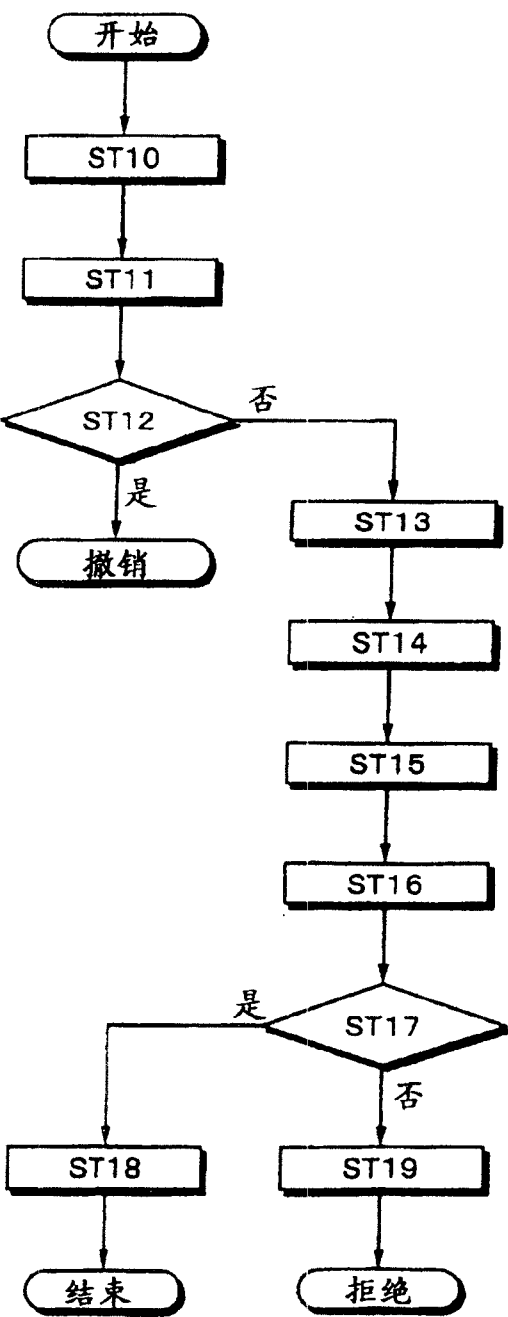
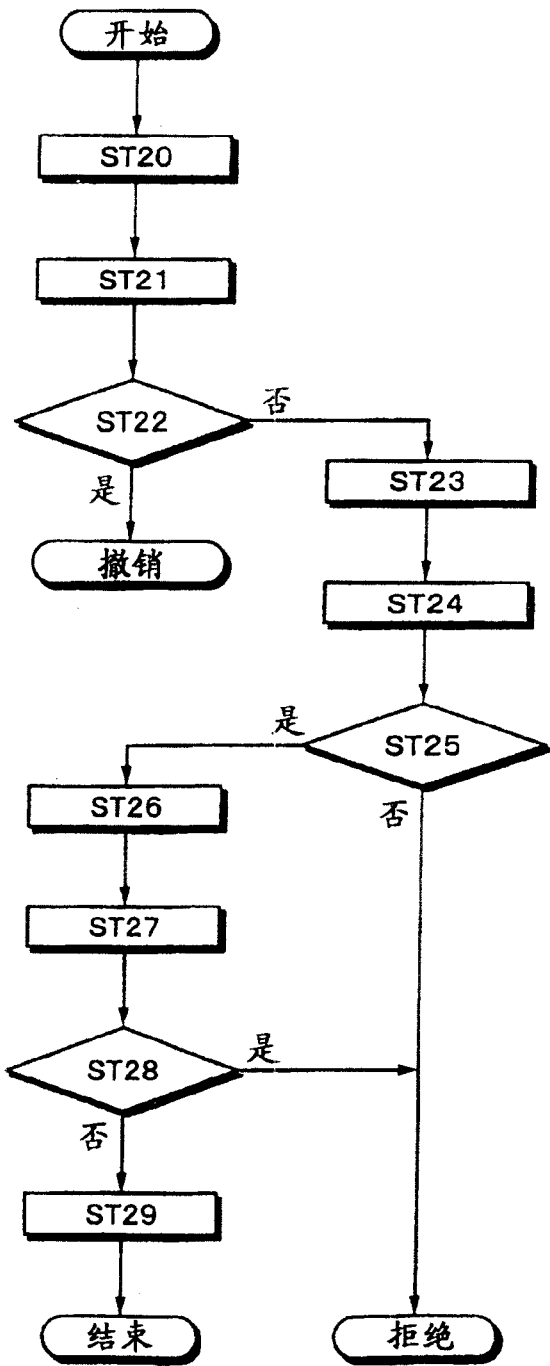
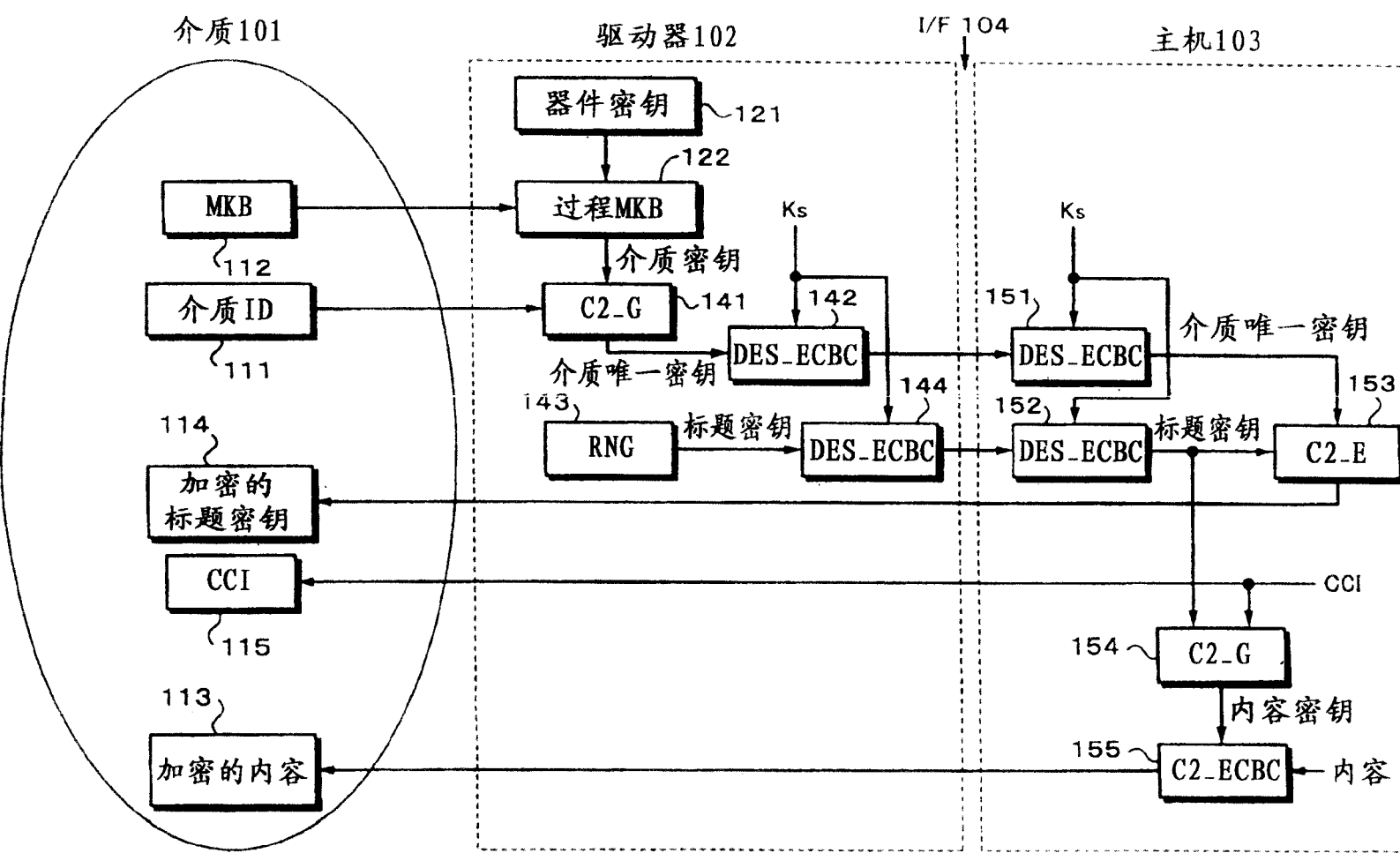


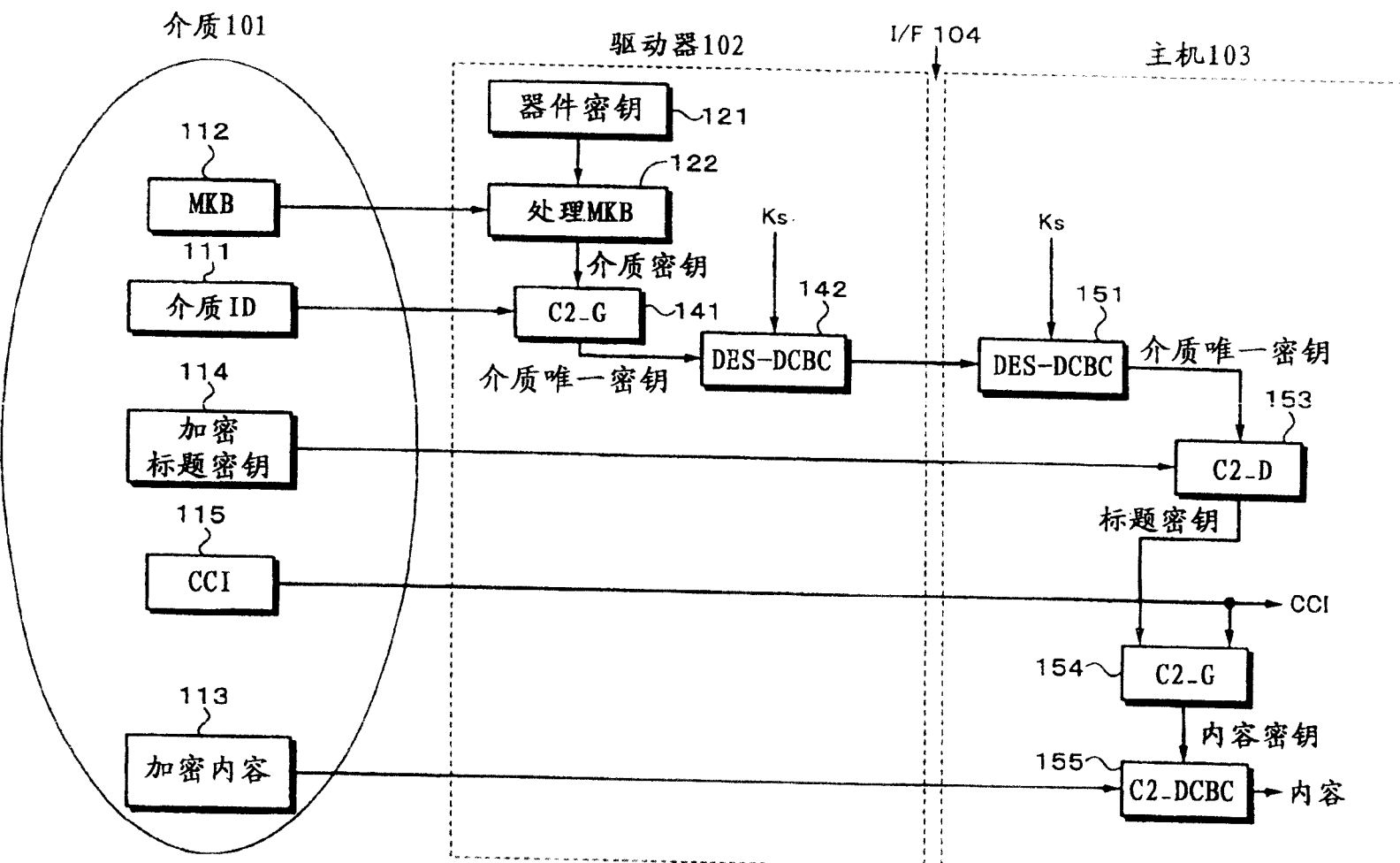
驱动器102

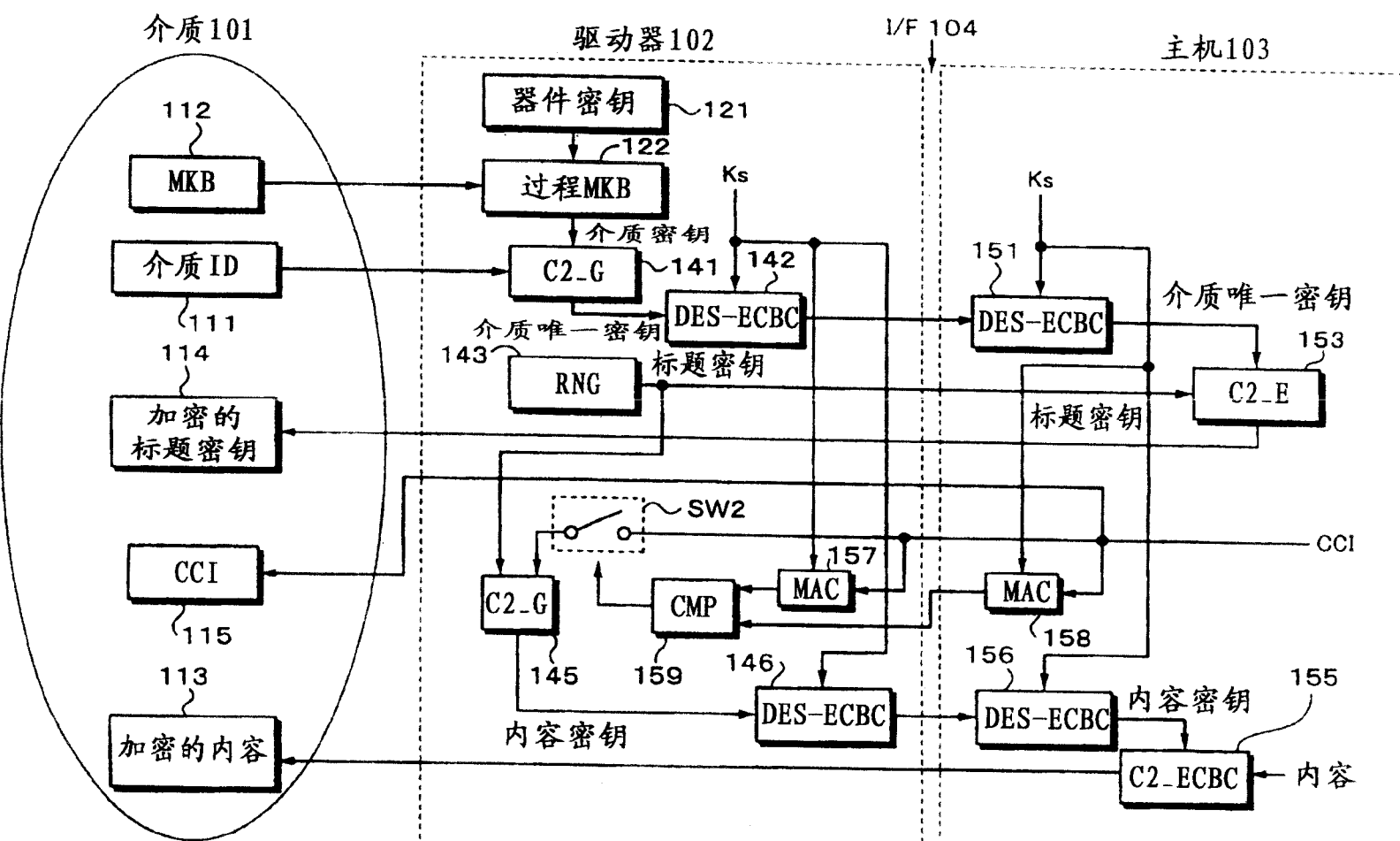


主机103









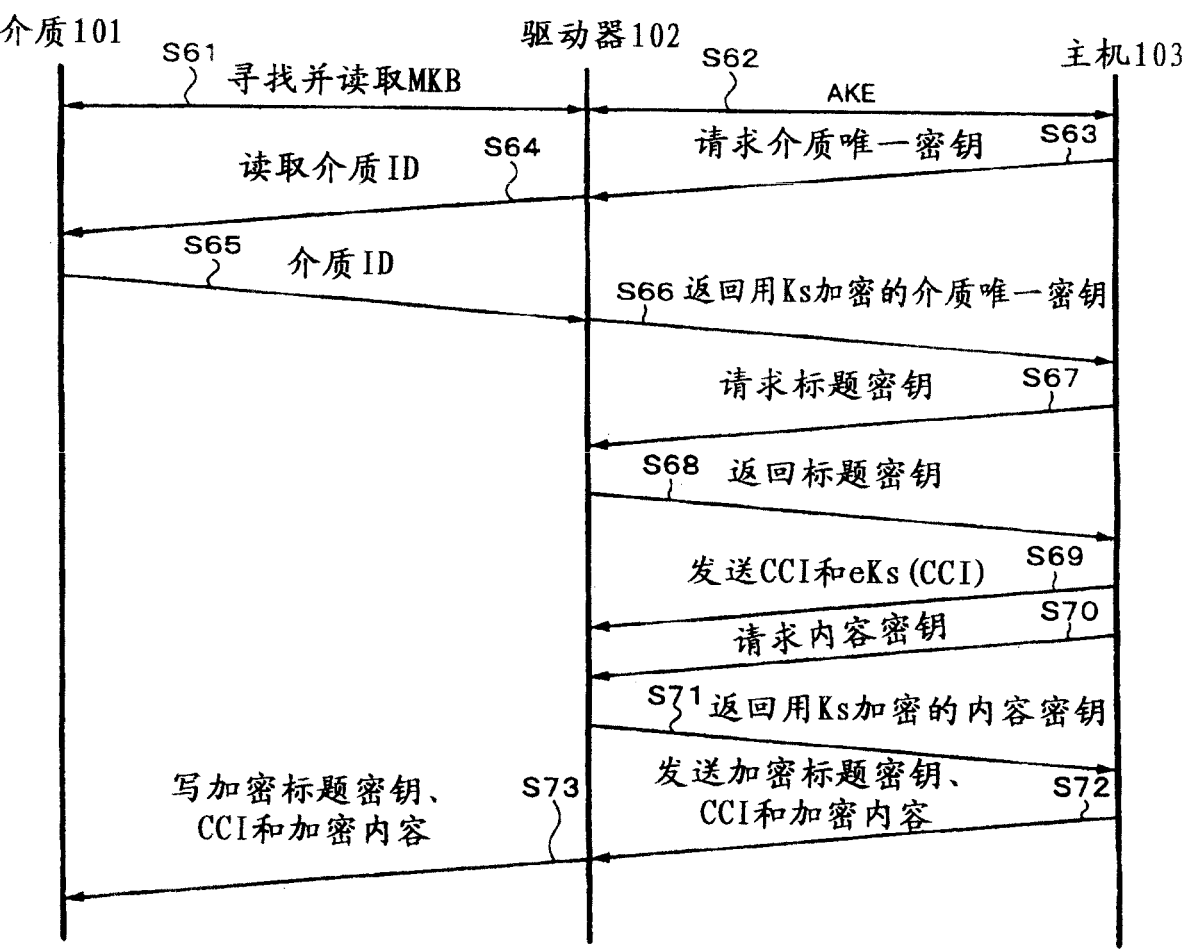


图1

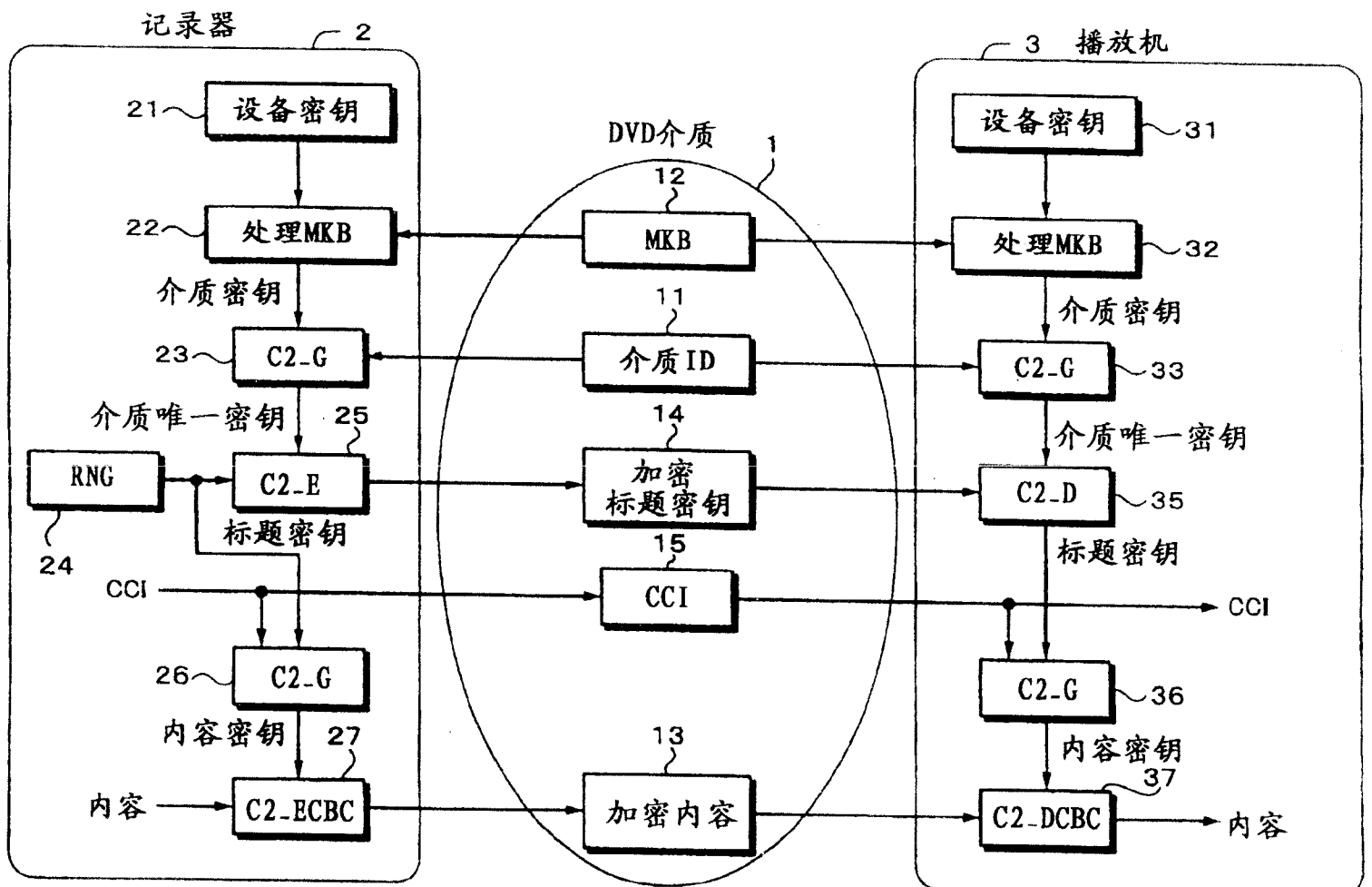


图2

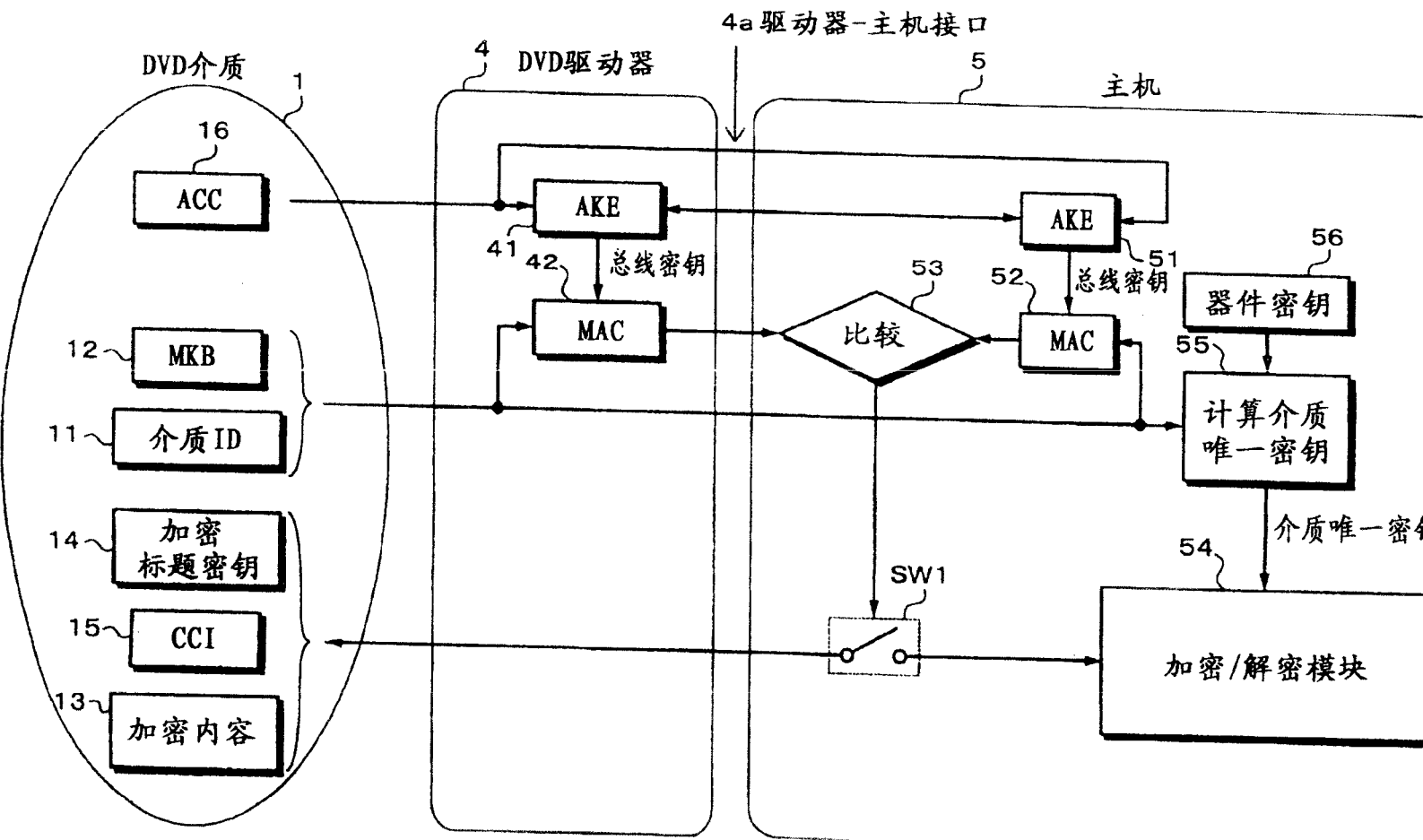


图 3

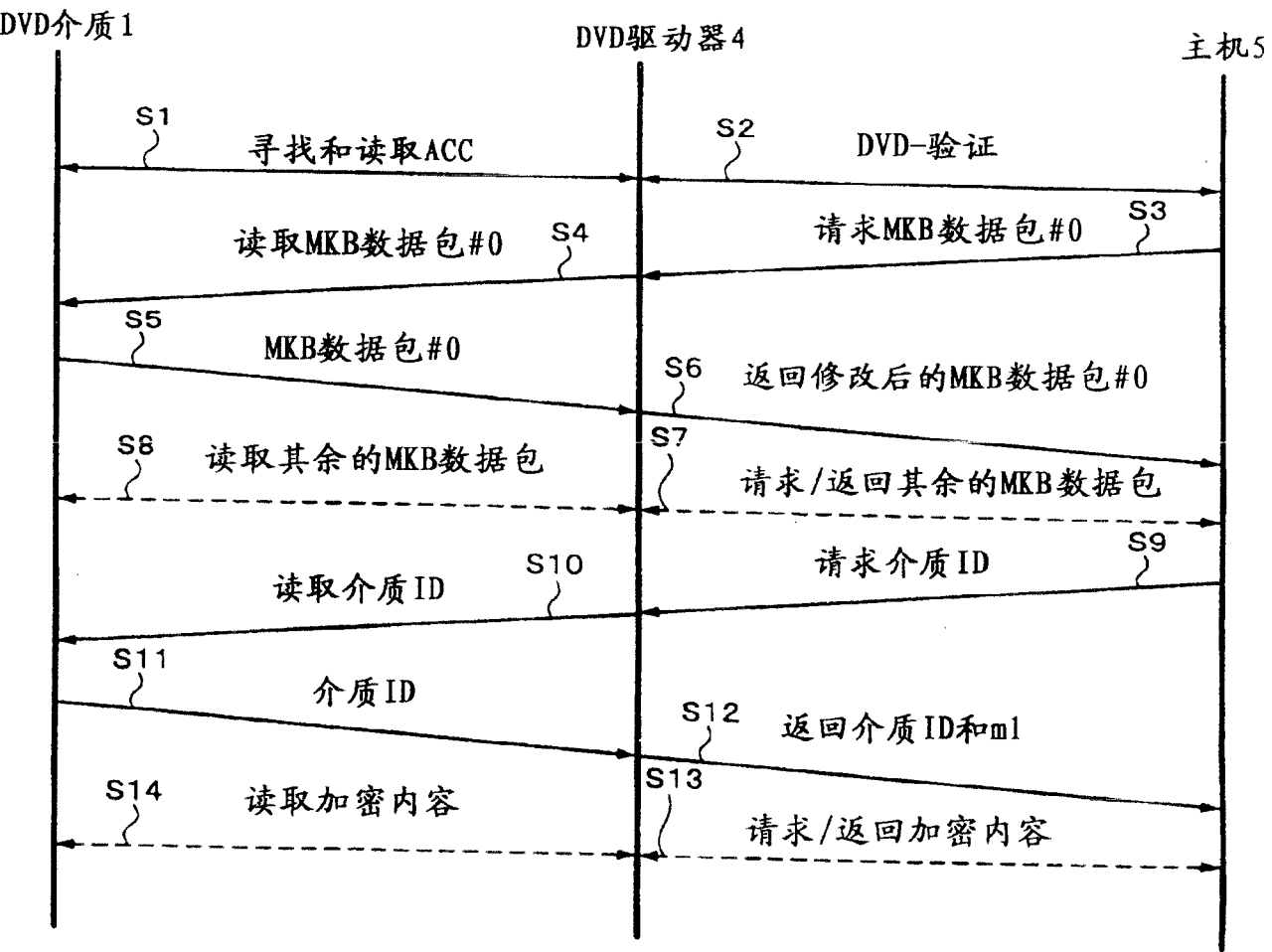


图 4

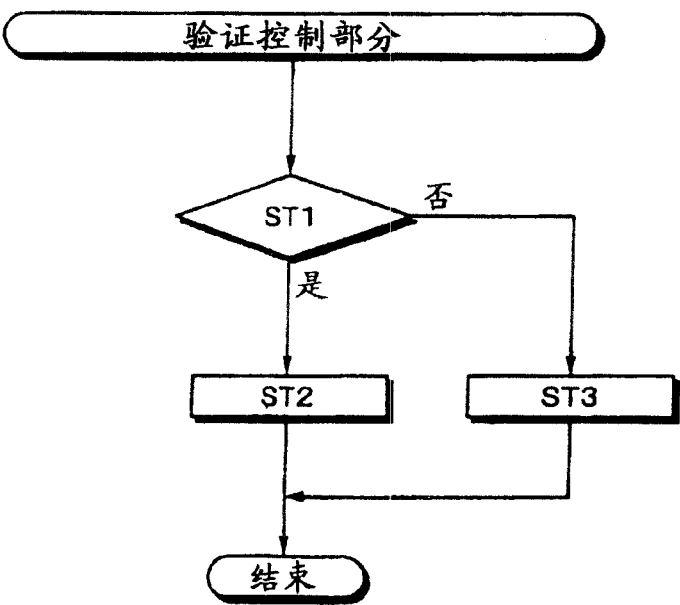


图5

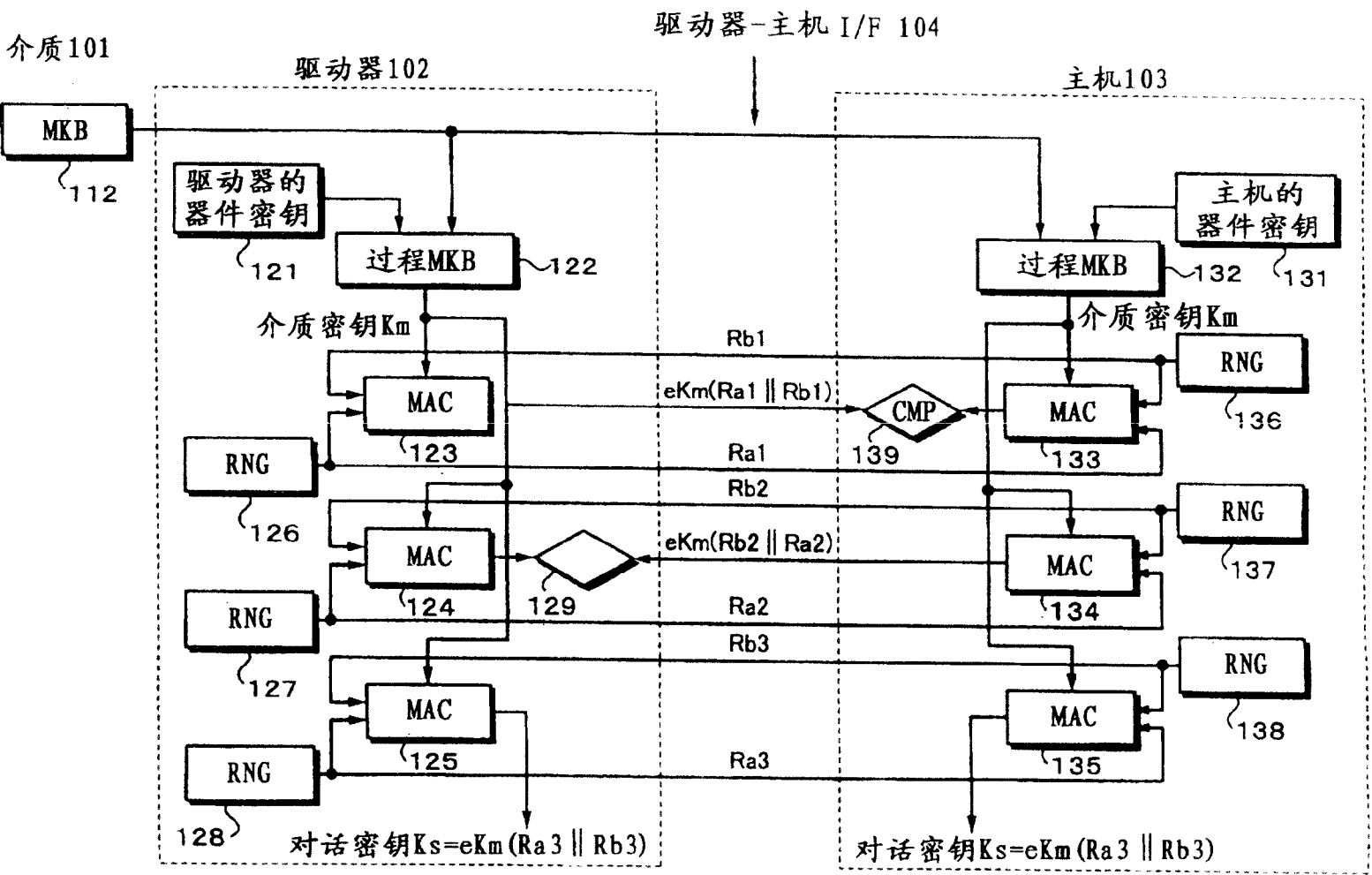


图6
驱动器102

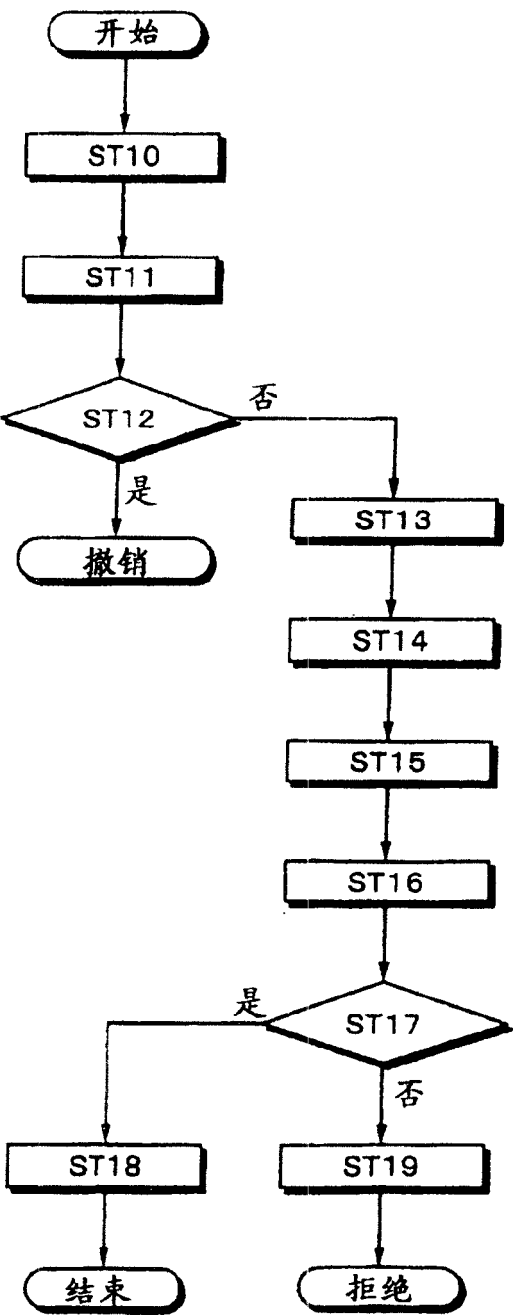


图7

主机103

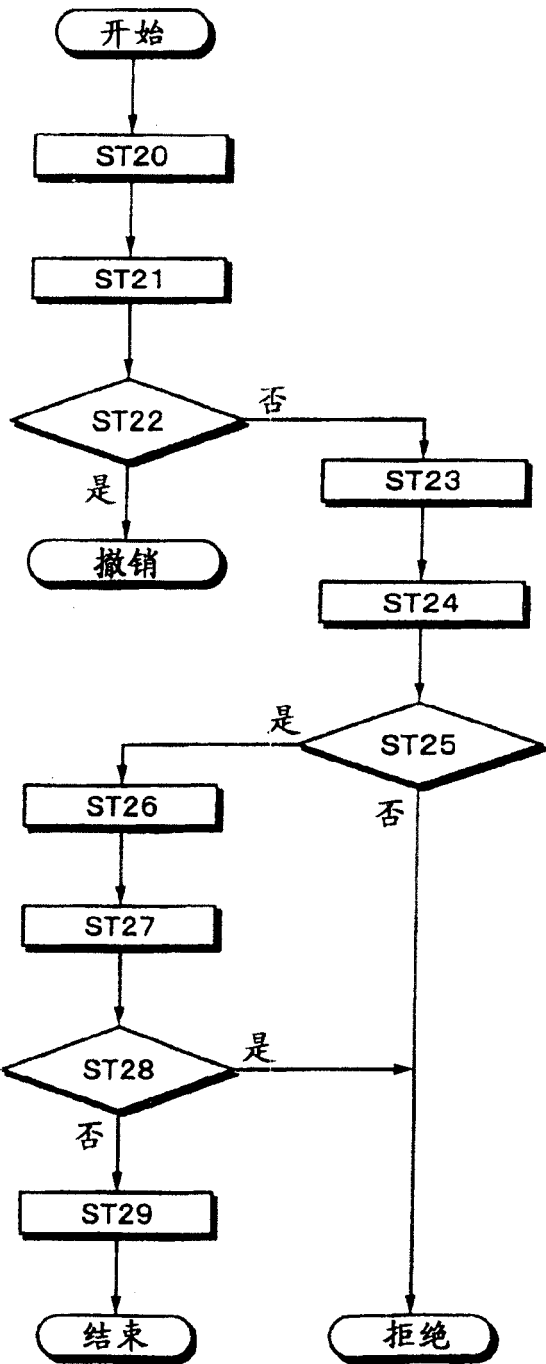


图 8

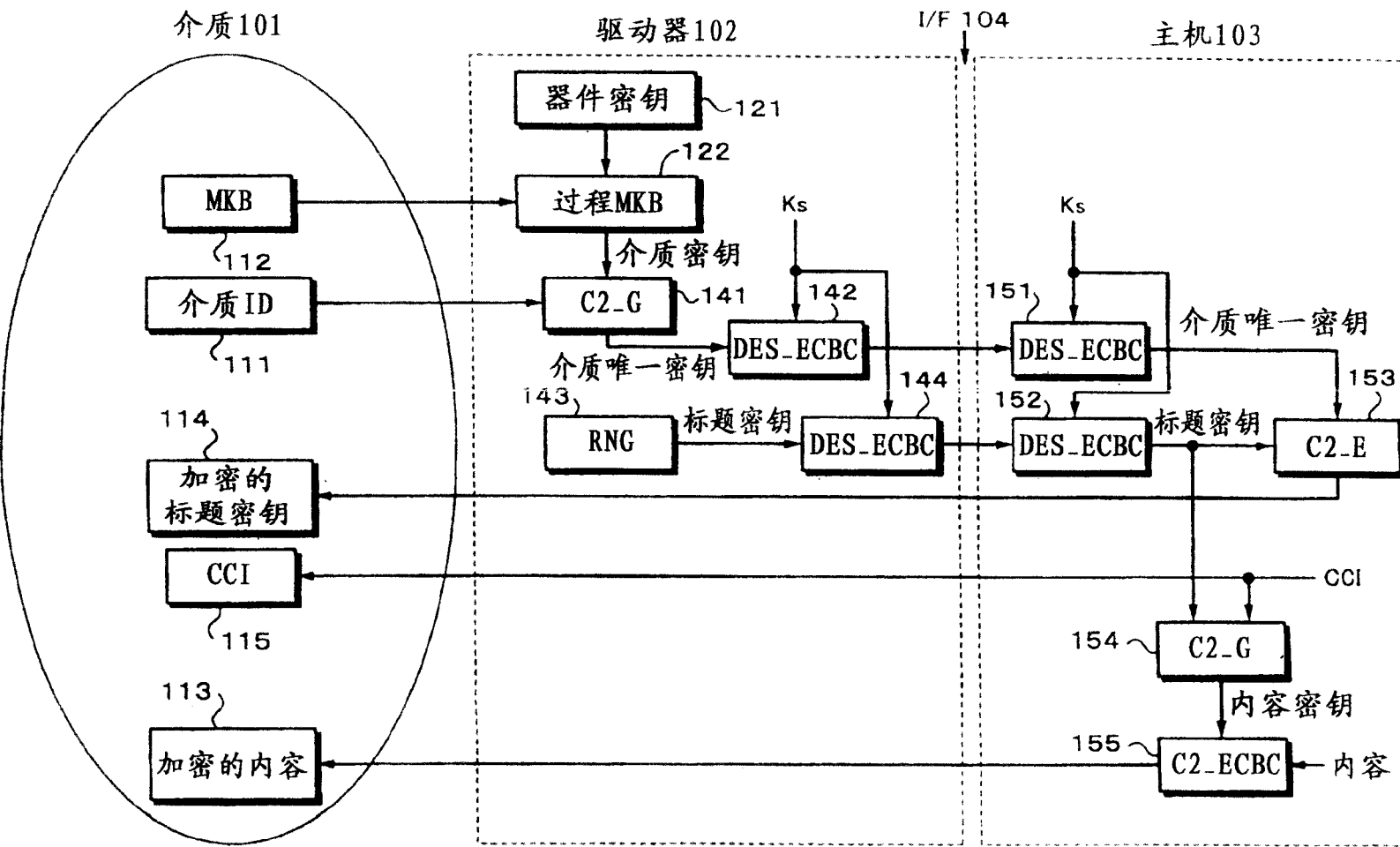


图 10

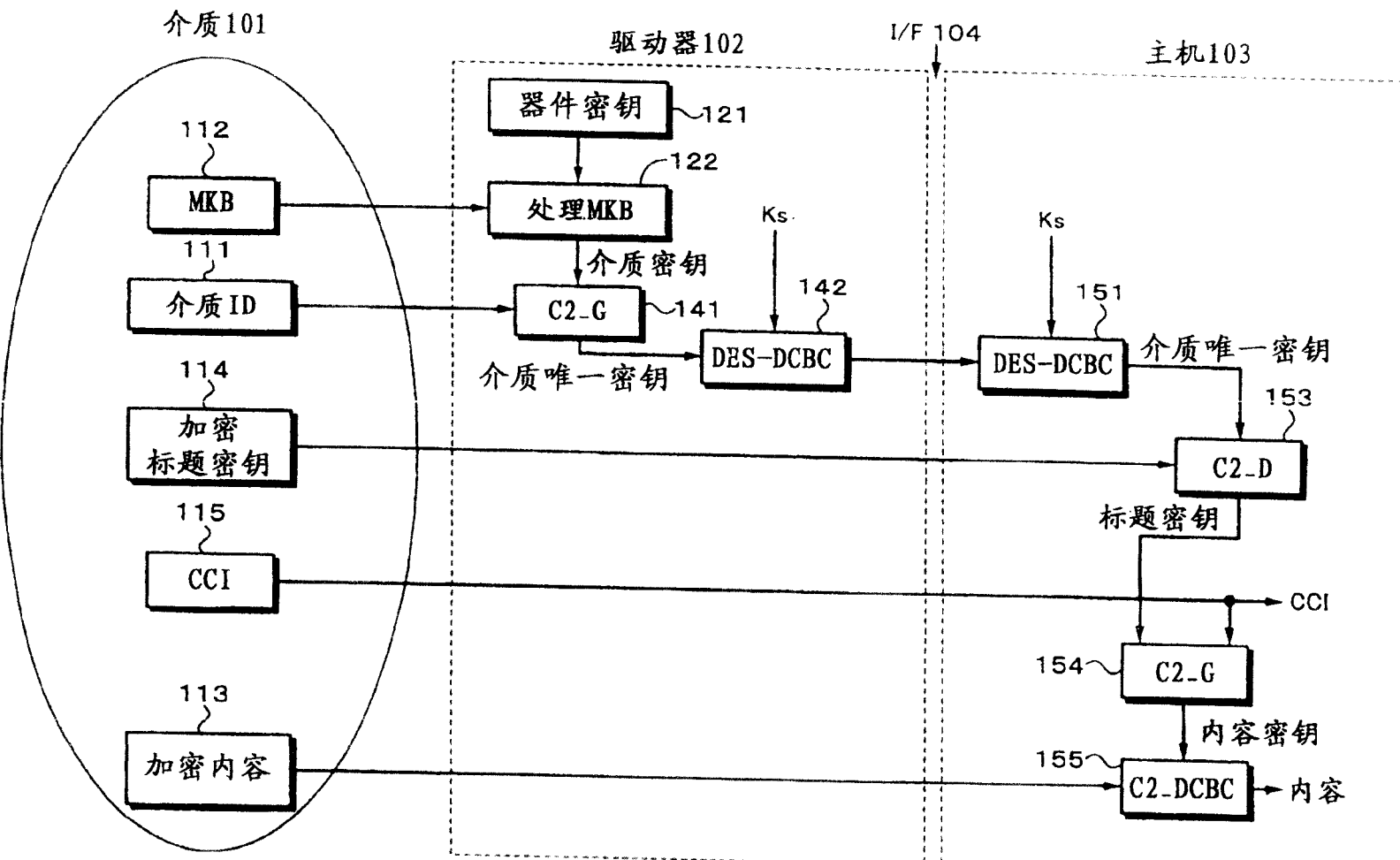


图 11

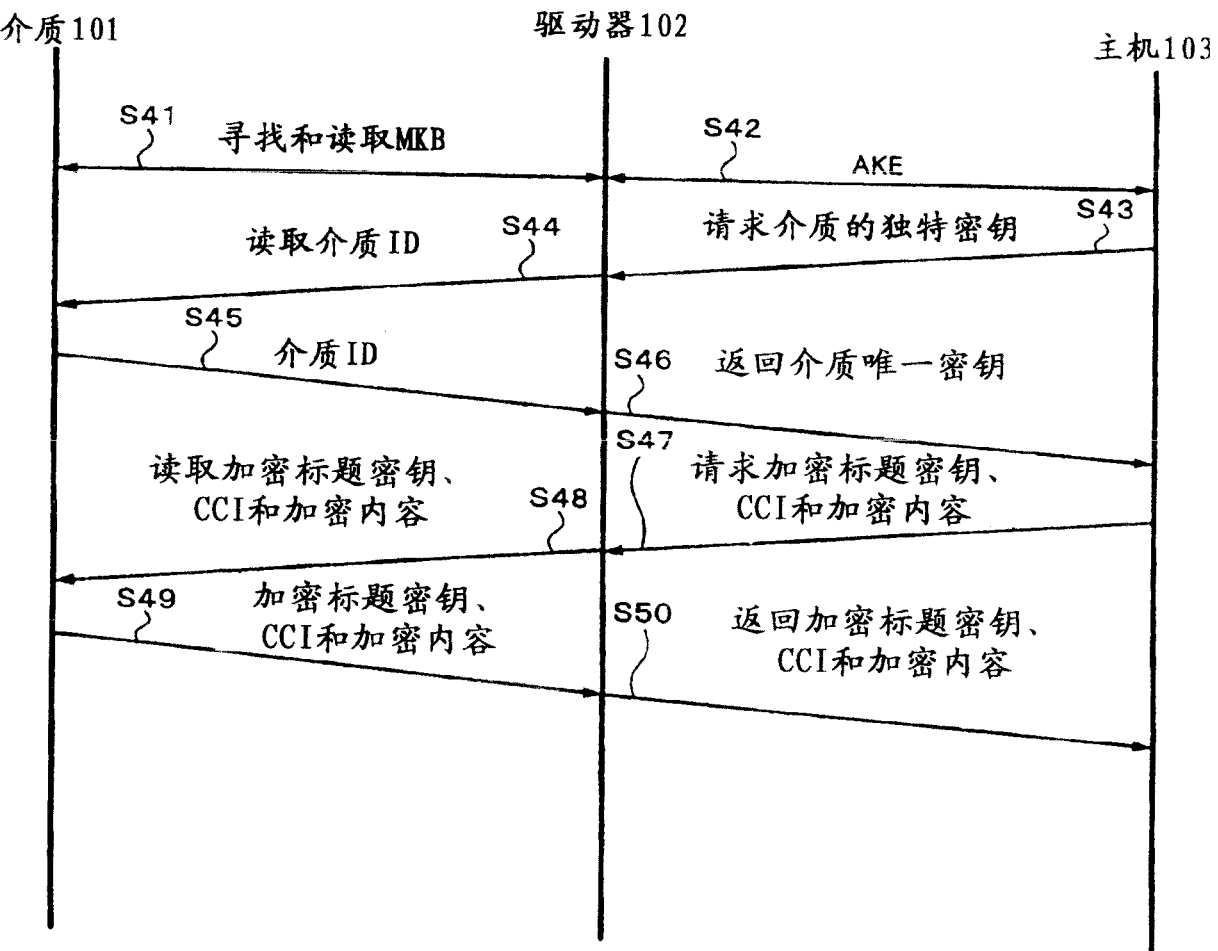


图 12

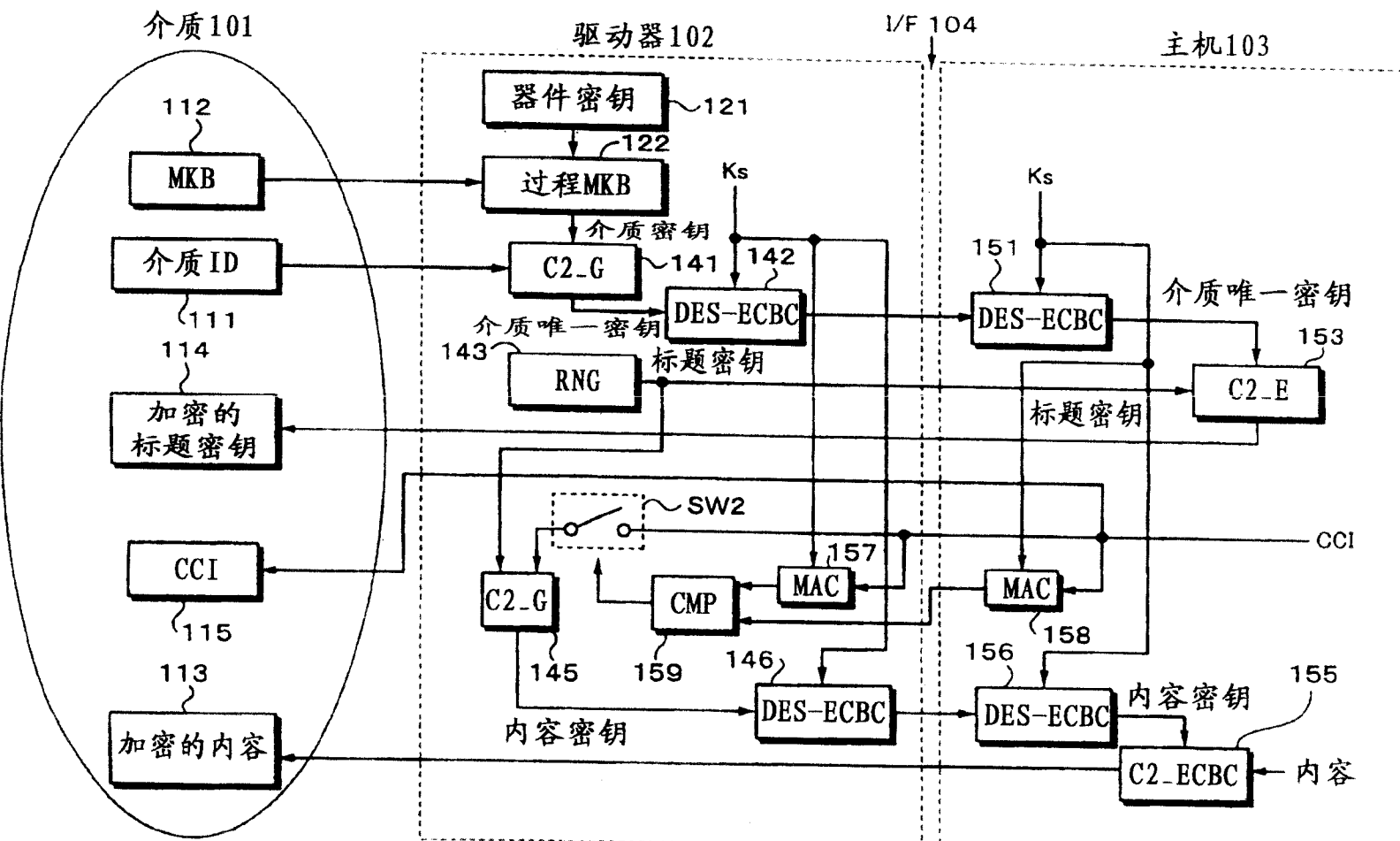
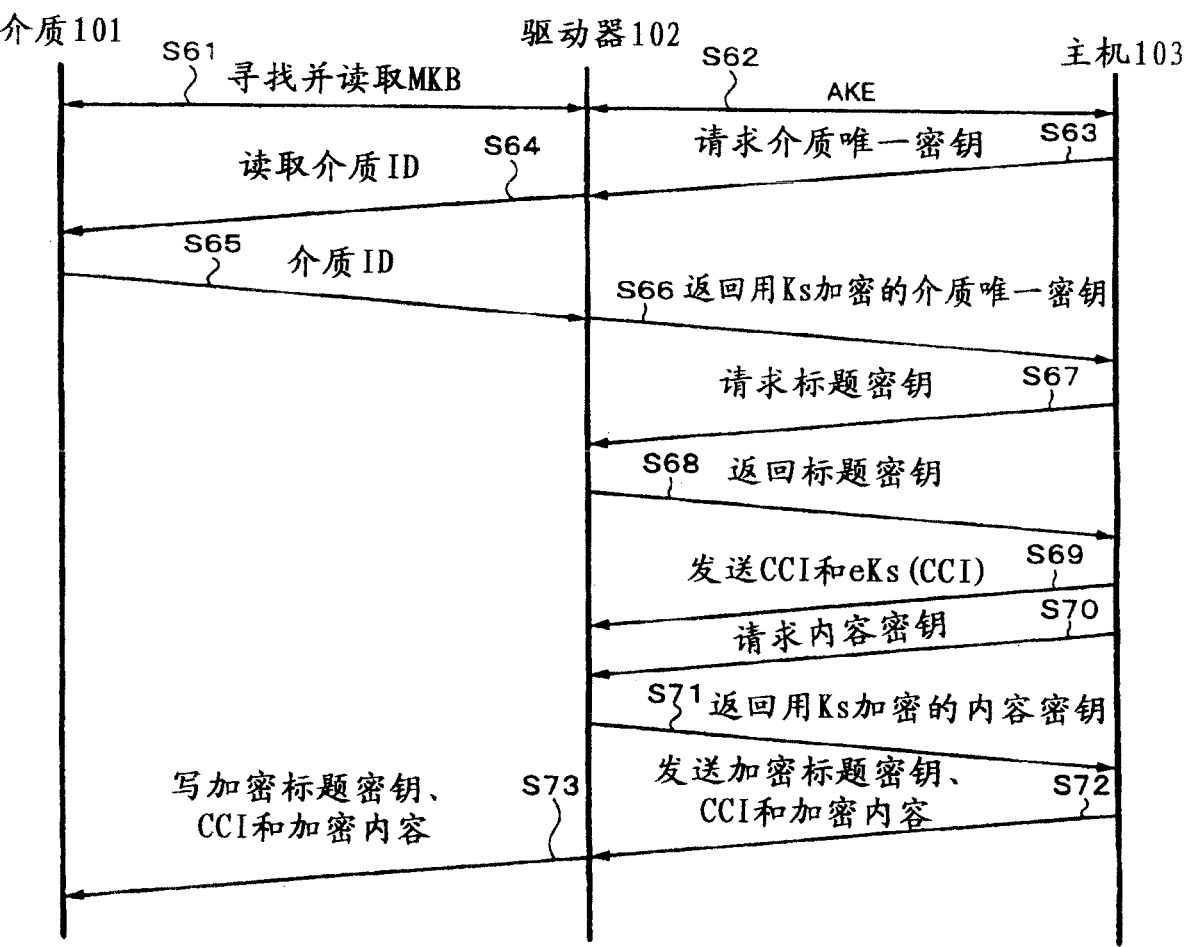


图 13



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)

