



(12) 发明专利

(10) 授权公告号 CN 101853352 B

(45) 授权公告日 2013.01.30

(21) 申请号 201010116310.1

US 2001056539 A1, 2001.12.27, 全文.

(22) 申请日 2004.08.26

审查员 刘彤

(30) 优先权数据

2003-301554 2003.08.26 JP

(62) 分案原申请数据

200480030743.8 2004.08.26

(73) 专利权人 松下电器产业株式会社

地址 日本大阪府

(72) 发明人 松岛秀树 广田照人 庄田幸惠

原田俊治

(74) 专利代理机构 永新专利商标代理有限公司

72002

代理人 刘炳胜

(51) Int. Cl.

G06F 21/14 (2013.01)

(56) 对比文件

US 2002144138 A1, 2002.10.03, 全文.

US 5991399 A, 1999.11.23, 全文.

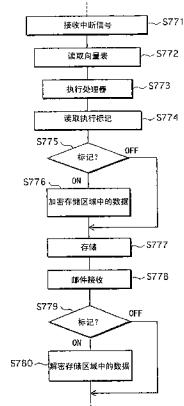
权利要求书 4 页 说明书 16 页 附图 18 页

(54) 发明名称

程序执行设备

(57) 摘要

提出了一种程序执行设备，该程序执行设备能够防止程序被未授权地分析或更改。该程序执行设备包括执行单元、第一保护单元和第二保护单元。执行单元执行第一程序和第二程序，并且与能够控制执行的外部设备相连接。当执行单元执行第一程序时，第一保护单元将执行单元从外部设备断开。当执行单元执行第二程序时，第二保护单元保护第一程序。



1. 一种程序执行设备,其执行 (i) 在第一安全级中运行的、确定另一程序是否被篡改的第一安全程序和 (ii) 在低于所述第一安全级的第二安全级中运行的、与所述第一安全程序不同的第二安全程序,所述程序执行设备包括:

执行单元,用于在指示所述第一安全级中的操作状态的第一模式下执行所述第一安全程序,和在指示所述第二安全级中的操作状态的第二模式下执行所述第二安全程序,同时在所述第一模式和所述第二模式之间进行切换;以及

外部设备断开单元,用于根据来自所述第一安全程序的指令,将所述执行单元与外部设备断开,其中

所述第一安全程序和所述第二安全程序彼此互相关联,用作单个应用程序,

所述第一安全程序命令所述外部设备断开单元将所述执行单元与所述外部设备断开,并且在所述执行单元被与所述外部设备断开之后,确定所述第二安全程序是否被篡改,以及

只有当作为所述确定的结果,所述第一安全程序确认所述第二安全程序没有被篡改时,执行所述第二安全程序的一部分。

2. 如权利要求 1 所述的程序执行设备,其中

所述第一安全程序持有所述第二安全程序所使用的秘密信息,以及

所述执行单元根据所述第一安全程序执行与所述第二安全程序的相互认证,与所述第二安全程序建立公共的会话密钥,使用所述会话密钥来加密所述秘密信息,并将加密后的秘密信息传递给所述第二安全程序。

3. 如权利要求 2 所述的程序执行设备,其中

所述第一安全程序所持有的所述秘密信息是从外部存储介质的安全区域获得的密钥信息。

4. 如权利要求 2 所述的程序执行设备,其中

所述执行单元根据所述第一安全程序,使用密钥对所述第二安全程序的至少一部分执行散列运算以计算第一篡改检测值,将所述第一篡改检测值与已经在生成所述第二安全程序时基于所述第二安全程序的所述至少一部分而计算出的第二篡改检测值进行比较,并且如果所述第一篡改检测值与所述第二篡改检测值不同,则终止操作,而如果所述第一篡改检测值与所述第二篡改检测值相同,则继续操作。

5. 如权利要求 4 所述的程序执行设备,其中

所述第二安全程序包括用于调用所述第一安全程序的调用指令,并且

所述执行单元根据所述调用指令将所述第二篡改检测值、所述第二安全程序的所述至少一部分的开始地址以及所述第二安全程序的所述至少一部分的大小传递给所述第一安全程序。

6. 如权利要求 5 所述的程序执行设备,其中

所述执行单元,

(a) 根据所述调用指令,将加密后的程序密钥传递给所述第一安全程序,

(b) 根据所述第一安全程序,如果所述第一篡改检测值与所述第二篡改检测值相同,则使用包含在所述第一安全程序中的主密钥来解密从所述第二安全程序接收的所述加密后的程序密钥,并将解密后的程序密钥传递给所述第二安全程序,以及

(c) 根据所述第二安全程序, 使用从所述第一安全程序接收的所述解密后的程序密钥来解密所述第二安全程序的经加密的部分, 然后删除所述解密后的程序密钥, 并且所述程序执行设备还包括:

保护单元, 用于在所述执行单元执行所述调用指令之前禁止由所述执行单元执行中断处理, 以及在所述执行单元删除所述解密后的程序密钥之后允许由所述执行单元执行所述中断处理。

7. 如权利要求 6 所述的程序执行设备, 进一步包括:

中断检测单元, 用于检测中断, 其中

所述保护单元包括存储区域, 当所述执行单元根据所述第二安全程序进行操作时将数据写入所述存储区域, 以及

当所述中断检测单元在所述执行单元根据所述第二安全程序进行操作时检测到中断时, 所述保护单元加密写入所述存储区域中的所述数据, 并且, 在所述执行单元完成处理所述中断之后, 在所述执行单元重新开始根据所述第二安全程序进行操作之前, 解密所述存储区域中的加密后的数据。

8. 如权利要求 1 所述的程序执行设备, 其中

所述第一安全程序将所述第二安全程序的执行所必须的执行信息传递给所述第二安全程序。

9. 如权利要求 8 所述的程序执行设备, 其中

所述第二安全程序的至少一部分被加密,

所述第一安全程序所持有的所述执行信息是用于对所述第二安全程序的经加密的部分进行解密的程序密钥, 以及

所述执行单元根据所述第一安全程序将所述程序密钥传递给所述第二安全程序, 根据所述第二安全程序使用从所述第一安全程序获得的所述程序密钥来解密并执行所述第二安全程序的所述经加密的部分。

10. 一种用于程序执行设备的程序执行方法, 所述程序执行设备执行在第一安全级中运行的、确定另一程序是否被篡改的第一安全程序和在低于所述第一安全级的第二安全级中运行的第二安全程序, 其中,

所述程序执行设备包括:

执行单元, 用于在指示所述第一安全级中的操作状态的第一模式下执行所述第一安全程序, 和在指示所述第二安全级中的操作状态的第二模式下执行所述第二安全程序, 同时在所述第一模式和所述第二模式之间进行切换; 以及

外部设备断开单元, 用于根据来自所述第一安全程序的指令, 将所述执行单元与外部设备断开,

一安全程序包括在所述第一安全级中运行的、确定另一程序是否被篡改的所述第一安全程序和在低于所述第一安全级的所述第二安全级中运行的所述第二安全程序,

所述第一安全程序和所述第二安全程序彼此互相关联, 用作单个应用程序,

所述程序执行方法包括如下步骤:

由所述第一安全程序命令所述外部设备断开单元将所述执行单元与所述外部设备断开;

在所述执行单元被与所述外部设备断开之后,由所述第一安全程序确定所述第二安全程序是否被篡改;以及

只有当作为所述确定的结果,所述第一安全程序确认所述第二安全程序没有被篡改时,执行所述第二安全程序的一部分。

11. 一种在多种操作模式其中之下运行的信息处理设备,包括:

存储单元,用于存储包括用于检测篡改的一个或多个程序指令的第一组程序指令,以及第二组程序指令;

控制单元,用于(i)通过使用受保护的存储器执行所述第一组程序指令中的一个或多个程序指令,判断所述第二组程序指令的至少一部分是否被篡改,所述受保护的存储器被保护成外部设备不能访问所述存储器的内容,以及(ii)在判断为否的情况下执行所述第二组程序指令中的一个或多个程序指令;

接口,用于将所述控制单元连接到所述外部设备;

断开单元,用于将所述控制单元与所述接口断开;以及

连接单元,用于将所述控制单元连接到所述接口,其中

所述第一组程序指令包括通过使所述断开单元将所述控制单元与所述接口断开而将所述控制单元与所述外部设备断开的一个或多个程序指令,以及通过使所述连接单元将所述控制单元连接到所述接口而将所述控制单元连接到所述外部设备的一个或多个程序指令,

所述控制单元还(i)当所述第一组程序指令中的一个或多个程序指令被执行时,将所述信息处理设备的操作模式改变成第一模式,在所述第一模式下通过使所述断开单元将所述控制单元与所述接口断开,所述存储器中的内容受到保护而不能被所述外部设备访问,以及(ii)当所述第二组程序指令中的一个或多个程序指令被执行时,将所述信息处理设备的操作模式改变成第二模式,在所述第二模式下通过使所述连接单元将所述控制单元连接到所述接口,所述存储器中的内容不受保护而能被所述外部设备访问。

12. 如权利要求11的信息处理设备,进一步包括:

密钥存储单元,用于存储(i)仅通过执行所述第一组程序指令中的一个或多个程序指令而允许访问的第一密钥;以及(ii)已使用所述第一密钥加密的第二密钥。

13. 如权利要求12的信息处理设备,其中

所述第一密钥对所述信息处理设备是唯一的。

14. 如权利要求11的信息处理设备,其中

由所述控制单元执行的所述第一组程序指令中的所述一个或多个程序指令通过如下方式来判断所述第二组程序指令的所述至少一部分是否被篡改:(i)计算所述第二组程序指令的所述至少一部分的散列值,以及(ii)将所计算的散列值与篡改检测值进行比较,其中所述篡改检测值是针对所述第二组程序指令的所述至少一部分而预先计算的散列值。

15. 如权利要求11的信息处理设备,其中

所述第一组程序指令包括用于管理对加密后的数字内容进行解密所使用的密钥的一个或多个其它程序指令。

16. 如权利要求11的信息处理设备,其中

所述第二组程序指令包括利用解密密钥对加密后的数字内容进行解密的一个或多个

其它程序指令。

17. 一种用于在多种操作模式其中之一下运行的信息处理设备的安全处理方法，

所述信息处理设备存储包括用于检测篡改的一个或多个程序指令的第一组程序指令，以及第二组程序指令，并且包括：

控制单元，用于执行所述第一组程序指令中的一个或多个程序指令和所述第二组程序指令中的一个或多个程序指令；以及

接口，用于将所述控制单元连接到外部设备，

所述安全处理方法包括如下步骤：

执行将所述控制单元与所述接口断开的一个或多个程序指令；

执行将所述控制单元连接到所述接口的一个或多个程序指令；

通过使用受保护的存储器执行所述第一组程序指令中的一个或多个程序指令，判断所述第二组程序指令的至少一部分是否被篡改，所述受保护的存储器被保护成外部设备不能访问所述存储器的内容；以及

在判断为否的情况下执行所述第二组程序指令中的一个或多个程序指令，其中

(i) 当所述第一组程序指令中的一个或多个程序指令被执行时，所述信息处理设备的操作模式被改变成第一模式，在所述第一模式下通过执行所述的将所述控制单元与所述接口断开的一个或多个程序指令，所述存储器中的内容受到保护而不能被所述外部设备访问，以及 (ii) 当所述第二组程序指令中的一个或多个程序指令被执行时，所述信息处理设备的操作模式被改变成第二模式，在所述第二模式下通过执行所述的将所述控制单元连接到所述接口的一个或多个程序指令，所述存储器中的内容不受保护而能被所述外部设备访问。

程序执行设备

[0001] 本申请是 2004 年 8 月 26 日提交的申请号为 200480030743.8、名称为“程序执行设备”专利申请的分案申请。

技术领域

[0002] 本发明涉及防止程序被未授权更改和分析的技术。

背景技术

[0003] 近年来，个人电脑和因特网的广泛使用使得可以容易地复制或编辑例如软件这样的数字内容。因此，需要使用抗篡改技术来防止软件被未授权更改和分析。

[0004] 已对抗篡改技术进行了多年的研究。例如，日经电子 (Nikkei Electronics) 1998 年 1 月 5 日的 209 页至 220 页的文章“Protecting Software against Inverse Analysis and Falsification”描述了防止未授权的软件分析的基本原理和具体方法。而且，富士施乐 (Fuji Xerox) 技术报告 13 号的 20 至 28 页中的文章“Software Tamper-resistant Techniques”涉及关于防止未授权的软件分析的技术问题和方法。

[0005] 尽管已有这些研究，但是仍需要更多各种用于保护程序对抗恶意用户的技术。

发明内容

[0006] 鉴于存在以上问题，本发明的目的是提供一种程序执行设备，该设备能够通过防止未授权的更改和分析来安全地执行程序。

[0007] 可以通过执行第一安全程序和第二安全程序的程序执行设备来实现上述目的，所述第一安全程序在第一安全级中运行，所述第二安全程序在低于所述第一安全级的第二安全级中运行，所述程序执行设备包括：执行单元，用于通过在第一模式和第二模式之间进行切换来进行操作，所述第一模式在所述第一安全级中，所述第二模式在所述第二安全级中；外部设备断开单元，用于根据所述第一安全程序的指令，将所述执行单元从外部设备断开；以及保护单元，用于保护所述第二安全程序。

[0008] 根据这种结构，可以保护程序免受使用硬件的外部攻击和使用软件的攻击。而且，通过断开外部设备可以获得高级别的安全性。

[0009] 这里，程序执行设备还包括中断检测单元，用于检测中断，其中，所述保护单元包括存储区域，当所述执行单元根据所述第二安全程序进行操作时，所述执行单元将数据写入所述存储区域，以及如果所述中断检测单元在所述执行单元根据所述第二安全程序进行操作时检测到中断，则所述保护单元加密写入所述存储区域中的所述数据，并且，在所述执行单元完成处理所述中断后，在所述执行单元重新开始根据所述第二安全程序进行操作之前，解密所述存储区域中的所述加密的数据。

[0010] 根据这种结构，在控制从第二安全程序转移到另一个程序之前，加密存储区域中的数据。因此，由于能够防止使用软件对第二安全程序进行未授权的分析，所以能够保护第二安全程序使用的数据免受其它程序的分析和影响。而且，通过仅加密存储区域中的数据

可以减少存储器的使用。这使得例如移动电话或 PDA 这样的、CPU 处理速度和存储容量等资源有限的设备能够保持较高的安全性。

[0011] 这里，第二安全程序可以包含用于调用所述第一安全程序的调用指令，其中，所述执行单元根据所述调用指令将所述第二篡改检测值、所述至少一部分所述第二安全程序的开始地址以及所述至少一部分所述第二安全程序的大小传递给所述第一安全程序。

[0012] 这里，在所述执行单元执行所述调用指令之前，所述保护单元可以禁止由所述执行单元执行中断处理，其中所述执行单元，(a) 根据所述调用指令，将加密的程序密钥传递给所述第一安全程序，(b) 如果所述第一篡改检测值与所述第二篡改检测值相同，则根据所述第一安全程序，使用包含在所述第一安全程序中的主密钥解密从所述第二安全程序接收的所述加密的程序密钥，并将所述解密过的程序密钥传递给所述第二安全程序，以及 (c) 根据所述第二安全程序，使用从所述第一安全程序接收的所述解密过的程序密钥来解密所述第二安全程序的加密的部分，然后删除所述解密过的程序密钥，以及在所述执行单元删除所述解密过的程序密钥后，所述保护单元允许由所述执行单元执行所述中断处理。

[0013] 根据这些结构，在删除用于解密加密的程序的程序密钥之前不接受任何中断。因此，由于能够防止第二安全程序的未授权的分析，所以可以防止程序密钥遭受通过中断而执行的未授权的分析。

[0014] 这里，所述执行单元根据所述第一安全程序，可以使用密钥对至少一部分所述第二安全程序执行散列运算，以计算第一篡改检测值；所述执行单元将所述第一篡改检测值与第二篡改检测值进行比较，其中，已经在生成所述第二安全程序时基于所述至少一部分所述第二安全程序计算出所述第二篡改检测值；以及如果所述第一篡改检测值与所述第二篡改检测值不同，则所述执行单元终止所述操作，如果所述第一篡改检测值与所述第二篡改检测值相同，则所述执行单元继续所述操作。

[0015] 根据这种结构，如果所述第二安全程序被判断为已被篡改，则所述执行单元终止所述操作。这减小了当第二安全程序已被篡改时的危害。

[0016] 而且，所述第二安全程序包含基于至少一部分第二安全程序生成的篡改检测值。因此，当所述第二安全程序需要被改变时，例如当第二安全程序已被篡改时，可以只对第二安全程序进行改变，而不改变程序执行设备的其它处理模块。

[0017] 根据本发明的另一方面，提供一种程序执行设备，其执行 (i) 判断另一程序是否被篡改的第一程序和 (ii) 与所述第一程序不同的第二程序，所述程序执行设备包括：

[0018] 执行单元，用于执行所述第一程序和第二程序；以及

[0019] 断开单元，用于当所述第一程序判断所述第二程序已经被篡改时将所述执行单元从外部设备断开，其中在所述执行单元被所述断开单元从所述外部设备断开后，所述第一程序对所述第二程序执行篡改检测处理，以及当作为篡改检测处理的结果没有检测到篡改时执行所述第二程序的一部分。

[0020] 根据本发明的另一方面，提供一种用于程序执行设备的程序执行方法，所述程序执行设备执行 (i) 判断另一程序是否被篡改的第一程序和 (ii) 与所述第一程序不同的第二程序，所述程序执行设备包括用于执行所述第一程序和第二程序的执行单元；所述程序执行方法包括：

[0021] 在所述执行单元执行所述第一程序时，保护用于运行所述第一程序的存储器免于

从外部看到：

- [0022] 当所述第一程序判断所述第二程序已经被篡改时从外部设备断开所述执行单元；
- [0023] 在所述执行单元通过所述断开从所述外部设备断开后执行对所述第二程序的篡改检测处理；以及
- [0024] 仅当作为篡改检测处理的结果没有检测到篡改时，执行所述第二程序的一部分。
- [0025] 根据本发明的另一方面，提供一种信息处理设备，包括：
- [0026] 存储单元，存储包括用于检测篡改的一个或多个程序指令的第一组程序指令，以及第二组程序指令；以及
- [0027] 控制单元，用于(i)通过使用受保护的存储器执行所述第一组程序指令中的一个或多个程序指令，判断所述第二组程序指令的至少一部分是否被篡改，所述受保护的存储器被保护成外部设备不能看到所述存储器的内容，以及(ii)在判断为否的情况下执行所述第二组程序指令中的一个或多个程序指令。
- [0028] 根据本发明的另一方面，提供一种用于信息处理设备的方法，所述信息处理设备存储包括用于检测篡改的一个或多个程序指令的第一组程序指令以及第二组程序指令；以及
- [0029] 所述方法包括如下步骤：
- [0030] 通过使用受保护的存储器执行所述第一组程序指令中的一个或多个程序指令，判断所述第二组程序指令的至少一部分是否被篡改，所述受保护的存储器被保护成外部设备不能看到所述存储器的内容；以及
- [0031] 在判断为否的情况下执行所述第二组程序指令中的一个或多个程序指令。

附图说明

- [0032] 图1显示了本发明的实施例所涉及的安全处理系统的整体结构；
- [0033] 图2是显示图1所示的认证机构设备的结构的框图；
- [0034] 图3是显示图2所示的编译器的操作的流程图；
- [0035] 图4是显示图1所示的存储卡的结构的框图；
- [0036] 图5是显示图1所示的便携终端的结构的框图；
- [0037] 图6显示存储在图5所示的存储器中的程序；
- [0038] 图7显示图6所示的第二安全处理程序的数据结构；
- [0039] 图8显示图7所示的调用程序的数据结构；
- [0040] 图9是显示图7所示的中断处理程序的执行过程的流程图；
- [0041] 图10显示图6所示的第一安全处理程序的数据结构；
- [0042] 图11显示图6所示的向量表的数据结构；
- [0043] 图12是显示图5所示的CPU的操作的流程图；
- [0044] 图13是显示音乐数据播放过程的流程图；
- [0045] 图14是显示音乐数据播放过程的流程图；
- [0046] 图15是显示音乐数据播放过程的流程图；
- [0047] 图16是显示音乐数据播放过程的流程图；

- [0048] 图 17 是显示音乐数据播放过程的流程图；
- [0049] 图 18 是显示认证过程的流程图；
- [0050] 图 19 是显示当中断出现时 CPU 的操作的流程图。

具体实施方式

- [0051] 下面参照附图详细描述本发明的实施例。
- [0052] 1. 安全处理系统 1 的结构
- [0053] 图 1 显示了本发明的实施例所涉及的安全处理系统的整体结构。在图中，总体上，安全处理系统 1 由认证机构 (certificate authority) 设备 100、ROM 写入器 200、便携式终端 300 以及存储卡 400 构成。
- [0054] 安全处理系统 1 保护在便携式终端 300 中执行的程序免受未授权地分析和更改。将被保护的程序是在认证机构设备 100 中生成的，并由 ROM 写入器 200 将其写入 ROM。然后将包含程序的 ROM 安装在便携式终端 300 中。
- [0055] 在本实施例中，作为一个例子，将被保护的程序是用于解密记录在存储卡 400 上的加密的音乐数据的加密音乐数据解密程序。
- [0056] 1.1. 认证机构设备 100
- [0057] 认证机构设备 100 生成第二安全处理程序，该第二安全处理程序包含图 7 所示的区域分配程序 511、中断禁止程序 512、调用程序 513、密钥接收程序 514、执行标记 515、中断处理程序 518、解密程序 516 以及安全程序。安全程序包含需要被保护的加密音乐数据解密程序 524。通过 ROM 写入器 200 将生成的第二安全处理程序写入 ROM，并将其安装在便携式终端 300 中。后面详细描述每一个程序。
- [0058] 图 2 显示了认证机构设备 100 的结构。在图中，证书机构设备 100 包括编译器 101、程序加密单元 102、密钥加密单元 103、散列值计算单元 104、数据嵌入单元 105、存储单元 106、以及传输单元 107。
- [0059] 实际上由包括微处理器、ROM、RAM、硬盘单元、显示单元以及键盘的计算机系统来实现证书机构设备 100。通过执行存储在 RAM 或硬盘单元中的计算机程序的微处理器来实现认证机构设备 100 的功能。
- [0060] (1) 编译器 101
- [0061] 编译器 101 接收保护程序、调用程序 513、解密程序 516 以及安全程序的源代码的输入。保护程序由区域分配程序 511、中断禁止程序 512、密钥接收程序 514、执行标记 515 以及中断处理程序 518 构成。调用程序 513 用于发送检测第二安全处理程序是否已被篡改所需的数据。调用程序 513 包含便携式终端 300 的存储器上的 TRS 区域程序的开始地址。TRS 区域程序对应于第二安全处理程序的解密程序 516 和加密的程序 517。通过加密安全程序生成加密的程序 517。
- [0062] 当接收到调用程序 513、解密程序 516、安全程序以及保护程序的源代码后，编译器 101 编译这些程序中的每一个。
- [0063] 图 3 是显示由编译器 101 编译程序的操作的流程图。
- [0064] 编译器 101 执行词法分析 (S621) 和语法分析 (S622)。最后，编译器 101 生成表示可由计算机执行的程序的二进制数据 (S623)。

[0065] 编译器 101 将调用程序 513 的二进制数据和保护程序的二进制数据输出到数据嵌入单元 105。编译器 101 还将解密程序 516 的二进制数据和安全程序的二进制数据输出到程序加密单元 102。

[0066] (2) 程序加密单元 102

[0067] 程序加密单元 102 接收解密程序 516 的二进制数据和安全程序的二进制数据。程序加密单元 102 还接收程序密钥。程序加密单元 102 根据加密算法 E1 使用程序密钥加密安全程序, 以生成加密的程序 517。作为一个例子, 加密算法 E1 是 AES(Advanced Encryption Standard, 高级加密标准)。在所述领域, AES 是公知的, 因此在此省略对其的说明。除 AES 以外的其它算法也可以被用作加密算法 E1。

[0068] 程序加密单元 102 将解密程序 516 和加密的程序 517 作为 TRS 区域程序输出到数据嵌入单元 105。

[0069] 程序加密单元 102 还将 TRS 区域程序输出至散列值计算单元 104。

[0070] (3) 密钥加密单元 103

[0071] 密钥加密单元 103 接收程序密钥和主密钥。

[0072] 密钥加密单元 103 根据加密算法 E1 使用主密钥加密程序密钥, 以生成加密的密钥。密钥加密单元 103 将加密的密钥输出到数据嵌入单元 105。

[0073] (4) 散列值计算单元 104

[0074] 散列值计算单元 104 计算第二安全处理程序的至少一部分的散列值。

[0075] 在该实施例中, 散列值计算单元 104 接收 TRS 区域程序和密钥, 并根据散列函数使用密钥计算 TRS 区域程序的散列值。

[0076] 例如, 用于 HMAC(Keyed-Hashing for Message Authentication, 用于消息认证的密钥散列法) 的算法可以被用于计算散列值。

[0077] 设 H 为散列函数, K 为密钥, 文本为将被散列的数据, opad 是由重复 64 次的字节值 0x36 构成的字符串, 并且 ipad 是由重复 64 次的字节值 0x5C 构成的字符串。因此, 用于计算散列值的算法可以被表示为 $H(K \text{XOR} opad, H(K \text{XOR} ipad, text))$ 。

[0078] 散列值计算单元 104 还计算 TRS 区域程序的二进制大小 (binarysize)。

[0079] 散列值计算单元 104 将散列值和二进制大小输出到数据嵌入单元 105。

[0080] (5) 数据嵌入单元 105

[0081] 数据嵌入单元 105 从编译器 101 接收调用程序 513 的二进制数据和保护程序的二进制数据, 并从散列值计算单元 104 接收散列值和二进制大小。数据嵌入单元 105 还从密钥加密单元 103 接收加密的密钥, 并从程序加密单元 102 接收 TRS 区域程序。

[0082] 数据嵌入单元 105 将散列值作为篡改检测值嵌入调用程序 513。数据嵌入单元 105 还将二进制大小和加密的密钥嵌入调用程序 513。数据嵌入单元 105 将生成的调用程序 513 包含到保护程序中, 并将保护程序和 TRS 区域程序进行组合以形成第二安全处理程序。数据嵌入单元 105 将第二安全处理程序写入存储单元 106。

[0083] (6) 存储单元 106

[0084] 存储单元 106 存储由数据嵌入单元 105 写入的第二安全处理程序。

[0085] (7) 传输单元 107

[0086] 传输单元 107 将存储在存储单元 106 中的第二安全处理程序输出到 ROM 写入器

200。

[0087] 1.2. ROM 写入器 200

[0088] ROM 写入器 200 与认证机构设备 100 相连。ROM 写入器 200 从认证机构设备 100 接收第二安全处理程序，并将第二安全处理程序写入 ROM。然后，将由 ROM 写入器 200 写入第二安全处理程序的 ROM 安装在便携式终端 300 中。

[0089] 13. 存储卡 400

[0090] 图 4 显示了存储卡 400 的结构。在图中，存储卡 400 包括控制单元 401、输入 / 输出单元 402、认证 (authentication) 单元 403、信息存储单元 404。

[0091] (1) 输入 / 输出单元 402

[0092] 当存储卡 400 连接到便携式终端 300 上时，输入 / 输出单元 402 在控制单元 401 和便携式终端 300 之间执行数据的传输。

[0093] (2) 信息存储单元 404

[0094] 信息存储单元 404 包括数据区域 410 和安全区域 420。

[0095] 数据区域 410 存储加密的音乐数据 411。通过根据加密算法 E1 使用标题密钥 421 加密 MP3 音乐数据从而生成加密的音乐数据 411。

[0096] 安全区域 420 存储标题密钥 421。只有当与认证单元 403 相互认证成功后，便携式终端 300 才能访问安全区域 420。

[0097] 这里，可以使用只有存储卡 400 才具有的信息来加密存储在信息存储单元 404 中的数据。

[0098] (3) 认证单元 403

[0099] 认证单元 403 基于 CPRM (Content Protection for Recordable Media, 可记录介质内容保护) 与便携式终端 300 执行相互认证。如果相互认证成功，则认证单元 403 与便携式终端 300 建立共享密钥，并将该共享密钥输出到控制单元 401。在本领域中，CPRM 是公知的，因此，在此不再对其进行说明。除 CPRM 以外的其它方法也可以被用于相互认证。

[0100] (4) 控制单元 401

[0101] 控制单元 401 经由输入 / 输出单元 402 与便携式终端 300 执行数据的传输。只有当便携式设备 300 与认证单元 403 的相互认证成功时，控制单元 401 才允许便携式终端 300 访问存储在安全区域 420 中的数据。当输出存储在安全区域 420 中的数据时，控制单元 401 使用从认证单元 403 接收的共享密钥加密数据。

[0102] 同时，控制单元 401 允许便携式终端 300 访问存储在数据区域 410 中的数据，而无需相互认证。

[0103] 1.4. 便携式终端 300

[0104] 图 5 显示了便携式终端 300 的结构。在图中，便携式终端 300 包括 CPU 301、调试器接口 302、调试器禁止电路 303、中断控制器 304、存储器 305、存储卡接口 306、输入单元 307、显示单元 308、扬声器 309、解码器 310、麦克风 312、转换单元 313、无线电控制单元 314、无线电单元 315 以及天线 316。便携式终端 303 的这些部件与总线 317 相连。而且，通过中断线 318，中断控制器 304 被连接到 CPU 301。

[0105] 下面描述便携式终端 300 的这些部件中的每一个。

[0106] (1) 调试器禁止电路 303 和调试器接口 302

[0107] 在 CPU 301 和调试器接口 302 之间设置调试器禁止电路 303，从而将 CPU 301 与调试器接口 302 连接 / 断开。

[0108] 从 CPU 301 接收到指示“允许”的调试器控制信号后，调试器禁止电路 303 将 CPU 301 连接到调试器接口 302。从 CPU 301 接收到指示“禁止”的调试器控制信号后，调试器禁止电路 303 将 CPU 301 从调试器接口 302 断开。

[0109] 当 CPU 301 和调试器接口 302 彼此连接时，允许连接到调试器接口 302 的外部调试器设备工作。如果将 CPU 301 和调试器接口 302 彼此断开，则禁止调试器设备工作。例如，可以通过开关来实现调试器禁止电路 303。这里，可以通过开关电路在 CPU 301 和调试器接口 302 之间进行物理地连接 / 断开，或者进行电气的连接 / 断开。

[0110] 调试器接口 302 用于连接便携式终端 300 和调试器设备。

[0111] (2) 存储器 305

[0112] 如图 6 所示，存储器 305 存储第一安全处理程序 501、第二安全处理程序 502、向量表 503、音乐播放程序 504、应用程序 505。

[0113] (A) 第二安全处理程序 502

[0114] 通过认证机构设备 100 生成第二安全处理程序 502，并通过 ROM 写入器 200 将其存储在 ROM 中。

[0115] 图 7 显示了第二安全处理程序 502 的数据结构。下面说明构成第二安全处理程序 502 的每一个程序。

[0116] (区域分配程序 511)

[0117] 区域分配程序 511 在存储器 305 中分配存储空间，以便动态地分配当执行认证程序 523 和加密音乐数据解密程序 524 时使用的存储区域。

[0118] (中断禁止程序 512)

[0119] 中断禁止程序 512 禁止（即，屏蔽）中断。

[0120] (调用程序 513)

[0121] 调用程序 513 调用第一安全处理程序 501。

[0122] 如图 8 所示，调用程序 513 包括篡改检测数据，该篡改检测数据包括篡改检测值 541、TRS 区域开始地址 542、二进制大小 543、以及加密的密钥 544。当调用第一安全处理程序 501 时，调用程序 513 还将由认证机构设备 100 的数据嵌入单元 105 嵌入的篡改检测数据传递给第一安全处理程序 501。

[0123] 这里，篡改检测值 541 是由认证机构设备 100 的散列值计算单元 104 为第二安全处理程序 502 中的 TRS 区域程序计算的散列值。

[0124] TRS 区域开始地址 542 是存储器 305 中的接受散列值计算的 TRS 区域程序的开始地址。

[0125] 二进制大小 543 是 TRS 区域程序的二进制大小。

[0126] 加密的密钥 544 是由认证机构设备 100 的密钥加密单元 103 使用主密钥加密的程序密钥。

[0127] (密钥接收程序 514)

[0128] 密钥接收程序 514 从第一安全处理程序 501 接收程序密钥，并将该程序密钥传递给解密程序 516。

[0129] (执行标记 515)

[0130] 执行标记 515 显示是否正在执行安全程序。在解密程序 516 解密加密的程序 517 之前, 执行标记 515 被设置为“ON”, 其指示正在执行安全程序。当完成执行通过解密加密的程序 517 而获得的安全程序时, 执行标记 515 被设置为“OFF”。

[0131] (解密程序 516)

[0132] 解密程序 516 从密钥接收程序 514 接收程序密钥, 并根据解密算法 D1 使用程序密钥解密加密的程序 517, 以获得安全程序。这里, 解密算法 D1 是加密算法 E1 的逆。

[0133] 例如, 在国际专利申请公开 No. WO 04/013744(2004 年 2 月 12 日公开) 中公开的技术可以被用于解密加密的程序 517。根据该技术, 加密的程序 517 被加载到存储器并且被以小部分为单位进行解密。这可以防止全部安全程序都存在于存储器中。因此, 即使当未授权的用户访问存储器中的数据时, 也不能获得全部安全程序。

[0134] (加密的程序 517)

[0135] 通过加密安全程序生成加密的程序 517。如图 7 所示, 安全程序包括中断允许程序 521、区域初始化程序 522、认证程序 523、加密音乐数据解密程序 524、区域密钥 525、区域加密程序 526、区域解密程序 527、区域释放程序 528。在加密的程序 517 中, 中断允许程序 521、区域初始化程序 522、认证程序 523、区域密钥 525、区域加密程序 526、区域解密程序 527、区域释放程序 528 保护加密音乐数据解密程序 524 免受其它程序的分析或更改。

[0136] (a) 中断允许程序 521

[0137] 中断允许程序 521 释放通过中断禁止程序 512 产生的中断禁止。

[0138] (b) 区域初始化程序

[0139] 区域初始化程序 522 对由区域分配程序 511 分配的存储空间进行初始化, 以在存储空间中分配将接受加密的存储区域。

[0140] 分配存储区域以将认证程序 523 和加密音乐数据解密程序 524 执行期间使用的数据写入。

[0141] (c) 认证程序 523

[0142] 认证程序 523 包含认证密钥 531。

[0143] 认证程序 523 执行单向认证以判断第一安全处理程序 501 是否有效。

[0144] (d) 加密音乐数据解密程序 524

[0145] 加密音乐数据解密程序 524 根据解密算法 D1, 使用标题密钥 421 解密存储在存储卡 400 上的加密的音乐数据 411, 以获得音乐数据。

[0146] (e) 区域密钥 525

[0147] 由区域加密程序 526 使用区域密钥 525 以加密由区域初始化程序 522 分配的存储区域中的数据, 并由区域解密程序 527 使用以解密存储区域中的加密数据。

[0148] (f) 区域加密程序 526

[0149] 区域加密程序 526 根据加密算法 E2 使用区域密钥 525 来加密存储区域中的数据。这里, 加密算法 E2 使得能够进行比加密算法 E1 更快速的处理。作为一个例子, 加密算法 E2 是 XOR(异或) 运算。或者, 除 XOR 运算以外的其它算法也可以被用作加密算法 E2, 这是基于所需的安全级别和 CPU 301 的处理能力来确定的。

[0150] 在第二安全处理程序 502 调用第一安全安全处理程序 501 以将控制传递给第一安

全处理程序 501 之前,区域加密程序 526 加密存储区域中的数据。

[0151] (g) 区域解密程序 527

[0152] 当控制从第一安全处理程序 501 返回到第二安全处理程序 502 时,区域解密程序 527 根据解密算法 D2 使用区域密钥 525 来解密存储区域中的加密数据,以获得原始的明文数据。

[0153] (h) 区域释放程序 528

[0154] 区域释放程序 528 释放由区域初始化程序 522 分配的存储区域,并调用第一安全处理程序 501 的退出函数以结束音乐数据播放过程。

[0155] (中断处理程序 518)

[0156] 当在第二安全处理程序 502 执行期间出现中断时,执行中断处理程序 518。中断处理程序 518 包含加密 / 解密密钥 (未说明)。

[0157] 图 9 是显示中断处理程序 518 的执行过程的流程图。虽然中断处理程序 518 实际上是计算机程序,但是图 9 以便于说明的流程图说明了中断处理程序 518 的执行过程。

[0158] 中断处理程序 518 读取执行标记 515(S611),判断执行标记 515 是“ON”还是“OFF”(S612)。如果执行标记是“ON”(S612:ON),则中断处理程序 518 根据加密算法 E2 使用加密 / 解密密钥来加密存储区域中的数据(S613)。之后,中断处理程序 518 处理中断。如果执行标记是“OFF”(S612:OFF),则中断处理程序 518 在不解密存储区域中的数据的情况下处理中断。

[0159] 在处理中断之后,如果执行标记 515 是“ON”(S614:ON),则在返回原始处理之前,中断处理程序 518 根据解密算法 D2 使用加密 / 解密密钥来解密存储区域中的加密数据(S615)。如果执行标记 515 是“OFF”(S614:OFF),则中断处理程序 518 在不解密存储区域中的数据的情况下返回到原始处理。

[0160] (B) 第一安全处理程序 501

[0161] 图 10 显示了第一安全处理程序 501 的数据结构。在图中,第一安全处理程序 501 包括断开程序 551、篡改检测程序 552、密钥解密程序 553、密钥发送程序 554、认证程序 555、数据读取程序 556 以及连接程序 557。在 CPU 301 的安全处理模式中执行第一安全处理程序 501。后面详细说明安全处理模式。

[0162] (断开程序 551)

[0163] 当第一安全处理程序 501 起动时,断开程序 551 向调试器禁止电路 303 输出指示“禁止”的调试器控制信号。

[0164] (篡改检测程序 552)

[0165] 篡改检测程序 552 包含密钥 562、并检测第二安全处理程序 502 是否已被篡改。为此,篡改检测程序 552 从第二安全处理程序 502 的调用程序 513 获取包含篡改检测值 541、TRS 区域开始地址 542、二进制大小 543 以及加密的密钥 544 的篡改检测数据。

[0166] 篡改检测程序 552 从由 TRS 区域开始地址指定的存储器 305 中的位置读取对应于二进制大小 543 的数据量,作为 TRS 区域程序。篡改检测程序 552 根据散列函数使用密钥 562 计算 TRS 区域程序的散列值。篡改检测程序 552 将计算的散列值与篡改检测值 541 进行比较。如果两个值匹配,则篡改检测程序 552 判断第二安全处理程序 502 还未被篡改。如果两个值不匹配,则篡改检测程序 552 判断第二安全处理程序 502 已被篡改,并且停止后续

处理。

[0167] (密钥解密程序 553)

[0168] 密钥解密程序 553 包含主密钥 563。如果篡改检测程序 552 判断第二安全处理程序 502 还未被篡改，则密钥解密程序 553 根据解密算法 D1 使用主密钥 563 解密加密的密钥 544，以获得程序密钥。密钥解密程序 553 将程序密钥传递给密钥发送程序 554。

[0169] (密钥发送程序 554)

[0170] 密钥发送程序 554 从密钥解密程序 553 接收程序密钥，并将程序密钥发送到第二安全处理程序 502。

[0171] (认证程序 555)

[0172] 认证程序 555 包含认证密钥 565，并且接受由第二安全处理程序 502 使用认证密钥 565 进行的认证。如果认证成功，则认证程序 555 与第二安全处理程序 502 建立共享会话密钥。使用该会话密钥来加密接下来在第一安全处理程序 501 和第二安全处理程序 502 之间传输的数据。

[0173] (数据读取程序 556)

[0174] 数据读取程序 556 基于 CPRM 与存储卡 400 执行相互认证。如果相互认证是成功的，则数据读取程序 556 访问存储卡 400 的安全区域 420 并获取标题密钥 421。

[0175] (连接程序 557)

[0176] 连接程序 557 向调试器禁止电路 303 输出指示“允许”的调试器控制信号。

[0177] (c) 向量表 503

[0178] 图 11 显示了向量表 503 的数据结构。如图所示，向量表 503 显示了当出现软件中断、终止以及硬件中断时将被执行的指令的地址。

[0179] (D) 音乐播放程序 504

[0180] 音乐播放程序 504 播放通过第二安全处理程序 502 解密的音乐数据。音乐播放程序 504 向解码器 310 中的缓冲器 311 输出音乐数据。

[0181] (E) 应用程序 505

[0182] 应用程序 505 接收用户操作的输入。如果用户操作将播放存储卡 400 中的音乐数据，则应用程序 505 起动第二安全处理程序 502。

[0183] (3) CPU 301

[0184] CPU 301 根据存储在存储器 305 中的程序进行操作。通过从与调试器接口 302 连接的调试器设备发出的指令来控制 CPU 301 的操作。

[0185] 图 12 是显示 CPU 301 的操作的流程图。CPU 301 提取存储在存储器 305 中的程序的指令 (S601)，解码该指令 (S602)，然后执行该指令 (S603)。然后 CPU 301 增加程序计数器 (S604) 以提取下一条指令。

[0186] 这里，CPU 301 工作在安全处理模式或常规处理模式。在常规处理模式中，CPU 301 执行常规处理。在安全处理模式中，CPU 301 以高级别的安全性执行处理，从而使得不能从外部访问存储器 305 中的数据。

[0187] CPU 301 在安全处理模式中执行第一安全处理程序 501，在常规处理模式中执行第二安全处理程序 502。

[0188] 当出现中断时，中断控制器 304 通过中断线 318 输出中断信号。如果由中断禁止

程序 512 禁止了中断，则 CPU 301 拒绝中断信号。如果未禁止中断，则 CPU 301 接受中断信号，参考图 11 所示的向量表 503，并读取对应于中断信号的地址。CPU 301 根据位于读取地址的中断处理程序处理中断。处理完中断之后，CPU 301 返回原始处理。

[0189] 当在执行第二安全处理程序 502 期间接收到中断信号时，CPU301 参考向量表 503 并执行图 9 所示的中断处理程序 518。

[0190] (4) 输入单元 307

[0191] 输入单元 307 接收用户操作的输入。

[0192] 当接收到输入时，输入单元 307 向中断控制器 304 通知中断。

[0193] (5) 中断控制器 304

[0194] 当输入单元 307 或无线电控制单元 314 向中断控制器 304 通知例如邮件接收、调用接收或用户操作这样的中断时，中断控制器 304 经由中断线 318 向 CPU 301 输出中断信号。

[0195] (6) 扬声器 309 和解码器 310

[0196] 解码器 310 包括缓冲器 311。缓冲器 311 对从 CPU 301 接收的音乐数据进行缓冲。扬声器 309 根据缓冲器 311 中的音乐数据生成音频信号，并输出音频信号。

[0197] (7) 存储卡接口 306

[0198] 存储卡接口 306 用于连接便携式终端 300 和存储卡 400。在 CPU301 的控制下，存储卡接口 306 将数据输出到存储卡 400，并从存储卡 400 接收数据并将其输出到 CPU 301。

[0199] (8) 无线电控制单元 314, 无线电单元 315, 天线 316

[0200] 天线 316、无线电单元 315、无线电控制单元 314 与一个设备发送 / 接收声音或信息，便携式终端 300 通过无线电基站和便携式终端网络连接到该设备。

[0201] 当经由天线 316 和无线电单元 315 接收到邮件或调用时，无线电控制单元 314 向中断控制器 304 通知中断。

[0202] (9) 麦克风 312 和转换单元 313

[0203] 转换单元 313 将从麦克风 312 接收到的声音转换为电子信号，并将其输出到无线电控制单元 314。

[0204] 2. 安全处理系统 1 的操作

[0205] 2.1. 认证机构设备 100 的操作

[0206] 编译器 101 接收调用程序 513 的源代码和保护程序的源代码的输入，并将所述源代码编译为调用程序 513 的二进制数据和保护程序的二进制数据。编译器 101 将二进制数据输出到数据嵌入单元 105。编译器 101 还接收解密程序 516 的源代码和安全程序的源代码的输入，并将所述源代码编译为解密程序 516 的二进制数据和安全程序的二进制数据。编译器 101 将所述二进制数据输出到程序加密单元 102。

[0207] 程序加密单元 102 接收解密程序 516 的二进制数据和安全程序的二进制数据。程序加密单元 102 还接收程序密钥。程序加密单元 102 使用所述程序密钥加密安全程序，以生成加密的程序 517。程序加密单元 102 将解密程序 516 和加密的程序 517 输出到数据嵌入单元 105 和散列值计算单元 104，作为 TRS 区域程序。

[0208] 散列值计算单元 104 接收 TRS 区域程序。散列值计算单元 104 还接收密钥。散列值计算单元 104 根据散列函数使用密钥计算 TRS 区域程序的散列值。散列值计算单元 104

还计算 TRS 区域程序的二进制大小。散列值计算单元 104 将散列值和二进制大小输出到数据嵌入单元 105。

[0209] 密钥加密单元 103 接收程序密钥和主密钥, 使用主密钥加密程序密钥以生成加密的密钥。密钥加密单元 103 将加密的密钥输出到数据嵌入单元 105。

[0210] 数据嵌入单元 105 从编译器 101 接收调用程序 513 的二进制数据, 并从散列值计算单元 104 接收散列值和二进制大小, 并从密钥加密单元 103 接收加密的密钥。数据嵌入单元 105 将散列值嵌入调用程序 513 作为篡改检测值 541。数据嵌入单元 105 还将二进制大小和加密的密钥嵌入调用程序 513 作为二进制大小 543 和加密的密钥 544。数据嵌入单元 105 还从编译器 101 接收保护程序的二进制数据, 并从程序加密单元 102 接收 TRS 区域程序。数据嵌入单元 105 将调用程序 513 包含进保护程序, 并将保护程序和 TRS 区域程序进行组合以形成第二安全处理程序 502。数据嵌入单元 105 将第二安全处理程序 502 写入存储单元 106。

[0211] 传输单元 107 从存储单元 106 读取第二安全处理程序 502, 并将第二安全处理程序 502 输出到 ROM 写入器 200。

[0212] 2.2. 便携式终端 300 的音乐数据播放操作

[0213] (1) 播放

[0214] 下面参考图 13 至 17 说明由便携式终端 300 通过执行程序来播放记录在存储卡 400 上的音乐数据的操作。

[0215] 当经由输入单元 307 接收到播放存储卡 400 上的音乐数据的用户操作的输入时, 应用程序 505 起动第二安全处理程序 502(S701)。

[0216] 在第二安全处理程序 502 中, 区域分配程序 511 在存储器 305 中分配虚拟的存储空间, 用于在安全程序的执行期间, 动态地分配存储区域 (S702)。并且, 中断禁止程序 512 禁止中断 (S703)。因此, 禁止了使用中断的未授权的程序分析和更改。中断的禁止一直有效直到中断允许。接着, 调用程序 513 调用第一安全处理程序 501, 并将由篡改检测值 541、TRS 区域开始地址 542、二进制大小 543 以及加密的密钥 544 构成的篡改检测数据传递给第一安全处理程序 501(S704)。

[0217] 第一安全处理程序 501 从第二安全处理程序 502 接收篡改检测数据 (S705)。在第一安全处理程序 501 中, 断开程序 551 将指示“禁止”的调试器控制信号输出到调试器禁止电路 303(S706)。因此, 调试器禁止电路 303 断开调试器设备。因此, 禁止使用调试器设备进行未授权的程序分析和更改。

[0218] 接着, 篡改检测程序 552 执行下列过程。

[0219] 篡改检测程序 552 从由 TRS 区域开始地址 542 指定的存储器 305 上的位置读取对应于二进制大小 543 的数据量, 作为 TRS 区域程序。篡改检测程序 552 使用密钥 562 计算 TRS 区域程序的散列值 (S709)。

[0220] 篡改检测程序 552 将所计算的散列值与篡改检测值 541 进行比较 (S710)。如果两个值不匹配 (S710 : 否), 则篡改检测程序 552 判断第二安全处理程序 502 已被篡改, 并且停止后续处理。连接程序 557 将指示“允许”的调试器控制信号输出到调试器禁止电路 303(S737), 并终止操作。

[0221] 如果两个值匹配 (S710 : 是), 则篡改检测程序 552 判断第二安全处理程序 502 未

被篡改。因此，密钥解密程序 553 使用主密钥 563 解密加密的密钥 544，以得到程序密钥 (S711)。密钥解密程序 553 将程序密钥传递给密钥发送程序 554。密钥发送程序 554 将程序密钥传递给第二安全处理程序 502 (S712)。

[0222] 在第二安全处理程序 502 中，密钥接收程序 514 接收程序密钥 (S713)。并且，将执行标记 515 设置为“ON”(S714)。之后，解密程序 516 使用程序密钥解密加密的程序 517，以得到安全程序 (S715)。完成之后，解密程序 516 删除程序密钥 (S716)。

[0223] 安全程序执行下列过程 (S717)。

[0224] 在安全程序中，中断允许程序 521 释放在步骤 S703 执行的中断的禁止 (S718)。其后，如果出现中断，则挂起安全程序以处理中断。后面详细说明当出现中断时将被执行的过程。

[0225] 然后，区域初始化程序 522 在存储空间中分配存储区域 (S719)，在该存储区域中将存储由认证程序 523 和加密音乐数据解密程序 524 使用的数据。

[0226] 认证程序 523 根据认证过程认证第一安全处理程序 501 (随后描述) (S720)。第一安全处理程序 501 中的认证程序 555 经受由认证程序 523 进行的认证。如果认证失败，则第二安全处理程序 502 停止后续处理，并且在终止操作之前，第一安全处理程序 501 中的连接程序 557 将指示“允许”的调试器控制信号输出到调试器禁止电路 303 (S737)。

[0227] 如果认证成功，则第二安全处理程序 502 与第一安全处理程序 501 建立共享的会话密钥。使用该会话密钥加密随后在第二安全处理程序 502 和第一安全处理程序 501 之间传输的数据。

[0228] 如果认证成功，则第二安全处理程序 502 将控制传递给音乐播放程序 504。

[0229] 音乐播放程序 504 从存储卡 400 读取加密的音乐数据 411 (S721)。音乐播放程序 504 还请求第二安全处理程序 502 解密加密的音乐数据 411 (S722)。

[0230] 当接收到解密加密的音乐数据 411 的请求时，第二安全处理程序 502 调用区域加密程序 526。区域加密程序 526 使用区域密钥 525 加密在步骤 S719 分配的存储区域中的数据 (S723)。之后，第二安全处理程序 502 请求第一安全处理程序 501 获取标题密钥 421 (S724)。

[0231] 在第一安全处理程序 501 中，数据读取程序 556 与存储卡 400 中的认证单元 403 执行相互认证 (S725)。如果相互认证成功 (S726 :是)，则数据读取程序 556 访问存储卡 400 中的安全区域 420 并获取标题密钥 421 (S727)。如果相互认证失败，则数据读取程序 556 不能获取标题密钥 421。在这种情况下，连接程序 557 在终止操作前将指示“允许”的调试器控制信号输出到调试器禁止电路 303 (S737)。

[0232] 第一安全处理程序 501 使用会话密钥加密标题密钥 421，以生成加密的标题密钥 (S728)。第一安全处理程序 501 将加密的标题密钥传递给第二安全处理程序 502。

[0233] 在第二安全处理程序 502 中，区域解密程序 527 使用区域密钥 525 解密存储区域中的加密的数据，以恢复原始数据 (S729)。认证程序 523 使用会话密钥解密加密的标题密钥，以获得标题密钥 421 (S730)。之后，加密音乐数据解密程序 524 使用标题密钥 421 解密由音乐播放程序 504 从存储卡 400 读取的加密的音乐数据 411 (S731)。因此，获得音乐数据。加密音乐数据解密程序 524 将音乐数据传递给音乐播放程序 504。

[0234] 音乐播放程序 504 播放音乐数据 (S732)。

[0235] 一旦完成音乐数据的播放 (S733), 则音乐播放程序 504 将控制传递给第二安全处理程序 502。在第二安全处理程序 502 中, 区域释放程序 528 释放在步骤 S719 中分配的存储区域 (S734), 并调用第一安全处理程序 501 的退出函数 (S735)。而且, 将执行标记 515 设置为“OFF” (S736)。

[0236] 在第一安全处理程序 501 中, 在终止操作前, 连接程序 557 将指示“允许”的调试器控制信号输出到调试器禁止电路 303 (S737)。

[0237] (2) 认证

[0238] 下面参照图 18 说明在步骤 S720 中由第二安全处理程序 502 对第一安全处理程序 501 进行认证的过程。

[0239] 第二安全处理程序 502 生成随机数 R0, 并将随机数 R0 传递给第一安全处理程序 501 (S751)。

[0240] 第一安全处理程序 501 接收随机数 R0, 并使用认证密钥 565 加密随机数 R0 以生成认证值 R1 (S752)。第一安全处理程序 501 将认证值 R1 传递给第二安全处理程序 502 (S753)。

[0241] 第二安全处理程序 502 从第一安全处理程序 501 接收认证值 R1。第二安全处理程序 502 使用认证密钥 531 加密随机数 R0, 以生成认证值 R2 (S754)。第二安全处理程序 502 将认证值 R1 与认证值 R2 进行比较 (S755)。如果两个值不匹配 (S755 : 否), 则第二安全处理程序 502 将指示“不匹配”的判断结果传递给第一安全处理程序 501 (S756), 并终止过程。如果两个值匹配 (S755 : 是), 则第二安全处理程序 502 将指示“匹配”的判断结果传递给第一安全处理程序 501 (S757)。然后, 第二安全处理程序 502 使用单向函数根据随机数 R0 和认证密钥 531 生成会话密钥 (S759)。

[0242] 如果所接收的判断结果指示“不匹配” (S758 : 否), 则第一安全处理程序 501 终止过程。如果所接收的判断结果指示“匹配” (S758 : 是), 则第一安全处理程序 501 使用单向函数根据随机数 R0 和认证密钥 565 生成会话密钥 (S760)。

[0243] 因此, 第二安全处理程序 502 认证第一安全处理程序 501, 并且如果认证成功, 则共享会话密钥。使用该会话密钥加密随后在第一安全处理程序 501 和第二安全处理程序 502 之间传输的数据。

[0244] (3) 中断

[0245] 下面参照图 19 说明当在执行第二安全处理程序 502 期间出现中断时的 CPU 301 的操作。这里, 以邮件接收作为中断的一个例子。

[0246] 当从中断控制器 304 接收到中断信号时 (S771), CPU 301 读取向量表 503 (S772), 并根据向量表 503 执行中断处理程序 518 (S773)。

[0247] 首先, CPU 301 读取执行标记 515 (S774)。如果执行标记 515 是“ON” (S775 : 否), 则 CPU 301 使用加密 / 解密密钥来加密存储区域中的数据 (S776)。CPU 301 还存储运行环境 (context) (S777), 并执行邮件接收处理 (S778)。如果执行标记 515 是“OFF” (S775 : OFF), 则 CPU 301 在不加密存储区域中的数据的情况下执行步骤 S777 和 S778。

[0248] 在邮件接收处理之后, 如果执行标记 515 是“ON” (S779 : ON), 则在返回原始处理之前, CPU 301 解密存储区域中的数据 (S780)。如果执行标记 515 是“OFF” (S779 : OFF), 则 CPU 301 在不解密存储区域中的数据的情况下返回原始处理。

[0249] 3. 变形

[0250] 已经通过以上实施例描述了本发明,但是很明显,本发明并不局限于上述实施例。以下给出示例性的变形。

[0251] (1) 上述实施例描述了保护加密音乐数据解密程序的例子,其中,由便携式终端执行加密音乐数据解密程序,但是本发明并不限于其。

[0252] 执行待保护的程序的示例性设备包括 DVD 播放器、DVD 记录器、PC 以及 PDA。

[0253] 而且,待保护的示例性程序包括当在便携式终端上播放视频内容或游戏时使用的解密程序,以及当在 DVD 记录器上记录内容时使用的记录程序。因此,本发明可应用于任何需要被保护以防止未授权的分析和更改的程序。

[0254] (2) 上述实施例描述了散列值被用作篡改检测值的例子,但是唯一属于 TRS 区域程序的任何值都能被用作篡改检测值。例如,对 TRS 区域程序的数字签名或通过加密 TRS 区域程序而生成的数据可以被用作篡改检测值。而且,除实施例中使用的算法以外的算法可以被用于计算散列值。

[0255] 上述实施例描述了为 TRS 区域程序生成篡改检测值的例子,但是也可以为至少一部分 TRS 区域程序生成篡改检测值。或者,可以为至少一部分第二安全处理程序生成篡改检测值。

[0256] 而且,可以通过为至少一部分 TRS 区域程序或第二安全处理程序执行匹配计算,或者通过将伪随机数 (psuedo-random number) 嵌入至少一部分 TRS 区域程序或第二安全处理程序来执行篡改检测。也就是说,任何能够检测程序是否已被篡改的篡改检测方法都是可用的。

[0257] 上述实施例描述了在调试器禁止电路断开调试器设备后执行篡改检测的例子。作为另一个例子,可以在由调试器禁止电路断开之前执行篡改检测。在这种情况下,如果未检测到篡改,则调试器禁止电路断开调试器设备以进行后续处理。

[0258] (3) 上述实施例描述了第二安全处理程序中的调用程序将篡改检测数据传递给第一安全处理程序的例子。作为另一个例子,不同于第二安全处理程序的程序可以将篡改检测数据传递给第一安全处理程序。在这种情况下,第二安全处理程序中的调用程序仅调用第一安全处理程序。同时,在存储器 305 中存储用于将篡改检测数据发送到第一安全处理程序的发送程序。因此,当被第二安全处理程序调用时,第一安全处理程序请求发送程序发送篡改检测数据。作为响应,发送程序将篡改检测数据发送到第一安全处理程序。

[0259] 在这种情况下,认证机构设备不在第二安全处理程序的保护程序中包括该发送程序,而是根据第二安全处理程序独立地生成其。

[0260] 而且,第一安全处理程序可以预先包含第二安全处理程序的篡改检测数据。

[0261] (4) 上述实施例描述了第二安全处理程序对第一安全处理程序执行单向认证的例子,但是,第二安全处理程序与第一安全处理程序可以执行双向认证。而且,上述实施例描述了挑战应答认证方法的使用,但是,可以等价地使用其它用于认证程序的认证方法。

[0262] 上述实施例描述了通过使用认证密钥来加密随机数 R0,从而生成认证值 R1 和 R2 的例子,但是,也可以通过对随机数 R0 应用单向函数来生成它们。

[0263] 上述实施例描述了使用单向函数根据随机数 R0 和认证密钥来生成会话密钥的例子,但是也可以通过加密来生成会话密钥。

[0264] (5) 上述实施例描述了在将控制从第二安全处理程序传递给第一安全处理程序之前,区域加密程序加密存储区域中的数据的例子。当将控制从第二安全处理程序传递给其它程序时,例如当第二安全处理程序调用外部函数时,区域加密程序也可以加密存储区域中的数据以保护数据。

[0265] 在这种情况下,当控制返回到第二安全处理程序时,区域解密程序解密存储区域中的加密数据以恢复原始数据。

[0266] (6) 可以为每个执行应被保护的程序的设备分配唯一的主密钥。在这种情况下,即使未授权的用户窃取了一个设备的主密钥并试图使用该主密钥去攻击其它设备,该未授权的用户也不能正确地操作其它设备。这最小化了由未授权行为导致的破坏。

[0267] (7) 上述实施例描述了第一安全处理程序和第二安全处理程序都分别包含认证密钥的例子。可选择地,可以基于程序密钥或篡改检测值来计算认证密钥。

[0268] 而且,认证机构设备可以使用主密钥加密认证密钥。在这种情况下,可以基于认证密钥计算用于解密加密的程序的程序密钥。

[0269] 当用于认证的密钥和用于解密加密的程序的密钥因此具有依赖关系时,任何密钥都可以被加密。此外,可以使用更多的密钥来进行多级加密,例如,通过使用另一个密钥加密已加密的密钥。

[0270] (8) 本发明还应用于上述方法。该方法可以通过由计算机执行的计算机程序来实现。这种计算机程序可以作为数字信号来分发。

[0271] 本发明可以通过其上记录有上述计算机程序或数字信号的计算机可读存储介质来实现,例如软盘、硬盘、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD 或半导体存储器。相反地,本发明也可以通过记录在这种存储介质上的计算机程序或数字信号来实现。

[0272] 也可以通过网络(例如,电子通信网络、有线或无线通信网络、或因特网)来传送实现本发明的计算机程序或数字信号。

[0273] 也可以通过包含微处理器和存储器的计算机系统来实现本发明。在这种情况下,计算机程序可以被存储在存储器中,微处理器根据该计算机程序运行。

[0274] 可以通过分发其上记录有计算机程序或数字信号的存储介质,或者通过经由网络传送计算机程序或数字信号,从而将计算机程序或数字信号提供给独立的计算机系统。然后,独立的计算机系统可以执行计算机程序或数字信号以用作本发明。

[0275] (8) 可以自由地组合上述实施例和变形。

[0276] 工业适用性

[0277] 可以将本发明反复地以及连续地用于提供软件(例如计算机程序和电影、音乐的数字内容等等)的软件行业。而且,可以在电子产品等的制造行业中制造并销售本发明。

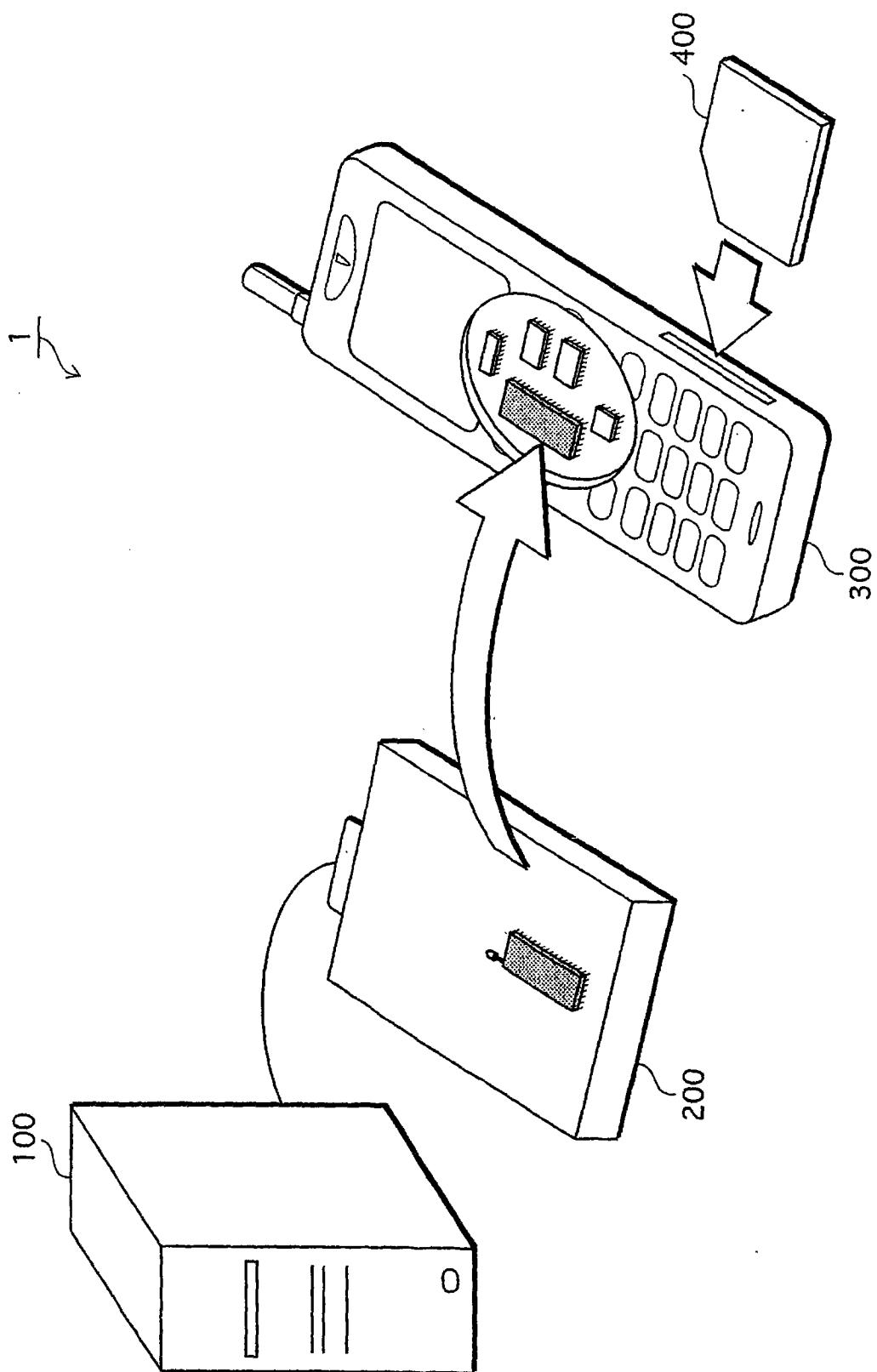


图 1

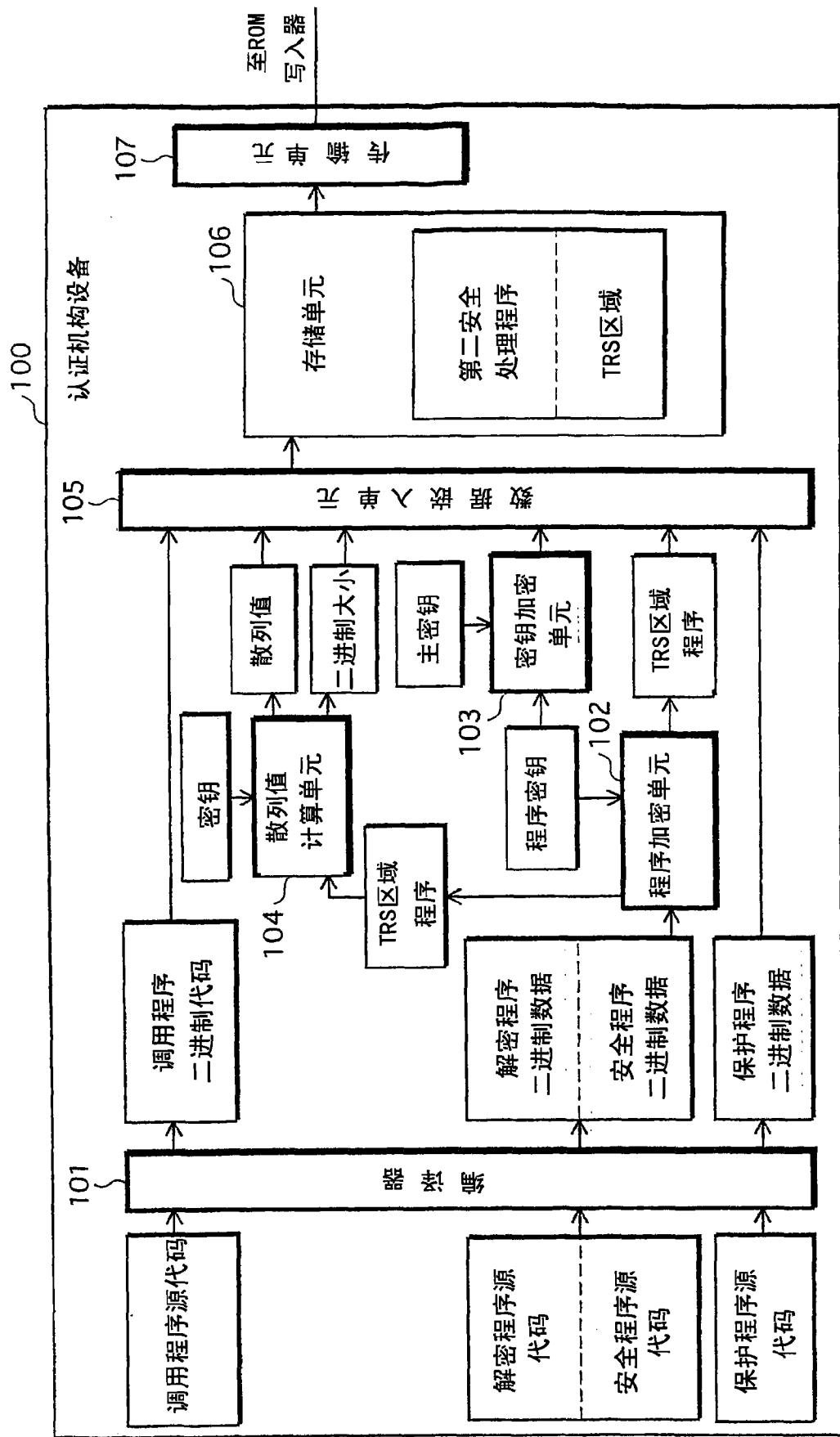


图 2

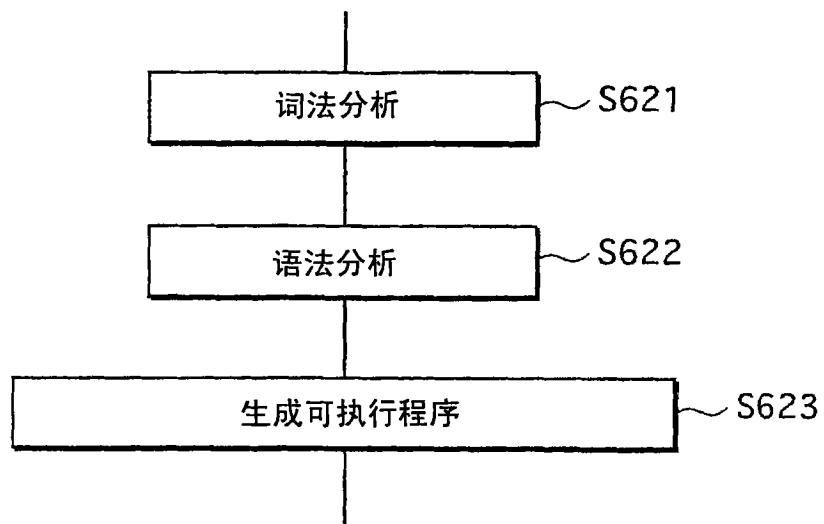


图 3

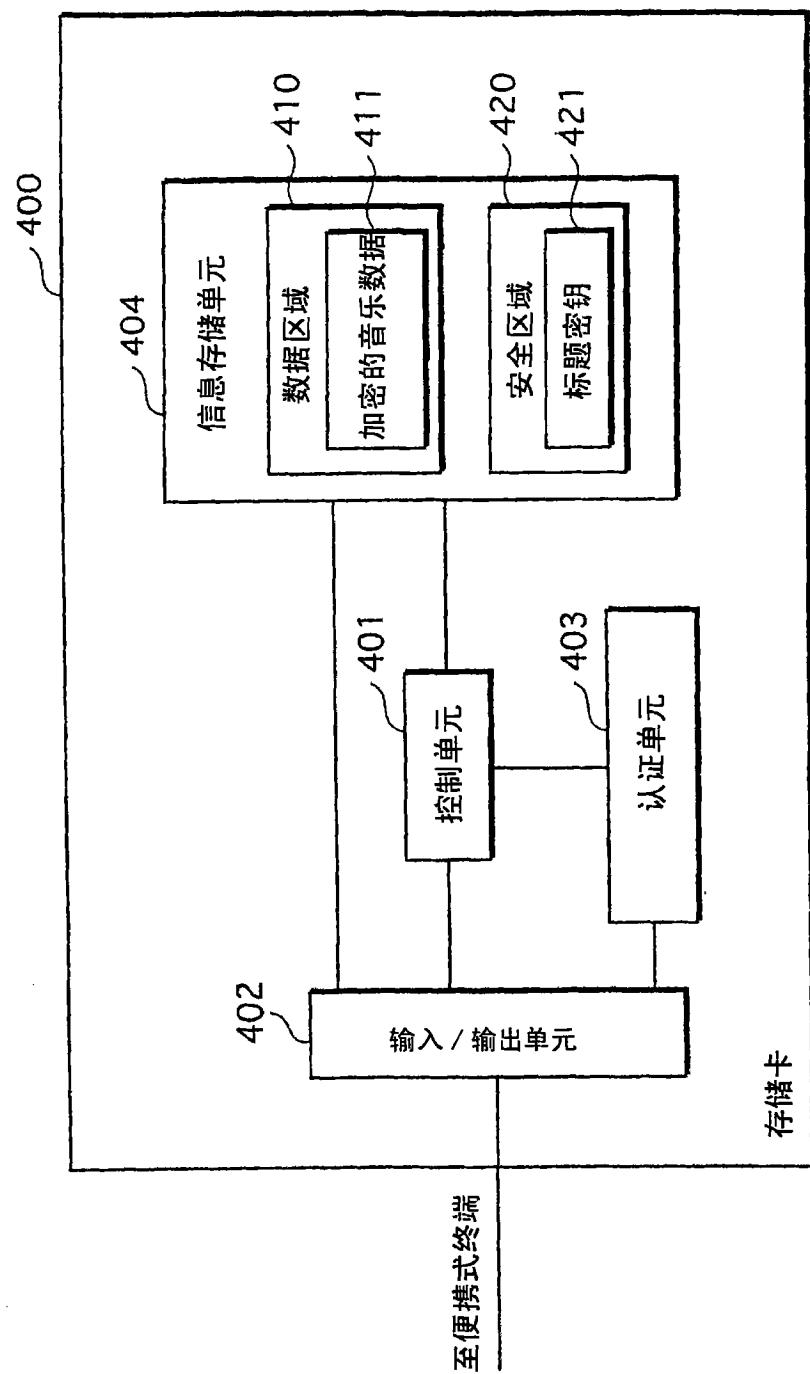


图 4

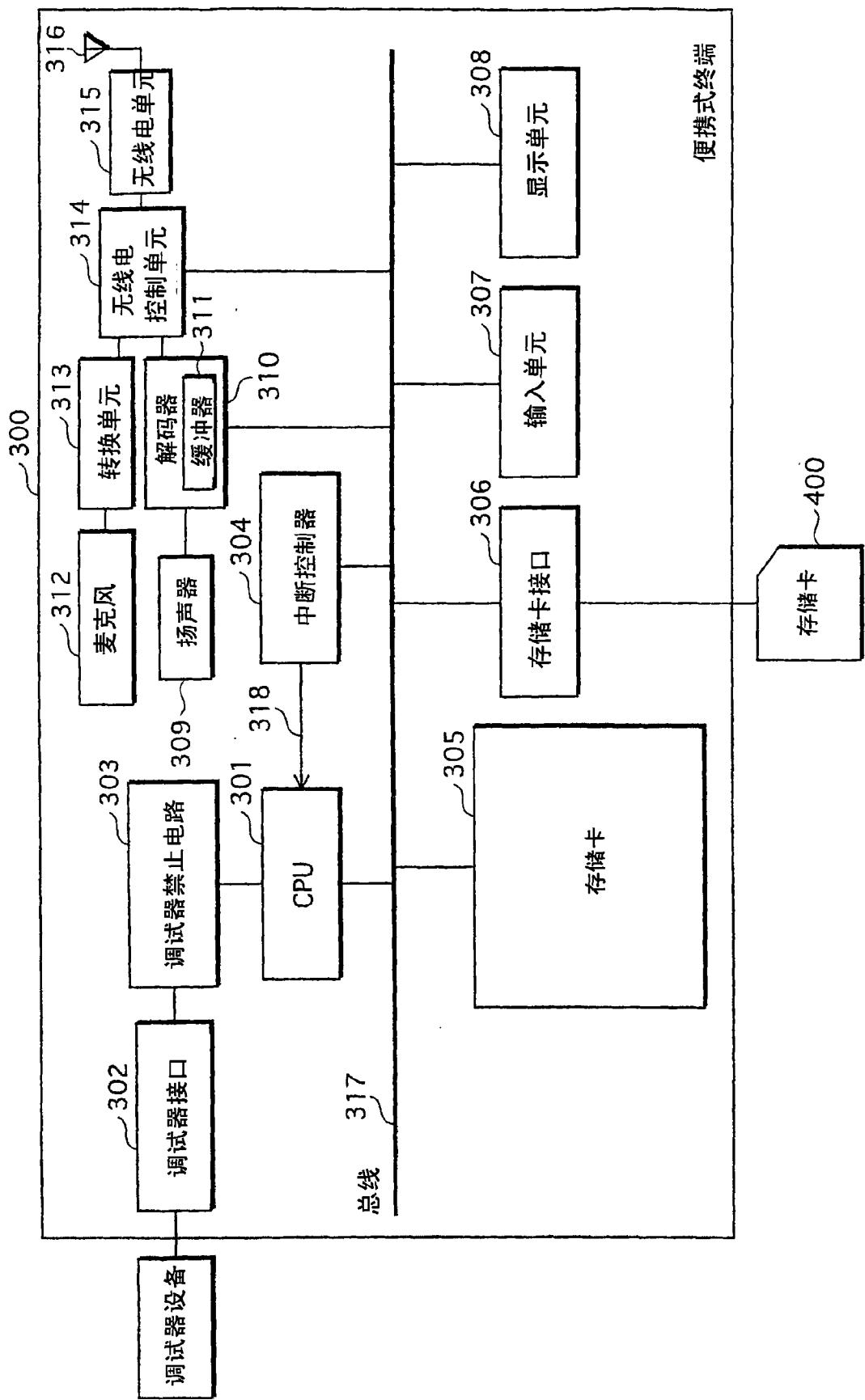


图 5

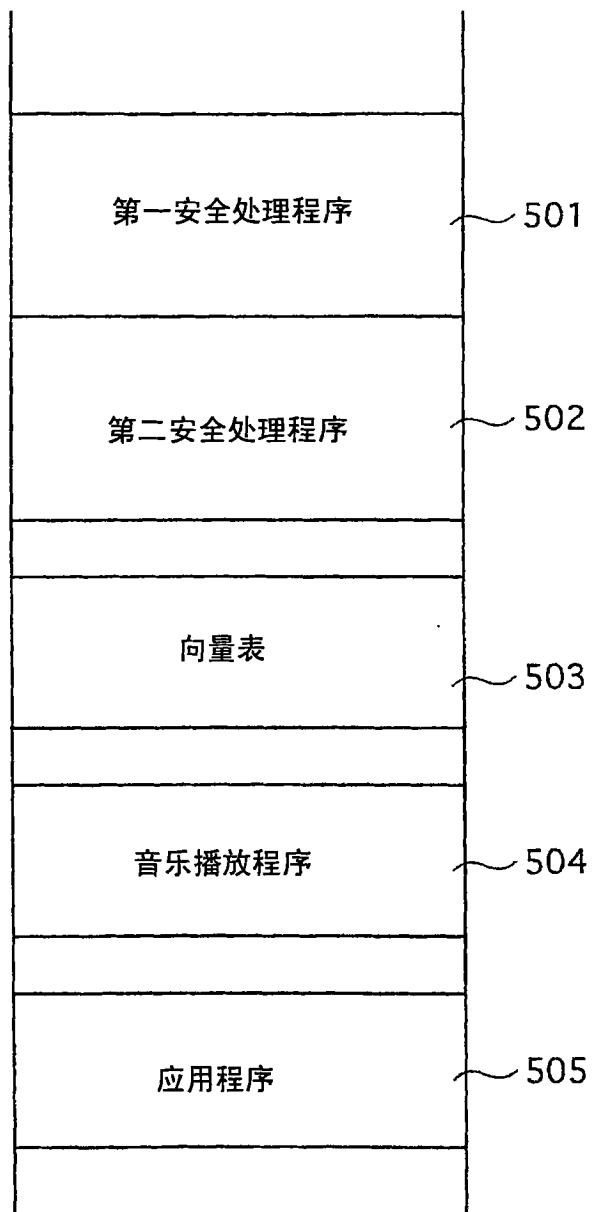


图 6

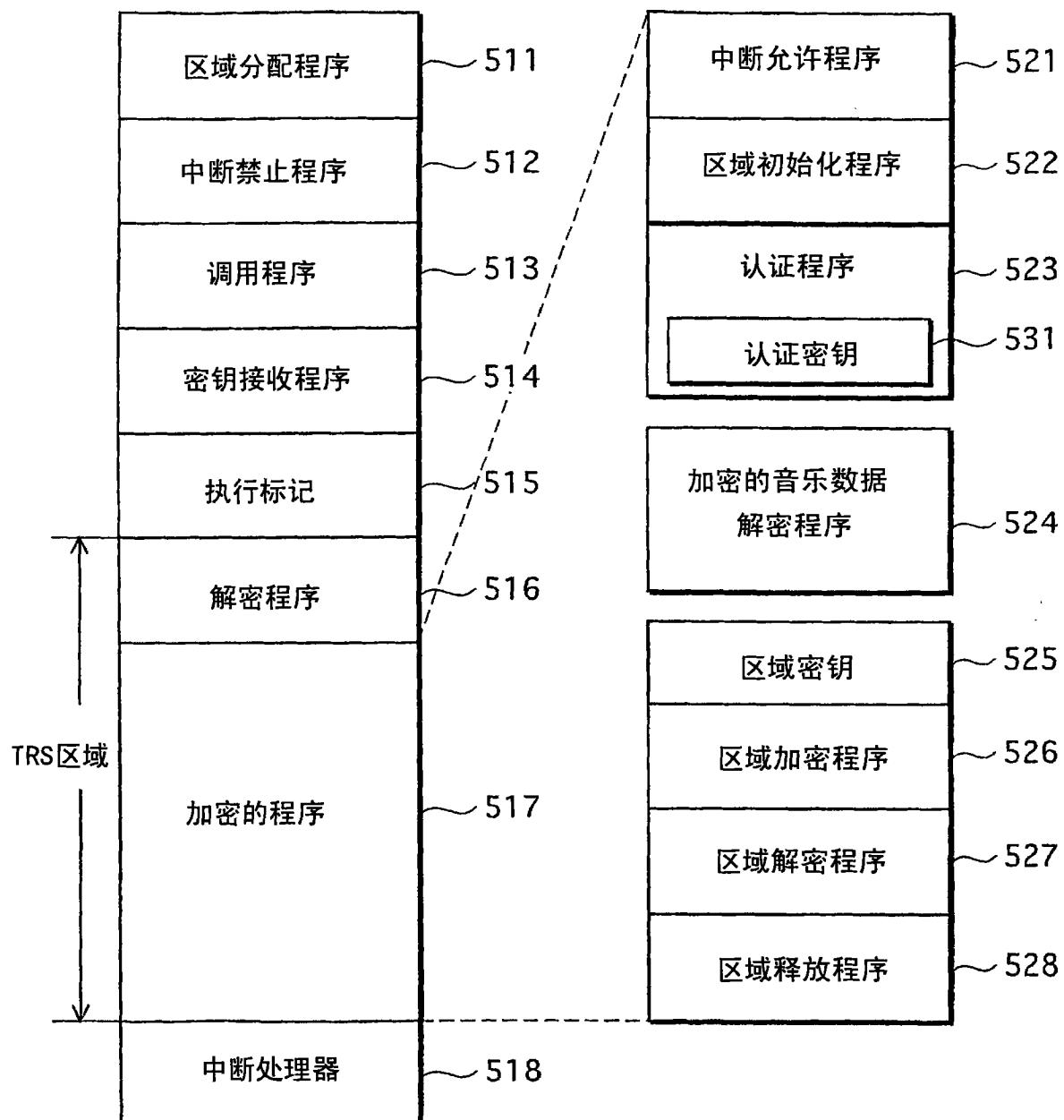


图 7

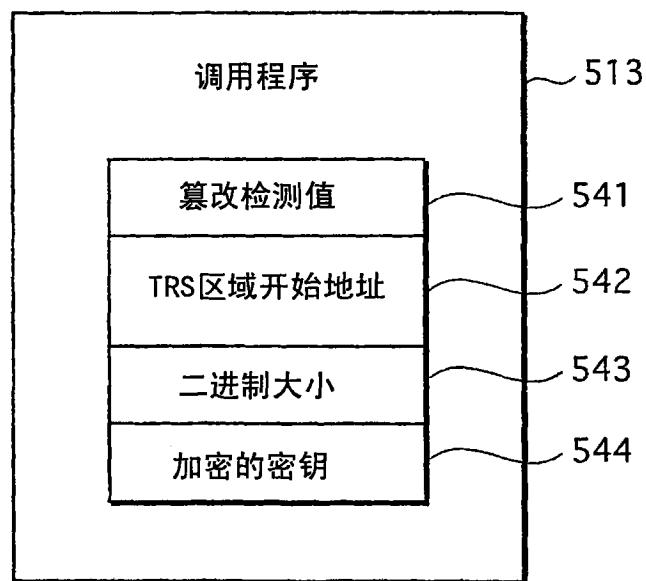


图 8

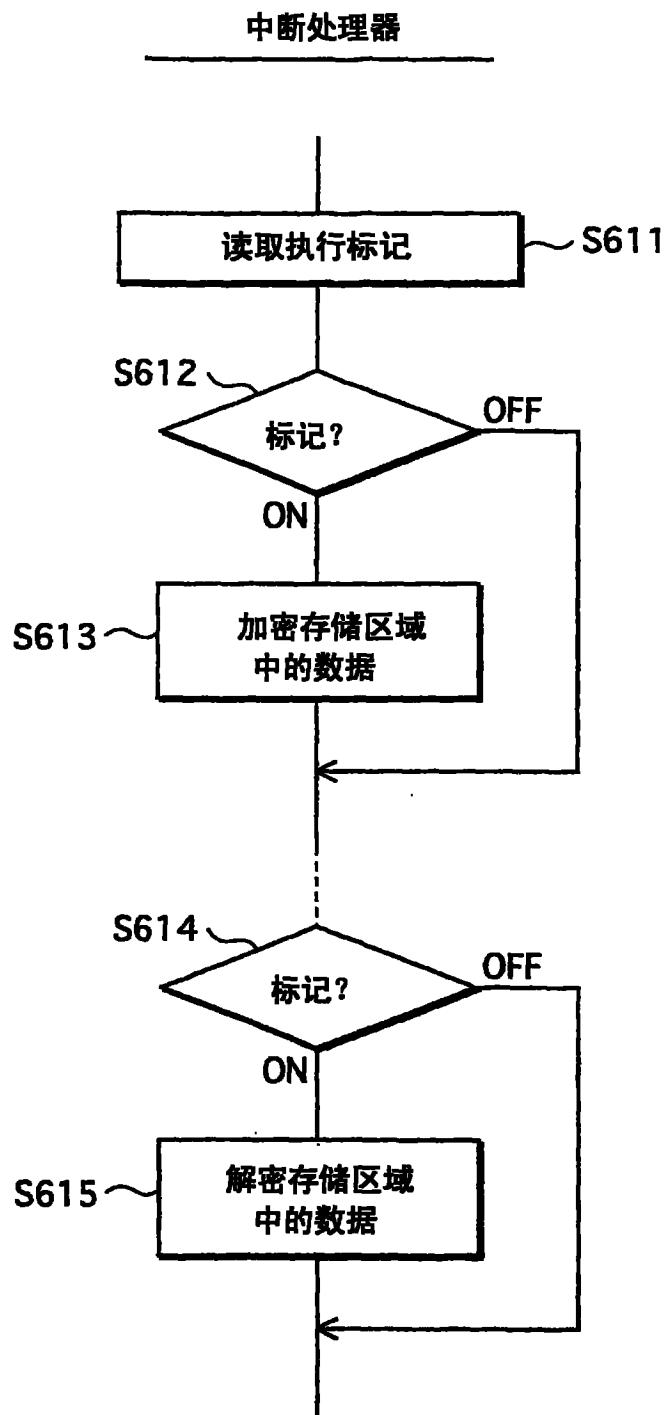


图 9

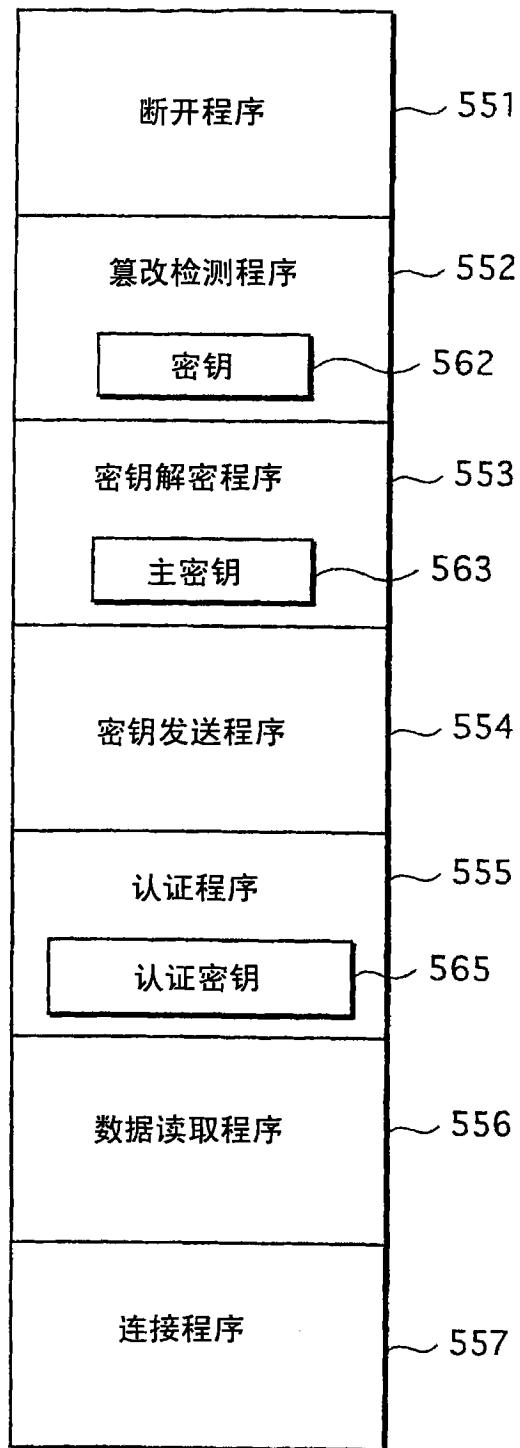


图 10

复位	BL0x0000AAAA
未定义指令	BL0xAAAA0000
中断	BL0xBBB0000
异常中止	BL0xCCCC0000
软件中断	BL0xDDD0000
⋮	⋮

图 11

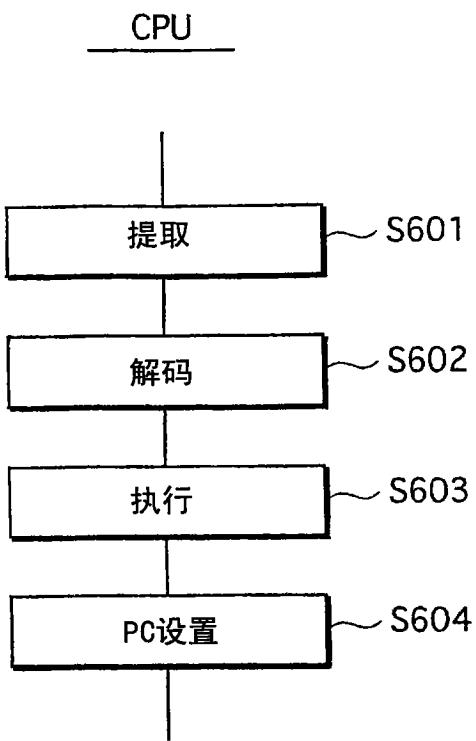


图 12

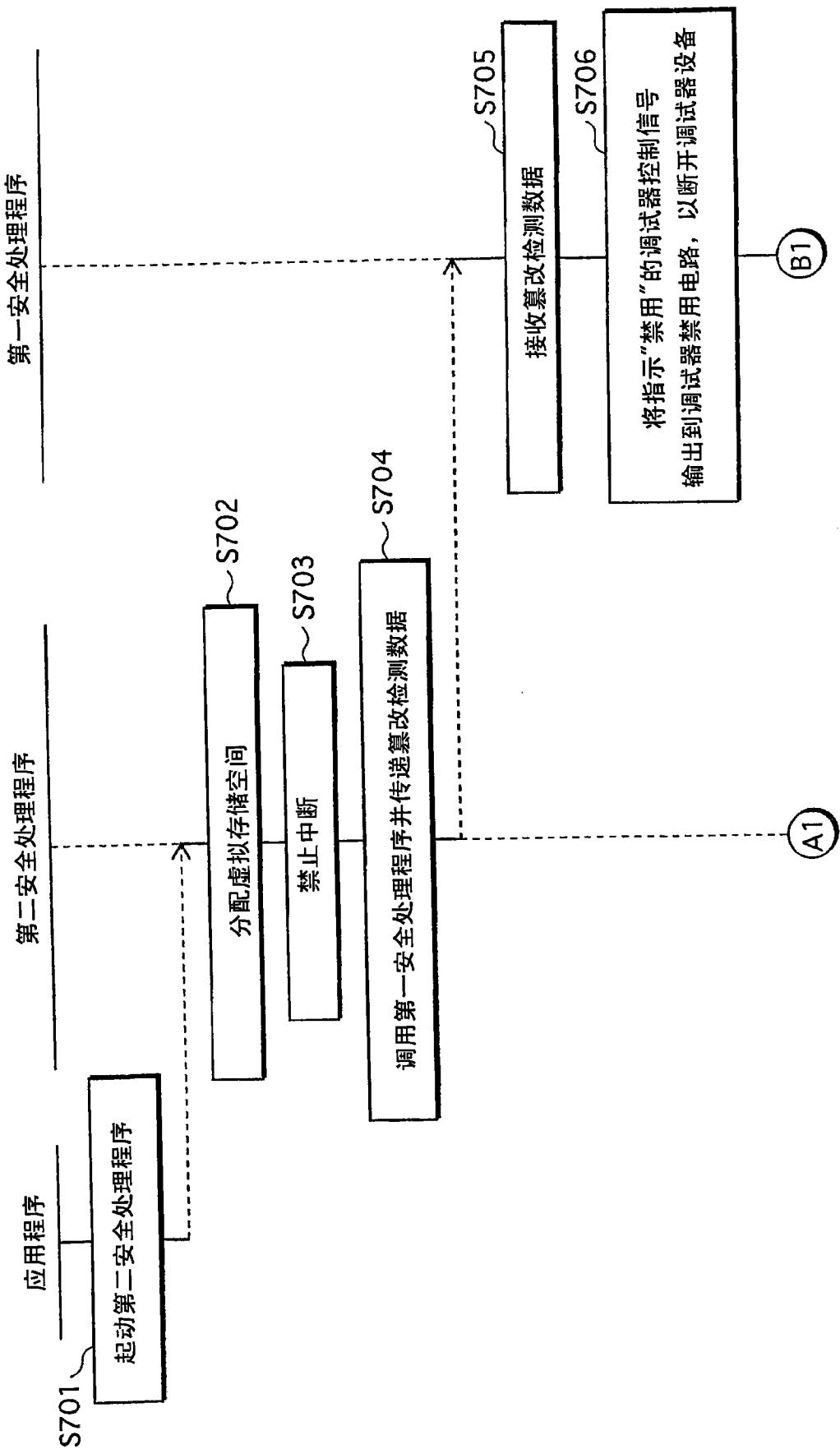


图 13

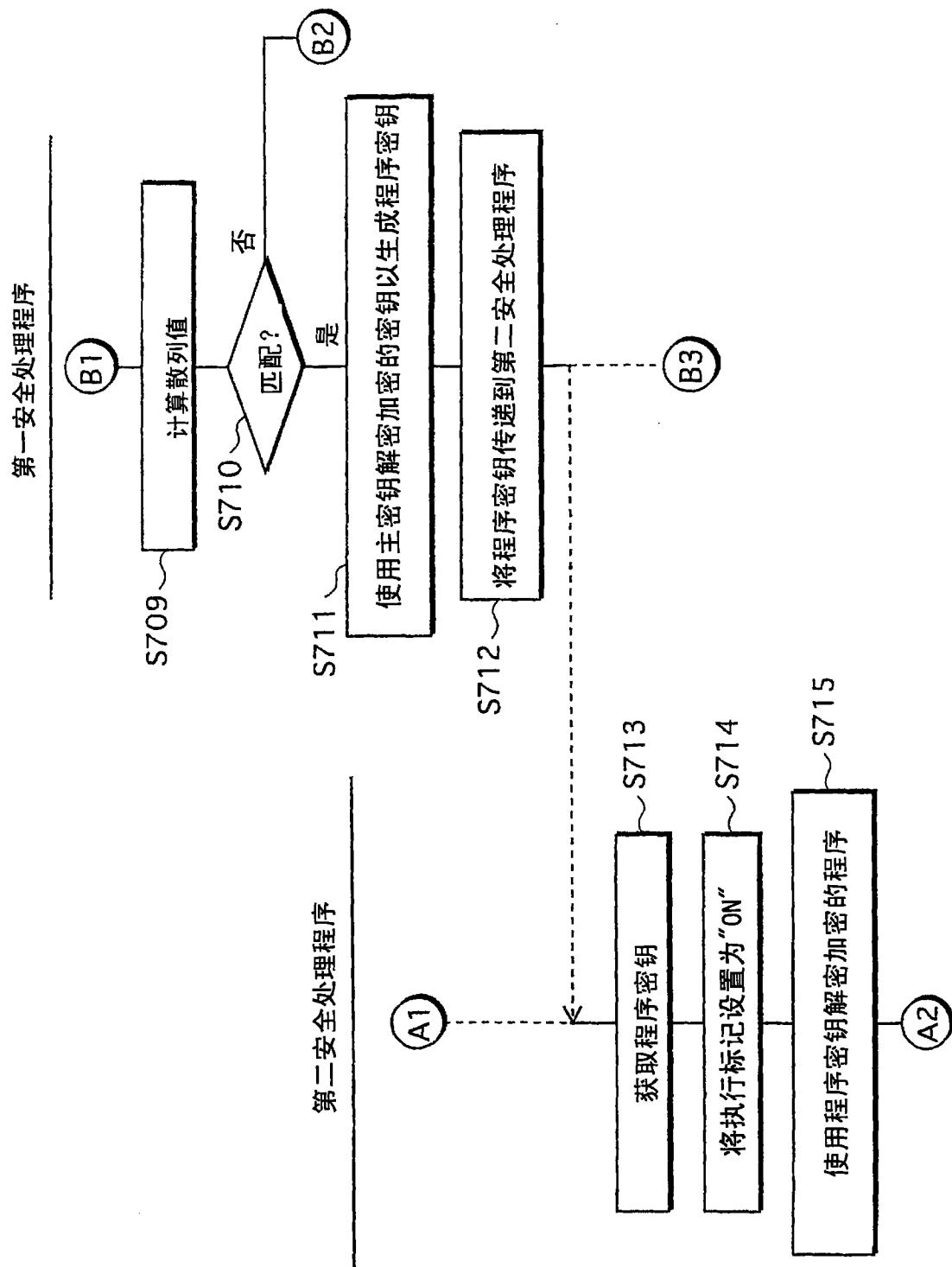


图 14

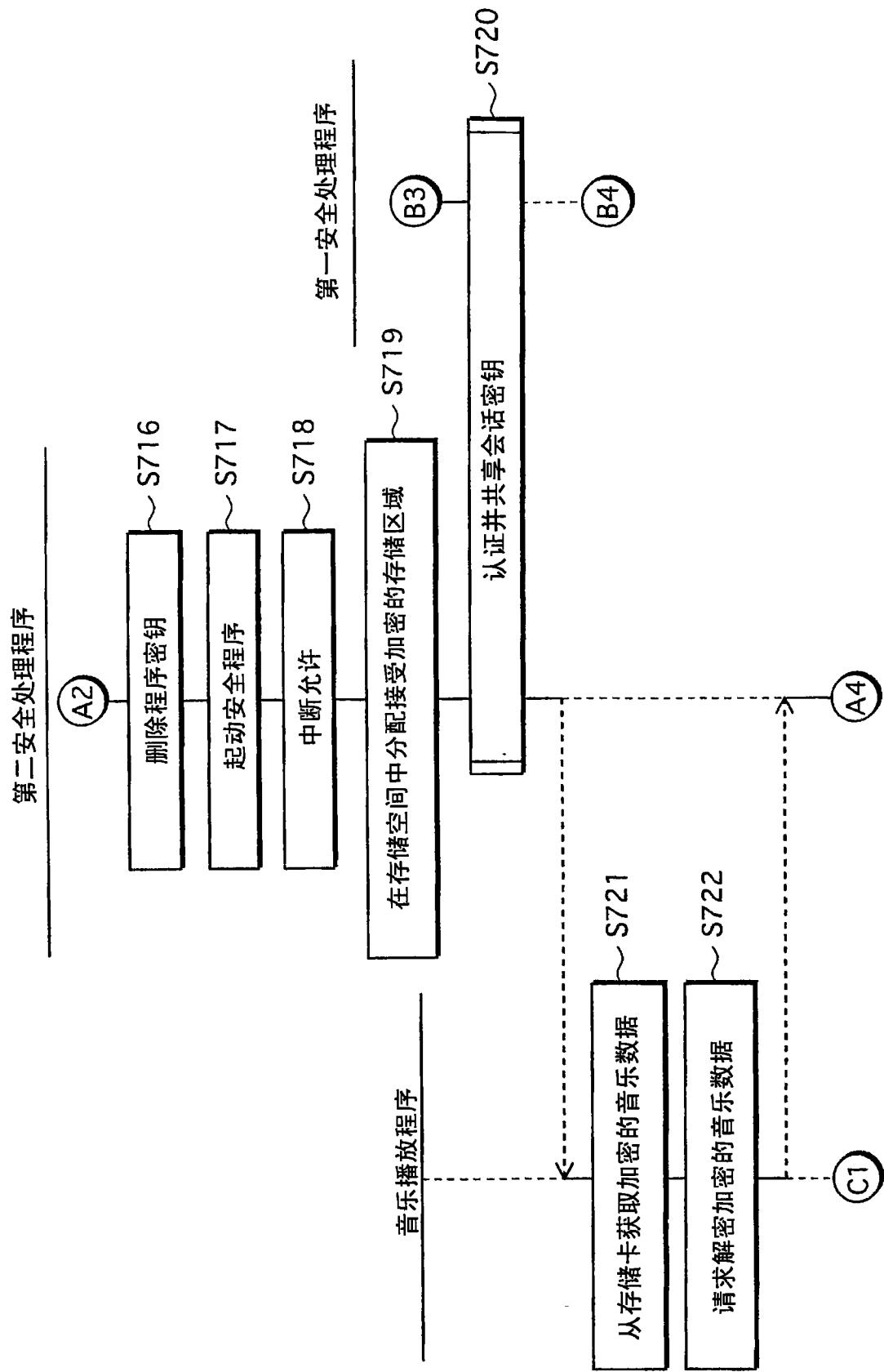


图 15

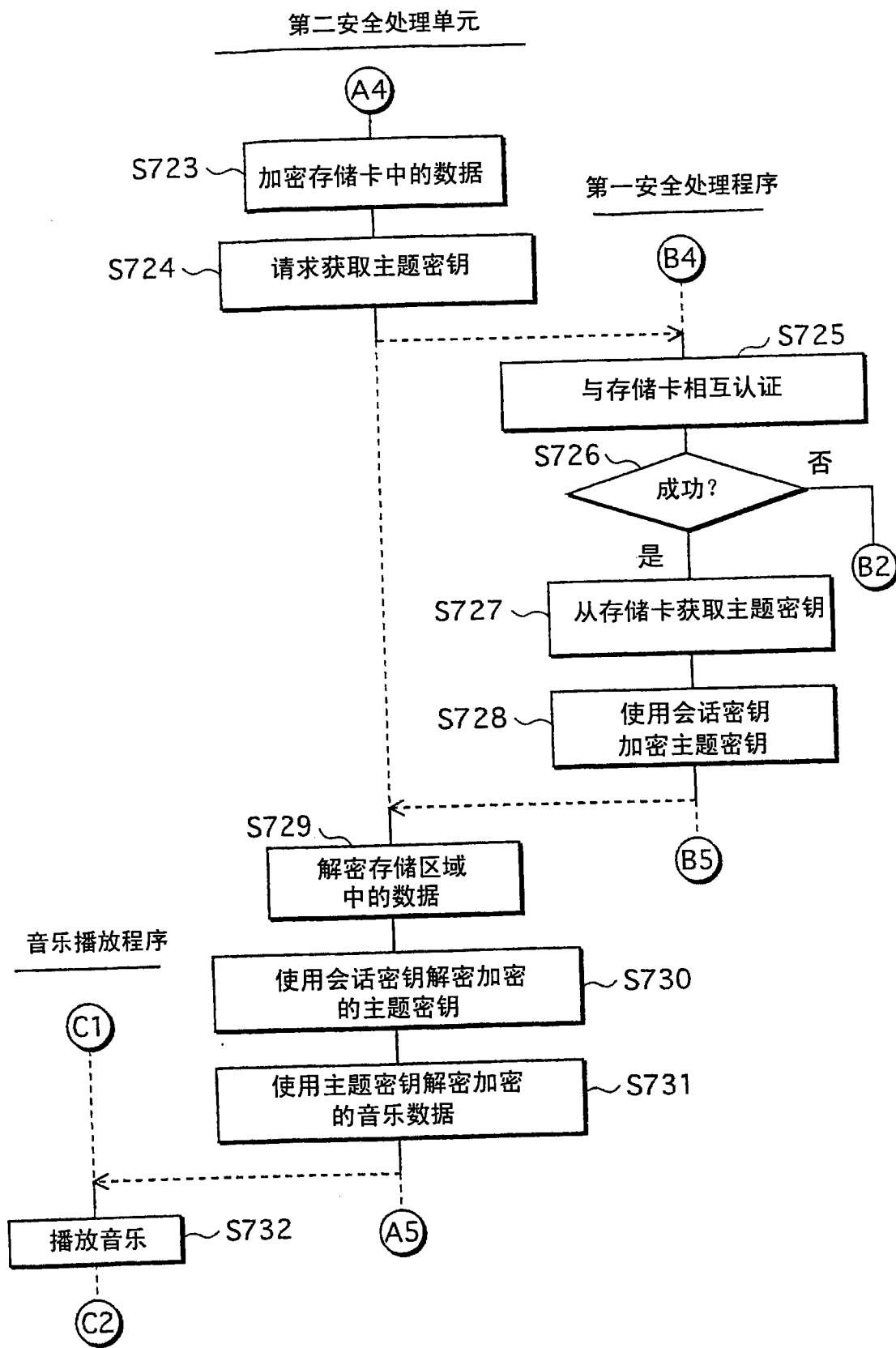


图 16

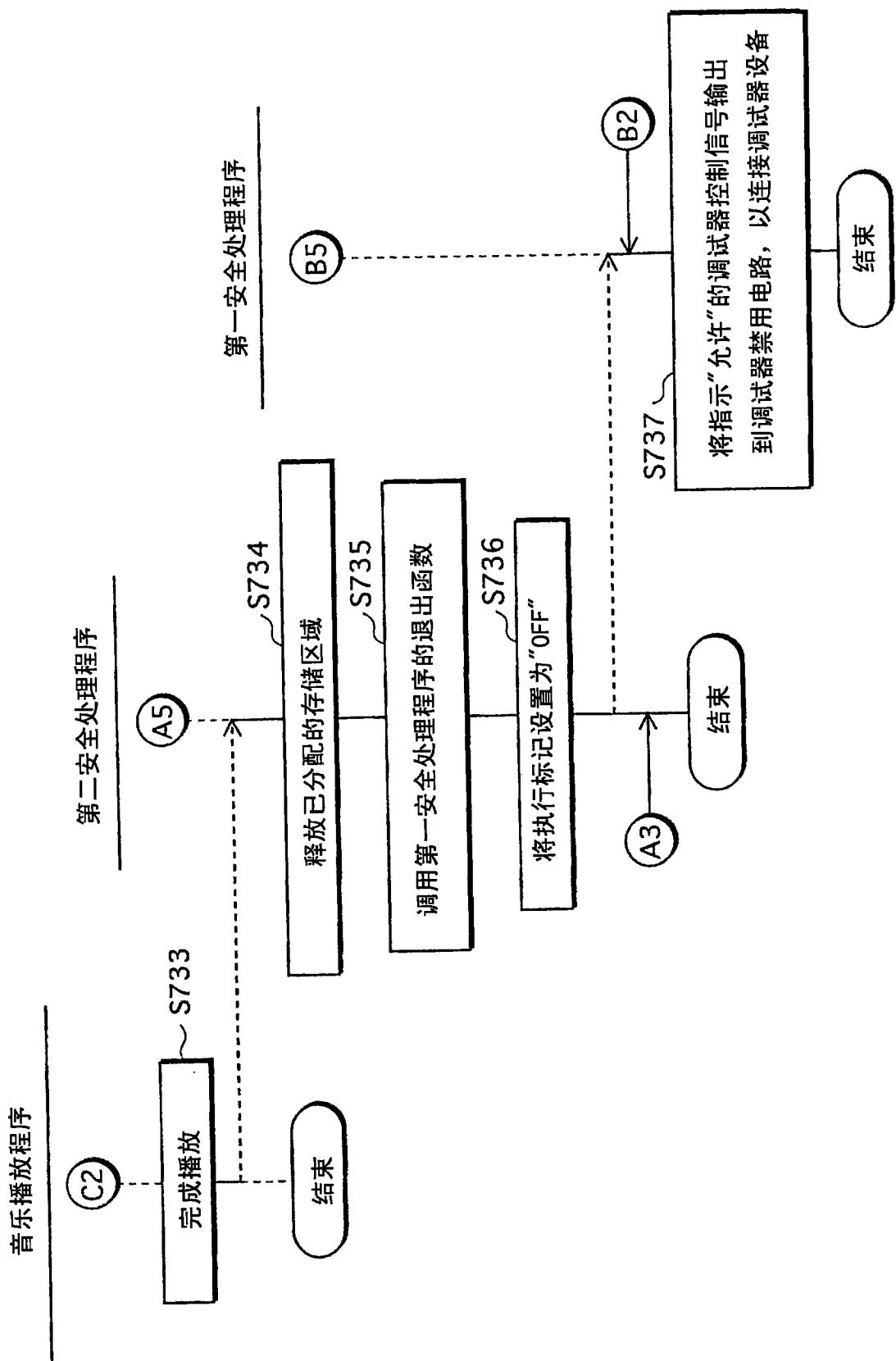


图 17

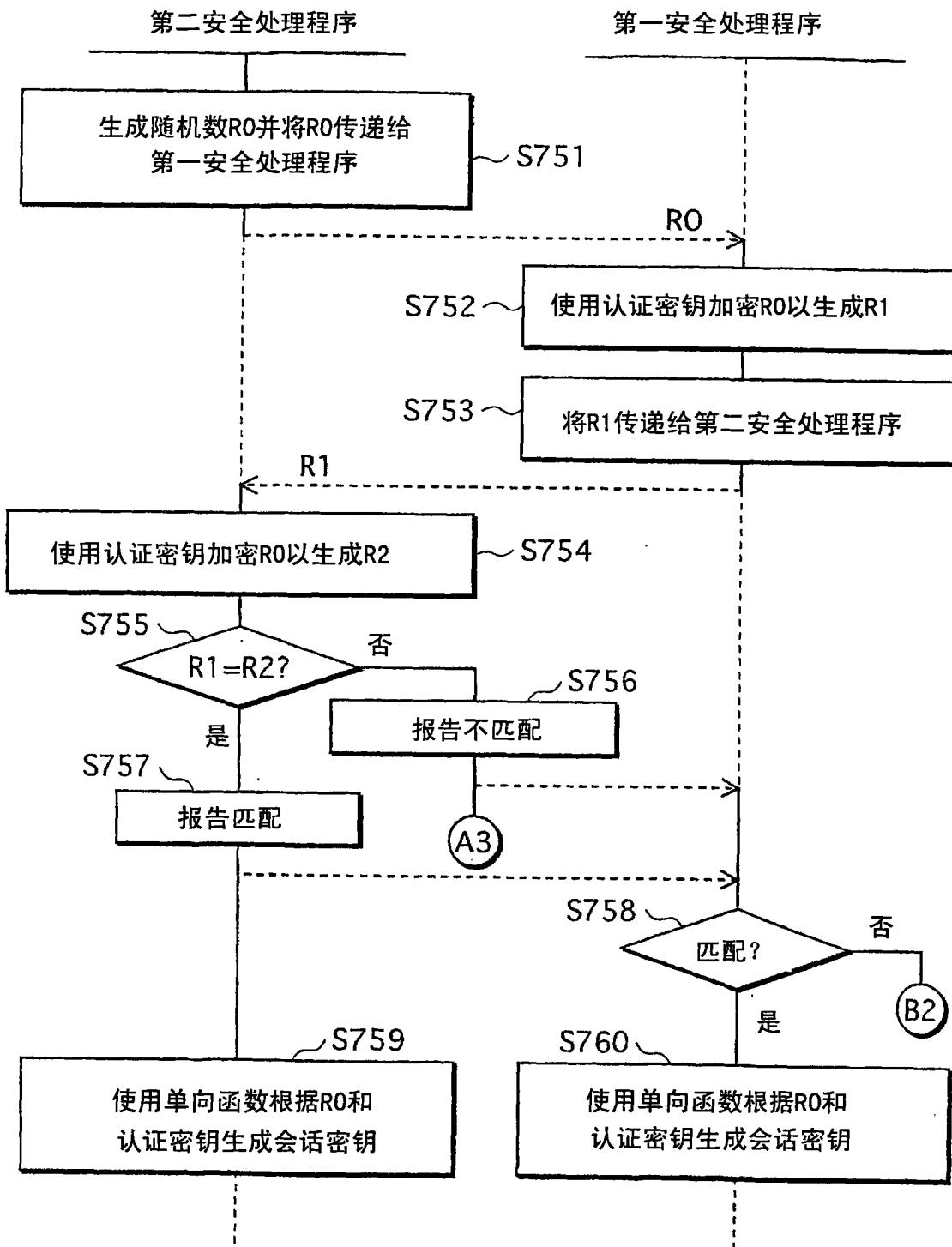


图 18

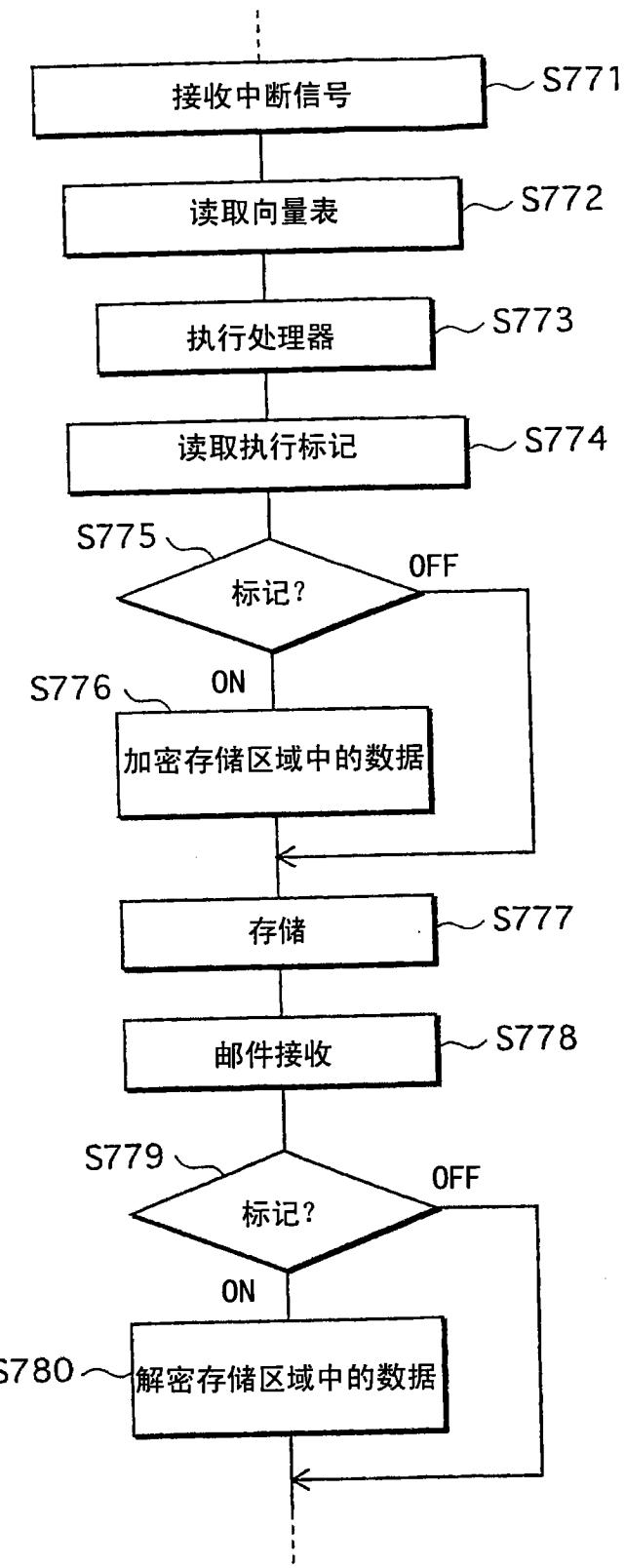


图 19