(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101409616 B
(45)授权公告日 2011.07.13

(21)申请号 200810169878.2

(22)申请日 2008.10.10

(30)优先权数据
2007-264967 2007.10.10 JP
2008-233094 2008.09.11 JP

(73)专利权人 佳能株式会社
地址 日本东京

(72)发明人 堀田博久 熊取谷昭彦

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 宋海宁

(51)Int.Cl.
H04L 9/06(2006.01)
G06F 7/00(2006.01)

(56)对比文件
CN 1921382 A,2007.02.28,
CN 1672352 A,2005.09.21,
US 2004/0071287 A1,2004.04.15,

审查员 文娟

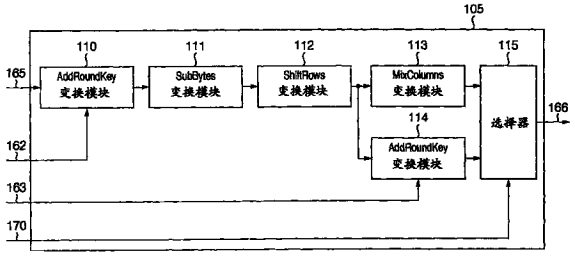
权利要求书 7 页 说明书 49 页 附图 74 页

(54)发明名称

AES 加密/解密电路

(57)摘要

本发明通过减小在每个时钟周期时段用于每个子块变换的信号处理时间总和之间的差,使得比以前更小的硬件实现AES加密或解密所要求的周期次数。为此,加密/解密电路包括第一AddRoundKey变换模块、第二AddRoundKey变换模块、ShiftRows变换模块、SubBytes变换模块、MixColumns变换模块及数据保持单元,其中在加密周期,第一AddRoundKey变换模块和第二AddRoundKey变换模块使用不同的轮回密钥被执行。



CN 101409616 B

1. 一种 AES 加密 / 解密电路，包括：

第一 AddRoundKey 变换模块；

第二 AddRoundKey 变换模块；

ShiftRows 变换模块；

SubBytes 变换模块；

MixColumns 变换模块；

第一选择器 (115)；

第二选择器 (107)；及

数据保持单元，

其特征在于：

在加密周期中，所述第一 AddRoundKey 变换模块和所述第二 AddRoundKey 变换模块使用不同的轮回密钥被执行，

所述第一 AddRoundKey 变换模块 (110) 接收输入信号 (165) 和第一轮回密钥 (A 162) 并且执行 AddRoundKey 变换，SubBytes 变换模块 (111) 接收来自所述第一 AddRoundKey 变换模块 (110) 的输出并且执行 SubBytes 变换，ShiftRows 变换模块 (112) 接收来自 SubBytes 变换模块 (111) 的输出并且执行 ShiftRows 变换，MixColumns 变换模块 (113) 接收来自 ShiftRows 变换模块 (112) 的输出并且执行 MixColumns 变换，所述第二 AddRoundKey 变换模块 (114) 接收来自 ShiftRows 变换模块 (112) 的输出和第二轮回密钥 (B 163) 并且执行 AddRoundKey 变换，第一选择器 (115) 按照选择信号 (170) 选择并输出来自 MixColumns 变换模块 (113) 的输出和来自所述第二 AddRoundKey 变换模块 (114) 的输出之一，以及

来自第一选择器 (115) 的输出 (166) 被输入到第二选择器 (107)，来自所述第二选择器 (107) 的输出 (168) 和输出保持控制信号 (160) 被输入到所述数据保持单元 (108)，并且从所述数据保持单元 (108) 输出所述 AES 加密 / 解密电路的输出信号 (151)。

2. 根据权利要求 1 所述的电路，还包括：

密钥扩展单元，它从密码密钥产生第一和第二轮回密钥，并且分别把第一和第二轮回密钥供给到所述第一和第二 AddRoundKey 变换模块；和

控制单元，它从加密开始对时钟周期进行计数，并且产生控制信号以执行加密。

3. 根据权利要求 1 所述的电路，其中

在加密的第一时钟周期，把通过对明文数据执行 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换及 MixColumns 变换得到的结果输出到所述数据保持单元，

从第二时钟周期至第 (NR-1) 时钟周期，其中 NR 是轮回数，把通过对来自所述数据保持单元的输出数据执行 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换及 MixColumns 变换得到的结果输出到所述数据保持单元，及

在第 NR 时钟周期，把通过对来自所述数据保持单元的输出数据执行第一 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换及第二 AddRoundKey 变换得到的结果输出到所述数据保持单元。

4. 一种 AES 加密 / 解密电路，包括：

第一 AddRoundKey 变换模块 (114)；

第二 AddRoundKey 变换模块 (110)；

ShiftRows 变换模块 (112)；

SubBytes 变换模块 (111)；

MixColumns 变换模块 (113)；

第一选择器 (137)；

第二选择器 (115)；

第三选择器 (107)；及

数据保持单元，

其特征在于：

在加密周期中，所述第一 AddRoundKey 变换模块和所述第二 AddRoundKey 变换模块使用不同的轮回密钥被执行，

所述第一 AddRoundKey 变换模块 (114) 接收输入信号 (165) 和第一轮回密钥 (B 163) 并且执行 AddRoundKey 变换，第一选择器 (137) 按照第一选择信号 (175) 选择并输出输入信号 (165) 和来自第一 AddRoundKey 变换模块 (114) 的输出之一，SubBytes 变换模块 (111) 接收来自第一选择器 (137) 的输出并且执行 SubBytes 变换，ShiftRows 变换模块 (112) 接收来自 SubBytes 变换模块 (111) 的输出并且执行 ShiftRows 变换，MixColumns 变换模块 (113) 接收来自 ShiftRows 变换模块 (112) 的输出并且执行 MixColumns 变换，所述第二选择器 (115) 按照第二选择信号 (170) 选择并输出来自 MixColumns 变换模块 (113) 的输出和来自 ShiftRows 变换模块 (112) 的输出之一，所述第二 AddRoundKey 变换模块 (110) 接收来自第二选择器 (115) 的输出和第二轮回密钥 (A 162) 并且执行 AddRoundKey 变换，以及

所述第二 AddRoundKey 变换模块 (110) 的输出 (166) 被输入到第三选择器 (107)，来自所述第三选择器 (107) 的输出 (168) 和输出保持控制信号 (160) 被输入到所述数据保持单元 (108)，并且从所述数据保持单元 (108) 输出所述 AES 加密 / 解密电路的输出信号 (151)。

5. 一种 AES 加密 / 解密电路，包括：

第一 AddRoundKey 变换模块 (110)；

第二 AddRoundKey 变换模块 (114)；

ShiftRows 变换模块 (112)；

SubBytes 变换模块 (111)；

MixColumns 变换模块 (113)；

第一选择器 (137)；

第二选择器 (115)；

第三选择器 (107)；及

数据保持单元，

其特征在于：

在加密周期中，所述第一 AddRoundKey 变换模块和所述第二 AddRoundKey 变换模块使用不同的轮回密钥被执行，

MixColumns 变换模块 (113) 接收输入信号 (165) 并且执行 MixColumns 变换，第一选择器 (137) 按照第一选择信号 (175) 选择并输出输入信号 (165) 和来自 MixColumns 变换模块

(113) 的输出之一，第一 AddRoundKey 变换模块 (110) 接收来自第一选择器 (137) 的输出和第一轮回密钥 (A 162) 并且执行 AddRoundKey 变换，SubBytes 变换模块 (111) 接收来自第一 AddRoundKey 变换模块 (110) 的输出并且执行 SubBytes 变换，ShiftRows 变换模块 (112) 接收来自 SubBytes 变换模块 (111) 的输出并且执行 ShiftRows 变换，第二 AddRoundKey 变换模块 (114) 接收来 ShiftRows 变换模块 (112) 的输出和第二轮回密钥 (B 163) 并且执行 AddRoundKey 变换，第二选择器 (115) 按照第二选择信号 (170) 选择并输出来自 ShiftRows 变换模块 (112) 的输出和来自第二 AddRoundKey 变换模块 (114) 的输出之一，以及

第二选择器 (115) 的输出 (166) 被输入到第三选择器 (107)，来自所述第三选择器 (107) 的输出 (168) 和输出保持控制信号 (160) 被输入到所述数据保持单元 (108)，并且从所述数据保持单元 (108) 输出所述 AES 加密 / 解密电路的输出信号 (151)。

6. 一种 AES 加密 / 解密电路，包括 ：

第一 AddRoundKey 变换模块 ；

第二 AddRoundKey 变换模块 ；

InvShiftRows 变换模块 ；

InvSubBytes 变换模块 ；

InvMixColumns 变换模块，

第一选择器 (118) ；

第二选择器 (107) ；及

数据保持单元，

其特征在于 ：

在解密周期，所述第一 AddRoundKey 变换模块和所述第二 AddRoundKey 变换模块使用不同的轮回密钥被执行，

InvMixColumns 变换模块 (116) 接收输入信号 (165) 并且执行 InvMixColumns 变换，第一 AddRoundKey 变换模块 (117) 接收输入信号 (165) 和第一轮回密钥 (B 163) 并且执行 AddRoundKey 变换，第一选择器 (118) 按照选择信号 (170) 选择并输出来自 InvMixColumns 变换模块 (116) 的输出和来自第一 AddRoundKey 变换模块 (117) 的输出之一，InvShiftRows 变换模块 (119) 接收来自第一选择器 (118) 的输出并且执行 InvShiftRows 变换，InvSubBytes 变换模块 (120) 接收来自 InvShiftRows 变换模块 (119) 的输出并且执行 InvSubBytes 变换，第二 AddRoundKey 变换模块 (121) 接收来自 InvSubBytes 变换模块 (120) 的输出并且执行 AddRoundKey 变换，以及

来自第二 AddRoundKey 变换模块 (121) 的输出 (167) 被输入到第二选择器 (107)，来自所述第二选择器 (107) 的输出 (168) 和输出保持控制信号 (160) 被输入到所述数据保持单元 (108)，并且从所述数据保持单元 (108) 输出所述 AES 加密 / 解密电路的输出信号 (151)。

7. 根据权利要求 6 所述的电路，其中

在解密的第一时钟周期，把通过对密文数据执行第一 AddRoundKey 变换、InvShiftRows 变换、InvSubBytes 变换及第二 AddRoundKey 变换得到的结果输出到所述数据保持单元，

从第二时钟周期至第 (NR-1) 时钟周期，其中 NR 是轮回数，把通过对来自所述数据保持单元的输出数据执行 InvMixColumns 变换、InvShiftRows 变换、InvSubBytes 变换及

AddRoundKey 变换得到的结果输出到所述数据保持单元，及

在第 NR 时钟周期，把通过对来自所述数据保持单元的输出数据执行 InvMixColumns 变换、InvShiftRows 变换、InvSubBytes 变换及 AddRoundKey 变换得到的结果输出到所述数据保持单元。

8. 一种 AES 加密 / 解密电路，包括：

第一 AddRoundKey 变换模块 (121)；

第二 AddRoundKey 变换模块 (117)；

InvMixColumns 变换模块 (116)，

InvShiftRows 变换模块 (119)；

InvSubBytes 变换模块 (120)；

第一选择器 (118)；

第二选择器 (138)；

第三选择器 (107)；及

数据保持单元，

其特征在于：

在解密周期，所述第一 AddRoundKey 变换模块和所述第二 AddRoundKey 变换模块使用不同的轮回密钥被执行，

所述第一 AddRoundKey 变换模块 (121) 接收输入信号 (165) 和第一轮回密钥 (A 162) 并且执行 AddRoundKey 变换，所述 InvMixColumns 变换模块 (116) 接收来自所述第一 AddRoundKey 变换模块 (121) 的输出并且执行 InvMixColumns 变换，所述第一选择器 (118) 按照第一选择信号 (170) 选择并输出来自所述 InvMixColumns 变换模块 (116) 的输出和来自所述第一 AddRoundKey 变换模块 (121) 的输出之一，所述 InvShiftRows 变换模块 (119) 接收来自所述第一选择器 (118) 的输出并且执行 InvShiftRows 变换，所述 InvSubBytes 变换模块 (120) 接收来自所述 InvShiftRows 变换模块 (119) 的输出并且执行 InvSubBytes 变换，所述第二 AddRoundKey 变换模块 (117) 接收来自所述 InvSubBytes 变换模块 (120) 的输出和第二轮回密钥 (B 163) 并且执行 AddRoundKey 变换，第二选择器 (138) 按照第二选择信号 (175) 选择并输出来自所述 InvSubBytes 变换模块 (120) 的输出和来自第二 AddRoundKey 变换模块 (117) 的输出之一，以及

所述第二选择器 (138) 的输出 (167) 被输入到所述第三选择器 (107)，来自所述第三选择器 (107) 的输出 (168) 和输出保持控制信号 (160) 被输入到所述数据保持单元 (108)，并且从所述数据保持单元 (108) 输出所述 AES 加密 / 解密电路的输出信号 (151)。

9. 一种 AES 加密 / 解密电路，包括：

第一 AddRoundKey 变换模块；

第二 AddRoundKey 变换模块；

第三 AddRoundKey 变换模块；

第一 ShiftRows 变换模块；

第二 ShiftRows 变换模块；

第一 SubBytes 变换模块；

第二 SubBytes 变换模块；

第一 MixColumns 变换模块；

第二 MixColumns 变换模块；

第一选择器 (115)；

第二选择器 (107)；及

数据保持单元，

其特征在于：

在加密周期，所述第一 AddRoundKey 变换模块、所述第二 AddRoundKey 变换模块及所述第三 AddRoundKey 变换模块使用不同的轮回密钥被执行，

第一 AddRoundKey 变换模块 (110) 接收输入信号 (165) 和第一轮回密钥 (A1462) 并且执行 AddRoundKey 变换，第一 SubBytes 变换模块 (111) 接收来自第一 AddRoundKey 变换模块 (110) 的输出并且执行 SubBytes 变换，第一 ShiftRows 变换模块 (112) 接收来自第一 SubBytes 变换模块 (111) 的输出并且执行 ShiftRows 变换，第一 MixColumns 变换模块 (113) 接收来自第一 ShiftRows 变换模块 (112) 的输出并且执行 MixColumns 变换，以及

第二 AddRoundKey 变换模块 (110) 接收来自第一 MixColumns 变换模块 (113) 的输出 (475) 和第二轮回密钥 (A2463) 并且执行 AddRoundKey 变换，第二 SubBytes 变换模块 (111) 接收来自第二 AddRoundKey 变换模块 (110) 的输出并且执行 SubBytes 变换，第二 ShiftRows 变换模块 (112) 接收来自第二 SubBytes 变换模块 (111) 的输出并且执行 ShiftRows 变换，第二 MixColumns 变换模块 (113) 接收来自第二 ShiftRows 变换模块 (112) 的输出并且执行 MixColumns 变换，第三 AddRoundKey 变换模块 (114) 接收来自第二 ShiftRows 变换模块 (112) 的输出和第三轮回密钥 (B 163) 并且执行 AddRoundKey 变换，第一选择器 (115) 按照选择信号 (170) 选择并输出来自第二 MixColumns 变换模块 (113) 的输出和来自第三 AddRoundKey 变换模块 (114) 的输出之一，以及

来自第一选择器 (115) 的输出 (166) 被输入到第二选择器 (107)，来自所述第二选择器 (107) 的输出 (168) 和输出保持控制信号 (160) 被输入到所述数据保持单元 (108)，并且从所述数据保持单元输出所述 AES 加密 / 解密电路的输出信号 (151)。

10. 根据权利要求 9 所述的电路，其中

在加密的第一时钟周期，把通过对明文数据执行第一 AddRoundKey 变换、第一 SubBytes 变换、第一 ShiftRows 变换、第一 MixColumns 变换、第二 AddRoundKey 变换、第二 SubBytes 变换、第二 ShiftRows 变换及第二 MixColumns 变换得到的结果输出到所述数据保持单元，

从第二时钟周期至第 (NR/2-1) 时钟周期，其中 NR 是轮回数，把通过对来自所述数据保持单元的输出数据执行第一 AddRoundKey 变换、第一 SubBytes 变换、第一 ShiftRows 变换、第一 MixColumns 变换、第二 AddRoundKey 变换、第二 SubBytes 变换、第二 ShiftRows 变换及第二 MixColumns 变换得到的结果输出到所述数据保持单元，及

在第 (NR/2) 时钟周期，把通过对来自所述数据保持单元的输出数据执行第一 AddRoundKey 变换、第一 SubBytes 变换、第一 ShiftRows 变换、第一 MixColumns 变换、第二 AddRoundKey 变换、第二 SubBytes 变换、第二 ShiftRows 变换及第三 AddRoundKey 变换得到的结果输出到所述数据保持单元。

11. 一种 AES 加密 / 解密电路，包括：

第一 AddRoundKey 变换模块；

第二 AddRoundKey 变换模块；

第三 AddRoundKey 变换模块；

第一 InvShiftRows 变换模块；

第二 InvShiftRows 变换模块；

第一 InvSubBytes 变换模块；

第二 InvSubBytes 变换模块；

第一 InvMixColumns 变换模块；

第二 InvMixColumns 变换模块；

第一选择器 (118)；

第二选择器 (107)；及

数据保持单元，

其特征在于：

在解密周期，所述第一 AddRoundKey 变换模块、所述第二 AddRoundKey 变换模块及所述第三 AddRoundKey 变换模块使用不同的轮回密钥被执行，

第一 InvMixColumns 变换模块 (116) 接收输入信号 (165) 并且执行 InvMixColumns 变换，第一 AddRoundKey 变换模块 (121) 接收输入信号 (165) 和第一轮回密钥 (B 163) 并且执行 AddRoundKey 变换，第一选择器 (118) 按照选择信号 (170) 选择并输出来自第一 InvMixColumns 变换模块 (116) 的输出和来自第一 AddRoundKey 变换模块 (121) 的输出之一，第一 InvShiftRows 变换模块 (119) 接收来自第一选择器 (118) 的输出并且执行 InvShiftRows 变换，第一 InvSubBytes 变换模块 (120) 接收来自第一 InvShiftRows 变换模块 (119) 的输出并且执行 InvSubBytes 变换，第二 AddRoundKey 变换模块 (117) 接收来自第一 InvSubBytes 变换模块 (120) 的输出和第二轮回密钥 (A1462) 并且执行 AddRoundKey 变换，

第二 InvMixColumns 变换模块 (116) 接收来自第二 AddRoundKey 变换模块 (117) 的输出 (476) 并且执行 InvMixColumns 变换，第二 InvShiftRows 变换模块 (119) 接收来自第二 InvMixColumns 变换模块 (116) 的输出并且执行 InvShiftRows 变换，第二 InvSubBytes 变换模块 (120) 接收来自第二 InvShiftRows 变换模块 (119) 的输出并且执行 InvSubBytes 变换，第三 AddRoundKey 变换模块 (117) 接收来自第二 InvSubBytes 变换模块 (120) 的输出和第三轮回密钥 (A2463) 并且执行 AddRoundKey 变换，以及

来自第三 AddRoundKey 变换模块 (117) 的输出 (167) 被输入到第二选择器 (107)，来自第二选择器 (107) 的输出 (168) 和输出保持控制信号 (160) 被输入到所述数据保持单元 (108)，并且从所述数据保持单元 (108) 输出所述 AES 加密 / 解密电路的输出信号 (151)。

12. 根据权利要求 11 所述的电路，其中

在解密的第一时钟周期，把通过对密文数据执行第一 AddRoundKey 变换、第一 InvSubBytes 变换、第一 InvShiftRows 变换、第一 InvMixColumns 变换、第二 AddRoundKey 变换、第二 InvSubBytes 变换、第二 InvShiftRows 变换及第二 InvMixColumns 变换得到的结果输出到所述数据保持单元，

从第二时钟周期至第 (NR/2-1) 时钟周期，其中 NR 是轮回数，把通过对来自所述数据保

持单元的输出数据执行第一 AddRoundKey 变换、第一 InvSubBytes 变换、第一 InvShiftRows 变换、第一 InvMixColumns 变换、第二 AddRoundKey 变换、第二 InvSubBytes 变换、第二 InvShiftRows 变换及第二 InvMixColumns 变换得到的结果输出到所述数据保持单元，及

在第 (NR/2) 时钟周期，把通过对来自所述数据保持单元的输出数据执行第一 AddRoundKey 变换、第一 InvSubBytes 变换、第一 InvShiftRows 变换、第一 InvMixColumns 变换、第二 AddRoundKey 变换、第二 InvSubBytes 变换、第二 InvShiftRows 变换及第三 AddRoundKey 变换得到的结果输出到所述数据保持单元。

AES 加密 / 解密电路

技术领域

[0001] 本发明涉及一种用来执行由 FIPS(联邦信息处理标准)197 定义的 AES(高级加密标准) 时理的 AES 加密 / 解密电路。

背景技术

[0002] 随着光纤网络的最近改进，每个人都能容易地在互联网上使用高速通信。这也便于诸如高质量视频发行之类的海量数据通信。然而，有对网络的威胁，包括窃听、改变及欺骗。为了保护网络通信免受这些威胁，对于加密的需要已经增长。

[0003] 尽管加密对于可靠通信是基本的，但是不期望传输速率的任何降低。这种趋势在处理大量数据的视频发行领域特别明显。为了以高速可靠地传输大量数据，高速加密是必要的。

[0004] 海量加密通信一般使用对称块密码。

[0005] 最广泛使用的对称块密码是由 FIPS(联邦信息处理标准)197 定义的 AES。

[0006] 为了对付高速加密通信，AES 需要使用专用硬件加速器加速。

[0007] 图 60A 和 60B 表示 AES 加密和解密算法。在图 60A 和 60B 中的 AddRoundKey、SubBytes、ShiftRows、MixColumns、InvSubBytes、InvShiftRows 及 InvMixColumns 是相同名称的处理，这些处理在 FIPS197 中定义为子块变换。NR 是按照密钥长度确定的轮回次数，在 AES-128 中是 10、在 AES-192 中是 12、或在 AES-256 中是 14。

[0008] 如图 60A 和 60B 所示，AES 算法在 AddRoundKey 之后重复由标准 NR 次数定义的轮回函数。轮回函数包括用于加密的四个处理 -SubBytes、ShiftRows、MixColumns 及 AddRoundKey ；和用于解密的四个处理 -InvShiftRows、InvSubBytes、AddRoundKey 及 InvMixColumns。例外地，第 NR 次的轮回函数包括用于加密的三个处理 -SubBytes、ShiftRows 及 AddRoundKey ；和用于解密的三个处理 -InvShiftRows、InvSubBytes 及 AddRoundKey。AddRoundKey 变换要求从密码密钥产生的、并且具有每轮回变化的值的轮回密钥 wkeyi(FIPS197 描述的轮回密钥 ;i 是轮回数)。

[0009] 为了把 AES 算法实施成硬件，所有 AES 信号处理都必须划分成可在供给到 AES 电路中的 1 个时钟周期时段内执行的处理。例如，在一般实施方法中，一个轮回函数在一个时钟周期内执行，两个轮回函数在一个时钟周期内执行，或一个轮回函数在两个时钟周期内执行。

[0010] 在常规方法中，AES-128 的加密和解密当一个轮回函数在一个时钟周期内执行时要求 11 个时钟周期，当两个轮回函数在一个时钟周期内执行时要求 6 个时钟周期，及当一个轮回函数在两个时钟周期内执行时要求 22 个时钟周期。

[0011] 硬件实施的 AES 算法可实现预定水平的高速处理。然而，要求 AES 处理速度更高。

发明内容

[0012] 本发明考虑上述情形而形成，并且提供一种通过减少加密和解密所要求的周期次

数以更高速度执行 AES 处理的加密 / 解密电路。

[0013] 本发明在第一方面提供一种 AES 加密 / 解密电路，该 AES 加密 / 解密电路包括

[0014] 第一 AddRoundKey 变换模块；

[0015] 第二 AddRoundKey 变换模块；

[0016] ShiftRows 变换模块；

[0017] SubBytes 变换模块；

[0018] MixColumns 变换模块；及

[0019] 数据保持单元，

[0020] 其中在加密周期中，第一 AddRoundKey 变换模块和第二 AddRoundKey 变换模块使用不同的轮回密钥被执行。

[0021] 本发明在第二方面提供一种 AES 加密 / 解密电路，该 AES 加密 / 解密电路包括

[0022] 第一 AddRoundKey 变换模块；

[0023] 第二 AddRoundKey 变换模块；

[0024] InvShiftRows 变换模块；

[0025] InvSubBytes 变换模块；

[0026] InvMixColumns 变换模块；及

[0027] 数据保持单元，

[0028] 其中在解密周期中，第一 AddRoundKey 变换模块和第二 AddRoundKey 变换模块使用不同的轮回密钥被执行。

[0029] 本发明在第三方面提供一种 AES 加密 / 解密电路，该 AES 加密 / 解密电路包括

[0030] 第一 AddRoundKey 变换模块；

[0031] 第二 AddRoundKey 变换模块；

[0032] 第三 AddRoundKey 变换模块；

[0033] 第一 ShiftRows 变换模块；

[0034] 第二 ShiftRows 变换模块；

[0035] 第一 SubBytes 变换模块；

[0036] 第二 SubBytes 变换模块；

[0037] 第一 MixColumns 变换模块；

[0038] 第二 MixColumns 变换模块；及

[0039] 数据保持单元，

[0040] 其中在加密周期中，第一 AddRoundKey 变换模块、第二 AddRoundKey 变换模块及第三 AddRoundKey 变换模块使用不同的轮回密钥被执行。

[0041] 本发明在第四方面提供一种 AES 加密 / 解密电路，该 AES 加密 / 解密电路包括

[0042] 第一 AddRoundKey 变换模块；

[0043] 第二 AddRoundKey 变换模块；

[0044] 第三 AddRoundKey 变换模块；

[0045] 第一 InvShiftRows 变换模块；

[0046] 第二 InvShiftRows 变换模块；

[0047] 第一 InvSubBytes 变换模块；

[0048] 第二 InvSubBytes 变换模块；

[0049] 第一 InvMixColumns 变换模块；

[0050] 第二 InvMixColumns 变换模块；及

[0051] 数据保持单元，

[0052] 其中在解密周期中，第一 AddRoundKey 变换模块、第二 AddRoundKey 变换模块及第三 AddRoundKey 变换模块使用不同的轮回密钥被执行。

[0053] 在本发明中，在一些时钟周期中的信号处理增加，从而在每个时钟周期时段在用于每个子块变换的信号处理时间总和之间的差最小。这使得通过硬件对 AES 加密或解密所要求的周期数量比以前小。

[0054] 当实施本发明时，在每个时钟周期时段用于每个子块变换的信号处理时间总和的最大值等于现有技术的最大值。为此，周期数量的减少意味着处理速度的提高。

[0055] 本发明适用于加密和解密（包括等效的逆密码）。本发明适用于任何实施方法，如 1Round/Cycle、2Round/Cycle、或 0.5Round/Cycle。本发明适用于任何加密模式，如 ECB 模式或 CBC 模式。本发明适用于任何密钥长度。

[0056] 作为本发明的效果，在 1Round/Cycle 的实施例方法中，在 AES-128 中可把 11 个周期减小到 10 个周期，在 AES-192 中可把 13 个周期减小到 12 个周期，及在 AES-256 中可把 15 个周期减小到 14 个周期。

[0057] 在 2Round/Cycle 的实施例方法中，在 AES-128 中可把 6 个周期减小到 5 个周期，在 AES-192 中可把 7 个周期减小到 6 个周期，及在 AES-256 中可把 8 个周期减小到 7 个周期。

[0058] 参照附图的示范实施例的如下描述，本发明的其它特征将变得明白。

附图说明

[0059] 图 1 是用来把现有技术在时钟周期中执行的加密过程内容与第一实施例的那些相比较的图；

[0060] 图 2 是用来把现有技术在每个时钟周期中用于每个子块变换的加密处理时间总和与第一实施例的总和相比较的图；

[0061] 图 3 是用来把现有技术在时钟周期中执行的解密过程内容与第一实施例的那些相比较的图；

[0062] 图 4 是用来把现有技术在每个时钟周期中用于每个子块变换的解密处理时间总和与第一实施例的总和相比较的图；

[0063] 图 5 是根据第一实施例的 AES 芯 (Core) 的方块图；

[0064] 图 6 是根据第一实施例的加密 / 解密单元的方块图；

[0065] 图 7 是根据第一实施例的用于加密的修改轮回函数模块的方块图；

[0066] 图 8 是根据第一实施例的用于解密的修改轮回函数模块的方块图；

[0067] 图 9A 和 9B 是根据第一实施例的加密时序图；

[0068] 图 10A 和 10B 是根据第一实施例的解密时序图；

[0069] 图 11 是表示根据第二实施例在时钟周期中执行的加密和解密过程内容的图；

[0070] 图 12 是用来把现有技术在每个时钟周期中用于每个子块变换的加密处理时间总

和与第二实施例的总和相比较的图；

[0071] 图 13 是用来把现有技术在每个时钟周期中用于每个子块变换的解密处理时间总和与第二实施例的总和相比较的图；

[0072] 图 14 是根据第二实施例的 AES 芯的方块图；

[0073] 图 15 是根据第二实施例的加密 / 解密单元的方块图；

[0074] 图 16 是根据第二实施例的用于加密的修改轮回函数模块的方块图；

[0075] 图 17 是根据第二实施例的用于解密的修改轮回函数模块的方块图；

[0076] 图 18A 和 18B 是根据第二实施例的加密时序图；

[0077] 图 19A 和 19B 是根据第二实施例的解密时序图；

[0078] 图 20 是表示根据第三实施例在时钟周期中执行的加密和解密过程内容的图；

[0079] 图 21 是用来把现有技术在每个时钟周期中用于每个子块变换的加密处理时间总和与第三实施例的总和相比较的图；

[0080] 图 22 是用来把现有技术在每个时钟周期中用于每个子块变换的解密处理时间总和与第三实施例的总和相比较的图；

[0081] 图 23 是根据第三实施例的 AES 芯的方块图；

[0082] 图 24 是根据第三实施例的加密 / 解密单元的方块图；

[0083] 图 25 是根据第三实施例的用于加密的修改轮回函数模块的方块图；

[0084] 图 26 是根据第三实施例的用于解密的修改轮回函数模块的方块图；

[0085] 图 27A 和 27B 是根据第三实施例的加密时序图；

[0086] 图 28A 和 28B 是根据第三实施例的解密时序图；

[0087] 图 29 是用来把现有技术在时钟周期中执行的加密过程内容与第四实施例的那些相比较的图；

[0088] 图 30 是用来把现有技术在时钟周期中执行的解密过程内容与第四实施例的那些相比较的图；

[0089] 图 31 是用来把现有技术用于在时钟周期中执行的每个子块变换的信号处理时间总和与第四实施例的总和相比较的图；

[0090] 图 32 是根据第四实施例的 AES 芯的方块图；

[0091] 图 33 是根据第四实施例的加密 / 解密单元的方块图；

[0092] 图 34 是根据第四实施例的修改轮回函数模块的方块图；

[0093] 图 35A 和 35B 是根据第四实施例的解密时序图；

[0094] 图 36 是表示根据第五实施例在时钟周期中执行的加密和解密过程内容的图；

[0095] 图 37 是用来把现有技术用于在时钟周期中执行的每个子块变换的信号处理时间总和与第五实施例的总和相比较的图；

[0096] 图 38 是根据第五实施例的 AES 芯的方块图；

[0097] 图 39 是根据第五实施例的加密 / 解密单元的方块图；

[0098] 图 40 是根据第五实施例的修改轮回函数模块的方块图；

[0099] 图 41A 和 41B 是根据第五实施例的解密时序图；

[0100] 图 42 是表示根据第六实施例在时钟周期中执行的加密和解密过程内容的图；

[0101] 图 43 是用来把现有技术用于在时钟周期中执行的每个子块变换的信号处理时间

总和与第六实施例的总和相比较的图；

[0102] 图 44 是根据第六实施例的 AES 芯的方块图；

[0103] 图 45 是根据第六实施例的加密 / 解密单元的方块图；

[0104] 图 46 是根据第六实施例的修改轮回函数模块的方块图；

[0105] 图 47A 和 47B 是根据第六实施例的解密时序图；

[0106] 图 48 是用来把现有技术在时钟周期中执行的加密过程内容与第七实施例的那些相比较的图；

[0107] 图 49 是用来把现有技术用于在每个时钟周期时段中的每个子块变换的加密处理时间总和与第七实施例的总和相比较的图；

[0108] 图 50 是用来把现有技术在时钟周期中执行的解密过程内容与第七实施例的那些相比较的图；

[0109] 图 51 是用来把现有技术用于在每个时钟周期时段中的每个子块变换的解密处理时间总和与第七实施例的总和相比较的图；

[0110] 图 52 是根据第七实施例的 AES 芯的方块图；

[0111] 图 53 是根据第七实施例的加密 / 解密单元的方块图；

[0112] 图 54A 和 54B 是根据第七实施例用于加密的修改轮回函数模块的方块图；

[0113] 图 55A 和 55B 是根据第七实施例用于解密的修改轮回函数模块的方块图；

[0114] 图 56A 和 56B 是根据第七实施例的加密时序图；

[0115] 图 57A 和 57B 是根据第七实施例的解密时序图；

[0116] 图 58 是根据第八实施例的加密 / 解密单元的方块图；

[0117] 图 59 是根据第九实施例的修改轮回函数模块的方块图；

[0118] 图 60A 和 60B 是表示 AES 算法的图；

[0119] 图 61A 和 61B 是表示时钟和数据保持单元的数据更新时序的时序图；及

[0120] 图 62 是表示另一实施方法的图。

具体实施方式

[0121] 这里，参照附图将详细地描述本发明的实施例。这个实施例中，将举例说明由 FIPS197 定义的 AES-128（下文简称为 AES）。

[0122] < 第一实施例 >

[0123] 图 1 表示在第一实施例中在时钟周期中执行的加密过程内容与现有技术之间的比较。

[0124] 参照图 1，周期计数指示在 AES 处理开始是“0”的时钟周期计数。轮回密钥 wkeyi 是 FIPS197 描述的轮回密钥 (i 是轮回数)。

[0125] 这个实施例中，AddRoundKey 变换、ShiftRows 变换、SubBytes 变换及 MixColumns 变换在第 0 至第八周期中被执行。在第九周期，第一 AddRoundKey 变换、ShiftRows 变换、SubBytes 变换及第二 AddRoundKey 变换被执行。至于轮回密钥，wkey0 被用在第 0 周期中，wkey1 被用在第一周期中，...，及 wkey8 被用在第八周期中。在第九周期中，使用两个轮回密钥 wkey9 和 wkey10。

[0126] 这个实施例中，与现有技术相同的处理被整体执行。然而，这个实施例中，AES 加

密可以少一个的时钟周期被执行。

[0127] 接着将描述根据这个实施例在每个时钟周期时段用于每个子块变换的加密处理时间总和。图 2 是表示现有技术在每个时钟周期时段用于每个子块变换的加密处理时间总和与第一实施例的总和之间的比较图。纵坐标代表时间。条带越长，处理时间越长。为了实施这个实施例，在每个时钟周期时段用于每个子块变换的信号处理时间总和的最大值必须小于一个时钟周期时间。如图 2 所示，每个子块变换的处理时间在 SubBytes 变换中最长，并且按 MixColumns 变换、AddRoundKey 变换及 ShiftRows 变换的顺序缩短。

[0128] 这个实施例中，在执行 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换及 MixColumns 变换的第 0 至第八周期的每个周期中，用于每个子块变换的信号处理时间总和比在执行 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换及 AddRoundKey 变换的第九周期中用于每个子块变换的信号处理时间总和更长。因此，这个实施例中在一个时钟周期时段执行的每个子块变换的信号处理时间总和的最大值与现有技术的最大值相等。如果在一个周期时段中执行的每个子块变换的信号处理时间总和的最大值比现有技术中的一个周期时间更短，则这个实施例也可实现。

[0129] 本发明也适用于 AES 解密。

[0130] 图 3 表示在本实施例中在时钟周期中执行的解密过程内容与现有技术之间的比较。

[0131] 参照图 3，周期计数指示在 AES 处理开始是“0”的时钟周期计数。

[0132] 这个实施例中，第一 AddRoundKey 变换、InvShiftRows 变换、InvSubBytes 变换及第二 AddRoundKey 变换在第 0 周期中执行。在第一周期至第九周期中，InvMixColumns 变换、InvShiftRows 变换、InvSubBytes 变换及 AddRoundKey 变换被执行。至于轮回密钥，两个轮回密钥 wkey9 和 wkey10 被用在第 0 周期中，wkey8 被用在第一周期中，wkey7 被用在第二周期中，...，及 wkey0 被用在第九周期中。

[0133] 这个实施例中，与现有技术相同的处理被总体上执行。然而，这个实施例中，AES 解密可以少一个的时钟周期被执行。

[0134] 接着将描述根据这个实施例在每个时钟周期时段用于每个子块变换的解密处理时间总和。图 4 是表示在第一实施例中在每个时钟周期时段用于每个子块变换的解密处理时间总和与现有技术的总和之间的比较图。纵坐标代表时间。条带越长，处理时间越长。为了实施这个实施例，在每个时钟周期时段用于每个子块变换的信号处理时间总和的最大值必须小于一个时钟周期时间。如图 4 所示，每个子块变换的处理时间在 InvSubBytes 变换中最长，并且按 InvMixColumns 变换、AddRoundKey 变换及 InvShiftRows 变换的顺序缩短。

[0135] 这个实施例中，在执行 AddRoundKey 变换、InvSubBytes 变换、InvShiftRows 变换及 InvMixColumns 变换的第一至第九周期的每一个周期中，用于每个子块变换的信号处理时间总和比在执行 AddRoundKey 变换、InvSubBytes 变换、InvShiftRows 变换及 AddRoundKey 变换的第 0 周期中用于每个子块变换的信号处理时间总和更长。这个实施例中在每个时钟周期时段用于每个子块变换的信号处理时间总和的最大值与现有技术的最大值相等。所以这个实施例也可实现。

[0136] 将概括本发明的上述特性特征。

[0137] 在一般常规实施方法中，标准定义的轮回函数被认为是处理中的断点，并且加密

和解密被分配给时钟周期。为此，在第 10 和第 0 周期中用于每个子块变换的信号处理时间总和比第一至第九周期的每一个周期的总和短。就是说，每个周期中用于每个子块变换的信号处理时间总和变化。

[0138] 另一方面，在本发明中，一些时钟周期中的信号处理增加，从而在每个时钟周期时段在用于每个子块变换的信号处理时间总和之间的差最小。在本发明中，AES 加密或解密所要求的时钟周期的数量被减小一个，而不增加在每个时钟周期时段用于每个子块变换的信号处理时间总和。这把 AES 处理速度提高约 10％。

[0139] 接着将描述用来实施 AES 加密和解密的 AES 芯的电路设置。

[0140] 图 5 是根据这个实施例的 AES 芯的方块图。

[0141] 参照图 5，AES 芯 101 执行 AES 处理。密钥扩展单元 102 从密码密钥产生对 AES 加密和解密必需的轮回密钥，并且输出轮回密钥。加密 / 解密单元 103 使用从密钥扩展单元 102 供给的轮回密钥执行 128- 位明文数据的加密或 128- 位密文数据的解密。控制单元 104 从 AES 芯 101 外部的单元接收控制信号，并且产生控制密钥扩展单元 102 和加密 / 解密单元 103 的操作的信号、并且向 AES 芯 101 外部的单元通知操作完成的信号。

[0142] 参照图 5，输入信号 150 是要加密的明文数据或要解密的密文数据。输出信号 151 是通过使加密 / 解密单元 103 加密或解密输入信号 150 得到的结果。密码密钥 152 被用于加密或解密。加密 / 解密选择信号 153 选择要执行的加密和解密之一。密钥准备开始信号 155 使密钥扩展单元 102 开始密钥扩展，以从密码密钥 152 产生轮回密钥。控制信号 157 能够使加密 / 解密处理晚一个周期。加密 / 解密开始信号 158 开始输入信号 150 的加密或解密。有效信号 159 代表输出信号 151 保持通过加密 / 解密单元 103 的加密或解密的结果。控制信号 160 使加密 / 解密单元 103 保持输出信号 151 的值。计数器信号 161 代表在密钥准备或加密 / 解密中从密钥准备开始信号 155 或加密 / 解密开始信号 158 的前沿起的周期数。轮回密钥 A162 是轮回密钥之一。轮回密钥 B163 是密钥扩展单元 102 产生的并且用在加密的最后周期或解密的第一周期中的轮回密钥。选择信号 170 切换在加密 / 解密单元 103 中子块变换的连接。选择信号 171 切换在加密 / 解密单元 103 中的目标过程数据。

[0143] 以上设置中，输入信号 150 从外部输入到加密 / 解密单元 103。输出信号 151 从加密 / 解密单元 103 输出到外部。密码密钥 152 从外部输入到密钥扩展单元 102。加密 / 解密选择信号 153 从外部输入到密钥扩展单元 102、加密 / 解密单元 103 及控制单元 104。密钥准备开始信号 155 从外部输入到密钥扩展单元 102 和控制单元 104。控制信号 157 从控制单元 104 输出到外部。加密 / 解密开始信号 158 从外部输入到密钥扩展单元 102 和控制单元 104。有效信号 159 从控制单元 104 输出到外部。输出保持控制信号 160 从控制单元 104 输出到加密 / 解密单元 103。计数器信号 161 从控制单元 104 输出到密钥扩展单元 102。轮回密钥 A162 从密钥扩展单元 102 输出到加密 / 解密单元 103。轮回密钥 B163 从密钥扩展单元 102 输出到加密 / 解密单元 103。选择信号 170 从控制单元 104 输出到加密 / 解密单元 103。选择信号 171 从控制单元 104 输出到加密 / 解密单元 103。

[0144] 接着将描述加密 / 解密单元 103。图 6 是加密 / 解密单元 103 的方块图。参照图 6，修改轮回函数模块 105 在选择信号 170 的控制下使用轮回密钥 A162 和轮回密钥 B163 执行一个周期的加密。修改轮回函数模块 106 在选择信号 170 的控制下使用轮回密钥 A162 和轮回密钥 B163 执行解密。

[0145] 选择器 107 按照加密 / 解密选择信号 153 选择来自修改轮回函数模块 105 的输出和来自修改轮回函数模块 106 的输出之一。数据保持单元 108 按照输出保持控制信号 160 保持选择器 107 选择的信号。选择器 109 按照选择信号 171 选择输入信号 150 和来自数据保持单元 108 的输出信号之一。

[0146] 参照图 6，输入信号 165 输入到修改轮回函数模块 105 和 106。输出信号 166 是通过使修改轮回函数模块 105 以处理输入信号 165 得到的结果。输出信号 167 是通过使修改轮回函数模块 106 以处理输入信号 165 得到的结果。输出信号 168 从选择器 107 输出。

[0147] 在以上设置中，输入信号 150、来自数据保持单元的输出及选择信号 171 输入到选择器 109。来自选择器 109 的输出、轮回密钥 A162、轮回密钥 B163 及选择信号 170 输入到修改轮回函数模块 105。来自选择器 109 的输出、轮回密钥 A162、轮回密钥 B163 及选择信号 170 输入到修改轮回函数模块 106。来自修改轮回函数模块 105 的输出信号、来自修改轮回函数模块 106 的输出信号及加密 / 解密选择信号 153 输入到选择器 107。来自选择器 107 的输出和输出保持控制信号 160 输入到数据保持单元 108。数据保持单元 108 输出加密 / 解密单元 103 的输出信号 151。

[0148] 在以上设置中，当选择信号 171 被取消 (negate) 时，选择器 109 选择并输出输入信号 150。当选择信号 171 被声明时，选择器 109 选择并输出来自数据保持单元 108 的输出信号 151。作为选择器 109 选择结果的输入信号 165 分别输入到进行加密和解密的修改轮回函数模块 105 和 106。当加密 / 解密选择信号 153 被取消时，选择器 107 选择并输出作为修改轮回函数模块 105 的输出结果的输出信号 166。当加密 / 解密选择信号 153 被声明时，选择器 107 选择并输出作为修改轮回函数模块 106 的输出结果的输出信号 167。来自选择器 107 的输出信号 168 被输入到数据保持单元 108，并被临时保持。数据保持单元 108 的输出信号 151 是加密 / 解密单元 103 的输出信号。输出信号也连接到选择器 109 的输入。在选择信号 171 被声明时，重复执行通过修改轮回函数模块 105 的加密或通过修改轮回函数模块 106 的解密。

[0149] 当已结束加密 / 解密，并且下一次加密 / 解密还没有开始时，控制单元 104 声明输出保持控制信号 160。这个时间期间，数据保持单元 108 独立于输出信号 168 持续地保持输出信号 151 的值。

[0150] 接着将描述修改轮回函数模块 105。图 7 是修改轮回函数模块 105 的方块图。参照图 7，AddRoundKey 变换模块 110（与第一 AddRoundKey 变换模块相对应）接收输入信号 165 和轮回密钥 A162，并且执行 AddRoundKey 变换。SubBytes 变换模块 111 接收来自 AddRoundKey 变换模块 110 的输出，并且执行 SubBytes 变换。ShiftRows 变换模块 112 接收来自 SubBytes 变换模块 111 的输出，并且执行 ShiftRows 变换。MixColumns 变换模块 113 接收来自 ShiftRows 变换模块 112 的输出，并且执行 MixColumns 变换。AddRoundKey 变换模块 114（与第二 AddRoundKey 变换模块相对应）接收来自 ShiftRows 变换模块 112 的输出和轮回密钥 B163，并且执行 AddRoundKey 变换。选择器 115 按照选择信号 170 选择并输出来自 MixColumns 变换模块 113 的输出和来自 AddRoundKey 变换模块 114 的输出之一。选择器 115 的输出信号是修改轮回函数模块 105 的输出信号。

[0151] 在以上设置中，当选择信号 170 被取消时，选择器 115 选择并输出来自 MixColumns 变换模块的输出。当选择信号 170 被声明时，选择器 115 选择并输出来自 AddRoundKey 变

换模块的输出。

[0152] 接着参照图 8 的方块图将描述修改轮回函数模块 106。

[0153] 参照图 8，InvMixColumns 变换模块 116 接收输入信号 165，并且执行 InvMixColumns 变换。AddRoundKey 变换模块 117 接收输入信号 165 和轮回密钥 B163，并且执行 AddRoundKey 变换。选择器 118 按照选择信号 170 选择并输出来自 InvMixColumns 变换模块 116 的输出和来自 AddRoundKey 变换模块 117 的输出之一。InvShiftRows 变换模块 119 接收来自选择器 118 的输出，并且执行 InvShiftRows 变换。InvSubBytes 变换模块 120 接收来自 InvShiftRows 变换模块 119 的输出，并且执行 InvSubBytes 变换。AddRoundKey 变换模块 121 接收来自 InvSubBytes 变换模块 120 的输出，并且执行 AddRoundKey 变换。AddRoundKey 变换模块 121 的输出是修改轮回函数模块 106 的输出。

[0154] 在以上设置中，当选择信号 170 被取消时，选择器 118 选择并输出来自 InvMixColumns 变换模块 116 的输出。当选择信号 170 被声明时，选择器 118 选择并输出来自 AddRoundKey 变换模块 117 的输出。

[0155] 接着将描述在以上设置中的加密操作。图 9A 和 9B 是根据这个实施例的加密时序图。参照图 9A 和 9B，横坐标代表时间。时序名称 T01、T02、...、T33 被赋予时钟脉冲的前沿。

[0156] 在图 9A 左端沿纵坐标的三位数指示信号线，并且与图 5 至 8 使用的信号线的附图标记具有一一对应性。

[0157] 在图 9A 和 9B 的时序图表示的加密操作大致划分成四部分。第一部分是用来设置诸如密码密钥之类的各种参数的参数设置时段 (T01 至 T06)。第二部分是用来产生 wkey10 并把它保持在寄存器中的密钥准备时段 (T06 至 T17)。第三部分是第一块加密时段 (T17 至 T27)。第四部分是第二块加密时段 (从 T27 起)。

[0158] 在参数设置时，按需要设置用于加密 / 解密的各种参数，如密钥长度和加密模式，除了密码密钥 152 和加密 / 解密选择信号 153 以外。加密 / 解密选择信号 153 和密码密钥 152 的值需要始终保持在外部，直到新参数设置。参数设置时段是紧接在复位之后具有任意长度的时段。当从 AES 芯 101 外的单元声明密钥准备开始信号 155 时 (T06)，参数设置时段结束。

[0159] 参数设置时段结束的同时，下一个密钥准备时段开始。在密钥准备时段中，密钥扩展单元 102 事先产生最后轮回密钥 (wkey10) 以在加密 / 解密的第九周期 (T26) 中把两个轮回密钥 (wkey9 和 wkey10) 同时供给到加密 / 解密单元 103。密钥准备时段是从密钥准备开始信号 155 的声明 (T06) 到 11 个周期后的时序 (T17) 的时段，在该时序 (T17) 产生最后轮回密钥 (wkey10)。

[0160] 接着将描述在密钥准备时段期间每个电路的操作。当密钥准备开始信号 155 被声明时，控制单元 104 从 0 依次向上计数计数器信号 161。密钥扩展单元 102 按照计数器信号 161 在每个时钟周期扩展 wkey0(密码密钥 152)，由此产生 10 个轮回密钥 wkey1、wkey2、...、wkey10。产生的轮回密钥被依次输出作为轮回密钥 A162。

[0161] 在时序 T16，计数器信号 161 达到“10”。密钥扩展单元 102 把产生的轮回密钥 (wkey10) 保持在寄存器中，并且输出它作为轮回密钥 B163。这之后，wkey10 被持续地保持，直到下一次执行密钥准备。

[0162] 当密钥准备时段已经结束时(T17),密钥扩展单元102输出在加密/解密中首先要使用的轮回密钥(在加密中的wkey0或在解密中的wkey9),作为轮回密钥A162。轮回密钥A162的值被保持,直到加密/解密开始信号158的声明。控制单元104停止向上计数计数器信号161,并且把计数器清除到0。

[0163] 在密钥准备时段结束的附近,当预计到密钥准备将在T17结束、并启动加密时,控制单元104在T16声明控制信号157。

[0164] 在T17检测到控制信号157的声明时,设置在AES芯101外的输入信号供给单元把明文数据P0供给到AES芯101作为输入信号150。加密/解密开始信号158被声明,以开始输入信号150的加密(T17)。在时序图中,加密/解密开始信号158在最短周期中被声明。然而,时序在AES芯101外自由确定。

[0165] 在加密时段中,输入信号150被加密。加密时段是从加密/解密开始信号158的声明(T17)到10个周期后的时序(T27)的时段。

[0166] 在检测到加密/解密开始信号158的声明时,控制单元104在下个周期(T18)中取消控制信号157、有效信号159及输出保持控制信号160。同时,控制单元104开始向上计数计数器信号161。

[0167] 密钥扩展单元102按照计数器信号161从轮回密钥wkey0起依次进行密钥扩展。密钥扩展单元102在T18把wkey1、在T19把wkey2、... 及在T26把wkey9输出到加密/解密单元103作为轮回密钥A162。

[0168] 从T17至T18,选择信号171被取消。因此,修改轮回函数模块105使用wkey0输出作为轮回密钥A对输入信号150执行子块变换。从T18至T27,选择信号171被声明。因此,修改轮回函数模块105从T18到T19使用wkey1,从T19到T20使用wkey2,...,及从T25到T26使用wkey8对数据保持单元108的输出执行子块变换。

[0169] 在加密的最后周期(T26)中,控制单元104声明选择信号170。相应地,修改轮回函数模块105的选择器115选择来自使用轮回密钥B163执行AddRoundKey变换的AddRoundKey变换模块114的输出,从而执行最后周期的子块变换。在T26,修改轮回函数模块105的输出信号166输出是作为输入信号的明文数据P0的加密结果的密文数据C0。一个周期后(T27),数据保持单元108向外部输出密文数据C0的值作为来自AES芯101的输出。同时,为了通知在AES芯101外部单元加密结束、以及输出信号151被启动,控制单元104声明有效信号159(T27)。在有效信号159被声明的同时,AES芯101保证输出信号151被启动。

[0170] 另一方面,输出保持控制信号160保持取消,因为在T27有效信号159被声明,但在T27加密/解密开始信号158也被声明。如果在T27加密/解密开始信号158不被声明,则在T27输出保持控制信号160被声明,并且数据保持单元108的值保持密文数据C0。

[0171] 在T27当加密结束时,密钥扩展单元102输出wkey0作为轮回

[0172] 密钥A162。轮回密钥A162的值被保持,直到下一个加密/解密开始信号156的声明。

[0173] 当预计加密结束时(T27),控制单元104在结束前的一个周期(T26)声明控制信号157。当控制信号157被声明时,在AES芯101外部的单元把输入信号150的值设置到下个明文数据P1,从而第二块的加密可开始。在图9A和9B的时序图中,在AES芯101外部

的单元在最短周期 (T27) 中声明下一个加密 / 解密开始信号。第二块的加密操作以与第一块相同的方式进行。从那时起，加密操作被重复进行与块的预定数量一样多次。在图 9A 和 9B 的时序图中，第二块的加密在距离第一块加密结束的最短间隔开始。AES 芯通过以这样一种时序执行所有块的加密可呈现其最大性能。然而，加密间隔基本上可设置到任意长度。

[0174] 当预定数量的块的加密已经完全结束，并且下一个作业要使用诸如密码密钥之类的不同参数执行时，处理再次从参数设置开始。

[0175] 接着将描述这个实施例的解密操作。图 10A 和 10B 是根据这个实施例的解密时序图。参照图 10A 和 10B，横坐标代表时间。时序名称 T01、T02、...、T33 被赋予时钟脉冲的前沿。在图 10A 的左端沿纵坐标的三位数指示信号线，并且与图 5 至 8 中使用的信号线的附图标记具有一一对应性。

[0176] 解密操作也大致划分成四部分 :参数设置时段 (T01 至 T06)、密钥准备时段 (T06 至 T17)、第一块解密时段 (T17 至 T27) 及第二块解密时段 (从 T27 起)。

[0177] 参数设置时段是从 T01 至 T06，并且其作用、开始条件及结束条件与本实施例的加密中相同。然而，加密 / 解密选择信号 153 在解密中被声明。

[0178] 密钥准备时段是从 T06 至 T17，并且开始条件和结束条件与本实施例的加密中相同。每个电路的操作也几乎与本实施例的加密中相同。然而，第一周期中使用的轮回密钥在加密和解密之间是不同的。因此，密钥扩展单元 102 在密钥准备时段的结束 (T17) 从 wkey10 反向地进行密钥扩展以产生 wkey9，并且输出密钥作为轮回密钥 A162。轮回密钥 A162 的值被保持，直到加密 / 解密开始信号 158 的声明。控制单元 104 停止向上计数计数器信号 161，并且把计数器清除到 0。

[0179] 在密钥准备时段结束的附近，当预计到密钥准备将在 T17 结束、并启动解密时，控制单元 104 在 T16 声明控制信号 157。

[0180] 在 T17 检测到控制信号 157 的声明时，设置在 AES 芯 101 外的输入信号供给单元把密文数据 C0 供给到 AES 芯 101 作为输入信号 150。加密 / 解密开始信号 158 被声明，以开始输入信号 150 的解密 (T17)。在时序图中，加密 / 解密开始信号 158 在最短周期中被声明。然而，时序在 AES 芯 101 外自由确定。

[0181] 在解密时段中，输入信号 150 被解密。解密时段是从加密 / 解密开始信号 158 的声明 (T17) 到 10 个周期后的时序 (T27) 的时段。

[0182] 在检测到加密 / 解密开始信号 158 的声明时，控制单元 104 在下个周期 (T18) 中取消控制信号 157、有效信号 159 及输出保持控制信号 160。同时，控制单元 104 开始向上计数计数器信号 161。

[0183] 密钥扩展单元 102 按照计数器信号 161 从轮回密钥 wkey9 反向地进行密钥扩展。密钥扩展单元 102 在 T18 把 wkey9、在 T19 把 wkey8、... 及在 T26 把 wkey0 输出到加密 / 解密单元 103 作为轮回密钥 A162。

[0184] 从 T17 至 T18，选择信号 171 被取消。因此，修改轮回函数模块 106 使用 wkey9 输出作为轮回密钥 A 对输入信号 150 执行子块变换。在解密的第一周期中，控制单元 104 声明选择信号 170。相应地，修改轮回函数模块 106 的选择器 118 选择来自 AddRoundKey 变换模块 117(其使用轮回密钥 B163 执行 AddRoundKey 变换) 的输出，从而执行第一周期的子块变换。

[0185] 从 T18 至 T27，选择信号 171 被声明。因此，修改轮回函数模块 106 从 T18 到 T19 使用 wkey8，从 T19 到 T20 使用 wkey7，...，及从 T25 到 T26 使用 wkey0 对来自数据保持单元 108 的输出执行子块变换。

[0186] 在 T26，修改轮回函数模块 106 的输出信号 167 输出是作为输入信号的密文数据 C0 的解密结果的明文数据 P0。一个周期后 (T27)，数据保持单元 108 向外部输出明文数据 P0 的值作为来自 AES 芯 101 的输出。同时，为了通知 AES 芯 101 外部的单元解密被结束、以及输出信号 151 被启动，控制单元 104 声明有效信号 159(T27)。在有效信号 159 被声明的同时，AES 芯 101 保证输出信号 151 被启动。

[0187] 另一方面，输出保持控制信号 160 保持取消，因为在 T27 有效信号 159 被声明，但在 T27 加密 / 解密开始信号 158 也被声明。如果在 T27 加密 / 解密开始信号 158 不被声明，则在 T27 输出保持控制信号 160 被声明，并且数据保持单元 108 的值保持明文数据 P0。

[0188] 在 T27 当解密结束时，密钥扩展单元 102 通过逆运算由 wkey10 得到 wkey9，并且输出它作为轮回密钥 A162。轮回密钥 A162 的值被保持，直到下一个加密 / 解密开始信号 156 的声明。

[0189] 当预计解密结束时 (T27)，控制单元 104 在结束前的一个周期 (T26) 声明控制信号 157。当控制信号 157 被声明时，在 AES 芯 101 外部的单元把输入信号 150 的值设置到下个密文数据 C1，从而第二块的解密可开始。在图 10A 和 10B 的时序图中，在 AES 芯 101 外部的单元在最短周期 (T27) 中声明下一个加密 / 解密开始信号 158。第二块的解密操作与第一块以相同方式进行。从那时起，解密操作被重复进行任意次。

[0190] 当解密已完全结束，并且下个作业要开始时，处理再次从参数设置开始。

[0191] 第一实施例能以上述方式实施。在第一实施例中，对 AES 加密所要求的时钟周期的数量被减小一个，而不增大在每个时钟周期用于每个子块变换的信号处理时间总和的最大值。这把 AES 处理速度提高约 10％。

[0192] < 第二实施例 >

[0193] 图 11 是表示根据第二实施例在时钟周期中执行加密和解密过程内容的图。

[0194] 参照图 11，周期计数指示在 AES 处理开始是“0”的时钟周期计数。

[0195] 在这个实施例的加密中，第一 AddRoundKey 变换、ShiftRows 变换、SubBytes 变换、MixColumns 变换及第二 AddRoundKey 变换在第 0 周期中被执行。在第一至第八周期中，AddRoundKey 变换、ShiftRows 变换、SubBytes 变换及 MixColumns 变换被执行。在第九周期中，AddRoundKey 变换、ShiftRows 变换及 SubBytes 变换被执行。至于轮回密钥，wkey0 和 wkey1 被用在第 0 周期中，wkey2 被用在第一周期中，...，及 wkey10 被用在第九周期中。

[0196] 在第二实施例中，与现有技术相同的处理被总体上执行。然而，这个实施例中，AES 加密可以少一个的时钟周期被执行。

[0197] 接着将描述根据第二实施例在时钟周期中用于执行的每个子块变换的信号处理时间总和。图 12 是表示在第二实施例中在时钟周期中执行每个子块变换的信号处理时间总和与现有技术的总和之间的比较图。纵坐标代表时间。条带越长，处理时间越长。为了实现第二实施例，在每个时钟周期时段用于每个子块变换的信号处理时间总和的最大值必须小于一个周期时间。如图 12 所示，每个子块变换的处理时间在 SubBytes 变换中最长，并且按 MixColumns 变换、AddRoundKey 变换及 ShiftRows 变换的顺序缩短。

[0198] 这个实施例中，在执行第一 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换、MixColumns 变换及第二 AddRoundKey 变换的第 0 周期中，用于每个子块变换的信号处理时间总和，比在执行 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换及 MixColumns 变换的第一至第八周期中用于每个子块变换的信号处理时间总和、或在执行 AddRoundKey 变换、SubBytes 变换及 ShiftRows 变换的第九周期中用于每个子块变换的信号处理时间总和更长。因此，这个实施例的每个子块变换的信号处理时间总和的最大值比现有技术的最大值更大一个对应于 AddRoundKey 变换处理时间的量。然而，一个 AddRoundKey 变换处理时间比一个周期中用于每个子块变换的信号处理时间总和短得多。每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值常常以足够的裕量设置为一个周期时间。为此，如果现有技术在每个时钟周期时段中用于每个子块变换的加密处理时间总和的最大值比一个周期时间短，则也假定本实施例在多数情况下是可实施的。

[0199] 本发明也适用于 AES 解密。

[0200] 如图 11 所示，在这个实施例的解密中，AddRoundKey 变换、InvShiftRows 变换及 InvSubBytes 变换在第 0 周期中被执行。在第一至第八周期中，AddRoundKey 变换、InvShiftRows 变换、InvSubBytes 变换及 InvMixColumns 变换被执行。在第九周期中，第一 AddRoundKey 变换、InvShiftRows 变换、InvSubBytes 变换、InvMixColumns 变换及第二 AddRoundKey 变换被执行。至于轮回密钥，wkey10 被用在第 0 周期中，wkey9 被用在第一周期中，...，及 wkey2 被用在第八周期中。在第九周期中，使用两个轮回密钥 wkey1 和 wkey0。

[0201] 在第二实施例中，与现有技术相同的处理被总体上执行。然而，在第二实施例中，AES 解密可以少一个的时钟周期被执行。

[0202] 接着将描述根据第二实施例在时钟周期中执行的每个子块变换的信号处理时间总和。图 13 是表示在第二实施例中在时钟周期中执行的每个子块变换的信号处理时间总和与现有技术的总和之间的比较图。纵坐标代表时间。条带越长，处理时间越长。为了实施这个实施例，在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值必须小于一个周期时间。如图 13 所示，每个子块变换的处理时间在 InvSubBytes 变换中最长，并且按 InvMixColumns 变换、AddRoundKey 变换及 InvShiftRows 变换的顺序缩短。

[0203] 在第二实施例中，在执行第一 AddRoundKey 变换、InvSubBytes 变换、InvShiftRows 变换、InvMixColumns 变换及第二 AddRoundKey 变换的第九周期中用于每个子块变换的信号处理时间总和，比在执行 AddRoundKey 变换、InvSubBytes 变换、InvShiftRows 变换及 InvMixColumns 变换的第一至第八周期中用于每个子块变换的信号处理时间总和、或在执行 AddRoundKey 变换、InvSubBytes 变换及 InvShiftRows 变换的第 0 周期中用于每个子块变换的信号处理时间总和更长。因此，第二实施例的每个子块变换的信号处理时间总和的最大值比现有技术的最大值大一个对应于 AddRoundKey 变换处理时间的量。然而，一个 AddRoundKey 变换处理时间比一个周期中用于每个子块变换的信号处理时间总和短得多。在每个时钟周期时段中每个子块变换的信号处理时间总和的最大值常常以足够的裕量设置为一个周期时间。为此，如果现有技术在每个时钟周期时段中每个子块变换的解密处理时间总和的最大值比一个周期时间短，则也假定本实施例在多数情况下是可实施的。

[0204] 将概括第二实施例的上述特性特征。

[0205] 在一般常规实施方法中，由标准定义的轮回函数被认为是处理中的断点，并且加密和解密被分配给时钟周期。为此，在第 10 和第 0 周期用于每个子块变换的信号处理时间总和比第一至第九周期的每一个周期中用于每个子块变换的解密处理时间总和更短。就是说，在每个周期中执行每个子块变换的信号处理时间总和变化。

[0206] 另一方面，在本发明中，在一些时钟周期中的信号处理增加，从而在每个时钟周期时段中用于每个子块变换的信号处理时间总和之间的差减小。

[0207] 这个实施例中，在一个周期中执行每个子块变换的信号处理时间总和的最大值稍微增大。为此，本实施例在现有技术可实施的条件下不一定是可实施的。然而，这在多数情况下几乎不成问题，因为在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值常常以足够的裕量设置为一个周期时间。多数情况下，AES 加密或解密所要求的时钟周期的数量可被减小一个。这把 AES 处理速度提高约 10％。

[0208] 接着将描述用来实施 AES 加密和解密的 AES 芯的电路设置。

[0209] 图 14 是根据这个实施例的 AES 芯的方块图。

[0210] 参照图 14，AES 芯 131 执行 AES 处理。密钥扩展单元 132 从密

[0211] 码密钥产生对 AES 加密和解密必需的轮回密钥，并且输出轮回密钥。加密 / 解密单元 133 使用从密钥扩展单元 132 供给的轮回密钥执行 128- 位明文数据的加密或 128- 位密文数据的解密。控制单元 134 从 AES 芯 131 外部的单元接收控制信号，并且产生控制密钥扩展单元 132 和加密 / 解密单元 133 的操作的信号、以及向 AES 芯 131 外部的单元通知操作完成的信号。

[0212] 参照图 14，选择信号 175 从控制单元 134 输出到加密 / 解密单元 133 以切换在加密 / 解密单元 133 中的子块变换的连接。

[0213] 将省略图 14 的构成元件和信号线的描述，这些构成元件和信号线与第一实施例中描述的那些相同。

[0214] 接着将描述加密 / 解密单元 133。图 15 是用来解释加密 / 解密单元 133 的方块图。参照图 15，修改轮回函数模块 135 在选择信号 170 和选择信号 175 的控制下使用轮回密钥 A162 和轮回密钥 B163 执行一个周期的加密。修改轮回函数模块 136 在选择信号 170 和 175 的控制下使用轮回密钥 A162 和轮回密钥 B163 执行解密。

[0215] 在以上设置中，当选择信号 171 被取消时，加密 / 解密单元 133 的选择器 109 选择输入信号 150。当选择信号 171 被声明时，选择器 109 选择来自数据保持单元 108 的输出。

[0216] 将省略图 15 的构成元件和信号线的描述，这些构成元件和信号线与第一实施例中描述的那些相同。

[0217] 接着将描述修改轮回函数模块 135。图 16 是修改轮回函数模块 135 的方块图。参照图 16，AddRoundKey 变换模块 114 接收输入信号 165 和轮回密钥 B163，并且执行 AddRoundKey 变换。选择器 137 按照选择信号 175 选择并输出输入信号 165 和来自 AddRoundKey 变换模块 114 的输出之一。SubBytes 变换模块 111 接收来自选择器 137 的输出，并且执行 SubBytes 变换。ShiftRows 变换模块 112 接收来自 SubBytes 变换模块 111 的输出，并且执行 ShiftRows 变换。MixColumns 变换模块 113 接收来自 ShiftRows 变换模块 112 的输出，并且执行 MixColumns 变换。选择器 115 按照选择信号 170 选择并输出来自 MixColumns 变换模块 113 的输出和来自 ShiftRows 变换模块 112 的输出之一。AddRoundKey

变换模块 110 接收来自选择器 115 的输出和轮回密钥 A162，并且执行 AddRoundKey 变换。AddRoundKey 变换模块 110 的输出信号是修改轮回函数模块 135 的输出信号。

[0218] 在以上设置中，当选择信号 170 被取消时，选择器 115 选择并输出来自 MixColumns 变换模块 113 的输出。当选择信号 170 被声明时，选择器 115 选择并输出来自 ShiftRows 变换模块 112 的输出。当选择信号 175 被取消时，选择器 137 选择并输出输入信号 165。当选择信号 175 被声明时，选择器 137 选择并输出来自 AddRoundKey 变换模块 114 的输出。

[0219] 接着将描述修改轮回函数模块 136。图 17 是修改轮回函数模块 136 的方块图。参照图 17，AddRoundKey 变换模块 121 接收输入信号 165 和轮回密钥 A162，并且执行 AddRoundKey 变换。InvMixColumns 变换模块 116 接收来自 AddRoundKey 变换模块 121 的输出，并且执行 InvMixColumns 变换。选择器 118 按照选择信号 170 选择并输出来自 InvMixColumns 变换模块 116 的输出和来自 AddRoundKey 变换模块 121 的输出之一。InvShiftRows 变换模块 119 接收来自选择器 118 的输出，并且执行 InvShiftRows 变换。InvSubBytes 变换模块 120 接收来自 InvShiftRows 变换模块 119 的输出，并且执行 InvSubBytes 变换。AddRoundKey 变换模块 117 接收来自 InvSubBytes 变换模块 120 的输出和轮回密钥 B163，并且执行 AddRoundKey 变换。选择器 138 按照选择信号 175 选择并输出来自 InvSubBytes 变换模块 120 的输出和来自 AddRoundKey 变换模块 117 的输出之一。选择器 138 的输出是修改轮回函数模块 136 的输出。

[0220] 在以上设置中，当选择信号 170 被取消时，选择器 118 选择并输出来自 InvMixColumns 变换模块 116 的输出。当选择信号 170 被声明时，选择器 118 选择并输出来自 AddRoundKey 变换模块 121 的输出。当选择信号 175 被取消时，选择器 138 选择并输出来自 InvSubBytes 变换模块 120 的输出。当选择信号 175 被声明时，选择器 138 选择并输出来自 AddRoundKey 变换模块 117 的输出。

[0221] 接着将描述以上设置中的加密操作。图 18A 和 18B 是根据第二实施例的加密时序图。参照图 18A 和 18B，横坐标代表时间。时序名称 T01、T02、...、T33 被赋予时钟脉冲的前沿。在图 18A 左端沿纵坐标的三位数指示信号线，并且与图 14 至 17 中使用的信号线的附图标记具有一一对应性。

[0222] 在图 18A 和 18B 的时序图中表示的加密操作大致划分成四部分。第一部分是用来设置诸如密码密钥之类的各种参数的参数设置时段 (T01 至 T06)。第二部分是用来产生 wkey0 并把它保持在寄存器中的密钥准备时段 (T06 至 T17)。第三部分是第一块加密时段 (T17 至 T27)。第四部分是第二块加密时段 (从 T27 起)。

[0223] 参数设置时段的作用、开始条件及结束条件与第一实施例相同。密钥准备时段是从 T06 至 T17，并且开始条件和结束条件与第一实施例相同。每个电路的操作也与第一实施例几乎相同。然而，密钥扩展单元 132 在时序 T16 的操作、密钥扩展单元 132 和控制单元 134 在时序 T17 的操作与第一实施例不同，因此将在下面描述。

[0224] 在时序 T16，密钥扩展单元 132 输出 wkey0 作为轮回密钥 B163。轮回密钥 wkey10 被保持于在密钥扩展单元 132 提供的寄存器中。

[0225] 在时序 T17，密钥扩展单元 132 输出 wkey1 作为轮回密钥 A162。控制单元 134 声明选择信号 175。

[0226] 第一块加密时段是从 T17 到 T27，并且开始条件和结束条件与第一实施例相同。每

个电路的操作也与第一实施例几乎相同。

[0227] 控制单元 134 在加密结束时声明选择信号 175，并且在加密的第一周期中取消它 (T18 或 T28)。控制单元 134 还在加密的最后周期 (T16) 声明选择信号 170，并且在加密结束 (T17) 时取消它。控制单元 134 还在加密的第一周期声明选择信号 171，并且在加密结束时取消它。

[0228] 如有关电路设置描述的那样，当选择信号 171 被取消时，选择器 109 选择输入信号 150。当选择信号 171 被声明时，选择器 109 选择来自数据保持单元 108 的输出。当选择信号 170 被取消时，选择器 115 选择并输出来自 MixColumns 变换模块 113 的输出。当选择信号 170 被声明时，选择器 115 选择并输出来自 AddRoundKey 变换模块 112 的输出。当选择信号 175 被取消时，选择器 137 选择并输出输入信号 165。当选择信号 175 被声明时，选择器 137 选择并输出来自 AddRoundKey 变换模块 114 的输出。

[0229] 因此，在第 0 周期 (T17 至 T18)，修改轮回函数模块 135 对输入信号 150 执行 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换、MixColumns 变换及 AddRoundKey 变换。从第一周期起，修改轮回函数模块输出通过对紧邻前一周期的结果执行 SubBytes 变换、ShiftRows 变换、MixColumns 变换及 AddRoundKey 变换得到的结果。在第九周期 (T26 至 T27)，修改轮回函数模块输出通过执行 SubBytes 变换、ShiftRows 变换及 AddRoundKey 变换得到的结果。

[0230] 修改轮回函数模块 135 通过按上述方式控制选择信号 171、170 及 175 可执行图 11 所示的加密。

[0231] 另一方面，密钥扩展单元 132 在密钥准备时段后输出作为轮回密钥 A162 的 wkey1 和作为轮回密钥 B163 的 wkey0。为此，wkey0 和 wkey1 在加密开始 (T17) 时被供给到修改轮回函数模块 135。基于加密 / 解密开始信号 158 检测到加密开始时 (T17)，密钥扩展单元 132 使用在轮回密钥 A 寄存器中保持的 wkey1 产生 wkey2，并且把 wkey2 保持在轮回密钥 A 寄存器中。因此，wkey2 在 T18 供给到修改轮回函数模块 135。轮回密钥以相同方式供给直到 T26。当 wkey10 被保持在轮回密钥 A 寄存器中，并且轮回密钥供给在 T26 结束时，密钥扩展单元 132 把从外部连续供给的 wkey0 产生 wkey1 用作密码密钥 152，并且把 wkey1 保持在轮回密钥 A 寄存器中以准备下次加密开始 (T27)。

[0232] 当密钥扩展单元 132 按上述方式操作时，修改轮回函数模块 135 可如图 11 所示在每个周期使用轮回密钥。

[0233] 根据第二实施例的加密时段期间操作按上述方式进行。第二块的加密操作以与第一块相同的方式进行。从那时起，加密操作被重复地进行与块的预定数量一样多次。在图 18A 和 18B 的时序图中，第二块的加密在距离第一块加密结束的最短间隔开始。AES 芯通过以这样一种时序执行所有块的加密可呈现其最大性能。然而，加密间隔基本上可设置到任意长度。

[0234] 当预定数量的块的加密已完全结束，并且下个作业要使用诸如密码密钥之类的不同参数执行时，处理再次从参数设置开始。

[0235] 接着将描述这个实施例的解密操作。图 19A 和 19B 是根据这个实施例的解密时序图。参照图 19A 和 19B，横坐标代表时间。时序名称 T01、T02、...、T33 被赋予时钟脉冲的前沿。在图 19A 左端沿纵坐标的三位数指示信号线，并且与图 14 至 17 中使用的信号线的

附图标记具有一一对应性。

[0236] 在图 19A 和 19B 的时序图中表示的解密操作也大致划分成四部分。第一部分是用来设置诸如密码密钥之类的各种参数的参数设置时段 (T01 至 T06)。第二部分是用来产生 wkey0 并把它保持在寄存器中的密钥准备时段 (T06 至 T17)。第三部分是第一块解密时段 (T17 至 T27)。第四部分是第二块解密时段 (从 T27 起)。

[0237] 参数设置时段的作用、开始条件及结束条件与第一实施例相同。密钥准备时段是从 T06 至 T17，并且开始条件和结束条件与第一实施例相同。每个电路的操作也与第一实施例几乎相同。然而，密钥扩展单元 132 在时序 T16 的操作、密钥扩展单元 132 和控制单元 134 在时序 T17 的操作与第一实施例不同，并因此将在下面描述。

[0238] 在时序 T16，密钥扩展单元 132 输出 wkey0 作为轮回密钥 B163。轮回密钥 wkey0 被保持于密钥扩展单元 132 提供的寄存器中。

[0239] 在时序 T17，密钥扩展单元 132 输出 wkey10 作为轮回密钥 A162。控制单元 134 声明选择信号 170。

[0240] 第一块解密时段是从 T17 到 T27，并且开始条件和结束条件与第一实施例相同。每个电路的操作也与第一实施例几乎相同。

[0241] 控制单元 134 在解密结束时声明选择信号 170，并且在解密的第一周期取消它 (T18 或 T28)。控制单元 134 还在解密的最后周期 (T16) 声明选择信号 175，并且在解密结束 (T17) 时取消它。控制单元 134 还在解密的第一周期声明选择信号 171，并且在解密结束时取消它。

[0242] 如有关电路设置描述的那样，当选择信号 171 被取消时，选择器 109 选择输入信号 150。当选择信号 171 被声明时，选择器 109 选择来自数据保持单元 108 的输出。当选择信号 170 被取消时，选择器 118 选择并输出来自 InvMixColumns 变换模块 116 的输出。当选择信号 170 被声明时，选择器 118 选择并输出来自 AddRoundKey 变换模块 121 的输出。当选择信号 175 被取消时，选择器 138 选择并输出来自 InvSubBytes 变换模块 120 的输出。当选择信号 175 被声明时，选择器 138 选择并输出来自 AddRoundKey 变换模块 117 的输出。

[0243] 因此，在第 0 周期 (T17 至 T18)，修改轮回函数模块 136 对输入信号 150 执行 AddRoundKey 变换、InvShiftRows 变换及 InvSubBytes 变换。从第一周期起，修改轮回函数模块输出通过对紧邻前一周期的结果执行 AddRoundKey 变换、InvMixColumns 变换、InvShiftRows 变换及 InvSubBytes 变换得到的结果。在第九周期 (T26 至 T27)，修改轮回函数模块输出通过执行 AddRoundKey 变换、InvMixColumns 变换、InvShiftRows 变换、InvSubBytes 变换及 AddRoundKey 变换得到的结果。

[0244] 修改轮回函数模块 136 通过按上述方式控制选择信号 171、170 及 175 可执行图 11 所示的解密。

[0245] 另一方面，密钥扩展单元 132 在密钥准备时段后输出作为轮回密钥 A162 的 wkey10 和作为轮回密钥 B163 的 wkey0。为此，wkey10 在解密开始 (T17) 时被供给到修改轮回函数模块 136。基于加密 / 解密开始信号 158 检测到解密开始时 (T17)，密钥扩展单元 132 使用在轮回密钥 A 寄存器中保持的 wkey10 产生 wkey9，并且把 wkey9 保持在轮回密钥 A 寄存器中。因此，wkey9 在 T18 供给到修改轮回函数模块 136。轮回密钥以相同方式供给直到 T26。当 wkey1 被保持在轮回密钥 A 寄存器中，并且轮回密钥供给在 T26 结束时，密钥扩展

单元 132 把在密钥扩展单元的内部寄存器中保持的 wkey10 加载在轮回密钥 A 寄存器中，以准备下次解密开始 (T27)。

[0246] 当密钥扩展单元 132 按上述方式操作时，修改轮回函数模块 136 可如图 11 所示在每个周期使用轮回密钥。

[0247] 根据第二实施例的解密时段期间操作按上述方式进行。第二块的解密操作以与第一块相同的方式进行。从那时起，解密操作被重复进行与块的预定数量一样多次。在图 19A 和 19B 的时序图中，第二块的解密在距离第一块解密结束的最短间隔开始。AES 芯通过以这样一种时序执行所有块的解密可呈现其最大性能。然而，解密间隔基本上可设置到任意长度。

[0248] 当预定数量的块的解密已经完全结束，并且下个作业要使用诸如密码密钥之类的不同参数执行时，处理再次从参数设置开始。

[0249] 第二实施例能以上述方式实施。在第二实施例中，在一个周期中必须执行的每个子块变换的信号处理时间总和的最大值稍微增大。然而，这在多数情况下几乎不成问题，因为在每个时钟周期时段用于每个子块变换的解密处理时间总和的最大值常常以足够的裕量设置为一个周期时间。为此，在多数情况下，AES 加密所要求的时钟周期的数量可被减小一个。这把 AES 处理速度提高约 10％。

[0250] 上述第二实施例仅是本发明的例子，并且本发明的效果不限于上述实施例的那些。

[0251] ＜第三实施例＞

[0252] 图 20 是表示根据第三实施例在时钟周期执行加密和解密过程内容的图。参照图 20，周期计数指示在 AES 处理开始是“0”的时钟周期计数。

[0253] 在第三实施例的加密中，AddRoundKey 变换、ShiftRows 变换及 SubBytes 变换在第 0 周期中被执行。在第一至第八周期中，AddRoundKey 变换、ShiftRows 变换、SubBytes 变换及 MixColumns 变换被执行。在第九周期中，MixColumns 变换、第一 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换及第二 AddRoundKey 变换被执行。至于轮回密钥，wkey0 被用在第 0 周期中，wkey1 被用在第一周期中，...，及 wkey8 被用在第八周期中。在第九周期中，使用两个轮回密钥 wkey9 和 wkey10。

[0254] 在第三实施例中，与现有技术相同的处理被总体上执行。然而，在第三实施例中，AES 加密可以少一个的时钟周期被执行。

[0255] 接着将描述根据第三实施例在时钟周期中执行的每个子块变换的信号处理时间总和。图 21 是表示第三实施例中在每个时钟周期中每个子块变换的加密处理时间总和与现有技术的总和之间的比较图。纵坐标代表时间。条带越长，处理时间越长。为了实现第三实施例，在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值必须小于一个周期时间。如图 21 所示，每个子块变换的处理时间在 SubBytes 变换中最长，并且按 MixColumns 变换、AddRoundKey 变换及 ShiftRows 变换的顺序缩短。

[0256] 在第三实施例中，在执行第一 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换、MixColumns 变换及第二 AddRoundKey 变换的第九周期中用于每个子块变换的信号处理时间总和，比在执行 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换及 MixColumns 变换的第一至第八周期中用于每个子块变换的信号处理时间总和、或在执行 AddRoundKey 变

换、SubBytes 变换及 ShiftRows 变换的第 0 周期中用于每个子块变换的信号处理时间总和更长。因此，第三实施例的用于每个子块变换的信号处理时间总和的最大值比现有技术的最大值大一个对应于 AddRoundKey 变换处理时间的量。然而，一个 AddRoundKey 变换处理时间比一个周期中用于每个子块变换的信号处理时间总和短得多。在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值常常以足够的裕量设置为一个周期时间。为此，如果现有技术在每个时钟周期时段中用于每个子块变换的加密处理时间总和的最大值比一个周期时间短，则也假定这个实施例在多数情况下是可实施的。

[0257] 本发明也适用于 AES 解密。

[0258] 如图 20 所示，在第三实施例的解密中，第一 AddRoundKey 变换、InvShiftRows 变换、InvSubBytes 变换、InvMixColumns 变换及第二 AddRoundKey 变换在第 0 周期中被执行。在第一至第八周期中，AddRoundKey 变换、InvShiftRows 变换、InvSubBytes 变换及 InvMixColumns 变换被执行。在第九周期中，AddRoundKey 变换、InvShiftRows 变换及 InvSubBytes 变换被执行。至于轮回密钥，wkey10 和 wkey9 被用在第 0 周期中，wkey8 被用在第一周期中，...，及 wkey0 被用在第九周期中。

[0259] 在第三实施例中，与在现有技术中相同的处理被总体上执行。然而，在此实施例中，AES 解密可以少一个的时钟周期被执行。

[0260] 接着将描述根据第三实施例在时钟周期中执行的每个子块变换的信号处理时间总和。图 22 是表示在第三实施例在时钟周期中执行的每个子块变换的信号处理时间总和与现有技术的总和之间的比较图。纵坐标代表时间。条带越长，处理时间越长。为了实施这个实施例，在每个时钟周期时段中每个子块变换的信号处理时间总和的最大值必须小于一个周期时间。如图 22 所示，每个子块变换的处理时间在 InvSubBytes 变换中最长，并且按 InvMixColumns 变换、AddRoundKey 变换及 InvShiftRows 变换的顺序缩短。

[0261] 在第三实施例中，在执行第一 AddRoundKey 变换、InvSubBytes 变换、InvShiftRows 变换、InvMixColumns 变换及第二 AddRoundKey 变换的第 0 周期中用于每个子块变换的信号处理时间总和，比在执行 AddRoundKey 变换、InvSubBytes 变换、InvShiftRows 变换及 InvMixColumns 变换的第一至第八周期中用于每个子块变换的信号处理时间总和、或在执行 AddRoundKey 变换、InvSubBytes 变换及 InvShiftRows 变换的第九周期中用于每个子块变换的信号处理时间总和更长。因此，第三实施例的每个子块变换的信号处理时间总和的最大值比现有技术的最大值大一个对应于 AddRoundKey 变换处理时间的量。然而，一个 AddRoundKey 变换处理时间比一个周期中用于每个子块变换的信号处理时间总和短得多。在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值常常以足够的裕量设置为一个周期时间。为此，如果现有技术在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值比一个周期时间短，则也假定这个实施例在多数情况下是可实施的。

[0262] 将概括第三实施例的上述特性特征。

[0263] 在一般常规实施方法中，由标准定义的轮回函数被认为是处理中的断点，并且加密和解密被分配给时钟周期。为此，在第 10 和第 0 周期中用于每个子块变换的信号处理时间总和比在第一至第九周期的每一个中用于每个子块变换的信号处理时间总和更短。就是说，每个周期中执行的每个子块变换的信号处理时间总和变化。

[0264] 另一方面，第三实施例中，一些时钟周期中的信号处理被增加，从而在每个时钟周期时段中用于每个子块变换的信号处理时间总和之间的差减小。

[0265] 在第三实施例中，在一个周期中执行每个子块变换的信号处理时间总和的最大值稍微增大。为此，本实施例在现有技术可实施的条件下不一定是可实施的。然而，这在多数情况下几乎不成问题，因为在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值常常以足够的裕量设置为一个周期时间。在多数情况下，AES 加密或解密所要求的时钟周期的数量可被减小一个。这把 AES 处理速度提高约 10％。

[0266] 接着将描述用来实施 AES 加密和解密的 AES 芯的电路设置。图 23 是根据这个实施例的 AES 芯的方块图。参照图 23，AES 芯 141 执行 AES 处理。密钥扩展单元 142 从密码密钥产生对于 AES 加密和解密必需的轮回密钥，并且输出轮回密钥。加密 / 解密单元 143 使用从密钥扩展单元 142 供给的轮回密钥执行 128- 位明文数据的加密或 128- 位密文数据的解密。控制单元 144 从在 AES 芯 141 外部的单元接收控制信号，并且产生控制密钥扩展单元 142 和加密 / 解密单元 143 的操作的信号、以及向在 AES 芯 141 外部的单元通知操作完成的信号。

[0267] 将省略图 23 中的构成元件和信号线的描述，这些构成元件和信号线与第一和第二实施例中描述的那些相同。

[0268] 接着将描述加密 / 解密单元 143。图 24 是表示加密 / 解密单元 143 的方块图。参照图 24，修改轮回函数模块 145 在选择信号 170 和 175 的控制下使用轮回密钥 A162 和轮回密钥 B163 执行一个周期的加密。修改轮回函数模块 146 在选择信号 170 和 175 的控制下使用轮回密钥 A162 和轮回密钥 B163 执行解密。

[0269] 在以上设置中，当选择信号 171 被取消时，加密 / 解密单元 143 的选择器 109 选择输入信号 150。当选择信号 171 被声明时，选择器 109 选择来自数据保持单元 108 的输出。

[0270] 将省略图 24 中的构成元件和信号线的描述，这些构成元件和信号线与第一实施例中描述的那些相同。

[0271] 接着将描述修改轮回函数模块 145。图 25 是修改轮回函数模块 145 的方块图。参照图 25，MixColumns 变换模块 113 接收输入信号 165，并且执行 MixColumns 变换。选择器 137 按照选择信号 175 选择并输出输入信号 165 和来自 MixColumns 变换模块 113 的输出之一。AddRoundKey 变换模块 110 接收来自选择器 137 的输出和轮回密钥 A162，并且执行 AddRoundKey 变换。SubBytes 变换模块 111 接收来自 AddRoundKey 变换模块 110 的输出，并且执行 SubBytes 变换。ShiftRows 变换模块 112 接收来自 SubBytes 变换模块 111 的输出，并且执行 ShiftRows 变换。AddRoundKey 变换模块 114 接收来 ShiftRows 变换模块 112 的输出和轮回密钥 B163，并且执行 AddRoundKey 变换。选择器 115 按照选择信号 170 选择并输出来自 ShiftRows 变换模块 112 的输出和来自 AddRoundKey 变换模块 114 的输出之一。选择器 115 的输出信号是修改轮回函数模块 145 的输出信号。

[0272] 在以上设置中，当选择信号 170 被取消时，选择器 115 选择并输出来自 ShiftRows 变换模块 112 的输出。当选择信号 170 被声明时，选择器 115 选择并输出来自 AddRoundKey 变换模块 114 的输出。当选择信号 175 被取消时，选择器 137 选择并输出来自 MixColumns 变换模块 113 的输出。当选择信号 175 被声明时，选择器 147 选择并输出输入信号 165。

[0273] 接着将描述修改轮回函数模块 146。图 26 是修改轮回函数模块 146 的方块

图。参照图 26，AddRoundKey 变换模块 121 接收输入信号 165 和轮回密钥 A162，并且执行 AddRoundKey 变换。选择器 118 按照选择信号 170 选择并输出输入信号 165 和来自 AddRoundKey 变换模块 121 的输出之一。InvShiftRows 变换模块 119 接收来自选择器 118 的输出，并且执行 InvShiftRows 变换。InvSubBytes 变换模块 120 接收来自 InvShiftRows 变换模块 119 的输出，并且执行 InvSubBytes 变换。AddRoundKey 变换模块 117 接收来自 InvSubBytes 变换模块 120 的输出和轮回密钥 B163，并且执行 AddRoundKey 变换。InvMixColumns 变换模块 116 接收来自 AddRoundKey 变换模块 117 的输出，并且执行 InvMixColumns 变换。选择器 138 按照选择信号 175 选择并输出来自 InvMixColumns 变换模块 116 的输出和来自 AddRoundKey 变换模块 117 的输出之一。选择器 138 的输出是修改轮回函数模块 146 的输出。

[0274] 在以上设置中，当选择信号 170 被取消时，选择器 118 选择并输出输入信号 165。当选择信号 170 被声明时，选择器 118 选择并输出来自 AddRoundKey 变换模块 121 的输出。当选择信号 175 被取消时，选择器 138 选择并输出来自 InvMixColumns 变换模块 116 的输出。当选择信号 175 被声明时，选择器 138 选择并输出来自 AddRoundKey 变换模块 117 的输出。

[0275] 接着将描述在以上设置中的加密操作。图 27A 和 27B 是根据这个实施例的加密时序图。参照图 27A 和 27B，横坐标代表时间。时序名称 T01、T02、...、T33 被赋予时钟脉冲的前沿。在图 27A 左端沿纵坐标的三位数指示信号线，并且与图 23 至 26 中使用的信号线的附图标记具有一一对应性。

[0276] 在图 27A 和 27B 的时序图中表示的加密操作大致划分成四部分。第一部分是用来设置诸如密码密钥之类的各种参数的参数设置时段 (T01 至 T06)。第二部分是用来产生 wkey0 并把它保持在寄存器中的密钥准备时段 (T06 至 T17)。第三部分是第一块加密时段 (T17 至 T27)。第四部分是第二块加密时段 (从 T27 起)。

[0277] 参数设置时段的作用、开始条件及结束条件与第一实施例相同。密钥准备时段是从 T06 至 T17，并且开始条件和结束条件与第一实施例相同。每个电路的操作也与第一实施例几乎相同。然而，控制单元 144 在密钥准备时段的结束 (T17) 时声明选择信号 175。

[0278] 第一块加密时段是从 T17 到 T27，并且开始条件和结束条件与第一实施例相同。每个电路的操作也与第一实施例几乎相同。

[0279] 控制单元 144 在加密结束时声明选择信号 175，并且在加密的第一周期取消它 (T18 或 T28)。控制单元 144 还在加密的最后周期 (T16) 声明选择信号 170，并且在加密结束 (T17) 时取消它。控制单元 144 还在加密的第一周期声明选择信号 171，并且在加密结束时取消它。

[0280] 如有关电路设置描述的那样，当选择信号 171 被取消时，选择器 109 选择输入信号 150。当选择信号 171 被声明时，选择器 109 选择来自数据保持单元 108 的输出。当选择信号 170 被取消时，选择器 115 选择并输出来自 ShiftRows 变换模块 112 的输出。当选择信号 170 被声明时，选择器 115 选择并输出来自 AddRoundKey 变换模块 114 的输出。当选择信号 175 被取消时，选择器 137 选择并输出来自 MixColumns 变换模块 113 的输出。当选择信号 175 被声明时，选择器 147 选择并输出输入信号 165。

[0281] 因此，在第 0 周期 (T17 至 T18)，修改轮回函数模块 145 对输入信号 150 执行

AddRoundKey 变换、SubBytes 变换及 ShiftRows 变换。从第一周期起，修改轮回函数模块输出通过对紧邻前一周期的结果执行 SubBytes 变换、ShiftRows 变换、MixColumns 变换及 AddRoundKey 变换得到的结果。在第九周期 (T26 至 T27)，修改轮回函数模块输出通过执行 MixColumns 变换、AddRoundKey 变换、SubBytes 变换、ShiftRows 变换及 AddRoundKey 变换得到的结果。

[0282] 修改轮回函数模块 145 通过按上述方式控制选择信号 171、170 及 175 可执行图 20 所示的加密。

[0283] 另一方面，密钥扩展单元 142 在密钥准备时段后输出作为轮回密钥 A162 的 wkey0 和作为轮回密钥 B163 的 wkey10。为此，wkey0 在加密开始 (T17) 时被供给到修改轮回函数模块 145。基于加密 / 解密开始信号 158 检测到加密开始时 (T17)，密钥扩展单元 142 使用在轮回密钥 A 寄存器中保持的 wkey0 产生 wkey1，并且把 wkey1 保持在轮回密钥 A 寄存器中。因此，wkey1 在 T18 供给到修改轮回函数模块 145。轮回密钥以相同方式供给直到 T26。在 T26，也供给作为轮回密钥 B163 的 wkey10。当 wkey10 被保持在轮回密钥 A 寄存器中，并且轮回密钥供给在 T26 结束时，密钥扩展单元 142 把从外部连续地供给的 wkey0 作为密码密钥 152 保持在轮回密钥 A 寄存器中以准备下次加密开始 (T27)。

[0284] 当密钥扩展单元 142 按上述方式操作时，修改轮回函数模块 145 可如图 20 所示在每个周期使用轮回密钥。

[0285] 根据第三实施例在加密时段期间的操作按上述方式进行。第二块的加密操作以与对于第一块相同的方式进行。从那时起，加密操作被重复地进行与块的预定数量一样多次。在图 27A 和 27B 的时序图中，第二块的加密在距离第一块加密结束的最短间隔处开始。AES 芯通过以这样一种时序执行所有块的加密可呈现其最大性能。然而，加密间隔基本上可设置到任意长度。

[0286] 当预定数量的块的加密已经完全结束，并且下个作业要使用诸如密码密钥之类的不同参数执行时，处理再次从参数设置开始。

[0287] 接着将描述这个实施例的解密操作。图 28A 和 28B 是根据这个实施例的解密时序图。参照图 28A 和 28B，横坐标代表时间。时序名称 T01、T02、...、T33 被赋予时钟脉冲的前沿。在图 28A 左端沿纵坐标的三位数指示信号线，并且与在图 23 至 26 中使用的信号线的附图标记具有一一对应性。

[0288] 在图 28A 和 28B 的时序图中表示的解密操作也大致划分成四部分。第一部分是用来设置诸如密码密钥之类的各种参数的参数设置时段 (T01 至 T06)。第二部分是用来产生 wkey0 并把它保持在寄存器中的密钥准备时段 (T06 至 T17)。第三部分是第一块解密时段 (T17 至 T27)。第四部分是第二块解密时段 (从 T27 起)。

[0289] 参数设置时段的作用、开始条件及结束条件与第一实施例相同。密钥准备时段是从 T06 至 T17，并且开始条件和结束条件与第一实施例相同。每个电路的操作也与第一实施例几乎相同。然而，控制单元 144 在密钥准备时段的结束 (T17) 时声明选择信号 170。

[0290] 第一块解密时段是从 T17 到 T27，并且开始条件和结束条件与第一实施例相同。每个电路的操作也与第一实施例几乎相同。

[0291] 控制单元 144 在解密结束时声明选择信号 170，并且在解密的第一周期取消它 (T18 或 T28)。控制单元 144 还在解密的最后周期 (T16) 声明选择信号 175，并且在解密结

束 (T17) 时取消它。控制单元 144 还在解密的第一周期声明选择信号 171，并且在解密结束时取消它。

[0292] 如有关电路设置描述的那样，当选择信号 171 被取消时，选择器 109 选择输入信号 150。当选择信号 171 被声明时，选择器 109 选择来自数据保持单元 108 的输出。当选择信号 170 被取消时，选择器 118 选择并输出输入信号 165。当选择信号 170 被声明时，选择器 118 选择并输出来自 AddRoundKey 变换模块 121 的输出。当选择信号 175 被取消时，选择器 138 选择并输出来自 InvMixColumns 变换模块 116 的输出。当选择信号 175 被声明时，选择器 138 选择并输出来自 AddRoundKey 变换模块 117 的输出。

[0293] 因此，在第 0 周期 (T17 至 T18)，修改轮回函数模块 146 对输入信号 150 执行 AddRoundKey 变换、InvShiftRows 变换、InvSubBytes 变换、AddRoundKey 变换及 InvMixColumns 变换。从第一周期起，修改轮回函数模块输出通过对紧邻前一周期的结果执行 InvShiftRows 变换、InvSubBytes 变换、AddRoundKey 变换及 InvMixColumns 变换得到的结果。在第九周期 (T26 至 T27)，修改轮回函数模块输出通过执行 InvShiftRows 变换、InvSubBytes 变换及 AddRoundKey 变换得到的结果。

[0294] 修改轮回函数模块 146 通过按上述方式控制选择信号 171、170 及 175 可执行图 20 所示的解密。

[0295] 另一方面，密钥扩展单元 142 在密钥准备时段后输出作为轮回密钥 A162 的 wkey9 和作为轮回密钥 B163 的 wkey10。为此，wkey10 和 wkey9 在解密开始 (T17) 时被供给到修改轮回函数模块 146。基于加密 / 解密开始信号 158 检测到解密开始时 (T17)，密钥扩展单元 142 使用在轮回密钥 A 寄存器保持的 wkey9 产生 wkey8，并且把 wkey8 保持在轮回密钥 A 寄存器。因此，wkey8 在 T18 供给到修改轮回函数模块 146。轮回密钥以相同方式供给直到 T26。当 wkey0 被保持在轮回密钥 A 寄存器中，并且轮回密钥供给在 T26 结束时，密钥扩展单元 142 使用在轮回密钥 B 寄存器保持的 wkey10 产生 wkey9，并且把 wkey9 保持在轮回密钥 A 寄存器以准备下次解密开始 (T27)。

[0296] 当密钥扩展单元 142 按上述方式操作时，修改轮回函数模块 146 可如图 20 所示在每个周期使用轮回密钥。

[0297] 根据这个实施例的在解密时段期间的操作按上述方式进行。第二块的解密操作以与第一块相同的方式进行。从那时起，解密操作被重复地进行与块的预定数量一样多次。在图 28A 和 28B 的时序图中，第二块的解密在距离第一块解密结束的最短间隔处开始。AES 芯通过以这样一种时序执行所有块的解密可呈现其最大性能。然而，解密间隔基本上可设置到任意长度。

[0298] 当预定数量的块的解密已经完全结束，并且下个作业要使用诸如密码密钥之类的不同参数执行时，处理再次从参数设置开始。

[0299] 第三实施例能以上述方式实施。在第三实施例中，在一个周期中必须执行的每个子块变换的信号处理时间总和的最大值稍微增大。然而，这在多数情况下几乎不成问题，因为在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值常常以足够的裕量设置为一个周期时间。为此，在多数情况下，AES 加密和解密所要求的时钟周期的数量可被减小一个。这把 AES 处理速度提高约 10％。

[0300] 如以上描述的那样，通过应用本发明的想法，除基本第一实施例以外还可得到多

个实施例。例子是第二和第三实施例。在加密的任意周期中执行 AddRoundKey 变换两次的设置也是可得到的，如图 26 所示，表明用来在第八周期执行 AddRoundKey 变换两次的设置。实施例仅是本发明的例子，并且本发明的效果不限于在实施例中描述的那些。

[0301] 〈第四实施例〉

[0302] 在第四实施例中，使用 FIPS197 描述的等效逆密码执行解密。

[0303] 图 29 表示在第四实施例在时钟周期中执行的加密过程内容与现有技术之间的比较。

[0304] 参照图 29，周期计数指示在 AES 处理开始是“0”的时钟周期计数。

[0305] 这个实施例中，AddRoundKey 变换、ShiftRows 变换、SubBytes 变换及 MixColumns 变换在第 0 至第八周期中被执行。在第九周期中，第一 AddRoundKey 变换、ShiftRows 变换、SubBytes 变换及第二 AddRoundKey 变换被执行。至于轮回密钥，wkey0 被用在第 0 周期中，wkey1 被用在第一周期中，...，及 wkey8 被用在八周期中。在第九周期中，使用两个轮回密钥 wkey9 和 wkey10。

[0306] 在第四实施例中，与在现有技术中相同的处理被总体上执行。然而，在第四实施例中，AES 加密可以少一个的时钟周期被执行。

[0307] 接着将描述根据第四实施例在每个时钟周期时段中用于每个子块变换的加密处理时间总和。图 31 是表示现有技术在每个时钟周期时段中用于每个子块变换的加密处理时间总和与第四实施例的总和之间的比较图。纵坐标代表时间。条带越长，处理时间越长。为了实现第四实施例，在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值必须小于一个时钟周期时间。如图 31 所示，每个子块变换的处理时间在 SubBytes 变换中最长，并且按 MixColumns 变换、AddRoundKey 变换及 ShiftRows 变换的顺序缩短。

[0308] 在第四实施例中，在执行 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换及 MixColumns 变换的第 0 至第八周期的每一个周期中每个子块变换的信号处理时间总和比在执行第一 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换及第二 AddRoundKey 变换的第九周期中每个子块变换的信号处理时间总和更长。因此，在第四实施例在一个时钟周期中执行的每个子块变换的信号处理时间总和的最大值与现有技术的最大值相等。如果在一个周期中执行的每个子块变换的信号处理时间总和的最大值比现有技术中的一个周期时间短，则这个实施例也可实现。

[0309] 本发明也适用于 AES 解密。

[0310] 图 30 表示在第四实施例中在时钟周期中执行解密过程内容与现有技术之间的比较。

[0311] 参照图 30，周期计数指示在 AES 处理开始是“0”的时钟周期计数。修改解密密钥 wkey′（i 是轮回数）是对 FIPS197 描述的等效逆密码必需的轮回密钥。

[0312] 在第四实施例中，AddRoundKey 变换、InvShiftRows 变换、InvSubBytes 变换及 InvMixColumns 变换在第 0 至第八周期中被执行。在第九周期，第一 AddRoundKey 变换、InvShiftRows 变换、InvSubBytes 变换及第二 AddRoundKey 变换被执行。至于轮回密钥，wkey10 被用在第 0 周期，wkey9′ 被用在第一周期中，...，wkey2′ 被用在第八周期中。在第九周期，使用两个轮回密钥 wkey1′ 和 wkey0。

[0313] 在第四实施例中，与在现有技术中相同的处理被总体上执行。然而，在第四实施例

中，AES 解密可以少一个的时钟周期被执行。

[0314] 接着将描述根据第四实施例在每个时钟周期时段用于每个子块变换的解密处理时间总和。图 31 是表示在第四实施例中每个时钟周期时段中用于每个子块变换的解密处理时间总和与现有技术的总和之间的比较图。纵坐标代表时间。条带越长，处理时间越长。为了实施这个实施例，在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值必须小于一个时钟周期时间。如图 31 所示，每个子块变换的处理时间在 InvSubBytes 变换中最长，并且按 InvMixColumns 变换、AddRoundKey 变换及 InvShiftRows 变换的顺序缩短。

[0315] 在第四实施例中，在执行 AddRoundKey 变换、InvSubBytes 变换、InvShiftRows 变换及 InvMixColumns 变换的第 0 至第八周期的每一个中用于每个子块变换的信号处理时间总和比在执行第一 AddRoundKey 变换、InvSubBytes 变换、InvShiftRows 变换及第二 AddRoundKey 变换的第九周期中用于每个子块变换的信号处理时间总和更长。因此，这个实施例中在一个时钟周期中执行每个子块变换的信号处理时间总和的最大值与现有技术的最大值相等。如果在一个时钟周期中执行每个子块变换的信号处理时间总和的最大值比在现有技术中的一个周期时间短，则也可实施这个实施例。

[0316] 将概括第四实施例的上述特性特征。

[0317] 在一般常规实施方法中，由标准定义的轮回函数被认为是处理中的断点，并且加密和解密被分配给时钟周期。为此，在第 10 和第 0 周期中用于每个子块变换的信号处理时间总和比在第一至第九周期的每一个周期中用于每个子块变换的信号处理时间总和短。就是说，在每个周期中用于执行每个子块变换的信号处理时间总和变化。

[0318] 另一方面，在第四实施例中，一些时钟周期中的信号处理被增加，从而在每个时钟周期时段中用于每个子块变换的信号处理时间总和之间的差最小。在本发明中，AES 加密或解密所要求的时钟周期数量被减小一个，而不增加一个周期中执行每个子块变换的信号处理时间总和。这把 AES 处理速度提高约 10％。

[0319] 接着将描述用来实施 AES 加密和解密的 AES 芯的电路设置。

[0320] 图 32 是根据第四实施例的 AES 芯的方块图。

[0321] 参照图 32，AES 芯 201 执行 AES 处理。密钥扩展单元 202 从密码密钥产生对于 AES 加密和解密必需的轮回密钥，并且输出轮回密钥。加密 / 解密单元 203 使用从密钥扩展单元 202 供给的轮回密钥执行 128- 位明文数据的加密或 128- 位密文数据的解密。控制单元 204 从在 AES 芯 201 外部的单元接收控制信号，并且产生控制密钥扩展单元 202 和加密 / 解密单元 203 的操作的信号、以及向在 AES 芯 201 外部的单元通知操作完成的信号。

[0322] 将省略图 32 的构成元件和信号线的描述，这些构成元件和信号线与第一实施例中描述的那些相同。

[0323] 接着将描述加密 / 解密单元 203。图 33 是加密 / 解密单元 203 的方块图。参照图 33，修改轮回函数模块 205 在选择信号 170、加密 / 解密选择信号 153 及选择信号 175 的控制下使用轮回密钥 A162 和轮回密钥 B163 执行一个周期的加密或解密。

[0324] 在以上设置中，当选择信号 171 被取消时，选择器 109 选择输入信号 150。当选择信号 171 被声明时，选择器 109 选择来自数据保持单元 108 的输出。

[0325] 将省略图 33 中的构成元件和信号线的描述，这些构成元件和信号线与第一实施

例中描述的那些相同。

[0326] 接着将描述修改轮回函数模块 205。图 34 是修改轮回函数模块 205 的方块图。参照图 34，AddRoundKey 变换模块 110 接收输入信号 165 和轮回密钥 A162，并且执行 AddRoundKey 变换。SubBytes/InvSubBytes 变换模块 222 接收来自 AddRoundKey 变换模块 110 的输出，并且按照加密 / 解密选择信号 153 执行 SubBytes 变换和 InvSubBytes 变换之一。ShiftRows/InvShiftRows 变换模块 223 接收来自 SubBytes/InvSubBytes 变换模块 222 的输出，并且按照加密 / 解密选择信号 153 执行 ShiftRows 变换和 InvShiftRows 变换之一。MixColumns/InvMixColumns 变换模块 224 接收来自 ShiftRows/InvShiftRows 变换模块 223 的输出，并且按照加密 / 解密选择信号 153 执行 MixColumns 变换和 InvMixColumns 变换之一。AddRoundKey 变换模块 114 接收来自 ShiftRows/InvShiftRows 变换模块 223 的输出，并且执行 AddRoundKey 变换。选择器 115 按照选择信号 170 选择并输出来自 MixColumns/InvMixColumns 变换模块 224 的输出和来自 AddRoundKey 变换模块 114 的输出之一。选择器 115 的输出信号是修改轮回函数模块 205 的输出信号。

[0327] 在以上设置中，当选择信号 170 被取消时，选择器 115 选择并输出来自 MixColumns/InvMixColumns 变换模块 224 的输出。当选择信号 170 被声明时，选择器 115 选择并输出来自 AddRoundKey 变换模块 114 的输出。当加密 / 解密选择信号 153 被取消时，SubBytes/InvSubBytes 变换模块 222、ShiftRows/InvShiftRows 变换模块 223 及 MixColumns/InvMixColumns 变换模块 224 分别执行 SubBytes 变换、ShiftRows 变换及 MixColumns 变换。当加密 / 解密选择信号 153 被声明时，它们分别执行 InvSubBytes 变换、InvShiftRows 变换及 InvMixColumns 变换。

[0328] 接着参照图 9A 和 9B 的时序图将描述以上设置中的加密操作。参照图 9A 和 9B，横坐标代表时间。时序名称 T01、T02、...、T33 被赋予时钟脉冲的前沿。

[0329] 图 9A 左端沿纵坐标的三位数指示信号线，并且与在图 32 至 34 中使用的信号线的附图标记具有一一对应性。

[0330] 在图 9A 和 9B 的时序图中表示的加密操作大致划分成四部分。第一部分是用来设置诸如密码密钥之类的各种参数的参数设置时段 (T01 至 T06)。第二部分是用来产生 wkey0 并把它保持在寄存器中的密钥准备时段 (T06 至 T17)。第三部分是第一块加密时段 (T17 至 T27)。第四部分是第二块加密时段 (从 T27 起)。

[0331] 参数设置时段的作用、开始条件及结束条件与第一实施例相同。密钥准备时段是从 T06 至 T17。在密钥准备时段中的开始条件、结束条件及每个电路的操作与第一实施例相同，并且将不重复描述。

[0332] 第一块加密时段是从 T17 到 T27，并且开始条件和结束条件与第一实施例相同。每个电路的操作也与第一实施例几乎相同。

[0333] 控制单元 204 在加密的最后周期 (T16) 声明选择信号 170，并且在加密结束 (T17) 时取消它。控制单元 204 还在加密的第一周期声明选择信号 171，并且在加密结束时取消它。

[0334] 如有关电路设置描述的那样，当选择信号 171 被取消时，选择器 109 选择输入信号 150。当选择信号 171 被声明时，选择器 109 选择来自数据保持单元 108 的输出。当选择信号 170 被取消时，选择器 115 选择并输出来自 MixColumns/InvMixColumns 变换模块

224 的输出。当选择信号 170 被声明时，选择器 115 选择并输出来自 AddRoundKey 变换模块 114 的输出。当加密 / 解密选择信号 153 被取消时，SubBytes/InvSubBytes 变换模块 222、ShiftRows/InvShiftRows 变换模块 223 及 MixColumns/InvMixColumns 变换模块 224 分别执行 SubBytes 变换、ShiftRows 变换及 MixColumns 变换。当加密 / 解密选择信号 153 被声明时，它们分别执行 InvSubBytes 变换、InvShiftRows 变换及 InvMixColumns 变换。

[0335] 因此，在第 0 周期 (T17 至 T18)，修改轮回函数模块 205 对输入信号 150 执行 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换及 MixColumns 变换。从第一周期起，修改轮回函数模块输出通过对紧邻前一周期的结果执行 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换及 MixColumns 变换得到的结果。在第九周期 (T26 至 T27)，修改轮回函数模块输出通过执行 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换及 AddRoundKey 变换得到的结果。

[0336] 修改轮回函数模块 205 通过按上述方式控制选择信号 171 和 170 可执行图 29 所示的加密。

[0337] 另一方面，密钥扩展单元 202 在密钥准备时段后输出作为轮回密钥 A162 的 wkey0 和作为轮回密钥 B163 的 wkey10。为此，wkey0 在加密开始 (T17) 时被供给到修改轮回函数模块 205。基于加密 / 解密开始信号 158 检测到加密开始时 (T17)，密钥扩展单元 202 使用在轮回密钥 A 寄存器中保持的 wkey0 产生 wkey1，并且把 wkey1 保持在轮回密钥 A 寄存器。因此，wkey1 在时序 T18 供给到修改轮回函数模块 205。轮回密钥以相同方式供给直到时序 T26。在 T26，供给用作轮回密钥 B163 的两个轮回密钥 wkey9 和 wkey10。当 wkey9 被保持在轮回密钥 A 寄存器，并且轮回密钥供给在 T26 结束时，密钥扩展单元 202 把从外部连续地供给的 wkey0 作为密码密钥 152 保持在轮回密钥 A 寄存器以准备下次加密开始 (T27)。

[0338] 当密钥扩展单元 202 按上述方式操作时，修改轮回函数模块 205 可如图 29 所示在每个周期使用轮回密钥。

[0339] 根据第四实施例在加密时段期间的操作按上述方式进行。第二块的加密操作以与第一块相同的方式进行。从那时起，加密操作被重复地进行与块的预定数量一样多次。在图 9A 和 9B 的时序图中，第二块的加密在距离第一块加密结束的最短间隔处开始。AES 芯通过以这样一种时序执行所有块的加密可呈现其最大性能。然而，加密间隔基本上可设置到任意长度。

[0340] 当预定数量的块的加密已经完全结束，并且下个作业要使用诸如密码密钥之类的不同参数执行时，处理再次从参数设置开始。

[0341] 接着将描述这个实施例的解密操作。图 35A 和 35B 是根据第四实施例的解密时序图。参照图 35A 和 35B，横坐标代表时间。时序名称 T01、T02、...、T33 被赋予时钟脉冲的前沿。在图 35A 左端沿纵坐标的三位数指示信号线，并且与图 32 至 34 中使用的信号线的附图标记具有一一对应性。

[0342] 在图 35A 和 35B 的时序图表示的解密操作大致划分成四部分。第一部分是用来设置诸如密码密钥之类的各种参数的参数设置时段 (T01 至 T06)。第二部分是用来产生 wkey0 并把它保持在寄存器中的密钥准备时段 (T06 至 T17)。第三部分是第一块解密时段 (T17 至 T27)。第四部分是第二块解密时段 (从 T27 起)。

[0343] 参数设置时段的作用、开始条件及结束条件与第一实施例的加密中相同。

[0344] 密钥准备时段是从 T06 至 T17，并且开始条件和结束条件与在第一实施例的加密中相同。每个电路的操作也与这个实施例的加密中几乎相同。然而，密钥扩展单元 202 在时序 T16 的操作、密钥扩展单元 202 和控制单元 204 在时序 T17 的操作与加密中的那些不同，因此将在下面描述。

[0345] 在时序 T16，密钥扩展单元 202 输出作为轮回密钥 B163 的 wkey0 和作为轮回密钥 A162 的 wkey10。轮回密钥 wkey10 也被分离地保持于密钥扩展单元 202 提供的寄存器中。在 T16，密钥扩展单元 202 由 wkey10 反向地进行密钥扩展，以产生修改解密密钥 wkey9′ 。

[0346] 在时序 T17，密钥扩展单元 202 输出 wkey9′ 作为轮回密钥 A162。控制单元 204 声明选择信号 170。

[0347] 第一块解密时段是从 T17 到 T27，并且开始条件和结束条件与第一实施例相同。每个电路的操作也与第一实施例几乎相同。

[0348] 控制单元 204 在解密的最后周期 (T16) 声明选择信号 170，并且在解密结束 (T17) 时取消它。控制单元 204 还在解密的第一周期声明选择信号 171，并且在解密结束时取消它。

[0349] 如有关电路设置描述的那样，当选择信号 171 被取消时，选择器 109 选择输入信号 150。当选择信号 171 被声明时，选择器 109 选择来自数据保持单元 108 的输出。当选择信号 170 被取消时，选择器 115 选择并输出来自 MixColumns/InvMixColumns 变换模块 224 的输出。当选择信号 170 被声明时，选择器 115 选择并输出来自 AddRoundKey 变换模块 114 的输出。当加密 / 解密选择信号 153 被取消时，SubBytes/InvSubBytes 变换模块 222、ShiftRows/InvShiftRows 变换模块 223 及 MixColumns/InvMixColumns 变换模块 224 分别执行 SubBytes 变换、ShiftRows 变换及 MixColumns 变换。当加密 / 解密选择信号 153 被声明时，它们分别执行 InvSubBytes 变换、InvShiftRows 变换及 InvMixColumns 变换。

[0350] 因此，在第 0 周期 (T17 至 T18)，修改轮回函数模块 205 对输入信号 150 执行 AddRoundKey 变换、InvSubBytes 变换、InvShiftRows 变换及 InvMixColumns 变换。从第一周期起，修改轮回函数模块输出通过对紧邻前一周期的结果执行 AddRoundKey 变换、InvSubBytes 变换、InvShiftRows 变换及 InvMixColumns 变换得到的结果。在第九周期 (T26 至 T27)，修改轮回函数模块输出通过执行 AddRoundKey 变换、InvSubBytes 变换、InvShiftRows 变换及 AddRoundKey 变换得到的结果。

[0351] 修改轮回函数模块 205 通过按上述方式控制选择信号 171 和 170 可执行图 30 所示的解密。

[0352] 另一方面，密钥扩展单元 202 在密钥准备时段后输出作为轮回密钥 A162 的 wkey10 和作为轮回密钥 B163 的 wkey0。为此，wkey10 在解密开始 (T17) 时被供给到修改轮回函数模块 205。基于加密 / 解密开始信号 158 检测到解密开始时 (T17)，密钥扩展单元 202 使用在轮回密钥 A 寄存器保持的 wkey10 产生 wkey9′ ，并且把 wkey9′ 保持在轮回密钥 A 寄存器。因此，wkey9′ 在时序 T18 供给到修改轮回函数模块 205。轮回密钥以相同方式供给直到时序 T26。在 T26，供给用作轮回密钥 B163 的两个轮回密钥 wkey1′ 和 wkey0。当 wkey1′ 被保持在轮回密钥 A 寄存器中，并且轮回密钥供给在 T26 结束时，密钥扩展单元 202 把在密钥扩展单元的内部寄存器保持的 wkey10 加载在轮回密钥 A 寄存器中以准备下次解密开始 (T27)。

[0353] 当密钥扩展单元 202 按上述方式操作时，修改轮回函数模块 205 可如图 30 所示在每个周期使用轮回密钥。

[0354] 根据第四实施例在解密时段期间的操作按上述方式进行。第二块的解密操作以与第一块相同的方式进行。从那时起，解密操作被重复地进行与块的预定数量一样多次。在图 35A 和 35B 的时序图中，第二块的解密在距离第一块解密结束的最短间隔处开始。AES 芯通过以这样一种时序执行所有块的解密可呈现其最大性能。然而，解密间隔基本上可设置到任意长度。

[0355] 当预定数量的块的解密已经完全结束，并且下个作业要使用诸如密码密钥之类的不同参数执行时，处理再次从参数设置开始。

[0356] 第四实施例能以上述方式实施。在第四实施例中，已经描述了电路设置和使用等效逆密码执行解密的操作。在第四实施例中，对于 AES 加密所要求的时钟周期的数量被减小一个，而不增大在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值。这把 AES 处理速度提高约 10％。

[0357] 上述第四实施例仅是本发明的例子，并且本发明的效果不限于上述实施例的那些。

[0358] ＜第五实施例＞

[0359] 在第五实施例中，使用 FIPS197 描述的等效逆密码执行解密。

[0360] 图 36 是表示根据第五实施例在时钟周期中执行加密和解密过程内容的图。

[0361] 参照图 36，周期计数指示在 AES 处理开始是“0”的时钟周期计数。

[0362] 在这个实施例的加密中，第一 AddRoundKey 变换、ShiftRows 变换、SubBytes 变换、MixColumns 变换及第二 AddRoundKey 变换在第 0 周期中使用两个轮回密钥被执行。在第一至第八周期中，AddRoundKey 变换、ShiftRows 变换、SubBytes 变换及 MixColumns 变换被执行。在第九周期，AddRoundKey 变换、ShiftRows 变换及 SubBytes 变换被执行。至于轮回密钥，wkey0 和 wkey1 被用在第 0 周期中，wkey2 被用在第一周期中，...，及 wkey10 被用在第九周期中。

[0363] 在第五实施例中，与在现有技术中相同的处理被总体上执行。然而，这个实施例中，AES 加密可以少一个的时钟周期被执行。

[0364] 接着将描述根据第五实施例在每个时钟周期时段中用于每个子块变换的加密处理时间总和。图 37 是表示在第五实施例中在时钟周期中执行每个子块变换的信号处理时间总和与现有技术的总和之间的比较图。纵坐标代表时间。条带越长，处理时间越长。为了实现第五实施例，在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值必须小于一个时钟周期时间。如图 37 所示，每个子块变换的处理时间在 SubBytes 变换中最长，并且按 MixColumns 变换、AddRoundKey 变换及 ShiftRows 变换的顺序缩短。

[0365] 在第五实施例中，在执行第一 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换、MixColumns 变换及第二 AddRoundKey 变换的第 0 周期中用于每个子块变换的信号处理时间总和，比在执行 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换及 MixColumns 变换的第一至第八周期中用于每个子块变换的信号处理时间总和、或在执行 AddRoundKey 变换、SubBytes 变换及 ShiftRows 变换的第九周期中用于每个子块变换的信号处理时间总和更长。因此，第五实施例用于每个子块变换的信号处理时间总和的最大值比现有技术的最

大值大一个对应于 AddRoundKey 变换处理时间的量。然而，一个 AddRoundKey 变换处理时间比一个周期中用于每个子块变换的信号处理时间总和短得多。在每个时钟周期时段用于每个子块变换的信号处理时间总和的最大值常常以足够的裕量设置为一个周期时间。为此，如果现有技术在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值比一个周期时间短，则也假定这个实施例在多数情况下是可实施的。

[0366] 本发明也适用于 AES 解密。

[0367] 如图 36 所示，在这个实施例的解密中，第一 AddRoundKey 变换、InvShiftRows 变换、InvSubBytes 变换、InvMixColumns 变换及第二 AddRoundKey 变换在第 0 周期被执行。在第一至第八周期，AddRoundKey 变换、InvShiftRows 变换、InvSubBytes 变换及 InvMixColumns 变换被执行。在第九周期，AddRoundKey 变换、InvShiftRows 变换及 InvSubBytes 变换被执行。至于轮回密钥，wkey10 和 wkey9′ 被用在第 0 周期中，wkey8′ 被用在第一周期中，...，wkey0 被用在第九周期中。

[0368] 在第五实施例中，与在现有技术中相同的处理被总体上执行。然而，在第五实施例中，AES 解密可以少一个的时钟周期被执行。

[0369] 接着将描述根据第五实施例在每个时钟周期时段中用于每个子块变换的解密处理时间总和。图 37 是表示在第五实施例中每个时钟周期时段中用于每个子块变换的解密处理时间总和与现有技术的总和之间的比较图。纵坐标代表时间。条带越长，处理时间越长。为了实施这个实施例，在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值必须小于一个时钟周期时间。如图 37 所示，每个子块变换的处理时间在 InvSubBytes 变换中最长，并且按 InvMixColumns 变换、AddRoundKey 变换及 InvShiftRows 变换的顺序缩短。

[0370] 在第五实施例中，在执行 AddRoundKey 变换、InvSubBytes 变换、InvShiftRows 变换、InvMixColumns 变换及 AddRoundKey 变换的第 0 周期中用于每个子块变换的信号处理时间总和，比在执行 AddRoundKey 变换、InvSubBytes 变换、InvShiftRows 变换及 InvMixColumns 变换的第一至第八周期中用于每个子块变换的信号处理时间总和、或在执行 AddRoundKey 变换、InvSubBytes 变换及 InvShiftRows 变换的第九周期中用于每个子块变换的信号处理时间总和更长。因此，第五实施例用于每个子块变换的信号处理时间总和的最大值比现有技术的最大值大一个对应于 AddRoundKey 变换处理时间的量。然而，一个 AddRoundKey 变换处理时间比一个周期中用于每个子块变换的信号处理时间总和短得多。每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值常常以足够的裕量设置为一个周期时间。为此，如果现有技术的在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值比一个周期时间短，则也假定这个实施例在多数情况下是可实施的。

[0371] 将概括第五实施例的上述特性特征。

[0372] 在一般常规实施方法中，由标准定义的轮回函数被认为是处理中的断点，并且加密和解密被分配给时钟周期。为此，在第 10 和第 0 周期中用于每个子块变换的信号处理时间总和比第一至第九周期的每一个周期中用于每个子块变换的信号处理时间总和更短。就是说，在每个周期中用于执行每个子块变换的信号处理时间总和变化。

[0373] 另一方面，在第五实施例中，一些时钟周期中的信号处理被增加，从而在每个时钟

周期时段中用于每个子块变换的信号处理时间总和之间的差减小。

[0374] 在第五实施例中，在一个周期中用于每个子块变换的信号处理时间总和的最大值稍微增大。为此，本实施例在现有技术可实施的条件下不一定是可实施的。然而，这在多数情况下几乎不成问题，因为在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值常常以足够的裕量设置为一个周期时间。在多数情况下，AES 加密或解密所要求的时钟周期的数量可被减小一个。这把 AES 处理速度提高约 10％。

[0375] 接着将描述用来实施 AES 加密和解密的 AES 芯的电路设置。

[0376] 图 38 是根据第五实施例的 AES 芯的方块图。参照图 38，AES 芯 231 执行 AES 处理。密钥扩展单元 232 从密码密钥产生对于 AES 加密和解密必需的轮回密钥，并且输出轮回密钥。加密 / 解密单元 233 使用从密钥扩展单元 232 供给的轮回密钥执行 128- 位明文数据的加密或 128- 位密文数据的解密。控制单元 234 从在 AES 芯 231 外部的单元接收信号，并且产生控制密钥扩展单元 232 和加密 / 解密单元 233 的操作的信号、以及向在 AES 芯 231 外部的单元通知操作完成的信号。

[0377] 将省略图 38 中的构成元件和信号线的描述，这些构成元件和信号线与在第一和第二实施例中描述的那些相同。

[0378] 接着将描述加密 / 解密单元 233。图 39 是加密 / 解密单元 233 的方块图。参照图 39，修改轮回函数模块 235 在选择信号 170 和 175 及加密 / 解密选择信号 153 的控制下使用轮回密钥 A162 和轮回密钥 B163 执行一个周期的加密或解密。

[0379] 在以上设置中，当选择信号 171 被取消时，加密 / 解密单元 233 的选择器 109 选择输入信号 150。当选择信号 171 被声明时，选择器 109 选择来自数据保持单元 108 的输出。

[0380] 将省略图 39 中的构成元件和信号线的描述，这些构成元件和信号线与在第一和第二实施例中描述的那些相同。

[0381] 接着将描述修改轮回函数模块 235。图 40 是修改轮回函数模块 235 的方块图。参照图 40，AddRoundKey 变换模块 114 接收输入信号 165 和轮回密钥 B163，并且执行 AddRoundKey 变换。选择器 137 按照选择信号 175 选择并输出输入信号 165 和来自 AddRoundKey 变换模块 114 的输出之一。SubBytes/InvSubBytes 变换模块 222 接收来自选择器 137 的输出，并且按照加密 / 解密选择信号 153 执行 SubBytes 变换和 InvSubBytes 变换之一。ShiftRows/InvShiftRows 变换模块 223 接收来自 SubBytes/InvSubBytes 变换模块 222 的输出，并且按照加密 / 解密选择信号 153 执行 ShiftRows 变换和 InvShiftRows 变换之一。MixColumns/InvMixColumns 变换模块 224 接收来自 ShiftRows/InvShiftRows 变换模块 223 的输出，并且按照加密 / 解密选择信号 153 执行 MixColumns 变换和 InvMixColumns 变换之一。选择器 115 按照选择信号 170 选择并输出来自 MixColumns/InvMixColumns 变换模块 224 的输出和来自 ShiftRows/InvShiftRows 变换模块 223 的输出之一。AddRoundKey 变换模块 110 接收来自选择器 115 的输出和轮回密钥 A162，并且执行 AddRoundKey 变换。AddRoundKey 变换模块 110 的输出信号是修改轮回函数模块 235 的输出信号。

[0382] 在以上设置中，当选择信号 170 被取消时，选择器 115 选择并输出来自 MixColumns/InvMixColumns 变换模块 224 的输出。当选择信号 170 被声明时，选择器 115 选择并输出来自 ShiftRows/InvShiftRows 变换模块 223 的输出。当选择信号 175 被取消时，选择器 137 选择并输出输入信号 165。当选择信号 175 被声明时，选择器 137 选择并输

出来自 AddRoundKey 变换模块 114 的输出。

[0383] 接着参照图 18A 和 18B 的时序图将描述以上设置中的加密操作。在图 18A 左端沿纵坐标的三位数指示信号线，并且与图 38 至 40 中使用的信号线的附图标记具有一一对应性。

[0384] 在图 18A 和 18B 的时序图中表示的加密操作大致划分成四部分。第一部分是用来设置诸如密码密钥之类的各种参数的参数设置时段 (T01 至 T06)。第二部分是用来产生 wkey0 并把它保持在寄存器中的密钥准备时段 (T06 至 T17)。第三部分是第一块加密时段 (T17 至 T27)。第四部分是第二块加密时段 (从 T27 起)。

[0385] 参数设置时段的作用、开始条件及结束条件与在第二实施例中相同。密钥准备时段是从 T06 至 T17。开始条件、结束条件及每个电路的操作也与在第二实施例中相同，并且将不重复描述。第一块加密时段是从 T17 到 T27，并且开始条件和结束条件与在第二实施例中相同。每个电路的操作也与在第二实施例中相同。

[0386] 控制单元 234 在加密结束时声明选择信号 175，并且在加密的第一周期取消它 (T18 或 T28)。控制单元 234 还在加密的最后周期 (T16) 声明选择信号 170，并且在加密结束 (T17) 时取消它。控制单元 234 还在加密的第一周期声明选择信号 171，并且在加密结束时取消它。

[0387] 如有关电路设置描述的那样，当选择信号 171 被取消时，选择器 109 选择输入信号 150。当选择信号 171 被声明时，选择器 109 选择来自数据保持单元 108 的输出。当选择信号 175 被取消时，选择器 137 选择并输出输入信号 165。当选择信号 175 被声明时，选择器 137 选择并输出来自 AddRoundKey 变换模块 114 的输出。当选择信号 170 被取消时，选择器 115 选择并输出来自 MixColumns/InvMixColumns 变换模块 224 的输出。当选择信号 170 被声明时，选择器 115 选择并输出来自 ShiftRows/InvShiftRows 变换模块 223 的输出。当加密 / 解密选择信号 153 被取消时，SubBytes/InvSubBytes 变换模块 222、ShiftRows/InvShiftRows 变换模块 223 及 MixColumns/InvMixColumns 变换模块 224 分别执行 SubBytes 变换、ShiftRows 变换及 MixColumns 变换。当加密 / 解密选择信号 153 被声明时，它们分别执行 InvSubBytes 变换、InvShiftRows 变换及 InvMixColumns 变换。

[0388] 因此，在第 0 周期 (T17 至 T18)，修改轮回函数模块 235 对输入信号 150 执行 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换、MixColumns 变换及 AddRoundKey 变换。从第一周期起，修改轮回函数模块输出通过对紧邻前一周期的结果执行 SubBytes 变换、ShiftRows 变换、MixColumns 变换及 AddRoundKey 变换得到的结果。在第九周期 (T26 至 T27)，修改轮回函数模块输出通过执行 SubBytes 变换、ShiftRows 变换及 AddRoundKey 变换得到的结果。

[0389] 修改轮回函数模块 235 通过按上述方式控制选择信号 171、170 及 175 可执行图 36 所示的加密。

[0390] 另一方面，密钥扩展单元 232 在密钥准备时段后输出作为轮回密钥 A162 的 wkey1 和作为轮回密钥 B163 的 wkey0。为此，wkey0 和 wkey1 在加密开始 (T17) 时被供给到修改轮回函数模块 235。基于加密 / 解密开始信号 158 检测到加密开始时 (T17)，密钥扩展单元 232 使用在轮回密钥 A 寄存器保持的 wkey1 产生 wkey2，并且把 wkey2 保持在轮回密钥 A 寄存器。因此，wkey2 在时序 T18 供给到修改轮回函数模块 235。轮回密钥以相同方式供给

直到时序 T26。当 wkey10 被保持在轮回密钥 A 寄存器中，并且轮回密钥供给在时序 T26 结束时，密钥扩展单元 232 把从外部连续地供给 wkey0 用作密码密钥 152 产生 wkey1，并且把 wkey1 保持在轮回密钥 A 寄存器中以准备下次加密开始 (T27)。

[0391] 当密钥扩展单元 232 按上述方式操作时，修改轮回函数模块 235 可如图 36 所示在每个周期使用轮回密钥。

[0392] 根据第五实施例在加密时段期间的操作按上述方式进行。第二块的加密操作以与对于第一块相同的方式进行。从那时起，加密操作被重复地进行与块的预定数量一样多次。在图 18A 和 18B 的时序图中，第二块的加密在距离第一块加密结束的最短间隔处开始。AES 芯通过以这样一种时序执行所有块的加密可呈现其最大性能。然而，加密间隔基本上可设置到任意长度。

[0393] 当预定数量的块的加密已经完全结束，并且下个作业要使用诸如密码密钥之类的不同参数执行时，处理再次从参数设置开始。

[0394] 接着将描述第五实施例的解密操作。图 41A 和 41B 是根据第五实施例的解密时序图。参照图 41A 和 41B，横坐标代表时间。时序名称 T01、T02、...、T33 被赋予时钟脉冲的前沿。

[0395] 图 41A 左端沿纵坐标的三位数指示信号线，并且与在图 38 至 40 中使用的信号线的附图标记具有一一对应性。

[0396] 图 41A 和 41B 的时序图中表示的解密操作大致划分成四部分。第一部分是用来设置诸如密码密钥之类的各种参数的参数设置时段 (T01 至 T06)。第二部分是用来产生 wkey0 并把它保持在寄存器中的密钥准备时段 (T06 至 T17)。第三部分是第一块解密时段 (T17 至 T27)。第四部分是第二块解密时段 (从 T27 起)。

[0397] 参数设置时段的作用、开始条件及结束条件与在这个实施例的加密中相同。然而，在解密中，声明加密 / 解密选择信号 153。

[0398] 密钥准备时段是从 T06 至 T17，并且开始条件和结束条件与在这个实施例的加密中相同。每个电路的操作也与在这个实施例的加密中几乎相同。然而，密钥扩展单元 232 在时序 T16 的操作、密钥扩展单元 232 和控制单元 234 在时序 T17 的操作与加密中的那些不同，因此将在下面描述。

[0399] 在时序 T16，密钥扩展单元 232 输出作为轮回密钥 B163 的 wkey10 和作为轮回密钥 A162 的 wkey10。在 T16，密钥扩展单元 232 由 wkey10 反向地进行密钥扩展，以产生修改解密密钥 wkey9′ 。

[0400] 在时序 T17，密钥扩展单元 232 输出 wkey9′ 作为轮回密钥 A162。控制单元 234 声明选择信号 175。

[0401] 在密钥准备时段结束时 (T17)，控制单元 234 声明选择信号 175。

[0402] 第一块解密时段是从 T17 到 T27，并且开始条件和结束条件与第一实施例相同。每个电路的操作也与第一实施例几乎相同。

[0403] 控制单元 234 在解密的最后周期 (T26) 声明选择信号 170，并且在第一周期解密 (T18 或 T28) 取消它。控制单元 234 还在解密结束 (T17) 时声明选择信号 175，并且在解密结束 (T17) 时取消它。控制单元 234 还在解密的第一周期声明选择信号 171，并且在解密结束时取消它。

[0404] 如有关电路设置描述的那样，当选择信号 171 被取消时，选择器 109 选择输入信号 150。当选择信号 171 被声明时，选择器 109 选择来自数据保持单元 108 的输出。

[0405] 当选择信号 175 被取消时，选择器 137 选择并输出输入信号 165。当选择信号 175 被声明时，选择器 137 选择并输出来自 AddRoundKey 变换模块 114 的输出。当选择信号 170 被取消时，选择器 115 选择并输出来自 MixColumns/InvMixColumns 变换模块 224 的输出。当选择信号 170 被声明时，选择器 115 选择并输出来自 ShiftRows/InvShiftRows 变换模块 223 的输出。

[0406] 因此，在第 0 周期 (T17 至 T18)，修改轮回函数模块 235 对输入信号 150 执行 AddRoundKey 变换、InvShiftRows 变换、InvSubBytes 变换、AddRoundKey 变换及 InvMixColumns 变换。从第一周期起，修改轮回函数模块输出通过对紧邻前一周期的结果执行 InvShiftRows 变换、InvSubBytes 变换、AddRoundKey 变换及 InvMixColumns 变换得到的结果。在第九周期 (T26 至 T27)，修改轮回函数模块输出通过执行 InvShiftRows 变换、InvSubBytes 变换及 AddRoundKey 变换得到的结果。

[0407] 修改轮回函数模块 235 通过按上述方式控制选择信号 171、170 及 175 可执行图 36 所示的解密。

[0408] 另一方面，密钥扩展单元 232 在密钥准备时段后输出作为轮回密钥 A162 的 wkey9′ 和作为轮回密钥 B163 的 wkey10。为此，wkey10 和 wkey9′ 在解密开始 (T17) 时被供给到修改轮回函数模块 235。基于加密 / 解密开始信号 158 检测到解密开始时 (T17)，密钥扩展单元 232 使用在轮回密钥 A 寄存器中保持的 wkey9′ 产生 wkey8′，并且把 wkey8′ 保持在轮回密钥 A 寄存器中。因此，wkey8′ 在 T18 供给到修改轮回函数模块 235。轮回密钥以相同方式供给直到时序 T26。当 wkey0 被保持在轮回密钥 A 寄存器中，并且轮回密钥供给在时序 T26 结束时，密钥扩展单元 232 使用在轮回密钥 B 寄存器中保持的 wkey10 产生 wkey9′，并且把 wkey9′ 保持在轮回密钥 A 寄存器中以准备下次解密开始 (T27)。

[0409] 当密钥扩展单元 232 按上述方式操作时，修改轮回函数模块 235 可如图 36 所示在每个周期使用轮回密钥。

[0410] 根据第五实施例的在解密时段期间的操作按上述方式进行。第二块的解密操作以与对于第一块相同的方式进行。从那时起，解密操作被重复地进行与块的预定数量一样多次。在图 41A 和 41B 的时序图中，第二块的解密在距离第一块解密结束的最短间隔处开始。AES 芯通过以这样一种时序执行所有块的解密可呈现其最大性能。然而，解密间隔基本上可设置到任意长度。

[0411] 当预定数量的块的解密已经完全结束，并且下个作业要使用诸如密码密钥之类的不同参数执行时，处理再次从参数设置开始。

[0412] 第五实施例能以上述方式实施。在第五实施例中，在一个周期中必须执行每个子块变换的信号处理时间总和的最大值稍微增大。然而，这在多数情况下几乎不成问题，因为在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值常常以足够的裕量设置为一个周期时间。为此，在多数情况下，AES 加密所要求的时钟周期的数量可被减小一个。这把 AES 处理速度提高约 10％。

[0413] 上述第五实施例仅是本发明的例子，并且本发明的效果不限于上述实施例的那些。

[0414] <第六实施例>

[0415] 在第六实施例中，使用 FIPS197 描述的等效逆密码执行解密。

[0416] 图 42 是表示根据第六实施例在时钟周期中执行加密和解密过程内容的图。

[0417] 参照图 42，周期计数指示在 AES 处理开始是“0”的时钟周期计数。

[0418] 在第六实施例中，第一 AddRoundKey 变换、SubBytes/InvSubBytes 变换、ShiftRows/InvShiftRows 变换、MixColumns/InvMixColumns 变换及第二 AddRoundKey 变换在第 0 周期中使用两个轮回密钥被执行。在第一至第八周期中，SubBytes/InvSubBytes 变换、ShiftRows/InvShiftRows 变换、MixColumns/InvMixColumns 变换及 AddRoundKey 变换被执行。在第九周期中，SubBytes/InvSubBytes 变换、ShiftRows/InvShiftRows 变换及 AddRoundKey 变换被执行。SubBytes/InvSubBytes 变换表示在加密中执行 SubBytes 变换并且在解密中执行 InvSubBytes 变换。ShiftRows/InvShiftRows 变换表示在加密中执行 ShiftRows 变换并且在解密中执行 InvShiftRows 变换。MixColumns/InvMixColumns 变换表示在加密中执行 MixColumns 变换并且在解密中执行 InvMixColumns 变换。

[0419] 这个实施例的加密中使用的轮回密钥是在第 0 周期中的 wkey0 和 wkey1、第一周期中的 wkey2、... 及在第九周期中的 wkey10。解密中使用的轮回密钥是在第 0 周期中的 wkey10 和 wkey9′、在第一周期中的 wkey8′、... 及在第九周期中的 wkey0。

[0420] 在第六实施例中，与在现有技术中相同的处理被总体上执行。然而，这个实施例中，AES 加密和解密可以少一个的时钟周期被执行。

[0421] 接着将描述根据这个实施例在每个时钟周期时段中用于每个子块变换的加密处理时间总和。图 43 是表示在第六实施例中在时钟周期中用于执行每个子块变换的信号处理时间总和与现有技术的总和之间的比较图。纵坐标代表时间。条带越长，处理时间越长。为了实现第六实施例，在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值必须小于一个时钟周期时间。如图 43 所示，每个子块变换的处理时间在 SubBytes 变换中最长，并且按 MixColumns 变换、AddRoundKey 变换及 ShiftRows 变换的顺序缩短。

[0422] 这个实施例中，在执行 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换、MixColumns 变换及 AddRoundKey 变换的第 0 周期中用于每个子块变换的信号处理时间总和，比在执行 AddRoundKey 变换、SubBytes 变换、ShiftRows 变换及 MixColumns 变换的第一至第八周期中用于每个子块变换的信号处理时间总和、或在执行 AddRoundKey 变换、SubBytes 变换及 ShiftRows 变换的第九周期中用于每个子块变换的信号处理时间总和更长。图 43 也适用于解密，并且以上所描述的同样应用于解密。因此，第六实施例用于每个子块变换的信号处理时间总和的最大值比现有技术的最大值大一个对应于 AddRoundKey 变换处理时间的量。然而，一个 AddRoundKey 变换处理时间比一个周期中用于每个子块变换的信号处理时间总和短得多。在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值常常以足够的裕量设置为一个周期时间。为此，如果现有技术在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值比一个周期时间短，则也假定这个实施例在多数情况下是可实施的。

[0423] 将概括第六实施例的上述特性特征。

[0424] 在一般常规实施方法中，由标准定义的轮回函数被认为是在处理中的断点，并且加密和解密被分配给时钟周期。为此，在第 10 和第 0 周期中用于每个子块变换的信号处理

时间总和比在第一至第九周期的每一个周期中用于每个子块变换的信号处理时间总和短。就是说，在每个周期中用于执行每个子块变换的信号处理时间总和变化。

[0425] 另一方面，在第六实施例中，在一些时钟周期中的信号处理被增加，从而在每个时钟周期时段中用于每个子块变换的信号处理时间总和之间的差减小。

[0426] 在第六实施例中，在一个周期中用于每个子块变换的信号处理时间总和的最大值稍微增大。为此，第六实施例在现有技术可实施的条件下不一定是可实施的。然而，这在多数情况下几乎不成问题，因为在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值常常以足够的裕量设置为一个周期时间。在多数情况下，AES 加密或解密所要求的时钟周期的数量可被减小一个。这把 AES 处理速度提高约 10％。

[0427] 接着将描述用来实施 AES 加密和解密的 AES 芯的电路设置。

[0428] 图 44 是根据这个实施例的 AES 芯的方块图。参照图 44，AES 芯 241 执行 AES 处理。密钥扩展单元 242 从密码密钥产生对于 AES 加密和解密必需的轮回密钥，并且输出轮回密钥。加密 / 解密单元 243 使用从密钥扩展单元 242 供给的轮回密钥执行 128- 位明文数据的加密或 128- 位密文数据的解密。控制单元 244 从在 AES 芯 241 外部的单元接收信号，并且产生控制密钥扩展单元 242 和加密 / 解密单元 243 的操作的信号、以及向在 AES 芯 241 外部的单元通知操作完成的信号。

[0429] 将省略图 44 中的构成元件和信号线的描述，这些构成元件和信号线与在第一和第二实施例中描述的那些相同。

[0430] 接着将描述加密 / 解密单元 243。图 45 是加密 / 解密单元 243 的方块图。参照图 45，修改轮回函数模块 245 在选择信号 170 和 175 及加密 / 解密选择信号 153 的控制下使用轮回密钥 A162 和轮回密钥 B163 执行一个周期的加密或解密。

[0431] 在以上设置中，当选择信号 171 被取消时，加密 / 解密单元 243 的选择器 109 选择输入信号 150。当选择信号 171 被声明时，选择器 109 选择来自数据保持单元 108 的输出。

[0432] 将省略图 45 中的构成元件和信号线的描述，这些构成元件和信号线与在第一和第二实施例中描述的那些相同。

[0433] 接着参照图 46 的方块图将描述修改轮回函数模块 245。参照图 46，输入信号 165 和加密 / 解密选择信号 153 输入到 MixColumns/InvMixColumns 变换模块 224。来自 MixColumns/InvMixColumns 变换模块 224 的输出、输入信号 165 及选择信号 175 输入到选择器 137。来自选择器 137 的输出和轮回密钥 A162 输入到 AddRoundKey 变换模块 110。来自 AddRoundKey 变换模块 110 的输出输入到 SubBytes/InvSubBytes 变换模块 222。来自 SubBytes/InvSubBytes 变换模块 222 的输出输入到 ShiftRows/InvShiftRows 变换模块 223。来自 ShiftRows/InvShiftRows 变换模块 223 的输出和轮回密钥 B163 输入到 AddRoundKey 变换模块 114。来自 ShiftRows/InvShiftRows 变换模块 223 的输出、来自 AddRoundKey 变换模块 114 的输出及选择信号 170 输入到选择器 115。选择器 115 的输出连接到来自修改轮回函数模块 245 的输出信号 168 上。将省略图 46 中的构成元件和信号线的描述，这些构成元件和信号线与在第一、第四及第五实施例中描述的那些相同。

[0434] 在以上设置中，当选择信号 175 被取消时，选择器 137 选择并输出来自 MixColumns/InvMixColumns 变换模块 224 的输出。当选择信号 175 被声明时，选择器 137 选择并输出输入信号 165。当选择信号 170 被取消时，选择器 115 选择并输出来自 ShiftRows/

InvShiftRows 变换模块 223 的输出。当选择信号 170 被声明时，选择器 115 选择并输出来自 AddRoundKey 变换模块 114 的输出。

[0435] 接着参照图 27A 和 27B 的时序图将描述以上设置中的加密操作。在图 27A 左端沿纵坐标的三位数指示信号线，并且与在图 44 至 46 中使用的信号线的附图标记具有一一对应性。

[0436] 在图 27A 和 27B 的时序图中表示的加密操作大致划分成四部分。第一部分是用来设置诸如密码密钥之类的各种参数的参数设置时段 (T01 至 T06)。第二部分是用来产生 wkey0 并把它保持在寄存器中的密钥准备时段 (T06 至 T17)。第三部分是第一块加密时段 (T17 至 T27)。第四部分是第二块加密时段 (从 T27 起)。

[0437] 参数设置时段的作用、开始条件及结束条件与在第三实施例中相同。密钥准备时段是从 T06 至 T17。开始条件、结束条件及每个电路的操作也与在第三实施例中相同，并且将不重复其描述。

[0438] 控制单元 244 在加密结束时声明选择信号 175，并且在加密的第一周期取消它 (T18 或 T28)。控制单元 244 还在加密的最后周期 (T16) 声明选择信号 170，并且在加密结束 (T17) 时取消它。控制单元 244 还在加密的第一周期声明选择信号 171，并且在加密结束时取消它。

[0439] 如有关电路设置描述的那样，当选择信号 171 被取消时，选择器 109 选择输入信号 150。当选择信号 171 被声明时，选择器 109 选择来自数据保持单元 108 的输出。当选择信号 170 被取消时，选择器 115 选择并输出来自 ShiftRows/InvShiftRows 变换模块 223 的输出。当选择信号 170 被声明时，选择器 115 选择并输出来自 AddRoundKey 变换模块 114 的输出。当选择信号 175 被取消时，选择器 137 选择并输出来自 MixColumns/InvMixColumns 变换模块 224 的输出。当选择信号 175 被声明时，选择器 137 选择并输出输入信号 165。当加密 / 解密选择信号 153 被取消时，SubBytes/InvSubBytes 变换模块 222、ShiftRows/InvShiftRows 变换模块 223 及 MixColumns/InvMixColumns 变换模块 224 分别执行 SubBytes 变换、ShiftRows 变换及 MixColumns 变换。当加密 / 解密选择信号 153 被声明时，它们分别执行 InvSubBytes 变换、InvShiftRows 变换及 InvMixColumns 变换。

[0440] 因此，在第 0 周期 (T17 至 T18)，修改轮回函数模块 245 对输入信号 150 执行 AddRoundKey 变换、SubBytes 变换及 ShiftRows 变换。从第一周期起，修改轮回函数模块输出通过对紧邻前一周期的结果执行 SubBytes 变换、ShiftRows 变换、MixColumns 变换及 AddRoundKey 变换得到的结果。在第九周期 (T26 至 T27)，修改轮回函数模块输出通过执行 MixColumns 变换、AddRoundKey 变换、SubBytes 变换、ShiftRows 变换及 AddRoundKey 变换得到的结果。

[0441] 修改轮回函数模块 245 通过按上述方式控制选择信号 171、170 及 175 可执行图 42 所示的加密。

[0442] 另一方面，密钥扩展单元 242 在密钥准备时段后输出作为轮回密钥 A162 的 wkey0 和作为轮回密钥 B163 的 wkey10。为此，wkey0 在加密开始 (T17) 时被供给到修改轮回函数模块 245。基于加密 / 解密开始信号 158 检测到加密开始时 (T17)，密钥扩展单元 242 使用在轮回密钥 A 寄存器中保持的 wkey0 产生 wkey1，并且把 wkey1 保持在轮回密钥 A 寄存器中。因此，wkey1 在时序 T18 供给到修改轮回函数模块 245。轮回密钥以相同方式供给直到

时序 T26。在时序 T26，用作轮回密钥 B163 的 wkey10 也被供给。当 wkey10 被保持在轮回密钥 A 寄存器中，并且轮回密钥供给在时序 T26 结束时，密钥扩展单元 242 把从外部连续地供给的 wkey0 作为密码密钥 152 保持在轮回密钥 A 寄存器中以准备下次加密开始 (T27)。

[0443] 当密钥扩展单元 242 按上述方式操作时，修改轮回函数模块 245 可如图 42 所示在每个周期使用轮回密钥。

[0444] 根据这个实施例在加密时段期间的操作按上述方式进行。第二块的加密操作以与对于第一块相同的方式进行。从那时起，加密操作被重复地进行与块的预定数量一样多次。在图 27A 和 27B 的时序图中，第二块的加密在距离第一块加密结束的最短间隔处开始。AES 芯通过以这样一种时序执行所有块的加密可呈现其最大性能。然而，加密间隔基本上可设置到任意长度。

[0445] 当预定数量的块的加密已经完全结束，并且下个作业要使用诸如密码密钥之类的不同参数执行时，处理再次从参数设置开始。

[0446] 接着将描述第六实施例的解密操作。图 47A 和 47B 是根据第六

[0447] 实施例的解密时序图。参照图 47A 和 47B，横坐标代表时间。时序名称 T01、T02、...、T33 被赋予时钟脉冲的前沿。在图 47A 左端沿纵坐标的三位数指示信号线，并且与在图 44 至 46 中使用的信号线的附图标记具有一一对应性。

[0448] 在图 47A 和 47B 的时序图中表示的解密操作大致划分成四部分。第一部分是用来设置诸如密码密钥之类的各种参数的参数设置时段 (T01 至 T06)。第二部分是用来产生 wkey0 并把它保持在寄存器中的密钥准备时段 (T06 至 T17)。第三部分是第一块解密时段 (T17 至 T27)。第四部分是第二块解密时段 (从 T27 起)。

[0449] 参数设置时段的作用、开始条件及结束条件与在这个实施例的加密中相同。然而，在解密中，声明加密 / 解密选择信号 153。密钥准备时段是从 T06 至 T17，并且开始条件和结束条件与在这个实施例的加密相同。每个电路的操作也与在这个实施例的加密中几乎相同。然而，在时序 T16，wkey10 被输出作为轮回密钥 B163。在密钥准备时段结束 (T17) 时，控制单元 244 声明选择信号 175。

[0450] 第一块解密时段是从 T17 到 T27，并且开始条件和结束条件与在这个实施例的加密相同。每个电路的操作也与以上描述几乎相同。

[0451] 控制单元 244 在解密的最后周期 (T26) 声明选择信号 170，并且在第一周期解密 (T18 或 T28) 取消它。控制单元 244 还在解密结束 (T17) 时声明选择信号 175，并且在解密结束 (T17) 时取消它。控制单元 244 还在解密的第一周期声明选择信号 171，并且在解密结束时取消它。

[0452] 如有关电路设置描述的那样，当选择信号 171 被取消时，选择器 109 选择输入信号 150。当选择信号 171 被声明时，选择器 109 选择来自数据保持单元 108 的输出。当选择信号 175 被取消时，选择器 137 选择并输出来自 MixColumns/InvMixColumns 变换模块 224 的输出。当选择信号 175 被声明时，选择器 137 选择并输出输入信号 165。当选择信号 170 被取消时，选择器 115 选择并输出来自 ShiftRows/InvShiftRows 变换模块 223 的输出。当选择信号 170 被声明时，选择器 115 选择并输出来自 AddRoundKey 变换模块 114 的输出。

[0453] 因此，在第 0 周期 (T17 至 T18)，修改轮回函数模块 245 对输入信号 150 执行 AddRoundKey 变换、InvShiftRows 变换及 InvSubBytes 变换。从第一周期起，修改轮回

函数模块输出通过对紧邻前一周期的结果执行 AddRoundKey 变换、InvMixColumns 变换、InvShiftRows 变换及 InvSubBytes 变换得到的结果。在第九周期 (T26 至 T27)，修改轮回函数模块输出通过执行 AddRoundKey 变换、InvMixColumns 变换、InvShiftRows 变换、InvSubBytes 变换及 AddRoundKey 变换得到的结果。

[0454] 修改轮回函数模块 245 通过按上述方式控制选择信号 171、170 及 175 可执行图 42 所示的解密。

[0455] 另一方面，密钥扩展单元 242 在密钥准备时段后输出作为轮回密钥 A162 的 wkey10 和作为轮回密钥 B163 的 wkey0。为此，wkey10 在解密开始 (T17) 时被供给到修改轮回函数模块 245。基于加密 / 解密开始信号 158 检测到解密开始时 (T17)，密钥扩展单元 242 使用在轮回密钥 A 寄存器中保持的 wkey10′ 产生 wkey9′，并且把 wkey9′ 保持在轮回密钥 A 寄存器中。因此，wkey9′ 在时序 T18 供给到修改轮回函数模块 245。以相同方式，wkey8′ 在 T19 供给，wkey7′ 在 T20 处供给，...，及 wkey1′ 在 T26 供给。注意，在最后周期的处理中必需的 wkey0 被连续地供给作为轮回密钥 B163。

[0456] 在 T26 当轮回密钥供给结束时，密钥扩展单元 242 使用在密钥扩展单元 242 的内部寄存器中保持的 wkey10 产生 wkey9′，并且在下个周期 (T27) 把 wkey9′ 保持在轮回密钥 A 寄存器中以准备下次解密开始。

[0457] 根据第六实施例的在解密时段期间的操作按上述方式进行。第二块的解密操作以与对于第一块相同的方式进行。从那时起，解密操作被重复地进行与块的预定数量一样多次。在图 47A 和 47B 的时序图中，第二块的解密在距离第一块解密结束的最短间隔处开始。AES 芯通过以这样一种时序执行所有块的解密可呈现其最大性能。然而，解密间隔基本上可设置到任意长度。

[0458] 当预定数量的块的解密已经完全结束，并且下个作业要使用诸如密码密钥之类的不同参数执行时，处理再次从参数设置开始。

[0459] 第六实施例能以上述方式实施。在第六实施例中，在一个周期中用于必须执行每个子块变换的信号处理时间总和的最大值稍微增大。然而，这在多数情况下几乎不成问题，因为在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值常常以足够的裕量设置为一个周期时间。为此，在多数情况下，AES 加密所要求的时钟周期的数量可被减小一个。这把 AES 处理速度提高约 10％。

[0460] 上述第六实施例仅是本发明的例子，并且本发明的效果不限于上述实施例的那些。

[0461] ＜第七实施例＞

[0462] 在第一至第六实施例中，如果在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值等于或小于一个周期时间的 1/2，则通过实现需要两个时钟周期的过程在一个时钟周期中执行，可以增大处理速度。在第七实施例中，通过举例说明第一实施例，来解释实施加速方法的例子。

[0463] 根据第七实施例与加密 / 解密电路的加密相关联的设置包括第一修改轮回函数模块、第二修改轮回函数模块及数据保持单元。第一修改轮回函数模块包括第一 AddRoundKey 变换模块、第一 ShiftRows 变换模块、第一 SubBytes 变换模块、第一 MixColumns 变换模块及第二 AddRoundKey 变换模块。第二修改轮回函数模块包括第三 AddRoundKey 变换模块、

第二 ShiftRows 变换模块、第二 SubBytes 变换模块及第二 MixColumns 变换模块。

[0464] 根据第七实施例与加密 / 解密电路的解密相关联的设置包括第一修改轮回函数模块、第二修改轮回函数模块及数据保持单元。第一修改轮回函数模块包括第一 AddRoundKey 变换模块、第一 InvShiftRows 变换模块、第一 InvSubBytes 变换模块、第一 InvMixColumns 变换模块及第二 AddRoundKey 变换模块。第二修改轮回函数模块包括第三 AddRoundKey 变换模块、第二 InvShiftRows 变换模块、第二 InvSubBytes 变换模块及第二 InvMixColumns 变换模块。

[0465] 加密和解密的设置由如下描述而清楚。

[0466] 图 48 表示在第七实施例中在时钟周期中执行的加密过程内容与现有技术的那些之间的比较。

[0467] 参照图 48，周期计数指示在 AES 处理开始是“0”的时钟周期计数。轮回密钥 wkeyi 是 FIPS197 描述的轮回密钥 (i 是轮回数)。

[0468] 在第七实施例中，第一 AddRoundKey 变换、第一 SubBytes 变换、第一 ShiftRows 变换、第一 MixColumns 变换、第二 AddRoundKey 变换、第二 SubBytes 变换、第二 ShiftRows 变换及第二 MixColumns 变换在第 0 至第三周期中被执行。在第四周期，第一 AddRoundKey 变换、第一 SubBytes 变换、第一 ShiftRows 变换、第一 MixColumns 变换、第二 AddRoundKey 变换、第二 ShiftRows 变换、第二 SubBytes 变换及第三 AddRoundKey 变换被执行。

[0469] 至于轮回密钥，wkey0 和 wkey1 被用在第 0 周期，wkey2 和 wkey3 被用在第一周期，...，wkey8、wkey9 及 wkey10 被用在第四周期。

[0470] 在第七实施例中，与在现有技术中相同的处理被总体上执行。然而，在第七实施例中，AES 加密可以少一个的时钟周期被执行。接着将描述根据第七实施例在每个时钟周期时段中用于每个子块变换的加密处理时间总和。图 49 是表示现有技术在每个时钟周期时段中用于每个子块变换的加密处理时间总和与第七实施例的总和之间的比较图。纵坐标代表时间。条带越长，处理时间越长。为了实施第七实施例，在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值必须小于一个时钟周期时间。如图 49 所示，每个子块变换的处理时间在 SubBytes 变换中最长，并且按 MixColumns 变换、AddRoundKey 变换及 ShiftRows 变换的顺序缩短。

[0471] 在第七实施例中，在执行第一 AddRoundKey 变换、第一 SubBytes 变换、第一 ShiftRows 变换、第一 MixColumns 变换、第二 AddRoundKey 变换、第二 SubBytes 变换、第二 ShiftRows 变换及第二 MixColumns 变换的第 0 至第三周期的每一个周期中用于每个子块变换的信号处理时间总和比在执行第一 AddRoundKey 变换、第一 SubBytes 变换、第一 ShiftRows 变换、第一 MixColumns 变换、第二 AddRoundKey 变换、第二 ShiftRows 变换、第二 SubBytes 变换及第三 AddRoundKey 变换的第四周期中用于每个子块变换的信号处理时间总和更长。因此，在第七实施例中在一个周期中用于执行每个子块变换的信号处理时间总和的最大值与现有技术的最大值相等。如果在一个周期中用于执行每个子块变换的信号处理时间总和的最大值比在现有技术中的一个周期时间短，则第七实施例也可实现。

[0472] 本发明也适用于 AES 解密。

[0473] 图 50 表示在第七实施例中在时钟周期中执行解密过程内容与现有技术的那些之间的比较。参照图 50，周期计数指示在 AES 处理开始是“0”的时钟周期计数。

[0474] 在第七实施例中，第一 AddRoundKey 变换、第一 InvShiftRows 变换、第一 InvSubBytes 变换、第二 AddRoundKey 变换、第一 InvMixColumns 变换、第二 InvShiftRows 变换、第二 InvSubBytes 变换及第三 AddRoundKey 变换在第 0 周期被执行。第一 InvMixColumns 变换、第一 InvShiftRows 变换、第一 InvSubBytes 变换、第一 AddRoundKey 变换、第二 InvMixColumns 变换、第二 InvShiftRows 变换、第二 InvSubBytes 变换及第二 AddRoundKey 变换在第一至第四周期被执行。至于轮回密钥，wkey10、wkey9 及 wkey8 被用在第 0 周期，wkey7 和 wkey6 被用在第一周期，wkey5 和 wkey4 被用在第二周期，...，及 wkey1 和 wkey0 被用在第四周期。

[0475] 在第七实施例中，与在现有技术中相同的处理被总体上执行。然而，在第七实施例中，AES 解密可以少一个的时钟周期被执行。

[0476] 接着将描述根据第七实施例在每个时钟周期时段中用于每个子块变换的解密处理时间总和。图 51 是表示第七实施例中每个时钟周期时段中用于每个子块变换的解密处理时间总和与现有技术的总和之间的比较图。纵坐标代表时间。条带越长，处理时间越长。为了实施第七实施例，在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值必须小于一个时钟周期时间。如图 51 所示，每个子块变换的处理时间在 InvSubBytes 变换中最长，并且按 InvMixColumns 变换、AddRoundKey 变换及 InvShiftRows 变换的顺序缩短。

[0477] 在第七实施例中，在执行第一 InvMixColumns 变换、第一 InvShiftRows 变换、第一 InvSubBytes 变换、第一 AddRoundKey 变换、第二 InvMixColumns 变换、第二 InvShiftRows 变换、第二 InvSubBytes 变换及第二 AddRoundKey 变换的第一至第四周期的每一个周期用于每个子块变换的信号处理时间总和比在执行第一 AddRoundKey 变换、第一 InvShiftRows 变换、第一 InvSubBytes 变换、第二 AddRoundKey 变换、第一 InvMixColumns 变换、第二 InvShiftRows 变换、第二 InvSubBytes 变换及第三 AddRoundKey 变换的第 0 周期用于每个子块变换的信号处理时间总和更长。因此，在第七实施例中在一个周期中用于执行每个子块变换的信号处理时间总和的最大值与现有技术的最大值相等。如果在一个周期中用于执行的每个子块变换的信号处理时间总和的最大值比在现有技术中的一个周期时间短，则这个实施例也可实现。

[0478] 将概括这个实施例的上述特性特征。

[0479] 在一般常规实施方法中，由标准定义的轮回函数被认为是在处理中的断点，并且加密和解密被分配给时钟周期。为此，在每个周期中用于每个子块变换的信号处理时间总和变化。另外，第一实施例描述了 11 个周期，即奇数个周期对于处理是必要的。如果两个周期的过程在一个周期中被执行，则一个周期的过程保持为零头。因此，处理要求六个周期。

[0480] 另一方面，在本发明中，AES 处理需要 10 个周期。即使当两个周期的过程在一个周期中被执行时，也没有零头剩下。当两个周期的过程在一个周期中被执行时，如第七实施例那样，一个周期的减少把 AES 处理速度提高约 20％。

[0481] 接着将描述用来实施 AES 加密和解密的 AES 芯的电路设置。

[0482] 图 52 是根据第七实施例的 AES 芯的方块图。

[0483] 参照图 52，AES 芯 401 执行 AES 处理。密钥扩展单元 402 从密码密钥产生对于 AES 加密和解密必需的轮回密钥，并且输出轮回密钥。加密 / 解密单元 403 使用从密钥扩展单

元 402 供给的轮回密钥执行 128- 位明文数据的加密或 128- 位密文数据的解密。控制单元 404 从在 AES 芯 401 外部的单元接收信号，并且产生控制密钥扩展单元 402 和加密 / 解密单元 403 的操作的信号、向在 AES 芯 401 外部的单元通知操作完成的信号。

[0484] 参照图 52，轮回密钥 A1462 是由密钥扩展单元 402 产生的轮回密钥之一。轮回密钥 A2463 是由密钥扩展单元 402 产生的轮回密钥之一。

[0485] 与第一实施例相同的附图标记在图 52 指示相同的构成元件和信号线，并将不重复其描述。

[0486] 在以上设置中，轮回密钥 A1462 从密钥扩展单元 402 输入到加密 / 解密单元 403，并且轮回密钥 A2463 从密钥扩展单元 402 输入到加密 / 解密单元 403。

[0487] 接着将描述加密 / 解密单元 403。图 53 是加密 / 解密单元 403 的方块图。参照图 53，修改轮回函数模块 405 使用轮回密钥 A1462 执行加密。修改轮回函数模块 407 在选择信号 170 的控制下使用轮回密钥 A2463 和轮回密钥 B163 执行加密。修改轮回函数模块 406 在选择信号 170 的控制下使用轮回密钥 A1462 和轮回密钥 B163 执行解密。修改轮回函数模块 408 使用轮回密钥 A2463 执行解密。

[0488] 参照图 53，修改轮回函数模块 407 接收输入信号 475。修改轮回函数模块 408 接收输入信号 476。与第一实施例相同的附图标记在图 53 中指示相同的构成元件和信号线，并将不重复其描述。

[0489] 图 54A 是修改轮回函数模块 405 的方块图。图 54B 是修改轮回函数模块 407 的方块图。

[0490] 接着参照图 54A 将描述修改轮回函数模块 405。参照图 54A，AddRoundKey 变换模块 110 接收输入信号 165 和轮回密钥 A1462，并且执行 AddRoundKey 变换。SubBytes 变换模块 111 接收来自 AddRoundKey 变换模块 110 的输出，并且执行 SubBytes 变换。ShiftRows 变换模块 112 接收来自 SubBytes 变换模块 111 的输出，并且执行 ShiftRows 变换。MixColumns 变换模块 113 接收来自 ShiftRows 变换模块 112 的输出，并且执行 MixColumns 变换。MixColumns 变换模块 113 的输出信号是修改轮回函数模块 405 的输出。

[0491] 接着参照图 54B 将描述修改轮回函数模块 407。参照图 54B，AddRoundKey 变换模块 110 接收输入信号 475 和轮回密钥 A2463，并且执行 AddRoundKey 变换。SubBytes 变换模块 111 接收来自 AddRoundKey 变换模块 110 的输出，并且执行 SubBytes 变换。ShiftRows 变换模块 112 接收来自 SubBytes 变换模块 111 的输出，并且执行 ShiftRows 变换。MixColumns 变换模块 113 接收来自 ShiftRows 变换模块 112 的输出，并且执行 MixColumns 变换。AddRoundKey 变换模块 114 接收来自 ShiftRows 变换模块 112 的输出和轮回密钥 B163，并且执行 AddRoundKey 变换。选择器 115 按照选择信号 170 选择并输出来自 MixColumns 变换模块 113 的输出和来自 AddRoundKey 变换模块 114 的输出之一。选择器 115 的输出信号是修改轮回函数模块 407 的输出。

[0492] 注意，上述变换名称与 FIPS197 描述的 AES 处理的子块变换的那些名称相同。

[0493] 在以上设置中，当选择信号 170 被取消时，选择器 115 选择并输出来自 MixColumns 变换模块 113 的输出。当选择信号 170 被声明时，选择器 115 选择并输出来自 AddRoundKey 变换模块 114 的输出。

[0494] 接着参照图 55A 和 55B 将描述修改轮回函数模块 406 和 408。图 55A 是修改轮回

函数模块 406 的方块图。

[0495] 参照图 55A，InvMixColumns 变换模块 116 接收输入信号 165，并且执行 InvMixColumns 变换。AddRoundKey 变换模块 121 接收输入信号 165 和轮回密钥 B163，并且执行 AddRoundKey 变换。选择器 118 按照选择信号 170 选择并输出来自 InvMixColumns 变换模块 116 的输出和来自 AddRoundKey 变换模块 121 的输出之一。InvShiftRows 变换模块 119 接收来自选择器 118 的输出，并且执行 InvShiftRows 变换。InvSubBytes 变换模块 120 接收来自 InvShiftRows 变换模块 119 的输出，并且执行 InvSubBytes 变换。AddRoundKey 变换模块 117 接收来自 InvSubBytes 变换模块 120 的输出和轮回密钥 A1462，并且执行 AddRoundKey 变换。AddRoundKey 变换模块 117 的输出是修改轮回函数模块 406 的输出。

[0496] 注意，上述变换名称与 FIPS197 描述的 AES 处理的子块变换的那些名称相同。

[0497] 在以上设置中，当选择信号 170 被取消时，选择器 118 选择并输出来自 InvMixColumns 变换模块 116 的输出。当选择信号 170 被声明时，选择器 118 选择并输出来自 AddRoundKey 变换模块 121 的输出。

[0498] 接着参照图 55B 的方块图将描述修改轮回函数模块 408。

[0499] 参照图 55B，InvMixColumns 变换模块 116 接收输入信号 476，并且执行 InvMixColumns 变换。InvShiftRows 变换模块 119 接收来自 InvMixColumns 变换模块 116 的输出，并且执行 InvShiftRows 变换。InvSubBytes 变换模块 120 接收来自 InvShiftRows 变换模块 119 的输出，并且执行 InvSubBytes 变换。AddRoundKey 变换模块 117 接收来自 InvSubBytes 变换模块 120 的输出和轮回密钥 A2463，并且执行 AddRoundKey 变换。AddRoundKey 变换模块 117 的输出是修改轮回函数模块 408 的输出。

[0500] 注意，上述变换名称与 FIPS197 描述的 AES 处理的子块变换的那些名称相同。

[0501] 接着参照图 56A 和 56B 的时序图将描述以上设置中的加密操作。

[0502] 参照图 56A 和 56B，横坐标代表时间。时序名称 T01、T02、...、T24 被赋予时钟脉冲的前沿。在图 56A 左端沿纵坐标的三位数指示信号线，并且与在图 52 至 55B 中使用的信号线的附图标记具有一一对应性。

[0503] 在图 56A 和 56B 的时序图中表示的加密操作大致划分成四部分。第一部分是用来设置诸如密码密钥之类的各种参数的参数设置时段 (T01 至 .T06)。第二部分是用来产生 wkey0 并把它保持在寄存器中的密钥准备时段 (T06 至 T12)。第三部分是第一块加密时段 (T12 至 T17)。第四部分是第二块加密时段 (T17 至 T22)。

[0504] 在参数设置时，除了密码密钥 152 和加密 / 解密选择信号 153 以外，按需要设置用于加密 / 解密所需的各种参数，如密钥长度和加密模式。参数设置时段是紧在复位之后具有任意长度的时段。当从 AES 芯 401 外的单元声明密钥准备开始信号 155 时 (T06)，参数设置时段结束。

[0505] 参数设置时段的结束同时，下个密钥准备时段开始。在密钥准备时段中，密钥扩展单元事先产生轮回密钥。密钥准备时段是从密钥准备开始信号 155 的声明 (T06) 到 6 个周期后的时序 (T12) 的时段，在该时序 (T12) 时产生最后轮回密钥 (wkey10)。

[0506] 接着将描述在密钥准备时段期间每个电路的操作。在密钥准备时段中密钥扩展单元 402 把 wkey0 已经用作密码密钥 152 产生 wkey1。与密钥准备开始信号 155 的声明同时，wkey1 被保持在轮回密钥 A2463 的寄存器中并且输出。按照密钥准备开始信号 155 的

声明，控制单元 404 从 0 依次向上计数计数器信号 161。在 T07，密钥扩展单元 402 使用作为轮回密钥 A2463 保持的 wkey1 进行密钥扩展以产生 wkey2 和 wkey3，并且输出它们分别作为轮回密钥 A1462 和轮回密钥 A2463。在下个周期 (T08)，密钥扩展单元使用作为轮回密钥 A2463 输出的 wkey3 产生 wkey4 和 wkey5，并且输出它们分别作为轮回密钥 A1462 和轮回密钥 A2463。轮回密钥以相同方式产生，从而在时序 T09 输出 wkey6 和 wkey7，并且在时序 T10 输出 wkey8 和 wkey9，分别作为轮回密钥 A1462 和轮回密钥 A2463。在时序 T11，密钥扩展单元 402 使用作为轮回密钥 A2463 输出的 wkey9 产生 wkey10，并且输出 wkey10 作为轮回密钥 B163。从那时，wkey10 被连续地输出作为轮回密钥 B163，直到再次执行密钥准备。

[0507] 在密钥准备时段的结束 (T12) 时，密钥扩展单元 402 使用作为密码密钥 152 供给的 wkey0 产生 wkey1，并且输出初始轮回密钥 (wkey0 和 wkey1) 以在加密 / 解密中分别用作轮回密钥 A1462 和轮回密钥 A2463。轮回密钥 A1462 和轮回密钥 A2463 的值被保持，直到加密 / 解密开始信号 158 的声明。控制单元 404 停止向上计数计数器信号 161，并且把计数器清除到 0。

[0508] 在密钥准备时段结束的附近，更明确地说，在密钥准备开始后的第五周期 (T11)，当预计到密钥准备将在下个周期 (T12) 中结束并启动加密时，控制单元 404 声明控制信号 157。

[0509] 在 T12 检测到控制信号 157 的声明时，设置在 AES 芯 401 外的输入信号供给单元把明文数据 P0 供给到 AES 芯 401 作为输入信号 150。加密 / 解密开始信号 158 被声明，以开始输入信号 150 的加密 (T12)。在时序图中，加密 / 解密开始信号 158 在最短周期中被声明。然而，时序在 AES 芯 401 外自由确定。

[0510] 在加密时段，输入信号 150 被加密。加密时段是从加密 / 解密开始信号 158 的声明 (T12) 到五个周期后的时序 (T17) 的时段。

[0511] 在检测到加密 / 解密开始信号 158 的声明时，控制单元 404 在下个周期 (T13) 取消控制信号 157、有效信号 159 及输出保持控制信号 160。同时，控制单元 404 开始向上计数计数器信号 161。

[0512] 密钥扩展单元 402 如在密钥准备时段那样产生轮回密钥，并且作为轮回密钥 A1462 在时序 T12 输出 wkey0、在时序 T13 输出 wkey2、... 及在时序 T16 输出 wkey8。密钥扩展单元 402 在时序 T12 输出 wkey1、在时序 T13 输出 wkey3、... 及在时序 T16 输出 wkey9，作为轮回密钥 A2463。

[0513] 从 T12 至 T13，选择信号 171 被取消。因此，修改轮回函数模块 405 使用 wkey0 输出作为轮回密钥 A1 对输入信号 150 执行子块变换。从 T13 至 T17，选择信号 171 被声明。因此，修改轮回函数模块 405 从 T13 到 T14 使用 wkey2、从 T14 到 T15 使用 wkey4、... 及从 T15 到 T16 使用 wkey6 对来自数据保持单元 108 的输出信号执行子块变换。

[0514] 另一方面，修改轮回函数模块 407 从 T12 到 T13 使用 wkey1、从 T13 到 T14 使用 wkey3、从 T14 到 T15 使用 wkey5、... 及从 T15 到 T16 使用 wkey7 对输入信号 475 执行子块变换。

[0515] 在加密的最后周期 (T16)，控制单元 404 声明选择信号 170。相应地，修改轮回函数模块 407 的选择器 115 选择来自使用轮回密钥 B163 执行 AddRoundKey 变换的 AddRoundKey 变换模块 114 的输出，从而执行最后周期的子块变换。在 T16，修改轮回函数模块 407 的

输出信号 166 输出是作为输入信号的明文数据 P0 的加密结果的密文数据 C0。一个周期后(T17),数据保持单元 108 向外部输出密文数据 C0 的值作为来自 AES 芯 401 的输出。同时,为了通知在 AES 芯 401 外部的单元加密被结束、以及输出信号 151 被启动,控制单元 404 声明有效信号 159(T17)。在有效信号 159 被声明的同时,AES 芯 401 保证输出信号 151 被启动。

[0516] 另一方面,控制信号 160 保持取消,因为在时序 T17 有效信号 159 被声明,但在 T17 加密 / 解密开始信号 158 也被声明。如果在 T17 加密 / 解密开始信号 158 不被声明,则在 T17 控制信号 160 被声明,并且数据保持单元 108 的值保持密文数据 C0。

[0517] 在当加密结束时的 T17,密钥扩展单元 402 输出作为轮回密钥 A1462 的 wkey0 和作为轮回密钥 A2463 的 wkey1。轮回密钥 A1462 和轮回密钥 A2463 的值被保持,直到下一个加密 / 解密开始信号 156 的声明。

[0518] 当预计到加密结束时 (T17),控制单元 404 在结束前的一个周期 (T16) 声明控制信号 157。当控制信号 157 被声明时,在 AES 芯 401 外部的单元把输入信号 150 的值设置到下个明文数据 P1,从而第二块的加密可开始。在图 56A 和 56B 的时序图中,在 AES 芯 401 外部的单元在最短周期 (T17) 声明下一个加密 / 解密开始信号。第二块加密时段是从 T17 至 T22,其中进行与对于第一块的操作相同的操作。从那时起,加密操作被重复地进行与块的预定数量一样多次。在图 56A 和 56B 的时序图中,第二块的加密在距离第一块加密结束的最短间隔处开始。AES 芯通过以这样一种时序执行所有块的加密可呈现其最大性能。然而,加密间隔基本上可设置到任意长度。

[0519] 当预定数量的块的加密已经完全结束,并且下个作业要使用诸如密码密钥之类的不同参数执行时,处理再次从参数设置开始。

[0520] 接着将描述第七实施例的解密操作。

[0521] 图 57A 和 57B 是根据这个实施例的解密时序图。参照图 57A 和 57B,横坐标代表时间。时序名称 T01、T02、...、T24 被赋予时钟脉冲的前沿。在图 57A 左端沿纵坐标的三位数指示信号线,并且与在图 52 至 55 中使用的信号线的附图标记具有一一对应性。

[0522] 解密操作也大致划分成四部分 :参数设置时段 (T01 至 T06)、密钥准备时段 (T06 至 T12)、第一块解密时段 (T12 至 T17) 及第二块解密时段 (从 T17 起)。

[0523] 参数设置时段的作用、开始条件及结束条件与在本实施例的加密中相同。然而,加密 / 解密选择信号 153 需要在解密中被声明。

[0524] 密钥准备时段是从 T06 至 T12,并且开始条件和结束条件与在本实施例的加密中相同。然而,在密钥准备时段的结束 (T12) 时,密钥扩展单元 402 使用作为轮回密钥 B163 保持的 wkey10 反向地进行密钥扩展,并且输出在解密中分别用作轮回密钥 A1462 和轮回密钥 A2463 的初始轮回密钥 (wkey9 和 wkey8)。轮回密钥 A1462 和轮回密钥 A2

[0525] 463 的值被保持,直到加密 / 解密开始信号 158 的声明。控制单元 404 停止向上计数计数器信号 161,并且把计数器清除到 0。

[0526] 在密钥准备时段结束的附近,当预计到密钥准备将在 T12 结束、并启动解密时,控制单元 404 在 T11 声明控制信号 157。

[0527] 在 T12 检测到控制信号 157 的声明时,设置在 AES 芯 401 外的输入信号供给单元把密文数据 C0 供给到 AES 芯 401 作为输入信号 150。加密 / 解密开始信号 158 被声明,以

开始输入信号 150 的解密 (T12)。在时序图中，加密 / 解密开始信号 158 在最短周期中被声明。然而，时序在 AES 芯 401 外自由确定。

[0528] 在解密时段中，输入信号 150 被解密。解密时段是从加密 / 解密开始信号 158 的声明 (T12) 到五个周期后的时序 (T17) 的时段。

[0529] 在检测到加密 / 解密开始信号 158 的声明时，控制单元 404 在下个周期 (T13) 中取消控制信号 157、输出保持信号 159 及控制信号 160。同时，控制单元 404 开始向上计数计数器信号 161。

[0530] 在 T13，密钥扩展单元 402 使用作为轮回密钥 A2463 保持的 wkey8 进行密钥扩展以产生 wkey7 和 wkey6，并且输出它们分别作为轮回密钥 A1462 和轮回密钥 A2463。在下个周期 (T14)，密钥扩展单元使用作为轮回密钥 A2463 输出的 wkey6 产生 wkey5 和 wkey4，并且输出它们分别作为轮回密钥 A1462 和轮回密钥 A2463。轮回密钥以相同方式产生，从而在 T15 输出 wkey3 和 wkey2，并且在时序 T16 输出 wkey1 和 wkey0 分别作为轮回密钥 A1462 和轮回密钥 A2463。

[0531] 在解密的第一周期 (T12)，控制单元 404 取消选择信号 171。为此，输入信号 150 的明文数据 P0 输入到修改轮回函数模块 406。由于选择信号 170 被声明，所以修改轮回函数模块 406 切换选择器 118 以选择来自 AddRoundKey 变换模块 121 的输出，从而执行一个周期的解密。来自修改轮回函数模块 406 的输出直接输入到修改轮回函数模块 408，从而执行多一个周期的解密。来自修改轮回函数模块 408 的输出结果由数据保持单元 108 保持。

[0532] 在下个周期 (T13) 时，控制单元 404 声明选择信号 171，并且把来自数据保持单元的输出输入到修改轮回函数模块 406。由于选择信号 170 被取消，所以修改轮回函数模块 406 切换选择器 118 以选择来自 InvMixColumns 变换模块 116 的输出，从而执行一个周期的解密。来自修改轮回函数模块 406 的输出直接输入到修改轮回函数模块 408，从而执行多一个周期的解密。处理以相同方式进行直到 T16。修改轮回函数模块 406 在 T12 使用 wkey10 和 wkey9，在 T13 使用 wkey7，在 T14 使用 wkey5，及在 T16 使用 wkey1，作为轮回密钥。修改轮回函数模块 408 在 T12 使用 wkey8，在 T13 使用 wkey6，及在 T16 使用 wkey0，作为轮回密钥。

[0533] 在 T16，修改轮回函数模块 408 的输出信号 167 输出是作为输入信号的密文数据 C0 的解密结果的明文数据 P0。一个周期后 (T17)，数据保持单元 108 向外部输出明文数据 P0 的值作为来自 AES 芯 401 的输出。同时，为了通知在 AES 芯 401 外部的单元解密被结束、以及输出信号 151 被启动，控制单元 404 声明有效信号 159(T17)。在有效信号 159 被声明的同时，AES 芯 401 保证输出信号 151 被启动。

[0534] 另一方面，控制信号 160 保持取消，因为在 T17 有效信号 159 被声明，但在 T17 加密 / 解密开始信号 158 也被声明。如果在 T17 加密 / 解密开始信号 158 不被声明，在 T17 控制信号 160 被声明，并且数据保持单元 108 的值保持明文数据 P0。

[0535] 在 T17 当解密结束时，密钥扩展单元 402 输出作为轮回密钥 A1

[0536] 462 的 wkey9 和作为轮回密钥 A2463 的 wkey8。轮回密钥 A1462 和轮回密钥 A2463 的值被保持，直到下一个加密 / 解密开始信号 156 的声明。

[0537] 当预计到解密结束时 (T17)，控制单元 404 在结束前的一个周期 (T16) 声明控制信号 157。当控制信号 157 被声明时，在 AES 芯 401 外部的单元把输入信号 150 的值设置到下

个密文数据 C1，从而第二块的解密可开始。

[0538] 第二块解密时段是从 T17 至 T22，其中进行与第一块的操作相同的操作。从那时起，解密操作被重复进行与块的预定数量一样多的次数。在图 57A 和 57B 的时序图中，第二块的解密在距离第一块解密结束的最短间隔处开始。AES 芯通过以这样一种时序执行所有块的解密可呈现其最大性能。然而，解密间隔基本上可设置到任意长度。

[0539] 当预定数量的块的解密已经完全结束，并且下个作业要使用诸如密码密钥之类的不同参数执行时，处理再次从参数设置开始。

[0540] 第七实施例能以上述方式实施。在第七实施例中，对于 AES 加密和解密所要求的时钟周期的数量被减小一个，而不增大在每个时钟周期时段中用于每个子块变换的信号处理时间总和的最大值。这把 AES 处理速度提高约 20％。

[0541] 以上已经举例说明了第七实施例。然而，即使对于任何其它实施例相同的实施也是可能的。

[0542] 上述第七实施例仅是本发明的例子，并且本发明的效果不限于上述实施例的那些。

[0543] ＜第八实施例＞

[0544] 作为第七实施例的一般形式，在第一实施例中的 N 个周期过程可以在一个周期中执行。N 是 2 或更大的自然数。在第八实施例中，将描述用来实施这种方法的电路设置。

[0545] 第一实施例中在一个时钟周期中用来执行 N 个周期过程的电路可分类成两种类型：一种类型是处理所需的周期总数可由 N 除尽而没有余数、一种类型是数字不能由 N 除尽。在例如 AES-128 中，处理必需的周期总数是 10（图 1）。其中 N 是 2 或 5 的情形分类成前者，其它情形分类成后者。

[0546] 首先将描述周期总数可由 N 除尽而没有余数的情形。在这种情况下，对于加密和解密的每一种实施 N 个（N 是 2 或更大的自然数）修改轮回函数模块，如在 N ＝ 2 的第七实施例中那样。在每个时钟周期中使用所有修改轮回函数模块执行处理。这时，处理必需的时钟周期数是 10/N。

[0547] 将描述当第一实施例的周期总数可由 N 除尽而没有余数时的加密／解密单元的电路设置。图 58 是根据第八实施例的加密／解密单元的方块图。参照图 58，附图标记 503 指示加密／解密单元；550 指示轮回密钥 A1；及 551 指示轮回密钥 A2。有 N 个轮回密钥 A，包括轮回密钥 A1550 和轮回密钥 A2551。与第七实施例相同的附图标记指示相同的构成元件和信号线，将不重复描述。

[0548] 在以上设置中，选择器 109 的输出连接到修改轮回函数模块 405 上。(N-1) 个修改轮回函数模块 405 串联连接。最后修改轮回函数模块 405 的输出连接到修改轮回函数模块 407。选择器 109 的输出也连接到修改轮回函数模块 406。修改轮回函数模块 406 的输出连接到修改轮回函数模块 408。(N-1) 个修改轮回函数模块 408 串联连接。最后修改轮回函数模块 408 的输出连接到选择器 107。修改轮回函数模块 405 分别按连接顺序接收轮回密钥 A1550、轮回密钥 A2551 及其余轮回密钥 A。修改轮回函数模块 407 接收第 N 个轮回密钥 A 和轮回密钥 B163。修改轮回函数模块 406 接收轮回密钥 A1550 和轮回密钥 B163。修改轮回函数模块 408 分别按连接顺序接收轮回密钥 A2551 和其余轮回密钥 A。将省略图 58 中与第七实施例具有相同连接关系的构成元件的描述。

[0549] 接着将描述第一实施例中周期总数不能由N除尽而没有余数的情形。在这种情况下，对于加密和解密各自实施N个修改轮回函数模块。在加密或解密的的特定周期中也必须绕过一些修改轮回函数模块。例如，当N＝4时，图1表示的第一实施例中的第0至第三周期的过程在第0时钟周期中执行。在第一时钟周期，执行在图1中的第一实施例中的第四至第七周期的过程。在第二时钟周期，执行在图1中的第一实施例中的第八和第九周期的过程。就是说，如果周期总数不能由N除尽而没有余数，则在第0和第一时钟周期使用所有四个修改轮回函数模块。然而，在第二时钟周期，仅两个修改轮回函数模块就足够了。这时，处理所必需的时钟周期数是10/N（分数部分被四舍五入）。

[0550] 当在第一实施例的周期总数不能由N除尽而没有余数时，各种电路设置是可用的。例如，选择器被提供在图58所示每个修改轮回函数模块紧之后以选择是否绕过修改轮回函数模块，并且每个选择器按照从加密或解密开始起的周期数切换。这种情形的电路设置容易从图58想象，并省略其方块图。

[0551] 第八实施例能以上述方式实施。根据本发明的第一实施例，处理所必需的时钟周期总数在AES-128中是10，在AES-192中是12，及在AES-256中是14。所有电路可通过把它们分类成周期总数可由N除尽而没有余数的情形、或该数不能由N除尽的情形而实施，如这个实施例中描述的那样。用来实施所有AES-128、AES-192及AES-256的电路设置也是可能的。这种情况下，如果N＝1、或N＝2，则处理所必需的时钟周期总数在AES-128、AES-192及AES-256全部都可由N除尽而没有余数。因此，使用时钟周期总数的设置（这个实施例中可由N除尽而没有余数）来实施电路。即使当N取任何其它值时，使用本实施例的可把加密／解密单元中实施的N个修改轮回函数模块的任意一个的输出选作加密／解密单元的输出的设置，来形成能够实施所有AES-128、AES-192及AES-256的电路，如在第一实施例中的周期总数不能由N除尽而没有余数的情形那样。

[0552] ＜第九实施例＞

[0553] 在本发明的第一至第六实施例中，一个周期的处理不适应一些情况下定义的一个时钟周期。这样一种情况下，把新的数据保持单元添加到修改轮回函数模块，从而在第一至第六实施例的一个周期处理在多个时钟周期中执行。作为详细例子将描述在第一实施例中在一个周期中执行的处理被在两个时钟周期中执行的电路设置。

[0554] 图59表示新数据保持单元添加到第一实施例的修改轮回函数模块的例子。参照图59，附图标记605指示修改轮回函数模块，并且数据保持单元608保持加密过程中的结果。

[0555] 在以上设置中，来自SubBytes变换模块111的输出输入到数据保持单元608。来自数据保持单元608的输出输入到ShiftRows变换模块112。

[0556] 添加新数据保持单元到加密单元使得能够在两个时钟周期中执行第一实施例的一个周期处理。在图59中，数据保持单元608添加在SubBytes变换模块111与ShiftRows变换模块112之间。然而，数据保持单元可连接到任意点。可选择地，SubBytes变换模块111可以包括数据保持单元。

[0557] 在上述实施例中，对第一实施例的一个周期处理要求两个时钟周期。然而，处理可以在N个时钟周期中进行。这种情况下，把(N-1)个数据保持单元新添加到变换模块之间的任意点或者实施在变换模块中。

[0558] 以上已经举例说明了第一实施例。然而，同样的实施甚至对于任何其它实施例也是可能的。

[0559] ＜第 10 实施例＞

[0560] 在本发明的第一至第九实施例中，数据保持单元的数据更新时段是一个时钟周期。然而，它不总是必需的。

[0561] 一般地，CPU 或 DMA 的操作时钟的频率在多数情况下很高。如果用于加密的数据保持单元使用相同时钟，则不可能保证在每个时钟周期时段中用于每个子块变换的信号处理时间总和，并且处理可能不适应一个时钟周期。

[0562] 这样一种情况下，例如，如果在每个时钟周期时段中用于每个子块变换的信号处理时间总和是一个时钟周期的两倍或较少，则可以在两个时钟周期中进行数据保持单元的数据更新一次。

[0563] 这种设置通过把启动信号新输入到数据保持单元而容易实施。

[0564] 参照图 61A 和 61B 的时序图，将描述这个实施例。图 61A 表示当数据保持单元的更新与时钟周期同步时的时序图。与时钟周期的后沿同步，数据保持单元更新数据。

[0565] 图 61B 表示当数据保持单元的更新与时钟周期不同步时的时序图。启动信号输入到数据保持单元，并且按 1/2 时钟的时段重复 HIGH（高）和 LOW（低）。只有当启动信号是 HIGH时，数据保持单元才进行数据更新。因此，数据保持单元在两个时钟周期中在时钟后沿更新数据一次。

[0566] 这种情况下，把一个周期处理在两个时钟周期中执行。

[0567] 这个实施例描述的例子中，把一个周期处理在两个时钟周期中执行。然而，当然，可以把一个周期处理在 N 个时钟周期中执行。

[0568] 在本发明的第一至第九实施例中，可以把 N 个时钟周期定义为一个周期。

[0569] 以上已经描述了本发明的实施例。每个实施例中，已经举例说明了 AES-128。然而，也可实施 AES-192 和 AES-256。与 AES-128 的实施例的不同点是输入到密钥扩展单元的密码密钥的位数、由密钥扩展单元产生的轮回密钥的数量及控制信号的声明／取消时序。这些基于每个实施例中描述的相同概念可容易实施。加密／解密单元和修改轮回函数模块不要求与 AES-128 的实施例中描述的那些不同。

[0570] 尽管参照示范实施例已经描述了本发明，但要理解，本发明不限于公开的示范实施例。如下权利要求要求书的范围要符合最广义解释，从而包容所有这样的修改和等效结构与功能。

周期号	现有技术		第一实施例	
	要执行的处理	要使用的轮回密钥	要执行的处理	要使用的轮回密钥
0	· AddRoundKey	·第0轮回密钥($wkey_0$)	· AddRoundKey · SubBytes · ShiftRows · MixColumns	·第0轮回密钥($wkey_0$)
1	· SubBytes · ShiftRows · MixColumns · AddRoundKey	·第1轮回密钥($wkey_1$)	· AddRoundKey · SubBytes · ShiftRows · MixColumns	·第1轮回密钥($wkey_1$)
8	· SubBytes · ShiftRows · MixColumns · AddRoundKey	·第8轮回密钥($wkey_8$)	· AddRoundKey · SubBytes · ShiftRows · MixColumns	·第8轮回密钥($wkey_8$)
9	· SubBytes · ShiftRows · MixColumns · AddRoundKey	·第9轮回密钥($wkey_9$)	· AddRoundKey · SubBytes · ShiftRows · AddRoundKey	·第9轮回密钥($wkey_9$) ·第10轮回密钥($wkey_{10}$)
10	· SubBytes · ShiftRows · AddRoundKey	·第10轮回密钥($wkey_{10}$)		

图 1

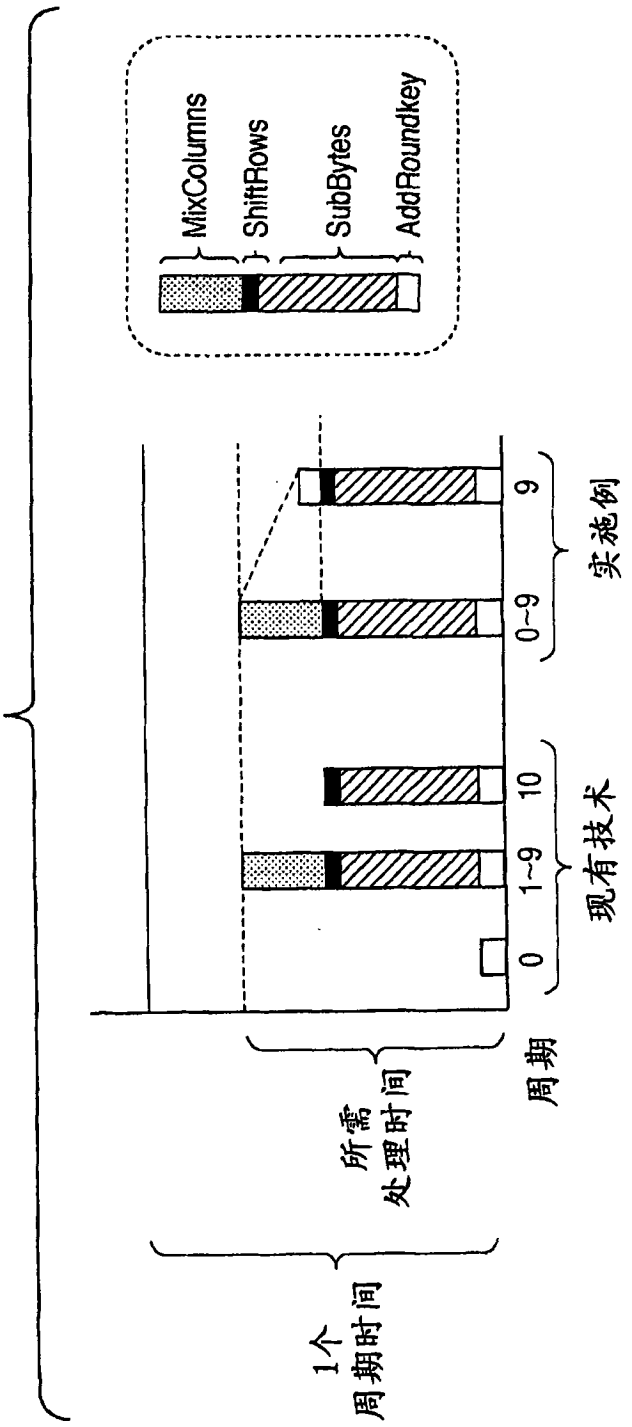

MixColumns
ShiftRows
SubBytes
AddRoundkey
1个
周期时间
所需
处理时间
周期
0
1~9
10
现有技术
0~9
9
实施例

图2

周期号	现有技术		第一实施例	
	要执行的处理	要使用的轮回密钥	要执行的处理	要使用的轮回密钥
0	· AddRoundKey	· 第10轮回密钥($wkey_{10}$)	· AddRoundKey · InvShiftRows · InvSubBytes · AddRoundKey	· 第10轮回密钥($wkey_{10}$) · 第9轮回密钥($wkey_9$)
1	· InvShiftRows · InvSubBytes · AddRoundKey · InvMixColumns	· 第9轮回密钥($wkey_9$)	· InvMixColumns · InvShiftRows · InvSubBytes · AddRoundKey	· 第8轮回密钥($wkey_8$)
8	· InvShiftRows · InvSubBytes · AddRoundKey · InvMixColumns	· 第2轮回密钥($wkey_2$)	· InvMixColumns · InvShiftRows · InvSubBytes · AddRoundKey	· 第1轮回密钥($wkey_1$)
9	· InvShiftRows · InvSubBytes · AddRoundKey · InvMixColumns	· 第1轮回密钥($wkey_1$)	· InvMixColumns · InvShiftRows · InvSubBytes · AddRoundKey	· 第0轮回密钥($wkey_0$)
10	· InvShiftRows · InvSubBytes ·	· 第0轮回密钥($wkey_0$)		

图 3

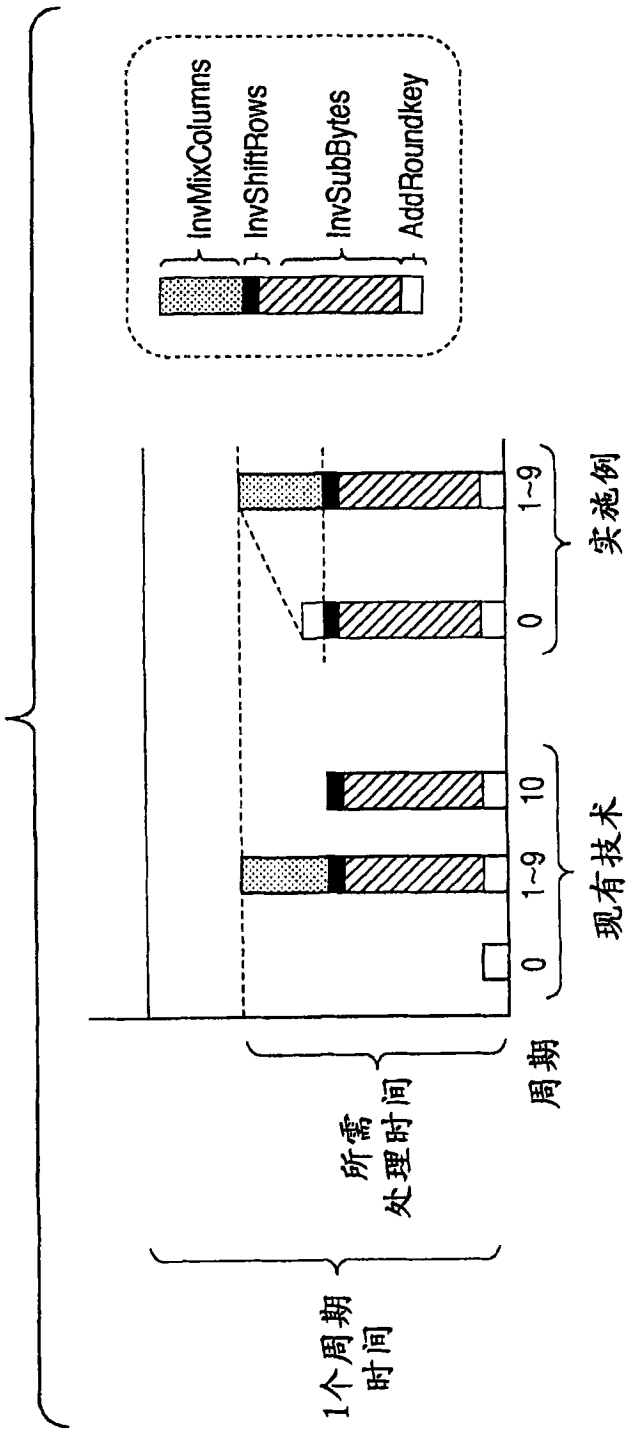

InvMixColumns
InvShiftRows
InvSubBytes
AddRoundkey
1个周期时间
所需处理时间
周期
0
1~9
10
现有技术
0
1~9
实施例

图 4

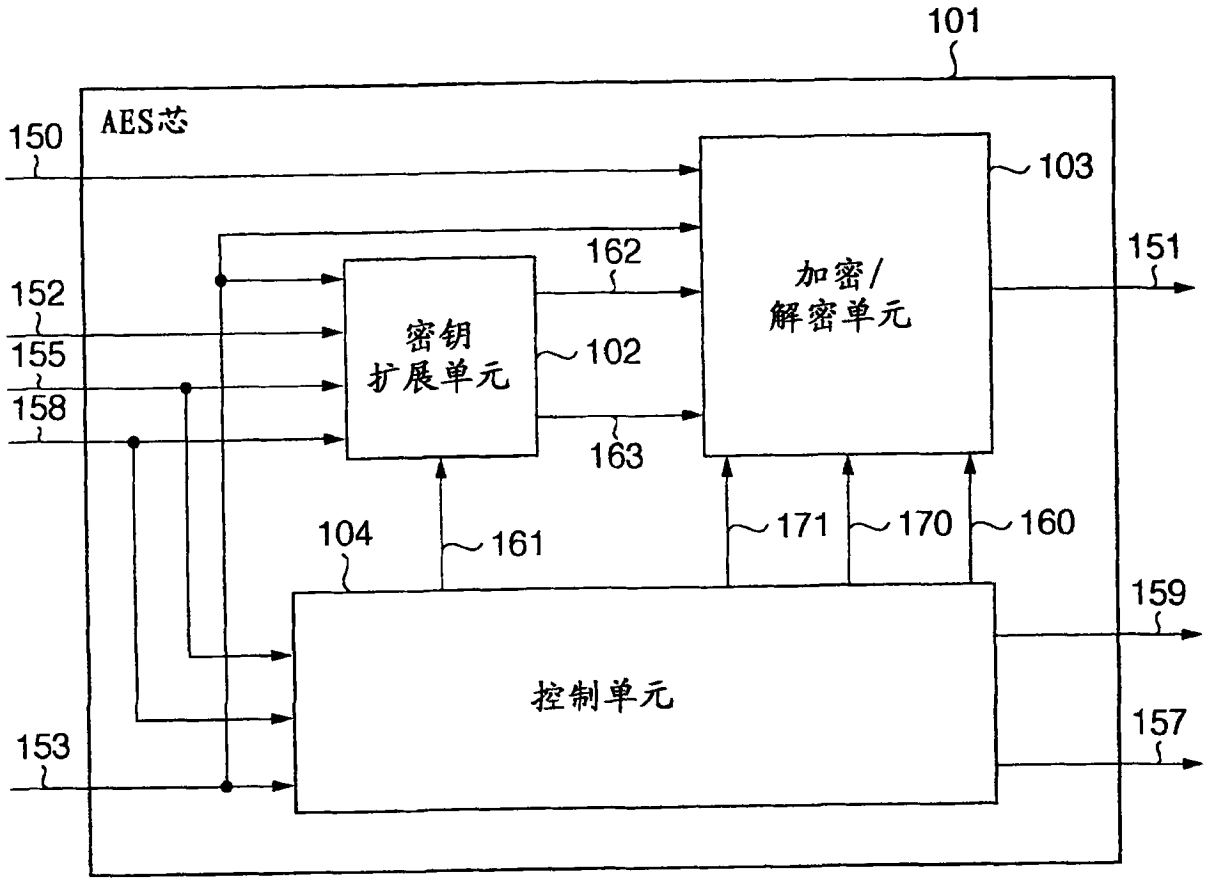

101
AES芯
150
152
155
158
153
密钥
扩展单元
162
102
163
加密/
解密单元
103
151
104
161
171
170
160
159
控制单元
157

图5

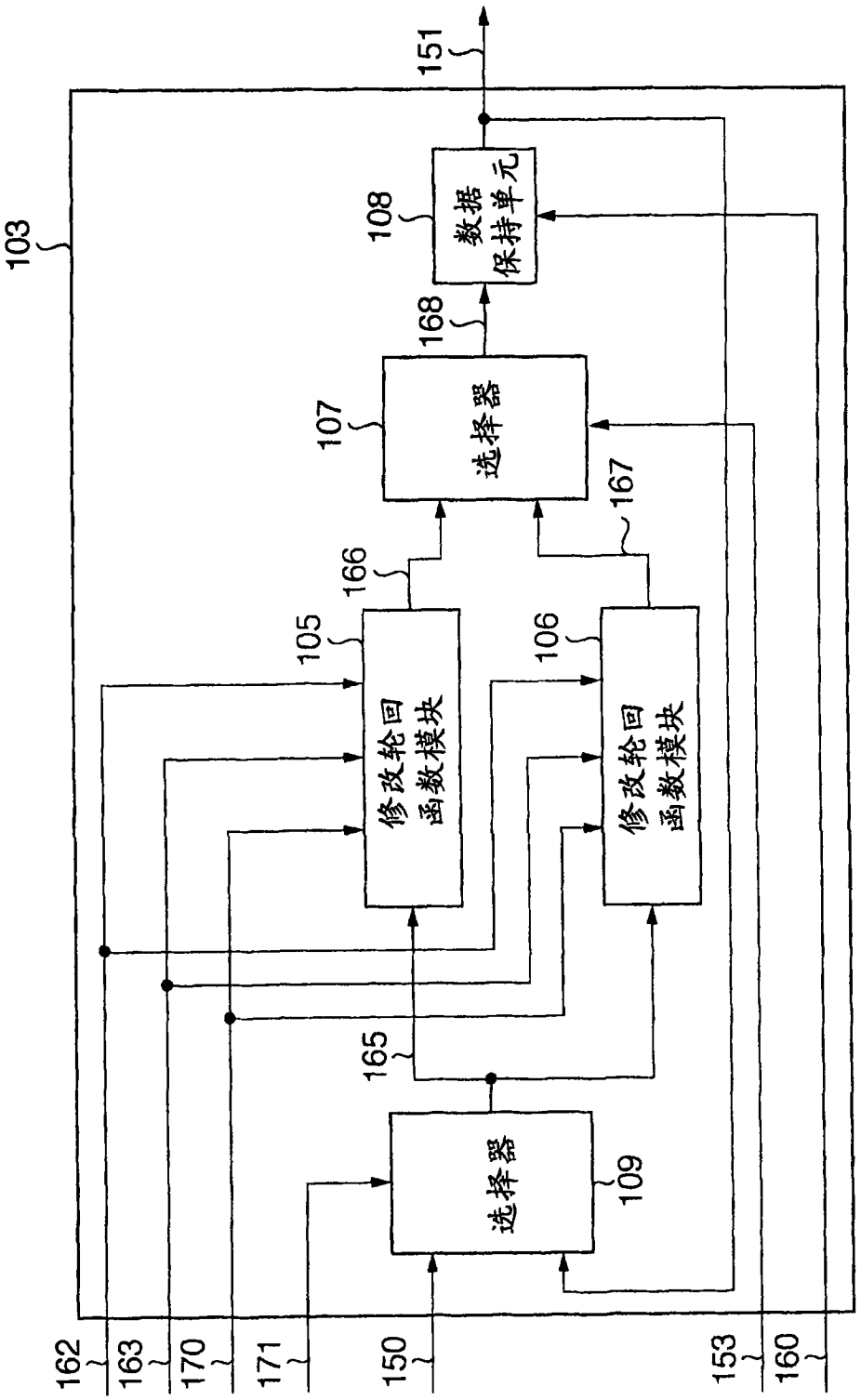

103
151
108
数据保持单元
168
107
选择器
167
166
105
修改轮回函数模块
106
修改轮回函数模块
165
109
选择器
162
163
170
171
150
153
160

图 6

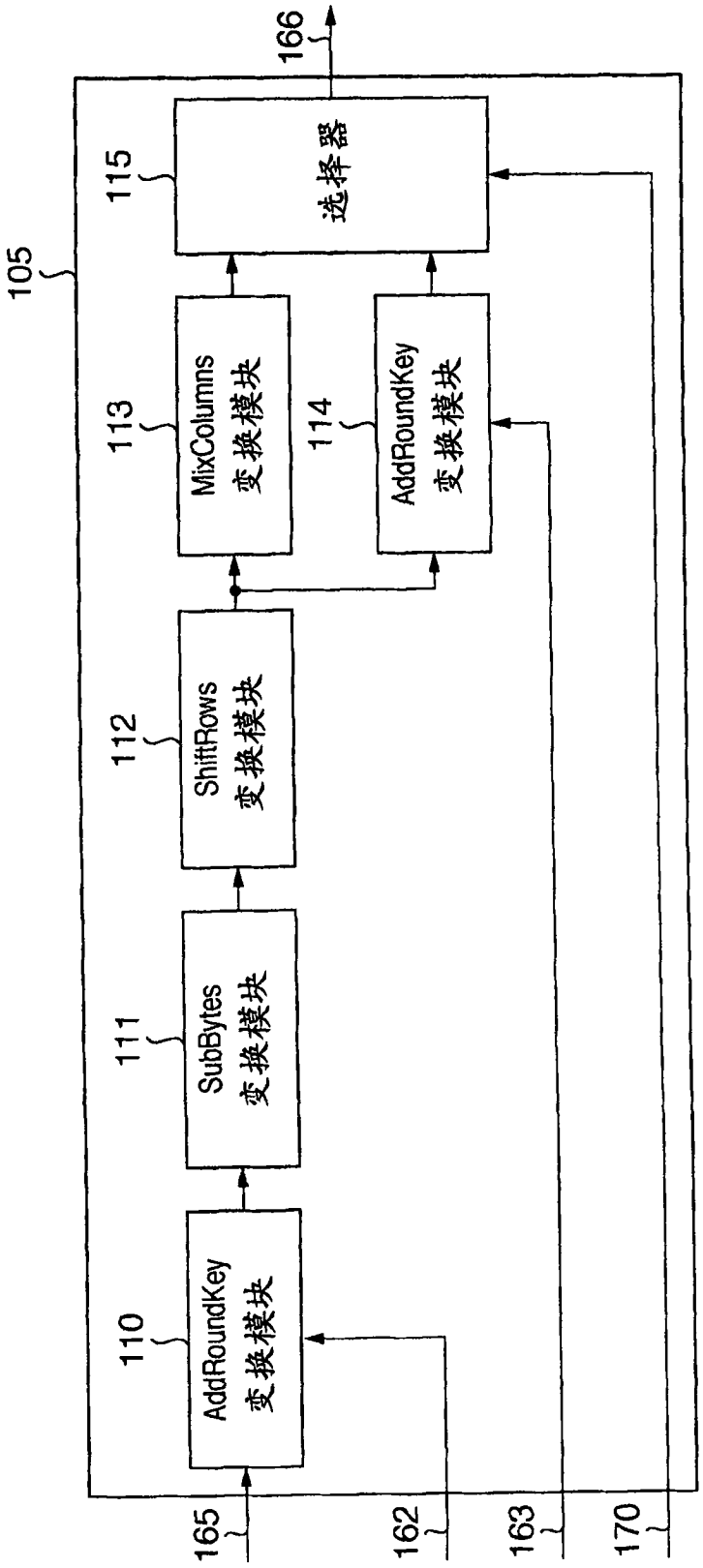

105
166
选择器
115
MixColumns
变换模块
113
AddRoundKey
变换模块
114
ShiftRows
变换模块
112
SubBytes
变换模块
111
AddRoundKey
变换模块
110
165
162
163
170

图 7

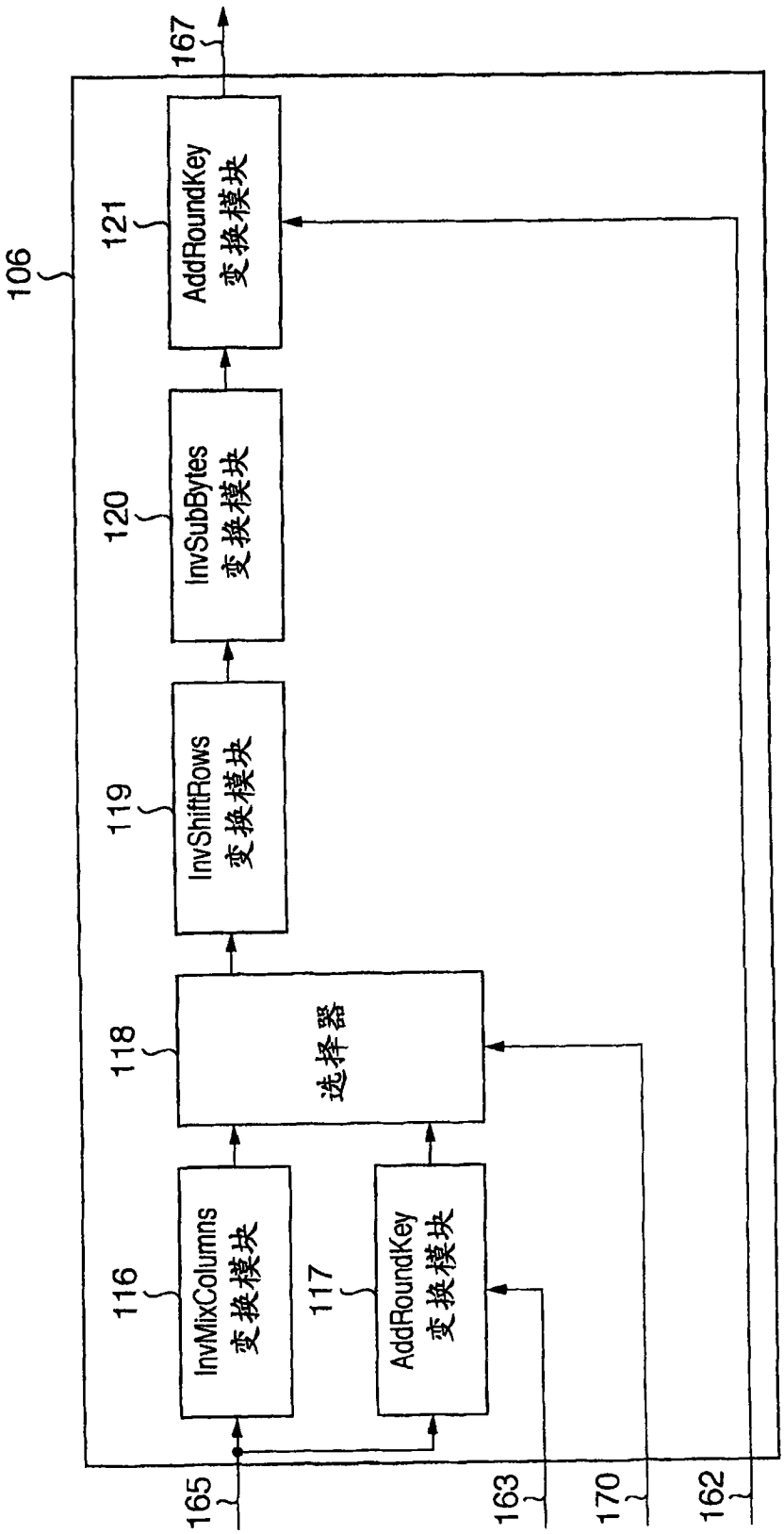

106
121
AddRoundKey
变换模块
167
120
InvSubBytes
变换模块
119
InvShiftRows
变换模块
118
选择器
116
InvMixColumns
变换模块
117
AddRoundKey
变换模块
165
163
170
162

图 8

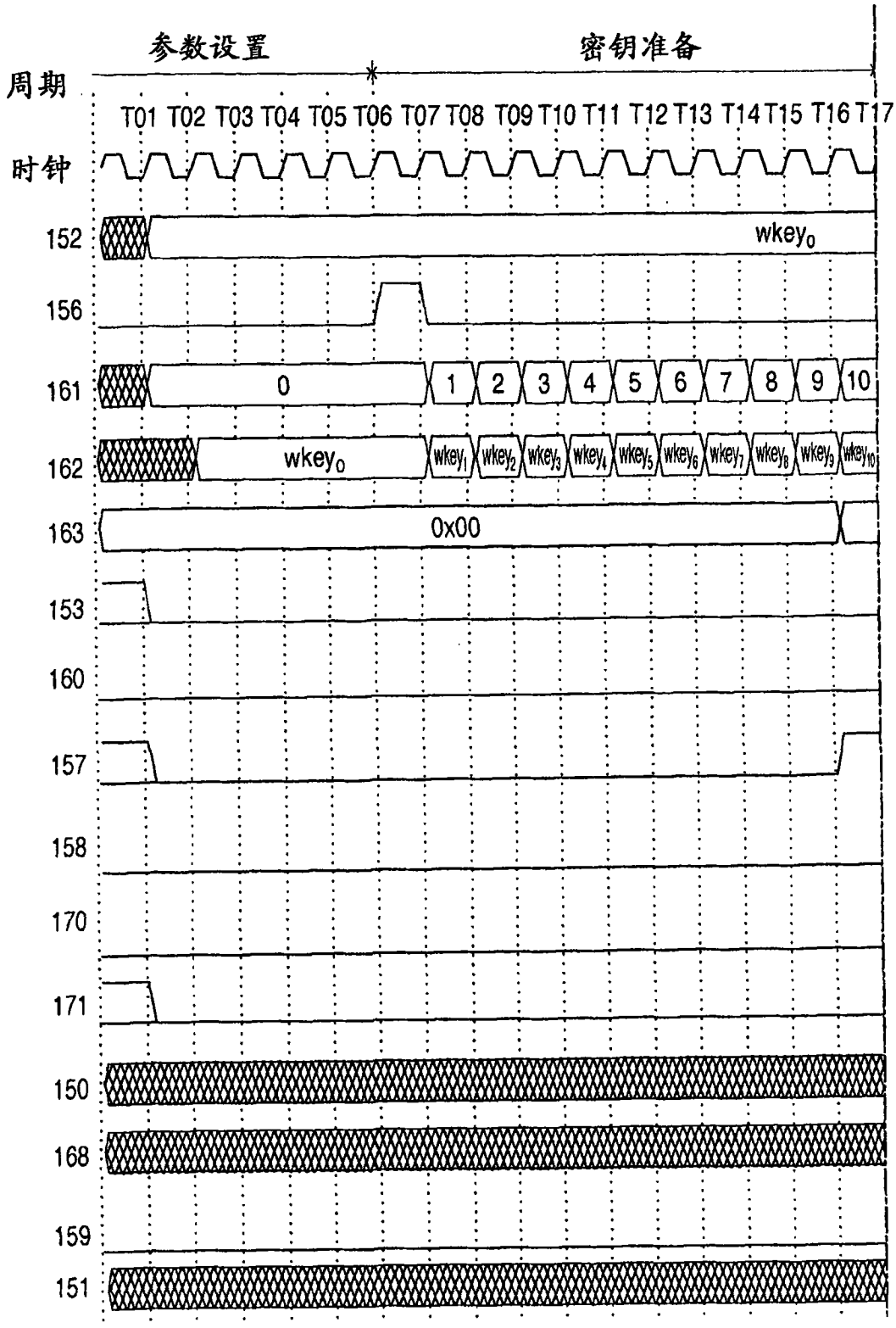

参数设置
密钥准备
周期
T01 T02 T03 T04 T05 T06 T07 T08 T09 T10 T11 T12 T13 T14 T15 T16 T17
时钟
152
wkey0
156
161
0 1 2 3 4 5 6 7 8 9 10
162
wkey0 wkey1 wkey2 wkey3 wkey4 wkey5 wkey6 wkey7 wkey8 wkey9 wkey10
163
0x00
153
160
157
158
170
171
150
168
159
151

图 9A

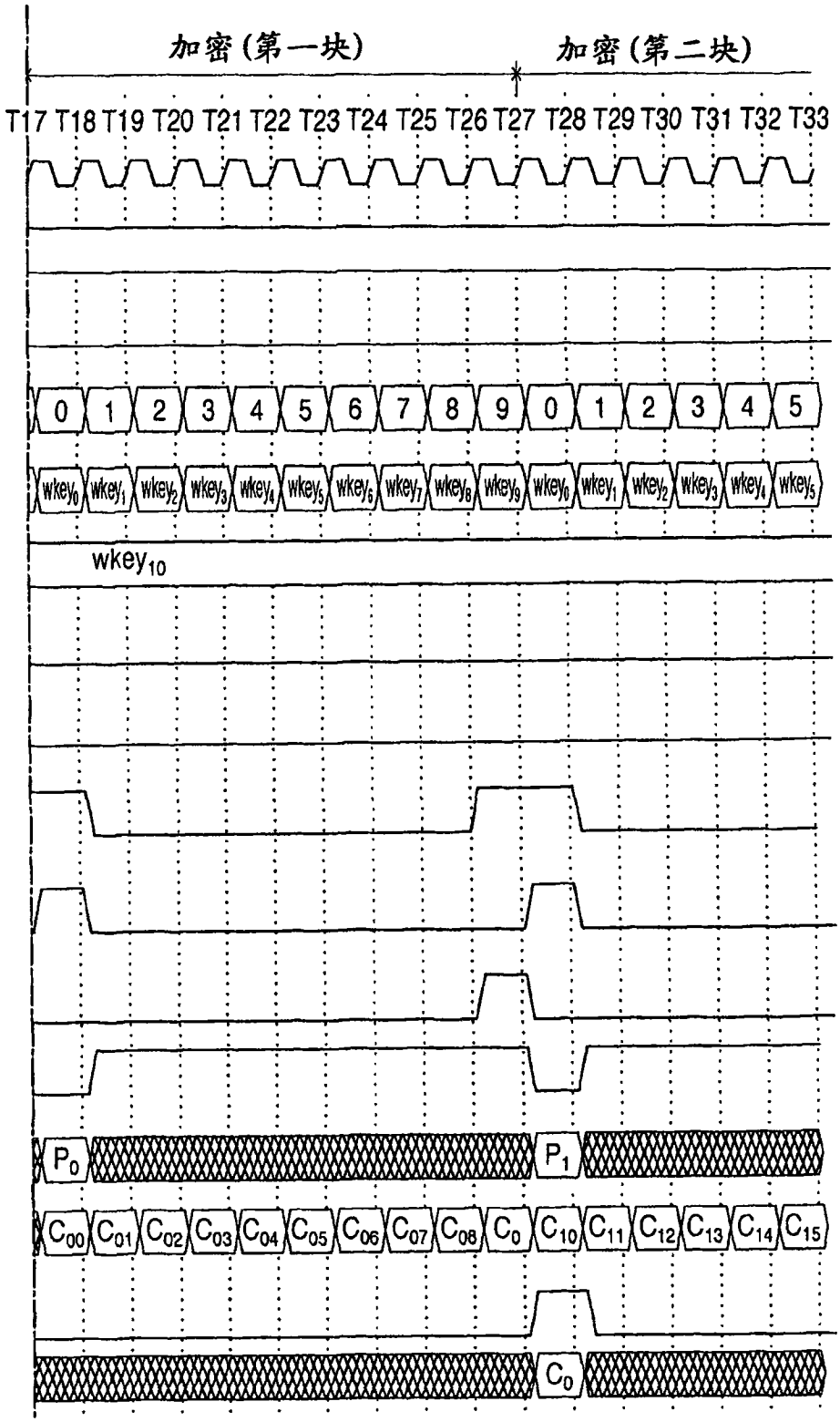

加密(第一块)
加密(第二块)
T17 T18 T19 T20 T21 T22 T23 T24 T25 T26 T27 T28 T29 T30 T31 T32 T33
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
wkey0 wkey1 wkey2 wkey3 wkey4 wkey5 wkey6 wkey7 wkey8 wkey9 wkey0 wkey1 wkey2 wkey3 wkey4 wkey5
wkey10
P0 P1
C00 C01 C02 C03 C04 C05 C06 C07 C08 C0 C10 C11 C12 C13 C14 C15
C0

图 9B

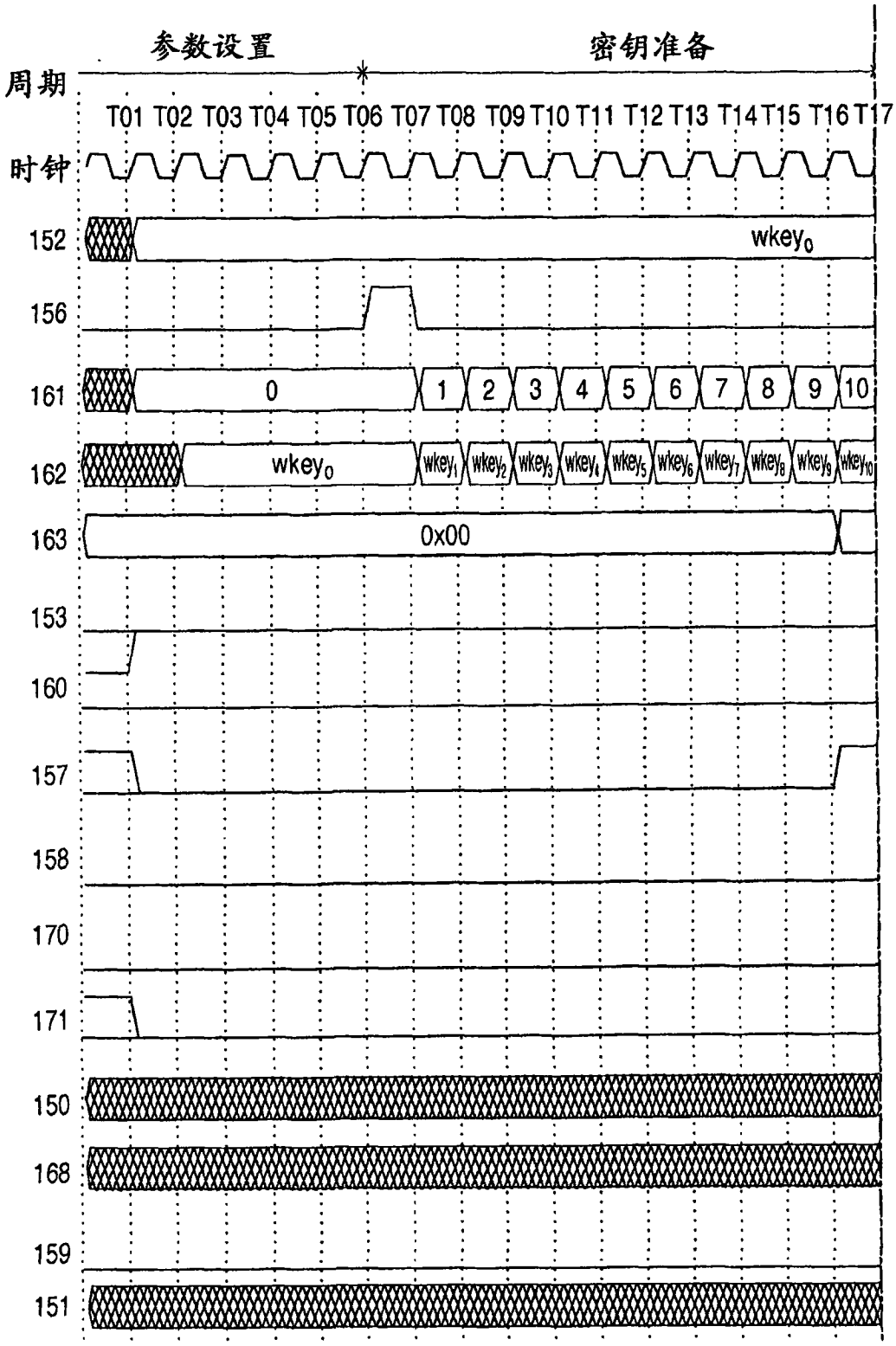

参数设置
密钥准备
周期
T01 T02 T03 T04 T05 T06 T07 T08 T09 T10 T11 T12 T13 T14 T15 T16 T17
时钟
152
wkey0
156
161
0 1 2 3 4 5 6 7 8 9 10
162
wkey0 wkey1 wkey2 wkey3 wkey4 wkey5 wkey6 wkey7 wkey8 wkey9 wkey10
163
0x00
153
160
157
158
170
171
150
168
159
151

图 10A

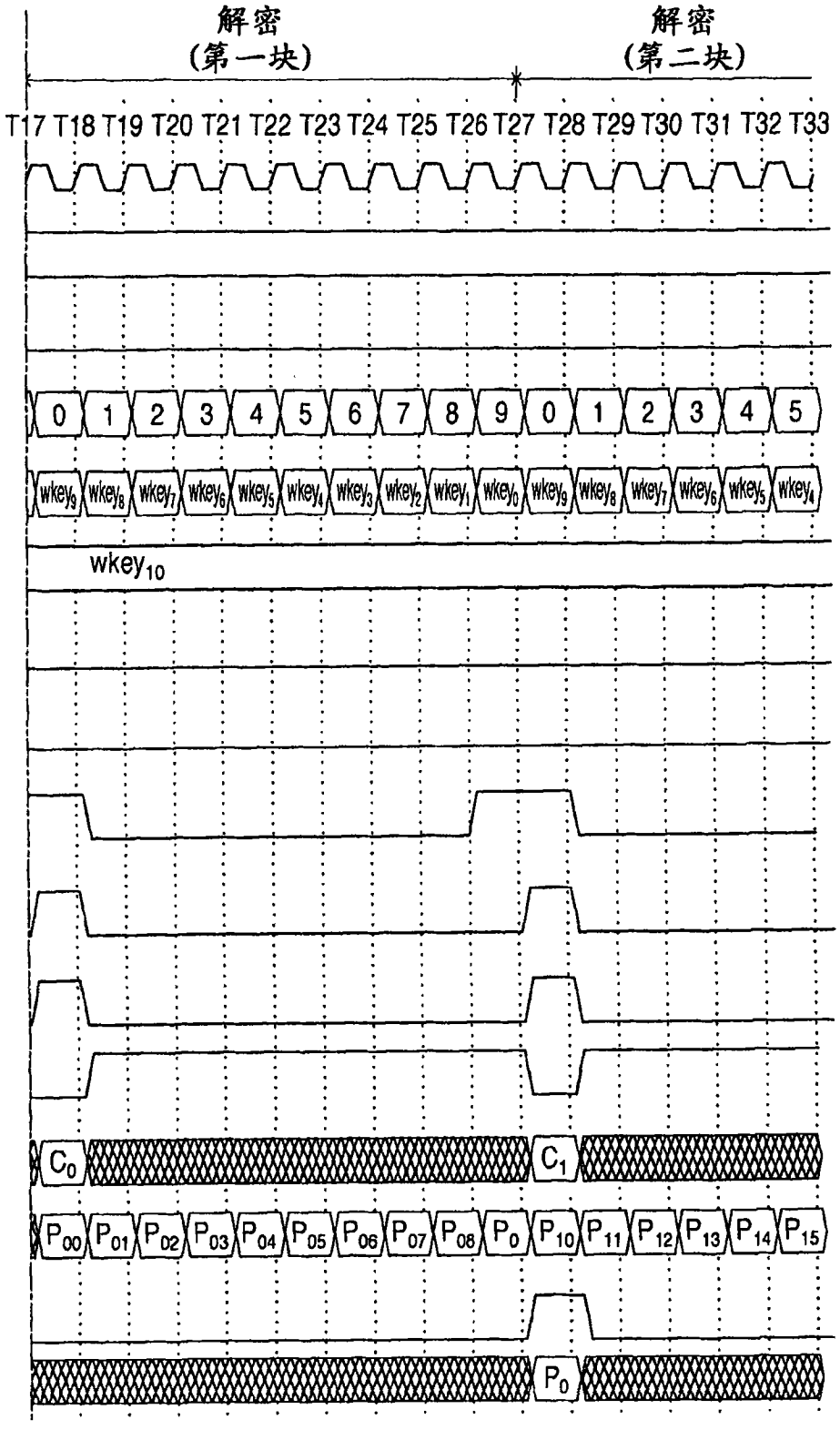

解密
(第一块)
解密
(第二块)
T17 T18 T19 T20 T21 T22 T23 T24 T25 T26 T27 T28 T29 T30 T31 T32 T33
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
wkey9 wkey8 wkey7 wkey6 wkey5 wkey4 wkey3 wkey2 wkey1 wkey0 wkey9 wkey8 wkey7 wkey6 wkey5 wkey4
wkey10
C0
C1
P00 P01 P02 P03 P04 P05 P06 P07 P08 P0 P10 P11 P12 P13 P14 P15
P0

图 10B

周期号	加密处理		解密处理	
	要执行的处理	要使用的轮回密钥	要执行的处理	要使用的轮回密钥
0	· AddRoundKey · SubBytes · ShiftRows · MixColumns · AddRoundKey	· 第0轮回密钥($wkey_0$) · 第1轮回密钥($wkey_1$)	· AddRoundKey · InvShiftRows · InvSubBytes	· 第10轮回密钥($wkey_{10}$)
1	· SubBytes · ShiftRows · MixColumns · AddRoundKey	· 第2轮回密钥($wkey_2$)	· AddRoundKey · InvMixColumns · InvShiftRows · InvSubBytes	· 第9轮回密钥($wkey_9$)
8	· SubBytes · ShiftRows · MixColumns · AddRoundKey	· 第9轮回密钥($wkey_9$)	· AddRoundKey · InvMixColumns · InvShiftRows · InvSubBytes	· 第2轮回密钥($wkey_2$)
9	· SubBytes · ShiftRows · AddRoundKey	· 第10轮回密钥($wkey_{10}$)	· AddRoundKey · InvMixColumns · InvShiftRows · InvSubBytes · AddRoundKey	· 第1轮回密钥($wkey_1$) · 第0轮回密钥($wkey_0$)

图 11

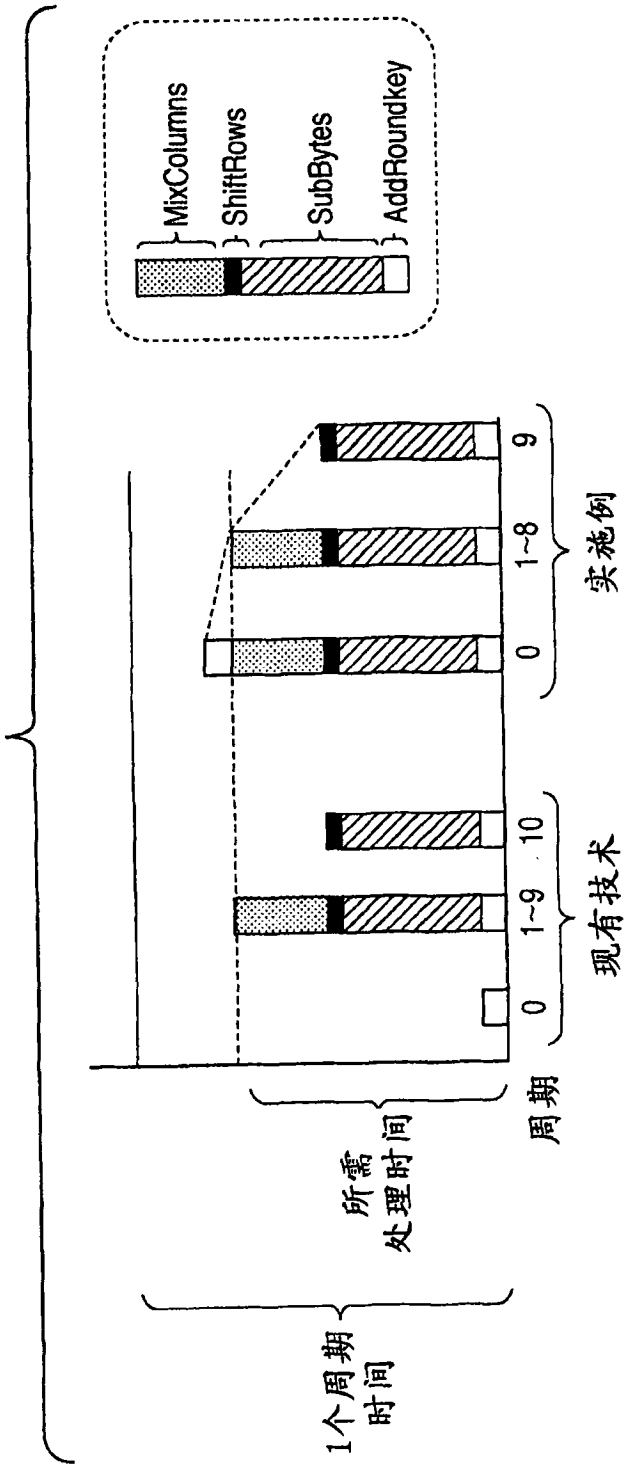

MixColumns
ShiftRows
SubBytes
AddRoundkey
1个周期时间
所需处理时间
周期
0
1~9
10
现有技术
0
1~8
9
实施例

图12

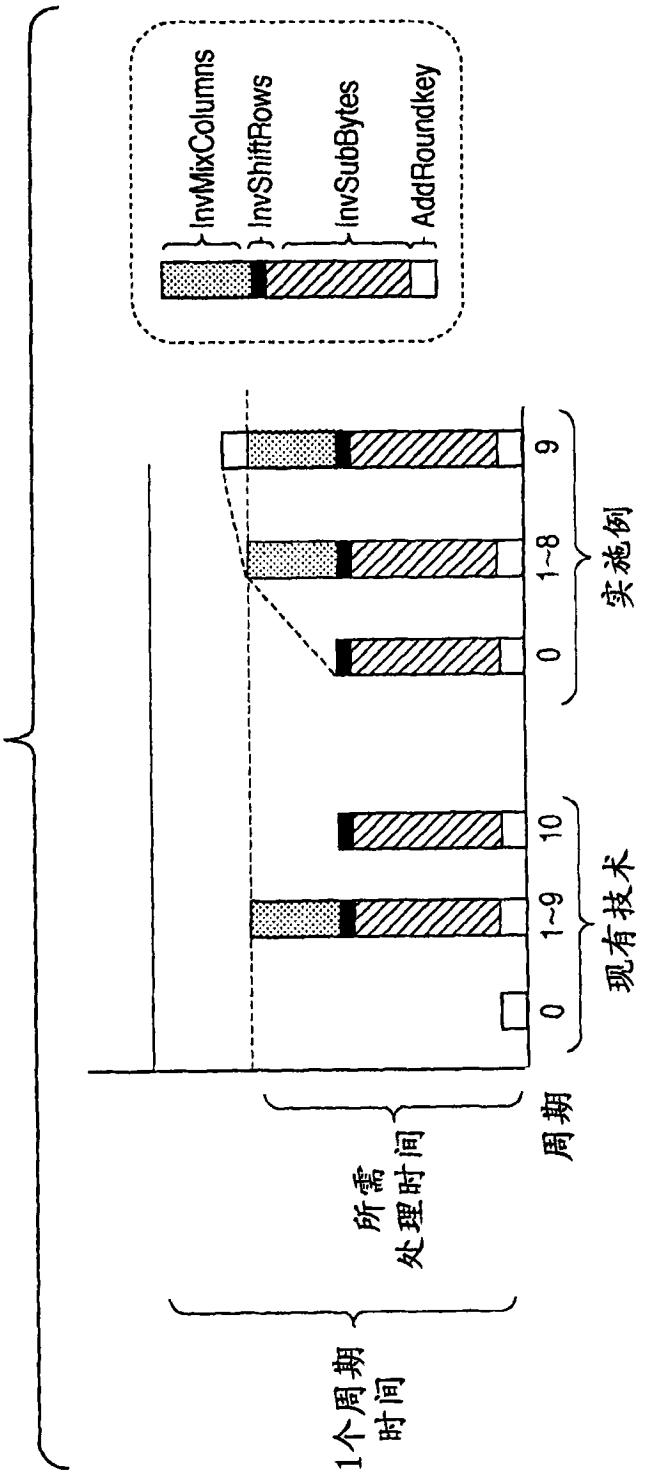

InvMixColumns
InvShiftRows
InvSubBytes
AddRoundkey
1个周期时间
所需处理时间
周期
0
1~9
10
现有技术
0
1~8
9
实施例

图13

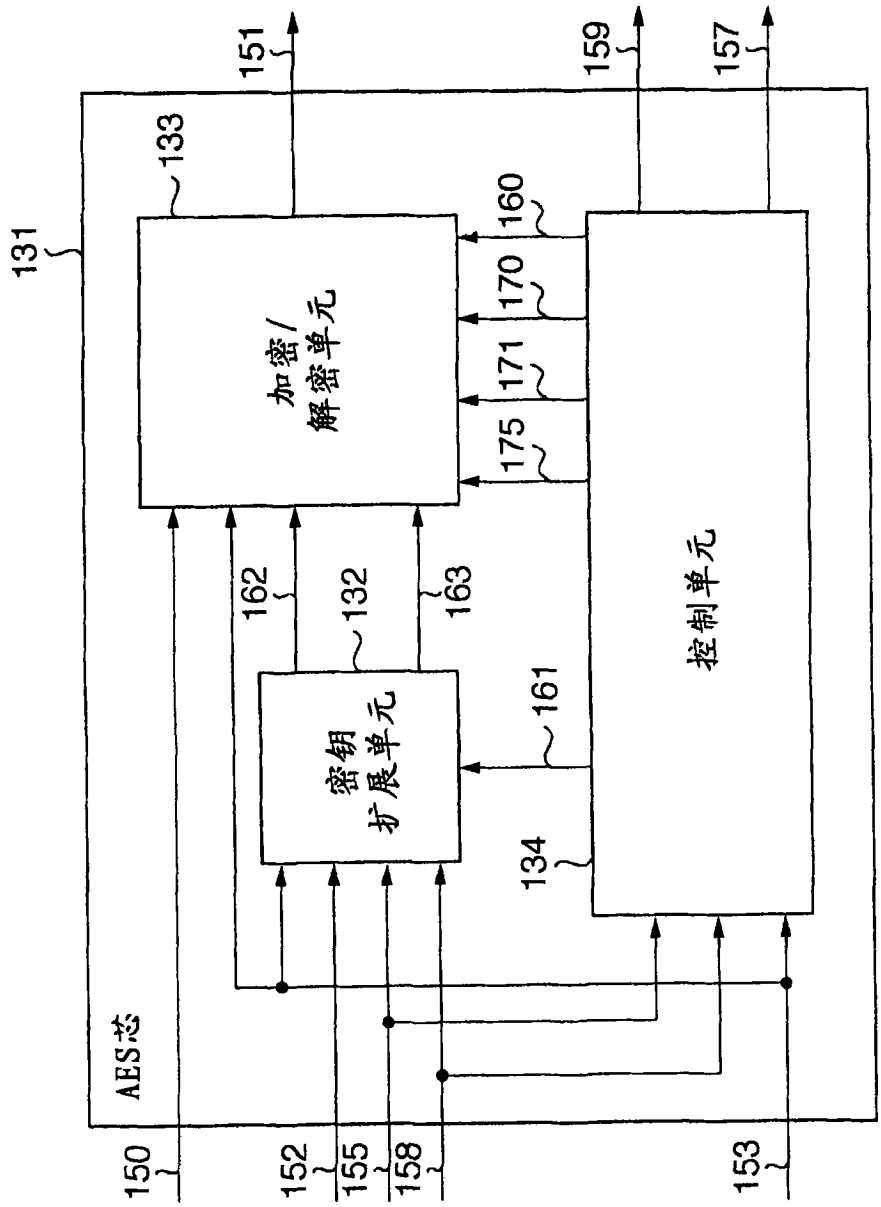

131
AES芯
133
加密/
解密单元
132
密钥
扩展单元
134
控制单元
150
151
152
153
155
157
158
159
160
161
162
163
170
171
175

图14

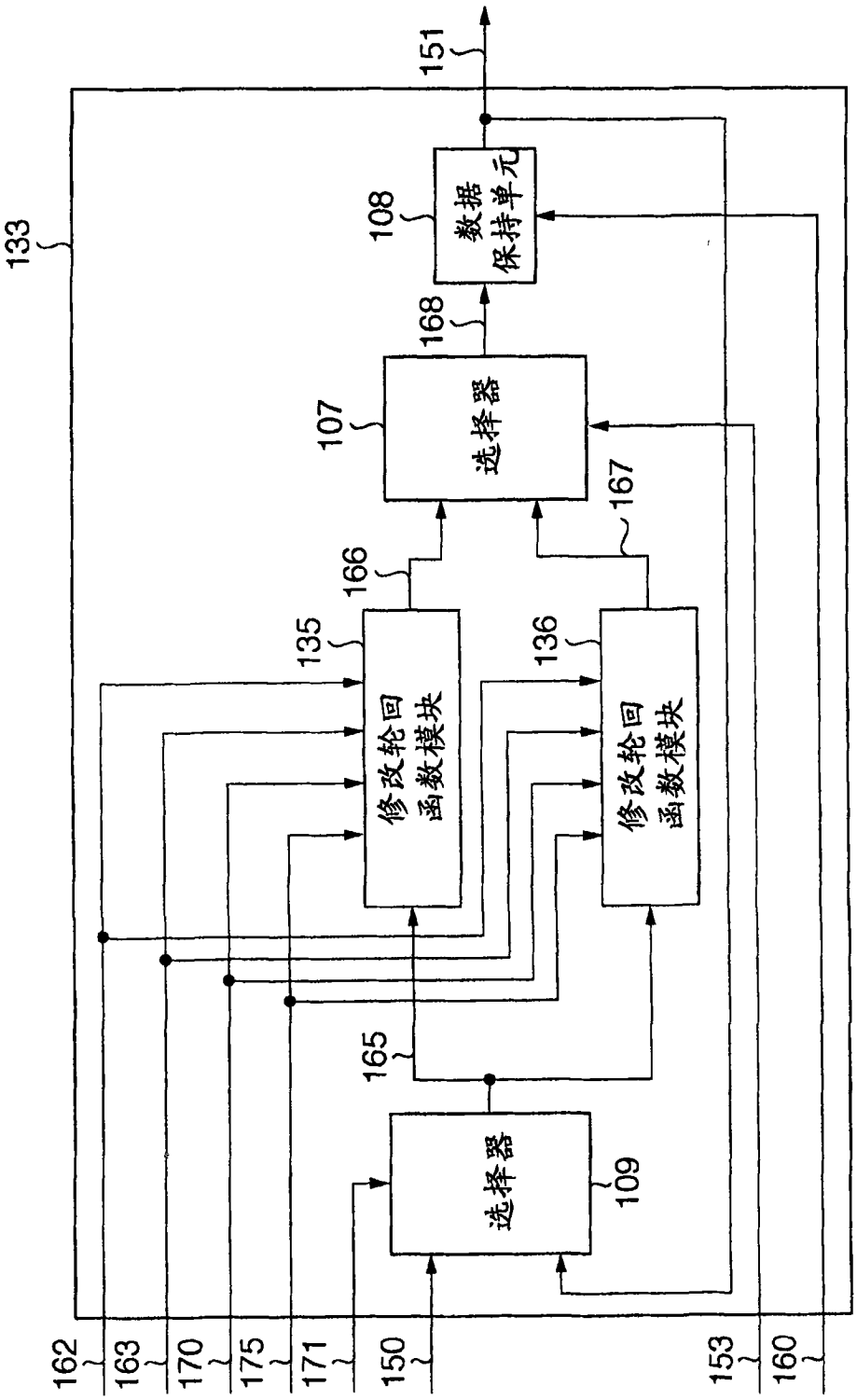

151
133
108
数据保持单元
168
107
选择器
167
166
135
修改轮回函数模块
136
修改轮回函数模块
165
选择器
109
162
163
170
175
171
150
153
160

图15

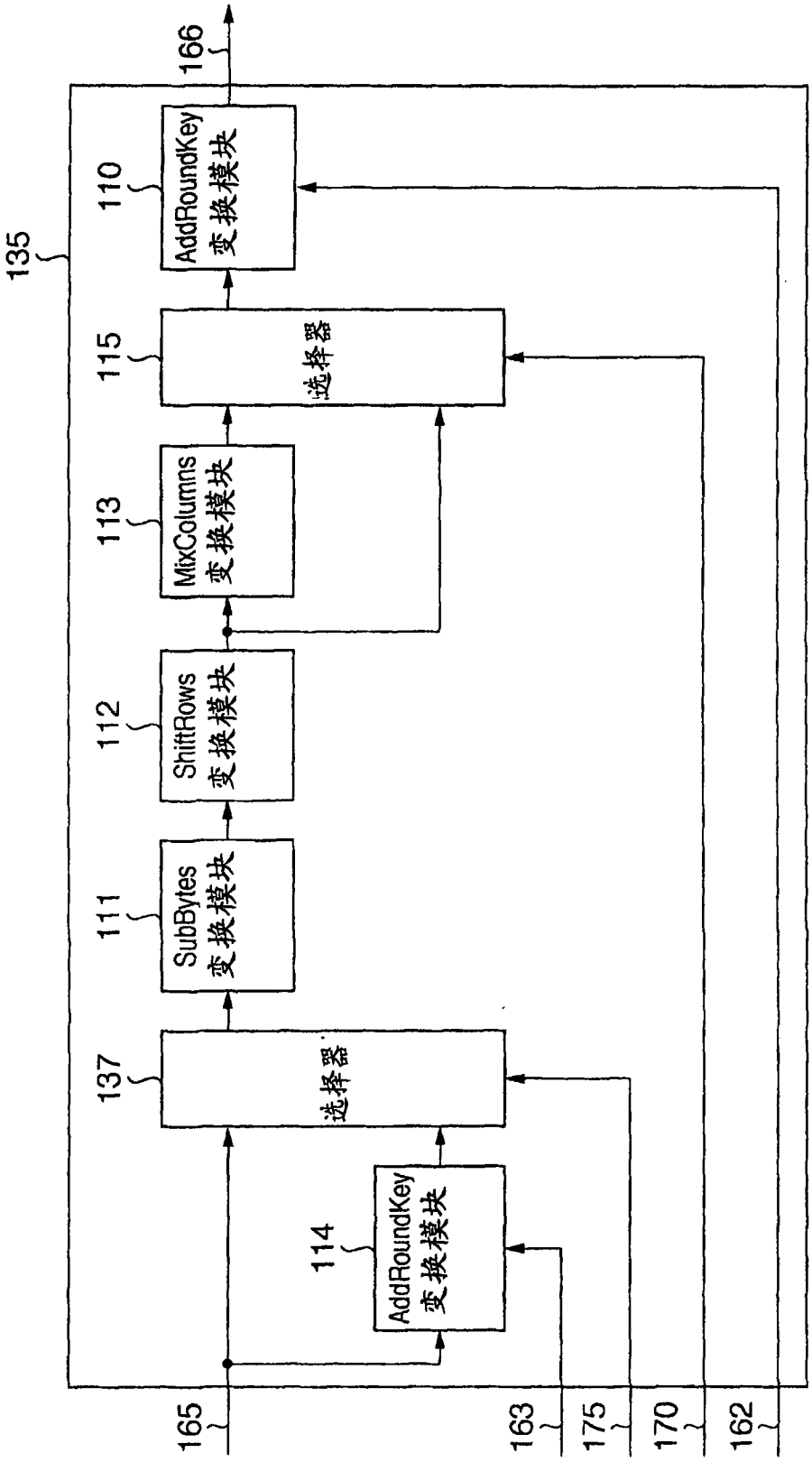

135
166
110
AddRoundKey
变换模块
115
选择器
113
MixColumns
变换模块
112
ShiftRows
变换模块
111
SubBytes
变换模块
137
选择器
114
AddRoundKey
变换模块
165
163
175
170
162

图16

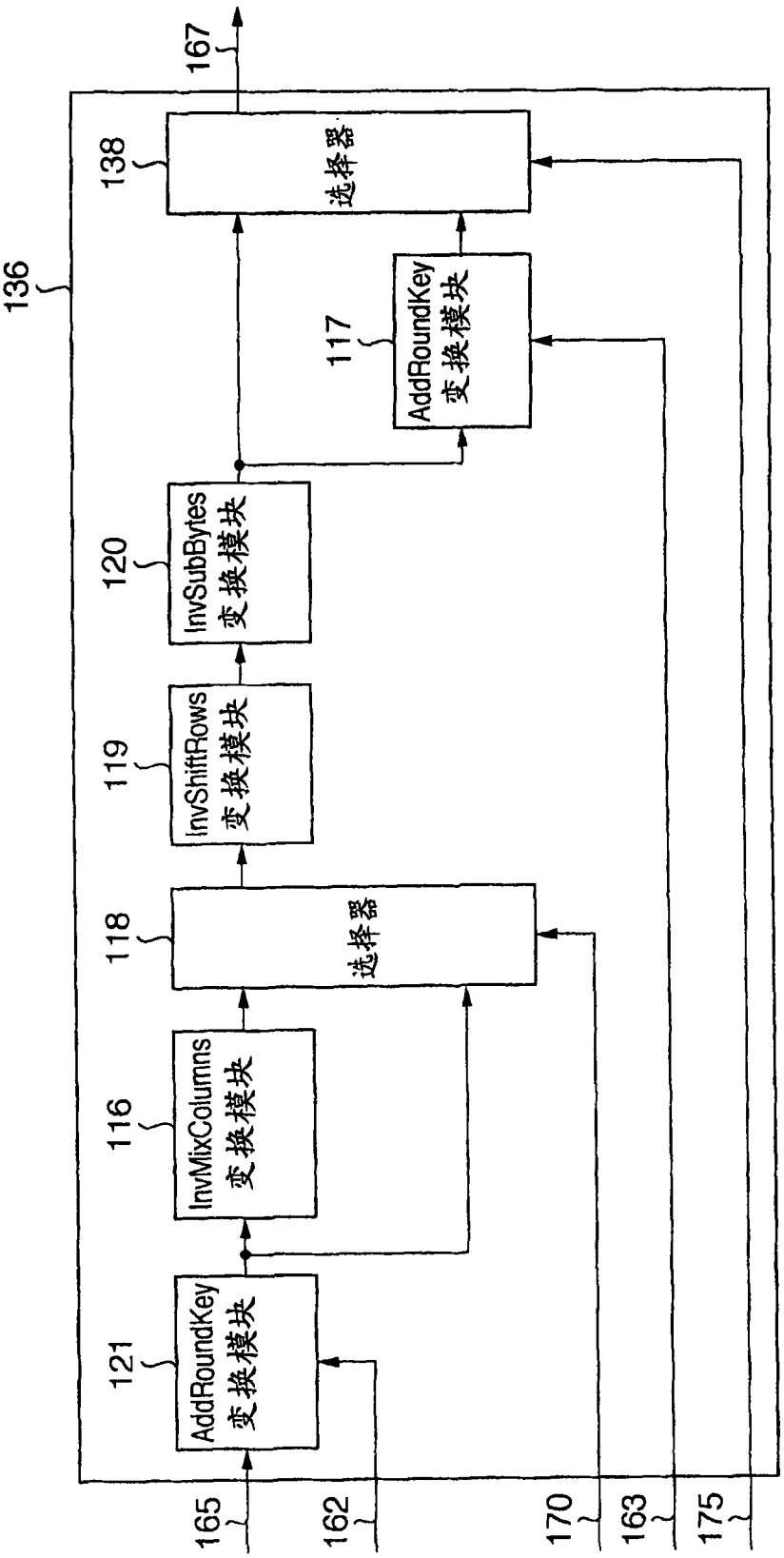

136
167
138
选择器
117
AddRoundKey
变换模块
120
InvSubBytes
变换模块
119
InvShiftRows
变换模块
118
选择器
116
InvMixColumns
变换模块
121
AddRoundKey
变换模块
165
162
170
163
175

图 17

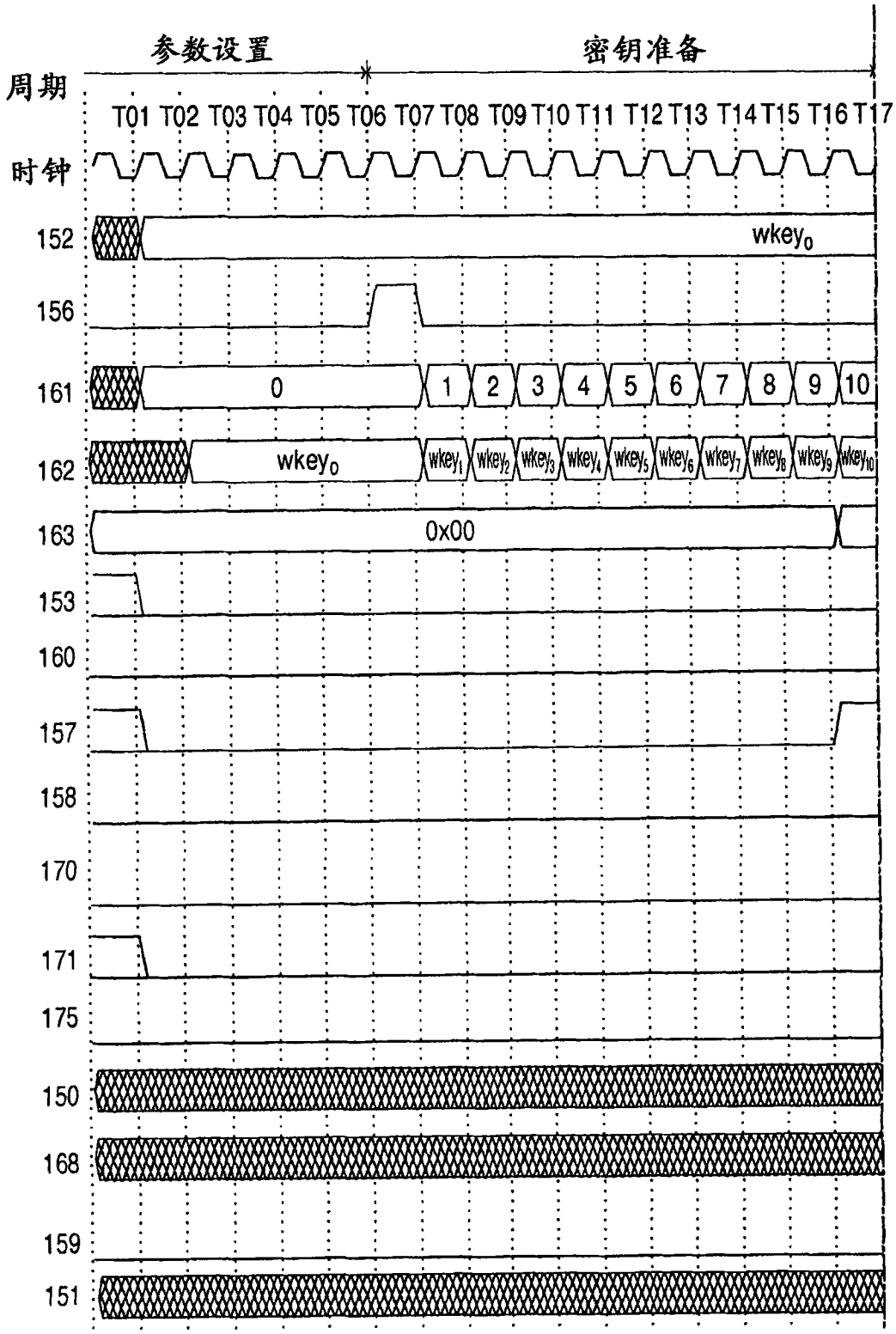

参数设置
密钥准备
周期
T01 T02 T03 T04 T05 T06 T07 T08 T09 T10 T11 T12 T13 T14 T15 T16 T17
时钟
152
wkey0
156
161
0
1 2 3 4 5 6 7 8 9 10
162
wkey0
wkey1 wkey2 wkey3 wkey4 wkey5 wkey6 wkey7 wkey8 wkey9 wkey10
163
0x00
153
160
157
158
170
171
175
150
168
159
151

图 18A

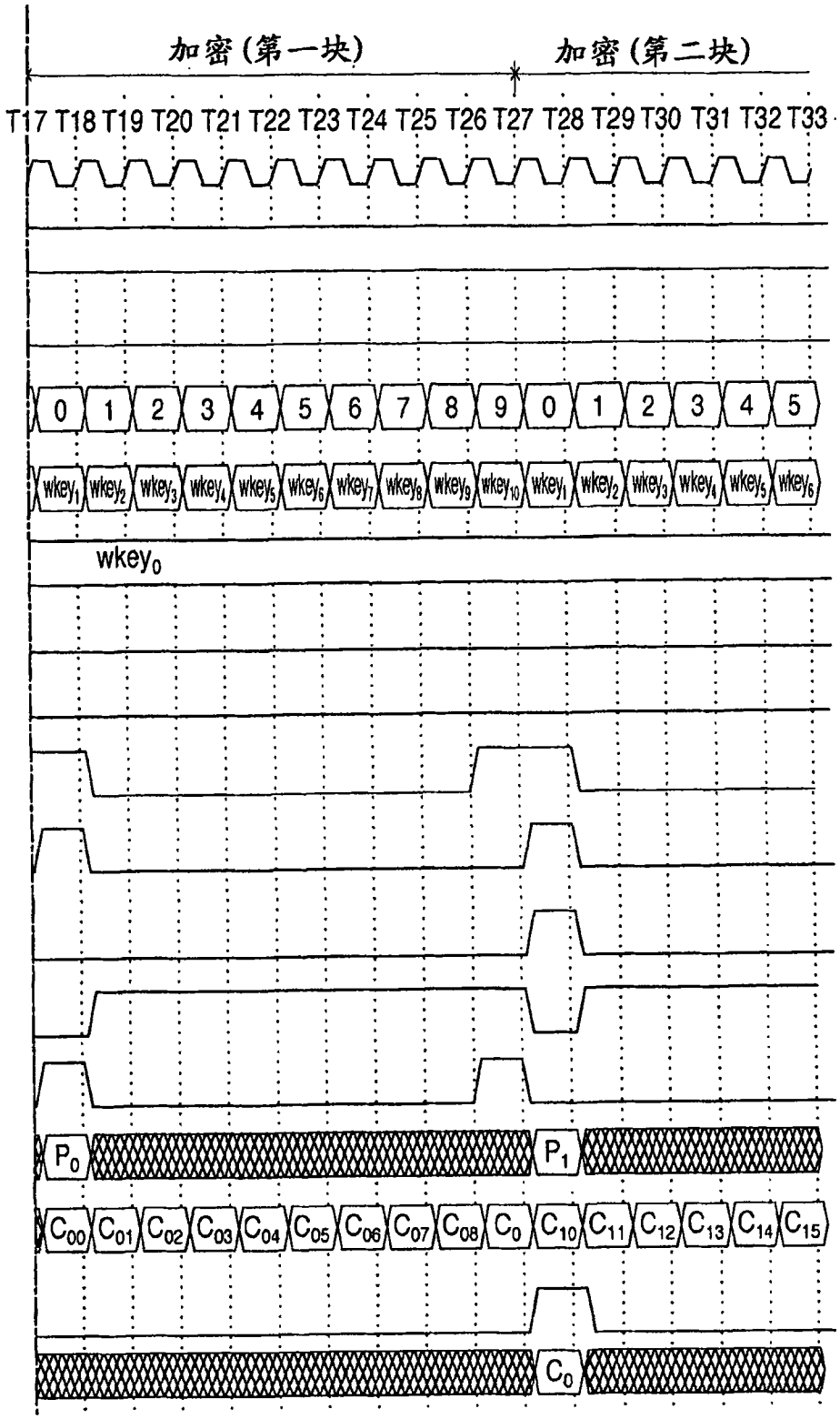

加密(第一块)
加密(第二块)
T17 T18 T19 T20 T21 T22 T23 T24 T25 T26 T27 T28 T29 T30 T31 T32 T33
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
wkey1 wkey2 wkey3 wkey4 wkey5 wkey6 wkey7 wkey8 wkey9 wkey10 wkey1 wkey2 wkey3 wkey4 wkey5 wkey6
wkey0
P0
P1
C00 C01 C02 C03 C04 C05 C06 C07 C08 C0 C10 C11 C12 C13 C14 C15
C0

图 18B

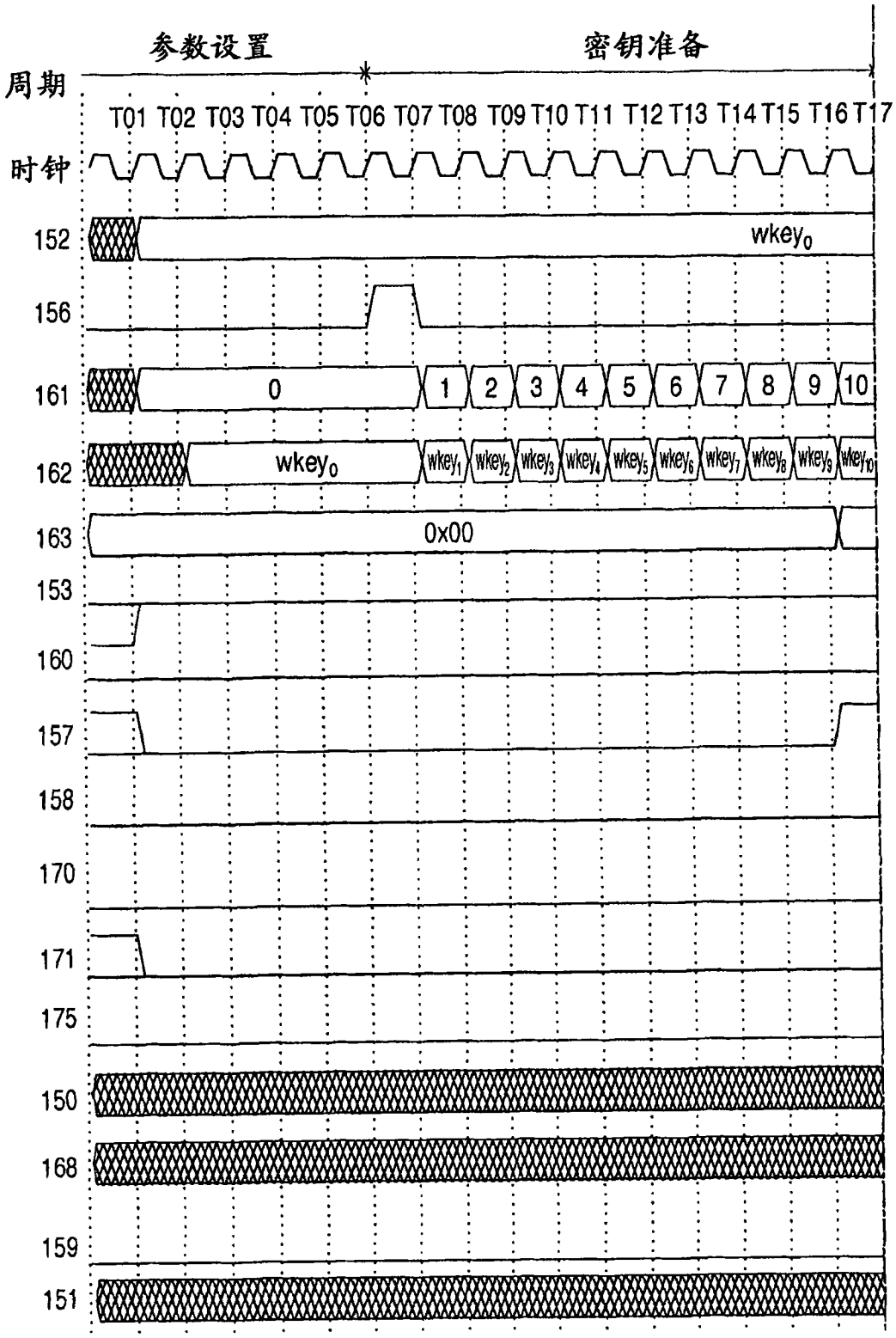

参数设置
密钥准备
周期
T01 T02 T03 T04 T05 T06 T07 T08 T09 T10 T11 T12 T13 T14 T15 T16 T17
时钟
152
wkey0
156
161
0 1 2 3 4 5 6 7 8 9 10
162
wkey0 wkey1 wkey2 wkey3 wkey4 wkey5 wkey6 wkey7 wkey8 wkey9 wkey10
163
0x00
153
160
157
158
170
171
175
150
168
159
151

图 19A

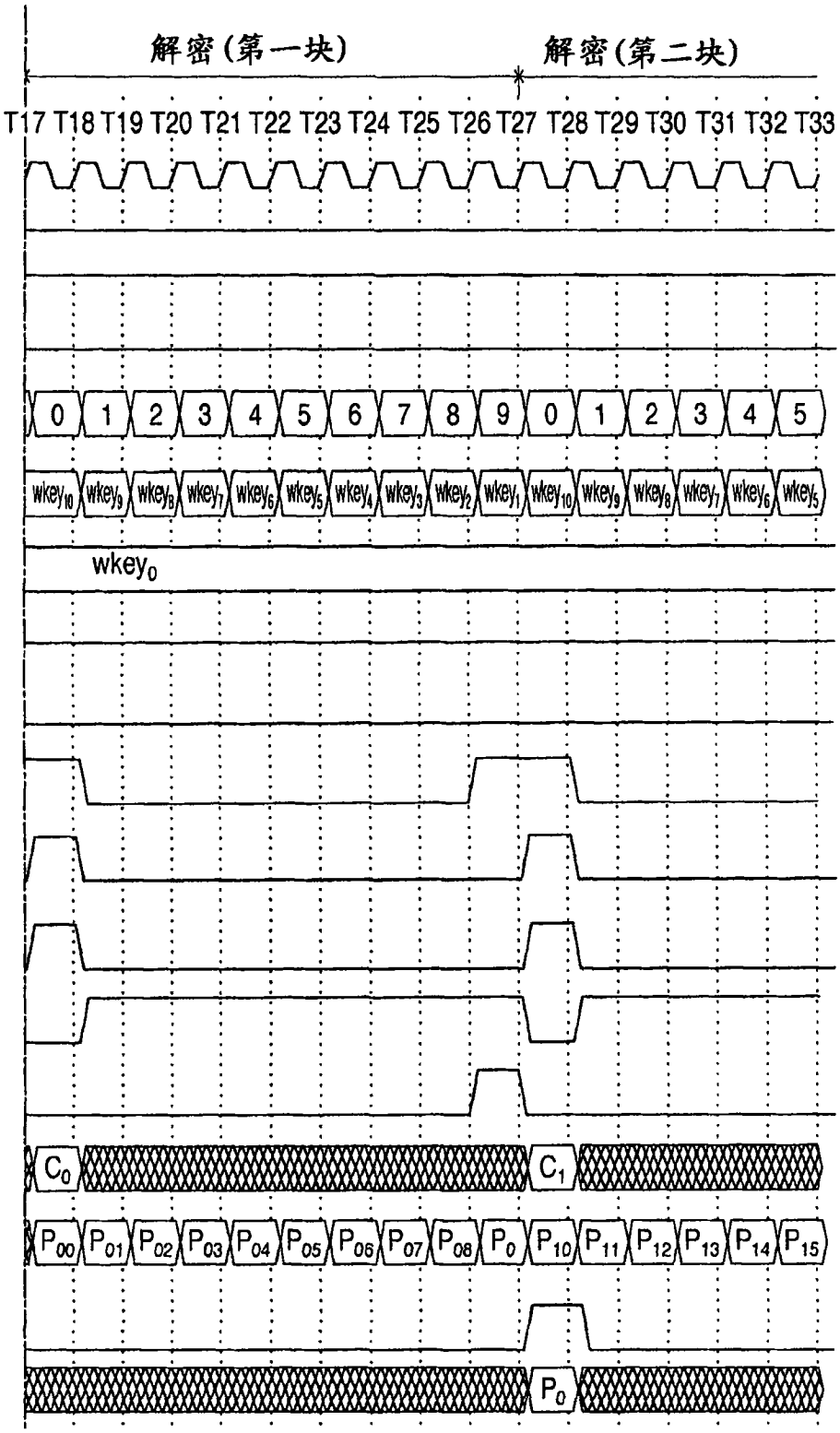

解密(第一块)
解密(第二块)
T17 T18 T19 T20 T21 T22 T23 T24 T25 T26 T27 T28 T29 T30 T31 T32 T33
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
wkey10 wkey9 wkey8 wkey7 wkey6 wkey5 wkey4 wkey3 wkey2 wkey1 wkey10 wkey9 wkey8 wkey7 wkey6 wkey5
wkey0
C0
C1
P00 P01 P02 P03 P04 P05 P06 P07 P08 P0 P10 P11 P12 P13 P14 P15
P0

图 19B

从处理开始的时钟周期号	加密处理		解密处理	
	要执行的处理	要使用的轮回密钥	要执行的处理	要使用的轮回密钥
0	· AddRoundKey · SubBytes · ShiftRows	· 第0轮回密钥($wkey_0$)	· AddRoundKey · InvShiftRows · InvSubBytes · AddRoundKey · InvMixColumns	· 第10轮回密钥($wkey_{10}$) · 第9轮回密钥($wkey_9$)
1	· MixColumns · AddRoundKey · SubBytes · ShiftRows	· 第1轮回密钥($wkey_1$)	· InvShiftRows · InvSubBytes · AddRoundKey · InvMixColumns	· 第8轮回密钥($wkey_8$)
8	· MixColumns · AddRoundKey · SubBytes · ShiftRows	· 第8轮回密钥($wkey_8$)	· InvShiftRows · InvSubBytes · AddRoundKey · InvMixColumns	· 第1轮回密钥($wkey_1$)
9	· MixColumns · AddRoundKey · SubBytes · ShiftRows · AddRoundKey	· 第9轮回密钥($wkey_9$) · 第10轮回密钥($wkey_{10}$)	· InvShiftRows · InvSubBytes · AddRoundKey	· 第0轮回密钥($wkey_0$)

图 20

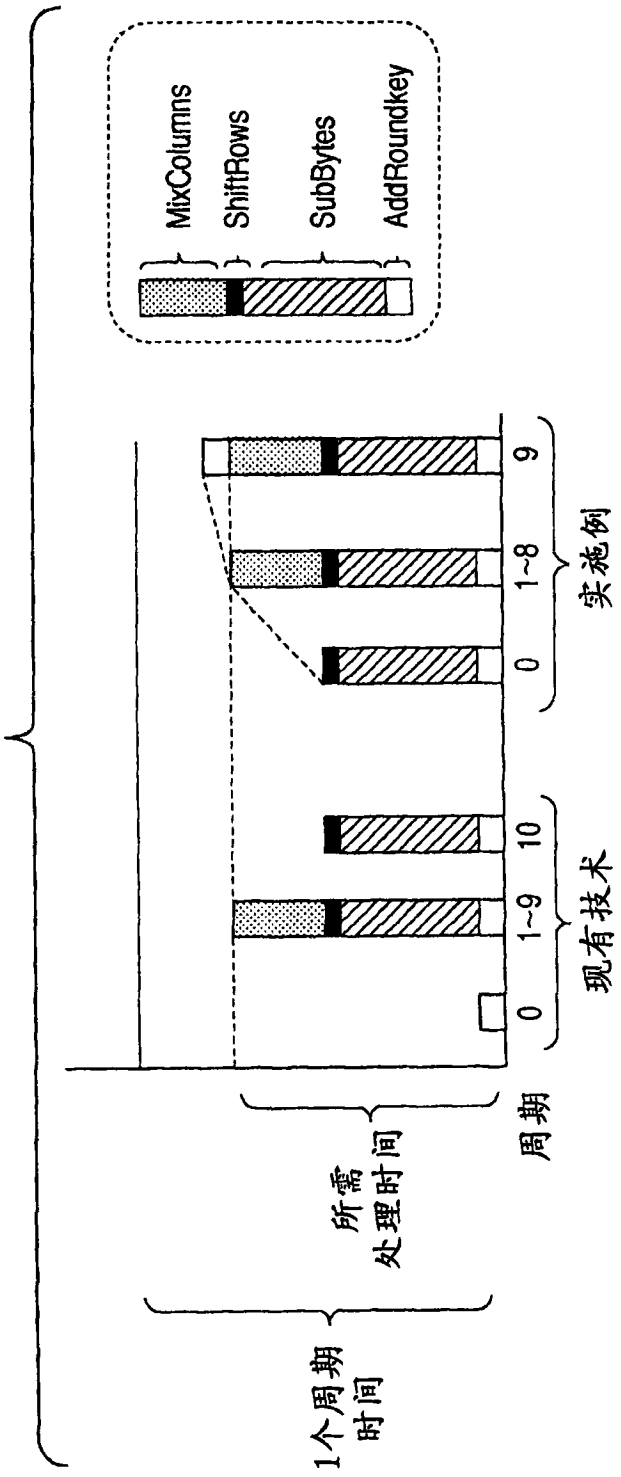

MixColumns
ShiftRows
SubBytes
AddRoundkey
1个周期时间
所需处理时间
周期
0
1~9
10
现有技术
0
1~8
9
实施例

图21

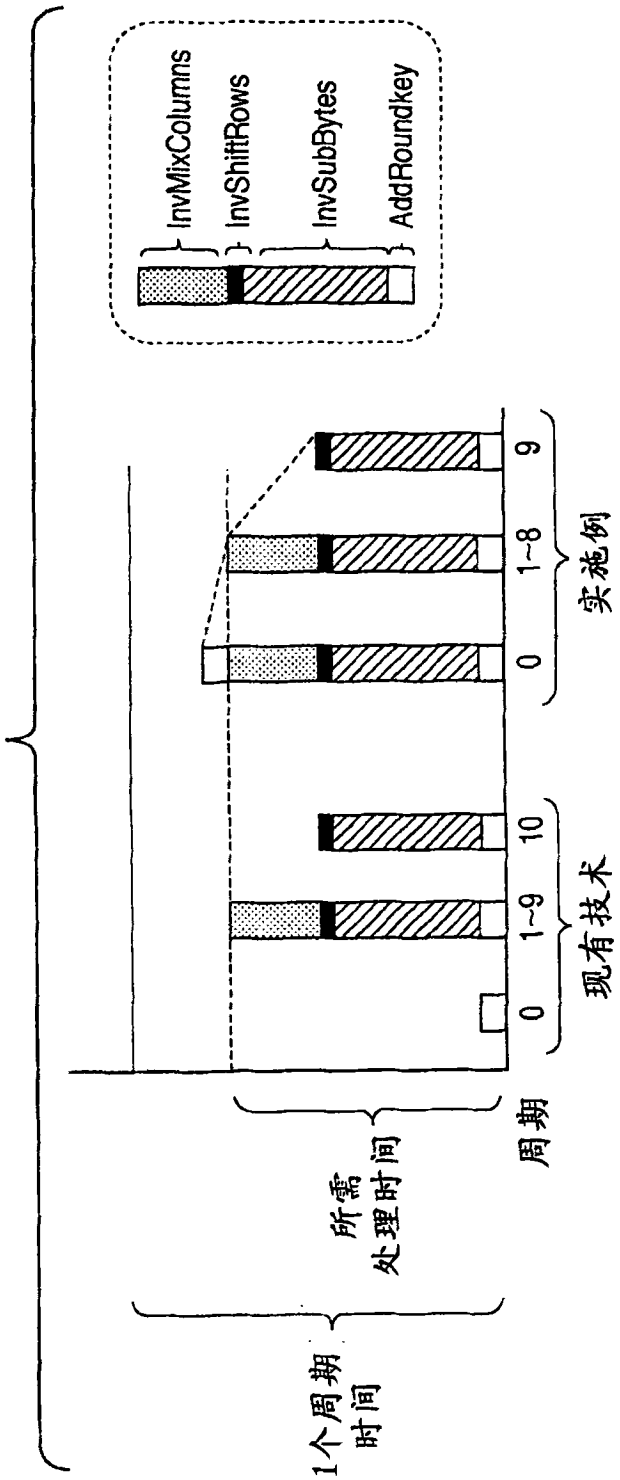

InvMixColumns
InvShiftRows
InvSubBytes
AddRoundkey
1个周期时间
所需处理时间
周期
0
1~9
10
现有技术
0
1~8
9
实施例

图22

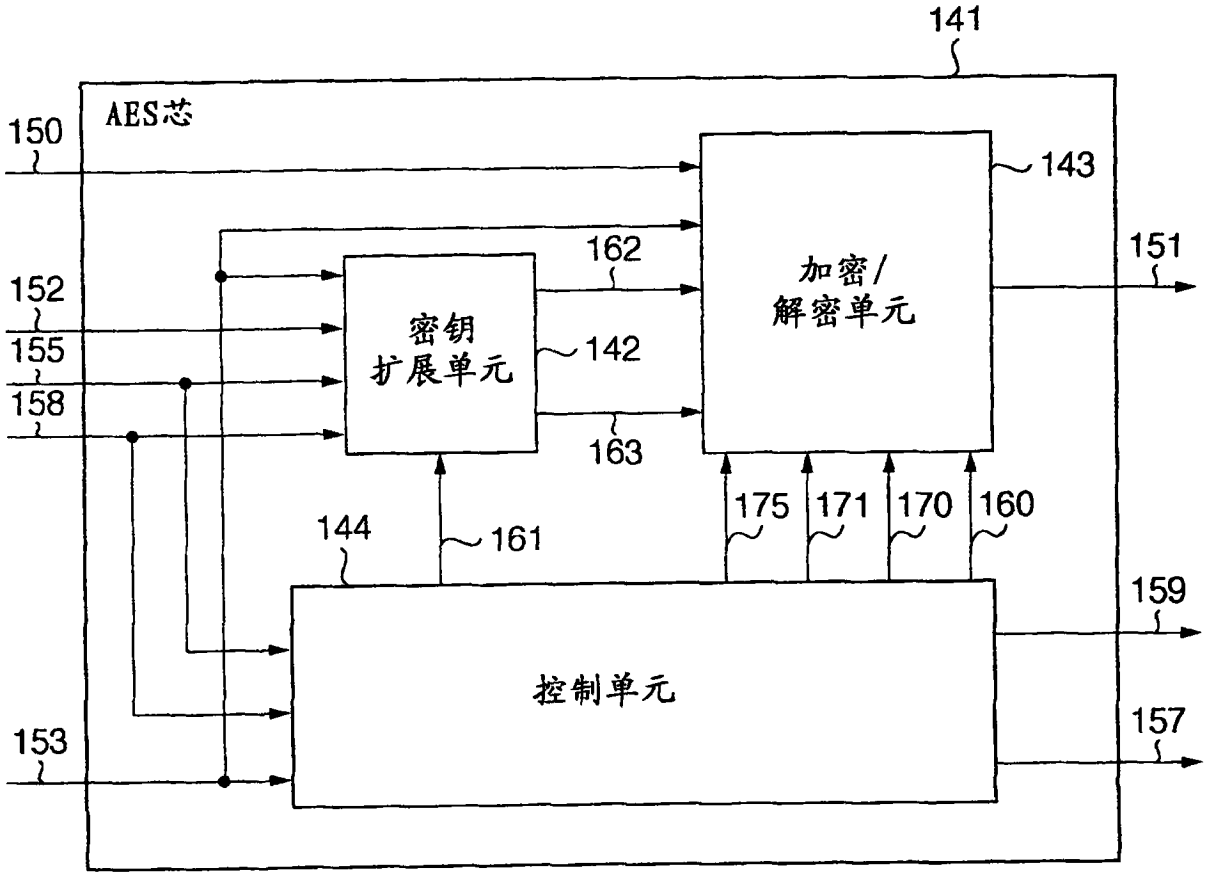

141
AES芯
150
143
162
151
152
密钥
扩展单元
加密/
解密单元
155
142
158
163
175
171
170
160
144
161
159
控制单元
153
157

图23

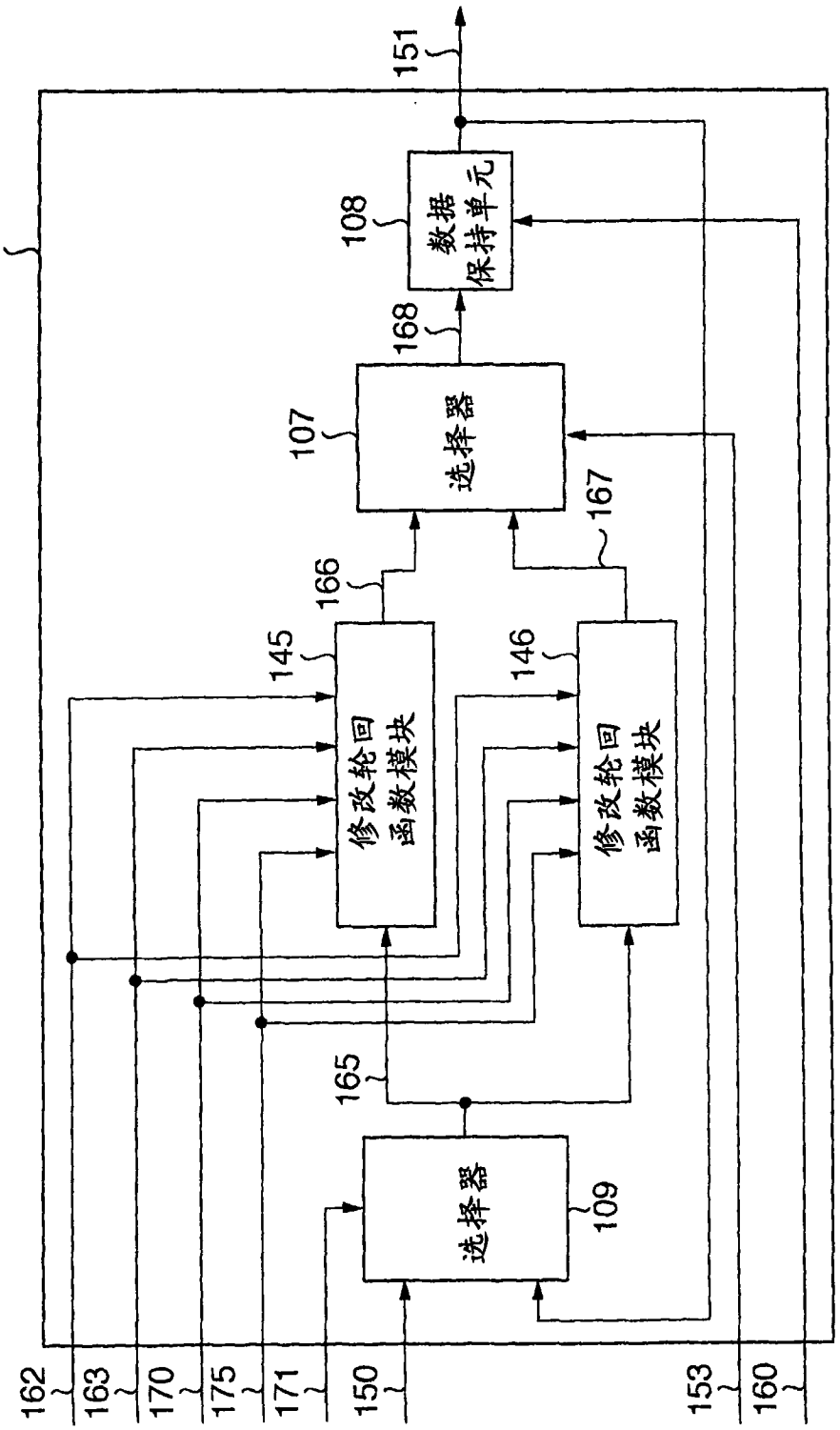

143
151
108
数据保持单元
168
107
选择器
167
166
145
修改轮回函数模块
146
修改轮回函数模块
165
选择器
109
162
163
170
175
171
150
153
160

图 24

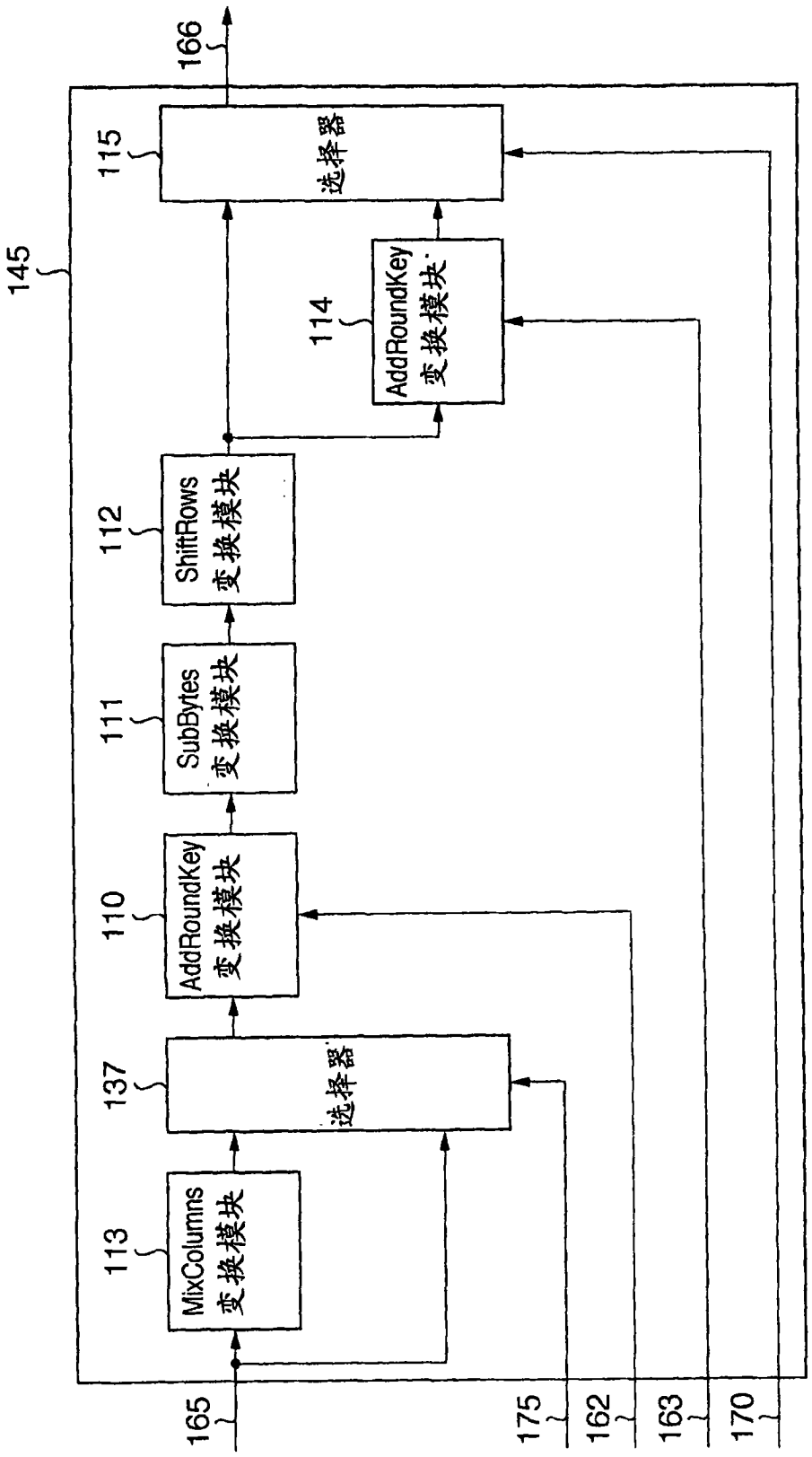

145
166
115
选择器
114
AddRoundKey
变换模块
112
ShiftRows
变换模块
111
SubBytes
变换模块
110
AddRoundKey
变换模块
137
选择器
113
MixColumns
变换模块
165
175
162
163
170

图 25

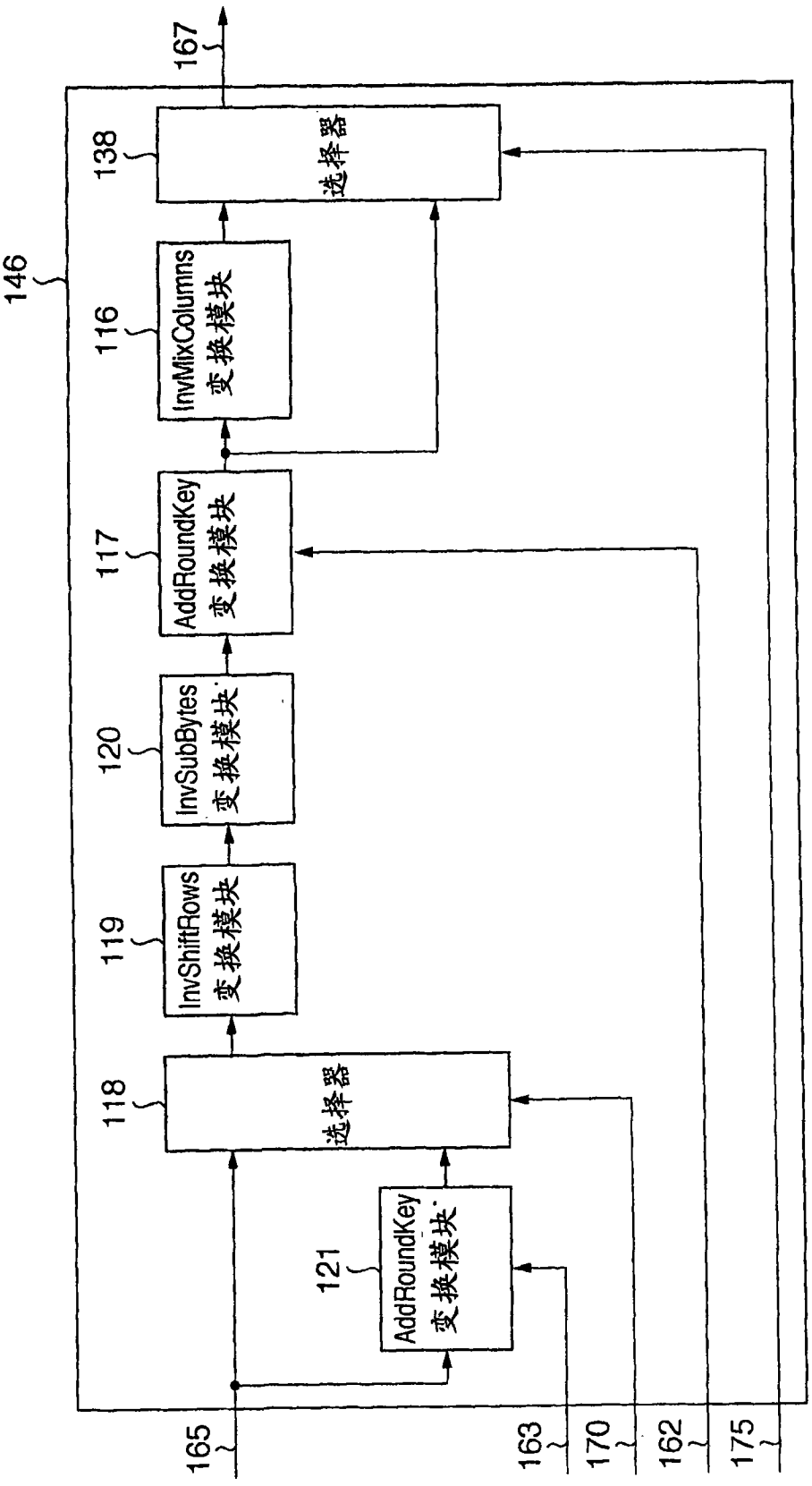

146
165
163
170
162
175
167
138
选择器
116
InvMixColumns
变换模块
117
AddRoundKey
变换模块
120
InvSubBytes
变换模块
119
InvShiftRows
变换模块
118
选择器
121
AddRoundKey
变换模块

图 26

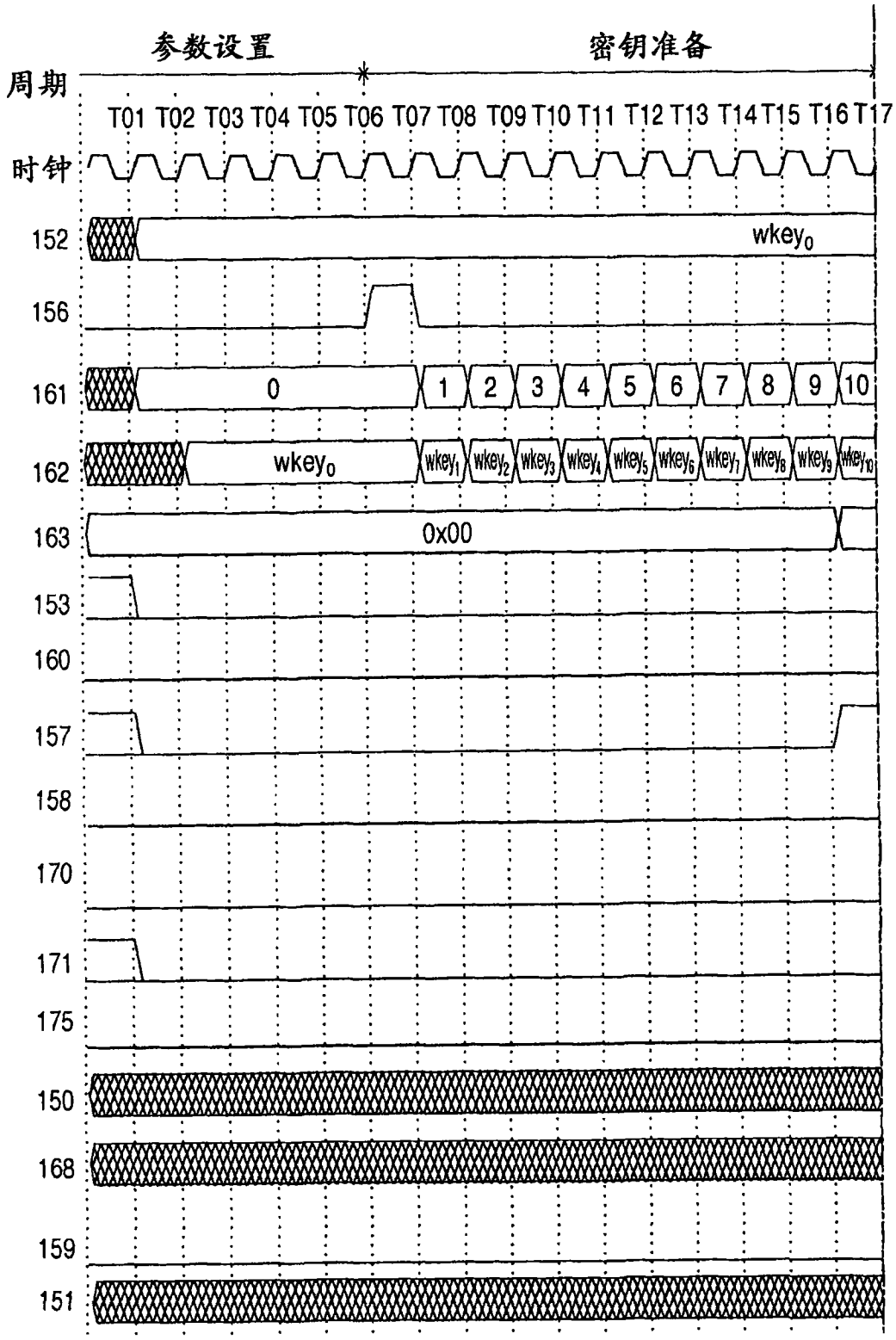

参数设置
密钥准备
周期
T01 T02 T03 T04 T05 T06 T07 T08 T09 T10 T11 T12 T13 T14 T15 T16 T17
时钟
152
wkey0
156
161
0 1 2 3 4 5 6 7 8 9 10
162
wkey0 wkey1 wkey2 wkey3 wkey4 wkey5 wkey6 wkey7 wkey8 wkey9 wkey10
163
0x00
153
160
157
158
170
171
175
150
168
159
151

图 27A

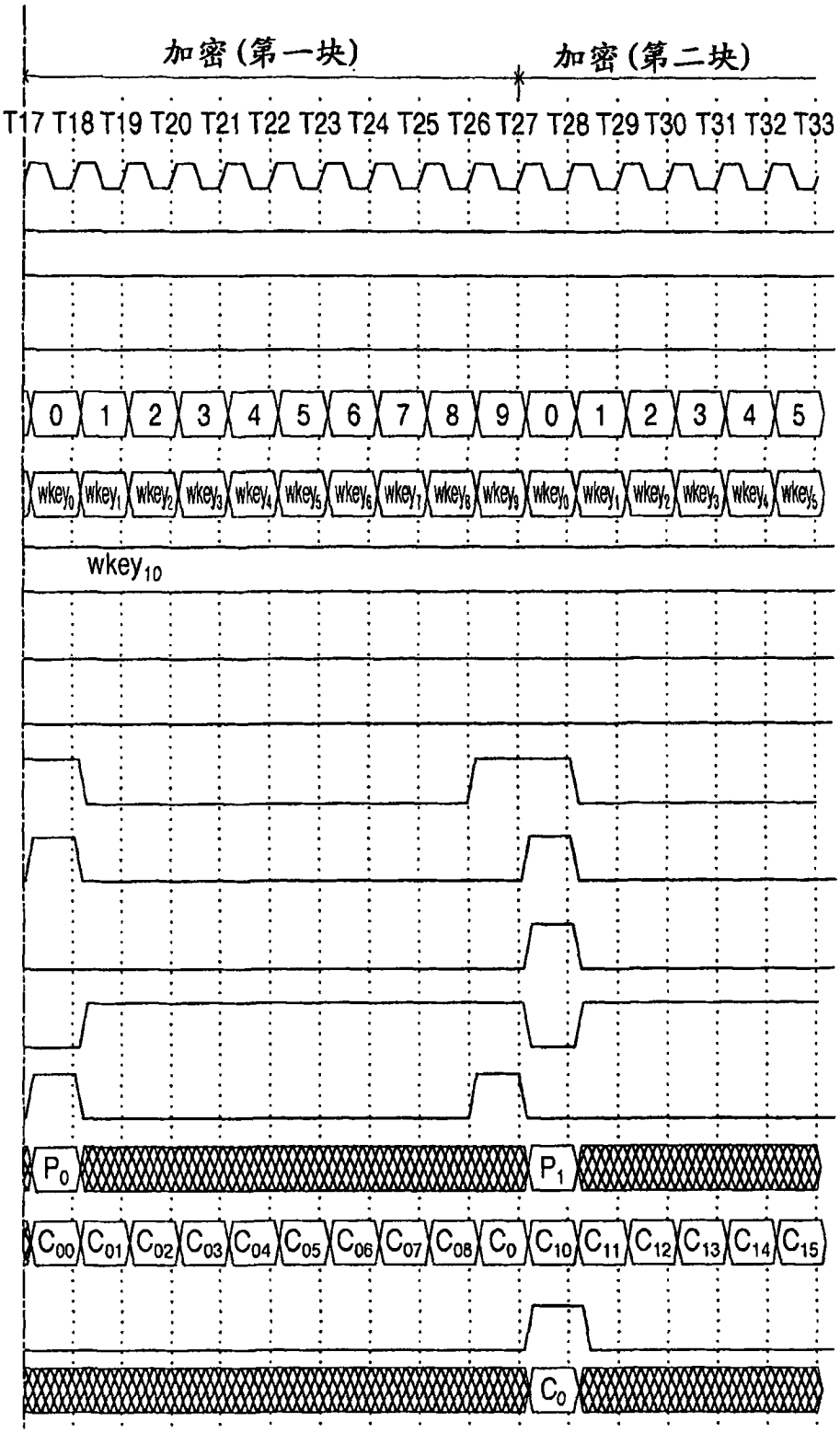

加密(第一块)
加密(第二块)
T17 T18 T19 T20 T21 T22 T23 T24 T25 T26 T27 T28 T29 T30 T31 T32 T33
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
wkey0 wkey1 wkey2 wkey3 wkey4 wkey5 wkey6 wkey7 wkey8 wkey9 wkey0 wkey1 wkey2 wkey3 wkey4 wkey5
wkey10
P0 P1
C00 C01 C02 C03 C04 C05 C06 C07 C08 C0 C10 C11 C12 C13 C14 C15
C0

图 27B

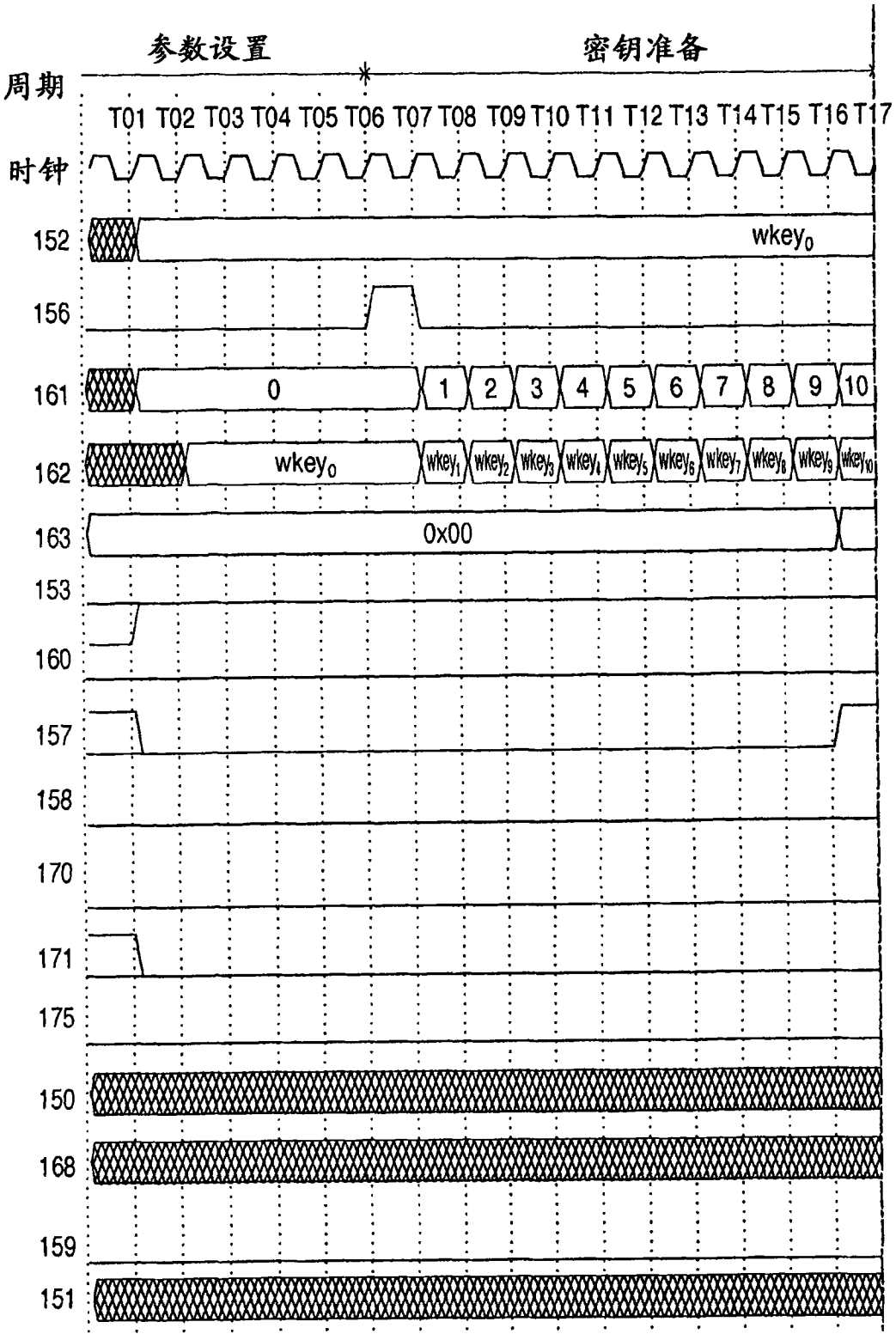

参数设置
密钥准备
周期
T01 T02 T03 T04 T05 T06 T07 T08 T09 T10 T11 T12 T13 T14 T15 T16 T17
时钟
152
wkey0
156
161
0 1 2 3 4 5 6 7 8 9 10
162
wkey0 wkey1 wkey2 wkey3 wkey4 wkey5 wkey6 wkey7 wkey8 wkey9 wkey10
163
0x00
153
160
157
158
170
171
175
150
168
159
151

图 28A

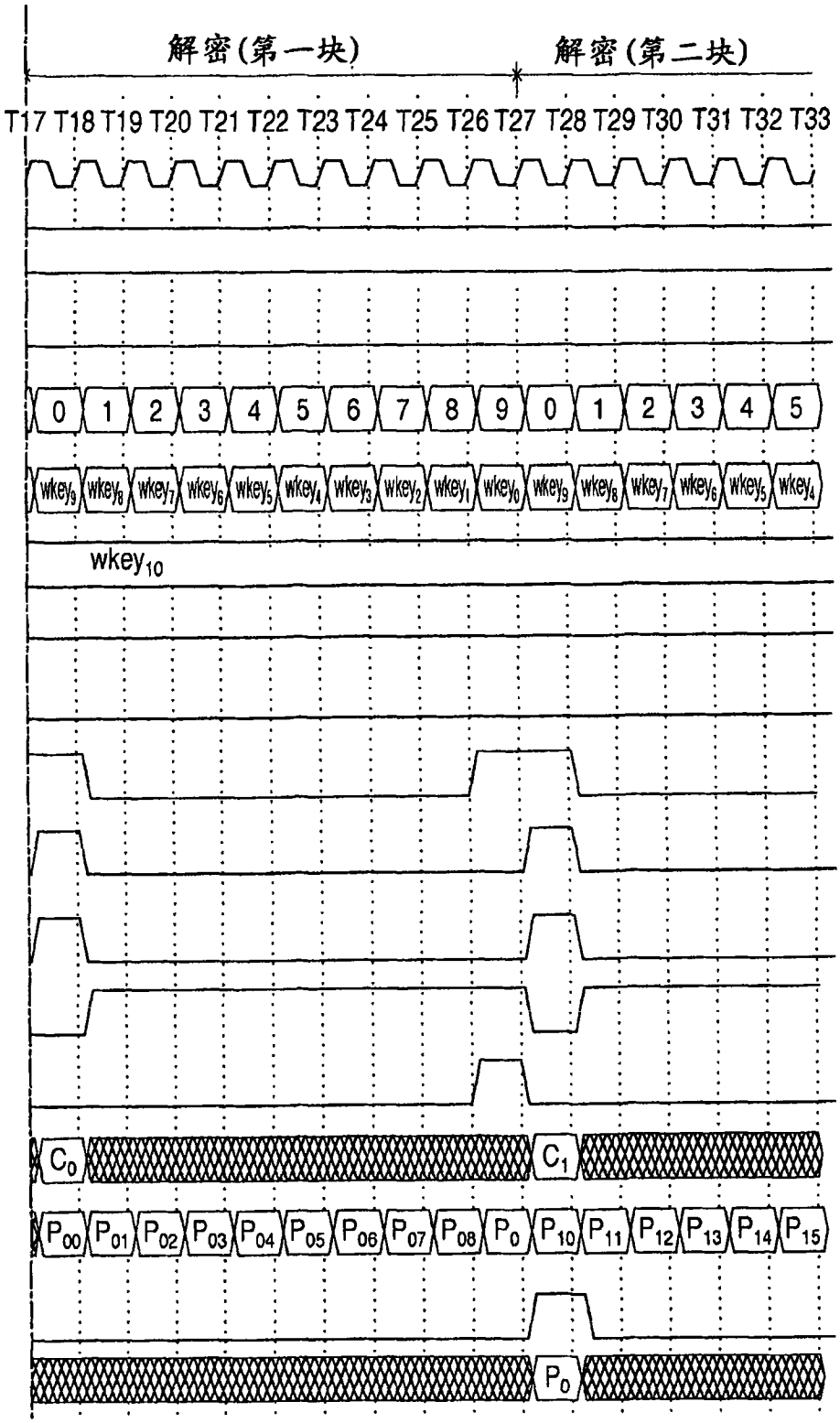

解密(第一块)
解密(第二块)
T17 T18 T19 T20 T21 T22 T23 T24 T25 T26 T27 T28 T29 T30 T31 T32 T33
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
wkey9 wkey8 wkey7 wkey6 wkey5 wkey4 wkey3 wkey2 wkey1 wkey0 wkey9 wkey8 wkey7 wkey6 wkey5 wkey4
wkey10
C0
C1
P00 P01 P02 P03 P04 P05 P06 P07 P08 P0 P10 P11 P12 P13 P14 P15
P0

图 28B

周期号	现有技术		第四实施例	
	要执行的处理	要使用的轮回密钥	要执行的处理	要使用的轮回密钥
0	· AddRoundKey	· 第0轮回密钥($wkey_0$)	· AddRoundKey · SubBytes · ShiftRows · MixColumns	· 第0轮回密钥($wkey_0$)
1	· SubBytes · ShiftRows · MixColumns · AddRoundKey	· 第1轮回密钥($wkey_1$)	· AddRoundKey · SubBytes · ShiftRows · MixColumns	· 第1轮回密钥($wkey_1$)
8	· SubBytes · ShiftRows · MixColumns · AddRoundKey	· 第8轮回密钥($wkey_8$)	· AddRoundKey · SubBytes · ShiftRows · MixColumns	· 第8轮回密钥($wkey_8$)
9	· SubBytes · ShiftRows · MixColumns · AddRoundKey	· 第9轮回密钥($wkey_9$)	· AddRoundKey · SubBytes · ShiftRows · AddRoundKey	· 第9轮回密钥($wkey_9$) · 第10轮回密钥($wkey_{10}$)
10	· SubBytes · ShiftRows · AddRoundKey	· 第10轮回密钥($wkey_{10}$)		

图 29

周期号	现有技术		第四实施例	
	要执行的处理	要使用的轮回密钥	要执行的处理	要使用的轮回密钥
0	· AddRoundKey	· 第10轮回密钥($wkey_{10}$)	· AddRoundKey · InvSubBytes · InvShiftRows · InvMixColumns	· 第10轮回密钥($wkey_{10}$)
1	· InvSubBytes · InvShiftRows · InvMixColumns · AddRoundKey	· 第九修改解密密钥($wkey_9'$)	· AddRoundKey · InvSubBytes · InvShiftRows · InvMixColumns	· 第九修改解密密钥($wkey_9'$)
8	· InvSubBytes · InvShiftRows · InvMixColumns · AddRoundKey	· 第二修改解密密钥($wkey_2'$)	· AddRoundKey · InvSubBytes · InvShiftRows · InvMixColumns	· 第二修改解密密钥($wkey_2'$)
9	· InvSubBytes · InvShiftRows · InvMixColumns · AddRoundKey	· 第一修改解密密钥($wkey_1'$)	· AddRoundKey · InvSubBytes · InvShiftRows · AddRoundKey	· 第一修改解密密钥($wkey_1'$) · 第0轮回密钥($wkey_0$)
10	· InvSubBytes · InvShiftRows · AddRoundKey	· 第0轮回密钥($wkey_0$)		

图 30

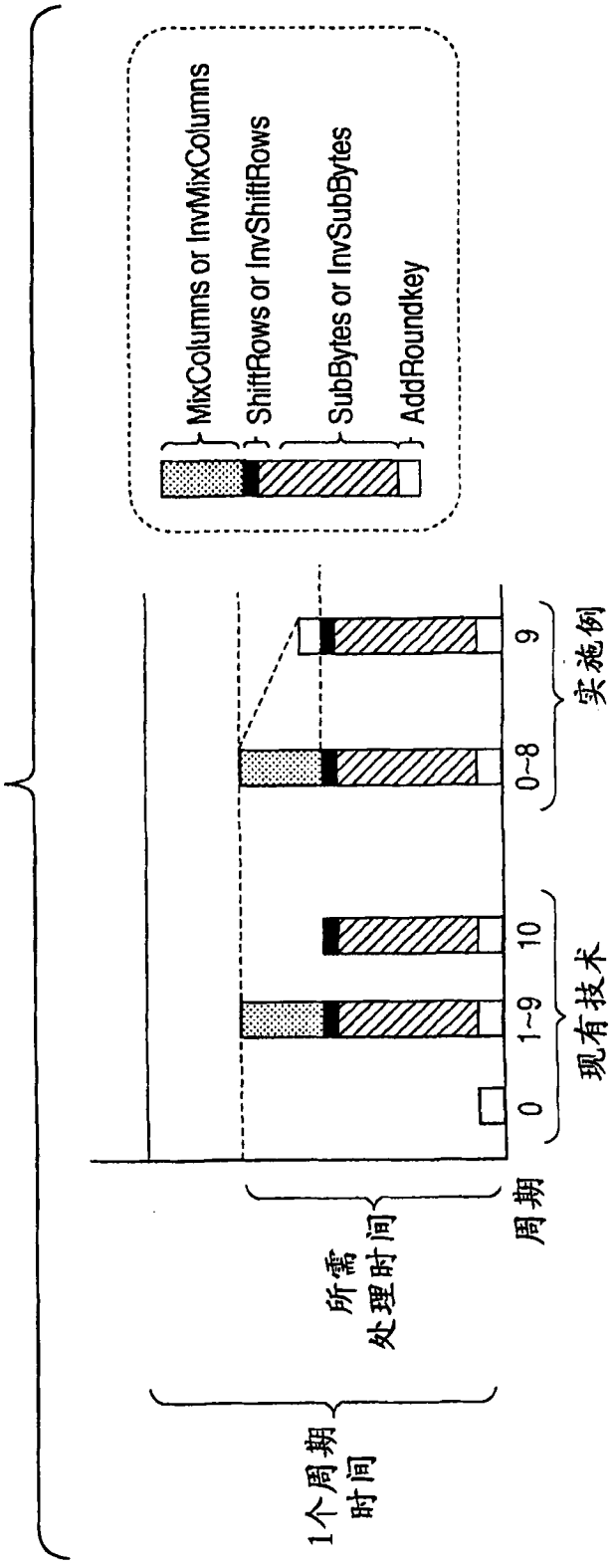

MixColumns or InvMixColumns
ShiftRows or InvShiftRows
SubBytes or InvSubBytes
AddRoundkey
1个周期时间
所需处理时间
周期
0
1~9
10
0~8
9
现有技术
实施例

图31

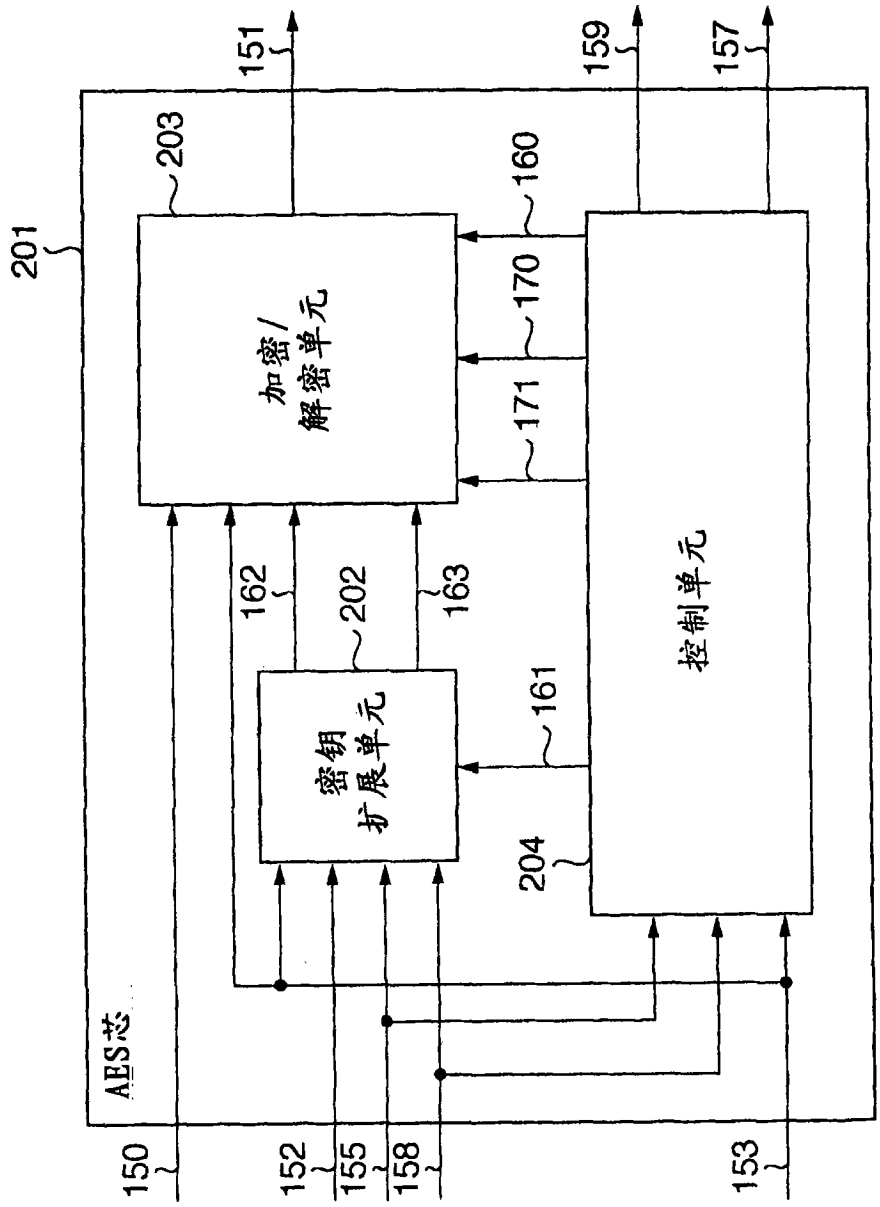

AES芯
201
203
加密/
解密单元
密钥
扩展单元
控制单元
150
151
152
153
155
157
158
159
160
161
162
163
170
171
202
204

图 32

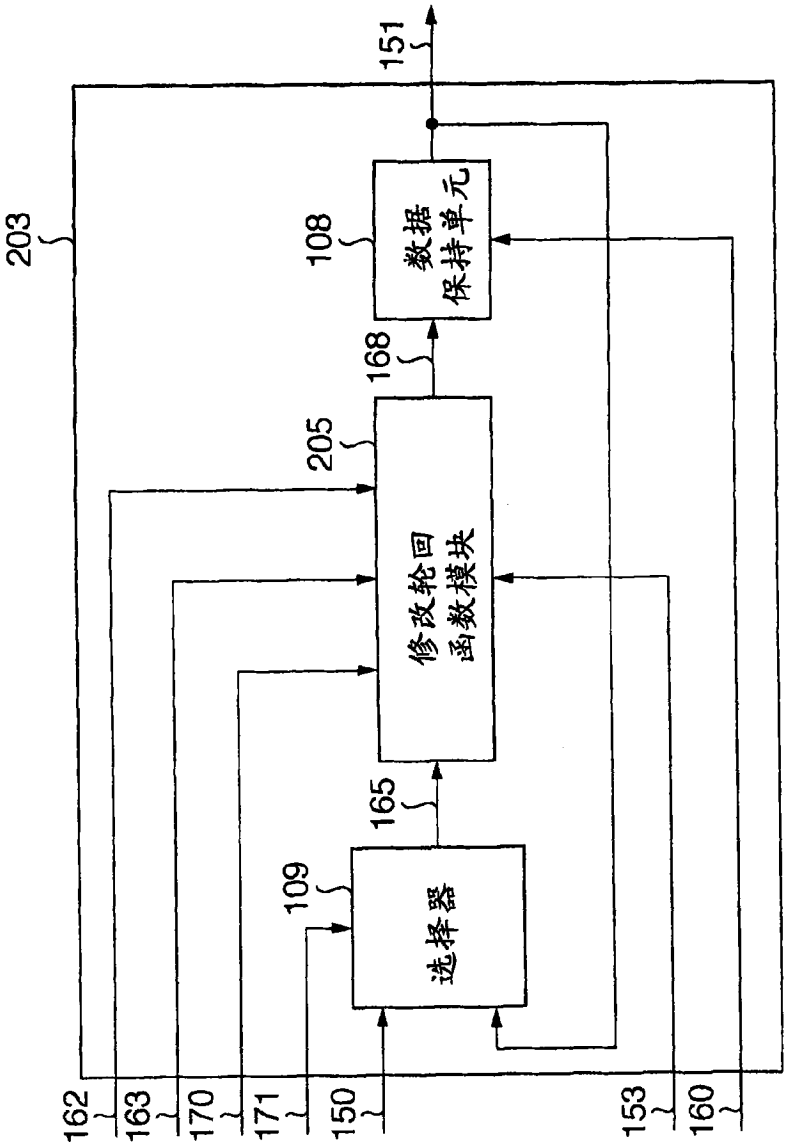

151
203
108
数据保持单元
168
205
修改轮回函数模块
165
109
选择器
162
163
170
171
150
153
160

图 33

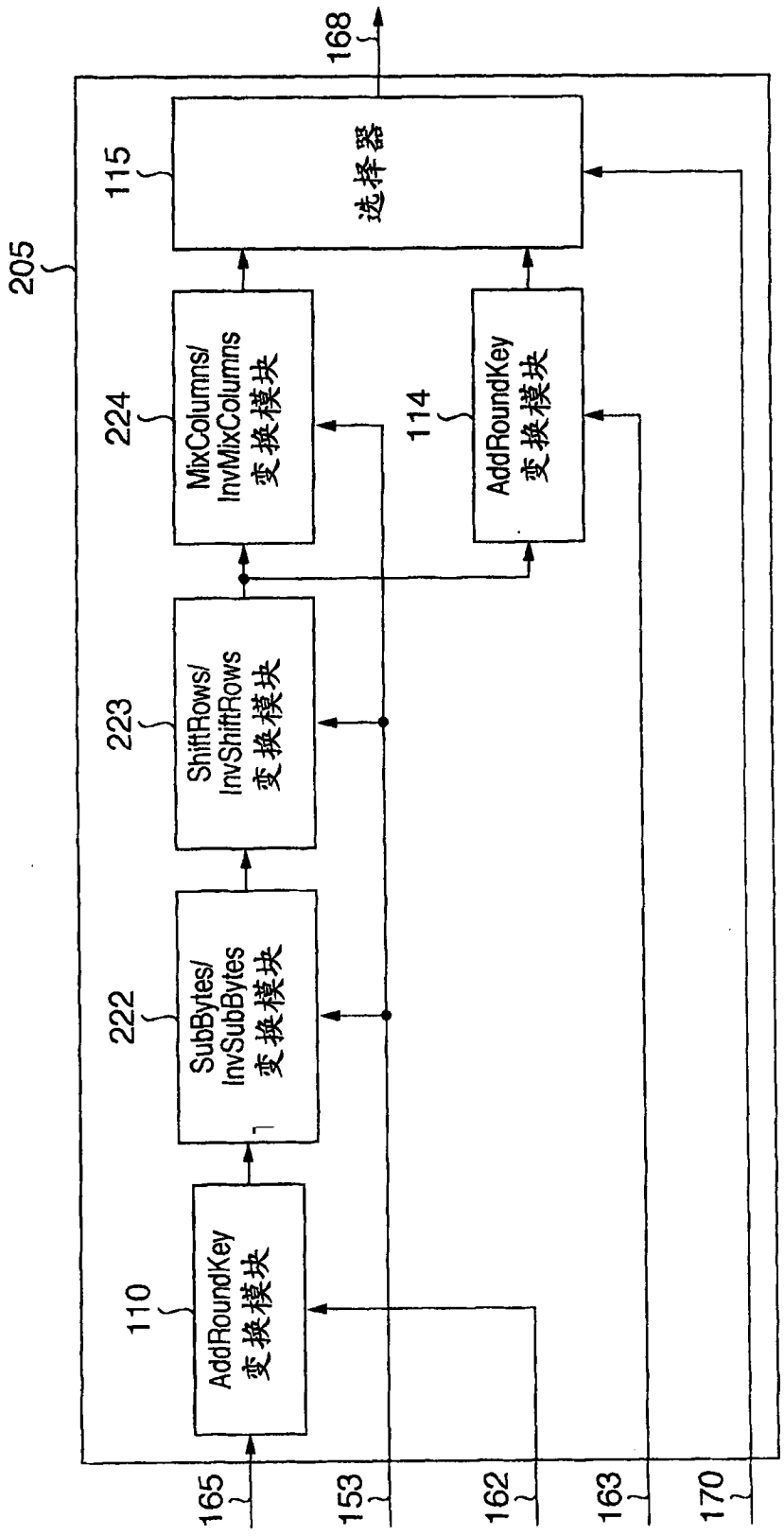

168
115
选择器
205
224
MixColumns/
InvMixColumns
变换模块
114
AddRoundKey
变换模块
223
ShiftRows/
InvShiftRows
变换模块
222
SubBytes/
InvSubBytes
变换模块
110
AddRoundKey
变换模块
165
153
162
163
170

图 34

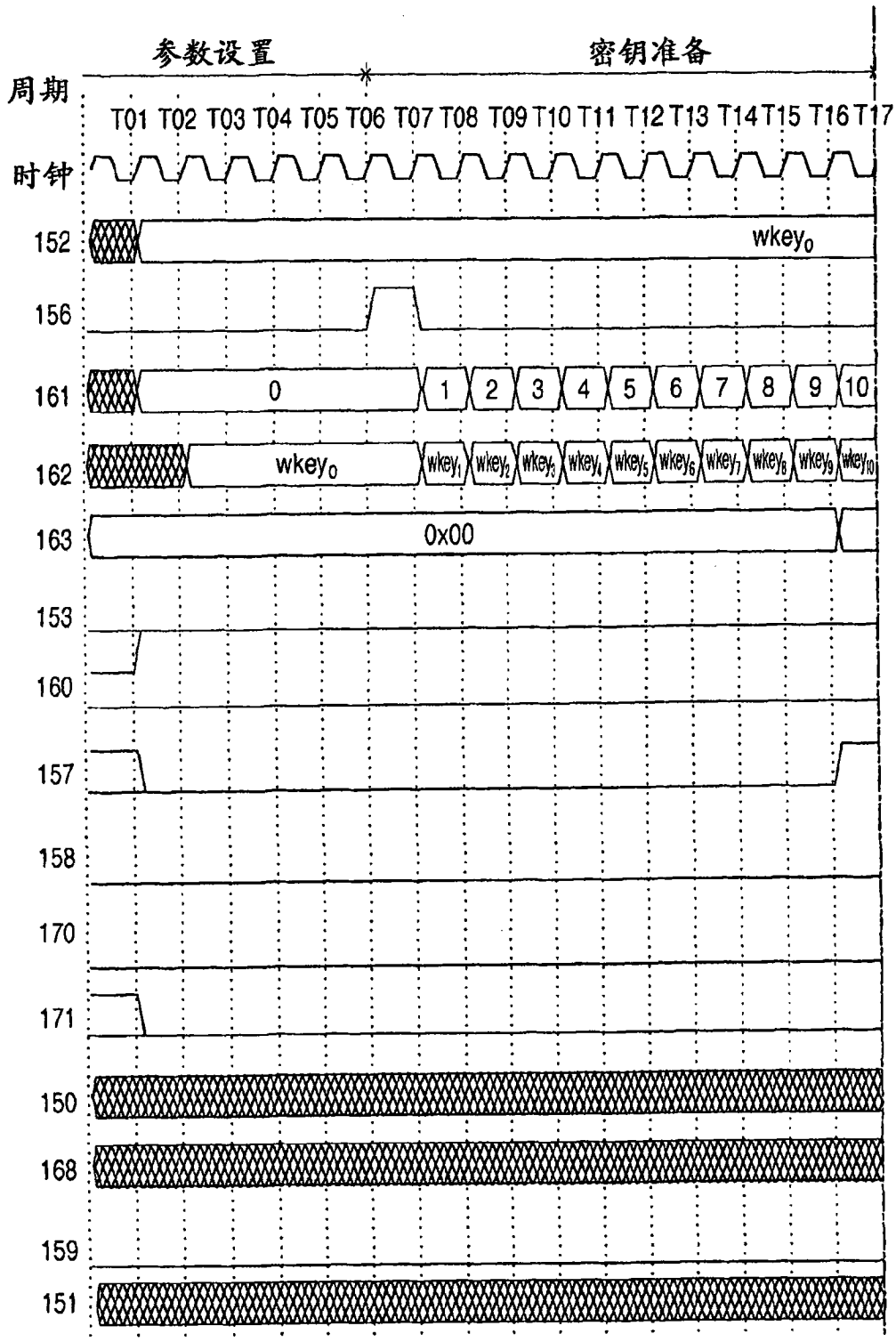

参数设置
密钥准备
周期
T01 T02 T03 T04 T05 T06 T07 T08 T09 T10 T11 T12 T13 T14 T15 T16 T17
时钟
152
wkey0
156
161
0
1 2 3 4 5 6 7 8 9 10
162
wkey0
wkey1 wkey2 wkey3 wkey4 wkey5 wkey6 wkey7 wkey8 wkey9 wkey10
163
0x00
153
160
157
158
170
171
150
168
159
151

图 35A

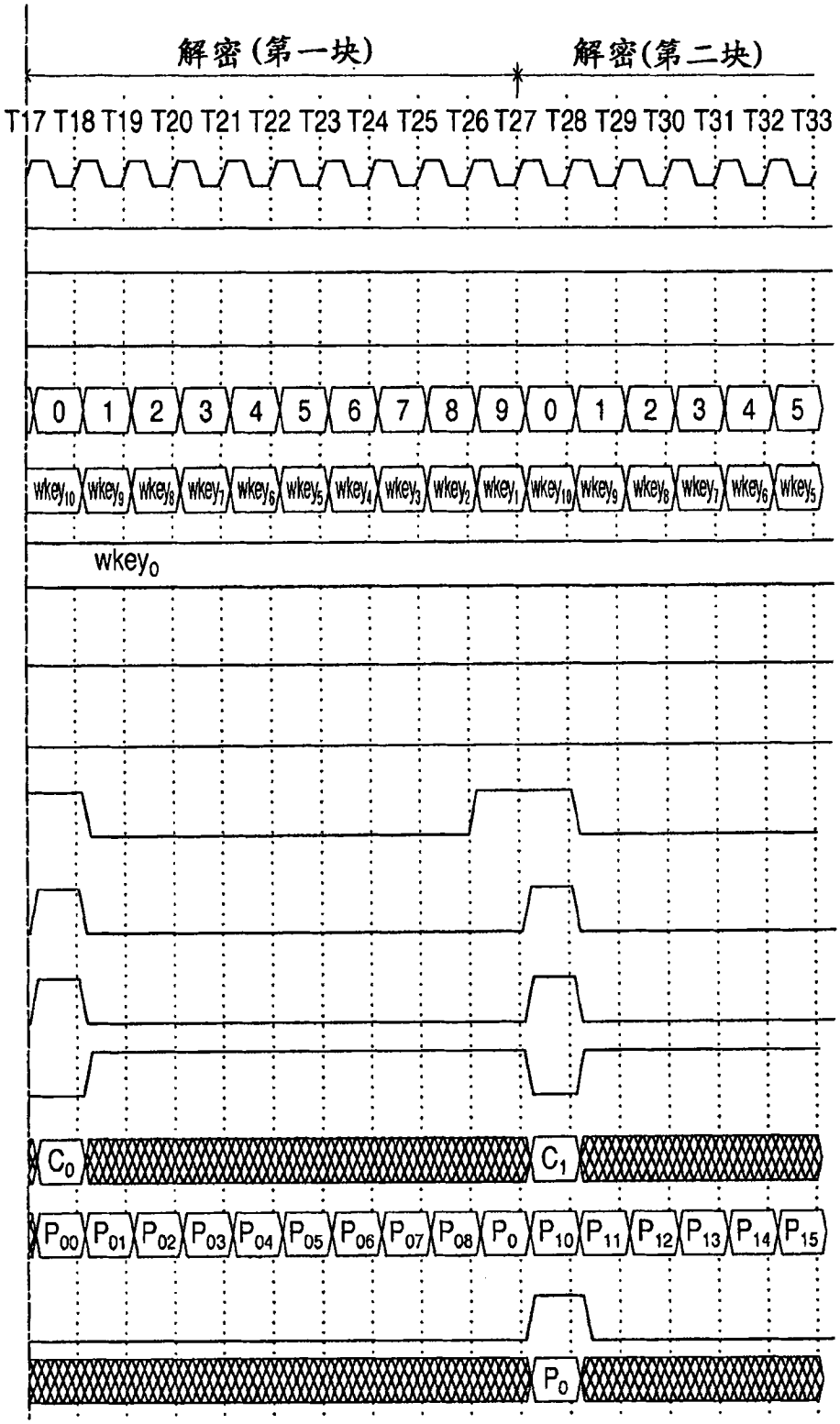

解密(第一块)
解密(第二块)
T17 T18 T19 T20 T21 T22 T23 T24 T25 T26 T27 T28 T29 T30 T31 T32 T33
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
wkey10 wkey9 wkey8 wkey7 wkey6 wkey5 wkey4 wkey3 wkey2 wkey1 wkey10 wkey9 wkey8 wkey7 wkey6 wkey5
wkey0
C0
C1
P00 P01 P02 P03 P04 P05 P06 P07 P08 P0 P10 P11 P12 P13 P14 P15
P0

图 35B

周期号	加密处理		解密处理	
	要执行的处理	要使用的轮回密钥	要执行的处理	要使用的轮回密钥
0	· AddRoundKey · SubBytes · ShiftRows · MixColumns · AddRoundKey	· 第0轮回密钥($wkey_0$) · 第1轮回密钥($wkey_1$)	· AddRoundKey · InvSubBytes · InvShiftRows · InvMixColumns · AddRoundKey	· 第10轮回密钥($wkey_{10}$) · 第9修改解密密钥($wkey_9'$)
1	· SubBytes · ShiftRows · MixColumns · AddRoundKey	· 第2轮回密钥($wkey_2$)	· InvSubBytes · InvShiftRows · InvMixColumns · AddRoundKey	· 第8修改解密密钥($wkey_8'$)
8	· SubBytes · ShiftRows · MixColumns · AddRoundKey	· 第9轮回密钥($wkey_9$)	· InvSubBytes · InvShiftRows · InvMixColumns · AddRoundKey	· 第1修改解密密钥($wkey_1'$)
9	· SubBytes · ShiftRows · AddRoundKey	· 第10轮回密钥($wkey_{10}$)	· InvSubBytes · InvShiftRows · AddRoundKey	· 第0轮回密钥($wkey_0$)

图 36

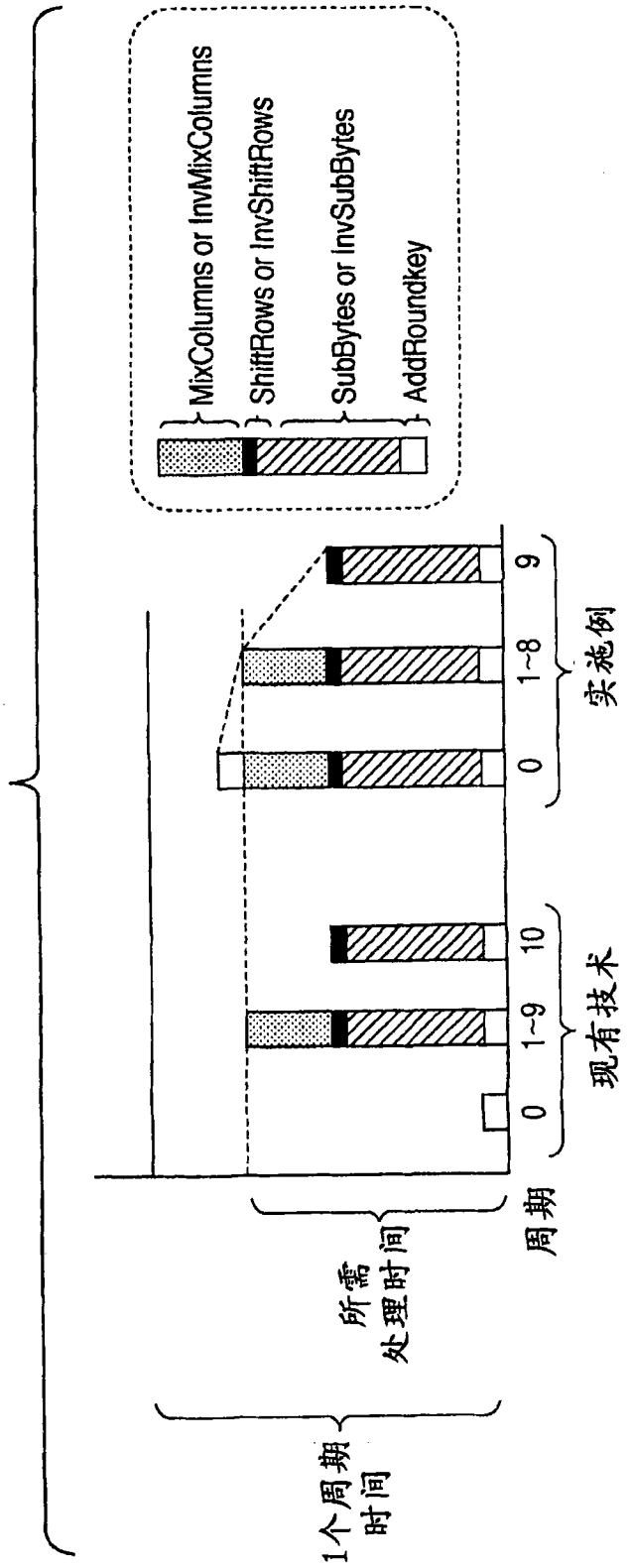

MixColumns or InvMixColumns
ShiftRows or InvShiftRows
SubBytes or InvSubBytes
AddRoundkey
1个周期时间
所需处理时间
周期
0
1~9
10
现有技术
0
1~8
9
实施例

图 37

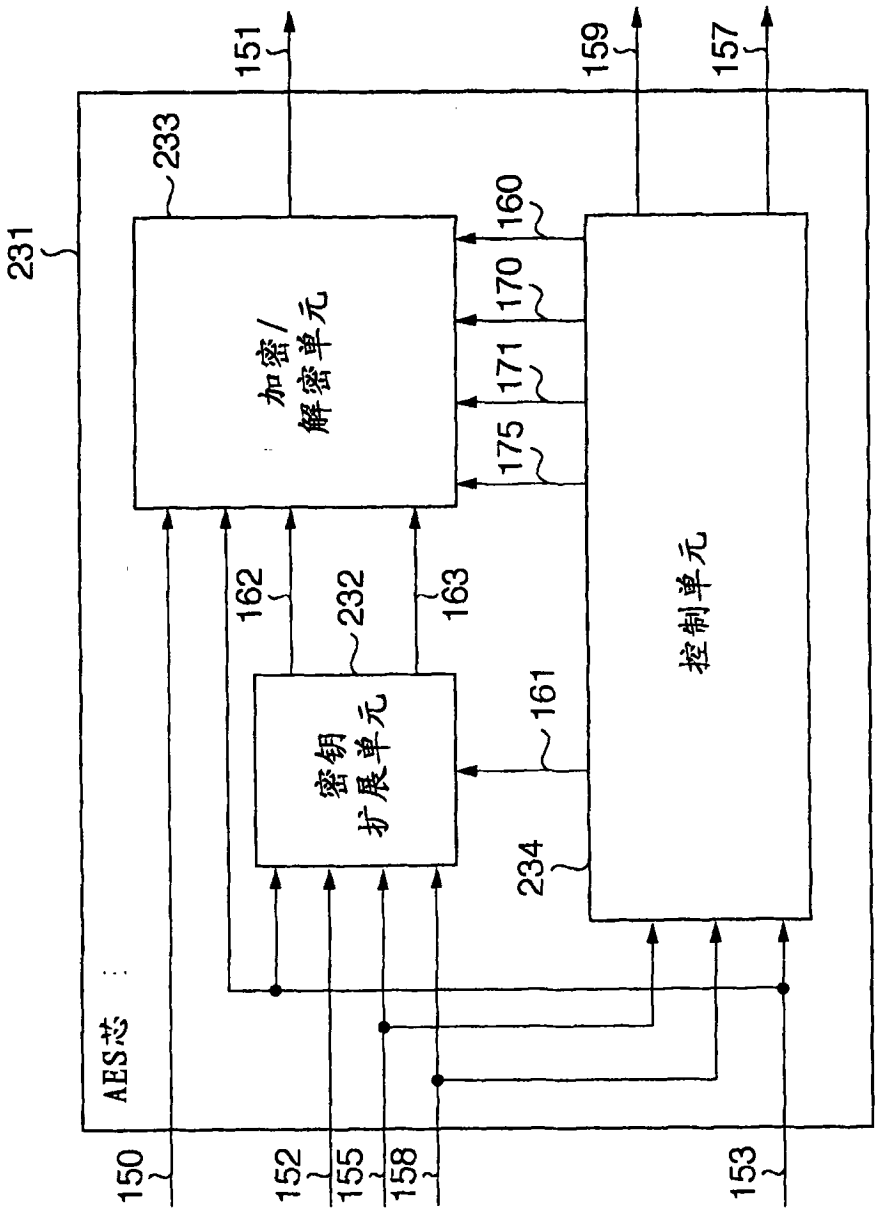

231
AES芯
233
加密/
解密单元
密钥
扩展单元
控制单元
150
151
152
153
155
157
158
159
160
161
162
163
170
171
175
232
234

图 38

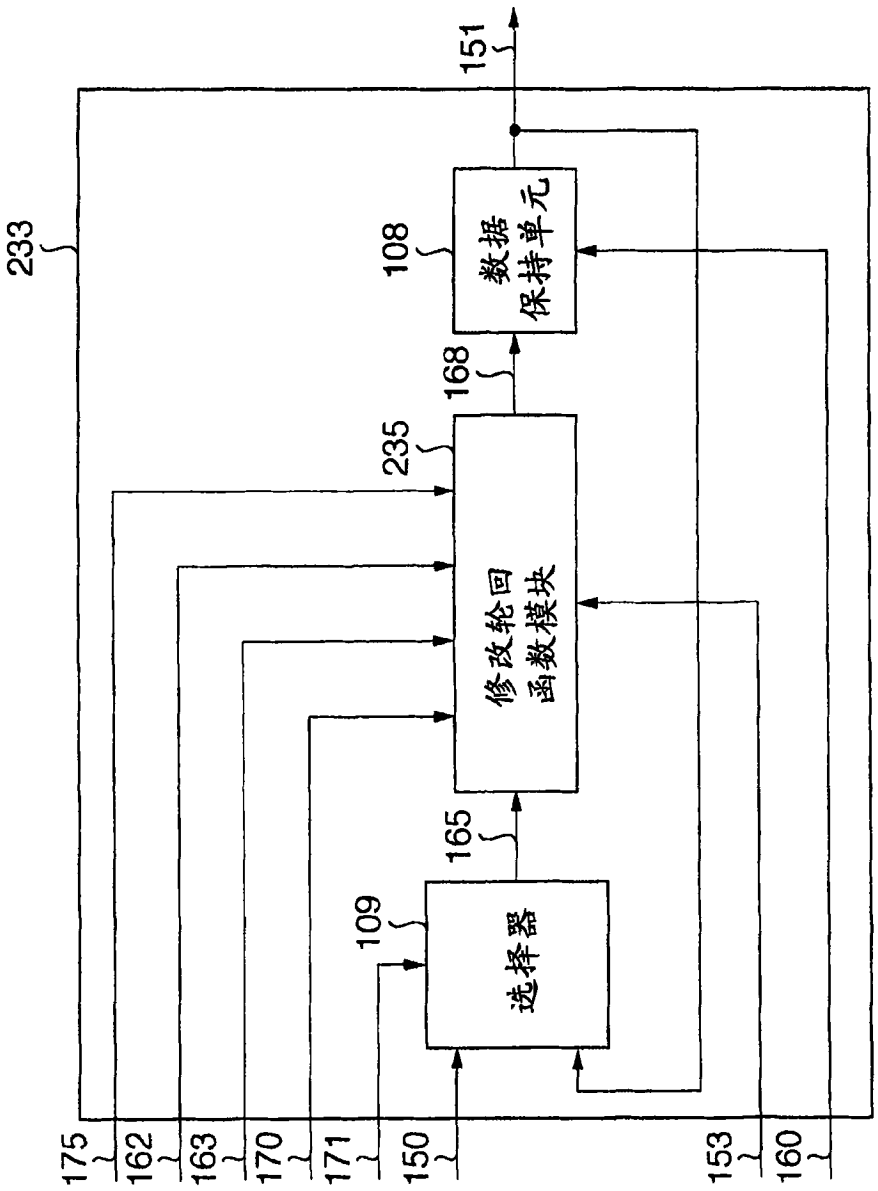

233
151
108
数据保持单元
168
235
修改轮回函数模块
165
109
选择器
175
162
163
170
171
150
153
160

图 39

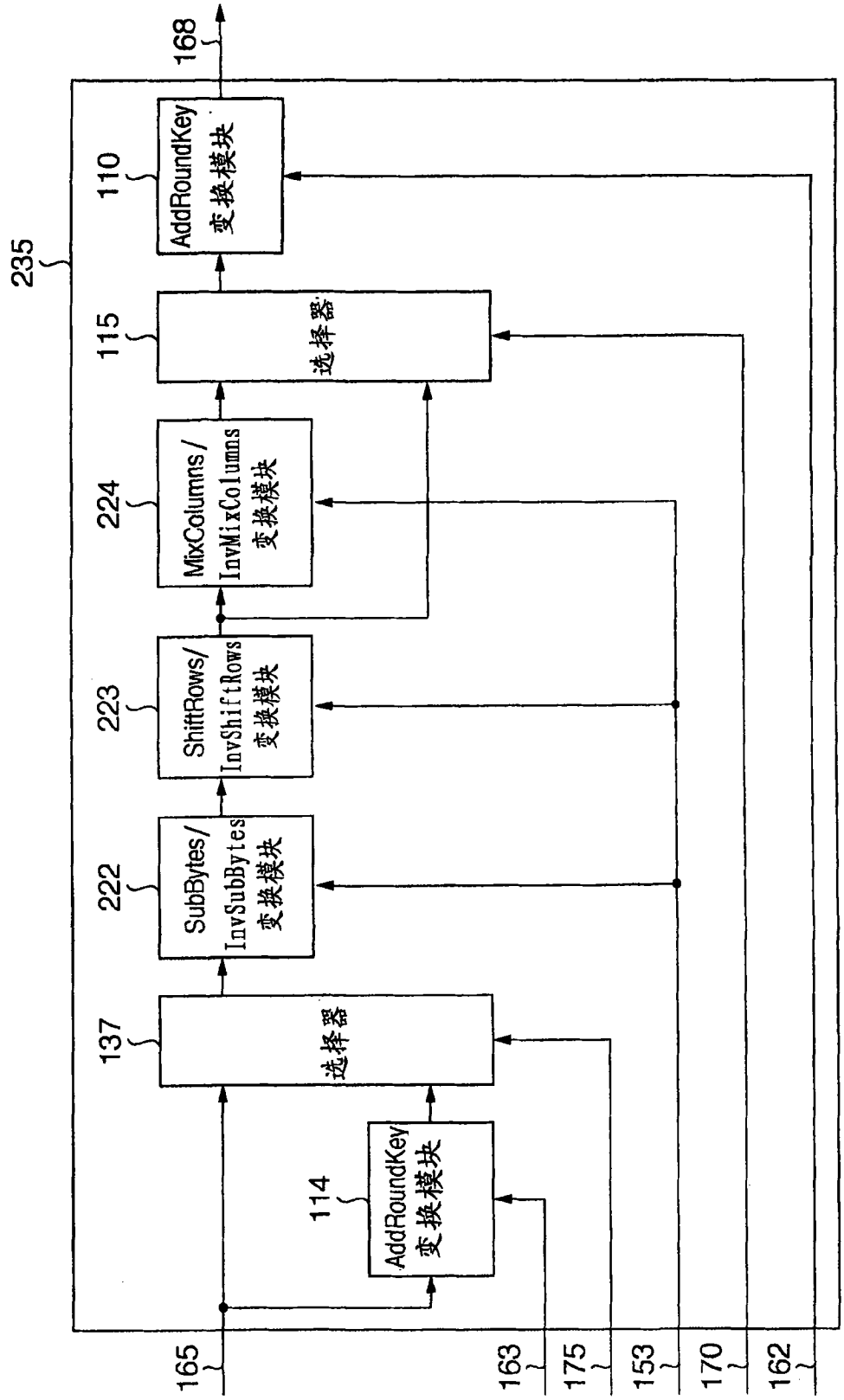

235
168
110
AddRoundKey
变换模块
115
选择器
224
MixColumns/
InvMixColumns
变换模块
223
ShiftRows/
InvShiftRows
变换模块
222
SubBytes/
InvSubBytes
变换模块
137
选择器
114
AddRoundKey
变换模块
165
163
175
153
170
162

图 40

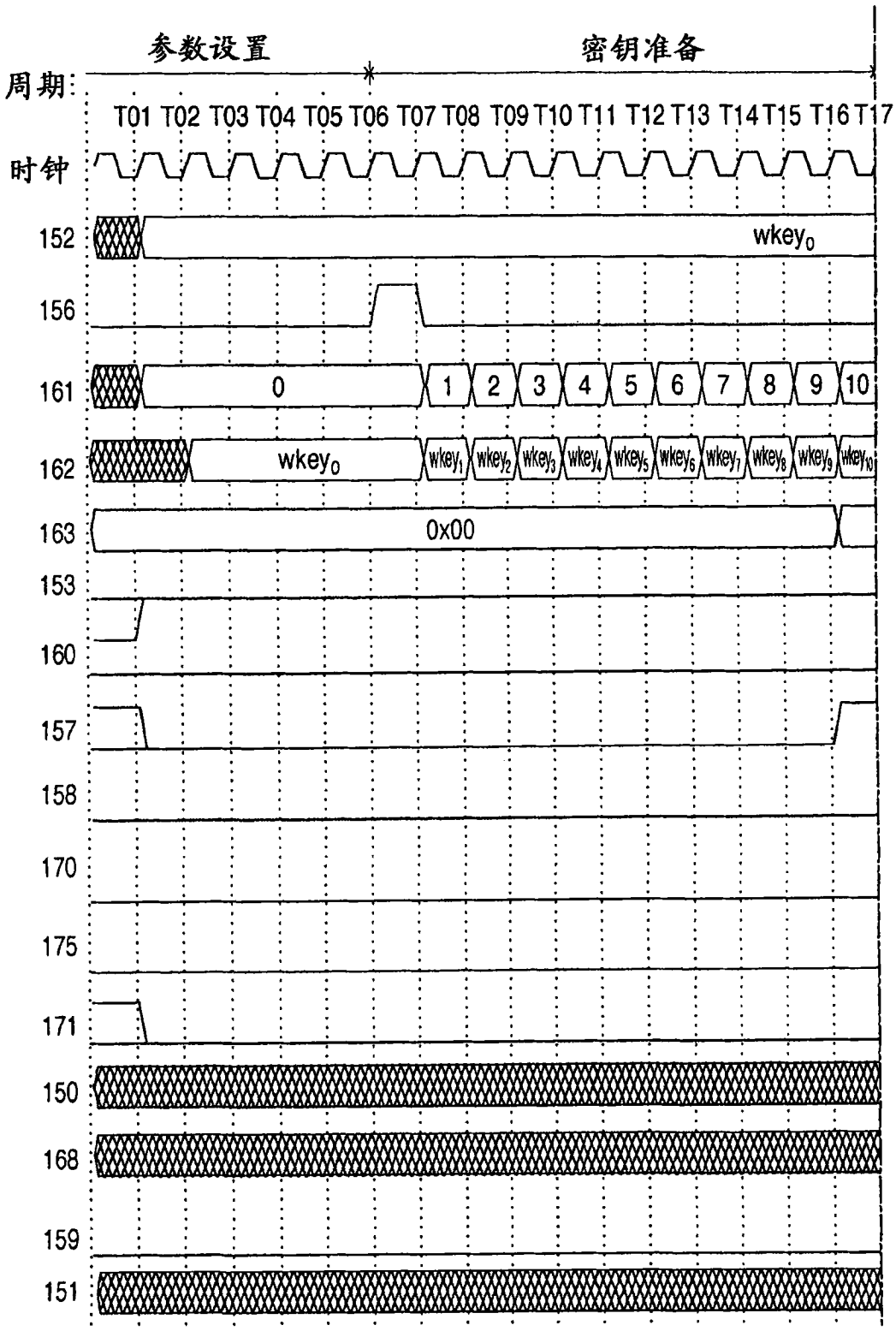

参数设置
密钥准备
周期:
T01 T02 T03 T04 T05 T06 T07 T08 T09 T10 T11 T12 T13 T14 T15 T16 T17
时钟
152
wkey0
156
161
0 1 2 3 4 5 6 7 8 9 10
162
wkey0 wkey1 wkey2 wkey3 wkey4 wkey5 wkey6 wkey7 wkey8 wkey9 wkey10
163
0x00
153
160
157
158
170
175
171
150
168
159
151

图 41A

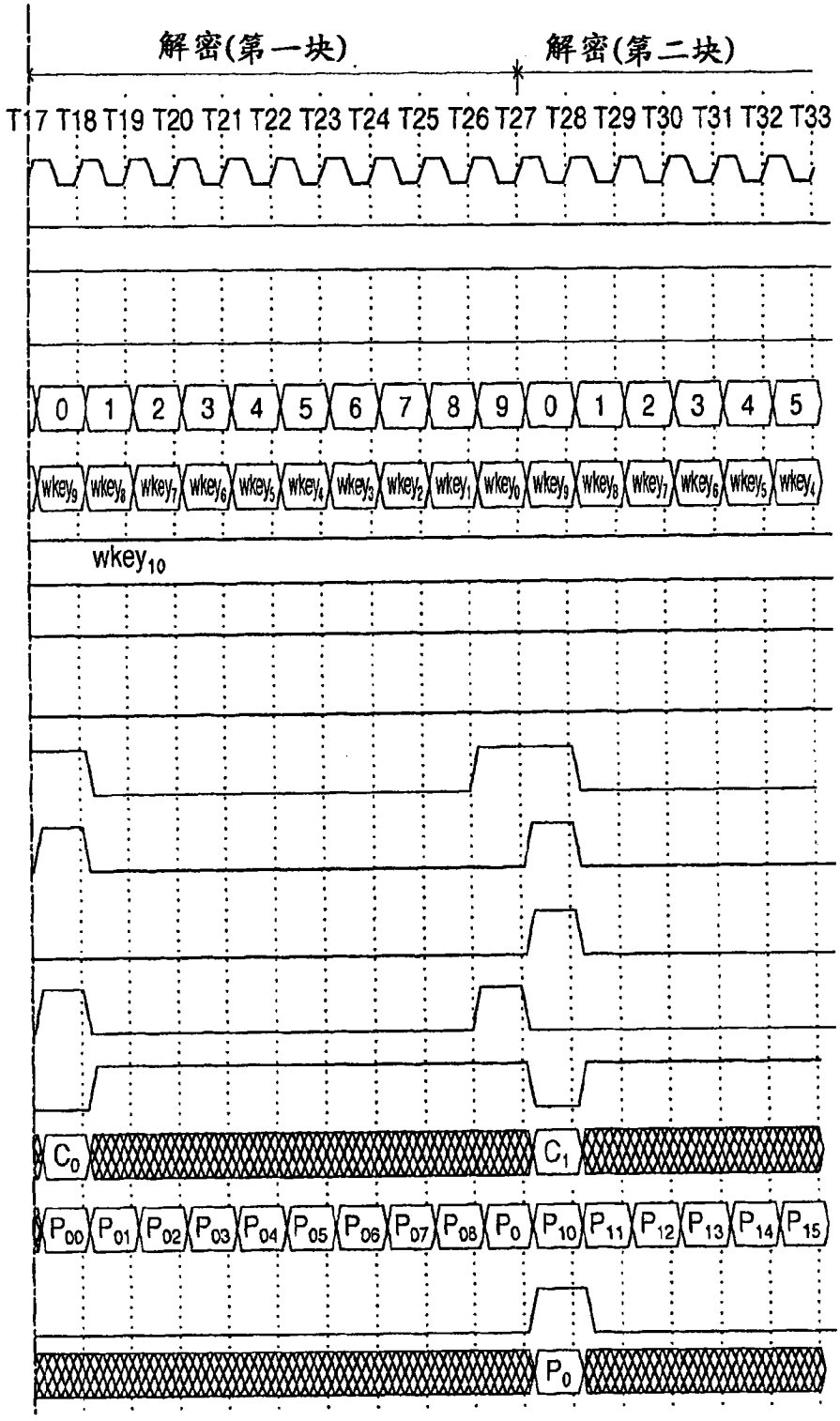

解密(第一块)
解密(第二块)
T17 T18 T19 T20 T21 T22 T23 T24 T25 T26 T27 T28 T29 T30 T31 T32 T33
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
wkey9 wkey8 wkey7 wkey6 wkey5 wkey4 wkey3 wkey2 wkey1 wkey0 wkey9 wkey8 wkey7 wkey6 wkey5 wkey4
wkey10
C0
C1
P00 P01 P02 P03 P04 P05 P06 P07 P08 P0 P10 P11 P12 P13 P14 P15
P0

图 41B

周期号	加密处理		解密处理	
	要执行的处理	要使用的轮回密钥	要执行的处理	要使用的轮回密钥
0	· AddRoundKey · SubBytes · ShiftRows · MixColumns · AddRoundKey	· 第0轮回密钥($wkey_0$) · 第1轮回密钥($wkey_1$)	· AddRoundKey · InvSubBytes · InvShiftRows · InvMixColumns · AddRoundKey	· 第10轮回密钥($wkey_{10}$) · 第9修改解密密钥($wkey_9'$)
1	· SubBytes · ShiftRows · MixColumns · AddRoundKey	· 第2轮回密钥($wkey_2$)	· InvSubBytes · InvShiftRows · InvMixColumns · AddRoundKey	· 第8修改解密密钥($wkey_8'$)
8	· SubBytes · ShiftRows · MixColumns · AddRoundKey	· 第9轮回密钥($wkey_9$)	· InvSubBytes · InvShiftRows · InvMixColumns · AddRoundKey	· 第1修改解密密钥($wkey_1'$)
9	· SubBytes · ShiftRows · AddRoundKey	· 第10轮回密钥($wkey_{10}$)	· InvSubBytes · InvShiftRows · AddRoundKey	· 第0轮回密钥($wkey_0$)

图 42

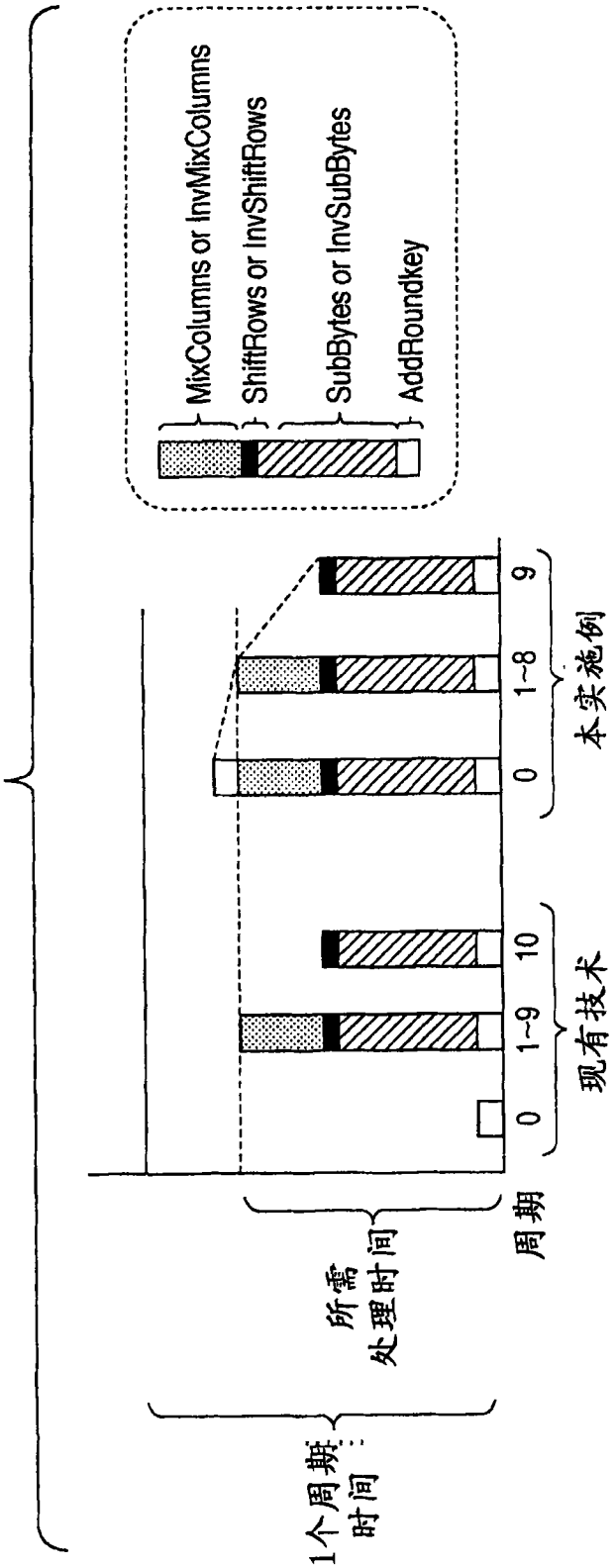

MixColumns or InvMixColumns
ShiftRows or InvShiftRows
SubBytes or InvSubBytes
AddRoundkey
1个周期时间
所需处理时间
周期
0
1~9
10
现有技术
0
1~8
9
本实施例

图43

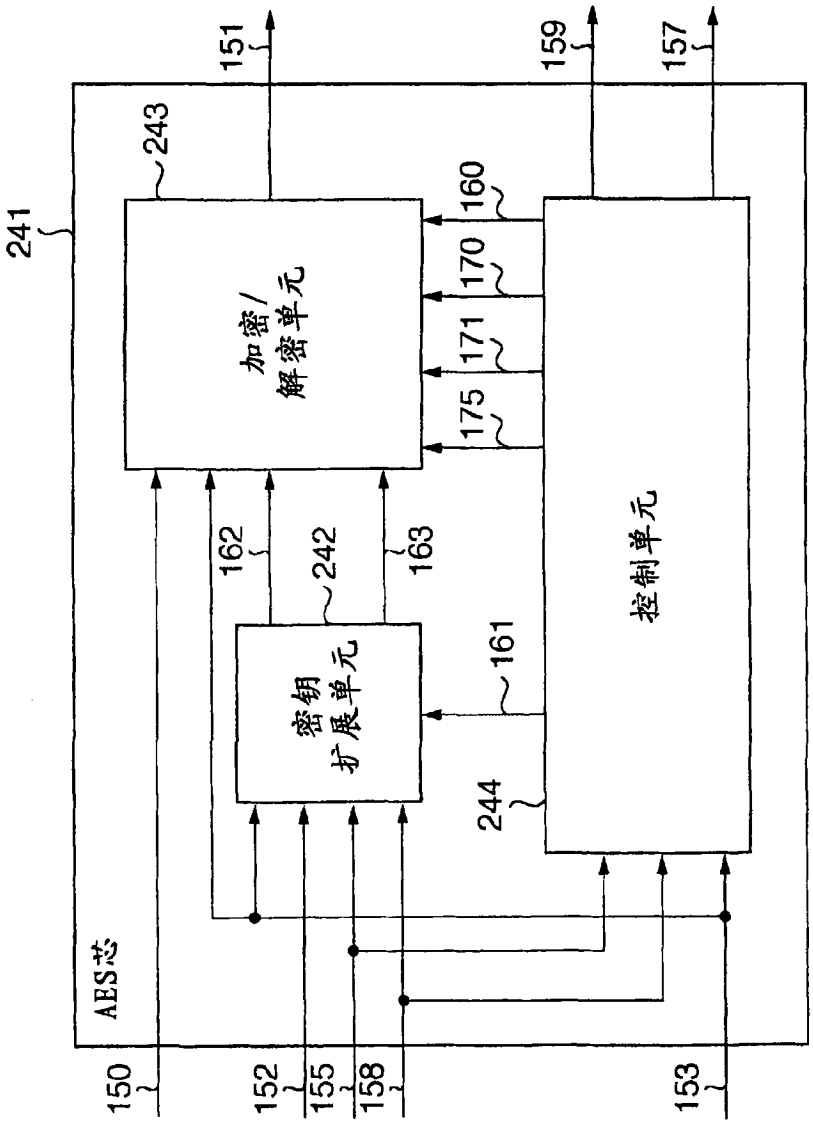

241
AES芯
243
加密/
解密单元
242
密钥
扩展单元
控制单元
150
151
152
153
155
157
158
159
160
161
162
163
170
171
175
244

图 44

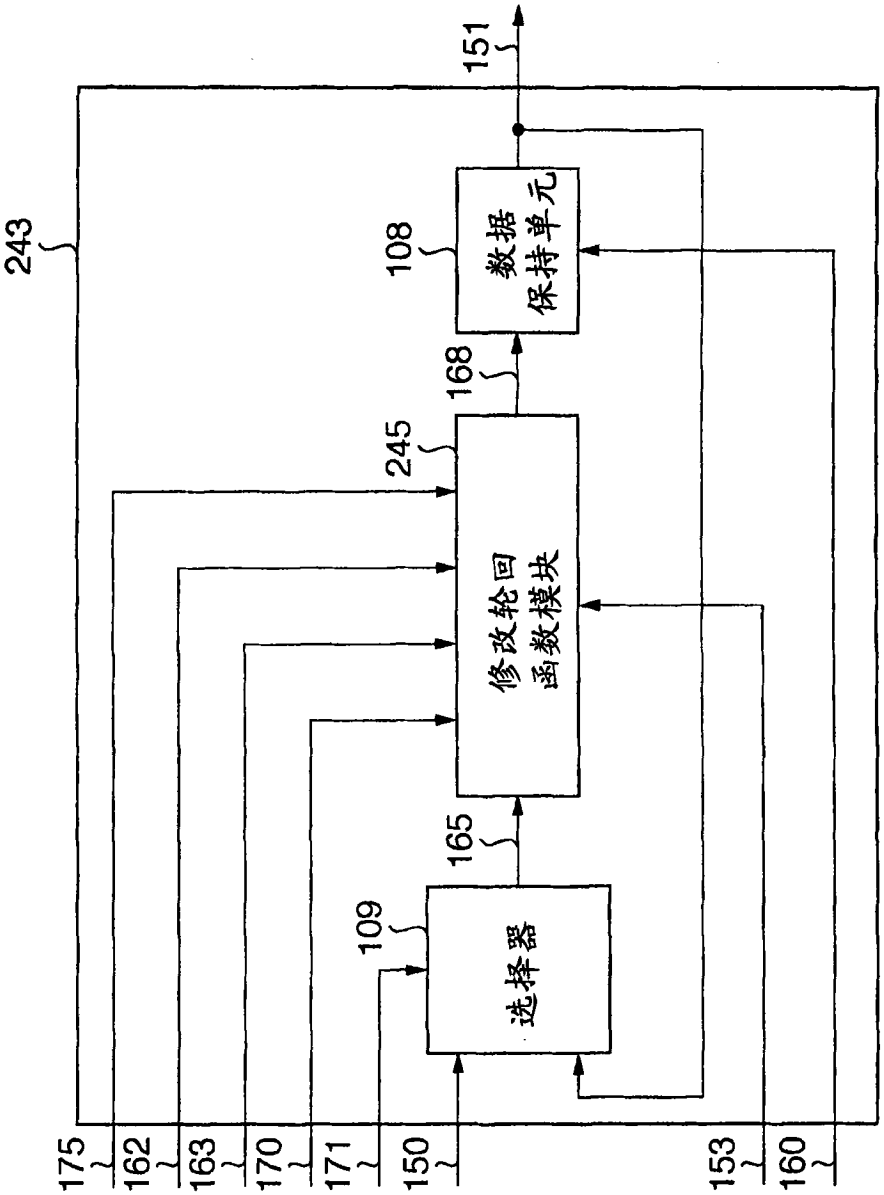

151
243
108
数据保持单元
168
245
修改轮回函数模块
165
109
选择器
175
162
163
170
171
150
153
160

图 45

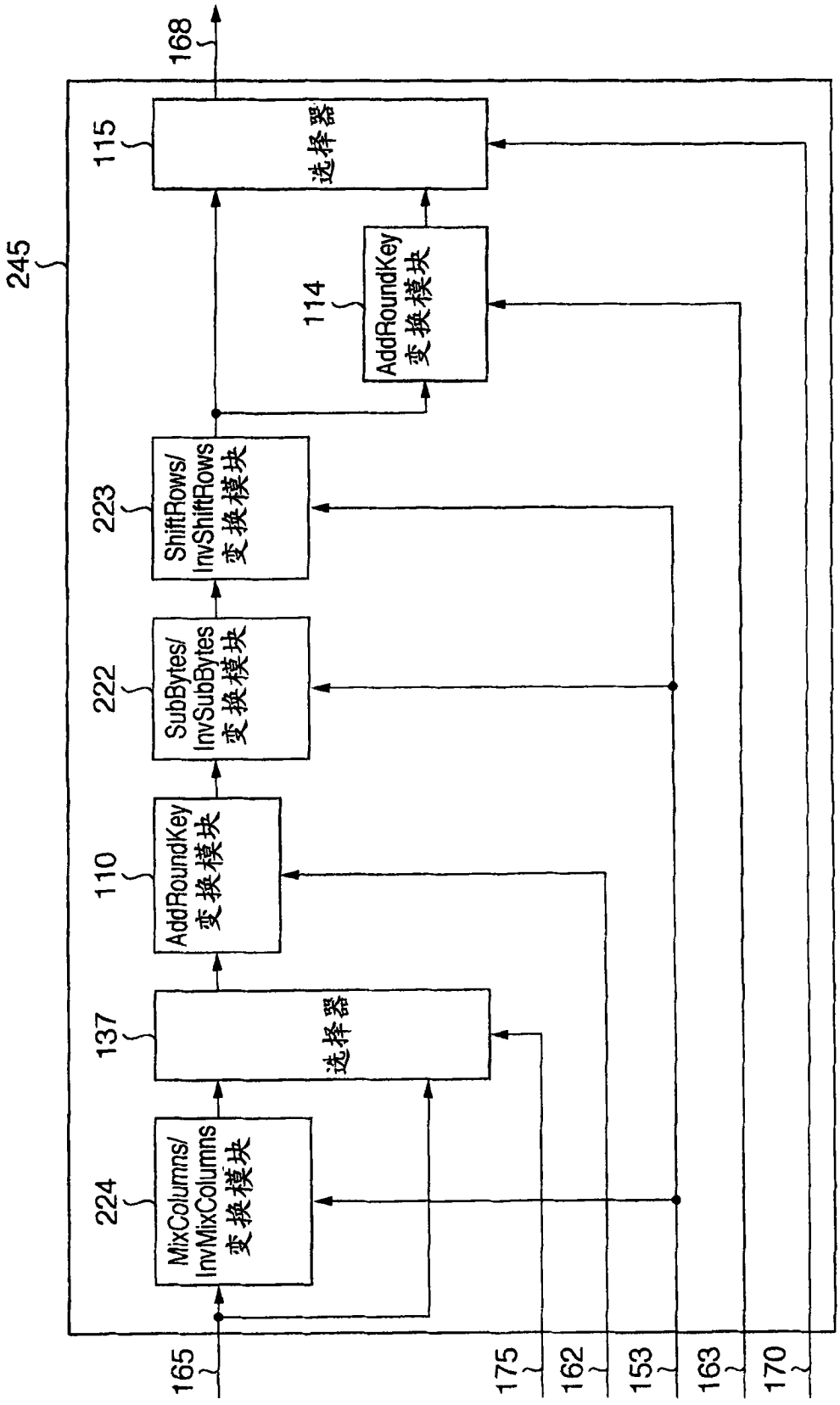

245
168
115
选择器
114
AddRoundKey
变换模块
223
ShiftRows/
InvShiftRows
变换模块
222
SubBytes/
InvSubBytes
变换模块
110
AddRoundKey
变换模块
137
选择器
224
MixColumns/
InvMixColumns
变换模块
165
175
162
153
163
170

图46

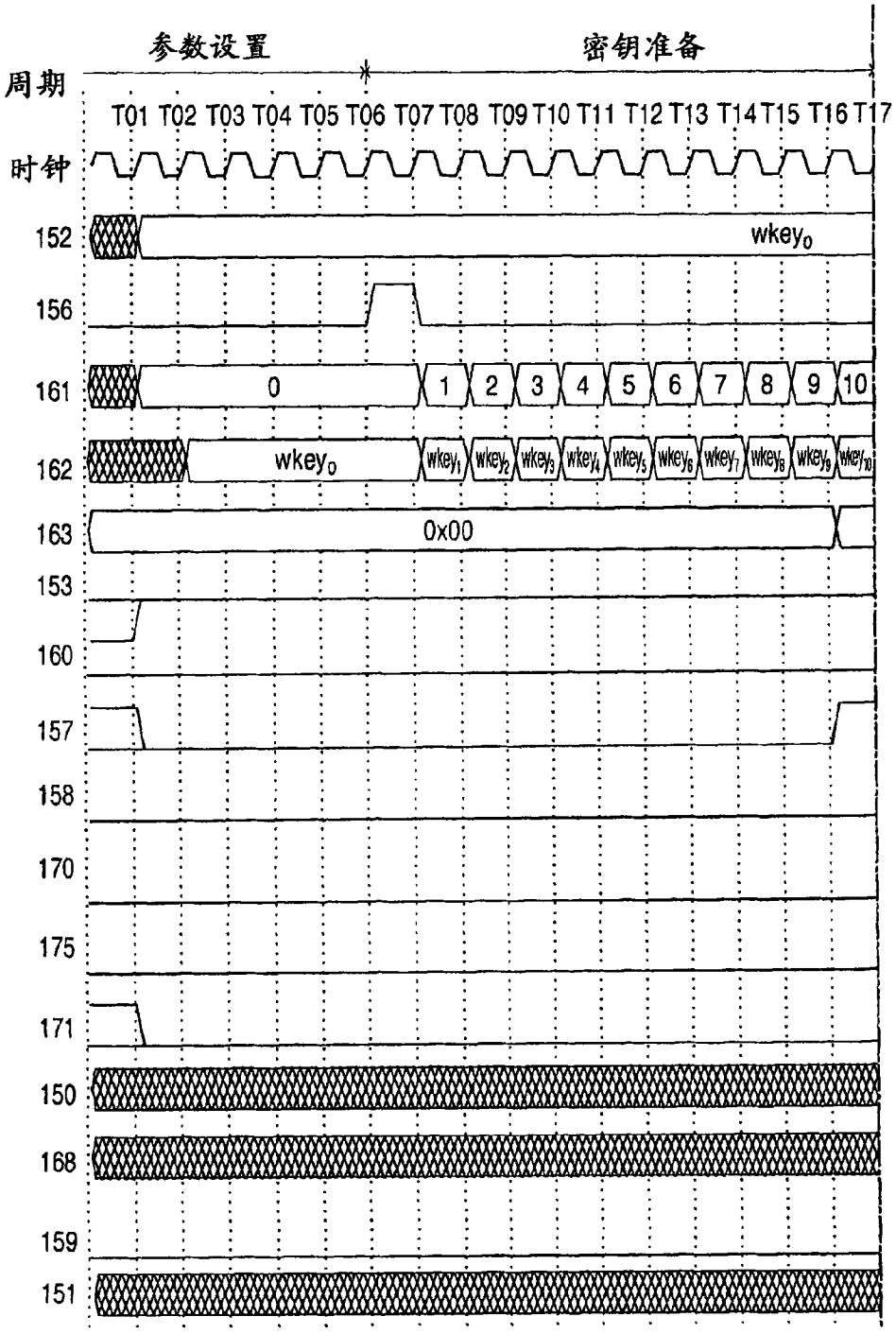

参数设置
密钥准备
周期
T01 T02 T03 T04 T05 T06 T07 T08 T09 T10 T11 T12 T13 T14 T15 T16 T17
时钟
152
wkey0
156
161
0
1 2 3 4 5 6 7 8 9 10
162
wkey0
wkey1 wkey2 wkey3 wkey4 wkey5 wkey6 wkey7 wkey8 wkey9 wkey10
163
0x00
153
160
157
158
170
175
171
150
168
159
151

图 47A

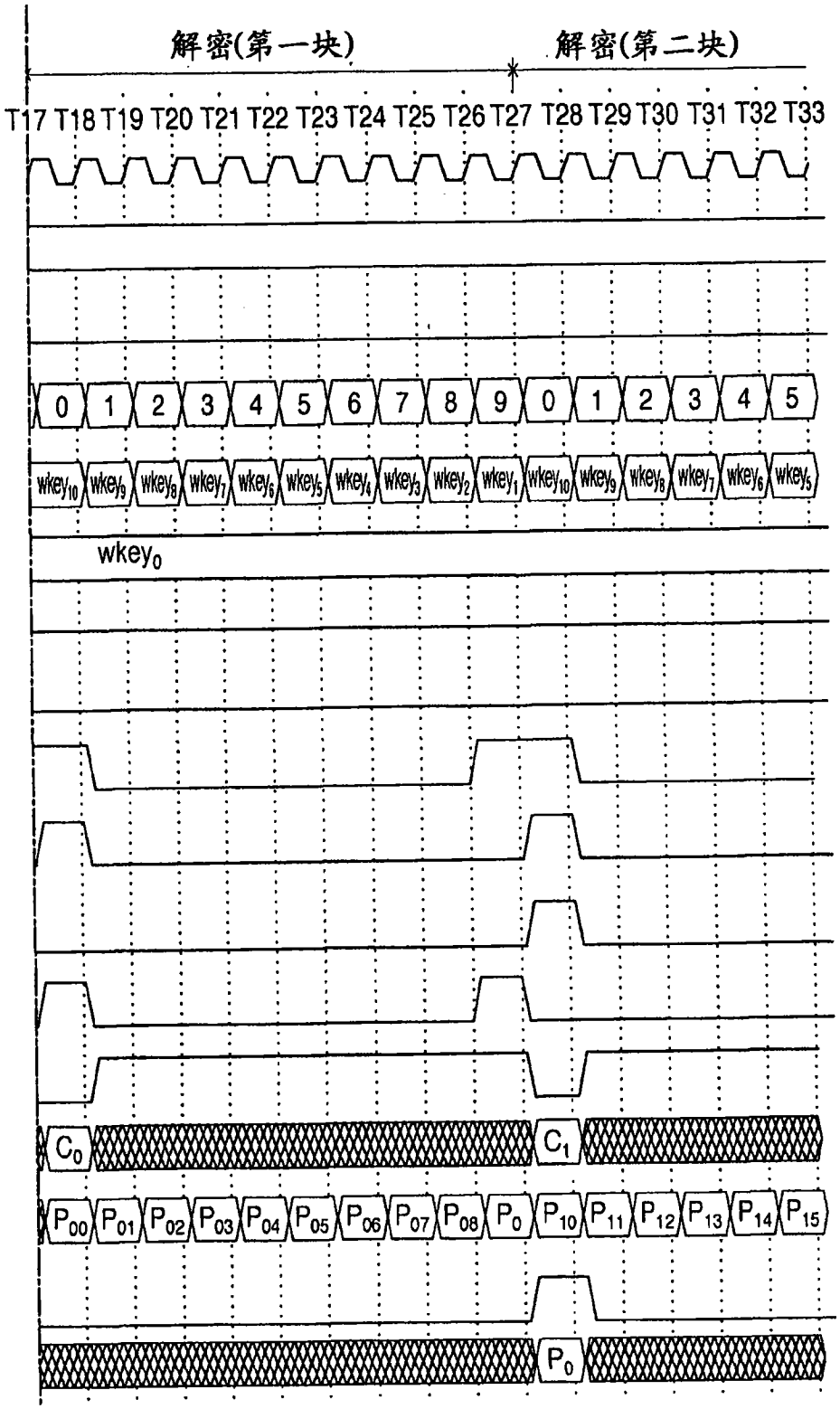

解密(第一块)
解密(第二块)
T17 T18 T19 T20 T21 T22 T23 T24 T25 T26 T27 T28 T29 T30 T31 T32 T33
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
wkey10 wkey9 wkey8 wkey7 wkey6 wkey5 wkey4 wkey3 wkey2 wkey1 wkey10 wkey9 wkey8 wkey7 wkey6 wkey5
wkey0
C0
C1
P00 P01 P02 P03 P04 P05 P06 P07 P08 P0 P10 P11 P12 P13 P14 P15
P0

图 47B

周期号	加密处理		第七实施例	
	要执行的处理	要使用的轮回密钥	要执行的处理	要使用的轮回密钥
0	· AddRoundKey	· 第0轮回密钥($wkey_0$)	· AddRoundKey · SubBytes · ShiftRows · MixColumns · AddRoundKey · SubBytes · ShiftRows · MixColumns	· 第0轮回密钥($wkey_0$) · 第1轮回密钥($wkey_1$)
1	· SubBytes · ShiftRows · MixColumns · AddRoundKey · SubBytes · ShiftRows · MixColumns · AddRoundKey	· 第1轮回密钥($wkey_1$) · 第2轮回密钥($wkey_2$)	· AddRoundKey · SubBytes · ShiftRows · MixColumns · AddRoundKey · SubBytes · ShiftRows · MixColumns	· 第2轮回密钥($wkey_2$) · 第3轮回密钥($wkey_3$)
4	· SubBytes · ShiftRows · MixColumns · AddRoundKey · SubBytes · ShiftRows · MixColumns · AddRoundKey	· 第7轮回密钥($wkey_7$) · 第8轮回密钥($wkey_8$)	· AddRoundKey · SubBytes · ShiftRows · MixColumns · AddRoundKey · SubBytes · ShiftRows · AddRoundKey	· 第8轮回密钥($wkey_8$) · 第9轮回密钥($wkey_9$) · 第10轮回密钥($wkey_{10}$)
5	· SubBytes · ShiftRows · MixColumns · AddRoundKey · SubBytes · ShiftRows · AddRoundKey	· 第9轮回密钥($wkey_9$) · 第10轮回密钥($wkey_{10}$)		

图 48

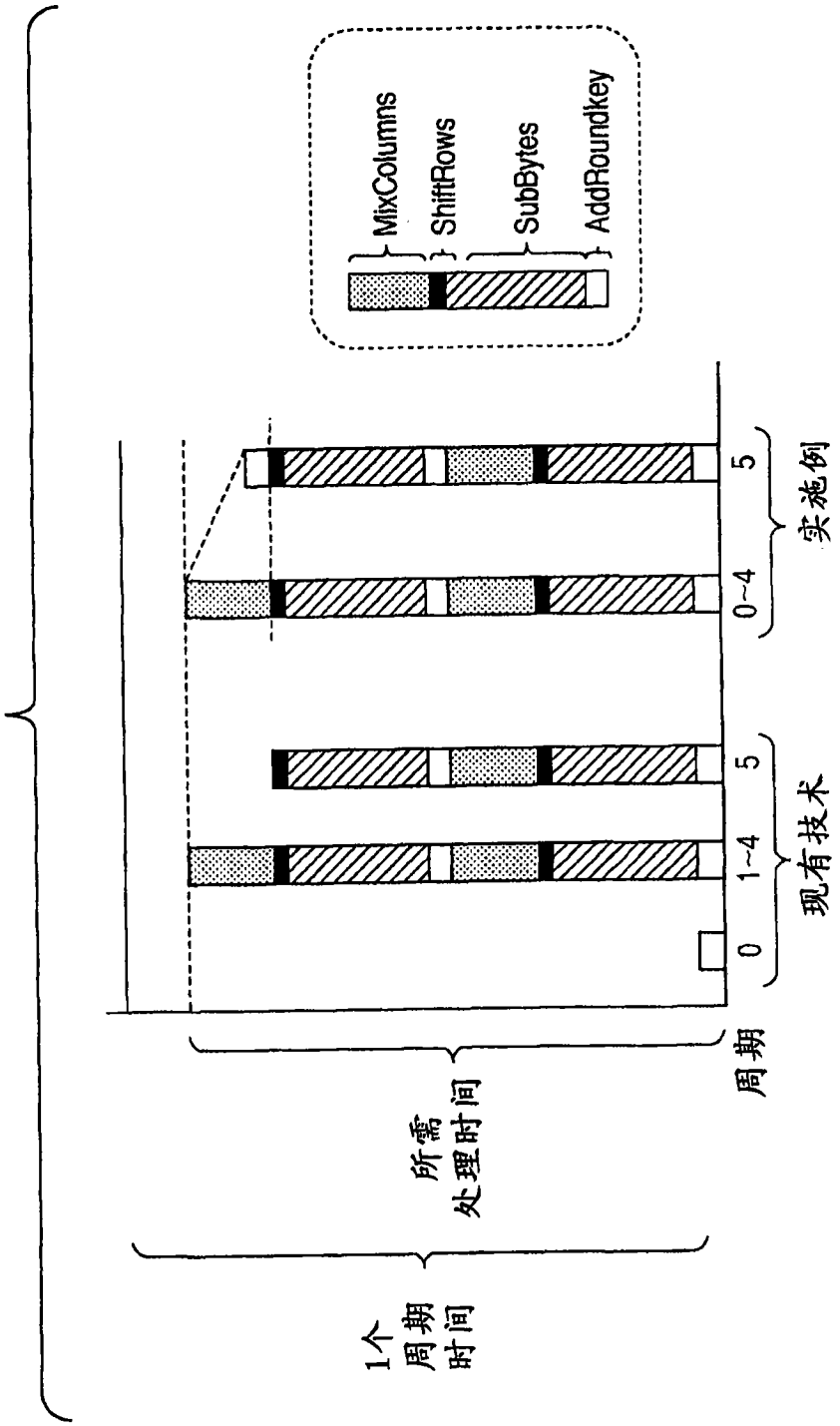

MixColumns
ShiftRows
SubBytes
AddRoundkey
1个周期时间
所需处理时间
周期
0
1~4
5
现有技术
0~4
5
实施例

图49

周期号	加密处理		第七实施例	
	要执行的处理	要使用的轮回密钥	要执行的处理	要使用的轮回密钥
0	· AddRoundKey	· 第10轮回密钥($wkey_{10}$)	· AddRoundKey · InvShiftRows · InvSubBytes · AddRoundKey · InvMixColumns · InvShiftRows · InvSubBytes · AddRoundKey	· 第10轮回密钥($wkey_{10}$) · 第9轮回密钥($wkey_9$) · 第8轮回密钥($wkey_8$)
1	· InvShiftRows · InvSubBytes · AddRoundKey · InvMixColumns · InvShiftRows · InvSubBytes · AddRoundKey · InvMixColumns	· 第9轮回密钥($wkey_9$) · 第8轮回密钥($wkey_8$)	· InvMixColumns · InvShiftRows · InvSubBytes · AddRoundKey · InvMixColumns · InvShiftRows · InvSubBytes · AddRoundKey	· 第7轮回密钥($wkey_7$) · 第6轮回密钥($wkey_6$)
4	· InvShiftRows · InvSubBytes · AddRoundKey · InvMixColumns · InvShiftRows · InvSubBytes · AddRoundKey · InvMixColumns	· 第3轮回密钥($wkey_3$) · 第2轮回密钥($wkey_2$)	· InvMixColumns · InvShiftRows · InvSubBytes · AddRoundKey · InvMixColumns · InvShiftRows · InvSubBytes · AddRoundKey	· 第1轮回密钥($wkey_1$) · 第0轮回密钥($wkey_0$)
5	· InvShiftRows · InvSubBytes · AddRoundKey · InvMixColumns · InvShiftRows · InvSubBytes · AddRoundKey	· 第1轮回密钥($wkey_1$) · 第0轮回密钥($wkey_0$)		

图 50

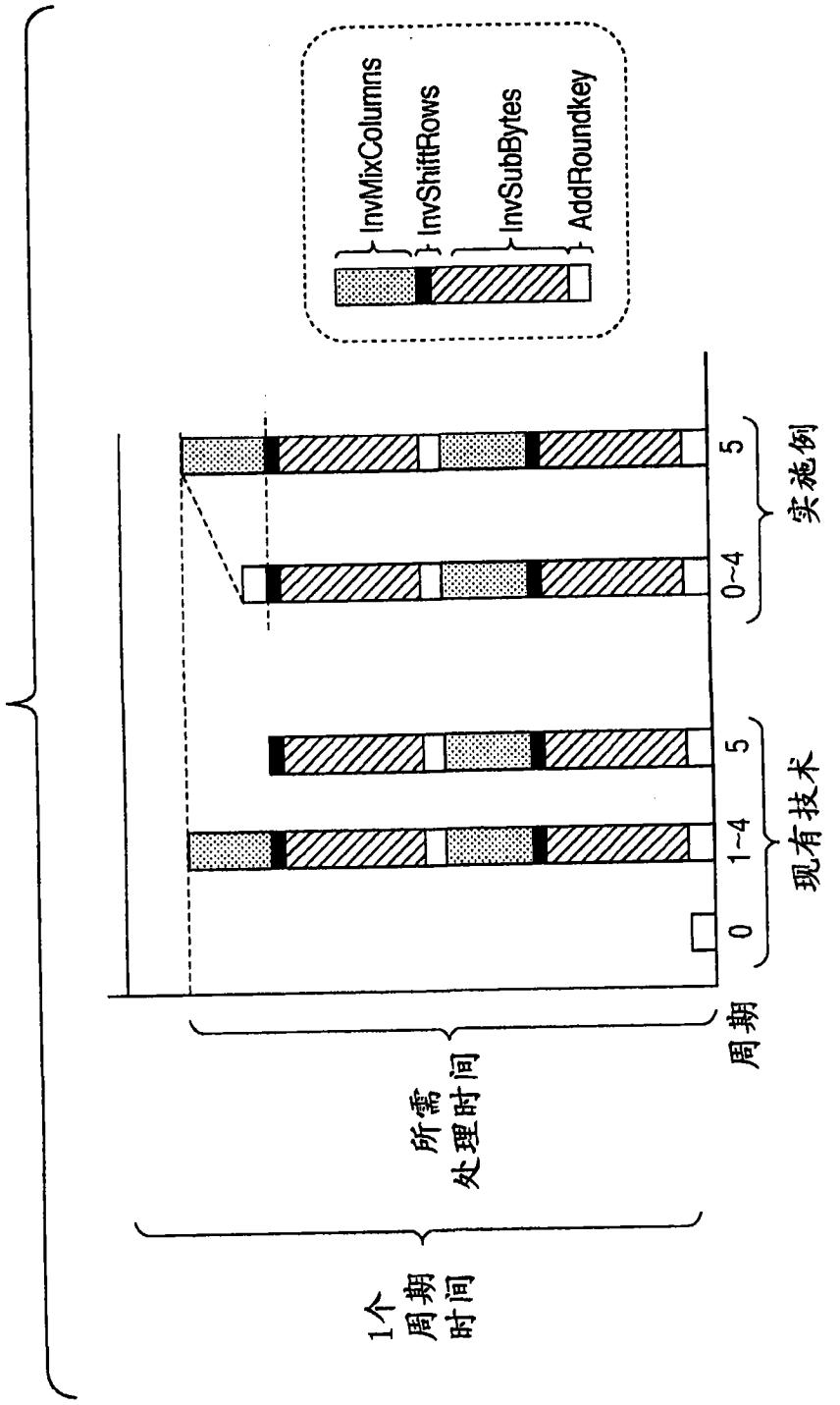

InvMixColumns
InvShiftRows
InvSubBytes
AddRoundkey
0
1~4
5
现有技术
0~4
5
实施例
周期
所需
处理时间
1个
周期
时间

图51

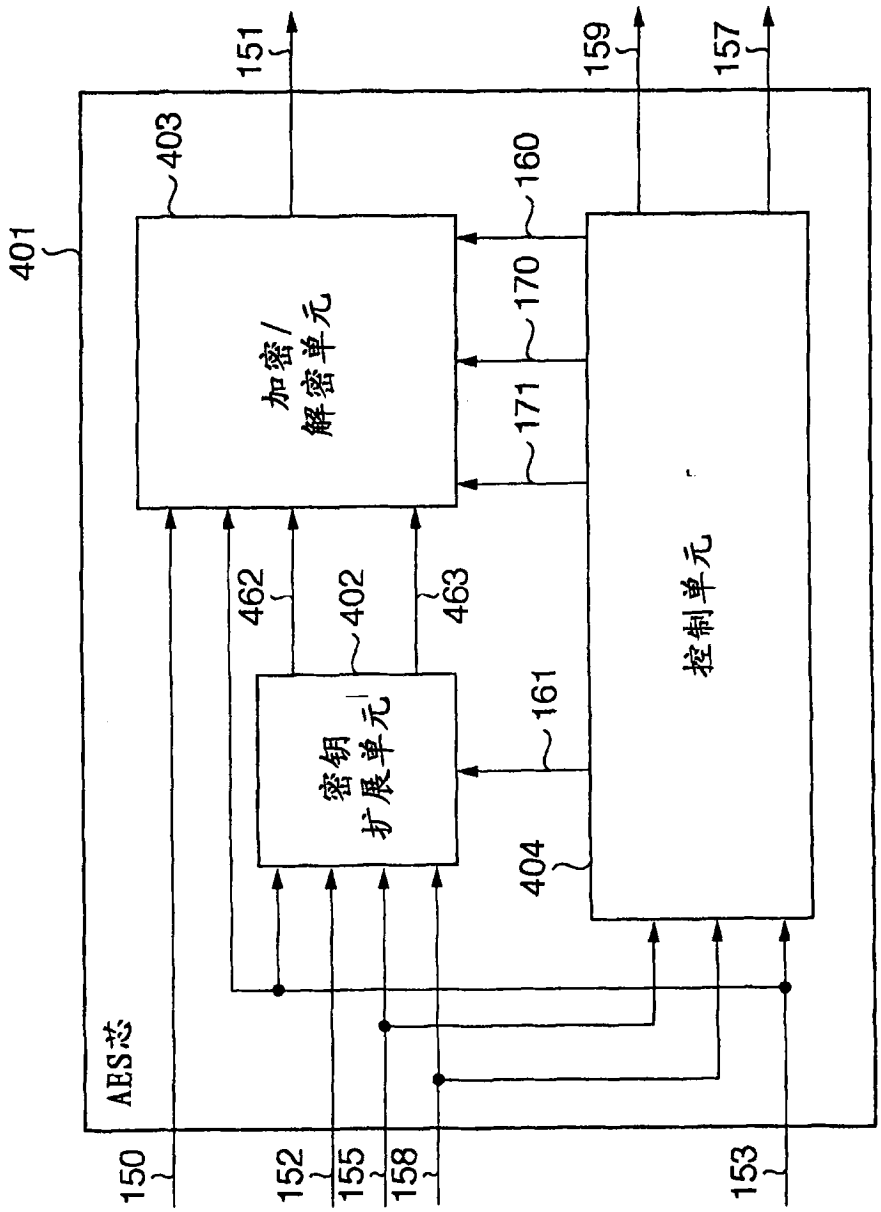

AES芯
401
403
加密/
解密单元
160
170
171
151
159
157
462
402
463
密钥
扩展单元
161
控制单元
404
150
152
155
158
153

图52

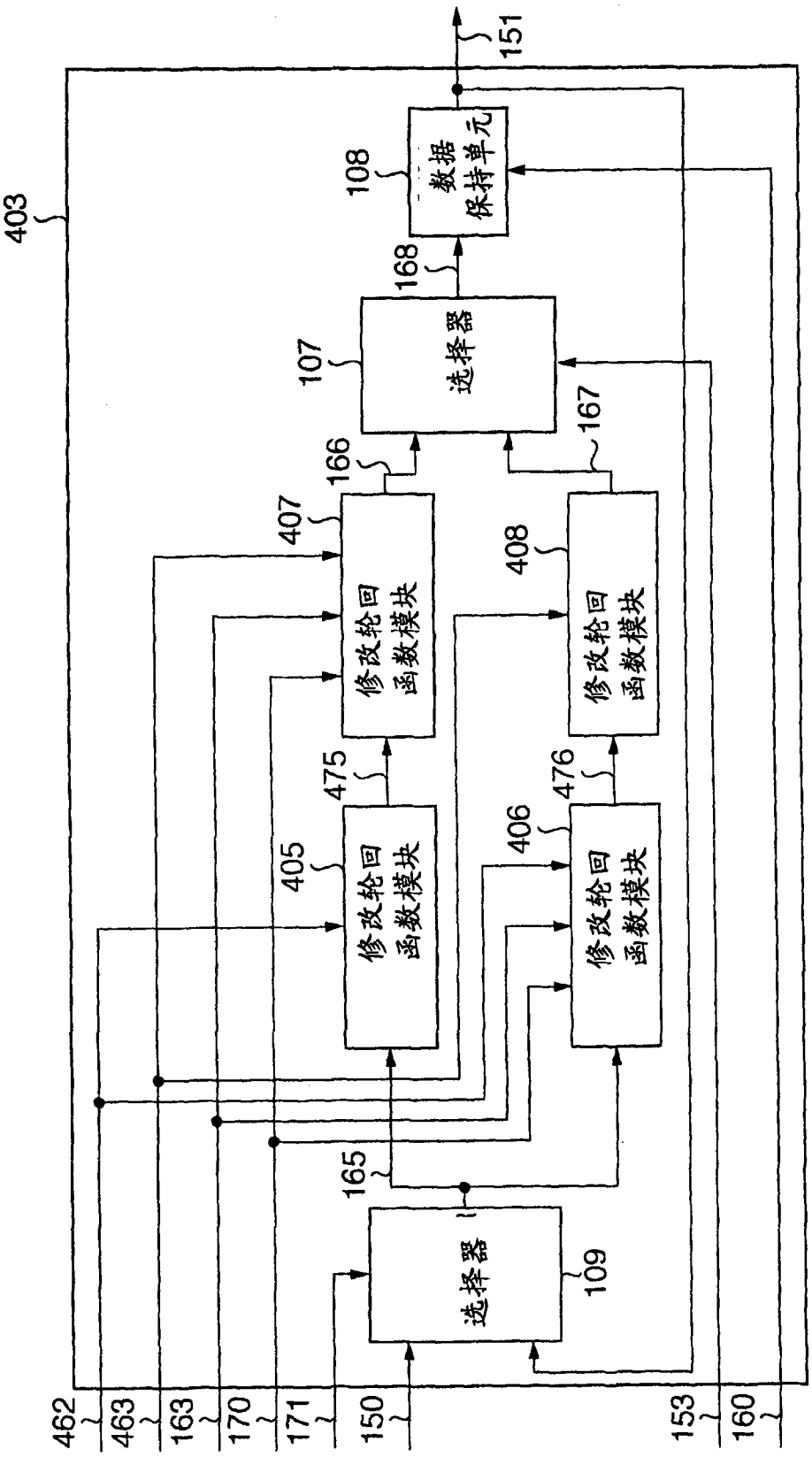

403
151
108
数据保持单元
168
107
选择器
167
166
407
408
修改轮回函数模块
修改轮回函数模块
475
476
405
406
修改轮回函数模块
修改轮回函数模块
165
选择器
109
462
463
163
170
171
150
153
160

图 53

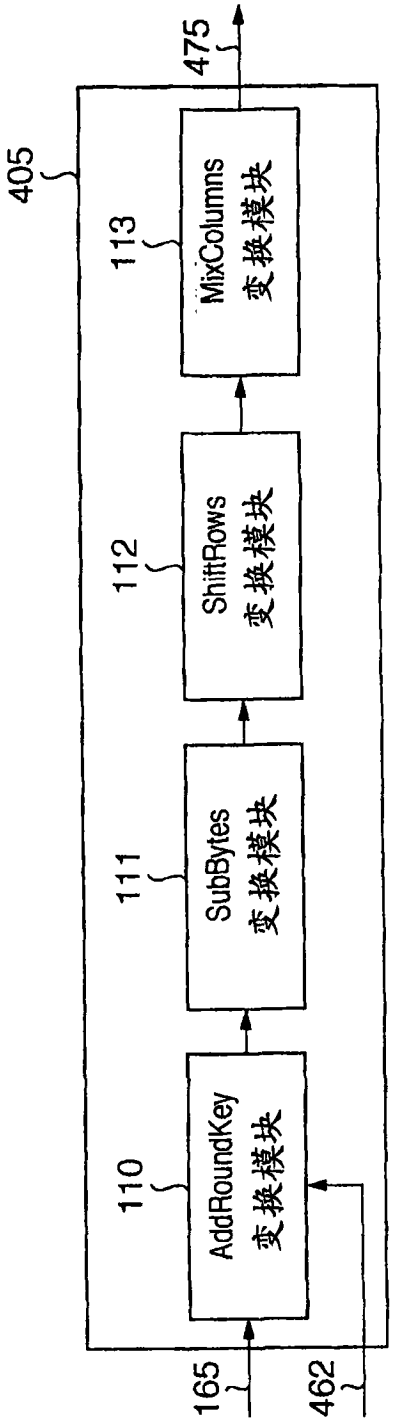

405
110
AddRoundKey
变换模块
111
SubBytes
变换模块
112
ShiftRows
变换模块
113
MixColumns
变换模块
475
165
462

图54A

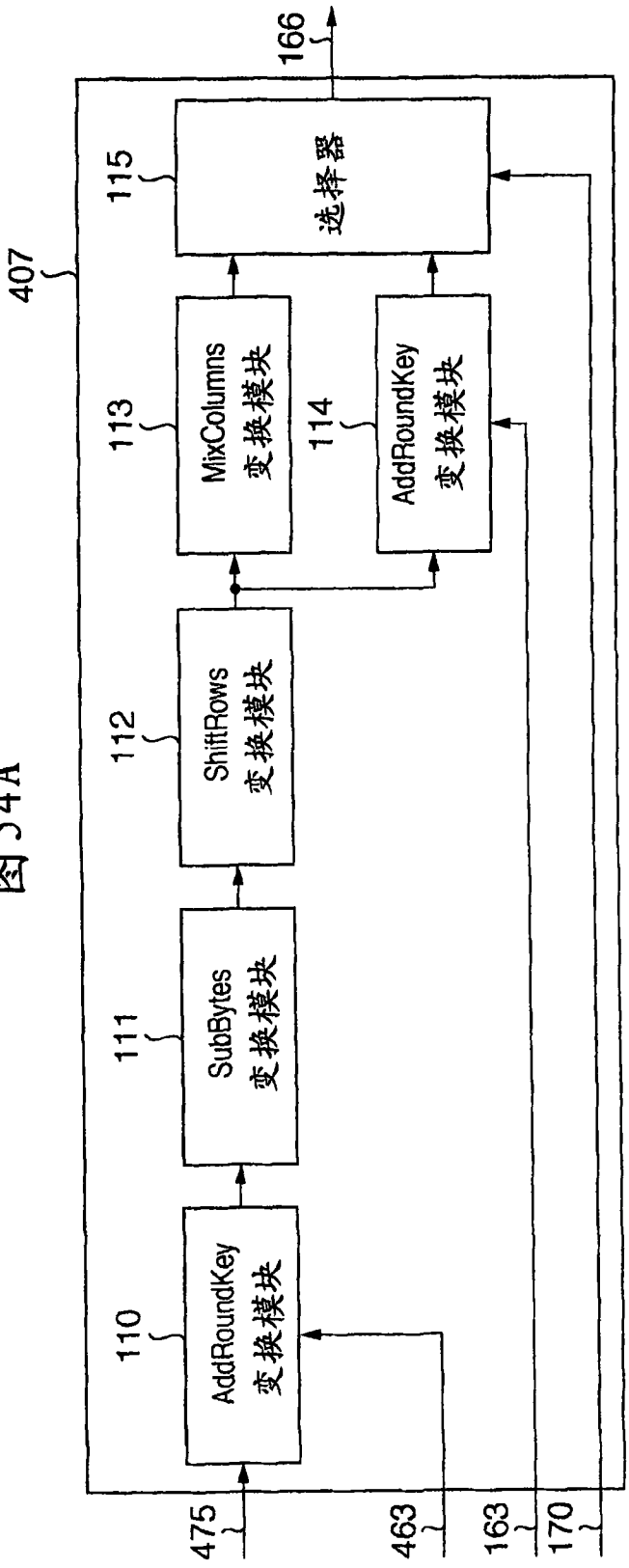

407
110
AddRoundKey
变换模块
111
SubBytes
变换模块
112
ShiftRows
变换模块
113
MixColumns
变换模块
114
AddRoundKey
变换模块
115
选择器
166
475
463
163
170

图54B

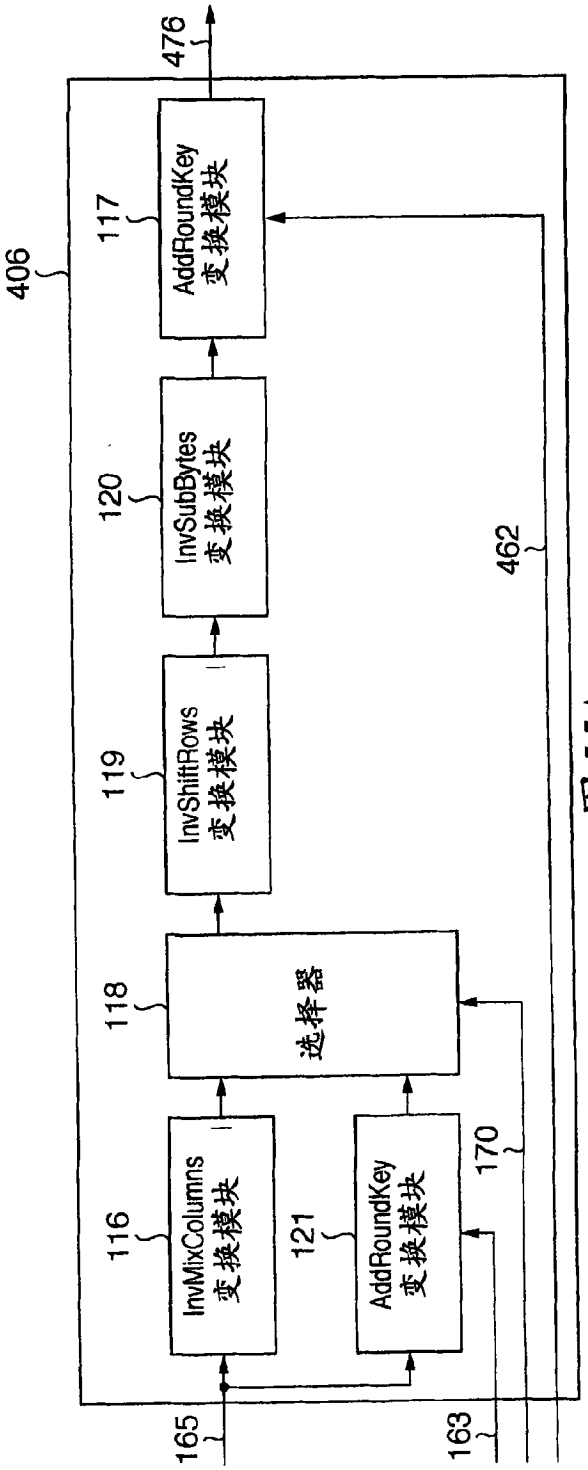

406
476
117
AddRoundKey
变换模块
120
InvSubBytes
变换模块
119
InvShiftRows
变换模块
118
选择器
116
InvMixColumns
变换模块
121
AddRoundKey
变换模块
165
163
170
462

图 55A

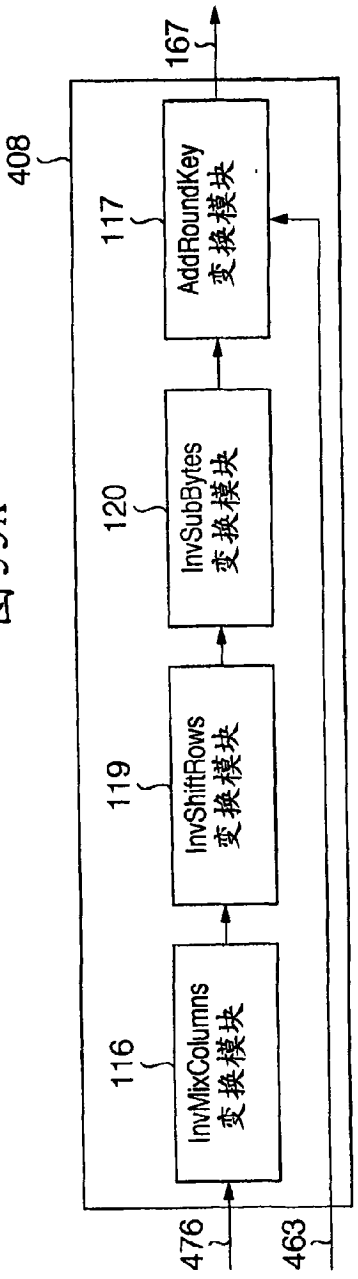

408
167
117
AddRoundKey
变换模块
120
InvSubBytes
变换模块
119
InvShiftRows
变换模块
116
InvMixColumns
变换模块
476
463

图 55B

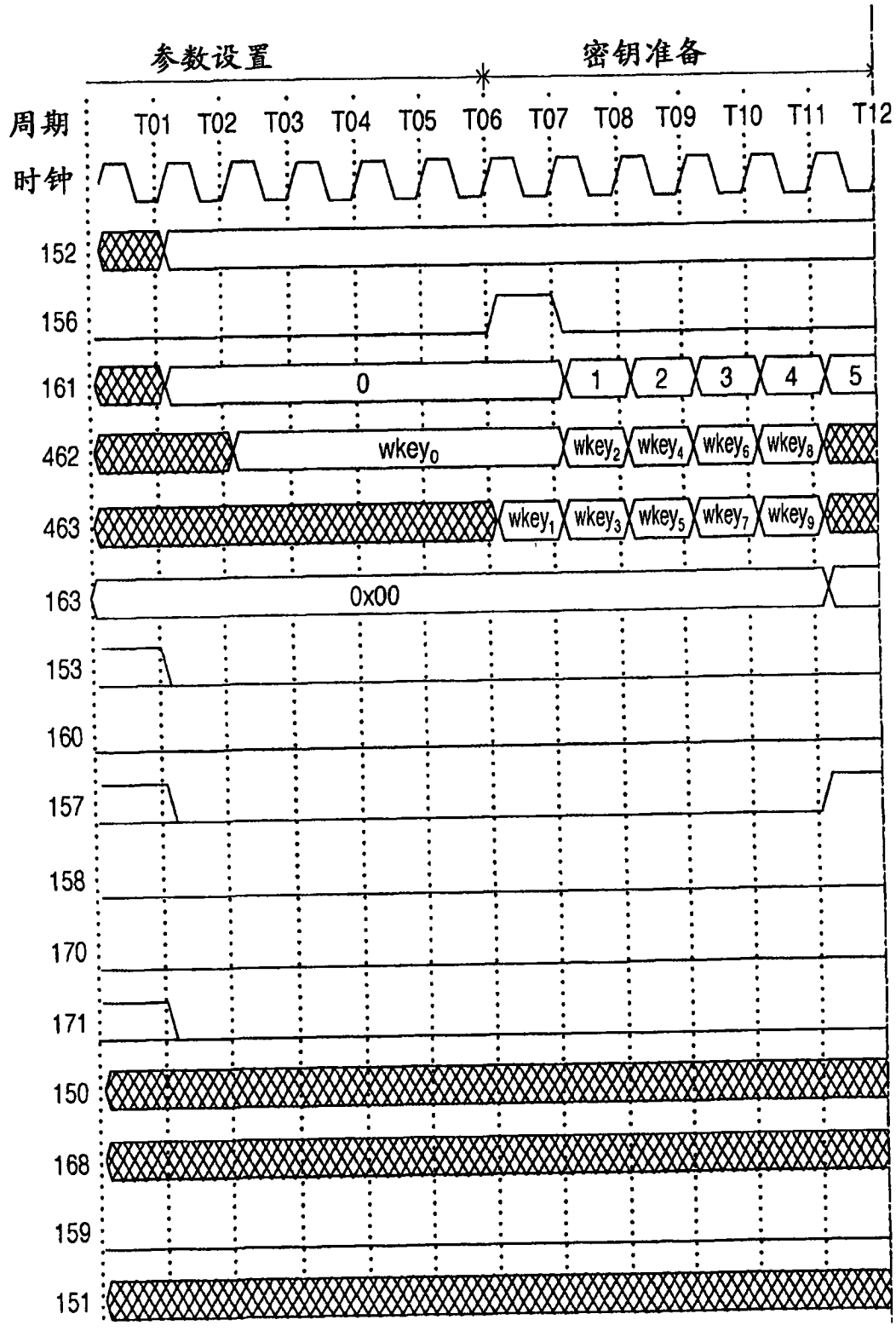

参数设置
密钥准备
周期
T01 T02 T03 T04 T05 T06 T07 T08 T09 T10 T11 T12
时钟
152
156
161
0 1 2 3 4 5
462
wkey0 wkey2 wkey4 wkey6 wkey8
463
wkey1 wkey3 wkey5 wkey7 wkey9
163
0x00
153
160
157
158
170
171
150
168
159
151

图 56A

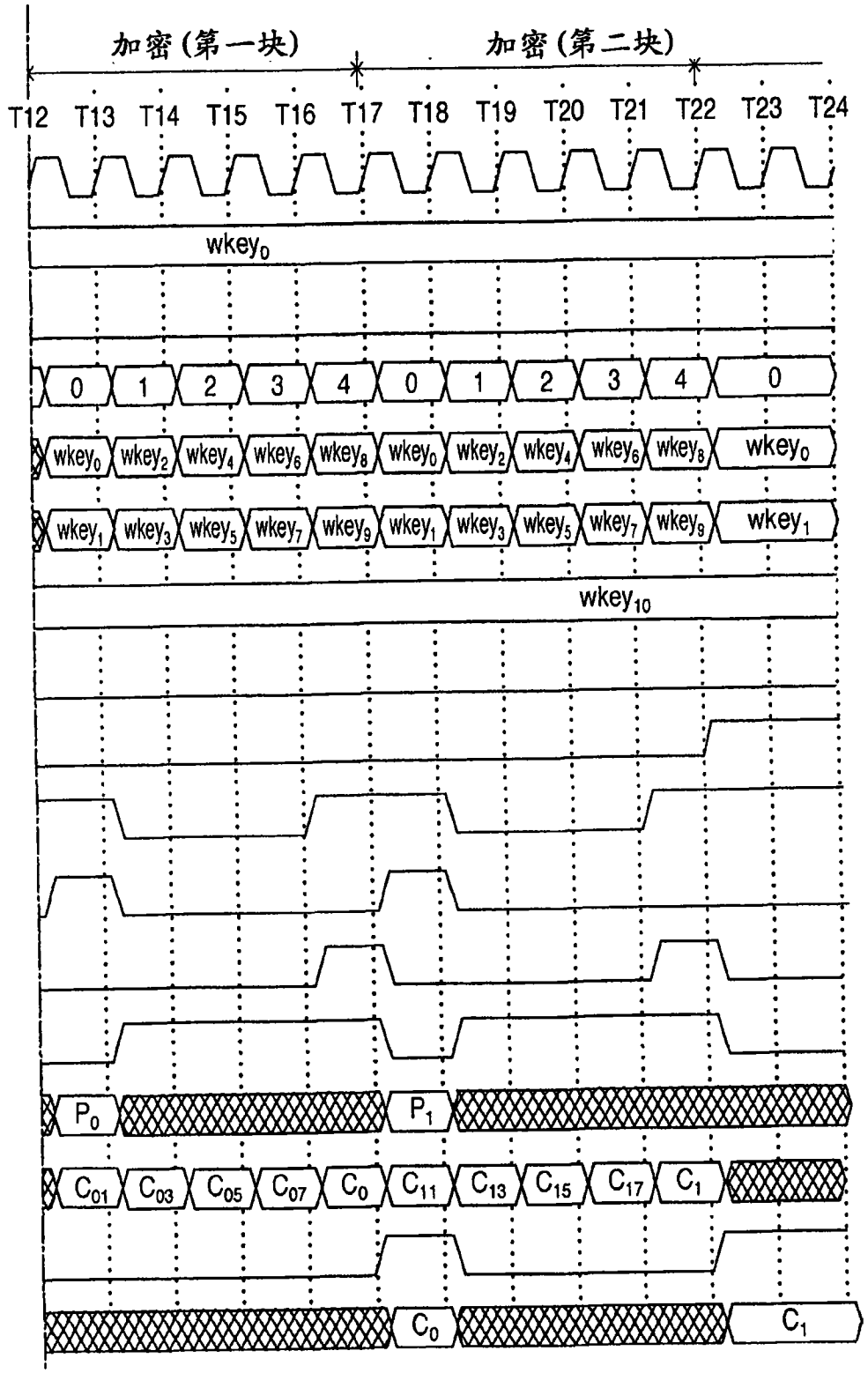

加密(第一块)
加密(第二块)
T12 T13 T14 T15 T16 T17 T18 T19 T20 T21 T22 T23 T24
wkey0
0 1 2 3 4 0 1 2 3 4 0
wkey0 wkey2 wkey4 wkey6 wkey8 wkey0 wkey2 wkey4 wkey6 wkey8 wkey0
wkey1 wkey3 wkey5 wkey7 wkey9 wkey1 wkey3 wkey5 wkey7 wkey9 wkey1
wkey10
P0 P1
C01 C03 C05 C07 C0 C11 C13 C15 C17 C1
C0 C1

图 56B

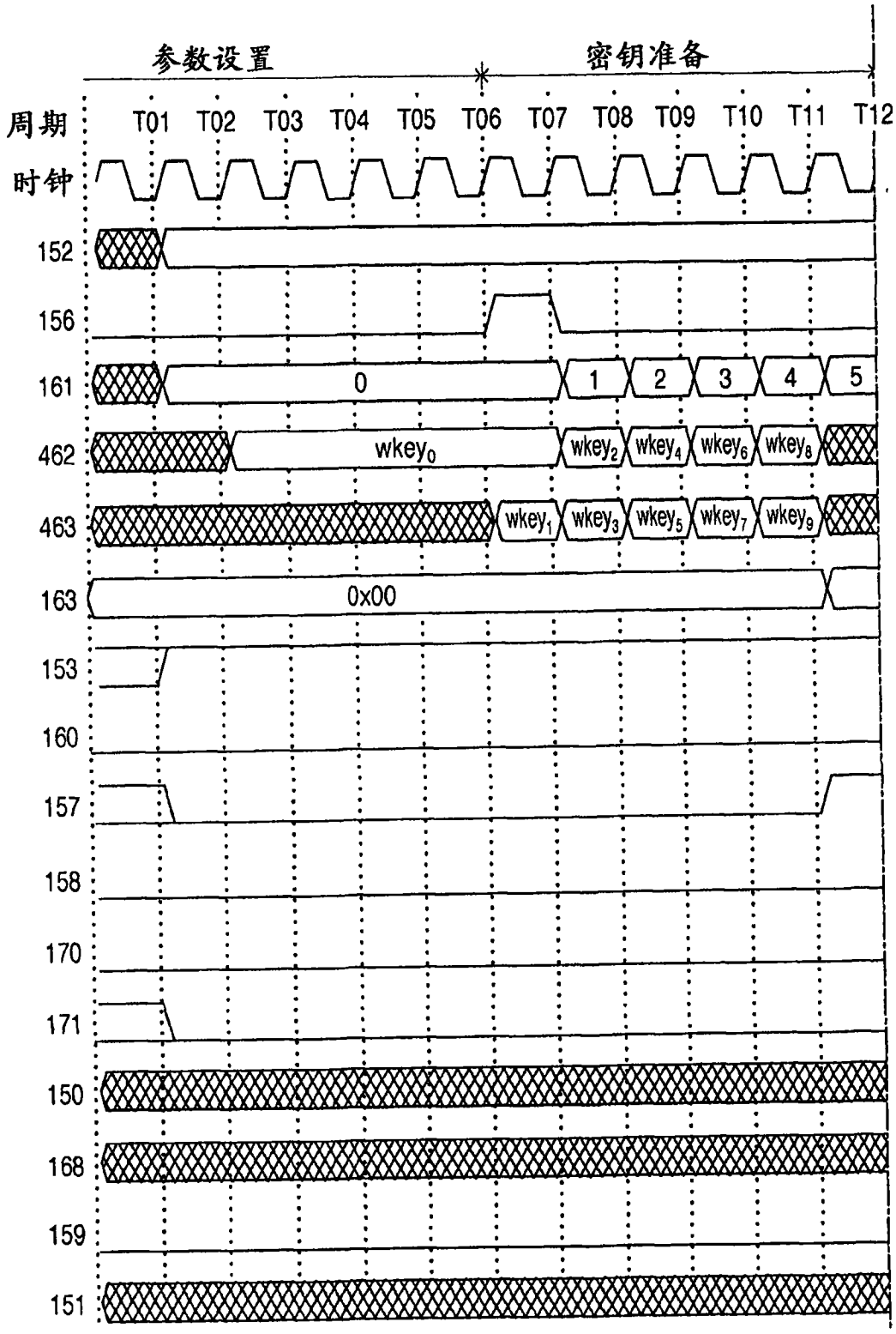

参数设置
密钥准备
周期
T01 T02 T03 T04 T05 T06 T07 T08 T09 T10 T11 T12
时钟
152
156
161
0 1 2 3 4 5
462
wkey0 wkey2 wkey4 wkey6 wkey8
463
wkey1 wkey3 wkey5 wkey7 wkey9
163
0x00
153
160
157
158
170
171
150
168
159
151

图 57A

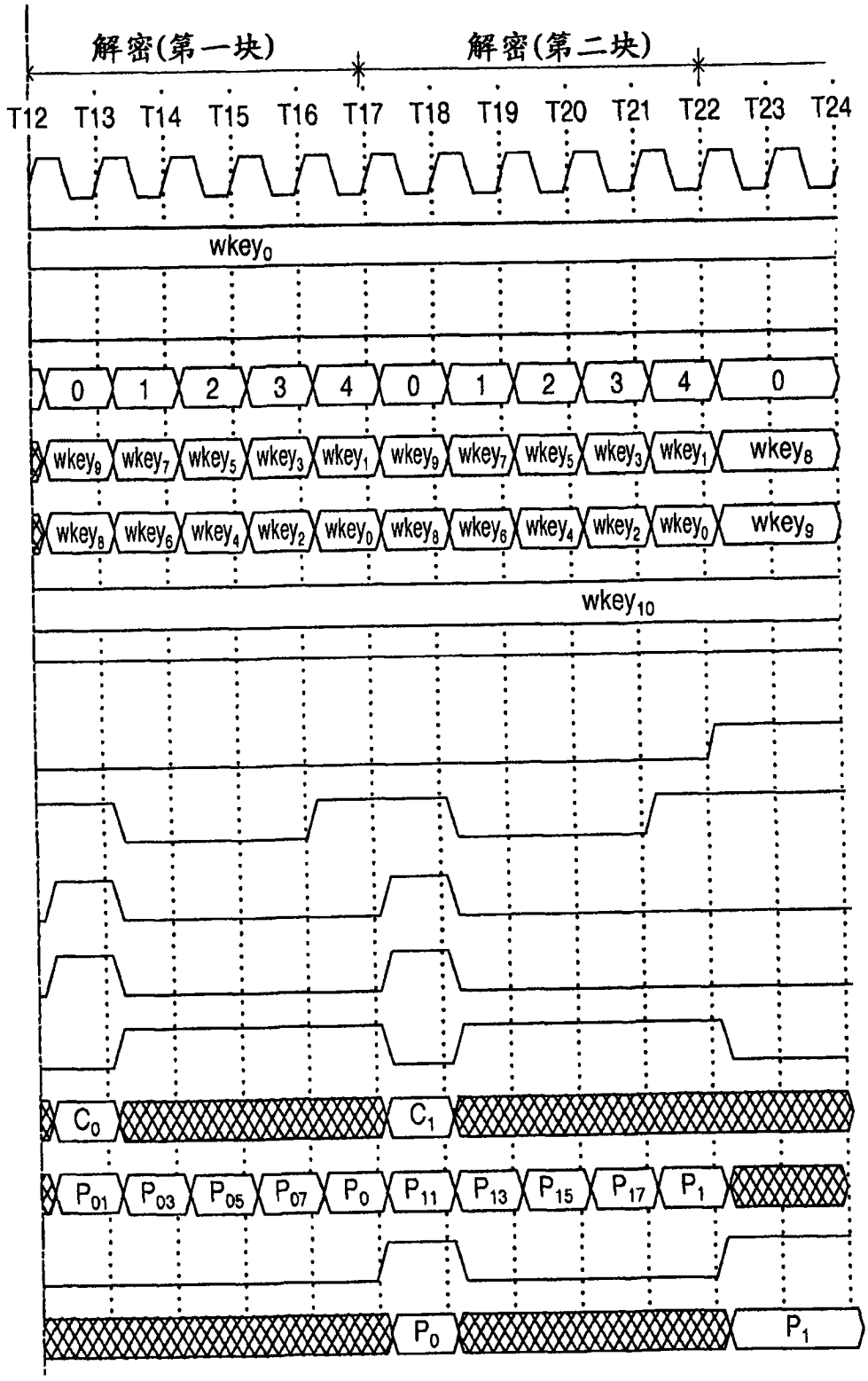

解密(第一块)
解密(第二块)
T12 T13 T14 T15 T16 T17 T18 T19 T20 T21 T22 T23 T24
wkey0
0 1 2 3 4 0 1 2 3 4 0
wkey9 wkey7 wkey5 wkey3 wkey1 wkey9 wkey7 wkey5 wkey3 wkey1 wkey8
wkey8 wkey6 wkey4 wkey2 wkey0 wkey8 wkey6 wkey4 wkey2 wkey0 wkey9
wkey10
C0 C1
P01 P03 P05 P07 P0 P11 P13 P15 P17 P1
P0 P1

图 57B

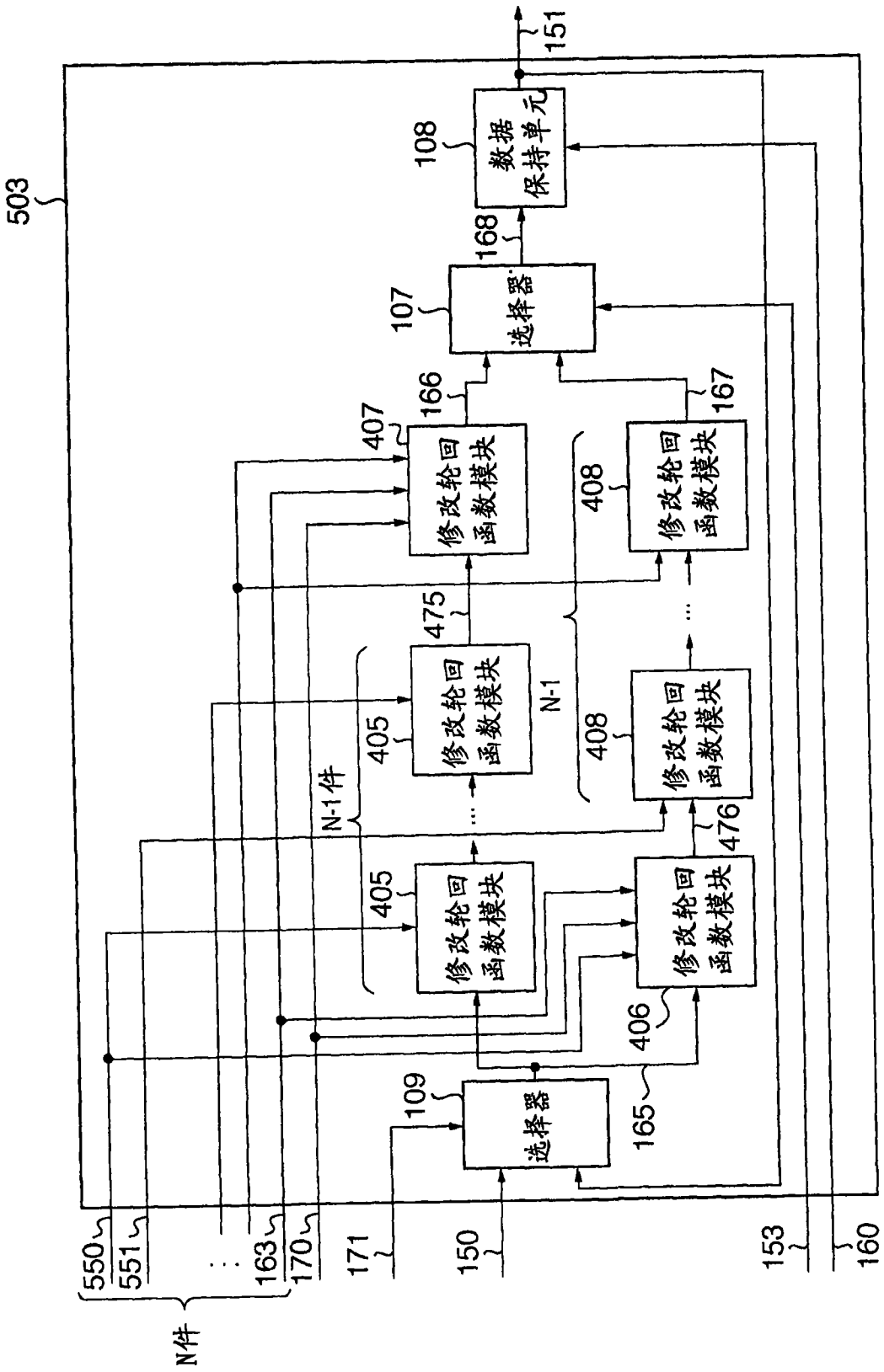

503
151
108
数据保持单元
168
107
选择器
166
167
407
408
修改轮回函数模块
475
N-1
405
N-1件
476
406
165
109
选择器
550
551
163
170
171
150
153
160
N件

图58

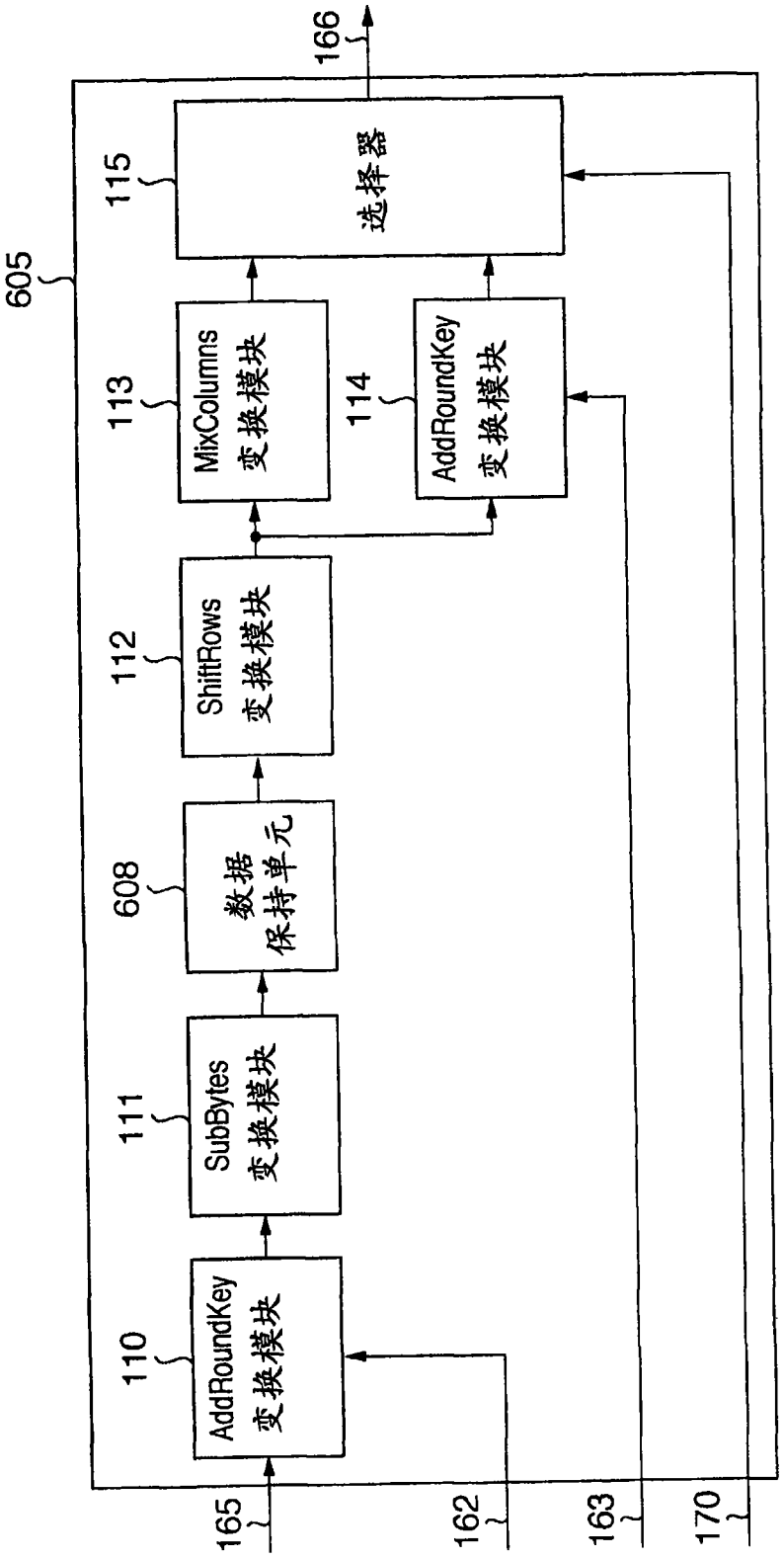

605
166
115
选择器
113
MixColumns
变换模块
114
AddRoundKey
变换模块
112
ShiftRows
变换模块
608
数据
保持单元
111
SubBytes
变换模块
110
AddRoundKey
变换模块
165
162
163
170

图 59

```
AddRoundKey ( )

For round = 1 step 1 to Nr-1
    InvShiftRows ( )
    InvSubBytes ( )
    AddRoundKey ( )
    InvMixColumns ( )
End for

InvShiftRows ( )
InvSubBytes ( )
AddRoundKey ( )
```

解密算法

图60B

```
AddRoundKey ( )

For round = 1 step 1 to Nr-1
    SubBytes ( )
    ShiftRows ( )
    MixColumns ( )
    AddRoundKey ( )
End for

SubBytes ( )
ShiftRows ( )
AddRoundKey ( )
```

加密算法

图60A

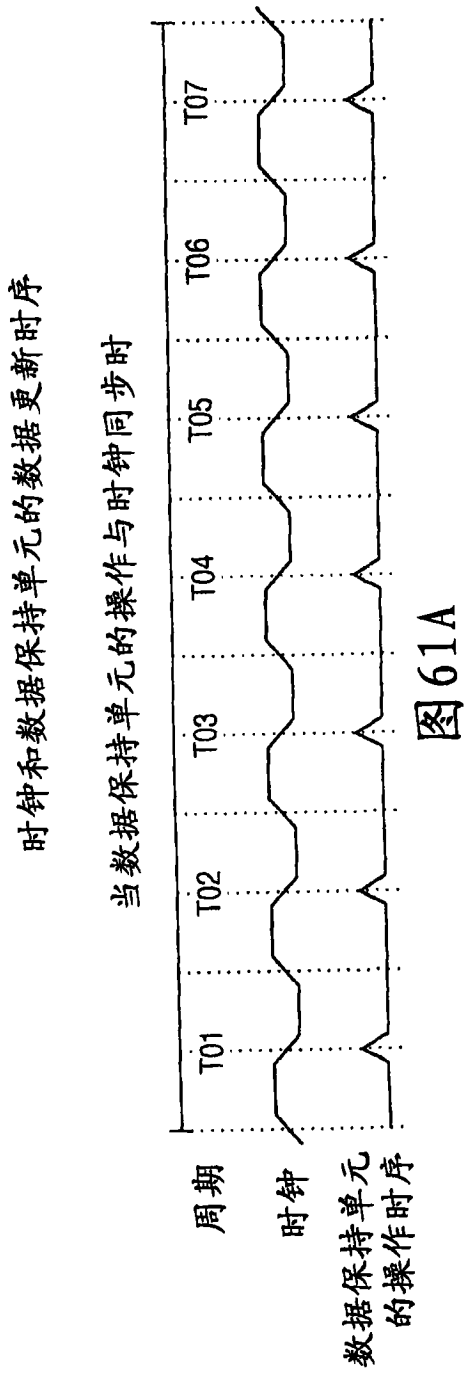


图61A

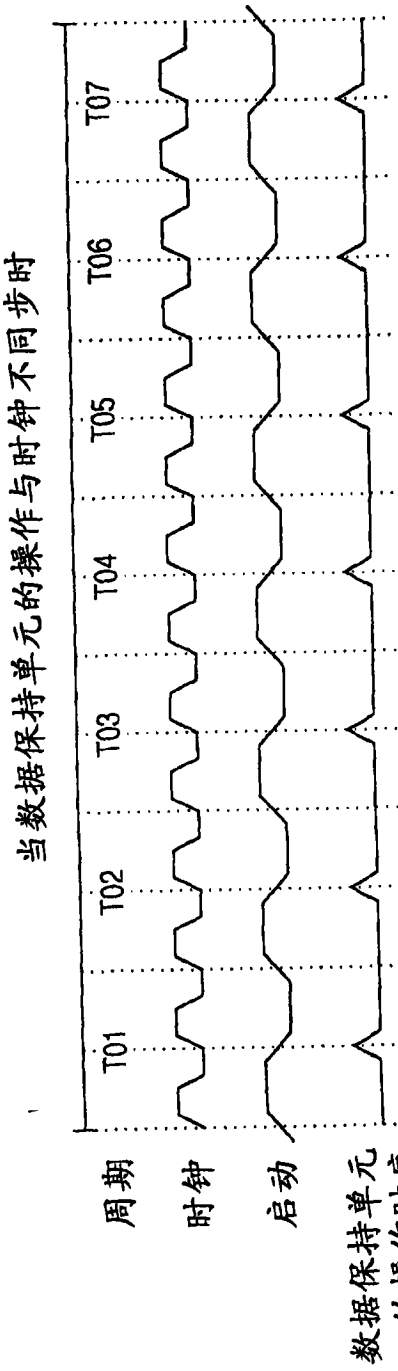

当数据保持单元的操作与时钟不同步时
T01
T02
T03
T04
T05
T06
T07
周期
时钟
启动
数据保持单元
的操作时序

图61B

另一实施方法

从处理开始的时钟周期号	第一实施例	
	要执行的处理	要使用的轮回密钥
0	· AddRoundKey · SubBytes · ShiftRows · MixColumns	·第0轮回密钥($wkey_0$)
1	· AddRoundKey · SubBytes · ShiftRows · MixColumns	·第1轮回密钥($wkey_1$)
7	· AddRoundKey · SubBytes · ShiftRows · MixColumns · AddRoundKey	·第7轮回密钥($wkey_7$) ·第8轮回密钥($wkey_8$)
8	· SubBytes · ShiftRows · MixColumns · AddRoundKey	·第9轮回密钥($wkey_9$)
9	· SubBytes · ShiftRows · AddRoundKey	·第10轮回密钥($wkey_{10}$)

图 62