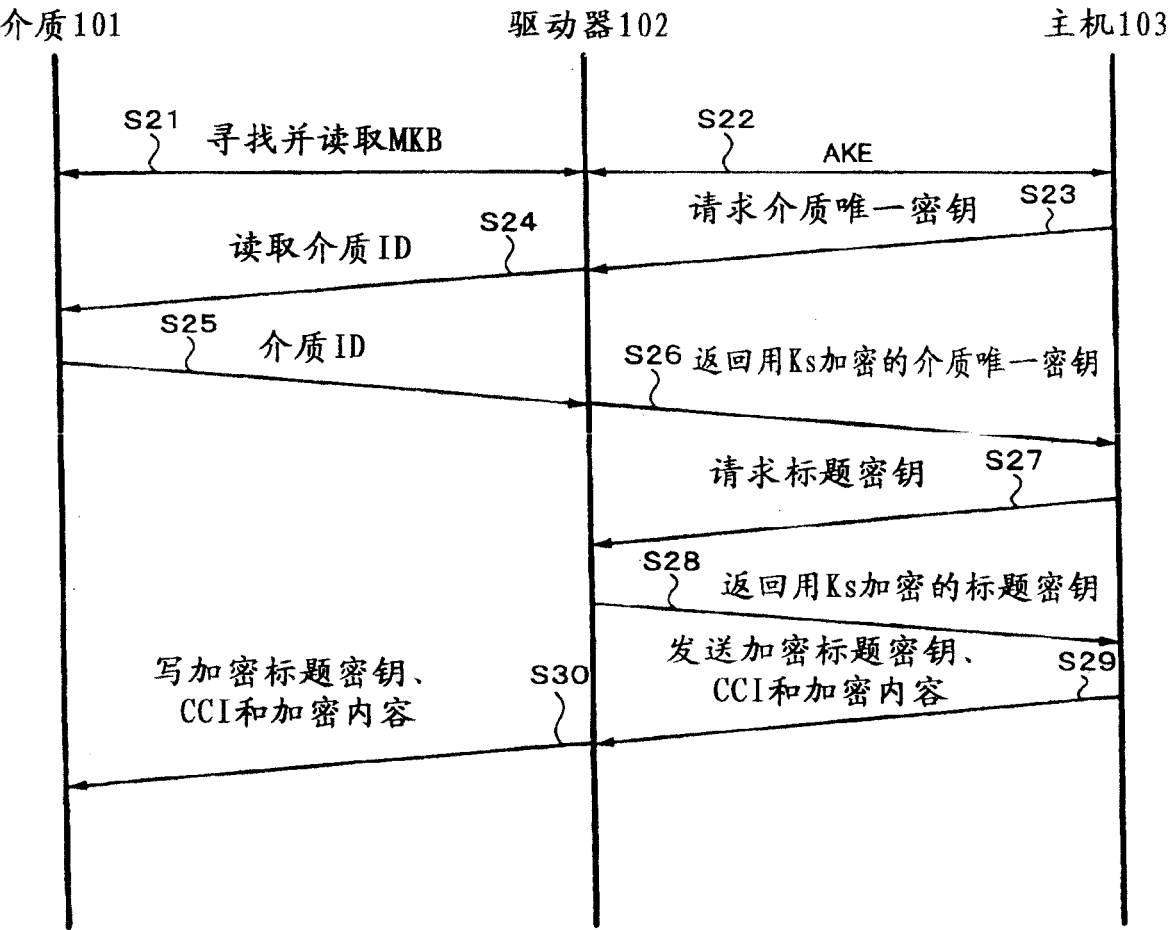

介质101
驱动器102
主机103
S21
寻找并读取MKB
S22
AKE
请求介质唯一密钥
S23
S24
读取介质ID
S25
介质ID
S26
返回用Ks加密的介质唯一密钥
请求标题密钥
S27
S28
返回用Ks加密的标题密钥
发送加密标题密钥、
CCI和加密内容
S29
写加密标题密钥、
CCI和加密内容
S30

图10

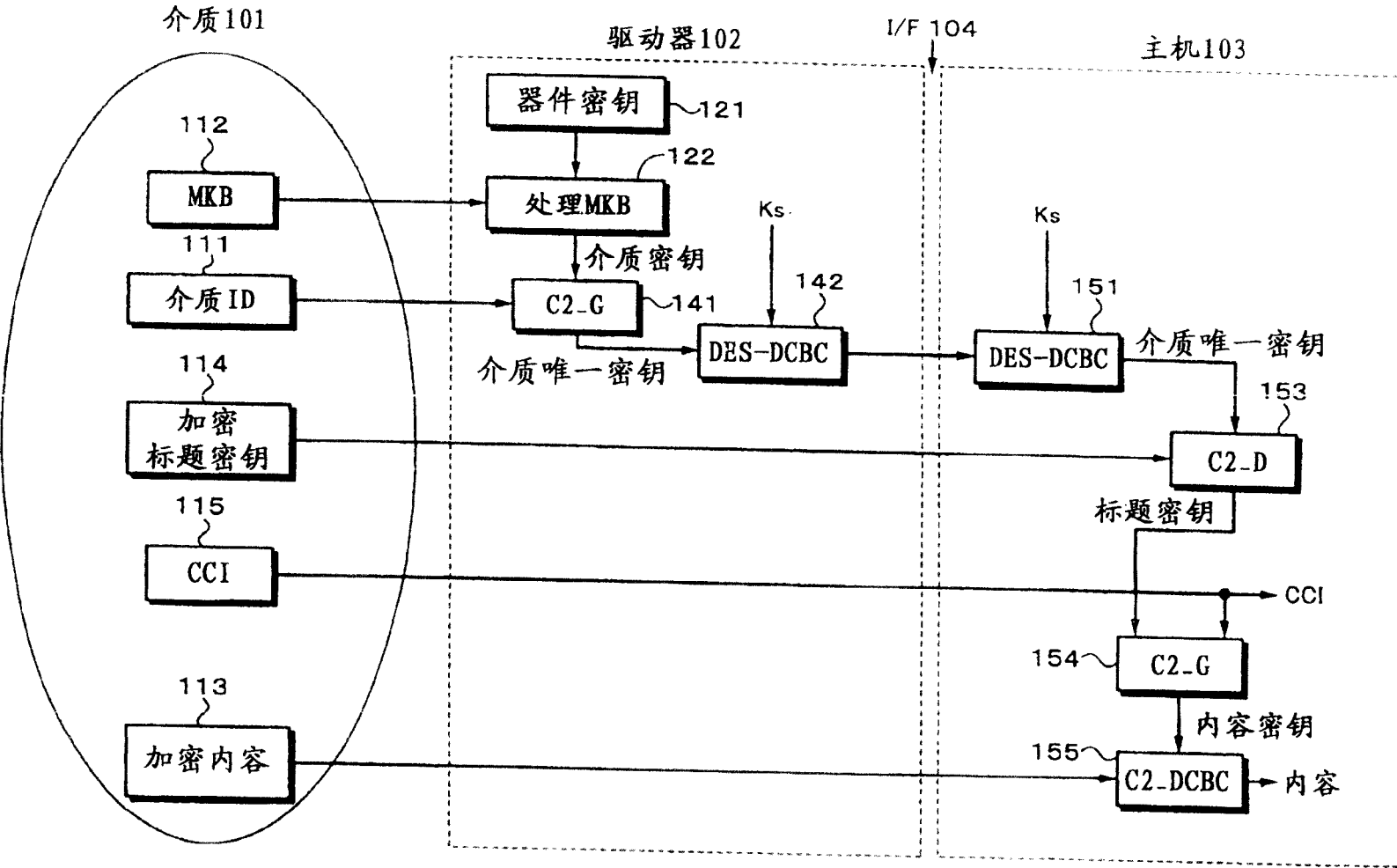

介质101
驱动器102
I/F 104
主机103
器件密钥
121
112
MKB
122
处理MKB
Ks
Ks
介质密钥
111
介质ID
C2_G
141
142
151
介质唯一密钥
DES-DCBC
DES-DCBC
介质唯一密钥
114
153
加密
标题密钥
C2_D
标题密钥
115
CCI
CCI
154
C2_G
内容密钥
113
155
加密内容
C2_DCBC
内容

图11

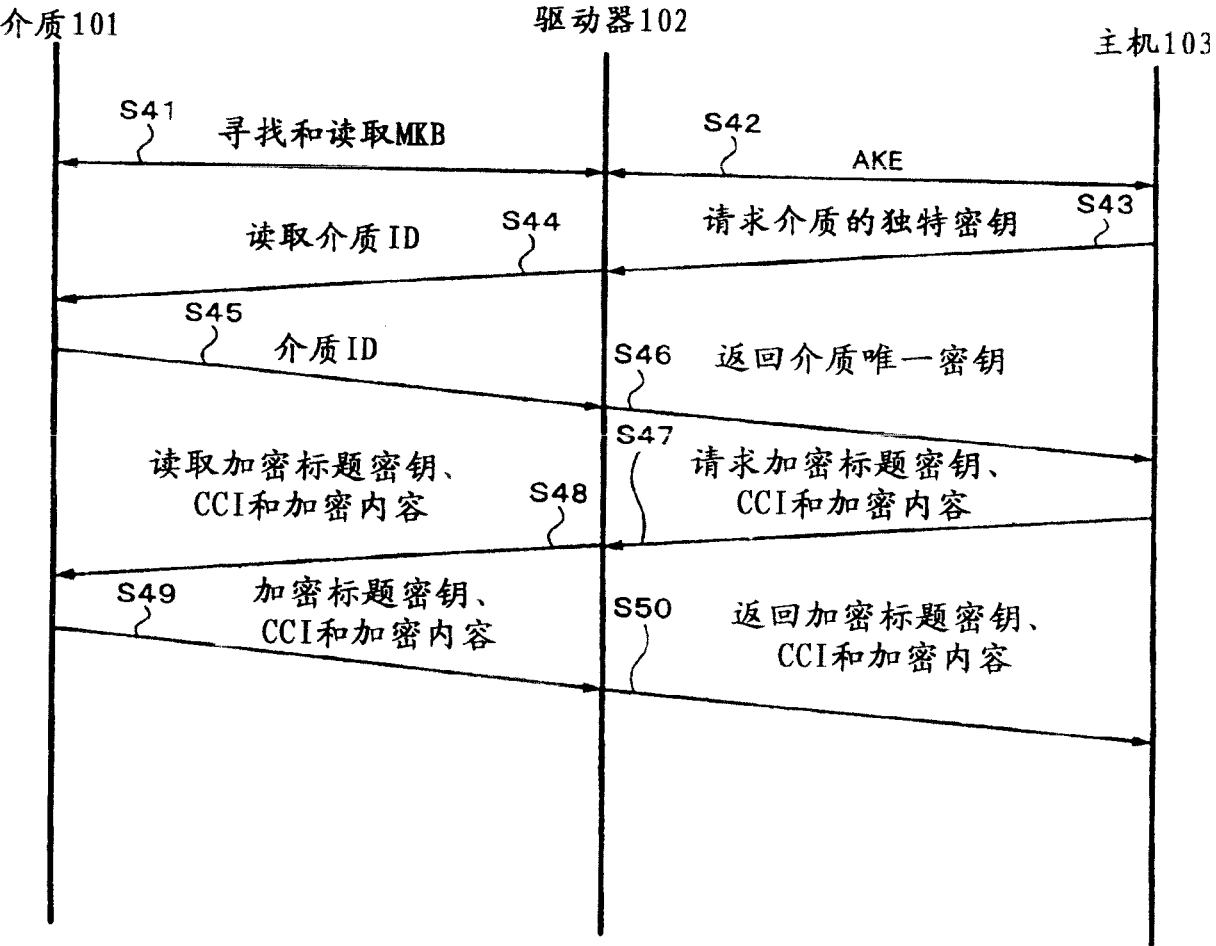

介质101
驱动器102
主机103
S41
寻找和读取MKB
S42
AKE
S43
请求介质的独特密钥
S44
读取介质ID
S45
介质ID
S46
返回介质唯一密钥
S47
请求加密标题密钥、
CCI和加密内容
S48
读取加密标题密钥、
CCI和加密内容
S49
加密标题密钥、
CCI和加密内容
S50
返回加密标题密钥、
CCI和加密内容

图12

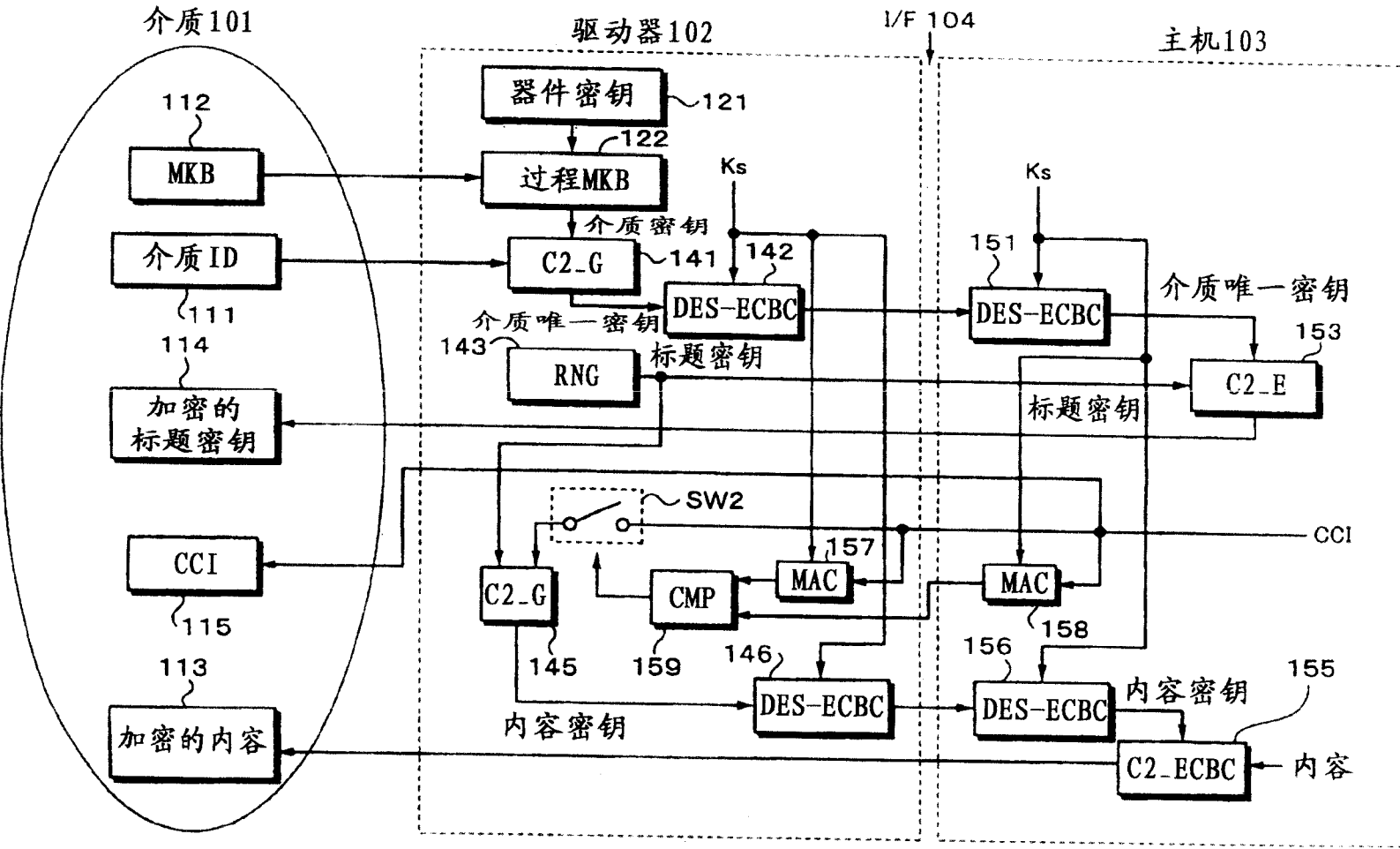
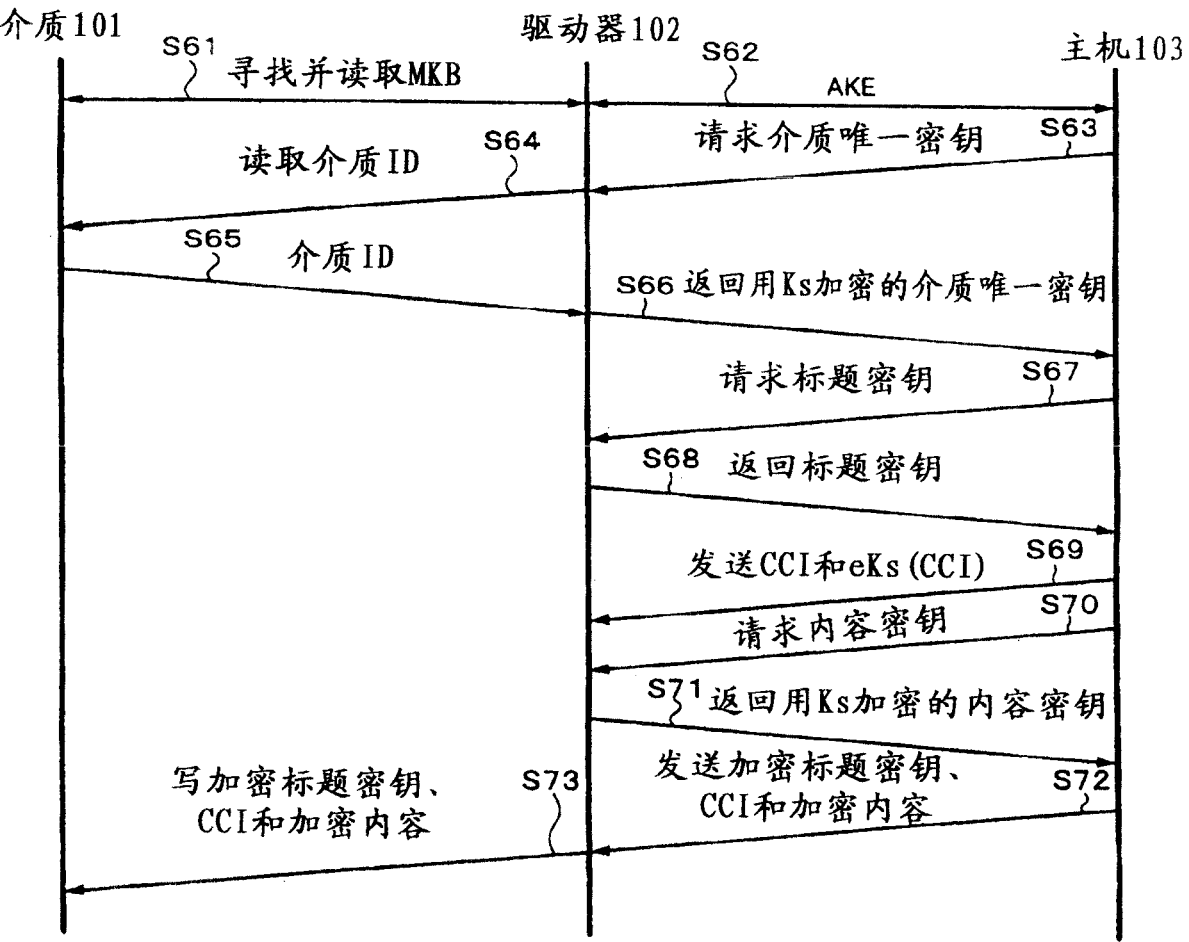

介质101
驱动器102
I/F 104
主机103
器件密钥
121
122
过程MKB
介质密钥
C2_G
141
142
DES-ECBC
介质唯一密钥
143
RNG
标题密钥
112
MKB
介质ID
111
114
加密的
标题密钥
CCI
115
113
加密的内容
SW2
C2_G
CMP
MAC
157
145
159
146
DES-ECBC
内容密钥
Ks
151
DES-ECBC
介质唯一密钥
153
C2_E
标题密钥
MAC
158
156
DES-ECBC
内容密钥
155
C2_ECBC
内容
CCI

图13


介质101
驱动器102
主机103
S61
寻找并读取MKB
S62
AKE
请求介质唯一密钥
S63
读取介质ID
S64
S65
介质ID
S66 返回用Ks加密的介质唯一密钥
请求标题密钥
S67
S68
返回标题密钥
发送CCI和eKs(CCI)
S69
请求内容密钥
S70
S71
返回用Ks加密的内容密钥
发送加密标题密钥、
CCI和加密内容
S72
写加密标题密钥、
CCI和加密内容
S73

参考号描述

1	DVD介质
2	记录器
3	播放器
4	DVD 驱动器
4a	接口
5	主机
11	介质 ID
12	介质密钥块（MKB）
13	加密内容
42, 52	MAC 计算部件
46	器件密钥
46a	器件密钥的第一半部分
47	DES 加密器
48	介质唯一密钥计算部件
49, 49a	DES 加密器
49b	DES 解密器
53	比较 MAC 的比较部分
54	加密/解密模块
55	介质唯一密钥计算部件
101	介质
102	驱动器
103	主机
104	接口
121	驱动器的器件密钥

122 过程 **MKB**

123, 124, 125 驱动器的 **MAC** 计算部件

126, 127, 128 驱动器的随机数产生器

129 比较

131 主机的器件密钥

132 过程 **MKB**

133, 134, 135 主机的 **MAC** 计算部件

136, 137, 138 主机的随机数产生器

139 比较

141, 154 C2_G

142, 144 **DES** 加密器

143 随机数产生器

151, 152, 156 **DES** 解密器

153 C2_E

155 C2_EBC

157, 158 **MAC** 计算部件

159 比较

ST1 计算的 **MAC** 值匹配?

ST2 接通开关

ST3 断开开关

ST10 报告密钥（**MKB**）

ST11 计算介质密钥 **Km**

ST12 撤销?

ST13 接收（**Rb1,Rb2**）

ST14 返回（**eKm(Ra1||Rb1),Ra1**）

ST15　返回（Ra2,Ra3）

ST16　接收（eKm(Rb2||Ra2),Rb3）

ST17　相同的 MAC?

ST18　确认的对话密钥 ekm(Ra3||Ra3)

ST19　返回（错误）

ST20　报告密钥（MKB）

ST21　计算介质密钥 Km

ST22　撤销?

ST23　发送密钥（Rb1,Rb2）

ST24　报告密钥（eKm(Ra1||Rb1),Ra1）

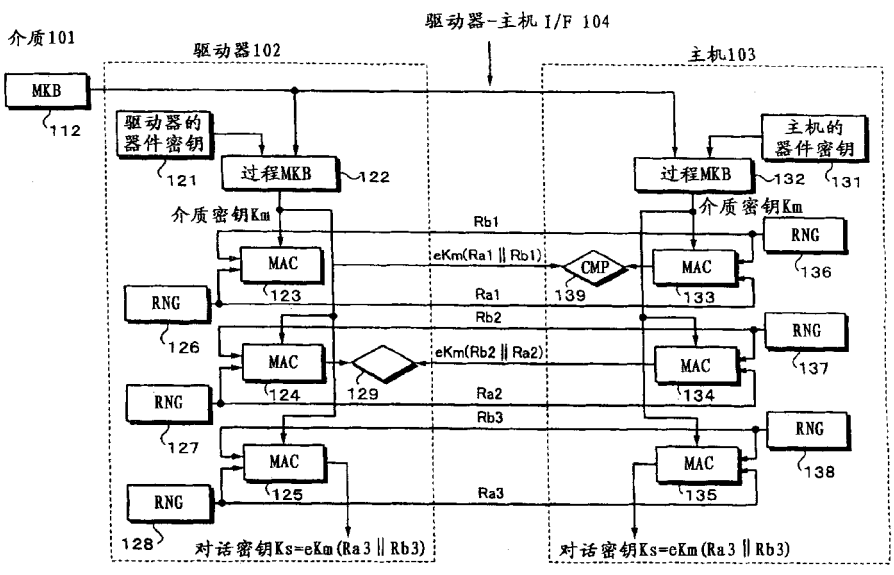
ST25　相同的 MAC?

ST26　报告密钥（Ra2，Ra3）

ST27　发送密钥（eKm(Rb2||Ra2),Rb3）

ST28　错误?

ST29　确认的对话密钥 ekm(Ra3||Ra3)


介质101
驱动器102
驱动器-主机 I/F 104
主机103
MKB
112
驱动器的器件密钥
121
过程MKB
122
介质密钥Km
主机的器件密钥
131
过程MKB
132
介质密钥Km
Rb1
eKm(Ra1 || Rb1)
CMP
139
RNG
136
MAC
123
MAC
133
RNG
126
Ra1
Rb2
RNG
137
MAC
124
129
eKm(Rb2 || Ra2)
MAC
134
RNG
127
Ra2
Rb3
RNG
138
MAC
125
MAC
135
RNG
128
Ra3
对话密钥Ks=eKm(Ra3 || Rb3)
对话密钥Ks=eKm(Ra3 || Rb3)