



(12) 发明专利

(10) 授权公告号 CN 1736056 B

(45) 授权公告日 2011.07.06

(21) 申请号 200380108230.X

(56) 对比文件

(22) 申请日 2003.11.05

US 4521853 A, 1985.06.04, 全文.

(30) 优先权数据

CN 1198062 A, 1998.11.04, 全文.

60/424,381 2002.11.05 US

US 6289455 B1, 2001.09.11, 说明书正文第
11栏第5行至65行、附图2.

10/388,002 2003.03.12 US

US 5852290 A, 1998.12.22, 全文.

10/690,192 2003.10.21 US

US 6278783 B1, 2001.08.21, 全文.

10/691,170 2003.10.22 US

审查员 张霞

(85) PCT申请进入国家阶段日

2005.07.04

(86) PCT申请的申请数据

PCT/US2003/035334 2003.11.05

(87) PCT申请的公布数据

W02004/042995 EN 2004.05.21

(73) 专利权人 索尼电子有限公司

地址 美国新泽西州

(72) 发明人 B·L·坎德洛尔

(74) 专利代理机构 中国专利代理(香港)有限公司 72001

代理人 杨凯 王勇

(51) Int. Cl.

H04L 9/00 (2006.01)

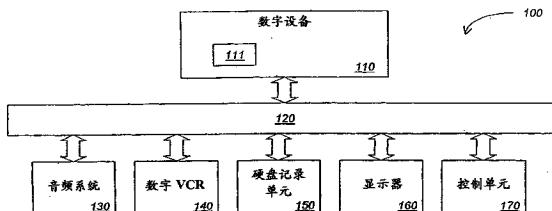
权利要求书 4 页 说明书 20 页 附图 30 页

(54) 发明名称

保护数字内容传送的机构

(57) 摘要

根据一个实施例，解扰器适配器作为集成电路(IC)。该解扰器包括控制字梯形逻辑以在其它数据之中产生控制字，以对输入的加扰内容进行解扰。该解扰器还包括复制保护密钥梯形逻辑，以恢复用于在随后将解扰内容传输到数字设备之前对其进行加密的复制保护密钥。



1. 一种解扰器，包括：

非易失性存储器，存储唯一密钥；

控制字密钥梯形逻辑电路，产生 (i) 基于条件存取随机值和所述唯一密钥生成的第一值，(ii) 使用第一值生成的第二值，以及 (iii) 使用第二值恢复的第三值；

第一密码单元，基于第三值对以加扰格式的输入内容进行解扰；

第二密码单元，使用第一值对输入的加密数据进行解密。

2. 如权利要求 1 所述的解扰器，其中所述解扰器是单个集成电路。

3. 如权利要求 1 所述的解扰器，其中所述解扰器在机顶盒内实现。

4. 如权利要求 1 所述的解扰器，其中第一值是通过使用所述唯一密钥在所述条件存取随机值上执行解密操作所生成的派生密钥。

5. 如权利要求 1 所述的解扰器，其中第一值是通过在所述条件存取随机值和填充数据的组合上执行解密操作所得到的派生密钥，所述组合的长度至少为 128 位。

6. 如权利要求 4 所述的解扰器，其中第二值是通过使用所述派生密钥在配对密钥生成元素上执行解密操作所恢复的配对密钥，所述配对密钥生成元素是包括以下一项或多项的消息：制造商标识符、服务提供商标识符、条件存取提供商标识符和配对密钥序号。

7. 如权利要求 5 所述的解扰器，其中第二值是通过在包括配对密钥生成元素的至少 128 位数据上执行解密操作所恢复的配对密钥，所述配对密钥生成元素是包括以下一项或多项的消息：制造商标识符、服务提供商标识符、条件存取提供商标识符和配对密钥序号。

8. 如权利要求 6 所述的解扰器，其中第三值是通过使用所述配对密钥在加密控制字上执行解密操作所恢复的控制字。

9. 如权利要求 7 所述的解扰器，其中第三值是通过执行以下操作恢复的控制字：(i) 使用所述配对密钥在第一加密控制字和第二加密控制字的第一组合上的第一解密操作；以及 (ii) 使用所述配对密钥在第三加密控制字和多位的第二组合上的第二解密操作，所述多位用长度至少为 128 位的第二组合的填充。

10. 如权利要求 1 所述的解扰器，还包括第三密码单元，以在将解扰的输入内容传输到数字设备之前对其进行加密。

11. 如权利要求 10 所述的解扰器，还包括复制保护梯形逻辑电路，以产生第三密码单元对所述解扰的输入内容进行加密所用的复制保护密钥。

12. 如权利要求 11 所述的解扰器，其中所述复制保护梯形逻辑电路通过使用逻辑派生在一系列随机值和多位上执行解密操作来产生长度至少为 128 位的结果以产生复制保护密钥，所述逻辑派生是所述唯一密钥与预定值的“异或”操作的结果。

13. 一种解扰器，包括：

控制字密钥梯形逻辑电路，产生 (i) 使用唯一密钥从在第一随机值上的密码操作中生成的第一值，(ii) 使用第一值从经历密码操作的配对密钥生成元素中恢复的第二值，以及 (iii) 通过使用第二值对加密控制字进行解密所恢复的控制字；以及

第一密码单元，使用所述控制字对以加扰格式的输入内容进行解扰。

14. 如权利要求 13 所述的解扰器，其中所述解扰器是单个集成电路。

15. 如权利要求 13 所述的解扰器，还包括第二密码单元，以对用所述解扰器实现的数字设备在带外接收的输入加密节目数据进行解密。

16. 如权利要求 15 所述的解扰器,其中所述加密节目数据包括加密授权管理消息,所述加密授权管理消息包括以下至少两项:(i) 智能卡标识符,(ii) 长度字段,(iii) 配对密钥生成元素,(iv) 至少一个密钥标识符以及(v) 与所述至少一个密钥标识符相关联的至少一个密钥。

17. 如权利要求 16 所述的解扰器,其中所述加密授权管理消息的所述配对密钥生成元素是包括以下一项或多项的消息:制造商标识符、服务提供商标识符、条件存取提供商标识符以及配对密钥序号。

18. 如权利要求 13 所述的解扰器,还包括复制保护梯形逻辑电路,以基于多个处理块产生复制保护密钥,其中:

第一处理块,配置为基于第二随机值和所述唯一密钥或所述唯一密钥的逻辑派生来生成派生密钥;

第二处理块,配置为使用所述派生密钥从加密用户密钥中恢复用户密钥;以及

第三处理块,配置为使用所述用户密钥从复制保护密钥生成元素生成复制保护密钥。

19. 如权利要求 18 所述的解扰器,还包括第三密码单元,以在将所述解扰输入内容传输到数字设备之前使用所述复制保护密钥对其进行加密。

20. 如权利要求 18 所述的解扰器,还包括耦合到所述控制字密钥梯形逻辑电路和所述复制保护梯形逻辑电路的一次可编程非易失性存储器,所述非易失性存储器存储所述唯一密钥。

21. 如权利要求 19 所述的解扰器,还包括存储所述复制保护密钥的存储器,所述存储器耦合到第三密码单元。

22. 一种解扰器,包括:

存储器,存储唯一密钥;

控制字密钥梯形逻辑电路,耦合到所述存储器,所述控制字梯形逻辑电路包括:

第一处理块,配置为生成所述唯一密钥的第一派生密钥;

第二处理块,配置为使用第一派生密钥从配对密钥生成元素生成配对密钥;

第三处理块,配置为通过使用所述配对密钥对加密控制字进行解密来恢复控制字;

第一密码单元,耦合到所述控制字密钥梯形逻辑电路,第一密码单元使用所述控制字对以加扰格式的输入内容进行解扰。

23. 如权利要求 22 所述的解扰器,其中所述解扰器是单个集成电路。

24. 如权利要求 22 所述的解扰器,还包括第二密码单元,以对用所述解扰器实现的数字设备在带外接收的输入的加密节目数据进行解密。

25. 如权利要求 24 所述的解扰器,其中所述加密节目数据包括加密授权管理消息,所述加密授权管理消息包括以下至少两项:(i) 智能卡标识符,(ii) 长度字段,(iii) 配对密钥生成元素,(iv) 至少一个密钥标识符,以及(v) 与所述至少一个密钥标识符相关联的至少一个密钥。

26. 如权利要求 22 所述的解扰器,还包括耦合到第一密码单元的复制保护梯形逻辑电路,所述复制保护梯形逻辑电路包括:

第四处理块,配置为基于随机值和所述唯一密钥生成第二派生密钥;

第五处理块,配置为使用第二派生密钥对加密用户密钥进行解密,以恢复用户密钥;以

及

第六处理块，配置为使用所述用户密钥从复制保护密钥生成元素生成复制保护密钥。

27. 如权利要求 26 所述的解扰器，还包括第二密码单元，以在将所述解扰输入内容传输到数字设备之前使用所述复制保护密钥对其进行加密。

28. 一种解扰器，包括：

非易失性存储器，存储多个唯一密钥；

控制字密钥梯形逻辑电路，产生 (i) 基于条件存取随机值和对应的多个唯一密钥而生成的多个派生密钥，(ii) 使用所述多个派生密钥生成的多个配对密钥，以及 (iii) 使用所述多个配对密钥恢复的多个控制字；以及

第一密码单元，基于所述多个控制字中的至少一个对以加扰格式的输入内容进行解扰。

29. 如权利要求 28 所述的解扰器，其中所述多个派生密钥包括：

(i) 第一派生密钥，由接连经历至少三个变换的所述条件存取随机值生成，其中经历所述至少三个变换包括：使用所述多个唯一密钥的第一唯一密钥在所述条件存取随机值上执行第一变换以产生第一结果，使用所述多个唯一密钥的第二唯一密钥在第一结果上执行第二变换以产生第二结果，以及使用所述多个唯一密钥的第三唯一密钥在第二结果上执行第三变换以产生第一派生密钥，

(ii) 第二派生密钥，由所述条件存取随机值和第一预定值生成，经历第一按位逻辑操作以产生第四结果，接着第四结果接连经历至少三个变换，其中经历所述至少三个变换包括：使用第一唯一密钥在第四结果上执行第四变换以产生第五结果，使用第二唯一密钥在第五结果上执行第五变换以产生第六结果，以及使用第三唯一密钥在第六结果上执行第六变换以产生第二派生密钥，以及

(iii) 第三派生密钥，由所述条件存取随机值和不同于第一预定值的第二预定值生成，经历第二按位逻辑操作以产生第七结果，接着第七结果接连经历至少三个变换，其中经历所述至少三个变换包括：使用第一唯一密钥在第七结果上执行第七变换以产生第八结果，使用第二唯一密钥在第八结果上执行第八变换以产生第九结果，以及使用第三唯一密钥在第九结果上执行第九变换以产生第三派生密钥。

30. 如权利要求 28 所述的解扰器，其中所述多个配对密钥包括：

(i) 第一配对密钥，由配对密钥生成元素生成，所述配对密钥生成元素是包括制造商标识符、服务提供商标识符、条件存取提供商标识符以及配对密钥序号中至少一项的消息，接连经历至少三个变换，其中经历所述至少三个变换包括：使用所述多个派生密钥的第一派生密钥在所述配对密钥生成元素上执行第一变换以产生第一结果，使用所述多个派生密钥的第二派生密钥在第一结果上执行第二变换以产生第二结果，以及使用所述多个派生密钥的第三派生密钥在第二结果上执行第三变换以产生第一配对密钥，

(ii) 第二配对密钥，由所述配对密钥生成元素和第一预定值生成，经历第一按位逻辑操作以产生第三结果，接着第三结果接连经历至少三个变换，其中经历所述至少三个变换包括：使用第一派生密钥在第三结果上执行第四变换以产生第四结果，使用第二派生密钥在第四结果上执行第五变换以产生第五结果，以及使用第三派生密钥在第五结果上执行第六变换以产生第二配对密钥，以及

(iii) 第三配对密钥,由所述配对密钥生成元素和不同于第一预定值的第二预定值生成,经历第二按位逻辑操作以产生第六结果,接着第六结果接连经历至少三个变换,其中经历所述至少三个变换包括:使用第一派生密钥在第六结果上执行第七变换以产生第七结果,使用第二派生密钥在第七结果上执行第八变换以产生第八结果,以及使用第三配对密钥在第八结果上执行第九变换以产生第三配对密钥。

31. 如权利要求 28 所述的解扰器,其中所述多个控制字包括:

(i) 第一控制字,由接连经历至少三个变换的第一加密控制字恢复,其中经历所述至少三个变换包括:使用所述多个配对密钥的第一配对密钥在第一加密控制字上执行第一变换以产生第一结果,使用所述多个配对密钥的第二配对密钥在第一结果上执行第二变换以产生第二结果,以及使用所述多个配对密钥的第三配对密钥在第二结果上执行第三变换以产生第一控制字,

(ii) 第二控制字,从第二加密控制字和第一预定值恢复,经历第一按位逻辑操作以产生第三结果,接着第三结果接连经历至少三个变换,其中经历所述至少三个变换包括:使用第一配对密钥在第三结果上执行第四变换以产生第四结果,使用第二配对密钥在第四结果上执行第五变换以产生第五结果,以及使用第三配对密钥在第五结果上执行第六变换以产生第二控制字,以及

(iii) 第三控制字,从第三加密控制字和不同于第一预定值的第二预定值恢复,经历第二按位逻辑操作以产生第六结果,接着第六结果接连经历至少三个变换,其中经历所述至少三个变换包括:使用第一配对密钥在第六结果上执行第七变换以产生第七结果,使用第二配对密钥在第七结果上执行第八变换以产生第八结果,以及使用第三配对密钥在第八结果上执行第九变换以产生第三控制字。

32. 如权利要求 30 所述的解扰器,其中所述第一和第二按位逻辑操作中的至少一个是“异或”操作。

保护数字内容传送的机构

[0001] 相关申请的交叉引用

[0002] 本申请是 2003 年 3 月 12 日提交的申请号为 10/388002 的美国专利申请的部分继续申请, 其要求 2002 年 11 月 5 日提交的申请号为 60/424381 的美国临时专利申请的优先权利益。

技术领域

[0003] 本发明的实施例涉及数字设备。更具体地说, 本发明的一个实施例涉及用于对数字设备 (诸如机顶盒) 中的数字内容进行解扰的系统、装置、解扰器和方法。

背景技术

[0004] 模拟通信系统正迅速给数字通信系统让路。目前正在确定数字电视在全国范围内可用的时间。高清电视 (HDTV) 广播已在大多数主要城市在有限基础上开通了。类似地, 互联网和万维网的急剧增长也导致了可下载视听文件 (诸如 mp3 格式音频文件以及其它内容) 的相关增长。

[0005] 同时, 部分由于向着数字通信系统的这种快速发展, 数字记录设备已取得了重大进步。数字通用光盘 (DVD) 记录器、数字 VHS 盒式录像机 (D-VHS VCR)、CD-ROM 记录器 (例如 CD-R 和 CD-RW)、MP3 记录设备, 以及基于硬盘的记录单元不过只代表能够产生高质量记录和记录复制的数字记录设备, 没有在模拟记录设备中已知的世代退化 (即, 连续复制之间增加的退化)。朝着数字通信系统和数字记录设备发展的结合引起了对诸如动画和音乐产业的内容提供商的关注, 由于担心未经批准而不受控制地复制这种数字内容, 内容提供商不愿提供可下载的数字内容。

[0006] 作为响应, 有这样一个运动, 要求内容提供商 (诸如地面广播、有线和直播卫星 (DBS) 公司以及具有提供可下载内容的网址的公司) 引入复制保护方案。这些期望的复制保护方案扩展到条件存取 (CA) 的作用 (其只将内容解扰为用于实时观看和 / 或收听的 CA 清除格式) 之外, 并且现在包括对记录和回放的约束和条件。

[0007] 用于脉冲式按次付费 (IPPV) 的传统 CA 系统源自单向广播系统。通常用信息和功能性注入条件存取单元 (诸如机顶盒) 中的密码处理器 (诸如智能卡), 以便自动准许存取节目。例如, 具有付费电视存取控制应用的智能卡适于接收准许某些服务授权的消息。如果允许机顶盒观看 IPPV 节目, 则还传输信用和费用限制信息。同样, 当调到某节目时, 智能卡接收描述该智能卡需要哪些授权的消息, 以便准许存取该节目。

[0008] 目前, 黑客已经操纵了两种类型的消息, 以便观看节目而无需付必要的定金。不仅可以操纵这些消息, 而且还可以攻击硬件。例如, 可畅行无阻地复制用于对加扰内容进行解扰的解扰密钥, 并在互联网上将其发送给其它机顶盒。对内容提供商和内容所有者而言, 这种剽窃是损失惨重的。

附图说明

- [0009] 在附图中通过示例而非限制性的方式示出了本发明的实施例，其中相同标号指示相同元件，附图中：
- [0010] 图 1 是包括数字设备的内容传送系统的示范性实施例；
- [0011] 图 2 是包括适于用智能卡操作的条件存取单元的安全内容传送系统的第一示范性实施例；
- [0012] 图 3 是用于将解扰密钥从智能卡安全传输到图 2 的条件存取单元的方法的示范性实施例；
- [0013] 图 4 是包括适用于经由网络连接的头端的解码器的安全内容传送系统的第二示范性实施例；
- [0014] 图 5 是适用于图 4 的头端的解码器的更详细说明；
- [0015] 图 6A 是安全内容传送系统的第三示范性实施例；
- [0016] 图 6B 是形成通过安全内容传送系统传输的配对密钥生成器的数据结构的示范性实施例；
- [0017] 图 6C 是路由到图 6A 系统的机顶盒的授权管理消息 (EMM) 的示范性实施例；
- [0018] 图 7 是在图 6A 系统的机顶盒的解码器内实现的解扰器的示范性实施例；
- [0019] 图 8 是安全内容传送系统的第四示范性实施例；
- [0020] 图 9A 是安全内容传送系统的第五示范性实施例；
- [0021] 图 9B 是路由到图 9A 系统的机顶盒的授权管理消息 (EMM) 的示范性实施例；
- [0022] 图 9C 是与路由到图 9A 系统的机顶盒的电子节目指南 (EPG) 相关联的元数据的示范性实施例；
- [0023] 图 10 是在图 9A 的机顶盒内实现的解扰器的示范性实施例；
- [0024] 图 11 是安全内容传送系统的第六示范性实施例的一部分；
- [0025] 图 12 是安全内容传送系统的第七示范性实施例的一部分，其中用复制保护功能适应数字设备；
- [0026] 图 13 是在图 12 的数字设备内实现的解码器的示范性实施例；
- [0027] 图 14 是形成图 12 的复制保护密钥生成器的数据结构的示范性实施例；
- [0028] 图 15 是在数字设备内实现的解扰器的另一示范性实施例；
- [0029] 图 16 是图 15 的解扰器的控制字 (CW) 密钥梯形逻辑的示范性实施例；
- [0030] 图 17A-17C 是图 16 的 CW 密钥梯形逻辑的第一处理块的示范性实施例；
- [0031] 图 18A-18C 是图 16 的 CW 密钥梯形逻辑的第二处理块的示范性实施例；
- [0032] 图 19A-19C 是图 16 的 CW 密钥梯形逻辑的第三处理块的示范性实施例；
- [0033] 图 20 是图 15 的解扰器的复制保护 (CP) 密钥梯形逻辑的示范性实施例；
- [0034] 图 21A-21C 是图 20 的 CP 密钥梯形逻辑的第四处理块的示范性实施例；
- [0035] 图 21A-21C 是图 20 的 CP 密钥梯形逻辑的第五处理块的示范性实施例；
- [0036] 图 22A-22C 是图 20 的 CP 密钥梯形逻辑的第六处理块的示范性实施例；
- [0037] 图 23A-23C 是图 15 的解扰器的数据解密逻辑的示范性实施例；以及
- [0038] 图 24 是图 15 的解扰器的实施例；
- [0039] 图 25 是图 24 的解扰器的更详细的实施例。

具体实施方式

[0040] 本发明的各种实施例涉及用于保护数据传送的解扰器。在一个实施例中，这种保护包括对完全在可配置为单个集成电路的解扰器内来自一个或多个内容提供商的数字内容进行解扰和 / 或解密。“内容提供商”的例子包括（但不限于）地面广播公司、有线电视运营商、直播卫星（DBS）公司、提供经由互联网下载的内容或任何类似内容资源的公司。

[0041] 在以下描述中，特定术语用于描述本发明的特征。例如，术语“部件”和“逻辑”都表示配置为执行一个或多个功能的硬件和 / 或软件。“硬件”的例子包括（但不限于）诸如处理器（例如微处理器、专用集成电路、数字信号处理器、微控制器等）的集成电路、有限状态机、组合逻辑等。

[0042] 术语“逻辑派生”是通过对数字信号执行逻辑操作（例如异或“XOR”、与、或、反转，或其任意组合）产生的结果。虽然可设想同时在多位上执行逻辑操作，但可以按位方式执行逻辑操作。

[0043] 术语“处理块”表示具有专用功能（诸如有限状态机）的硬件和 / 或软件。“软件”的例子包括以应用程序、小应用程序、乃至例程形式的一系列可执行指令。软件可存储在任何类型的机器可读媒体（诸如可编程电路）、半导体存储设备（诸如易失性存储器（例如随机存取存储器等）和 / 或非易失性存储器（例如任何类型的只读存储器“ROM”、闪速存储器）、软盘、光盘（例如压缩盘或数字视盘“DVD”）、硬驱动盘、磁带等）。

[0044] 参考图 1，其示出了内容传送系统 100 的示范性实施例。内容传送系统 100 包括接收来自一个或多个内容提供商的包括节目数据的信息的数字设备 110。节目数据例如可作为数位流传播。数字设备 110 可操作为许多电子产品（或其中集成的一个或多个部件），诸如机顶盒、电视机、计算机、音频回放设备（例如数字无线电、MP3 播放器）、音频记录设备、视频记录设备（例如数字记录器）等。

[0045] 例如，可根据嵌入式结构、分离安全结构或外部安全结构来配置数字设备 110。在一个实施例中，作为嵌入式结构，数字设备 110 实现为机顶盒或包括支持授权管理和解扰操作的固定内部电路的另一电子产品。

[0046] 备选地，根据分离安全结构实施例，数字设备 110 可适于接收处理授权管理的可移动智能卡，而数字内容的解扰受内部电路控制。

[0047] 然而，根据外部安全实施例，数字设备 110 可以是具有通过在带外频道上发送和接收消息来处理授权管理和解扰操作的网卡的“配置点”产品。当然，外部安全类型还可被划分以使网卡处理解扰操作，但适于与处理授权管理的智能卡通信。可实现数字设备 110 的这些和其它实施例，同时仍落在本发明的精神和范围内。

[0048] 数字设备 110 包括接收器 111，该接收器处理输入信息、从其中提取包括数字内容的节目数据、并提供可感觉格式（例如可视和 / 或可听）的数字内容。“节目数据”包括以下任一项或全部：系统信息、授权控制消息、授权管理消息或数字内容。节目数据流中的“数字内容”可包括图像、音频、视频或其中任意组合。内容可以是加扰或清除格式。

[0049] 这里，“系统信息”可包括关于节目名称、广播时间、来源、检索和解码方法、以及复制管理命令的信息，其中复制管理命令给数字接收器和其它设备提供将控制可以如何以及何时重放、转播和 / 或记录数字内容的信息。这些复制管理命令还可与授权控制消息（ECM）

一起传输,该授权控制消息通常用于调整存取特定频道或服务。“授权管理消息”(EMM)可用于将授权(有时称为“特权”)传送到数字接收器111。某些授权的例子可包括(但不限于)存取权或解扰密钥。解扰密钥通常是解扰逻辑基于准许的授权来不受阻碍地从加扰格式中恢复数据所需的代码。

[0050] 如所示,当实现为机顶盒时,数字设备110可经由传输媒体120耦合到内容传送系统100中的其它部件。传输媒体120操作上在数字设备110与内容传送系统100中的其它部件之间传输节目数据。传输媒体120可包括(但不限于)电线、光纤、电缆、由无线信令电路建立的无线链路等。

[0051] 根据对应数字设备110的产品类型,内容传送系统100可包括耦合到传输媒体120的音频系统130。数字VCR140(诸如D-VHS VCR)还可通过传输媒体120耦合到数字设备110和内容传送系统100的其它部件。

[0052] 硬盘记录单元150还可经由传输媒体120耦合到数字设备110和其它部件。显示器160可包括高清电视显示器、监视器或能够处理数字视频信号的其它设备。最后,控制单元170可耦合到传输媒体120。控制单元170可用于协调并控制内容传送系统100上的某些或每一个部件的操作。

[0053] 可以加扰形式传输节目数据的数字内容。在一个实施例中,作为一部分节目数据,可将存取需求与加扰内容一起传输到数字设备110(例如机顶盒),该数字设备用接收器111实现,从而用作条件存取单元。“存取需求”是限制性参数,用于为了观看和收听而确定是否批准用条件存取功能性实现的数字设备110(下文称“条件存取单元110”)对加扰的内容进行解扰。例如,存取需求可以是感觉(观看和/或收听)内容所需的密钥、与给定内容提供商相关联的服务标签、乃至特定的解扰软件代码。

[0054] 当条件存取单元110接收加扰节目时,节目的存取需求与条件存取单元110实际具有的授权相比较。为了使条件存取单元110以清除形式显示加扰内容,在一个实施例中,与数字内容相关联的存取需求与条件存取单元110的授权相比较。该授权可规定条件存取单元110有权观看/回放来自给定内容提供商(诸如家庭售票处(HBO))的内容。该授权还包括对数字内容解扰所需的一个或多个密钥。该授权还可定义条件存取单元110可对数字内容进行解扰的周期。

[0055] 因此,在一个实施例中,存取需求和授权形成一部分存取控制系统,以确定是否批准条件存取单元乃至解码器观看特定节目。可设想以下描述集中在恢复音频/视觉内容(诸如电视广播、购买的电影等)的机构。然而,可设想本发明还适于仅对可听内容(例如数字化音乐文件)进行解扰。

[0056] 存取需求和授权可给消费者提供用于为内容付费并有权使用加扰内容的各种选择。这些选择可包括即时付费(PPP)、按次付费(PPV)、脉冲式按次付费(IPPV)、基于时间的历史、按时付费(PPT)。“脉冲式按次付费”的特征是,允许通过之前已下载到机顶盒的信用来购买PPV电影。可通过电话来存储购买记录,并将其转发到计费中心。“基于时间的历史”允许存取在过去一段时间(诸如1997年3月至12月)期间传送的内容。存取需求和授权还可给消费者提供用于存储加扰内容的不同选项。

[0057] 可使用包标识符(PID)将存取需求传送到位于数字设备110内或通过传输媒体耦合到此的条件存取单元。各PID可包含与给定服务相关联的存取需求。传送到条件存取单元的

内容还可包括大量 PID, 从而使特定收入特征、技术特征或其它特定特征能被本地执行。

[0058] 在接收内容之前, 可给用户有权使用将存储到媒体的数字内容的多个选择。可要求用户购买存取和观看内容的权利。因此, 如果用户希望记录该内容以便随后检索和观看, 则还需将用户购买的存取需求与数字内容一起存储。

[0059] 此外, 如图 12 和 13 所示, 可存在应用到解扰数字内容 (例如传输流) 的复制保护。通过互连目标接口与源接口的接口, 将对复制保护数字内容重新加扰。源和目标接口必须对用于对这个内容进行重新加密的密钥的意见一致。可用与数字设备相关联的唯一密钥来加密这个复制保护密钥。可通过 EMM 或其它方法 (例如工厂加载过程) 来接收唯一密钥。

[0060] 如图 2 所示, 其示出了安全内容传送系统的第一示范性实施例, 该系统包括适于用智能卡接口 220 操作的条件存取单元 201。该实施例与分离安全结构以及外部安全结构一致。在分离安全结构实现中, 数字设备 110 操作为条件存取单元 201 (例如, 相当于图 1 的条件存取单元 110), 但实现为机顶盒或其它类型的数字设备。

[0061] 虽然可将智能卡接口 220 嵌入数字接收器 111 中, 但希望数字接收器 111 具有扩展插槽 (诸如 PCMCIA 插槽或通用串行总线 (USB) 插槽), 以接收补充接口 220 的智能卡 210。对于该实施例, 数字接收器 111 包括可选处理器 230 和解扰器 240。这里, 对于本实施例, 解扰器 240 实现为集成电路 (IC)。

[0062] 智能卡接口 220 适于附在智能卡 210 上, 该智能卡存储用于对输入的数字内容进行解扰的一个或多个加密解扰密钥。智能卡 210 将加密形式的解扰密钥传输到智能卡接口 220。为了保护解扰密钥 (通常称为“DK”) 不被在监视智能卡 210 与智能卡接口 220 之间通信的闯入者不正当地提取, 智能卡 210 可使用对条件存取单元 201 唯一的加密密钥来对 DK 进行加密。这允许条件存取单元 201 可以安全方式对 DK 解密, 并用清除格式的 DK 对数字内容进行解扰。

[0063] 更具体地说, 根据本发明的一个实施例, 智能卡 210 的外部密码处理器 215 接收对内容进行解扰所需的 DK。之前用一个或多个用于对 DK 加密的密钥来加载存储元件 212 (例如易失性或非易失性存储器)。当存储元件 212 在片上时, 可在智能卡 210 制造期间、存储元件 212 的制造期间或由密码处理器 215, 执行这种加载。智能卡 210 的加密逻辑 214 用对解扰器 240 唯一的一个或多个密钥对 DK 加密。

[0064] 对于这个实施例, 智能卡 210 将加密 DK 216 传送到解扰器 240。这里, 虽然可直接将加密 DK 216 发送到解密逻辑 260, 但处理器 230 通过接口 220 接收加密 DK 216。可实现处理器 230 执行附加操作, 以抵消在 DK 上执行的附加困惑 (obfuscation) 技术。

[0065] 解扰器 240 的解密逻辑 260 将使用存储元件 250 中存储的一个或多个唯一密钥对 DK 解密。在一个实施例中, 存储元件 250 包括一个或多个密钥寄存器, 该寄存器是通过传输到条件存取单元 201 的初始节目数据在制造时或在条件存取单元 201 内实现之后加载的。然后解密逻辑 260 交替地将解密的 DK 写入解扰器逻辑 270 的“奇”和“偶”密钥存储元件 (未示出) 中。

[0066] 然后解扰器逻辑 270 在适当时间将“奇 / 偶”解扰器密钥应用到输入的加扰内容 280, 并输出解扰节目内容 290。当然, “奇”和“偶”密钥存储元件加载的备选可用于对输入的加扰内容 280 进行解扰。解扰器逻辑 270 可作为解扰器 240 的内部逻辑实现或外部实现 (如说明性示出的)。

[0067] 因此,从智能卡 210 到条件存取单元 201 传送解扰密钥是安全的,因为是以加密形式传送解扰密钥的。在条件存取单元 201 中,解扰密钥保持安全,因为解扰密钥没被非安全处理器 230 解密。只在实际使用解扰密钥的解扰器 240 中对解扰密钥进行解密,并且因此决不会毫无阻碍地暴露解扰密钥,且不可能被黑客获取。

[0068] 此外,用于对加密的 DK 216 进行解密的密钥存储在解扰器 240 的硬件(例如存储元件 250)中。除非探测到存储元件 250 的硅,否则不可能窃取存储元件 250。此外,由于智能卡 210 使用对于相关条件存取单元 201 唯一的密钥来对 DK 加密,所以该密钥仅适用于一个特定条件存取单元 201,且不可能被其它单元使用以对加密的 DK 216 解密。因此,加密 DK 216 到条件存取单元 201 的传输是安全的。

[0069] 解扰器 240 处理解扰密钥的安全处理。这个解扰器 240 没有 CPU、没有固件且没有软件。没有复杂的密钥分级。基于非处理器的解扰器 240 接收加密 DK 216,将唯一密钥应用到该加密 DK,并对其进行解密。没有指令、没有代码、没有散列(hash)法且没有软件加载到解密逻辑 260 中。完全通过解密逻辑 260(其是硬件电路或状态机)只使用单个密钥函数来执行解密。

[0070] 可在制造期间或在机顶盒、电视机或 NRSS-B 模块内实现期间,将一个或多个唯一密钥(这里通常称为“唯一密钥”)编程到存储元件 250 中。例如,在一个实施例中,用可编程非易失性存储元件 250(诸如闪速存储器)实现解扰器 240。在另一实施例中,用仅可写一次的非可编程非易失性存储器实现解扰器 240,以便增强安全性。结果,决不会不正当读取或改写最初加载到存储元件 250 中的唯一密钥。可以记录条件存取单元 201 的序列号与加载到条件存取单元 201 的解扰器 240 中的唯一密钥之间的联系。

[0071] 当制造条件存取单元 201 并安装智能卡 210 时,智能卡 210 可在配对时接收与条件存取单元 201 相关联的唯一密钥。从那时起,智能卡 210 就配对到那个特定主机(例如条件存取单元 201)。随后,如果曾经替换智能卡 210 或移到新主机,则智能卡 210 可适于经由授权管理消息(EMM)接收与该新主机相关联的唯一密钥。当然,作为备选,也可将具有新编程的唯一密钥的新智能卡传给用户。

[0072] 图 3 中示出了用于将解扰密钥从智能卡 210 传输到图 2 的条件存取单元 201 的示范性方法。在智能卡中使用智能卡的非易失性存储器中存储的密钥对解扰密钥进行加密(块 300)。智能卡中存储的这个密钥(即唯一密钥)与解扰器的存储元件中存储的密钥相关联。从智能卡中接收加密的解扰密钥(块 310)。

[0073] 这个方法包括接收解扰器中包括节目数据的数位流,其中节目数据包括系统信息和加扰数字内容(块 320)。使用解扰器的存储元件中存储的密钥对加密的解扰密钥进行解密(块 330)。在解扰器中使用解密的解扰密钥对加扰的数字内容进行解扰(块 340),并输出解扰的数字内容(块 350)。

[0074] 作为图 2 的条件存取单元实现的备选实施例,可用单向或双向网络 420 的头端服务器(以下称为“头端”)410 代替智能卡,如图 4 中所示。头端 410 维持操作为解码器(例如“解码器”401)的数字设备的存取权,而不是维持图 2 的智能卡 210 的本地密码处理器 215 中的这种存取权。

[0075] 头端 410 可基于解扰器 440 中存储的唯一密钥传送一个或多个服务密钥(通常称为“服务密钥”)。加密服务密钥可本地存储在解码器 401 中,以便于从一个频道到另一频

道的转换。服务密钥以加密形式存储，并按需要加载到解扰器 440 中。在解扰器 440 内通过使用解扰器 440 的存储元件 450 中存储的唯一密钥对服务密钥解密。

[0076] 在本发明的一个实施例中，服务密钥用作对内容进行直接解扰的解扰密钥。在本发明的另一实施例中，服务密钥用于对一个或多个解扰密钥进行解密，其中在带内接收该解扰密钥和加扰内容，并随后用于解扰目的。可使用不同的公共和专用加密算法对服务密钥的每个密钥加密。这些不同的专用算法可看作是使“克隆”硬件无效的任何剽窃措施。

[0077] 头端 410 可在 EMM 中在频道或“服务等级”基础上传送服务密钥。服务密钥被加密，并被本地存储在解码器 401 中，并在转到不同频道时根据需要由处理器 430 使用。虽然本实施例工作在单向（非 IPPV）广播网络中，但本实施例也在双向、交互式网络中执行，在该网络中请求特定服务的服务密钥，诸如 IPPV 或 VOD 购买或任何其它非预订服务。由于是头端 410 而非本地控制密码处理器执行准许存取新服务的能力，所以返回频道 421 用于请求服务密钥。

[0078] 为了避免在头端 410 由 IPPV 节目的大量同时即兴购买引起的超载问题，可以确定自由预览期，并可在实际观看之前销售 IPPV 节目。在本实施例中，可由解码器 401 请求并提早传送个人表演或电影的服务密钥。例如，诸如具有返回频道 421（诸如 DOCSIS 调制解调器或带外传输器 / 接收器）的有线系统的交互式网络，可将节目密钥（RPK）消息的请求从解码器 401 传送到头端 410。备选地，解码器 401 可为每个存取的节目实时请求服务密钥。

[0079] 头端 410 上的控制器（未示出）处理 RPK 消息。RPK 消息可包含解码器 401 的地址以及标识要观看的频道所需的信息（所有这些可从运动图象专家组“MPEG”系统获得，且节目信息已由不安全处理器处理）。如果需要，可对 RPK 请求进行加密，用于拒绝服务攻击的认可和预防，诸如 IPPV 或 VOD 请求。

[0080] 一旦接收到 RPK 消息，头端 410 就存取存取控制列表（其列出解码器 401 的各授权）的项目，并检验解码器 401 被批准接收特定服务密钥。如果批准，则头端 410 将服务密钥（使用位于解扰器 440 中的存储元件 450 中包含的唯一密钥加密的）发送到解码器 401。

[0081] 图 5 提供了适于头端 410 请求并接收服务密钥的图 4 的解码器 401 的更加详细说明。根据本发明的一个实施例，由内容提供商将节目数据 500（诸如与电子节目指南（EPG）相关的授权控制消息（ECM）或元数据）提供给解码器 401。节目数据 500 适于传送至少期望频道或服务的标识符（称为“频道或服务 ID”）。在节目数据 500 是 IPPV 或 VOD 节目的情况下，节目数据 500 还可包括节目标识符（PID）。

[0082] MPEG 多路分配器 510 操作为提取频道或服务 ID 的消息处理器。频道或服务 ID 被路由到处理器 430，该处理器与传输器 / 接收器逻辑 520 共同生成 RSK 消息 421，用于在返回频道 421 上路由到头端 410。

[0083] 作为响应，传输器 / 接收器逻辑 520 接收加密形式的请求的服务密钥（SK），该传输器 / 接收器逻辑将 SK 提供给处理器 430。处理器 430 可将 SK 存储在存储器 435 中，和 / 或将 SK 提供给解扰器 440，用于对输入的加扰内容进行实时解扰。例如，如果希望本地存储 SK，则存储器 435 是所用的可选部件。

[0084] 一旦接收到节目数据的加扰内容，解扰器 440 就对这种内容解扰，如果用 MPEG 格式压缩该内容，则随后将该内容提供给 MPEG 解码器 530。MPEG 解码器 530 将数字内容解压

缩，并随后将解压缩的数字内容路由到用于在电视上显示的数模 (D/A) 转换器、数字视频接口 (DVI) 链路或网络接口（例如 IEEE 1394 链路）。

[0085] 如所示，可在通过总线跟踪或另一通信方案（例如有线、光纤等）互连的两个或多个集成电路上实现处理器 430、存储器 435、解扰器 440、MPEG 多路分配器 510、传输器 / 接收器逻辑 520 和 MPEG 解码器 530。备选地，可在单个集成电路上实现这些部件。

[0086] 在本实施例中，SK 可在某一时段有效。解码器 401 可将 SK 存储在存储器 435 中，允许解码器 401 在 SK 仍然有效的情况下重新存取服务，而不必再次请求那个服务密钥。在本实施例中，SK 以加密形式（由于它来自网络上的头端 410）存储在存储器 435 中。

[0087] SK 可在节目的持续时间内有效，或可在选择的时段（例如 6 小时）内有效。在较长时段使用密钥会降低解码器 401 与头端 410 之间业务的总量，因为一旦 SK 存储在解码器 401 的存储器 435 中，就容易得到它。根据当前服务密钥（例如 SK）的持续时间，可将下一服务密钥 (SK_{next}) 与 SK 一起传送。备选地，在检测到 SK 的有效出现时间（例如 SK 的持续时间）结束之后，解码器 401 可请求 SK_{next} 。在不同的实施例中，服务密钥可在用户的预订期的持续时间内有效。

[0088] 可照单销售或作为包来销售服务。有几个服务等级，每个都由服务 ID 标识。例如，可有基本服务等级、提供更多服务的中等等级、以及提供不同保费服务的高级等级。可给每个递增的服务等级一个单独的服务密钥。

[0089] 总之，图 4 的解码器 401 包括解扰器 240，该解扰器具有在解码器的 IC 制造或创建期间加载的唯一密钥。服务密钥被传送到由唯一密钥加密的解码器 401，并以加密形式存储在解码器 401 中。备选地，每当解码器 401 调到某一频道时，解码器 401 就可请求服务密钥，而无需本地存储服务密钥。

[0090] 由控制管理机构（诸如图 4 的头端 410 中的密钥服务器）保持通常由图 2 的安全密码处理器保持的授权。解码器 401 中的处理器 430 可接收消息（例如 ECM 或 EMM），该消息告诉它批准它对什么进行解扰，以使该处理器可正确地向观众显示观看选项。然后处理器 430 可以为选择的频道请求服务密钥。

[0091] 没有嵌入式的“安全”固件或软件。使用上述硬件解密电路，不需要执行密码函数的嵌入式处理器核心或固件。这允许多个条件存取应用，其可下载到不安全处理器。服务密钥是加密的单元密钥。它可以是公共非对称密钥或秘密对称密钥。

[0092] 额外的优点包括付费电视应用，无需通过给具有解扰器 440 的解码器 401 提供硬连接在此的唯一密钥来使用密码处理器。解码器 401 可请求来自网络提供商的服务密钥或解扰密钥。由于在解扰器 440 中隔绝了关键“安全”功能，所以处理器 430 可执行本地存取控制。

[0093] 现在参考图 6A，其示出了安全内容传送系统 600 的第三示范性实施例。安全内容传送系统 600 包括用户管理系统 610、条件存取 (CA) 控制系统 620、与不同数字设备（例如机顶盒）制造商 630₁-630_N ($N \geq 2$) 相关联的多个配对密钥服务器、以及适于接收智能卡 650 的数字设备（例如机顶盒）640。智能卡 650 与解扰器 660 通信，解扰器 660 包括配置为存储机顶盒 640 的唯一密钥（称为“唯一密钥”）680 的本地存储器 670。在机顶盒 640 的 IC 制造或创建期间，加载唯一密钥 680。

[0094] 一旦机顶盒 640 的用户期望接收特定节目数据，机顶盒 640 就确定是否已在此存

储了与请求的节目数据相关的授权。如果没存储该授权，则可通过屏幕显示通知用户，并提示用户发出请求 611。用户可经由以下通路提供请求 611：(i) 带外通信通路（例如互联网上的电子邮件、用户的电话呼叫等）；或 (ii) 到与所示机顶盒 640 通信的 CA 控制系统 620 的带内通信通路。备选地，可自动发送请求 611，或可将其路由到 CA 控制系统 620，该 CA 控制系统执行信息查找以基本上实时地批准用户。

[0095] 对于一个实施例，请求 611 是包括请求内容的标识符（例如字符或数字代码）、机顶盒的序列号（称为“STB 序列号”）和 / 或智能卡 650 的标识符（称为“智能卡 ID”）的消息。实现为任何信息处理系统（例如服务器、中继站或由服务提供商或内容提供商控制的其它装置），用户管理系统 610 处理请求 611，并确定要给机顶盒 640 提供什么授权。虽然未示出，但可设想将 CA 控制系统 620 配置为执行包含机顶盒序列号或智能卡 ID 的数据库的查找，从而取消存取用户管理系统 610。

[0096] 一旦从用户管理系统 610 接收到批准 (AUTH) 消息 612，其中该消息可包括 STB 序列号和可能全局密钥（例如用于对在带内与内容一起发送的 ECM 进行解密的密钥），CA 控制系统 620 就将 STB 序列号 641 和配对密钥生成器 621 路由到配对密钥服务器 630₁、...、或 630_N（通常称作“配对密钥服务器 630_i”，其中 $i \geq 1$ ）中的至少一个。CA 控制系统 620 操作为协调配对密钥 622 的传送的媒介，该配对密钥用于从下载的加扰内容中恢复数字内容。CA 控制系统 620 可实现为头端、广播站、卫星上行链路等。

[0097] 备选地，代替 CA 控制系统 620 将配对密钥生成器 621 和 STB 序列号 641 路由到配对密钥服务器 630₁-630_N，可设想这种信息可发送到可信第三方 635，该第三方维持并控制存取以配对密钥为特征的数据库。与配对密钥生成器 621 和 / 或 STB 序列号 641 相关联的值用于检索配对密钥 622。“可信第三方”635 可包括（但不限于）政府实体、独立于任何制造商管理的公司等。

[0098] 在传输 STB 序列号 641 和配对密钥生成器 621 之前，CA 控制系统 620 可用选择的配对密钥服务器（诸如服务器 630₁）执行验证方案，以便在 CA 控制系统 620 和配对密钥服务器 630₁ 之间建立会话密钥。当然，如果代替配对密钥服务器 630₁ 实现验证方案，则将用可信第三方执行该验证方案。会话密钥可用于对各方之间交换的信息进行加密，以便提供其间的安全链路。各种类型验证方案的例子包括数字证书、数字签名、散列值等的交换。

[0099] 如图 6B 所示，配对密钥生成器 621 是包括以下一项或多项的消息：机顶盒制造商标识符 (STB 制造商 ID) 623、服务提供商 ID 624、条件存取 (CA) 提供商 ID 625 和配对密钥序号 626。当然，可改变这些值 / 字段的大小（以位为单位）。

[0100] 对于本实施例，“STB 制造商 ID”623 是标识机顶盒 640 的制造商的预定值。当然，可设想 STB 制造商 ID 623 是可选的，取决于 STB 序列号 641 的特定排列。“服务提供商 ID”624 是标识通信系统提供商以及选择的分配机构的值（例如一位或多位，诸如 16 位）。例如，服务提供商 ID 624 可标识哪个有线、卫星、地面或互联网公司正在提供请求的节目数据和 / 或那个公司的特定头端服务器。“CA 提供商 ID”625 表示 CA 控制系统 620 的提供商。如果配对密钥 622 的长度大于一个包，则“配对密钥序号”626 用于重新安排信息包，并且在某些系统中，还可用于指示配对密钥生成器 621 的到期。

[0101] 往回参考图 6A，STB 序列号 641 可具有用于各 STB 制造商 ID 623 的唯一部分，以便标识请求存取的配对密钥服务器 630₁、...、630_N（或可信第三方 635 的数据库）。备选地，

STB 序列号 641 可扩展到包括机顶盒 640 的序列号以及代码字段, 以标识那个机顶盒 640 的制造商。当然, 位数是一个设计选择。

[0102] 一旦接收到配对密钥生成器 621 和 STB 序列号 641, 适当的配对密钥服务器 (例如服务器 630_i, 其中 $i \geq 1$) 就返回配对密钥 622。在本实施例中, 配对密钥 622 用于加密对发送到机顶盒 640 的加扰内容进行解扰所需的解扰密钥。更具体地说, 配对密钥服务器 630_i 存取是唯一密钥 680 的相同副本的预存储密钥, 并使用存取的密钥对配对密钥生成器 621 加密。这产生了相当于配对密钥 622 的密钥。备选地, 可设想配对密钥生成器 621 经历单向散列操作, 其中对结果进行加密, 或可仅对一部分配对密钥生成器 621 加密, 以产生配对密钥 622。然而, 需要在解扰器 660 内重复类似操作。

[0103] 一旦接收到配对密钥 622, CA 控制系统 620 就生成授权管理消息 (EMM) 648 以及发送到智能卡 640 的一个或多个 ECM 642。在图 6C 中示出了 EMM 648 的一个实施例。

[0104] 如图 6C 所示, EMM 648 包括以下至少两项: 智能卡 ID 643、长度字段 644、配对密钥生成器 621、分别与密钥标识符 645₁-645_M 相关联的“M”($M \geq 1$) 密钥标识符 645₁-645_M 和密钥 646₁-646_M。当然, 其它授权 647 也可包括在 EMM 648 中。同样, 可设想配对密钥生成器 621 可排除在 EMM 648 之外, 并可单独发送, 且通常与 EMM 648 同时发生。

[0105] 具体地说, 就图 6C 而言, 智能卡 ID 643 是用于指示特定机顶盒和可能机顶盒制造商的位值。“EMM 长度字段”644 是用于指示 EMM 648 长度的位值。如所示, 配对密钥生成器 621 是包括来自上图 6B 中的参数的位值。每个“密钥标识符”645₁-645_M 是 16 位授权标签值, 其被标记以便在校验是否已非法改变了密钥 646₁-646_M 时使用。密钥 646₁-646_M 用于对 ECM 642 解密, ECM 642 用于传送存取需求和加密格式的至少一个解扰密钥。

[0106] 如图 7A-7C 中描述的, 智能卡 650 接收 EMM 648, 并将配对密钥生成器 621 和从 ECM 642 恢复的加密的解扰密钥 651 转发到机顶盒 640 的解扰器 660。

[0107] 图 7A 是在图 6A 的机顶盒 640 内实现的解扰器 660 的第一示范性实施例。在接收来自智能卡 650 的配对密钥生成器 621 和加密解扰密钥 651 时, 解扰器 660 包括第一处理块 661, 该第一处理块使用解扰器 660 中存储的唯一密钥 680 在配对密钥生成器 621 上执行加密操作。可根据密码函数, 诸如数据加密标准 (DES)、高级加密标准 (AES)、IDEA、三重 DES (3DES) 等, 来执行与处理块相关联的加密或解密操作。只为说明性目的标识这些密码函数中的某一些。

[0108] 在配对密钥生成器 621 上的加密操作产生与配对密钥 622 相同的密钥 663, 该密钥 663 被加载到第二处理块 664 中。处理块 664 用于对加密的解扰密钥 651 进行解密, 以产生解扰密钥 665。解扰密钥 665 用于对加载到机顶盒 640 (更具体地说是解扰器 660) 中的加扰内容 666 进行解扰。解扰可包括在加扰的内容 666 上执行 3DES 操作。结果是以清除格式的内容, 该内容可从解扰器 660 传输, 并随后加载到如图 5 所示的 MPEG 解码器, 或可选地加载到 D/A 转换器、DVI 接口或 IEEE 1394 接口。

[0109] 可设想改变处理块 661 和 664, 以分别支持解密和加密, 这取决于如何公式化配对密钥 622。

[0110] 图 7B 是在图 6A 的机顶盒 640 内实现的解扰器 660 的第二示范性实施例。根据 3DES 用 2 个密钥进行解扰。如图 7A 中阐述的, 解扰器 660 包括使用唯一密钥 680 在配对密钥生成器 621 上执行加密操作的第一处理块 661。

[0111] 在配对密钥生成器 621 上的加密操作产生与配对密钥 622 相同的密钥 663。密钥 663 被加载到两个 DES 处理块 664₁ 和 664₂ 中。处理块 664₁ 用于对第一加密解扰密钥 652 解密, 以产生第一解扰密钥 (DK1) 665₁。处理块 664₂ 用于对第二加密解扰密钥 653 解密, 以产生第二解扰密钥 (DK2) 665₂。低电平 3DES 解扰逻辑 667 使用 DK1 665₁ 和 DK2 665₂ 周以对加扰内容 666 进行解扰。

[0112] 当然, 还可设想处理块 661 可配置为用图 7C 中所示的多个密钥支持 3DES。对于本实施例, 智能卡 650 提供多个配对密钥生成器 621₁ 和 621₂, 以产生分别提供给处理块 664₁ 和 664₂ 的两个密钥 663₁ 和 663₂。这些处理块 664₁ 和 664₂ 产生解扰密钥 665₁ 和 665₂, 低电平 3DES 解扰逻辑 667 使用这些密钥用于对加扰内容 666 进行解扰。

[0113] 如图 7C 所示, 第一配对密钥生成器 621₁ 可配置为图 6B 的配对密钥生成器 621。然而, 第二配对密钥生成器 621₂ 可配置为验证放在密钥 663₂ 中的复制保护参数。例如, 第二配对密钥生成器 621₂ 可包括提供复制控制的复制控制信息 (CCI) 字段以及标识复制控制所应用到的输入内容的内容标识符字段。例如, CCI 字段可标识不能复制内容以便永久存储, 或可复制特定次数 (一次、两次等)。CCI 字段可用于标识可回放内容的次数, 或为这种内容设置指定观看时间。

[0114] 第二配对密钥生成器 621₂ 还可包括内容 ID 字段 (其包括标识与其相关的数字内容的值), 并可包括管理该数字内容有效性 / 期满的数据。第二配对密钥生成器 621₂ 还可包括复制世代数字段, 该字段包括标识可复制数字内容的次数的值。当然, 为了减小字段大小, 可散列多个参数, 并将其存储在字段中。

[0115] 现在参考图 8, 其示出了安全内容传送系统 700 的第四示范性实施例。安全内容传送系统 700 包括用户管理系统 610、CA 控制系统 620、配对密钥入口 (gateway) 710、配对密钥服务器 630₁-630_N 和机顶盒 640。代替将配对密钥生成器 621 和 STB 序列号 641 从 CA 控制系统 620 传输到配对密钥服务器 630₁-630_N (如图 6A 所示), 这种信息可路由到配对密钥入口 710。配对密钥入口 710 存取来自配对密钥生成器 621 的图 6B 的 STB 制造商 ID 623, 并适当地将配对密钥生成器 621 和 STB 序列号 641 路由到选择的配对密钥服务器 630_i。这减少了 CA 控制系统 620 或服务器 630₁-630_N 恢复配对密钥 622 的处理时间量。

[0116] 备选地, 代替配对密钥入口 710 将配对密钥生成器 621 和 STB 序列号 641 路由到选择的配对密钥服务器 630_i, 可设想将这种信息路由到可信第三方 635, 该第三方存取用于配对密钥检索的目标数据库。为配对密钥 622 检索所选的数据库基于与配对密钥生成器 621 和 / 或 STB 序列号 641 相关联的值。例如, 在一系列地址上基于与配对密钥生成器 621 和 / 或 STB 序列号 641 相关联的值, 可存取各数据库。这些值用于标识目标数据库。

[0117] 图 9A 是安全内容传送系统 800 的第五示范性实施例。安全内容传送系统 800 包括用户管理系统 610 和 CA 控制系统 810、与不同机顶盒制造商相关联的多个配对密钥服务器 630₁-630_N、机顶盒 820、配对密钥入口 830 (类似于图 8 的入口 710) 和网络接口 840 (例如 DOCSIS CMTS)。机顶盒 820 包括解扰器 860, 该解扰器包括配置为存储机顶盒 820 唯一密钥 880 (称为“唯一密钥”) 的本地存储器 870。在机顶盒 820 的 IC 制造或创建期间, 加载唯一密钥 880。

[0118] 机顶盒 820 接收具有以未加扰格式的电子节目指南 (EPG) 的 EPG 元数据, 并接收以加扰格式的数字节目内容 850。在一个实施例中, CA 控制系统 810 在带外提供 EPG 元数

据 900。如图 9C 所示, EPG 元数据 900 的一个实施例包括用于内容提供商提供的不同类型内容的多个标签项 910₁-910_S(S ≥ 1)。各标签项 910_j(1 ≤ j ≤ S) 包括至少频道名称 920_j、内容名称 930_j 以及指示与频道相关的服务等级的密钥标识符 940_j。此外, 各标签项 910_j 还包括节目标识符 (PID) 950_j 和配对密钥生成器 (MKG) 960_j。元数据 900 用于提供验证在 EMM 885 中提供的密钥的配对密钥生成器 (例如配对密钥生成器 621) 和密钥标识符。

[0119] 往回参考图 9A, 一旦机顶盒 820 的用户期望接收特定类型内容 (例如 PPV 电影、广播频道等), 机顶盒 820 就确定是否已在此存储了与请求内容相关联的授权。如果没有存储该授权, 则可直接通过屏幕显示或音频回放来通知用户, 并提示向用户管理系统 610(或 CA 控制系统 810) 提供请求 811。备选地, 可在没有用户控制的情况下自动发送该请求 811。如所示, 可在带外 (例如电话呼叫或在互联网上经由 DOCSIS 的电子邮件) 或在带内向用户管理系统 610 提供请求 811。

[0120] 如本实施例所示, 一旦从用户管理系统 610 接收到包括 STB 序列号 831 和授权的验证消息 815(或在 CA 控制系统 810 查找 STB 序列号 831), CA 控制系统 810 就将 STB 序列号 831 和配对密钥生成器 832 路由到配对密钥入口 830。配对密钥入口 830 操作为协调配对密钥 833 传送的媒介, 该配对密钥用于从下载的加扰信息中提取请求内容。当然, CA 控制系统 810 可用配对密钥入口 830 执行验证方案, 以便建立其间的安全通信。

[0121] 一旦接收到配对密钥 833, CA 控制系统 810 就生成一个或多个授权管理消息 (EMM) 885。不提供 ECM; 例如只提供 EMM 885 上的频道密钥。在图 9B 中示出了 EMM 885 的一个实施例。

[0122] 如图 9B 所示, EMM 885 包括至少以下两项: STB 序列号 831、EMM 长度字段 842、配对密钥生成器 832、分别与密钥标识符 844₁-844_M 相关联的“M”(M ≥ 1) 密钥标识符 844₁-844_M 和加密服务密钥 846₁-846_M。当然, 除了标识符或服务密钥还可将其它类型授权包括在 EMM 885 中, 并可改变这些值的大小 (以位为单位)。同样, 可设想将配对密钥生成器 832 排除在 EMM 885 之外, 并将其单独发送, 且通常与 EMM 885 同时发生。

[0123] STB 序列号 831 是用于指示特定机顶盒和可能机顶盒制造商的值。“EMM 长度字段”842 是用于指示 EMM 885 长度的位值。如所示, 配对密钥生成器 832 是包括来自上面图 6B 的参数的位值。每个“密钥标识符”844₁-844_M 都是分别指示与对应加密服务密钥 846₁-846_M 相关的服务等级的 16 位值。由对应于图 9A 的配对密钥 833 的解扰器 860 内产生的密钥对加密的服务密钥 846₁-846_M 进行解密。

[0124] 图 10 是在图 9A 的机顶盒 820 内实现的解扰器 860 的第一示范性实施例。在接收到 EMM 885 中包括的配对密钥生成器 832 和加密服务密钥 846_j(1 ≤ j ≤ M) 时, 解扰器 860 包括使用之前存储在解扰器 860 中的唯一密钥 880 在配对密钥生成器 832 上执行加密操作的第一处理块 861。加密操作可根据对称密钥密码函数, 诸如 DES、AES、IDEA、3DES 等。当然, 可设想改变处理块 861 以执行代替加密函数的散列函数。

[0125] 在配对密钥生成器 832 上的加密操作产生与配对密钥 833 相同的密钥 863。密钥 863 加载到第二处理块 864 中, 第二处理块用于对加密的服务密钥 846_j 解密, 以恢复用于对加载到机顶盒 840(且具体地说是解扰器 860) 中的加扰内容 850 进行解扰的服务密钥。解扰可包括在加扰内容上执行 3DES 操作。结果可以是以清除格式的内容, 该内容从解扰器 860 传输, 并随后加载到 MPEG 解码器 (如图 5 所示), 或可选地加载到 D/A 转换器、DVI 接

口或 IEEE 1394 接口。

[0126] 现在参考图 11, 其示出了安全内容传送系统 900 的第六示范性实施例的一部分。代替图 9A 的用户管理系统 610 和 CA 控制系统 810, 配对密钥入口 830 可适于与多个用户管理系统 (SMS) 910_1 – 910_K ($K \geq 1$) 通信, 其中每个与不同的内容提供商相关联。这些用户管理系统 910_1 – 910_K 中的每一个都将配对密钥生成器和 STB 序列号 920_1 – 920_K 提供给配对密钥入口 830, 且反过来接收对应的配对密钥 930_1 – 930_K 。这些配对密钥 930_1 – 930_K 用于对提供给一个或多个目标机顶盒 (未示出) 的服务密钥加密。备选地, 可利用可信第三方 635, 如图 6A、8 和 9A 所示。

[0127] 例如, 对于这个说明的实施例, 用户管理系统 910_1 和 910_2 是地面广播公司, 每个都将配对密钥生成器和 STB 序列号 920_1 、 920_2 提供给配对密钥入口 830, 并接收对应的配对密钥 930_1 、 930_2 。操作上类似, 用户管理系统 910_3 和 910_4 是有线电视运营商, 用户管理系统 910_5 是直播卫星 (DBS) 公司, 且用户管理系统 910_{K-1} 和 910_K 是互联网内容资源。

[0128] 参考图 12, 其示出了安全内容传送系统 1000 的第七示范性实施例的一部分。系统 1000 的机顶盒 1010 接收来自第一源的加扰或加密内容 1020, 并接收来自第二源的授权管理消息 (EMM) 1040。第二源可以是智能卡或 CA 控制系统。

[0129] 根据本发明的一个实施例, EMM 1040 包括复制保护密钥生成器 (CPKG) 1042 和加密用户密钥 1041。如图 12 和 13 所示, 加密用户密钥 (E_{key}) 1041 是在唯一密钥 (“唯一密钥”) 1031 或其派生对 E_{key} 1041 解密时计算的以在解扰器 1030 中生成复制保护密钥 1035 的值。在机顶盒 1010 的 IC 制造或创建期间加载唯一密钥 1031。为了解密, 与诸如另一机顶盒 1070、便携式计算机 (例如 PDA) 1071、乃至便携式自动点唱机 1072 的其他设备共享复制保护密钥 1035。

[0130] 如图 14 所示, CPKG 1042 包括 STB 制造商 ID 1050、标识提供 EMM 1040 (例如类似于图 6B 的 CA 提供商 ID 625) 的系统的系统 ID 1051、标识数字内容提供商 (例如类似于图 6B 的服务提供商 ID 624) 的内容提供商 ID 1052、以及通常故意等于图 6B 的配对密钥序号 626 的 CP 序号 1053。此外, CPKG 1042 包括复制保护状态值 1054, 该值提供内容管理控制, 诸如是否可以复制输入内容、回放的次数或回放的日期 / 时间。

[0131] 往回参考图 13, 解扰器 1030 的一个实施例接收来自第二源的 E_{key} 1041、CPKG 1042 和加密的解扰密钥 1043。CPKG 1042 基本上等于图 9A 的配对密钥生成器 832。解扰器 1030 包括第一处理块 1032, 该第一处理块根据对称密钥密码函数 (诸如 DES、AES、IDEA、3DES 等) 用唯一密钥 1031 对 E_{key} 1041 进行解密。

[0132] E_{key} 1041 上的解密操作恢复了用户密钥 1033, 该用户密钥被加载到用于对 CPKG 1042 加密以产生复制保护密钥 1035 的第二处理块 1034 中。使用唯一密钥 1031 (或其派生) 对加密的解扰密钥 1043 进行解密以恢复清除格式的解扰密钥, 用于对加载到机顶盒 1010 (具体地说是解扰器 1030) 的加密内容 1020 进行解扰和 / 或解密。解扰和 / 或解密可包括执行 3DES 操作。

[0133] 结果, 暂时以清除格式放置内容, 但将其路由到低电平加密逻辑 1060, 该低电平加密逻辑用与任一或所有目标数字设备相关联的复制保护密钥 1035 对解扰内容加密。因此, 在随后传输期间该内容是安全的。

[0134] 现在参考图 15, 其示出了在数字设备 1100 内实现的解扰器 1110 的另一示范性实

施例。适于与数字设备 1100 通信,解扰器 1110 接收来自内容提供商的节目数据,并将其路由到目标数字设备。通过对节目数据加密或加扰可“复制保护”该节目数据,以避免畅行无阻地存取该节目数据。

[0135] 对于本发明的一个实施例,解扰器 1110 包括存储器 1120、控制字 (CW) 密钥梯形逻辑 1130、复制保护 (CP) 密钥梯形电路 1140 以及多个密码单元 1150、1160 和 1170。这里,解扰器 1110 配置为单个集成电路。然而,可设想解扰器 1110 备选地配置为多芯片封装内包含的多个集成电路。

[0136] 如图 15 所示,存储器 1120 是只可写一次的可编程非易失性存储器,以便增强安全性。因此,被加载到一次可编程存储器 1120 之后,至少一个唯一密钥 1122(下文通常称为“STB 密钥”,且每个都称为 STB 密钥 -t,其中 $t \geq 1$) 不能被不正当地读取或改写。STB 密钥 1122 被提供给 CW 密钥梯形逻辑 1130 和 CP 密钥梯形逻辑 1140。这样,一旦 STB 密钥 1122 被编程,就不能被重新编程、改变或从解扰器 1110 外部读取。此外,编程后 J- 标签不能用于读取值。STB 密钥 1122 可配置在许多实施例中,诸如单个 56 位数据子密钥、3 个 56 位 3DES 子密钥或单个 128 位 AES 密钥。

[0137] 如图 15 还示出,CW 密钥梯形逻辑 1130 接收输入信息,即条件存取 (CA) 随机值 1200、配对密钥生成器 1205 和一个或多个加密控制字 1210。CW 密钥梯形逻辑 1130 处理输入信息,并产生 STB 密钥 1122 的一个或多个派生密钥 1124(下文通称为“Skey”,且每个都称为 Skey-u,其中 $u \geq 1$)。Skey 1124 被提供给第三密码单元 1170,用于对输入数据 1215 解密。输入数据 1215 的例子包括在带外发送的节目数据或数字设备 1100 产生的散列数据,其可用于例如在将传送回头端或 CA 控制系统时确认来自数字设备 1100 的起源。

[0138] CW 密钥梯形逻辑 1130 还处理输入信息,以从加密控制字 1210 中恢复一个或多个控制字 1126(下文通称为“控制字”,且每个都称为“CW-v”,其中 $v \geq 1$)。控制字 1126 被提供给第一密码单元 1150,用于对加扰内容 1220 解扰。此后,清除内容 1225 被提供给第二密码单元 1160,该单元配置为复制保护机构以在将清除内容 1225 传输到数字设备(诸如数字记录器、机顶盒等)之前对其进行加密。

[0139] 参考图 16,其示出图 15 的解扰器 1110 的控制字 (CW) 密钥梯形逻辑 1130 的示范性实施例。通常,CW 密钥梯形逻辑 1130 包括第一处理块 1300、第二处理块 1330 和第三处理块 1360。第一处理块 1300 配置为生成 Skey 1124,其是 STB 密钥 1122 的派生。第二处理块 1330 配置为基于配对密钥生成器 1205 或其逻辑派生来生成一个或多个配对密钥 1335(下文通常称为“配对密钥”,且每个都称为“配对密钥 -w”,其中 $w \geq 1$)。第三处理块 1360 配置为在使用配对密钥 1335 或其逻辑派生对加密控制字 1210 解密时恢复控制字 1126。

[0140] 现在参考图 17A-17C,其示出了图 16 的 CW 密钥梯形逻辑 1130 的第一处理块 1300 操作的示范性实施例。就图 17A 而言,第一处理块 1300 在 CA 随机 1200 上执行 DES 密码操作,该 CA 随机是从内容提供商传送到解扰器 1110 的消息中的种子值。基于 CA 随机 1200 和 STB 密钥 -1 1122₁ 生成 Skey-1 1124₁。Skey-1 1124₁ 是 STB 密钥 -1 1122₁ 的派生密钥。

[0141] 就图 17B 而言,第一处理块 1300 可适于执行代替 DES 密码操作的 AES 密码操作。具体地说,第一处理块 1300 配置为基于输入位值 1305 和 STB 密钥 -1 1122₁ 生成 Skey-1 1124₁(STB 密钥 -1 1122₁ 的派生密钥)。对于本发明的一个实施例,输入值 1305 包括结合设置为预定逻辑值(例如所有逻辑“0”)的“M”附加位 1307 的 CA 随机 1200。对于一个

实施例,位 1307 定位为输入值 1305 的最重要的位。使用 STB 密钥 -11122₁ 对输入值 1305 解密,以产生 Skey-1 1124₁。这里,其中“M”为 64,且 CA 随机 1200 的长度为 64 位,Skey-1 1124₁ 的长度为 128 位。然而,可设想利用其它的位大小。

[0142] 就图 17C 而言,第一处理块 1300 可适于执行代替 DES 或 AES 密码操作的 3DES 密码操作。当执行 3DES 密码操作时,第一处理块 1300 可配置为执行预定值与 CA 随机 1200 间的逻辑操作。“逻辑”操作可包括至少一个“异或”操作,或者,如果输入 1200 进入数据输入 1310、1314 和 1315 的三个独立输入路径,则该“逻辑”操作可包括多个数据值的按位逻辑校验,以确保这些数据值不同。问题是,如果数据输入 1310、1314 和 1315 相同,则数据输出 1124₁、1124₂、1124₃ 将相同。这可将 3DES 归为单个 DES 操作,因为其中两个密钥将相互抵消。这会削弱整个实现的安全性。

[0143] 如本实施例所示,经由第一计算路径 1310 来路由 CA 随机 1200。然而,将 CA 随机 1200 与第一预定值 1311 以及第二预定值 1312 相“异或”(例如一种类型的按位逻辑操作),其中分别沿第二和第三计算路径路由结果 1314 和 1315。这种“异或”操作可以彼此并行处理。对于本发明的这个实施例,预定值 1311 和 1312 彼此不同(例如,x01H、x02H)。

[0144] CA 随机 1200 与结果 1314 和 1315 一起使用第一唯一密钥“STB 密钥 -1”1122₁ 来经历 DES 解密操作。随后使用第二唯一密钥“STB 密钥 -2”1122₂ 对解密的结果进行加密,并然后使用第三唯一密钥“STB 密钥 -3”1122₃ 对其解密。结果,第一处理块 1300 产生 Skey 1124;对于本实施例,也就是第一派生密钥“Skey-1”1124₁、第二派生密钥“Skey-2”1124₂ 和第三派生密钥“Skey-3”1124₃。

[0145] 不考虑所用的密码函数类型,将 Skey 1124 提供给第二处理块 1330,以便产生配对密钥 1335。

[0146] 参考图 18A-18C,其示出了图 16 的 CW 密钥梯形逻辑 1130 的第二处理块 1330 的示范性实施例。就图 18A 而言,第二处理块 1330 利用 Skey-1 1124₁ 在配对密钥生成器 1205 上执行 DES 密码操作,其中 Skey-1 1124₁ 是本实施例的 STB 密钥 -1 1122₁ 的单个派生密钥。这产生了提供给第三处理块 1360 的配对密钥 -1 1335₁。

[0147] 就图 18B 而言,在执行 AES 密码操作时,第二处理块 1330 配置为基于配对密钥生成器 1205 和 Skey-1 1124₁ 生成配对密钥 -1 1335₁。对于本发明的一个实施例,输入值 1340 包括结合了具有预定逻辑值(如所有位设为逻辑“0”)的 M 位 1345 的配对密钥生成器 1205。M 位 1345 定位为输入值 1340 的最重要的位,对于该实施例 M ≤ 64。使用 Skey-1 1124₁ 对输入值 1340 解密,以产生配对密钥 -1 1335₁。

[0148] 就图 18C 而言,在执行 3DES 密码操作时,第二处理块 1330 配置为在预定值和配对密钥生成器 1205 之间执行逻辑操作。更具体地说,经由第一计算路径 1350 路由配对密钥生成器 1205。同样,将配对密钥生成器 1205 与第一预定值 1351 以及第二预定值 1352 相“异或”。分别经由第二和第三计算路径 1356 和 1357 路由这些结果 1354 和 1355。可彼此并行地处理这种“异或”操作。

[0149] 不同于图 17C,配对密钥生成器 1205 和结果 1354 以及 1355 使用派生密钥 1124₁-1124₃(即 Skey-1 1124₁、Skey-2 1124₂ 和 Skey-3 1124₃) 经历 DES 解密操作。这产生了配对密钥 1335,即配对密钥 -1 1335₁、配对密钥 -2 1335₂ 和配对密钥 -3 1335₃。

[0150] 参考图 19A-19C,其示出了图 16 的 CW 密钥梯形逻辑 1130 的第三处理块 1360 的

示范性实施例。就如图 19A 所示的 DES 密码函数而言,配对密钥 -1 1335₁ 用于恢复控制字 1126。作为说明性实施例,控制字 1126 具有多个控制字的特征,即第一控制字 (CW-1) 1126₁、第二控制字 (CW-2) 1126₂ 和第三控制字 (CW-3) 1126₃。

[0151] 就图 19B 而言,在执行 AES 密码操作时,第三处理块 1360 配置为以集合方式恢复控制字。例如,根据本发明的一个实施例,输入值 1365 包括位于最不重要部分的第一加密控制字 1210₁。第二加密字 1210₂ 定位为输入值 1365 的最重要部分。根据 AES 密码函数,使用图 16 的第二处理块 1330 产生的配对密钥 -1 1335₁ 对输入值 1365 进行解密,产生位宽等于输入值 1365 位宽的结果 1370。对于结果 1370,CW-1 1126₁ 定位为最不重要的部分,而 CW-2 1126₂ 定位为最重要的部分。

[0152] 此外,第三处理块 1360 还配置为对第三加密控制字 1210₃ 解密,该控制字可能结合了定位为最重要位的多个位 1375。用配对密钥 -1 1335₁ 执行这种解密,并产生结果 1376。这种解密是根据 AES 密码函数。可从结果 1376 中提取 CW-3 1126₃。在一个实施例中,通过存取来自结果 1376 的预定数量的最不重要位,来实现该提取。

[0153] 如图 19C 所示,通过在此示出的 3DES 密码函数来路由多个加密控制字。这通过 CW-3 1126₃ 来恢复 CW-1 1126₁。作为例子,根据 DES 函数使用配对密钥 -1 1335₁ 对第一加密控制字 1210₁ 解密。然后,使用配对密钥 -2 1335₂ 对解密控制字加密,且随后根据第三配对密钥 1335₃ 使用 DES 函数对其进行解密以恢复 CW-1 1126₁。

[0154] 然而,使用由第一配对密钥 1335₁ 与第一预定值 1382(例如 x02H) 相“异或”产生的密钥信息 1385,对第二加密控制字 1210₂ 进行解密。这个“异或”操作防止了密钥的抵消,其中恢复的 CW-1 1126₁ 和恢复的 CW-2 1126₂ 相等。该第一预定值 1382 与其它交替密钥 1335₂-1335₃ 相“异或”,以产生加载到 DES 加密逻辑用于处理的密钥信息 1386 和 1387。相同函数应用到 CW-3 1126₃ 的恢复,但基于与第二预定值 1394(例如 x04H) 相“异或”的配对密钥 1335₁-1335₃ 根据密码 DES 使用密钥加密信息 1390、1391、1392,来处理第三加密控制字 1210₃。

[0155] 现在参考图 20,其示出了图 15 的解扰器 1110 的 CP 密钥梯形逻辑 1140 的示范性实施例。这里,CP 密钥梯形逻辑 1140 包括第四处理块 1400、第五处理块 1430 和第六处理块 1460。第四处理块 1400 配置为基于 CP 随机 1250 和 STB 密钥 1122 或其逻辑派生来生成一个或多个派生密钥 1410(下文通称为“SCP 密钥”,且每个都称为“SCP 密钥 -x”,其中 $x \geq 1$)。第五处理块 1430 配置为基于加密的用户密钥 1255 或其逻辑派生来生成一个或多个用户密钥 1435(下文通称为“用户密钥”,且每个都称为“用户密钥 -y”,其中 $y \geq 1$)。第六处理块 1460 配置为通过使用第五处理块 1430 产生的用户密钥 1435(或其派生) 对一个或多个复制保护 (CP) 密钥生成器 1260 进行解密来生成一个或多个 CP 密钥 1465(下文通称为“CP 密钥”,且每个都称为“CP 密钥 -z”,其中 $z \geq 1$)。

[0156] 就图 21A 而言,第四处理块 1400 在 CP 随机 1250 上执行 DES 密码操作,其中 CP 随机是从内容提供商传送到解扰器 1110 的消息中的种子值。基于 CP 随机 1250 和 STB 密钥 1122(如 STB 密钥 -11122₁) 的逻辑派生 1405,产生 SCP 密钥 -1 1410₁。逻辑派生 1405 是 STB 密钥 -1 1122₁ 与预定值 1407 相“异或”产生的结果。因此,SCP 密钥 -1 1410₁ 是 STB 密钥 -1 1122₁ 的派生密钥。

[0157] 就图 21B 而言,在执行 AES 密码操作时,第四处理块 1400 配置为基于输入位值

1415 和逻辑派生 1405 生成 SCP 密钥 1410 (STB 密钥 1122 的派生密钥)。对于本发明的一个实施例,输入位值 1415 包括结合了多个位 (M) 1417 的 CP 随机 1250。位 1417 定位为输入位值 1415 的最重要的位。虽然可利用另一个位大小和不同的逻辑值,但在此这些“M”可以是全部设为逻辑“0”的 64 位。使用逻辑派生 1405 对输入位值 1415 解密,以产生 SCP 密钥 -1 1410₁。

[0158] 就图 21C 而言,在执行 3DES 密码操作时,第四处理块 1400 配置为在 CP 随机 1250 上执行密码操作。更具体地说,基于第一逻辑派生 1420 对 CP 随机值 1250 解密,其中第一逻辑派生是由预定值 (例如 x0AH) 1407 与 STB 密钥 -1 1122₁ 相“异或”产生的值。可彼此并行地处理这种“异或”操作。

[0159] 解密的结果 1421、1422 和 1423 使用第二逻辑派生 1424 经历 DES 加密操作,该第二逻辑派生是 STB 密钥 -2 1122₂ 与预定值 1407 相“异或”的结果。这产生了加密结果 1425、1426 和 1427,使用第三逻辑派生 1428 对这些加密结果进行解密。第三逻辑派生是 STB 密钥 -3 1122₃ 与预定值 1407 相“异或”的结果。结果输出是第一派生密钥“SCP 密钥 -1”1410₁、第二派生密钥“SCP 密钥 -2”1410₂ 和第三派生密钥“SCP 密钥 -3”1410₃。

[0160] 参考图 22A-22C,其示出了图 20 的 CP 密钥梯形逻辑 1140 的第五处理块 1430 的示范性实施例。对于本发明的该实施例,就图 22A 而言,第五处理块 1430 利用来自第四处理块 1400 的 SCP 密钥 1410 (例如 SCP 密钥 -1 1410₁) 在加密用户密钥 1255 上执行 DES 密码操作。这产生了提供给第六处理块 1460 的用户密钥 1435 (例如用户密钥 -1 1435₁)。

[0161] 可设想在第五处理块 1430 接收加密用户密钥 1255 之前在该用户密钥上执行“异或”操作。备选地,可代替“异或”操作来执行逻辑校验,以确保所有 SCP 密钥 1410₁-1410_x 都是唯一的。

[0162] 就图 22B 而言,在执行 AES 密码操作时,第五处理块 1430 配置为基于加密用户密钥 1255 和预定值 1440 生成用户密钥 1435 (例如用户密钥 -1 1435₁)。对于本发明的一个实施例,输入值 1445 包括结合了多个位 1440 的加密用户密钥 1255,该多个位 1440 设置为预定逻辑值并定位为输入值 1445 的最重要位。虽然可利用另一个位大小,但这里可用 64 位。使用 SCP 密钥 (例如 SCP 密钥 -1 1410₁) 对输入值 1445 解密,以产生用户密钥 1435₁。

[0163] 就图 21C 而言,在执行 3DES 密码操作时,第五处理块 1430 配置为执行预定值和加密用户密钥 1255 之间的逻辑操作。更具体地说,在第一计算路径 1450 上路由加密的用户密钥 1255。此外,第一预定值 1451 (例如 x01H) 与加密用户密钥 1255 相“异或”以产生逻辑派生 1452,在第二计算路径 1453 上路由该逻辑派生。同样,加密用户密钥 1255 与第二预定值 1454 相“异或”以产生逻辑派生 1455,在第三计算路径 1456 上路由该逻辑派生。可彼此并行地处理这种“异或”操作。对于本发明的该实施例,预定值 1451 和 1454 是不同的 (x01H、x02H)。

[0164] 上述结果使用 SCP 密钥 1410 (即 SCP 密钥 -1 1410₁、SCP 密钥 -2 1410₂ 和 SCP 密钥 -3 1410₃) 经历 DES 解密操作。在经历加密 - 解密 - 加密操作之后,最终结果产生了用户密钥 -1 1435₁、用户密钥 -2 1435₂ 和用户密钥 -3 1435₃。

[0165] 参考图 23A-23C,其示出了 CP 密钥梯形逻辑 1140 的第六处理块 1460 的示范性实施例。就图 23A 中所示的 DES 密码函数而言,一个或多个 CP 密钥生成器 1260 (下文通称为“CP 密钥生成器”,且每个都称为“CP 密钥生成器 -r”,其中 r ≥ 1) 可用于恢复对应的 CP 密

钥 1465。例如,使用用户密钥 -1 1435₁由密码函数对 CP 密钥生成器 -1 1260₁解密以产生 CP 密钥 -1 1465₁。同样,使用用户密钥 -21435₂和用户密钥 -3 1435₃由密码函数对第二和第三 CP 密钥生成器 1260₂ 和 1260₃解密。这分别产生 CP 密钥 -2 1465₂ 和 CP 密钥 -3 1465₃。

[0166] 就图 23B 而言,在执行 AES 密码操作时,第六处理块 1460 配置为恢复复制保护密钥,用于在将内容传输到另一数字设备之前对其进行重新加密。例如,根据本发明的一个实施例,第一输入值 1470 包括一系列 CP 密钥生成器 -1 1260₁ 和预定值 1475。如所示,出于说明目的,使 CP 密钥生成器 -1 1260₁ 位于第一输入值 1470 的最不重要的部分,且使预定值 1475 位于最重要的部分。根据 AES 密码函数使用用户密钥(例如第五处理块 1430 产生的用户密钥 1435₁)对第一输入值 1470 进行解密。这产生了 CP 密钥 -1 1465₁。在 CP 密钥生成器 -2 1260₂ 和 CP 密钥生成器 -3 1260₃ 上执行类似操作,以分别产生 CP 密钥 -2 1465₂ 和 CP 密钥 -3 1465₃。

[0167] 如图 23C 中所示,在执行 3DES 密码操作时,第六处理块 1460 配置为恢复复制保护密钥,用于在将内容传输到另一数字设备之前对其进行重新加密。根据本发明的一个实施例,使用用户密钥 -1 1435₁ 对 CP 密钥生成器 -1 1260₁ 解密。使用用户密钥 -2 1435₂ 对该结果加密,且然后使用用户密钥 -3 1435₃ 对加密的结果进行解密。这产生 CP 密钥 -1 1465₁。

[0168] 类似地,使用用户密钥 -1 1435₁ 的第一逻辑派生 1480 对第二 CP 密钥生成器 1260₂ 解密。作为本发明的一个实施例,第一逻辑派生 1480 是用户密钥 -1 1435₁ 与预定值 1482 相“异或”的结果。这产生了解密结果 1484,随后使用第二逻辑派生 1485 对该解密结果进行加密。第二逻辑派生 1485 是用户密钥 -2 1435₂ 与预定值 1482 相“异或”的结果。这产生了加密结果 1486,随后使用第三逻辑派生 1487(即用户密钥 -3 1435₃ 与预定值 1482“异或”的结果)对该加密结果进行解密。这产生了 CP 密钥 -2 1465₂。

[0169] 此外,使用用户密钥 -1 1435₁ 的第四逻辑派生 1480 对 CP 密钥生成器 -3 1260₃ 解密。作为本发明的一个实施例,第四逻辑派生 1490 是用户密钥 -1 1435₁ 与预定值 1492“异或”的结果。这产生了解密结果 1494,随后使用第五逻辑派生 1495 对该解密结果加密。第五逻辑派生 1495 是用户密钥 -2 1435₂ 与预定值 1492 “异或”的结果。这产生了加密结果 1496,随后使用第六逻辑派生 1497(即用户密钥 -3 1435₃ 与预定值 1492 “异或”的结果)对该加密结果解密。这产生了 CP 密钥 -3 1465₃。

[0170] 现在参考图 15 和 24,其示出了在解扰器 1110 内实现的验证逻辑的具体实施例。这里,验证逻辑包括适于将 CA 随机 1200 路由到第一密码单元 1150 的第一部件 1290。验证逻辑还包括适于将至少部分 CP 随机 1250 路由到第一密码单元 1150 的第二部件 1292,以及适于将至少部分 CP 密钥生成器 1260 路由到第一密码单元 1150 的第三部件 1294。

[0171] 通常 CA 随机 1200 的验证与 3DES 低电平加密一起使用,以便检验正在使用 CA 随机 1200 的正确值。通过启用 CA 随机验证信号 1275 来实现这种验证,该验证信号允许第一部件 1290 将部分 CA 随机 1200 加载到 3DES 函数的初始化向量 1152,诸如两个最不重要的字节。即使已更新了安全内容传送系统,但也调节初始化向量 1152 以防止黑客连续使用非法获取的配对密钥。

[0172] 此外,在将更新的 CA 随机传输到解扰器 1110 时,可通过临时禁用 CA 随机验证信号 1275 来实现将 CA 随机值 1200 更新为另一值。这防止当前 CA 随机值在更新过程中被不正当地加载到第一密码单元 1150 中。

[0173] 在允许通过安全内容传送系统传播更新的 CA 随机值经过了一段时间之后,再次启用 CA 随机验证信号 1275。

[0174] 仍参考图 15 和 24, CA 随机 1250 的验证与 3DES 低电平加密一起使用,以检验正在使用正确的 CP 随机值和派生用户密钥。在启用时,CP 随机验证信号 1280 允许第二部件 1292 将 CP 随机 1250 的至少一部分(诸如 CP 随机 1250 的两个最不重要字节)加载到 3DES 函数的初始化向量 1152 中。否则,有可能黑客写入恶意代码以用同一用户密钥来标记所有内容,以便恢复 CP 密钥并与通常不会存取特定内容的其它玩家共享内容。

[0175] 至少部分 CP 密钥生成器 1260 的验证用于验证内容的复制保护状态。当启用时,CP 密钥生成器验证信号 1285 允许第三部件 1294 将部分 CP 密钥生成器 1260 加载到 3DES 低电平加密函数的初始化向量 1152 中。对于一个实施例,加载 CP 密钥生成器 1260 的两个最不重要的字节。当然,出于验证目的,可加载形成 CP 密钥生成器 1260 的不同组字节。否则,有可能黑客写入恶意代码以将所有内容标记为“免复制”。

[0176] 根据本发明一个实施例,内容提供商负责启用和禁用 CA 随机验证信号 1275、CP 随机验证信号 1280 和 CP 密钥生成器验证信号 1285。

[0177] 现在参考图 25,其示出了图 24 的解扰器 1110 的具体实施例。如上所述,解扰器 1110 包括一次可编程存储器 1120;多个处理块 1300、1330、1360、1400、1430、1460;多个密码单元 1150、1160、1170;以及验证逻辑 1290、1292、1294。

[0178] 通常,第一处理块 1300 基于 CA 随机 1200 和 STB 密钥 1122 产生 Skey 1124。第二处理块 1330 基于配对密钥生成器 1205 和 Skey 1124 产生配对密钥 1335。第三处理块 1360 使用配对密钥 1335 产生从一个或多个加密控制字 1210 恢复的控制字 1126。控制字 1126 存储在一个或多个存储部件 1500 中,诸如随机存取存储器、闪速存储器或寄存器。

[0179] 通过启用更新 CW 信号 1505,允许将附加控制字存储在存储部件 1500 内。然而,通过禁用清除 CW 信号 1510,删除了存储部件 1500 中存储的一些或所有控制字 1126(即,可改写它们的存储位置)。

[0180] 第四处理块 1400 基于 CP 随机 1250 和 STB 密钥 1122 产生一个或多个 SCP 密钥 1410。第五处理块 1430 基于一个或多个加密用户密钥 1255 和 SCP 密钥 1410 产生用户密钥 1435。第六处理块 1460 基于 CP 密钥生成器 1260 和用户密钥 1435 产生 CP 密钥 1465。CP 密钥 1465 存储在一个或多个密钥存储部件 1520 中,诸如寄存器、随机存取存储器、闪速存储器等。通过启用更新 CP 密钥信号 1525,可将附加 CP 密钥 1465 存储在密钥存储部件 1520 内。然而,通过启用清除 CP 密钥信号 1530,不保存存储部件 1520 中存储的一些或所有 CP 密钥 1465。

[0181] 如图 25 中还示出,CP 解密逻辑 1550 是图 15 的第二密码单元 1160 的一部分。CP 解密逻辑 1550 使用密钥存储部件 1520 内存储的 CP 密钥对来自数字设备的加密(复制保护的)内容进行解密。CP 加密逻辑 1560 使用密钥存储部件 1520 内存储的 CP 密钥不受阻碍地对内容进行加密。解码电路 1570 执行视频和音频内容的解压缩。在解压缩之后存在两种可能性:1) 数模转换,例如对于基带视频输出和音频输出,或 2) 可对解压缩的数字内容进行编码,用于通过数字视频接口(DVI)传输。

[0182] 在上述描述中,参考本发明的具体示范性实施例描述了本发明。然而,显然可在不脱离附属权利要求中阐述的本发明更广的精神和范围前提下对本发明作出各种修改和改

动。说明书和附图也相应地视为说明性而非限制性的。

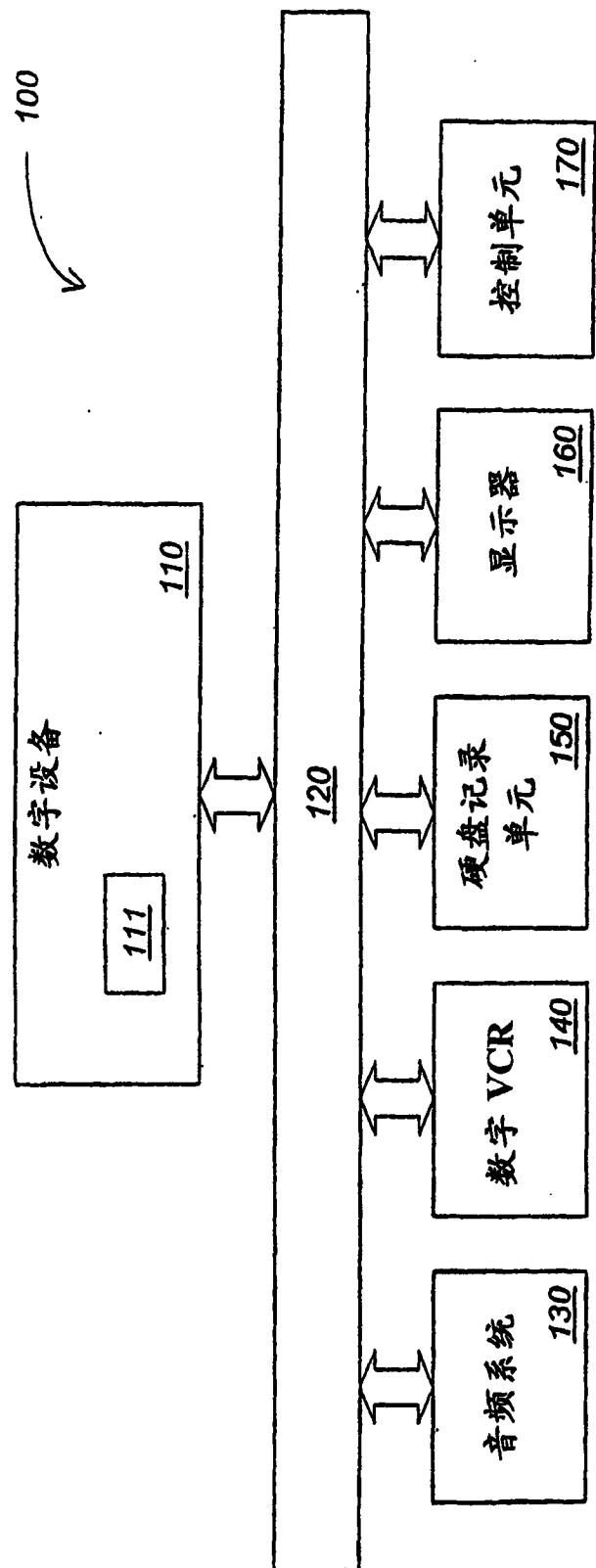
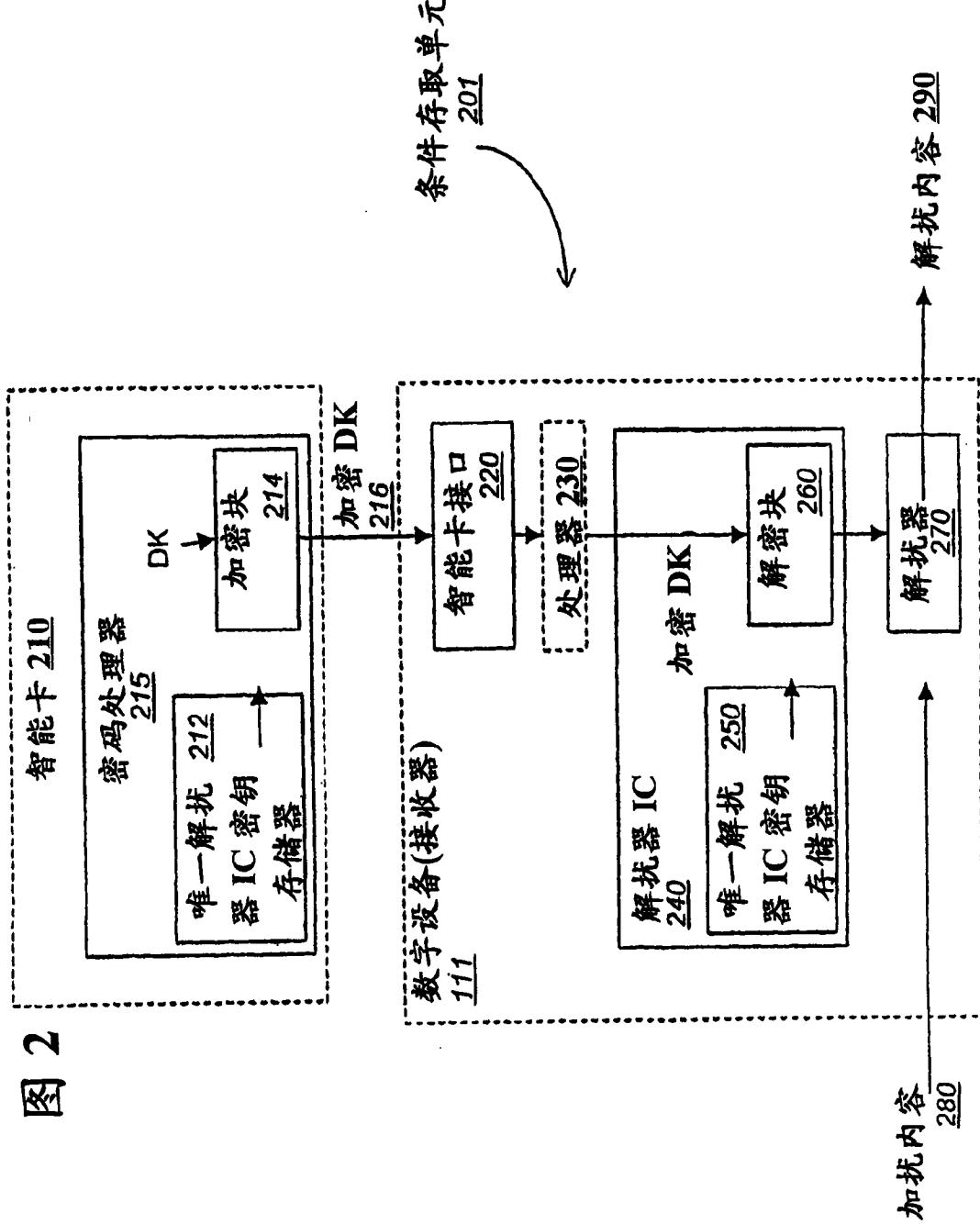


图 1

图 2



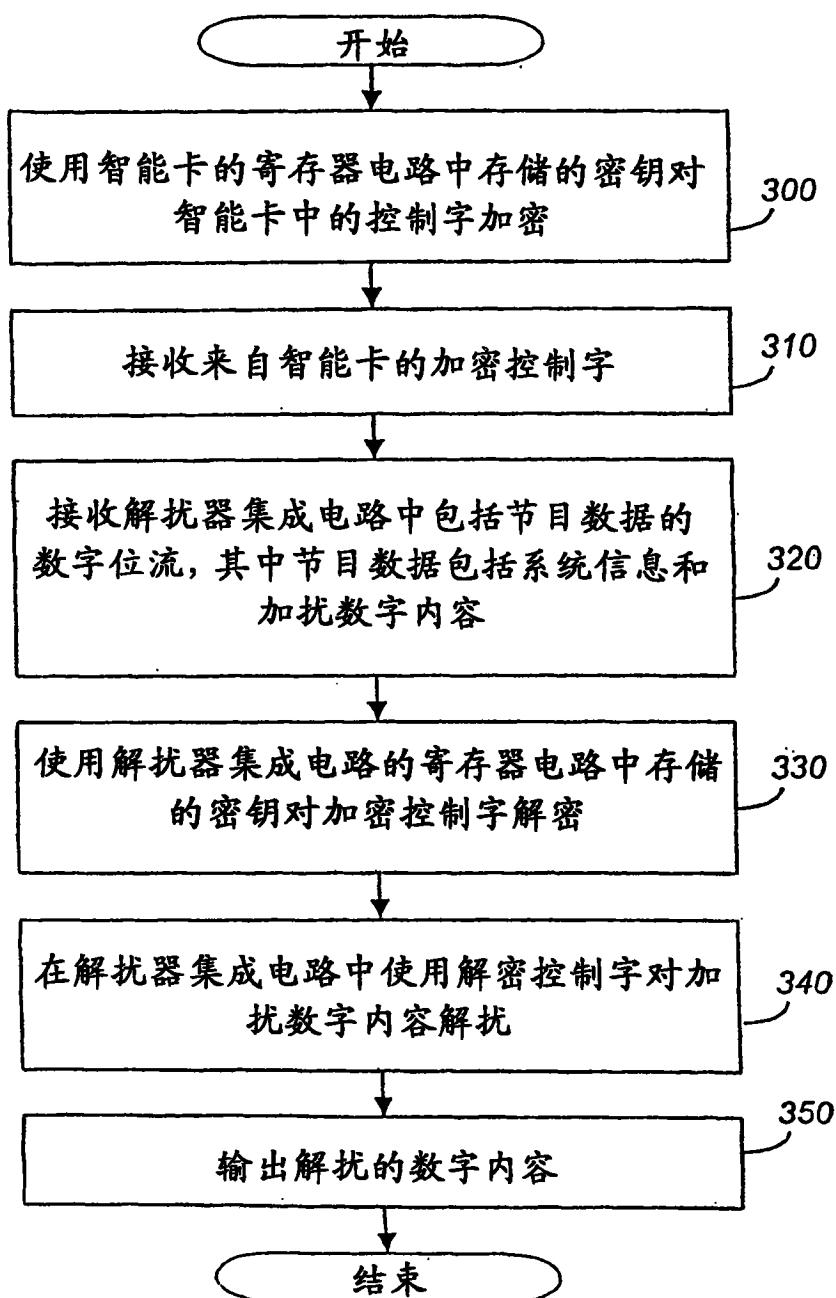


图 3

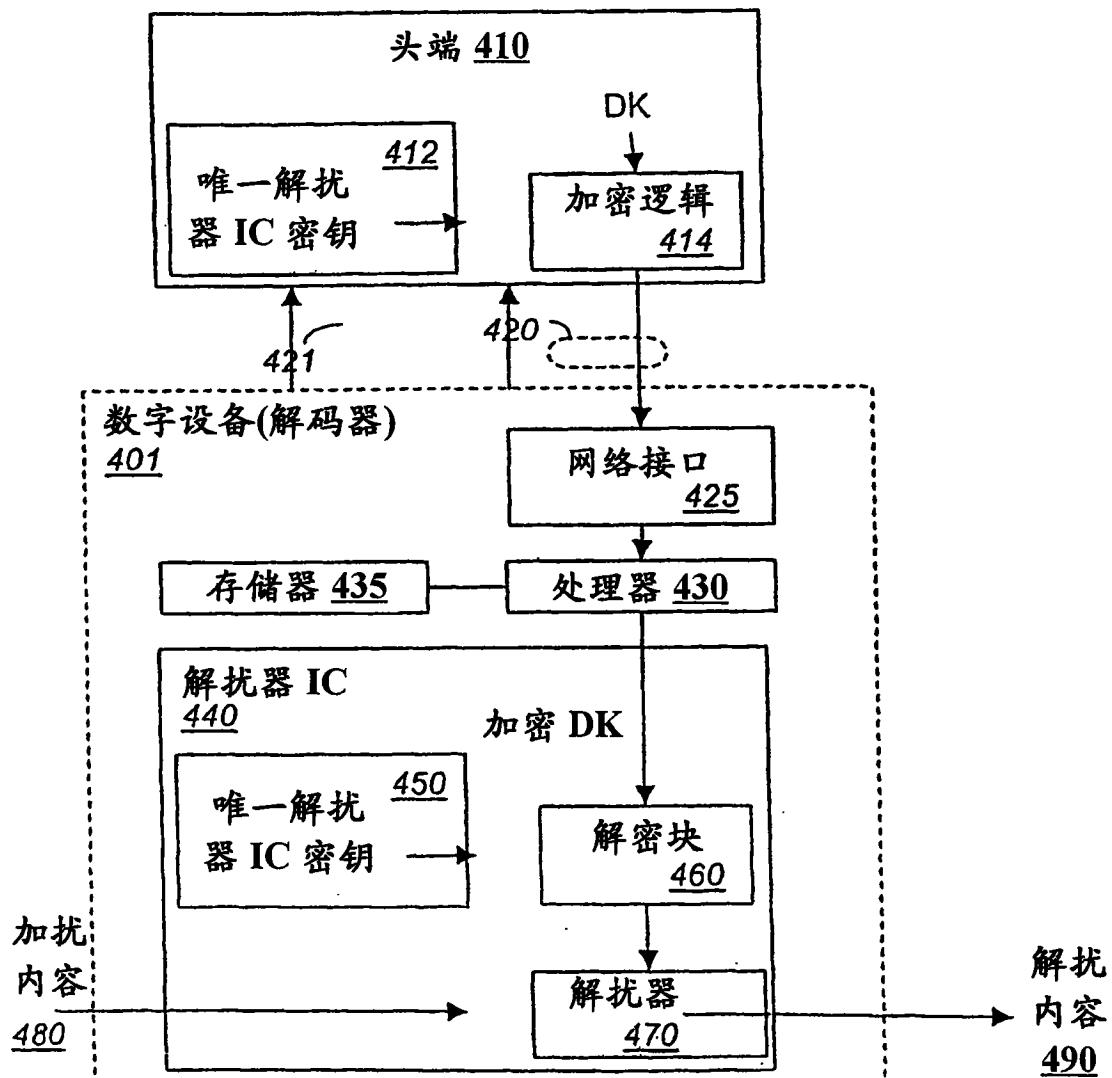


图 4

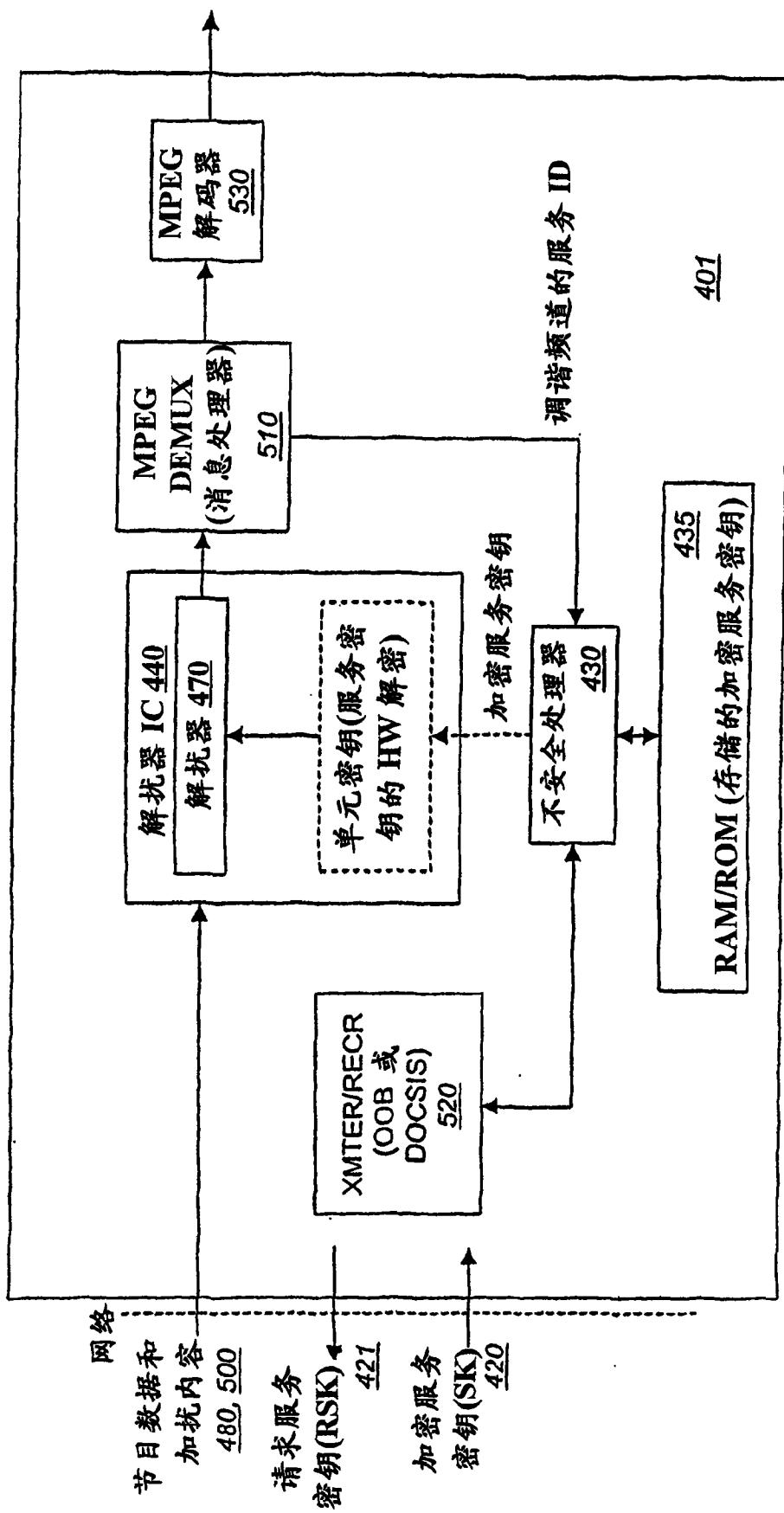


图 5

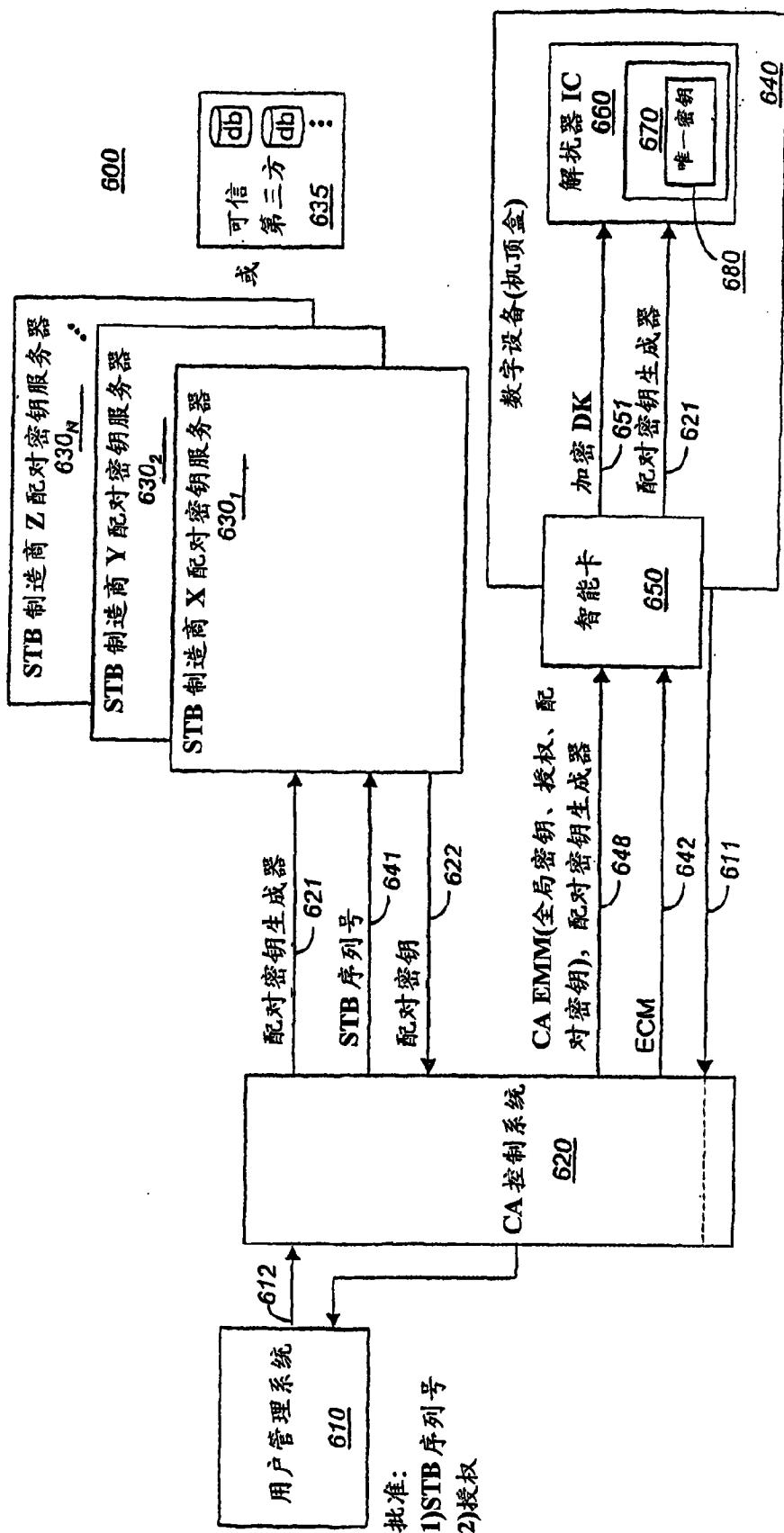


图 6A

图 6B

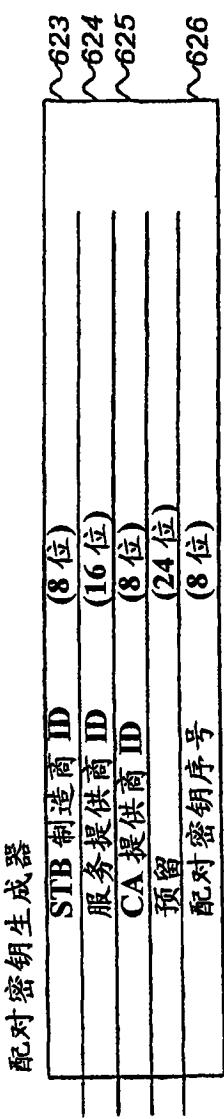
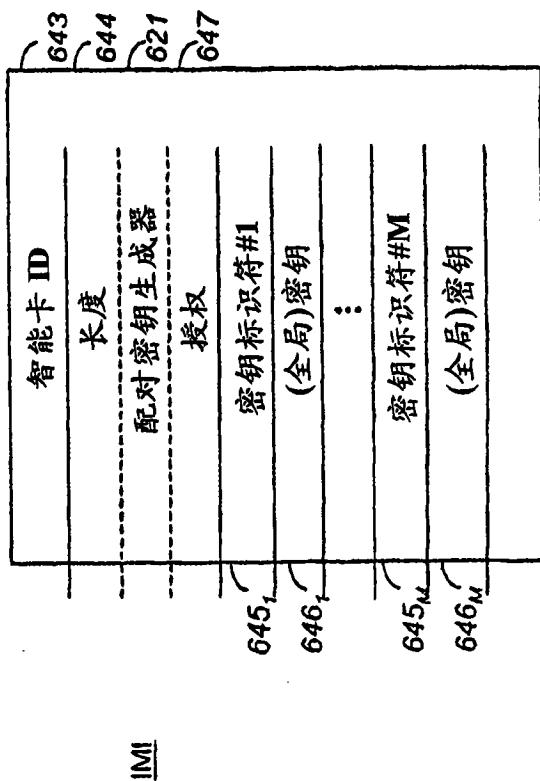


图 6C



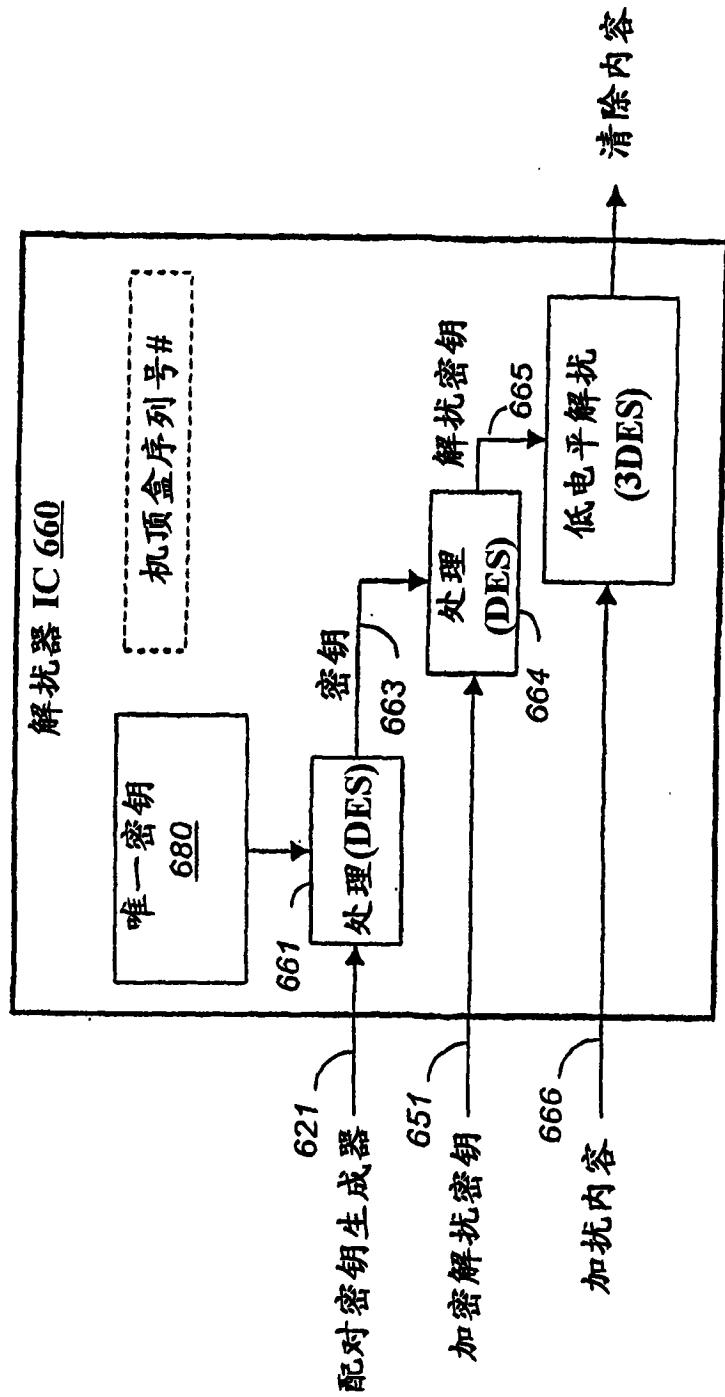


图 7A

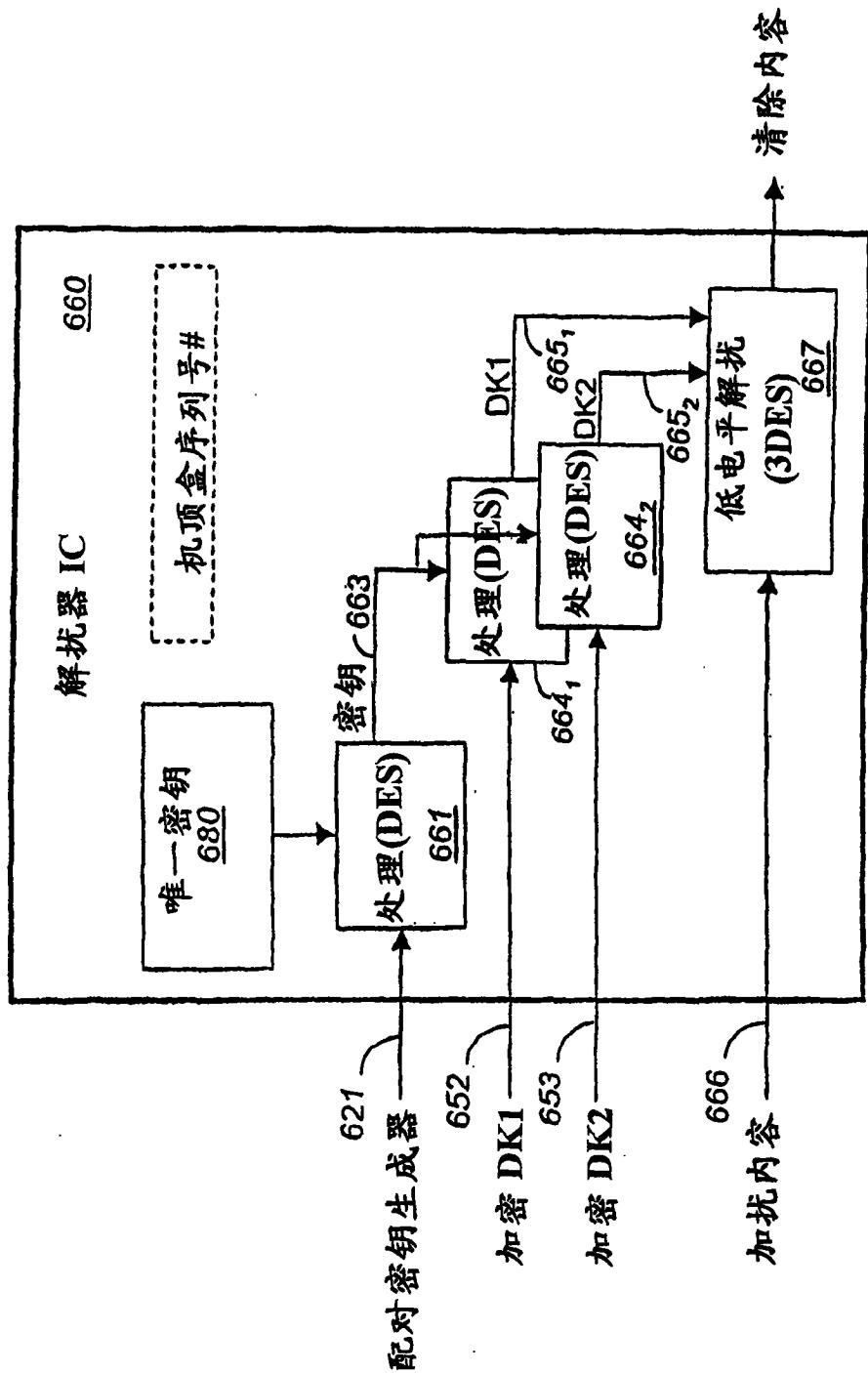
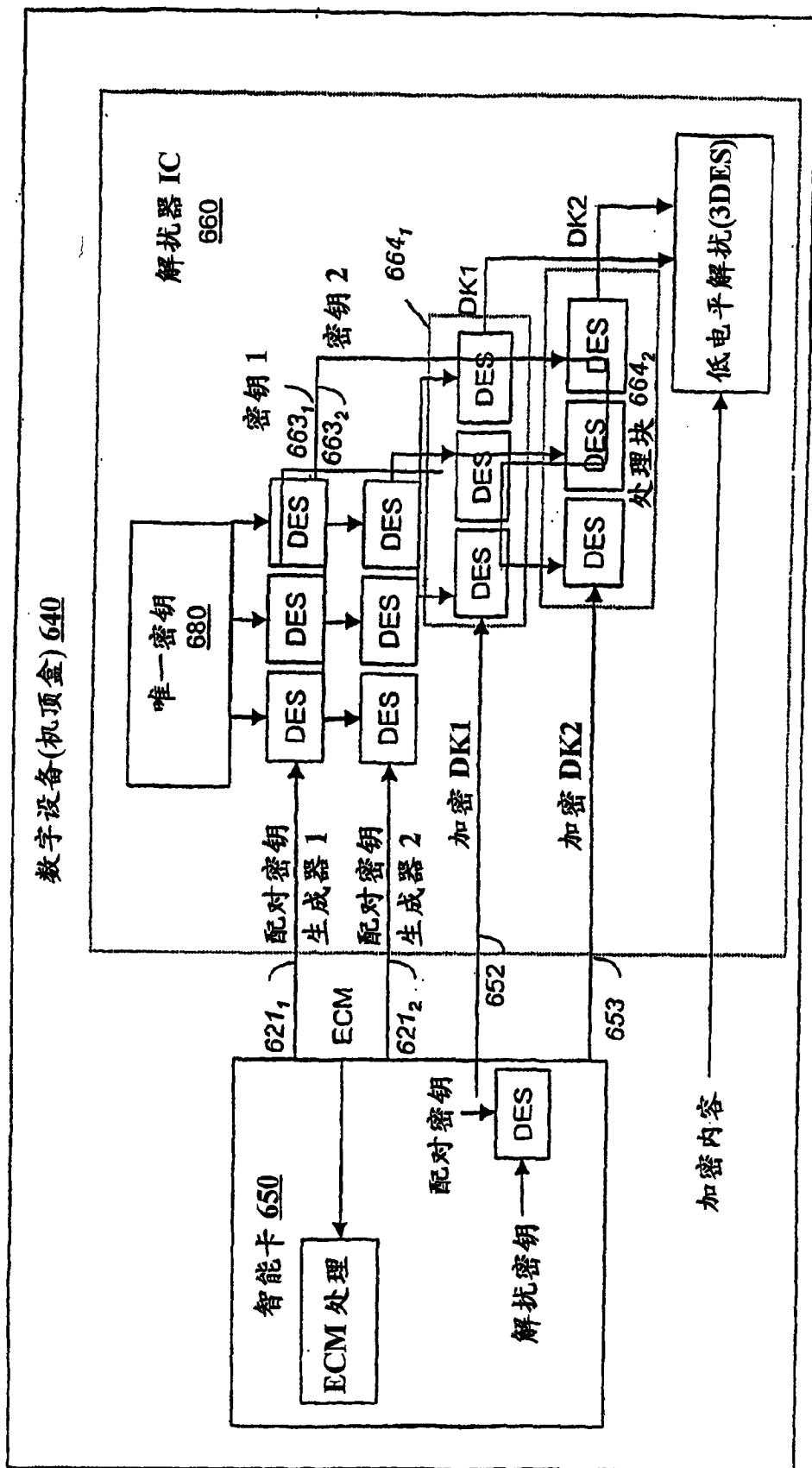


图 7B



7C
四

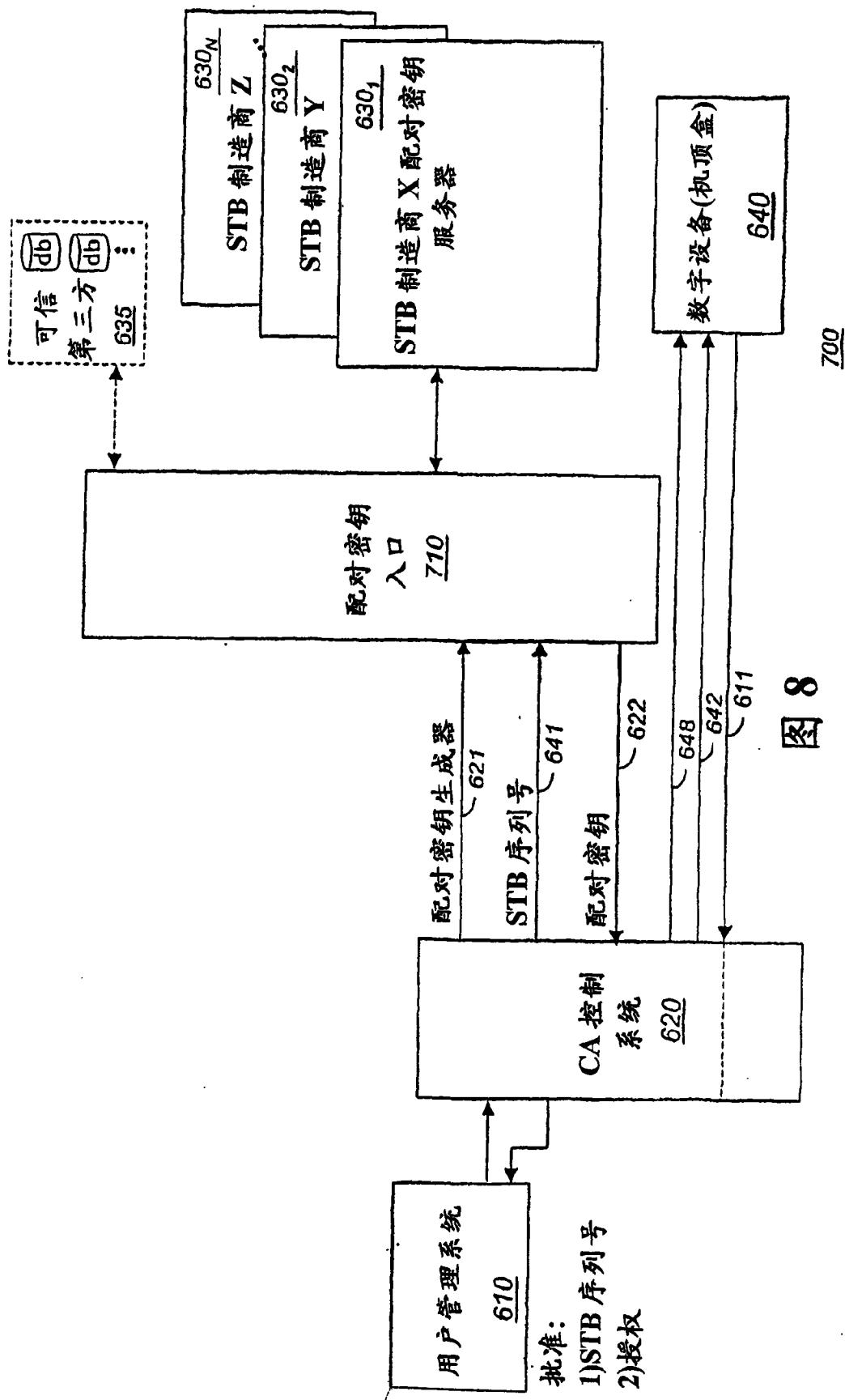


图 8

图 9A

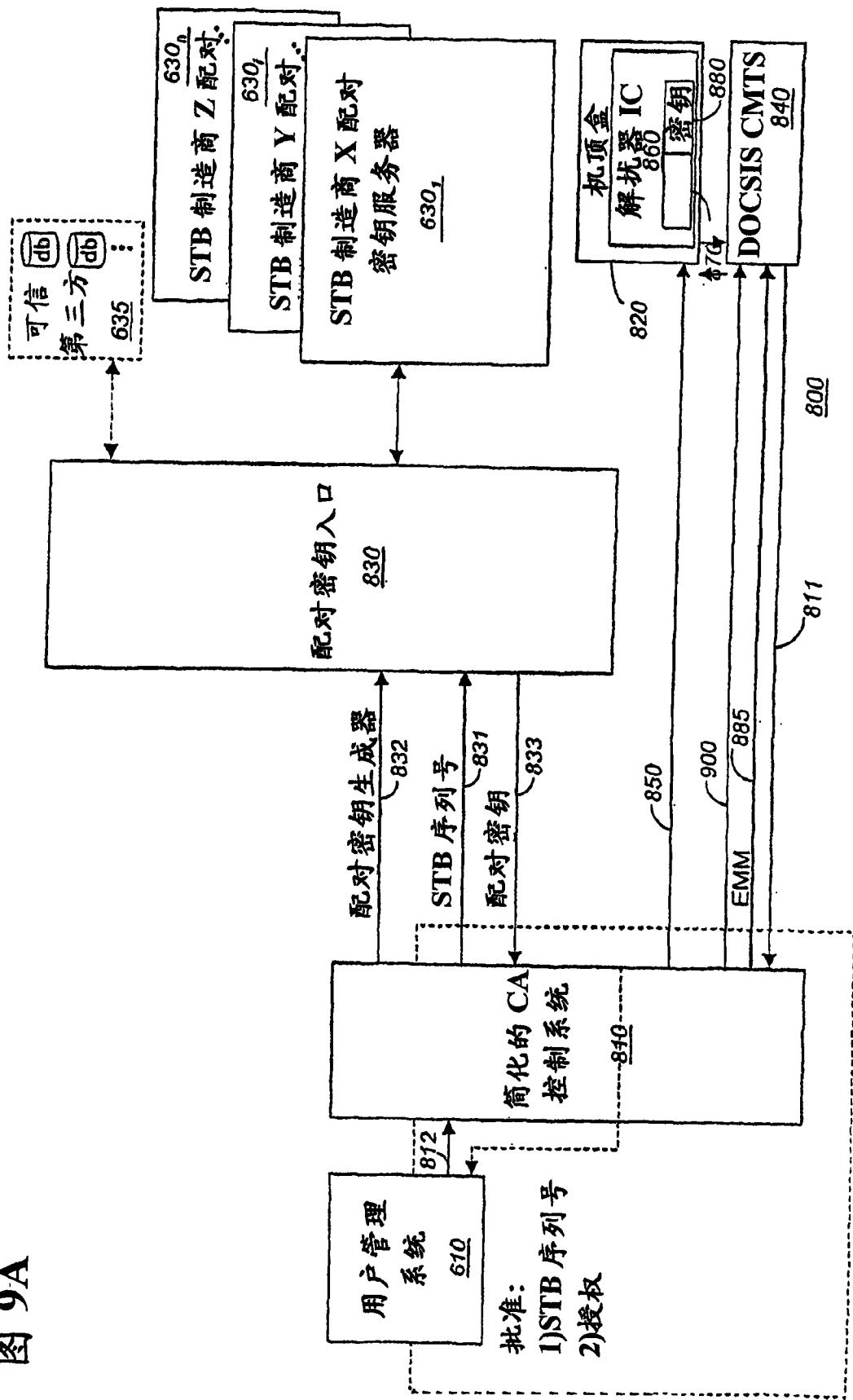




图 9B

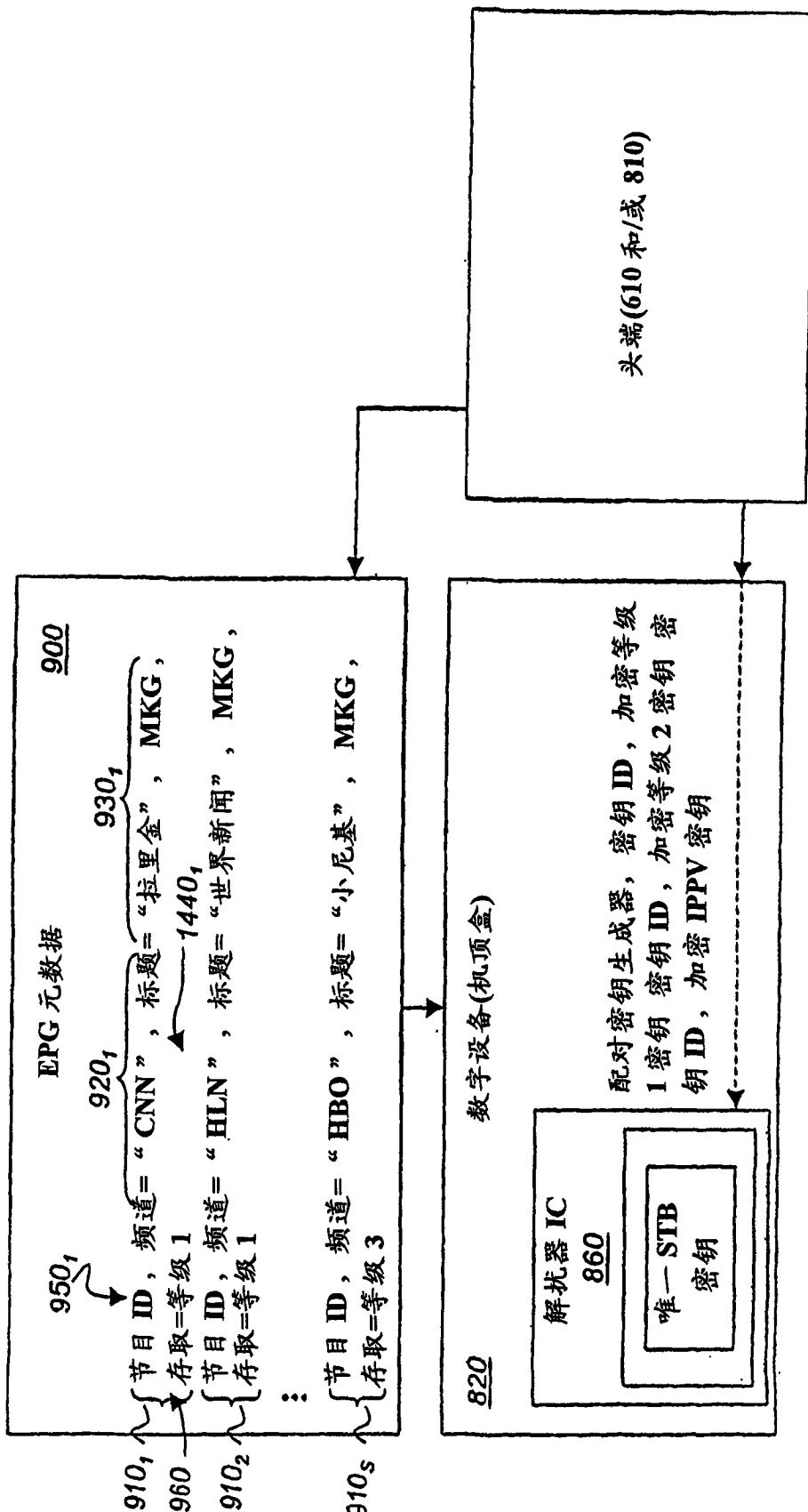


图 9C

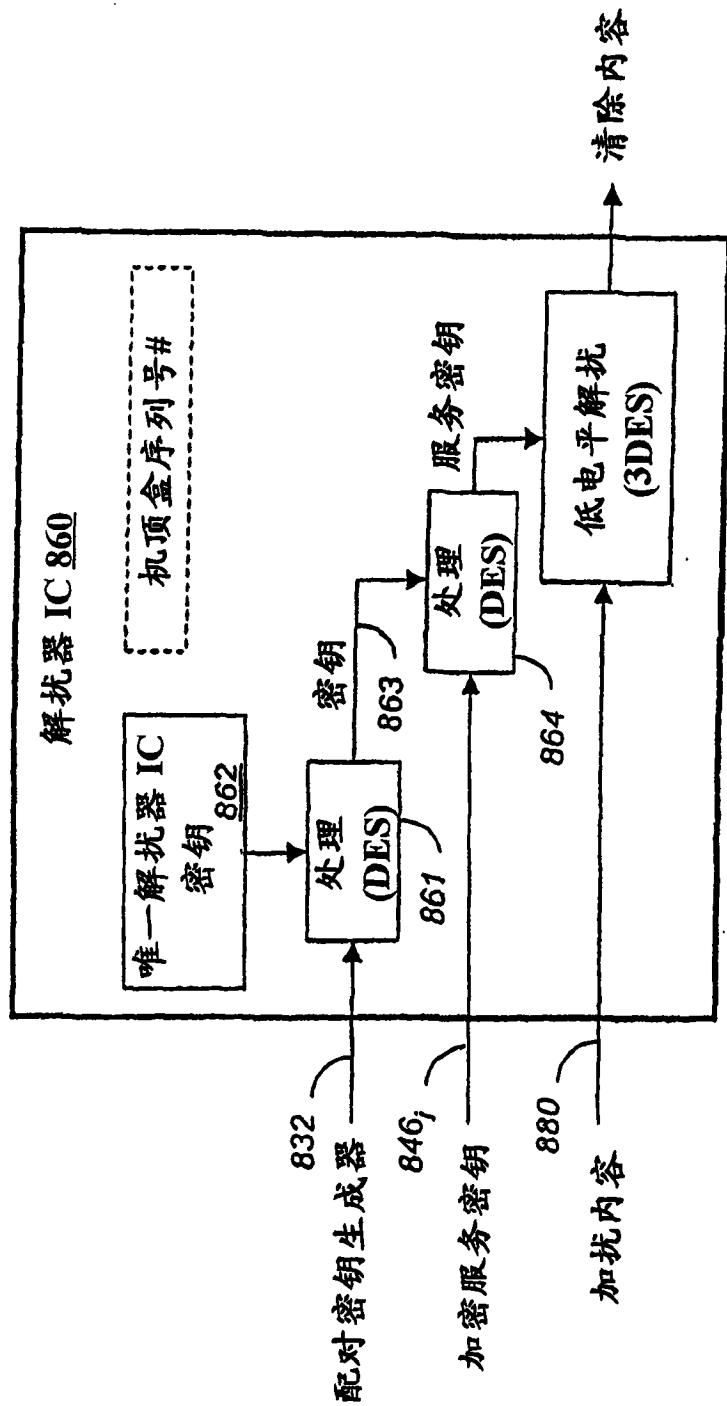


图 10

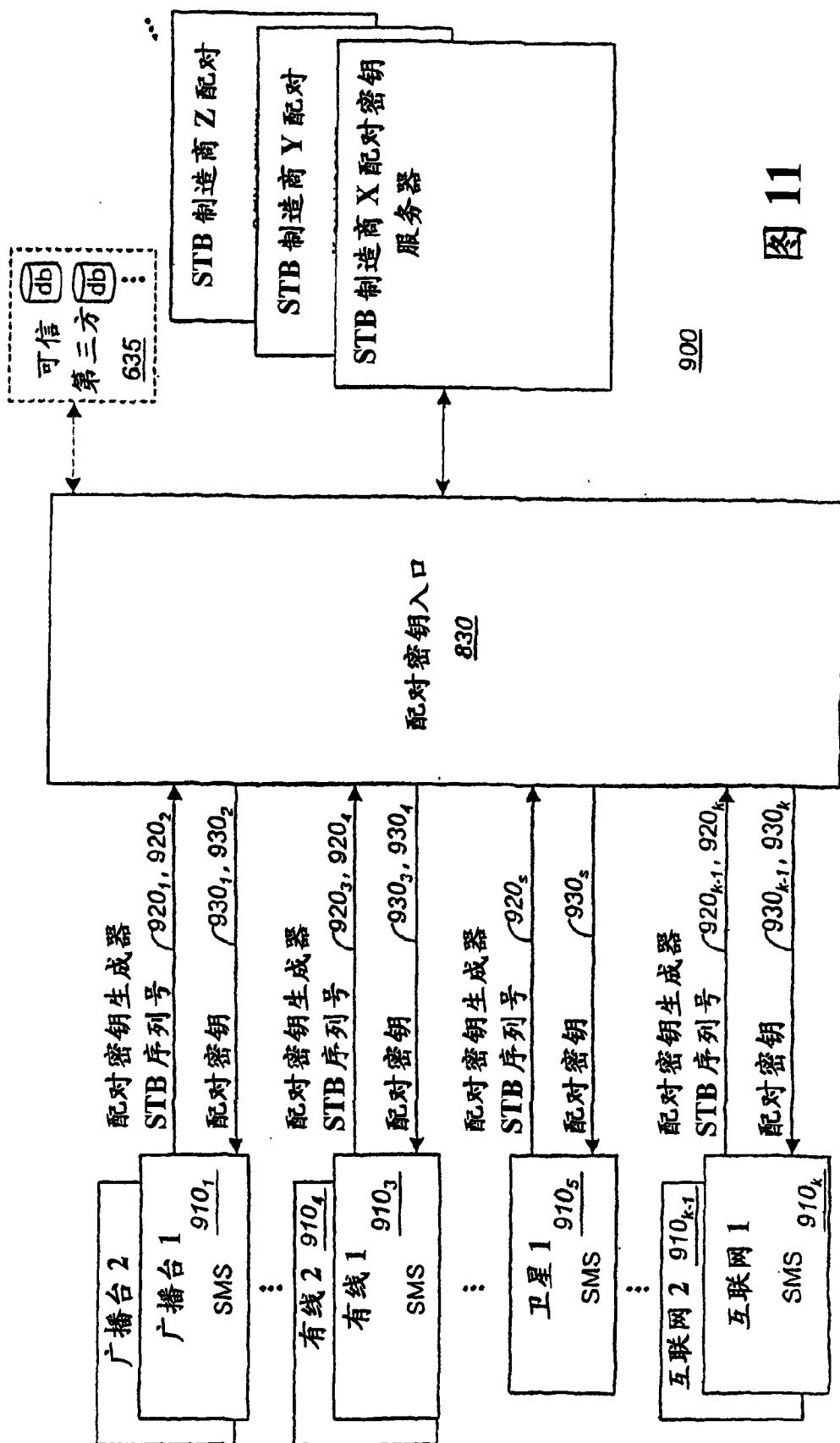


图 11

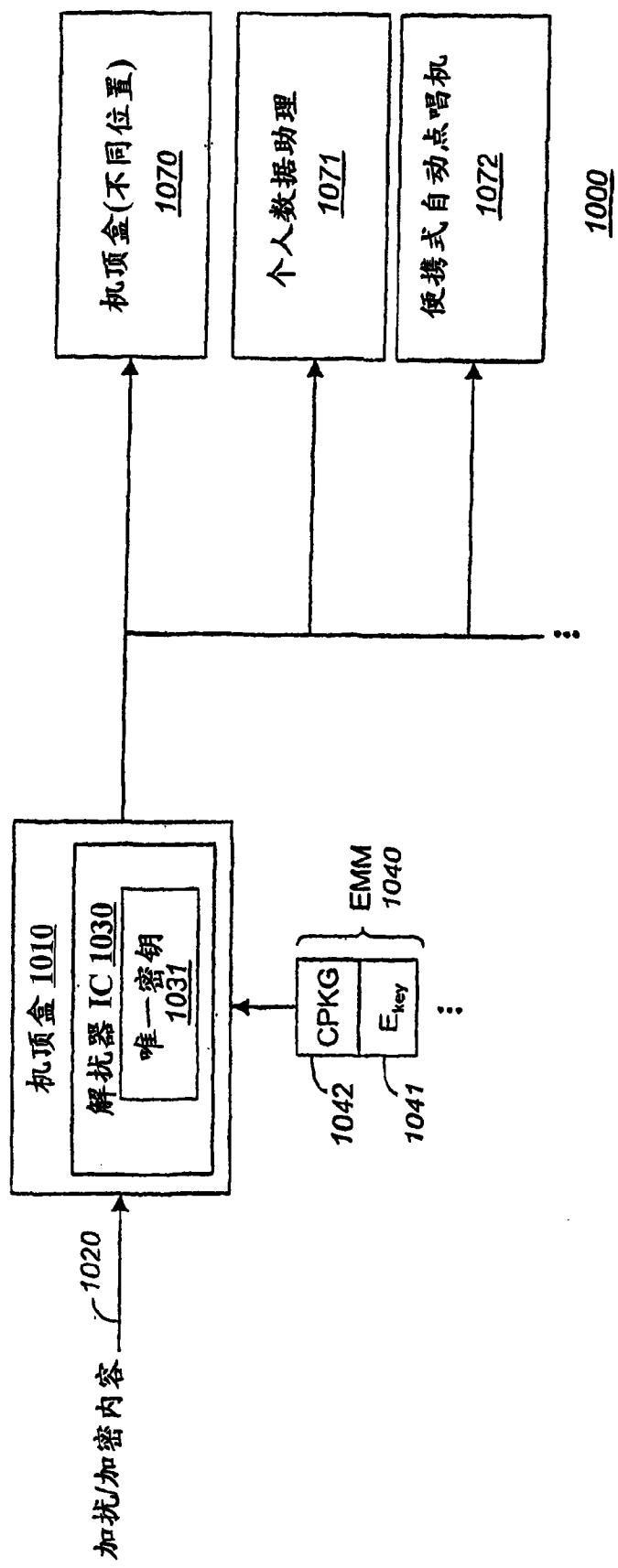


图 12

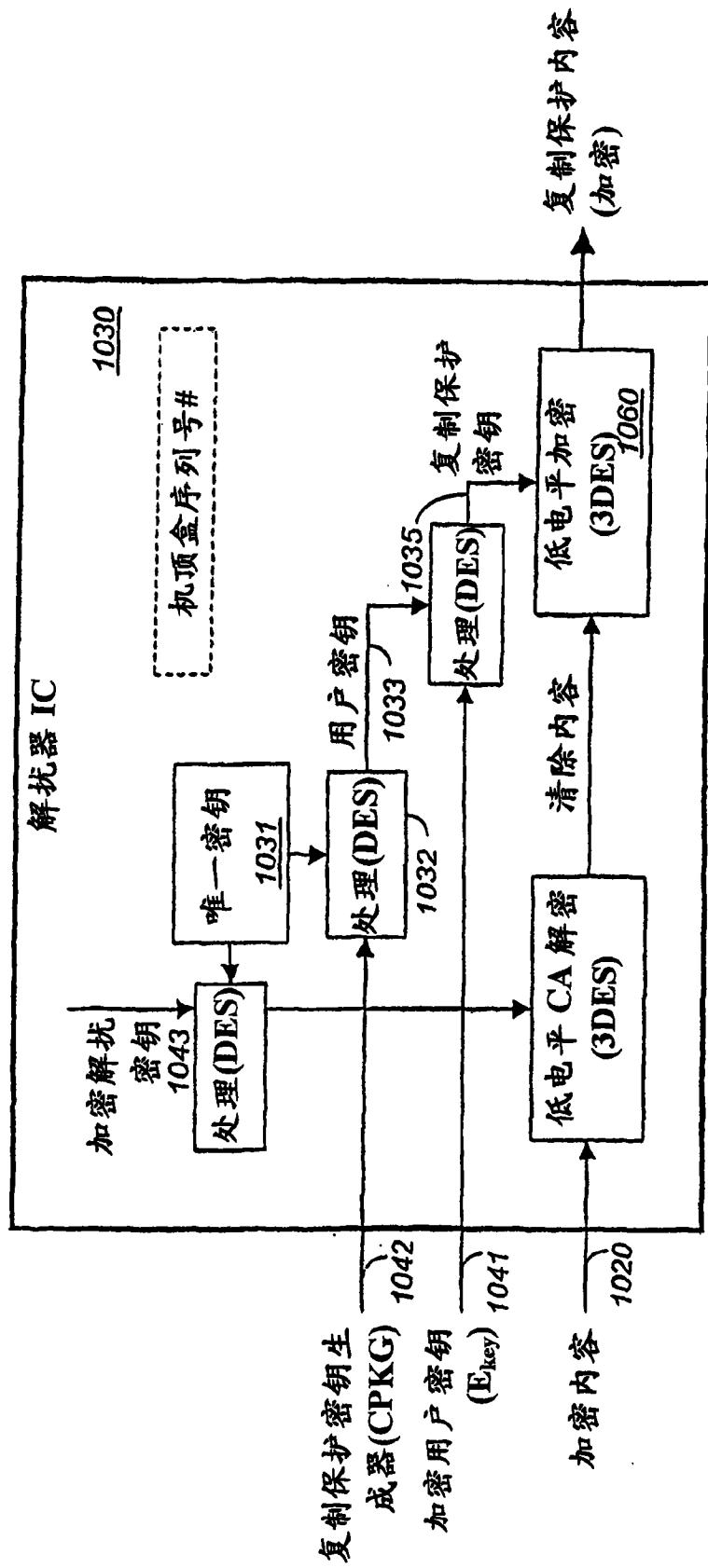


图 13

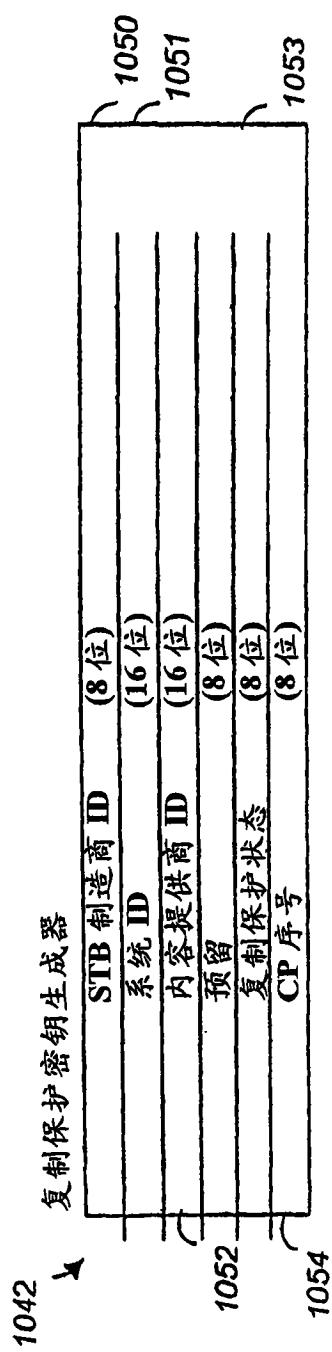


图 14

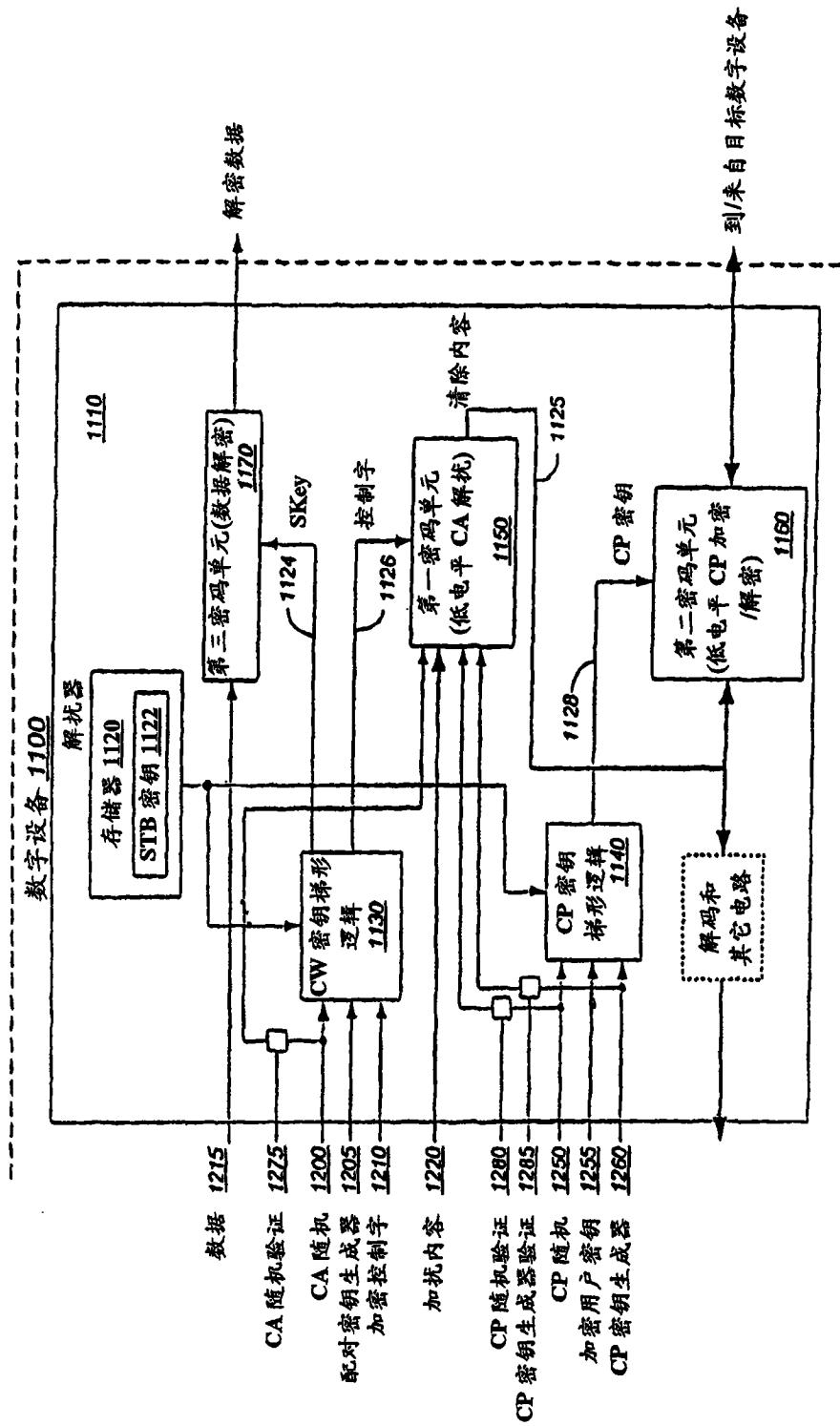


图 15

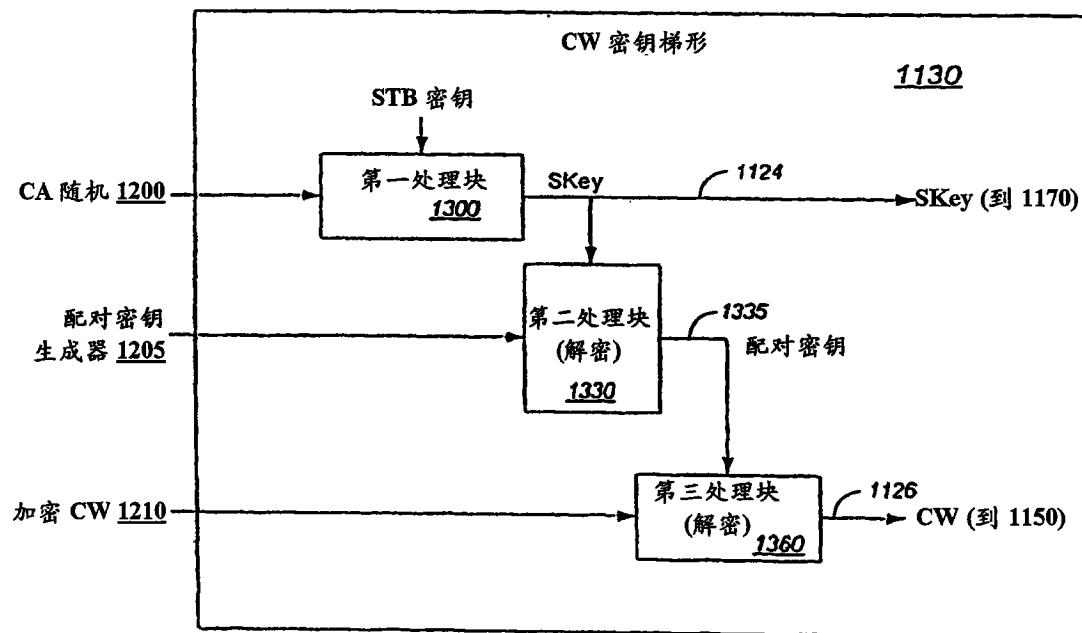


图 16

图 17A

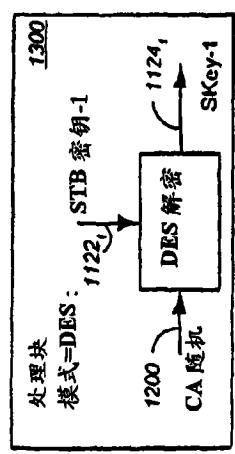


图 17B

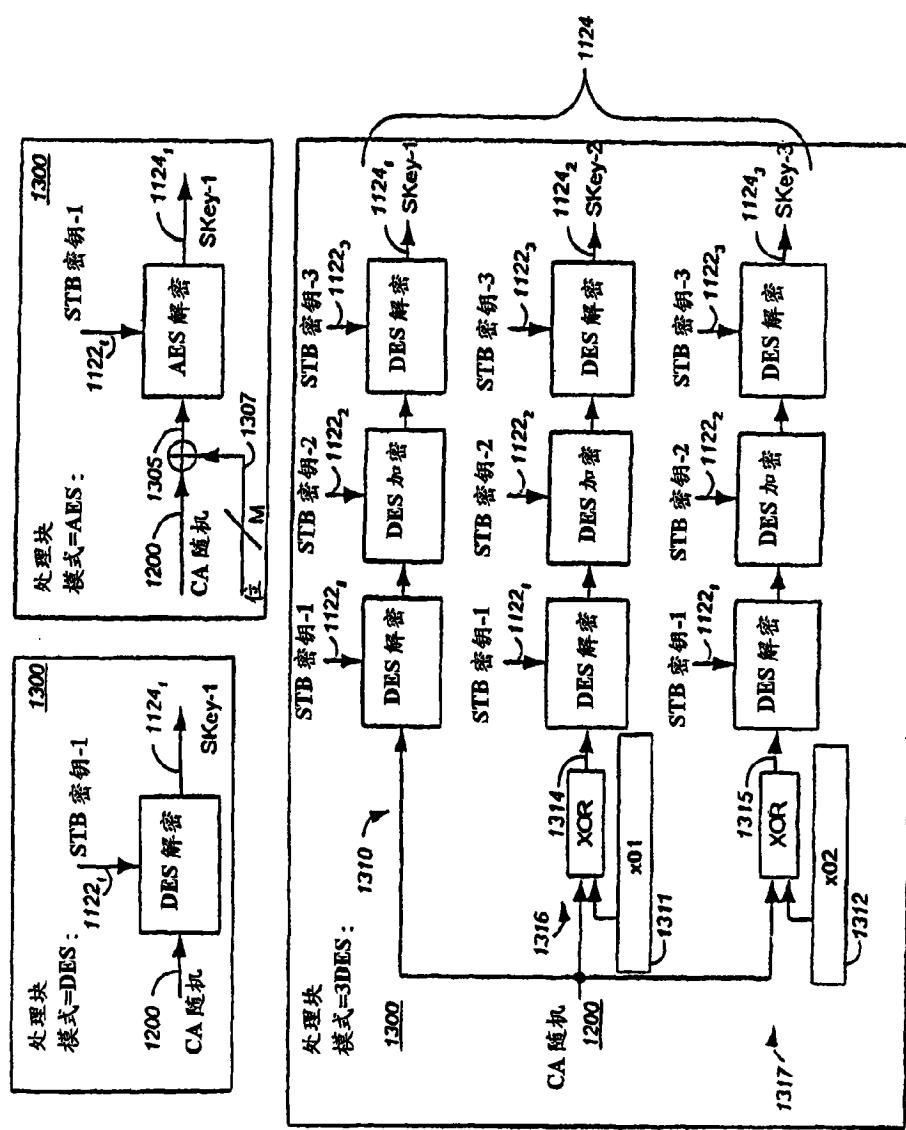


图 17C

图 18A

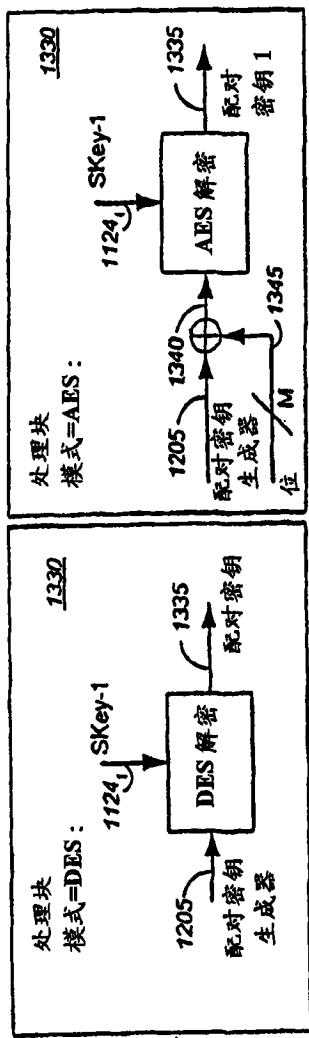


图 18B

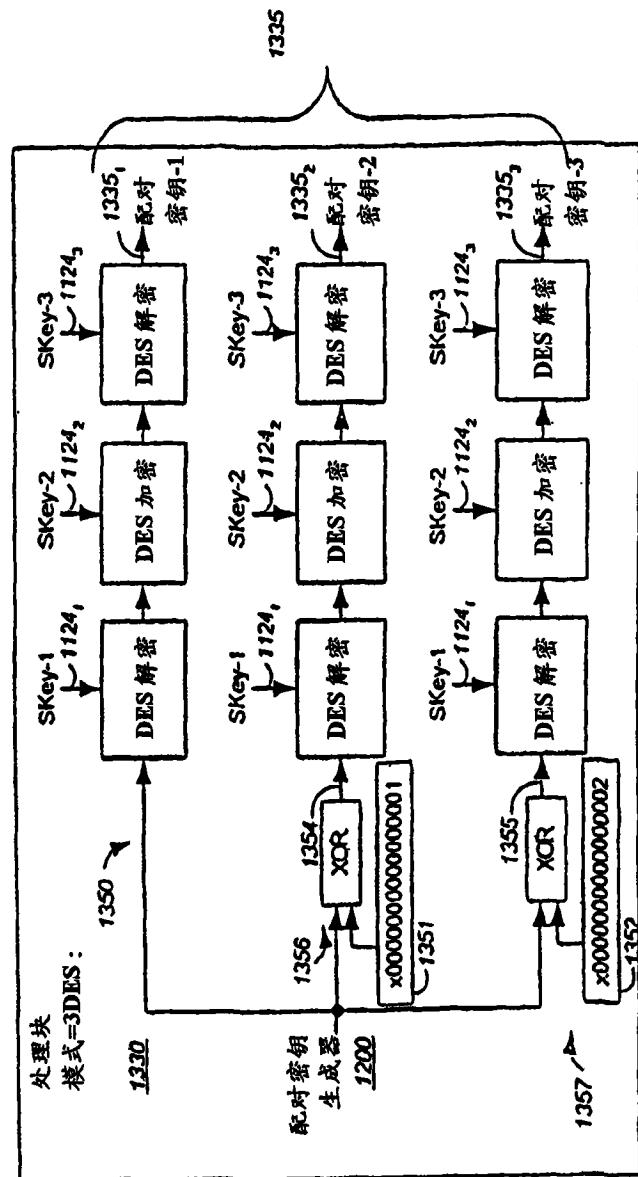


图 18C

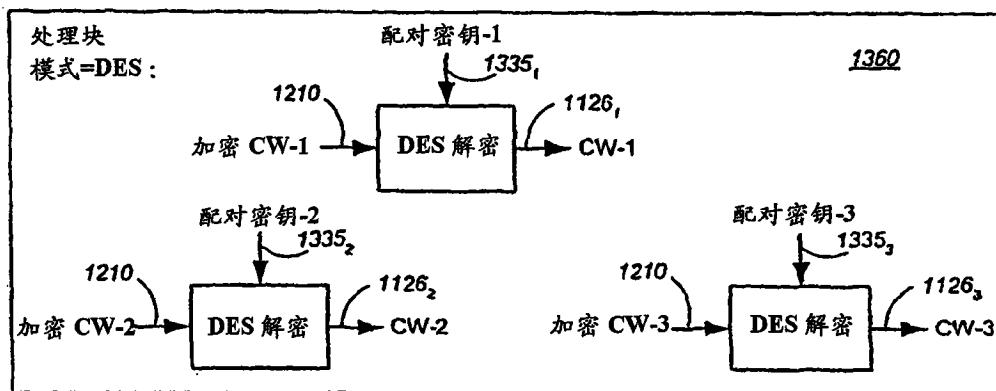


图 19A

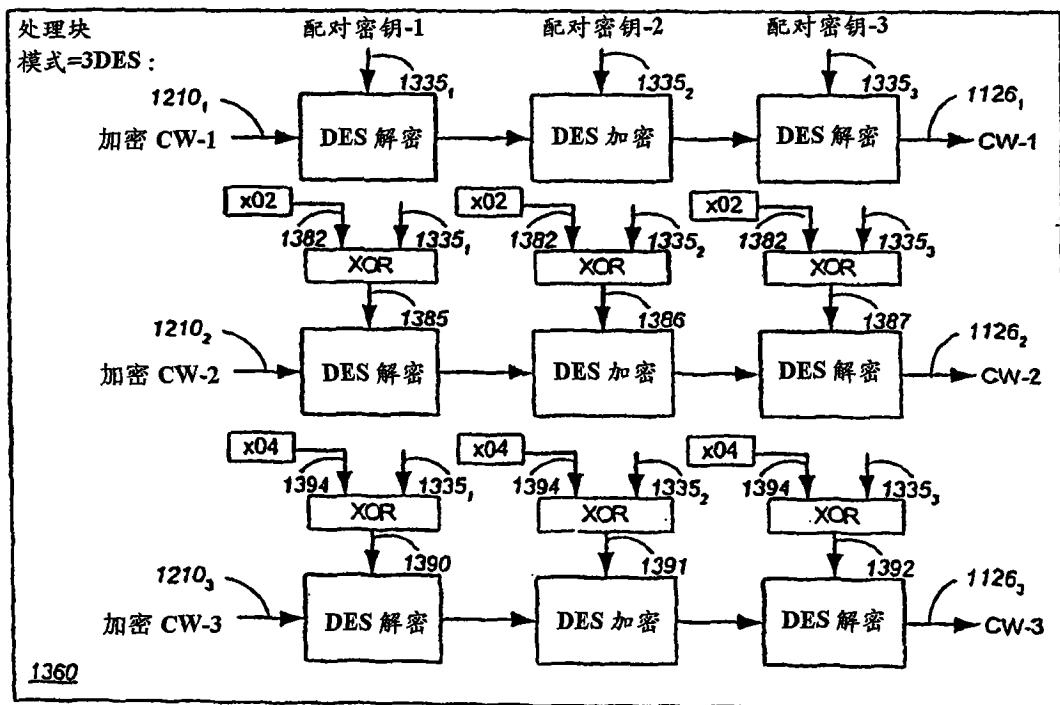


图 19C

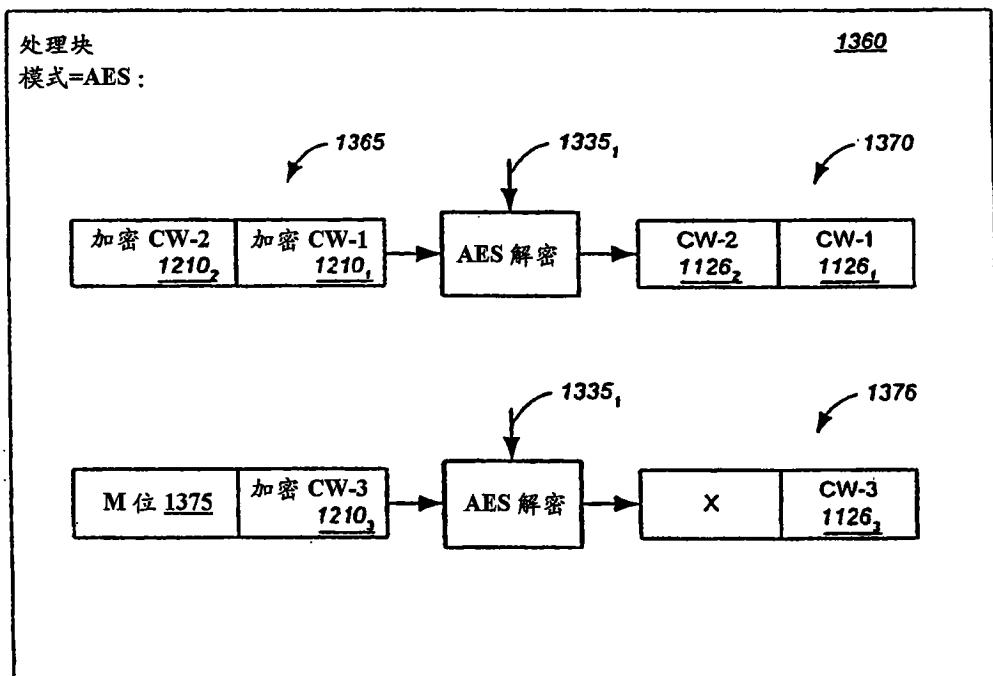


图 19B

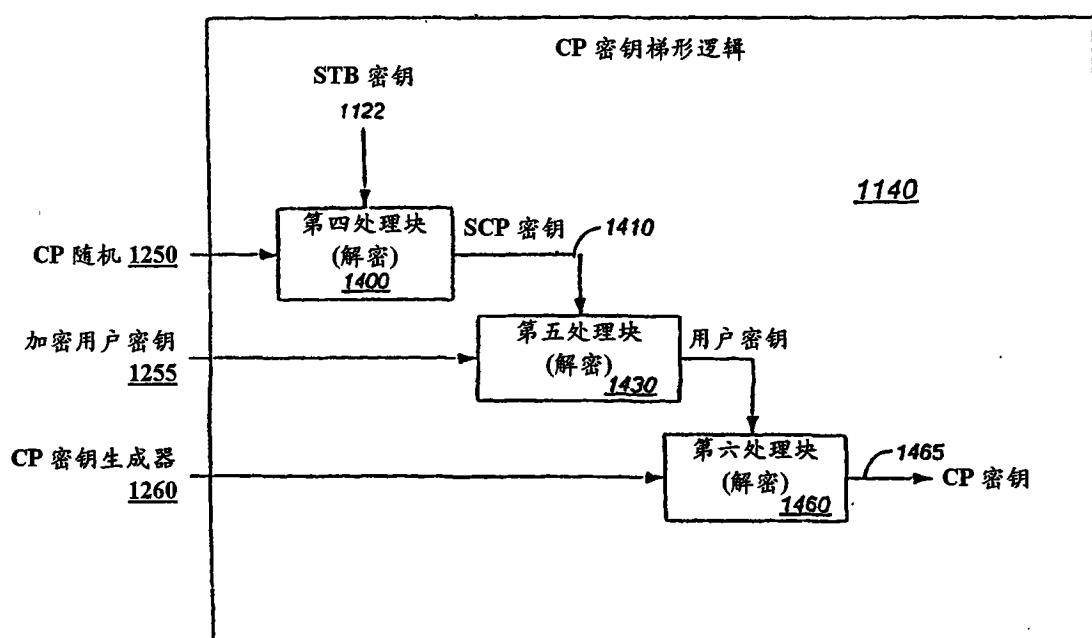


图 20

图 21A

图 21B

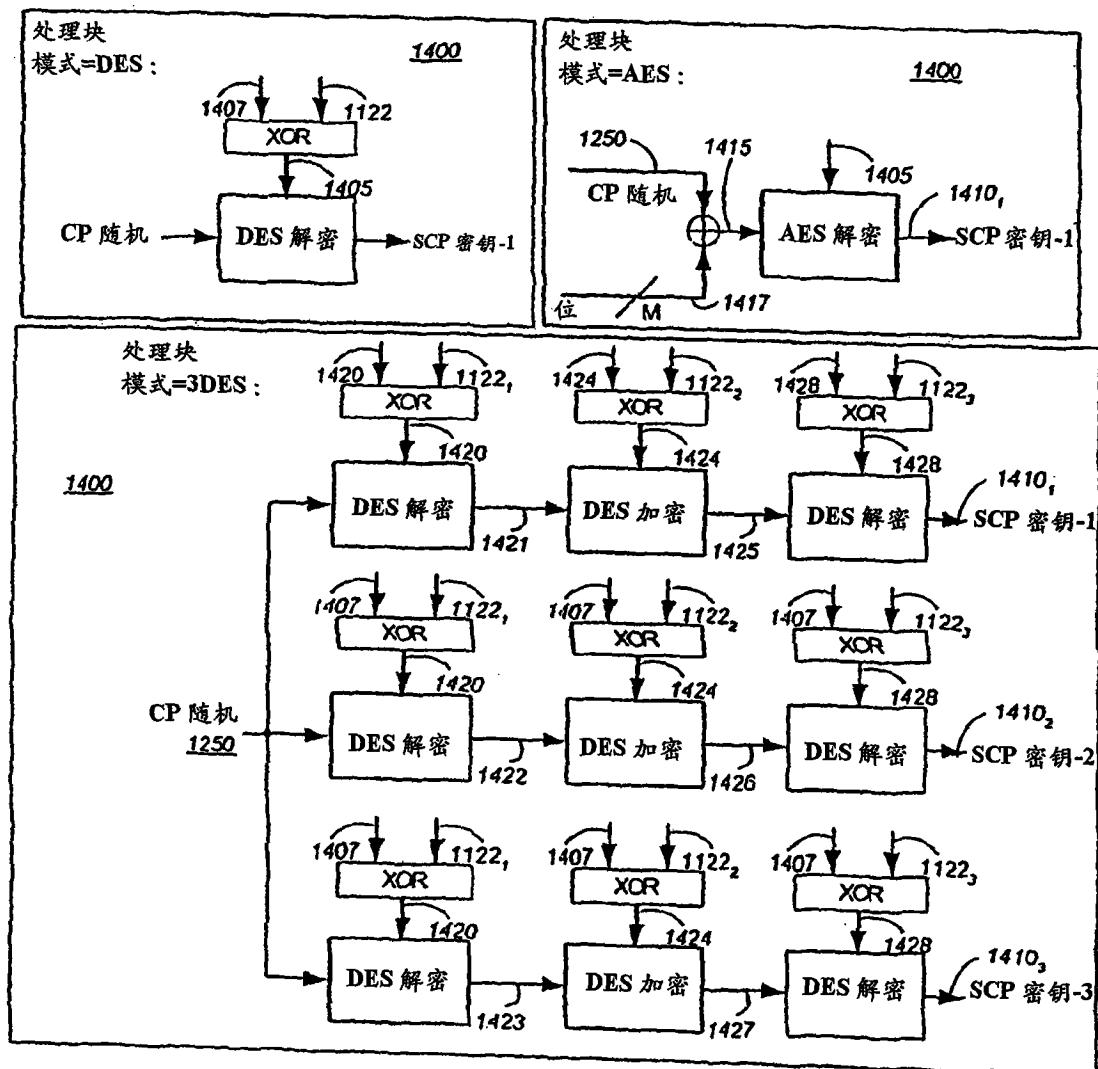


图 21C

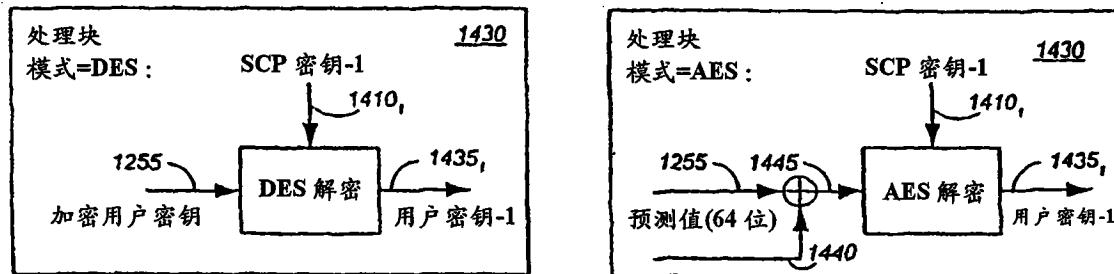


图 22A

图 22B

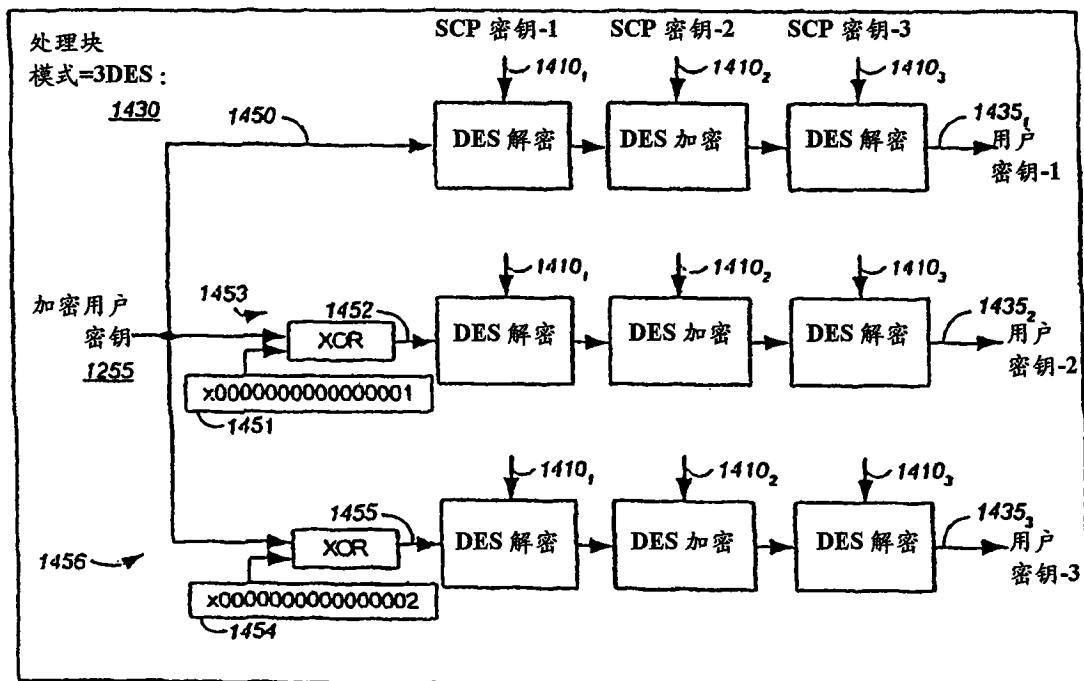


图 22C

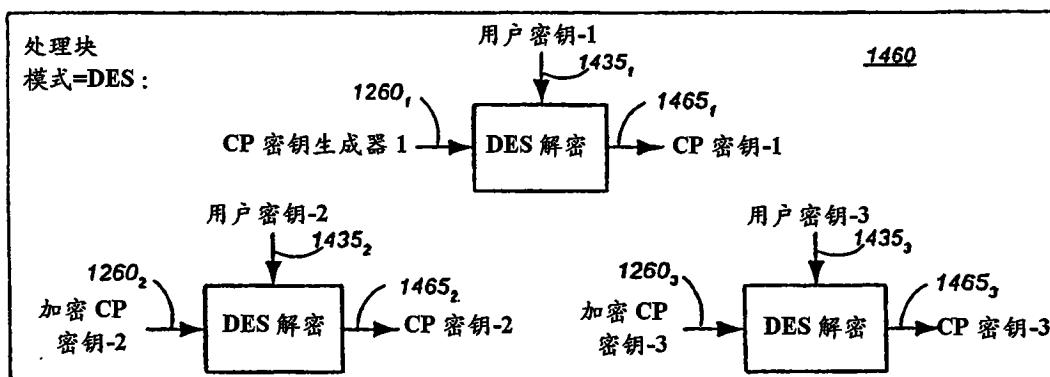


图 23A

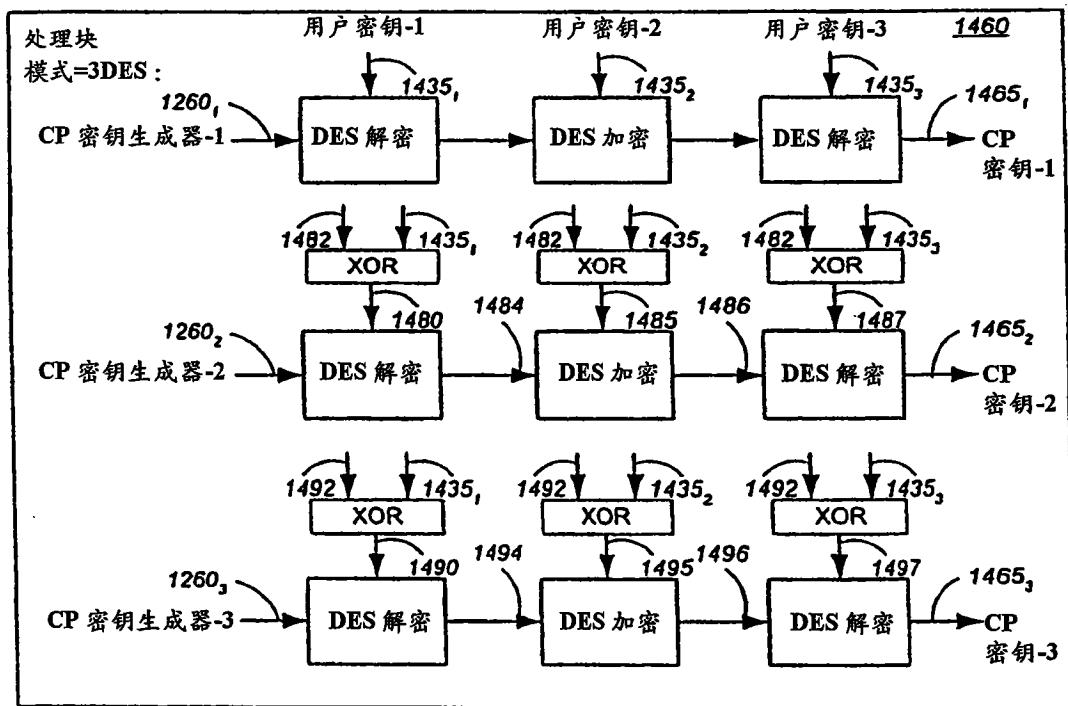


图 23C

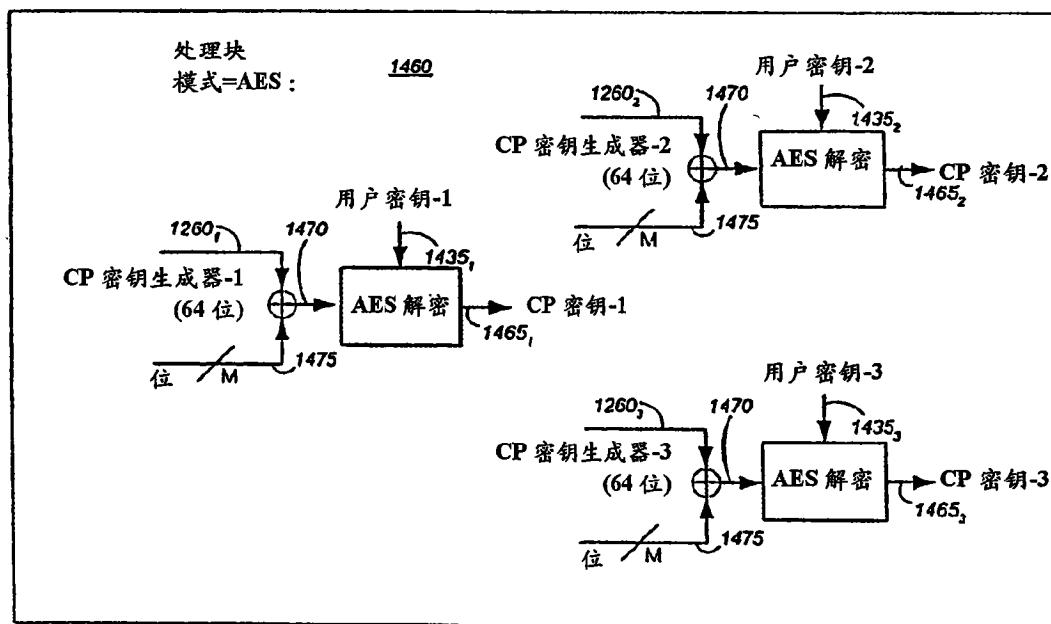


图 23B

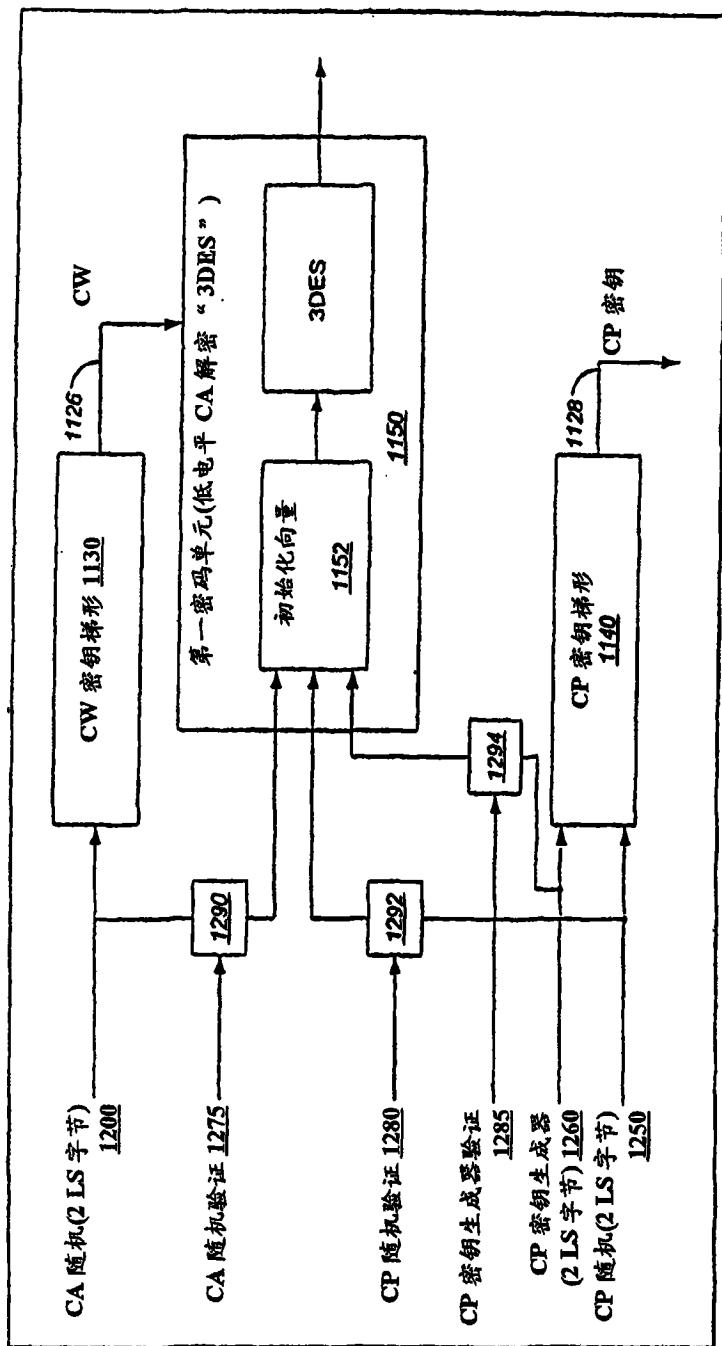


图 24

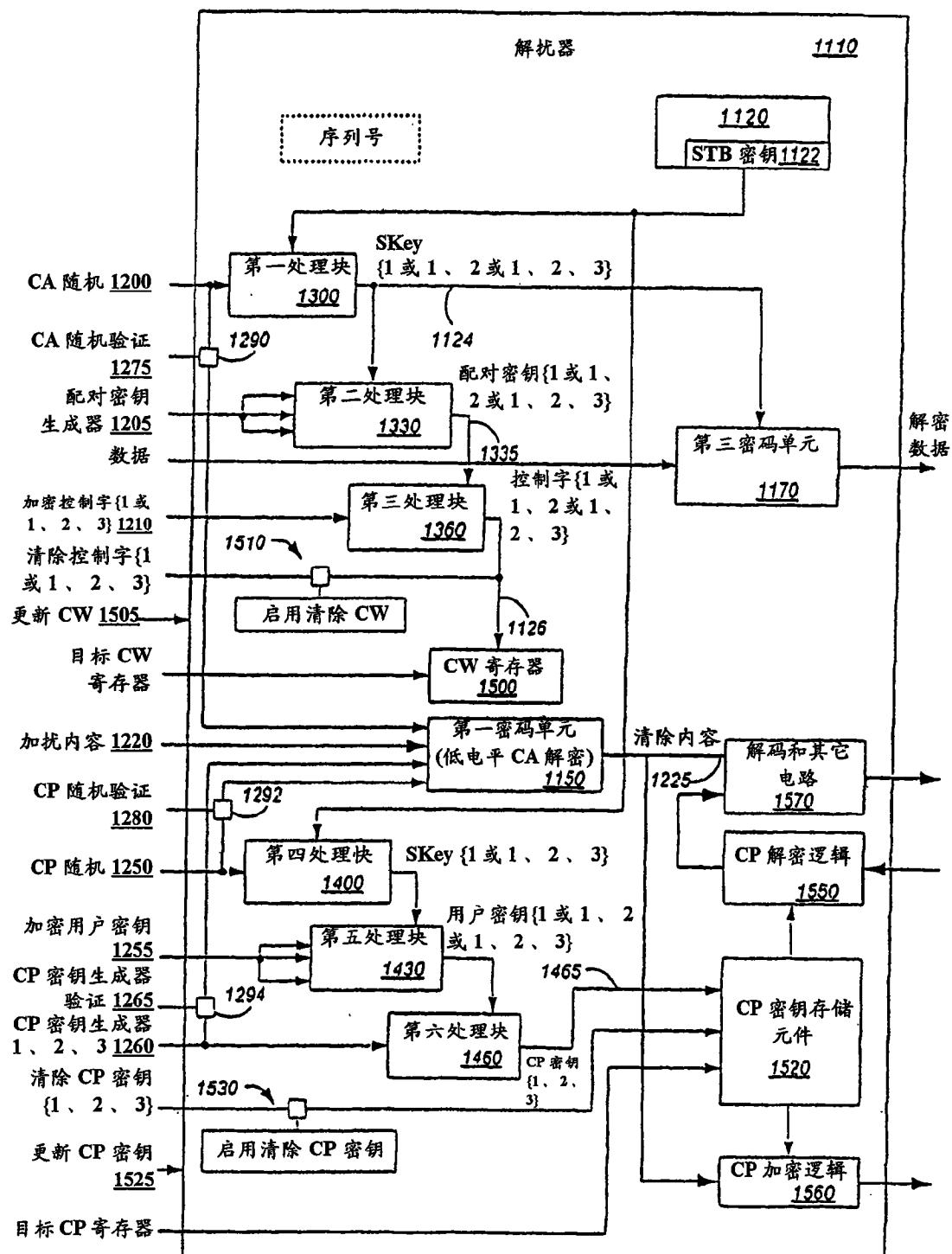


图 25