[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/06 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200510125164.8

[43] 公开日 2006 年 6 月 7 日

[11] 公开号 CN 1783774A

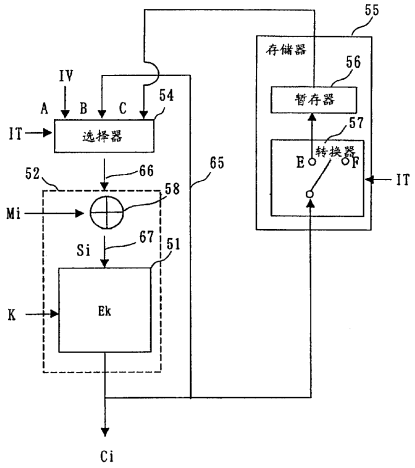
[22] 申请日 2000.12.22
[21] 申请号 200510125164.8
分案原申请号 00805031.7
[30] 优先权
[32] 2000. 1.14 [33] JP [31] 5161/00
[71] 申请人 三菱电机株式会社
地址 日本东京
[72] 发明人 反町亨 时田俊雄
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 浦柏明 张志醒
权利要求书 5 页 说明书 36 页 附图 49 页

[54] 发明名称

加密装置和加密方法及解密装置和解密方法

[57] 摘要

为在加密过程中进行其他数据的加密，配置存储器(55)，其针对用于从使用加密键 K 的加密模块(51)反馈至选择器(54)的反馈线(65)被并行设置。当在明文块数据 M_i 的处理过程中发生了对其他数据明文块数据 N_i 进行处理的中断 IT 时，将中断 IT 发生时的密文块数据 C_i 存储于暂存器(56)中，当明文块数据 N_i 的处理结束时，通过由选择器选择存储器(55)所存储的密文块数据 C_i，并开始明文块数据 M_{i+1} 的处理。



1. 一种加密装置，用于将由 1 个以上明文块数据所组成的明文通过加密单元加密成密文，并针对密文生成为保证密文完整性的认证码，其特征在于：包括

加密部，具有在对明文块数据通过加密单元加密后，将加密单元输出的密文块数据 C_i 反馈至加密单元的第 1 反馈回路，并用于输入明文块数据，而且通过第 1 反馈回路反馈密文块数据 C_i 进行加密处理，输出密文块数据；

认证码生成部，具有用于反馈认证码演算中间结果的第 2 反馈回路，每当从加密部输出密文块数据时，用于输入密文块数据，进行数据处理，并通过第 2 反馈回路反馈认证码演算中间结果，从而生成为保证密文完整性的认证码。

2. 权利要求 1 记载的加密装置，其特征还在于：

所述加密部和认证码生成部，兼用单一加密模块和单一反馈回路并交互进行加密处理和认证码生成处理，同时

所述单一反馈回路，包括

用于分别记录并输出加密处理和认证码生成处理结果的存储器；

用于为交互进行加密处理和认证码生成处理，而从存储器交互选择加密处理和认证码生成处理的结果，并输出至加密模块的选择器。

3. 一种加密方法，用于将由 1 个以上明文块数据所组成的明文通过加密单元加密成密文，并针对密文生成为保证密文完整性的认证码，其特征在于，包括以下步骤：

加密步骤，具有在对明文块数据通过加密单元进行加密后，将加密单元输出的密文块数据 C_i 反馈至加密单元的第 1 反馈步骤，并输入明文块数据，而且通过第 1 反馈回路反馈密文块数据 C_i 进行加密处理，输出密文块数据；

认证码生成步骤，具有反馈认证码演算中间结果的第 2 反馈步骤，每当从加密步骤输出密文块数据时，输入密文块数据，进行数据处理，并通过第 2 反馈步骤反馈认证码演算中间结果，从而生成为保证密文完整性的认证码。

4. 一种解密装置，用于将由 1 个以上密文块数据所组成的密文解密成明文，并针对密文生成为确认密文完整性的认证码，其特征在于：包括

解密部，具有通过解密模块对数据进行解密后，将所生成的模块输出块数据 T_i 反馈至解密模块的第 1 反馈回路，并用于输入密文块数据，而且通过第 1 反馈回路反馈模块输出块数据 T_i 进行解密处理，输出明文块数据；

认证码生成部，具有用于反馈认证码演算中间结果的第 2 反馈回路，并用于输入与输入到解密部的密文块数据相同的密文块数据，进行数据处理输出认证码演算中间结果，并通过第 2 反馈回路反馈认证码演算中间结果，从而生成为确认密文完整性的认证码。

5. 权利要求 4 记载的解密装置，其特征还在于：

所述解密部和认证码生成部，兼用单一解密模块和单一反馈回路并交互进行解密处理和认证码生成处理，同时

所述单一反馈回路，包括

用于分别记录并输出解密处理和认证码生成处理结果的存储器；

用于为交互进行解密处理和认证码生成处理，而从存储器交互选择解密处理和认证码生成处理的结果，并输出至解密模块的选择器。

6. 一种解密方法，用于将由 1 个以上密文块数据所组成的密文解密成明文，并针对密文生成为确认密文完整性的认证码，其特征在于，包括以下步骤：

解密步骤，具有通过解密模块对数据进行解密后，将所生成的模块输出块数据 T_i 反馈至解密模块的第 1 反馈步骤，并输入密文块数据，而且通过第 1 反馈回路反馈模块输出块数据 T_i 进行解密处理，输出明文块数据；

认证码生成步骤，具有用于反馈认证码演算中间结果的第 2 反馈步骤，并输入与输入到解密步骤的密文块数据相同的密文块数据，进行数据处理输出认证码演算中间结果，并通过第 2 反馈步骤反馈认证码演算中间结果，从而生成为确认密文完整性的认证码。

7. 一种加密装置，用于将由 1 个以上明文块数据所组成的明文通过加密模块加密成密文，并针对密文生成为保证密文完整性的认证码，其特征在于：包括

加密部，具有在通过加密模块对明文块数据进行加密后，将加密模块输出的模块输出块数据 T_i 反馈至加密模块的第 1 反馈回路，并用于输入明文块数据，而且通过第 1 反馈回路反馈模块输出块数据 T_i 进行加密处理，输出密文块数据；

认证码生成部，具有用于反馈认证码演算中间结果的第 2 反馈回路，每当从加密部输出密文块数据时，用于输入密文块数据，进行数据处理，并通过第 2 反馈回路反馈认证码演算中间结果，从而生成为保证密文完整性的认证码。

8. 权利要求 7 记载的加密装置，其特征还在于：

所述加密部和认证码生成部，兼用单一加密模块和单一反馈回路并交互进行加密处理和认证码生成处理，同时

所述单一反馈回路，包括

用于分别记录并输出加密处理和认证码生成处理结果的存储器；

用于为交互进行加密处理和认证码生成处理，而从存储器交互选择加密处理和认证码生成处理的结果，并输出至加密模块的选择器。

9. 一种加密方法，用于将由 1 个以上明文块数据所组成的明文通过加密模块加密成密文，并针对密文生成为保证密文完整性的认证码，其特征在于，包括以下步骤：

加密步骤，具有在通过加密模块对明文块数据进行加密后，将加密模块所输出的模块输出块数据 T_i 反馈至加密模块的第 1 反馈步骤，并输入明文块数据，而且通过第 1 反馈回路反馈模块输出块数据 T_i 进行加密处理，输出密文块数据；

认证码生成步骤，具有用于反馈认证码演算中间结果的第 2 反馈步骤，每当从加密步骤输出密文块数据时，用于输入密文块数据，进行数据处理，并通过第 2 反馈步骤反馈认证码演算中间结果，从而生成为保证密文完整性的认证码。

10. 一种解密装置，用于将由 1 个以上密文块数据所组成的密文通过解密单元解密成明文，并针对密文生成为确认密文完整性的认证码，其特征在于：包括

解密部，具有将密文块数据 C_i 反馈至解密单元的第 1 反馈回路，并用于输入密文块数据，而且通过第 1 反馈回路反馈密文块数据 C_i 进行解密处理，输出明文块数据；

认证码生成部，具有用于反馈认证码演算中间结果的第 2 反馈回路，并用于输入与输入到解密部的密文块数据相同的密文块数据，进行数据处理输出认证码演算中间结果，并通过第 2 反馈回路反馈认证码演算中间结果，从而生成为确认密文完整性的认证码。

11. 权利要求 10 记载的解密装置，其特征还在于：

所述解密部和认证码生成部，兼用单一解密模块和单一反馈回路并交互进行解密处理和认证码生成处理，同时

所述单一反馈回路，包括

用于分别记录并输出解密处理和认证码生成处理结果的存储器；

用于为交互进行解密处理和认证码生成处理，而从存储器交互选择解密处理和认证码生成处理的结果，并输出至解密模块的选择器。

12. 一种解密方法，用于将由 1 个以上密文块数据所组成的密文通过解密单元解密成明文，并针对密文生成为确认密文完整性的认证码，其特征在于，包括以下步骤：

解密步骤，具有将密文块数据 C_i 反馈至解密单元的第 1 反馈步骤，并输入密文块数据，而且通过第 1 反馈回路反馈密文块数据 C_i 进行解密处理，输出明文块数据；

认证码生成步骤，具有用于反馈认证码演算中间结果的第 2 反馈步骤，并输入与输入到解密步骤的密文块数据相同的密文块数据，进行数据处理输出认证码演算中间结果，并通过第 2 反馈步骤反馈认证码演算中间结果，从而生成为确认密文完整性的认证码。

13. 一种加密装置，其特征在于：

包括

输入数据进行加密，并输出密码数据的加密部；

输入加密部所输出的密码数据，并生成为保证密文完整性的认证码的认证码生成部，

认证码生成部，在加密部完成数据加密之前，既开始认证码的生成。

14. 一种解密装置，其特征在于：

包括

输入数据进行解密，并输出解密数据的解密部；

输入解密部所输入的数据，并生成为保证密文完整性的认证码的认证码生成部，

认证码生成部，在解密部完成数据解密之前，既开始认证码的生成。

15. 一种加密方法，其特征在于：

包括

输入数据进行加密，并输出密码数据的加密步骤；

输入加密步骤所输出的密码数据，并生成为保证密文完整性的认证码的认证码生成步骤，

认证码生成步骤，在加密步骤完成数据加密之前，既开始认证码的生成。

16. 一种解密方法，其特征在于：

包括

输入数据进行解密，并输出解密数据的解密步骤；

输入解密步骤所输入的数据，并生成为保证密文完整性的认证码的认证码生成步骤，

认证码生成步骤，在解密步骤完成数据解密之前，既开始认证码的生成。

加密装置和加密方法及解密装置和解密方法

本申请是下述申请的分案申请:

发明名称:“加密装置和加密方法及解密装置和解密方法以及用于记录程序的计算机可读取记录媒体”

申请日:2000年12月22日

申请号:00805031.7(PCT/JP00/09129)

技术领域

本发明所涉及的是一种加密、解密装置以及加密、解密方法,特别是在数据的加密、解密过程中,能够进行其他数据的加密、解密处理。

背景技术

图43是基于加密块连锁模式(cipher block chaining mode,以下称CBC模式)的加密装置的示意图。

在图43所示的CBC模式加密方法中,是以块为单位输入64位明文块数据M_i,并通过使用加密键K的加密模块51进行加密,然后再将此加密后的密文块数据C_i与下一个明文块数据M_{i+1}进行“异”逻辑演算,并将“异”逻辑演算的结果作为下次加密处理的输入,提供至使用加密键K的加密模块51。于是,通过反复此处理使彼此链接,就能将整个明文M加密成密文C。

图44是采用CBC模式的解密装置的示意图。

图44所示的解密装置,是用来对由图43所示的加密装置所加密的密文进行解密的装置。密文块数据C_1输入到使用加密键K的解密模块71,并与初始值IV进行“异”逻辑演算,解密成明文块数据M_1。当输入密文块数据C_2时,则在使用加密键K的解密模块71解密,然后与先前输入并储存在暂存器111的密文块数据C_1进行“异”逻辑演算,进而解密成明文块数据M_2。

在这里,暂存器111亦可设置于选择器73的内部。

如果明文块数据以M_i($i=1, 2, \cdots\cdots, n$)表示,密文块数据以

C_i（i = 1，2，……，n）表示，使用加密键 K 的加密处理以 E_K 表示，使用加密键 K 的解密处理以 D_K 表示的话，则 CBC 模式可以用以下公式表示：

$C_1 = E_K(M_1 \quad EXR \quad IV)$

$C_i = E_K(M_i \quad EXR \quad C_{i-1})$（i = 2，3，……，n）

$M_1 = D_K(C_1) \quad EXR \quad IV$

$M_i = D_K(C_i) \quad EXR \quad C_{i-1}$（i = 2，3，……，n）

这里，EXR 表示“异”逻辑演算。IV（Initial Value）为初始值，在最初的加密和解密处理时被使用。初始值 IV 在加密端和解密端采用相同的值。

图 45 是输出反馈模式（Output Feedback Mode，以下称 OFB 模式）的加密装置示意图。

图 46 是 OFB 模式的解密装置的示意图。

图 47 是加密反馈模式（Cipher Feedback Mode，以下称 CFB 模式）的加密装置示意图。

图 46 是 CFB 模式的解密装置的示意图。

在这里，暂存器 111 亦可设置于选择器 73 的内部。

图 49 是用 CBC 模式的加密装置对明文 M 和明文 N 进行加密处理步骤的示意图。

在这里，对明文 M 由明文块数据 M_1、明文块数据 M_2、和明文块数据 M_3 所构成，而明文 N 只由明文块数据 N_1 所构成的情况进行说明。

当开始明文块数据 M_1 的加密处理后，则密文块数据 C_1 在被输出的同时，密文块数据 C_1 还被用于明文块数据 M_2 的加密处理。如此，密文块数据 C_i 被反馈到明文块数据 M_{i+1} 的加密处理中进行连锁处理。因此，明文块数据 M_1 到明文块数据 M_3 的加密处理未结束，就不能进行明文块数据 N_1 的加密处理。

图 50 与图 49 同样，表示以 CBC 模式进行加密处理的情况。

在图 50 中，表示了为准备明文块数据 M_1、明文块数据 M_2、和明文块数据 M_3 所花费时间的情况。另一方面，加密处理在下一个明文块数据 M_{i+1} 准备完成前结束，会出现空闲的时间（例如 T1～T2、T3～T4 的时间）。如此，即使是出现空闲时间，由于密文块数据 C_i 必须反馈到下一个明文块数据 M_{i+1} 进行链锁处理，所以明文块数据 N_1 的

加密不得不等到明文块数据 M_3 的处理结束后再进行。

图 51 是数据保密处理和保证数据完整性处理的示意图。例如，明文 M 是利用 OFB 模式的加密装置被加密成密文 C。利用 CBC 模式的加密装置演算出认证码 P，并将认证码 P 附加在密文 C 的最后。当接收到被加密、且附加了认证码 P 的数据时，利用 OFB 模式的解密装置从密文 C 解密成明文 M，同时利用 CBC 模式的解密装置从密文 C 演算出认证码 P，并与传送来的认证码 P 比较是否相同，由此可以确认传送来的 C 是否被篡改。

图 52 是图 51 所示的保密处理和认证码演算处理步骤的示意图。

明文块数据 M_1～明文块数据 M_3 依序加密成密文块数据 C_1～密文块数据 C_3。然后，依序输入密文块数据 C_1～密文块数据 C_3 从而演算出认证码 P。

在图 42～图 48 所示的各模式的加密装置和解密装置中，由于必须将前一块数据的加密、解密数据反馈到下一个块数据的加密、解密处理上，所以一旦加密处理或解密处理开始后，只要整个处理不结束，就不能开始其他的加密处理或解密处理。这样一来，如果先前开始了的加密、解密处理需要很长时间的话，则以后开始的加密、解密处理就要等很长的时间。

另外，当加密、解密处理所需要的时间比准备加密、解密数据所需要的时间短时，则加密、解密装置会出现空闲时间。

而且，当进行保密处理和保证完整性处理时，必须在进行保密处理之后再进行保证完整性处理，因而处理很花费时间。

本发明理想的实施方式的目的，是提供一种在进行某数据的加密、解密处理过程中，能对其他数据进行加密、解密处理的加密装置、解密装置、加密方法和解密方法。

另外，在本发明理想的实施方式中，可以对优先权较高的数据优先进行加密、解密处理。

另外，在本发明理想的实施方式中，可以高速并行地进行保密处理和保证保证完整性处理。

发明内容

本发明的加密装置，用于进行第 1 处理数据和第 2 处理数据的加

密处理，其特征在于：

包括存储加密处理状态的存储器，

用于在第1处理数据的加密处理结束之前开始第2处理数据的加密处理，在开始第2处理数据的加密处理时将第1处理数据的加密处理状态存储于所述存储器中，当再开始第1处理数据的加密处理时，首先将加密装置的加密处理状态恢复到存储器所存储的第1处理数据的加密处理状态后再开始第1处理数据的加密处理。

所述加密装置，其特征还在于：

在第2处理数据的加密处理结束之前再开始第1处理数据的加密处理，当再开始第1处理数据的加密处理时所述存储器存储第2处理数据的加密处理状态，当再开始第2处理数据的加密处理时，首先将加密装置的加密处理状态恢复到存储器所存储的第2处理数据的加密处理状态后再开始第2处理数据的加密处理。

以所述第1处理数据是第1明文，所述第2处理数据是第2明文为特征。

以所述加密装置通过中断开始第2处理数据的加密处理为特征。

本发明的加密装置，用于对构成明文M的明文块数据M_i（i＝1，2，3，……）和构成明文N的明文块数据N_j（j＝1，2，3，……）进行加密，其特征在于：包括

机构，用于在明文M的加密处理过程中接收在明文M的加密处理结束之前的明文N的加密要求；

加密单元，用于对明文块数据M_i进行加密处理并输出密文块数据C_i；

反馈回路，用于将加密单元所输出的密文块数据C_i通过反馈线反馈到加密单元；

存储器，与反馈回路的反馈线并行设置，当由于接收所述明文N的加密要求，开始明文N的某一明文块数据的加密处理，而紧接在明文块数据M_i之后，不继续接着进行所述明文块数据M_{i+1}的加密处理时，用于存储被反馈的密文块数据C_i；

选择器，当明文块数据M_{i+1}继续接着明文块数据M_i进行加密时，用于选择由所述反馈回路的反馈线所反馈的密文块数据C_i并提供至

反馈回路，当所述明文块数据 M_{i+1} 不是继续接着明文块数据 M_i 进行加密，而是接着明文 N 的某一明文块数据进行加密时，用于选择所述存储器所存储的密文块数据 C_i 并提供至反馈回路。

所述存储器，其特征在于：包括

对应多件明文的多个暂存器；

根据加密处理的明文而对暂存器进行转换的转换器。

本发明的加密方法，其特征是包括以下步骤：

利用加密模块所输出的密文块数据 C_i（$i=1, 2, 3, \ldots\ldots$）对第 1 明文 M 的明文块数据 M_i（$i=1, 2, 3, \ldots\ldots$）进行加密；

在所述明文块数据 M_i 的加密过程中或是明文块数据 M_i 的加密之后，将用于第 1 明文 M 的明文块数据 M_{i+1} 加密的密文块数据 C_i 存储于存储器；

在将用于所述明文块数据 M_{i+1} 加密的密文块数据 C_i 存储于存储器之后，对第 2 明文 N 的至少 1 个明文块数据进行加密；

在对所述第 2 明文 N 的至少 1 个明文块数据进行加密之后，输入存储器所存储的用于明文块数据 M_{i+1} 加密的密文块数据 C_i，并利用加密模块对第 1 明文 M 的明文块数据 M_{i+1} 进行加密。

本发明的加密装置，用于通过加密单元将由 1 个以上明文块数据所组成的明文加密成密文，并针对密文生成为保证密文完整性的认证码，其特征在于：包括

加密部，具有在通过加密单元对明文块数据进行加密后，将加密单元输出的密文块数据 C_i 反馈至加密单元的第 1 反馈回路，并用于输入明文块数据，而且通过第 1 反馈回路反馈密文块数据 C_i 进行加密处理，输出密文块数据；

认证码生成部，具有用于反馈认证码演算中间结果的第 2 反馈回路，每当从加密部输出密文块数据时，用于输入密文块数据，进行数据处理，并通过第 2 反馈回路反馈认证码演算中间结果，从而生成为保证密文完整性的认证码。

所述加密部和认证码生成部，兼用单一加密模块和单一反馈回路并交互进行加密处理和认证码生成处理，同时

所述单一反馈回路，其特征在于：包括

用于分别记录并输出加密处理和认证码生成处理结果的存储

器；

用于为交互进行加密处理和认证码生成处理，而从存储器交互选择加密处理和认证码生成处理的结果，并输出至加密模块的选择器。

本发明的加密方法，用于通过加密单元将由 1 个以上明文块数据所组成的明文加密成密文，并针对密文生成为保证密文完整性的认证码，其特征在于：包括

加密步骤，具有在通过加密单元对明文块数据进行加密后，将加密单元输出的密文块数据 C_i 反馈至加密单元的第 1 反馈步骤，并输入明文块数据，而且通过第 1 反馈回路反馈密文块数据 C_i 进行加密处理，输出密文块数据；

认证码生成步骤，具有反馈认证码演算中间结果的第 2 反馈步骤，每当从加密步骤输出密文块数据时，输入密文块数据，进行数据处理，并通过第 2 反馈步骤反馈认证码演算中间结果，从而生成为保证密文完整性的认证码。

本发明的解密装置，用于进行第 1 处理数据和第 2 处理数据的解密处理，其特征在于：

包括存储解密处理状态的存储器，

用于在第 1 处理数据的解密处理结束之前开始第 2 处理数据的解密处理，在开始第 2 处理数据的解密处理时将第 1 处理数据的解密处理状态存储于所述存储器中，当再开始第 1 处理数据的解密处理时，首先将解密装置的解密处理状态恢复到存储器所存储的第 1 处理数据的解密处理状态后再开始第 1 处理数据的解密处理。

所述解密装置，其特征还在于：

在第 2 处理数据的解密处理结束之前再开始第 1 处理数据的解密处理，当再开始第 1 处理数据的解密处理时所述存储器存储第 2 处理数据的解密处理状态，当再开始第 2 处理数据的解密处理时，首先将解密装置的解密处理状态恢复到存储器所存储的第 2 处理数据的解密处理状态后再开始第 2 处理数据的解密处理。

以所述第 1 处理数据是第 1 密文，所述第 2 处理数据是第 2 密文为特征。

以所述解密装置通过中断开始第 2 处理数据的最初块数据的解

密处理为特征。

本发明的解密装置，用于对构成密文 C 的密文块数据 C_i（i＝1，2，3，……）和构成密文 D 的密文块数据 D_j（j＝1，2，3，……）进行解密，其特征在于：包括

机构，用于在密文 C 的解密处理过程中的任一时间接收密文 D 的解密要求；

解密单元，用于对密文块数据 C_i 进行解密处理并输出明文块数据 M_i；

反馈回路，用于将为解密密文块数据 C_{i+1} 的密文块数据 C_i 通过反馈线反馈到解密单元；

存储器，与反馈回路的反馈线并行设置，当由于接收所述密文 D 的解密要求，开始密文 D 的某一密文块数据的解密处理，而紧接在密文块数据 C_i 之后，不继续接着进行所述密文块数据 C_{i+1} 的解密处理时，用于存储被反馈的密文块数据 C_i；

选择器，当密文块数据 C_{i+1} 接着密文块数据 C_i 继续进行解密时，用于选择由所述反馈回路的反馈线所反馈的密文块数据 C_i 并提供至反馈回路，当所述密文块数据 C_{i+1} 不是接着密文块数据 C_i 继续进行解密，而是接着密文 D 的某一密文块数据进行解密时，用于选择所述存储器所存储的密文块数据 C_i 并提供至反馈回路。

所述存储器，其特征在于：包括

对应多件密文的多个暂存器；

根据解密处理的密文而对暂存器进行转换的转换器。

本发明的解密方法，其特征是包括以下步骤：

利用解密模块对第 1 密文 C 的密文块数据 C_i（i＝1，2，3，……）进行解密；

在所述密文块数据 C_i 的解密过程中或是密文块数据 C_i 的解密之后，将第 1 密文 C 的密文块数据 C_{i+1} 解密用的密文块数据 C_i 存储于存储器；

在将所述密文块数据 C_{i+1} 解密用的密文块数据 C_i 存储于存储器之后，对第 2 密文 D 的至少 1 个密文块数据进行解密；

在对所述第 2 密文 D 的至少 1 个密文块数据进行解密之后，输入存储器所存储的用于密文块数据 C_{i+1} 解密的密文块数据 C_i，并利用

解密模块对第 1 密文 C 的密文块数据 C_{i+1} 进行解密。

本发明的解密装置，用于将由 1 个以上密文块数据所组成的密文解密成明文，并针对密文生成为确认密文完整性的认证码，其特征在于：包括

解密部，具有在通过解密模块对数据进行解密后，将所生成的模块输出块数据 T_i 反馈至解密模块的第 1 反馈回路，并用于输入密文块数据，而且通过第 1 反馈回路反馈模块输出块数据 T_i 进行解密处理，输出明文块数据；

认证码生成部，具有用于反馈认证码演算中间结果的第 2 反馈回路，并用于输入与输入到解密部的密文块数据相同的密文块数据，进行数据处理输出认证码演算中间结果，并通过第 2 反馈回路反馈认证码演算中间结果，从而生成为确认密文完整性的认证码。

所述解密部和认证码生成部，兼用单一解密模块和单一反馈回路并交互进行解密处理和认证码生成处理，同时

所述单一反馈回路，其特征在于：包括

用于分别记录并输出解密处理和认证码生成处理结果的存储器；

用于为交互进行解密处理和认证码生成处理，而从存储器交互选择解密处理和认证码生成处理的结果，并输出至解密模块的选择器。

本发明的解密方法，用于将由 1 个以上密文块数据所组成的密文解密成明文，并针对密文生成为确认密文完整性的认证码，其特征在于：包括

解密步骤，具有在通过解密模块对数据进行解密后，将所生成的模块输出块数据 T_i 反馈至解密模块的第 1 反馈步骤，并输入密文块数据，而且通过第 1 反馈回路反馈模块输出块数据 T_i 进行解密处理，输出明文块数据；

认证码生成步骤，具有用于反馈认证码演算中间结果的第 2 反馈步骤，并输入与输入到解密步骤的密文块数据相同的密文块数据，进行数据处理输出认证码演算中间结果，并通过第 2 反馈步骤反馈认证码演算中间结果，从而生成为确认密文完整性的认证码。

本发明的加密装置，用于对构成明文 M 的明文块数据 M_i（$i = 1$，

2，3，……）和构成明文 N 的明文块数据 N_j（j＝1，2，3，……）进行加密，其特征在于：包括

机构，用于在明文 M 的加密处理过程中接收在明文 M 的加密处理结束之前的明文 N 的加密要求；

加密模块，用于将加密处理了的数据作为模块输出块数据 T_i 进行输出；

反馈回路，用于将加密模块所输出的模块输出块数据 T_i 通过反馈线反馈到加密模块；

存储器，与反馈回路的反馈线并行设置，当由于接收所述明文 N 的加密要求，开始明文 N 的某一明文块数据的加密处理，而紧接在明文块数据 M_i 之后，不继续接着进行所述明文块数据 M_{i+1} 的加密处理时，用于存储被反馈的模块输出块数据 T_i；

选择器，当明文块数据 M_{i+1} 继续接着明文块数据 M_i 进行加密时，用于选择由所述反馈回路的反馈线所反馈的模块输出块数据 T_i 并提供至反馈回路，当所述明文块数据 M_{i+1} 不是继续接着明文块数据 M_i 进行加密，而是接着明文 N 的某一明文块数据进行加密时，用于选择所述存储器所存储的模块输出块数据 T_i 并提供至反馈回路。

所述存储器，其特征在于：包括

对应多件明文的多个暂存器；

根据加密处理的明文而对暂存器进行转换的转换器。

本发明的加密方法，其特征是包括以下步骤：

利用加密模块所输出的模块输出块数据 T_i（i＝1，2，3，……）对第 1 明文 M 的明文块数据 M_i（i＝1，2，3，……）进行加密；

在所述明文块数据 M_i 的加密过程中或是明文块数据 M_i 的加密之后，将用于第 1 明文 M 的明文块数据 M_{i+1} 加密的模块输出块数据 T_i 存储于存储器；

在将用于所述明文块数据 M_{i+1} 加密的模块输出块数据 T_i 存储于存储器之后，对第 2 明文 N 的至少 1 个明文块数据进行加密；

在对所述第 2 明文 N 的至少 1 个明文块数据进行加密之后，输入存储器所存储的用于明文块数据 M_{i+1} 加密的模块输出块数据 T_i，并利用加密模块对第 1 明文 M 的明文块数据 M_{i+1} 进行加密。

本发明的加密装置，用于将由 1 个以上明文块数据所组成的明文

通过加密模块加密成密文，并针对密文生成为保证密文完整性的认证码，其特征在于：包括

加密部，具有在通过加密模块对明文块数据进行加密后，将加密模块输出的模块输出块数据 T_i 反馈至加密模块的第 1 反馈回路，并用于输入明文块数据，而且通过第 1 反馈回路反馈模块输出块数据 T_i 进行加密处理，输出密文块数据；

认证码生成部，具有用于反馈认证码演算中间结果的第 2 反馈回路，每当从加密部输出密文块数据时，用于输入密文块数据，进行数据处理，并通过第 2 反馈回路反馈认证码演算中间结果，从而生成为保证密文完整性的认证码。

所述加密部和认证码生成部，兼用单一加密模块和单一反馈回路并交互进行加密处理和认证码生成处理，同时

所述单一反馈回路，其特征在于：包括

用于分别记录并输出加密处理和认证码生成处理结果的存储器；

用于为交互进行加密处理和认证码生成处理，而从存储器交互选择加密处理和认证码生成处理的结果，并输出至加密模块的选择器。

本发明的加密方法，用于将由 1 个以上明文块数据所组成的明文通过加密模块加密成密文，并针对密文生成为保证密文完整性的认证码，其特征是包括以下步骤：

加密步骤，具有在通过加密模块对明文块数据进行加密后，将加密模块所输出的模块输出块数据 T_i 反馈至加密模块的第 1 反馈步骤，并输入明文块数据，而且通过第 1 反馈回路反馈模块输出块数据 T_i 进行加密处理，输出密文块数据；

认证码生成步骤，具有用于反馈认证码演算中间结果的第 2 反馈步骤，每当从加密步骤输出密文块数据时，用于输入密文块数据，进行数据处理，并通过第 2 反馈步骤反馈认证码演算中间结果，从而生成为保证密文完整性的认证码。

本发明的解密装置，用于对构成密文 C 的密文块数据 C_i（i = 1，2，3，……）和构成密文 D 的密文块数据 D_j（j = 1，2，3，……）进行解密，其特征在于：包括

机构，用于在密文 C 的解密处理过程中的任一时间接收密文 D 的解密要求；

解密模块，用于将经过解密处理的数据作为模块输出块数据 T_i 进行输出；

反馈回路，用于将从解密模块输出的模块输出块数据 T_i 通过反馈线反馈到解密模块；

存储器，与反馈回路的反馈线并行设置，当由于接收所述密文 D 的解密要求，开始密文 D 的某一密文块数据的解密处理，而紧接在密文块数据 C_i 之后，不继续接着进行所述密文块数据 C_{i+1} 的解密处理时，用于存储被反馈的模块输出块数据 T_i；

选择器，当密文块数据 C_{i+1} 接着密文块数据 C_i 继续进行解密时，用于选择由所述反馈回路的反馈线所反馈的模块输出块数据 T_i 并提供至反馈回路，当所述密文块数据 C_{i+1} 不是接着密文块数据 C_i 继续进行解密，而是接着密文 D 的某一密文块数据进行解密时，用于选择所述存储器所存储的模块输出块数据 T_i 并提供至反馈回路。

所述存储器，其特征在于：包括

对应多件密文的多个暂存器；

根据解密处理的密文而对暂存器进行转换的转换器。

本发明的解密方法，其特征是包括以下步骤：

利用从解密模块输出的模块输出块数据 T_i（$i = 1, 2, 3, \cdots\cdots$）对第 1 密文 C 的密文块数据 C_i（$i = 1, 2, 3, \cdots\cdots$）进行解密；

在所述密文块数据 C_i 的解密过程中或是密文块数据 C_i 的解密之后，将第 1 密文 C 的密文块数据 C_{i+1} 解密用的模块输出块数据 T_i 存储于存储器；

在将所述密文块数据 C_{i+1} 解密用的模块输出块数据 T_i 存储于存储器之后，对第 2 密文 D 的至少 1 个密文块数据进行解密；

在对所述第 2 密文 D 的至少 1 个密文块数据进行解密之后，输入存储器所存储的用于密文块数据 C_{i+1} 解密的模块输出块数据 T_i，并利用解密模块对第 1 密文 C 的密文块数据 C_{i+1} 进行解密。

本发明的解密装置，用于将由 1 个以上密文块数据所组成的密文通过解密单元解密成明文，并针对密文生成为确认密文完整性的认证码，其特征在于：包括

解密部，具有将密文块数据 C_i 反馈至解密单元的第 1 反馈回路，并用于输入密文块数据，而且通过第 1 反馈回路反馈密文块数据 C_i 进行解密处理，输出明文块数据；

认证码生成部，具有用于反馈认证码演算中间结果的第 2 反馈回路，并用于输入与输入到解密部的密文块数据相同的密文块数据，进行数据处理输出认证码演算中间结果，并通过第 2 反馈回路反馈认证码演算中间结果，从而生成为确认密文完整性的认证码。

所述解密部和认证码生成部，兼用单一解密模块和单一反馈回路并交互进行解密处理和认证码生成处理，同时

所述单一反馈回路，其特征在于：包括

用于分别记录并输出解密处理和认证码生成处理结果的存储器；

用于为交互进行解密处理和认证码生成处理，而从存储器交互选择解密处理和认证码生成处理的结果，并输出至解密模块的选择器。

本发明的解密方法，用于将由 1 个以上密文块数据所组成的密文通过解密单元解密成明文，并针对密文生成为确认密文完整性的认证码，其特征是包括以下步骤：

解密步骤，具有将密文块数据 C_i 反馈至解密单元的第 1 反馈步骤，并输入密文块数据，而且通过第 1 反馈回路反馈密文块数据 C_i 进行解密处理，输出明文块数据；

认证码生成步骤，具有用于反馈认证码演算中间结果的第 2 反馈步骤，并输入与输入到解密步骤的密文块数据相同的密文块数据，进行数据处理输出认证码演算中间结果，并通过第 2 反馈步骤反馈认证码演算中间结果，从而生成为确认密文完整性的认证码。

所述加密处理，以采用块密码算法为特征。

所述解密处理，以采用块密码算法为特征。

所述存储器，以下述内容为特征：将

第 1 处理数据的加密中间结果，和

为加密第 1 处理数据所使用的加密键，

作为加密处理的状态而进行存储。

所述存储器，以下述内容为特征：将

第 2 处理数据的解密中间结果，和

为解密第 2 处理数据所使用的解密键，

作为解密处理的状态而进行存储。

本发明的加密装置，其特征在于：

包括

输入数据进行加密，并输出密码数据的加密部；

输入加密部所输出的密码数据，并生成为保证密文完整性的认证码的认证码生成部，

认证码生成部，在加密部完成数据加密之前，既开始认证码的生成。

本发明的解密装置，其特征在于：

包括

输入数据进行解密，并输出解密数据的解密部；

输入解密部所输入的数据，并生成为保证密文完整性的认证码的认证码生成部，

认证码生成部，在解密部完成数据解密之前，既开始认证码的生成。

本发明的加密方法，其特征在于：

包括

输入数据进行加密，并输出密码数据的加密步骤；

输入加密步骤所输出的密码数据，并生成为保证密文完整性的认证码的认证码生成步骤，

认证码生成步骤，在加密步骤完成数据加密之前，既开始认证码的生成。

本发明的解密方法，其特征在于：

包括

输入数据进行解密，并输出解密数据的解密步骤；

输入解密步骤所输入的数据，并生成为保证密文完整性的认证码的认证码生成步骤，

认证码生成步骤，在解密步骤完成数据解密之前，既开始认证码的生成。

另外，本发明是以用于在计算机上实现所述加密装置的各部处理

以及所述加密方法的各步骤处理的程序为特征。而且，以记录其程序的计算机可读取的记录媒体为特征。

另外，本发明是以用于在计算机上实现所述解密装置的各部处理以及所述解密方法的各步骤的程序为特征。而且，以记录其程序的计算机可读取的记录媒体为特征。

附图说明

图 1 是实施方式 1 中 CBC 模式的加密装置示意图。

图 2 是 CBC 模式的加密装置的操作顺序示意图。

图 3 是 CBC 模式的加密装置的操作流程图。

图 4 是选择器 54 的操作流程图。

图 5 是转换器 57 的中断处理流程图。

图 6 是存储器 55 的另一例的示意图。

图 7 是存储器 55 的中断处理流程图。

图 8 是存储器 55 的另一例的示意图。

图 9 是优先权处理示意图。

图 10 是优先权处理示意图。

图 11 是优先权处理示意图。

图 12 是存储器 55 与反馈线 66 的并行设置图。

图 13 是图 12 的加密装置的操作顺序示意图。

图 14 是存储器 55 与反馈线 67 的并行设置图。

图 15 是图 14 的加密装置的操作顺序示意图。

图 16 是 OFB 模式的加密装置示意图。

图 17 是图 16 的加密装置的操作顺序示意图。

图 18 是 CFB 模式的加密装置示意图。

图 19 是图 18 的加密装置的操作顺序示意图。

图 20 是 CBC 模式的解密装置示意图。

图 21 是图 20 的解密装置的操作顺序示意图。

图 22 是 OFB 模式的解密装置示意图。

图 23 是图 22 的解密装置的操作顺序示意图。

图 24 是 CFB 模式的解密装置示意图。

图 25 是图 24 的解密装置的操作顺序示意图。

图 26 是保存键的 CBC 模式的加密装置示意图。

图 27 是 CBC 模式的加密装置的操作顺序示意图。

图 28 是保存键的 CBC 模式的解密装置示意图。

图 29 是实施方式 2 中具有加密部 100 和认证码生成部 200 的加密装置示意图。

图 30 是具有加密部 100 和认证码生成部 200 的加密装置的操作顺序示意图。

图 31 是具有加密部 100 和认证码生成部 200 的加密装置的流程图。

图 32 是将加密部 100 和认证码生成部 200 合二为一的加密装置示意图。

图 33 是将加密部 100 和认证码生成部 200 合二为一的加密装置的操作顺序示意图。

图 34 是具有解密部 300 和认证码生成部 400 的解密装置示意图。

图 35 是将解密部 300 和认证码生成部 400 合二为一的解密装置示意图。

图 36 是将解密部 300 和认证码生成部 400 合二为一的解密装置的操作顺序示意图。

图 37 是实施方式 2 中具有加密部 100 和认证码生成部 200 的加密装置示意图。

图 38 是具有解密部 300 和认证码生成部 400 的解密装置示意图。

图 39 是使用加密键 K 的加密模块 51 的代表性结构图。

图 40 是加密装置及解密装置的硬件实现示意图。

图 41 是加密装置及解密装置的硬件实现示意图。

图 42 是由应用程序 46 调用加密程序 47 的示意图。

图 43 是传统的 CBC 模式的加密装置示意图。

图 44 是传统的 CBC 模式的解密装置示意图。

图 45 是传统的 OFB 模式的加密装置示意图。

图 46 是传统的 OFB 模式的解密装置示意图。

图 47 是传统的 CFB 模式的加密装置示意图。

图 48 是传统的 CFB 模式的解密装置示意图。

图 49 是传统的加密顺序示意图。

图 50 是传统的加密顺序示意图。

图 51 是保密处理和完整性保证处理的说明图。

图 52 是传统的保密处理和完整性保证处理的操作顺序示意图。

具体实施方式

实施方式 1

图 1 是本实施方式中 CBC 模式的加密装置示意图。

本实施方式的加密装置，是由选择器 54、“异”逻辑电路 58、使用加密键 K 的加密模块 51、和存储器 55 所构成。“异”逻辑电路 58 和使用加密键 K 的加密模块 51 构成加密单元 52。选择器 54、“异”逻辑电路 58、和使用加密键 K 的加密模块 51，通过反馈线 65、反馈线 66、和反馈线 67 构成反馈回路。由使用加密键 K 的加密模块 51 加密的密文块数据 C_i，通过反馈回路被再输入“异”逻辑电路 58，并在“异”逻辑电路 58 生成模块输入数据 S_i。然后，所生成的模块输入数据 S_i 被提供至使用加密键 K 的加密模块 51。

存储器 55，与反馈线 65 并行设置。存储器 55 由暂存器 56 和转换器 57 构成。转换器 57 用于转换使用加密键 K 的加密模块 51 的输出是输入至暂存器 56 或是忽略。此转换，例如是通过中断 IT 来进行。当发生中断 IT 时，转换器 57 连接 E，当中断 IT 解除时，转换器 57 连接 F。暂存器 56 输入并存储经由 E 传来的密文块数据 C_i。存储在暂存器 56 的密文块数据 C_i 输出至选择器 54。选择器 54 有 A、B、C3 个输入，并从其中选择某 1 个输入。这些选择是依据后述的中断 IT。

图 2 是图 1 所示的加密装置的操作顺序示意图。

图 3 是图 1 所示的加密装置的操作流程图。

当该加密装置接通电源时，选择器 54 的输入设定为 A，转换器 57 连接 E。接着，如果有明文 N 的加密要求时，则发生中断 IT，并且到明文 N 的加密要求解除为止，中断 IT 一直维持在发生（ON）状态。另外，明文 M 使用键 K_1 加密，明文 N 使用键 K_2 加密。而且，在中断 IT 发生或中断 IT 解除时，键 K_2 或键 K_1 被提供给加密模块 51 进

行更改。

在时刻 T0，提供键 K_1，开始明文块数据 M_1 的加密处理。在时刻 T0，当明文块数据 M_1 的加密开始后，一旦从选择器 54 的输入 A 输入初始值 IV，则选择器 54 转换到 B。接着，在明文块数据 M_1 使用键 K_1 进行加密过程中的时刻 X，发生了明文块数据 N_1 要求加密的中断 IT。到时刻 T1 为止，密文块数据 C_1 被存储在存储器 55。接着，由于中断 IT 的发生，在时刻 T1，键 K_2 被提供给加密模块 51。同时，在时刻 T1，选择器 54 设定输入为 A。同时，在时刻 T1，转换器 57 连接到 F。在时刻 T1 之后，使用键 K_2 对明文块数据 N_1 进行加密，并输出密文块数据 D_1。在时刻 Y，明文块数据 N_1 的加密处理结束，中断 IT 被解除。由于该中断 IT 的解除，在时刻 T2，键 K_1 被提供给加密模块 51，选择器 54 的输入转换到 C，转换器 57 连接到 E。由于选择器 54 转换到 C，存储在存储器 55 的密文块数据 C_1 为了明文块数据 M_2 的加密而被输入，通过使用键 K_1 的加密模块 51 对明文块数据 M_2 进行加密，并输出密文块数据 C_2。在时刻 T3 之前，当选择器 54 的输入转换到 B，并对明文块数据 M_3 进行加密时，从反馈回路的反馈线 65 所反馈的密文块数据 C_2 被输入，通过使用键 K_1 的加密模块 51 明文块数据 M_3 被加密，并输出密文块数据 C_3。

另外，如果明文 M 和明文 N 的键相同（$K_1 = K_2$），则在加密处理开始时只一次提供键即可。

使用图 3 的流程图对全体的操作进行说明。

在 S1，开始或继续明文 M 的加密处理。到最后的块数据处理结束时，结束处理。在 S2，监视在任意时刻的中断 IT 的发生。如果没有中断 IT 的发生，则继续 S1 的处理。当在明文块数据 M_i 的处理过程中发生了中断 IT 时，则在 S3，将目前处理中的明文块数据 M_i 的密文块数据 C_i 存储于存储器 55 的暂存器 56。在 S4，由于中断 IT，对有加密处理要求的明文 N 进行加密处理。该 S4 的加密处理，如 S5 所示，到中断 IT 的解除为止连续进行。当中断 IT 解除时，在 S6，使用存储在存储器 55 的暂存器 56 中的密文块数据 C_i 对明文块数据 M_{i+1} 进行加密处理。其后的处理为返回 S1，并继续加密处理。

图 4 是选择器 54 的操作处理示意图。

当接通电源时，如 S11 所示，将输入设定为 A。在 S12，当加密

开始时，则在 S13，将输入设定为 B。即由反馈回路的反馈线 65 所反馈的密文块数据 C_i 被使用。在 S14，当判定目前正处理的是最后的块数据时，则返回 S11 返回与接通电源时相同的状态。在 S15，当确认了中断 IT 的发生时，则在 S16，设定输入为 A，当加密开始时，则在 S18，设定输入为 B。到中断 IT 解除为止，维持输入为 B 的状态进行操作。即由反馈回路的反馈线 65 所反馈的密文块数据 C_i 被使用。在 S19，当探测到中断 IT 的解除时，则在 S20，设定输入为 C。通过将该输入设定为 C，则存储在存储器 55 中的密文块数据 C_i 被输入。当基于该 C 输入的加密开始后，则返回 S13 设定输入为 B。

由此，根据中断 IT 的发生，可以转换选择器 54。

另外，明文 M 的加密处理，也可根据中断 IT 在任意时刻开始。

图 5 是转换器 57 的中断处理流程图。

当接通电源，而且，在其后最初的明文加密处理时，转换器 57 连接 E。接着，在 S31，当中断 IT 发生时，转换器 57 离开 E 连接 F。接着，在 S33，当探测到中断 IT 的解除时，转换器 57 离开 F 连接 E。由此，从中断 IT 的发生到解除，转换器 57 将一直忽略密文块数据 C_i。所以，在存储器 55 的暂存器 56 中，中断 IT 发生时所生成的密文块数据 C_i 将一直被储存。

如以上所述，图 1～图 5 所示的加密装置，用于对构成明文 M 的明文块数据 M_i（$i=1, 2, 3, \ldots\ldots$）和构成明文 N 的明文块数据 N_j（$j=1, 2, 3, \ldots\ldots$）进行加密，表示在明文 M 的加密处理过程中接收在明文 M 的加密处理结束之前的明文 N 的加密要求的中断处理机构。

另外，图 1～图 5 所示的加密装置，具有

加密模块 51，用于进行明文块数据 M_i 的加密处理，并输出密文块数据 C_i；

反馈回路 65、66，用于将从加密模块 51 输出的密文块数据 C_i 通过反馈线 65 反馈至加密单元 52；

存储器 55，与反馈回路的反馈线 65 并行设置，当由于根据所述中断处理接收所述明文 N 的加密要求，开始明文 N 的某一明文块数据的加密处理，而紧接在明文块数据 M_i 之后，不继续接着进行所述明文块数据 M_{i+1} 的加密处理时，用于存储被反馈的密文块数据 C_i。

另外，图 1～图 5 所示的加密装置，具有

选择器 54，当明文块数据 M_{i+1} 继续接着明文块数据 M_i 进行加密时，用于选择由所述反馈回路的反馈线 65 所反馈的密文块数据 C_i 并通过反馈回路提供至加密单元 52，当所述明文块数据 M_{i+1} 不是继续接着明文块数据 M_i 进行加密，而是接着明文 N 的某一明文块数据进行加密时，用于选择所述存储器所存储 55 的密文块数据 C_i 并通过反馈回路提供至加密单元 52。

存储器 55 是当中断 IT 发生时存储加密装置状态的存储器。通过存储器 55 存储加密处理的状态，即使在某数据的加密进行中进行了其他数据的加密，也可以再恢复某数据的加密处理。即通过利用存储在存储器 55 中的数据，可以将加密装置恢复到与加密中断时完全相同的状态，并继续进行中断了的加密处理。

图 6 是存储器 55 的另一例的示意图。

存储器 55 具有中断控制部 52、输入转换器 96、输出转换器 97、和多个暂存器（REG1、2、3）。这样，通过多个暂存器可以接收多个中断。

图 7 是存储器 55 中断处理的操作示意图。

如果中断 IT 发生，则在 S41，存储当前使用中的暂存器 K 的号码 K。在 S42，输入转换器 96 和输出转换器 97 连接暂存器 K 以外的暂存器 1。在此状态下，继续明文 N 的加密。而且，监视在明文 N 的加密过程中是否发生了其他的中断。在 S43，当探测出发生了其他的中断 IT 时，再调用自己本身的 S40。如此一来，每当中断 IT 发生时，可以通过递归调用自己本身的 S40 处理，进行多层的中断处理。在 S44，探测中断是否解除，当中断已解除时，利用所存储的号码 K 将输入转换器 96 和输出转换器 97 转换至暂存器 K。在图 6 所示的情况下，因为有 3 个暂存器，所以可以进行 3 层的中断处理。

图 8 是存储器 55 的另一例示意图。

存储器 55，具有存储栈 64。存储栈 64 是先到后出（FIFO）型的暂存器。当在使用存储栈 1 过程中发生了中断 IT 时，存储栈 1 的数据移到存储栈 2，其后的数据堆入存储栈 1，当中断 IT 解除时，输出堆积在存储栈 1 的数据，存储栈 2 的数据返回存储栈 1。图 8 所示的情况，表示了可以进行 4 层中断处理的情况。

如图 6 所示，在进行多层中断处理的情况下，可以对各中断赋予优先权。例如，中断 IT1 为优先权 1，中断 IT2 为比优先权 1 低的优先权 2，这样，当优先权 1 的中断 IT1 发生时，可以迟缓优先权 2 的处理。

图 9 表示优先权 1 的加密处理优先于优先权 2 的加密处理的情况。优先权 1 的加密处理首先结束。

图 10 表示优先权都相等时的加密处理情况。

当优先权都相等时，2 个明文的各块数据交互进行加密。

图 11 表示优先权 1 的数据和 2 个优先权 2 的数据的加密情况。

如图 9～图 11 所示，通过对中断赋予优先权，可以实现用户所希望的加密处理顺序。对急用数据和短数据，可以通过提高优先权而进行高效率的处理。

图 12 表示存储器 55 与反馈线 66 并行的情况。

“异”逻辑电路 58 和使用加密键的加密模块 51 构成了加密单元 52。

图 13 是图 12 加密装置的操作顺序示意图。

第 1 选择器 61 和第 2 选择器 62，通过以下的选择连接实现与图 1 的选择器 54 相同的选择动作。

第 1 选择器 61 + 第 2 选择器 62 = 选择器 54

A	+	D	=	A
B	+	D	=	B
A	+	C	=	C
B	+	C	=	C

在图 13，当第 2 选择器 62 选择 D 时，第 1 选择器 61 的选择（A 或 B）有效，当第 2 选择器 62 选择 C 时，输出存储器 55 的内容。

即第 2 选择器 62，在希望使用存储器 55 的内容时（在中断 IT 解除并从明文 N 返回原明文 M 的加密时），选择 C 即可。

图 14 表示存储器 55 与反馈线 67 并行的情况。

图 15 是图 14 加密装置的操作顺序示意图。

当中断 IT 的发生时刻 X 是在“异”逻辑电路 58 进行“异”逻辑演算之前时，存储器 55，存储通过“异”逻辑电路 58 进行“异”逻辑演算的模块输入数据 S_i。然后，加密明文块数据 N_1。接着，通过

第 2 选择器 62 选择存储在存储器 55 中的模块输入数据 S_i，输入使用加密键 K 的加密模块 51 进行加密，并输出密文块数据 C_1。

如图 1、图 12 及图 14 所示，存储器 55，可与反馈线 65、反馈线 66 和反馈线 67 中的任意一条线并行设置。存储器 55，当加密装置在某数据的加密处理过程中开始其他数据的加密时，存储其他数据开始加密之前的状态，在其他数据的加密处理结束时，只要加密装置能利用存储在存储器 55 中的数据恢复到原状态，存储器 55 设置在什么位置都可以。而且，存储器 55 设置在多个位置也可以。

如以上所述，本实施方式的加密装置，用于对由 1 个以上明文块数据 M_i（i＝1，2，3，……，m）所构成的第 1 处理数据（明文 M）和由 1 个以上明文块数据 N_j（j＝1，2，3，……，n）所构成的第 2 处理数据（明文 N）进行加密，其特征为：具有存储加密处理状态的存储器 55，在第 1 处理数据的所有块数据（M_1～M_m）加密处理结束之前开始第 2 处理数据的最初块数据 N_1 加密处理的同时，当第 2 处理数据的最初块数据 N_1 的加密处理开始时，将第 1 处理数据的加密处理状态（例如，密文块数据 C_i）存储于所述存储器 55，当重新开始第 1 处理数据的加密处理时，将加密装置的加密处理状态恢复至存储器所存储的第 1 处理数据的加密处理状态之后，再开始第 1 处理数据的加密处理。

所述加密装置，其特征还在于：在第 2 处理数据的所有块数据（N_1～N_n）加密处理结束之前再开始第 1 处理数据的加密处理的同时，所述存储器 55，在重新开始第 1 处理数据的加密处理时，存储第 2 处理数据的加密处理状态（例如，密文块数据 D_j），当重新开始第 2 处理数据的加密处理时，将加密装置的加密处理状态恢复至存储器所存储的第 2 处理数据的加密处理状态之后，再开始第 2 处理数据的加密处理。

图 16 是 OFB 模式加密装置的结构图。

与图 45 相比，其特征是增加了存储器 55。存储器 55，存储从加密模块 51 输出的模块输出块数据 T_1。

图 16，是对构成明文 M 的明文块数据 M_i（i＝1，2，3，……）和构成明文 N 的明文块数据 N_j（j＝1，2，3，……）进行加密的加密装置，其特征是包括：中断处理机构，用于在明文 M 的加密处理

过程中接收在明文 M 的加密处理结束之前的明文 N 的加密要求；加密模块 51，用于将加密处理了的数据作为模块输出块数据 T_i 进行输出；反馈回路 65、66，用于将加密模块 51 所输出的模块输出块数据 T_i 通过反馈线 65 反馈到加密模块；存储器 55，与反馈回路的反馈线 65 并行设置，当由于接收所述明文 N 的加密要求，开始明文 N 的某一明文块数据的加密处理，而紧接在明文块数据 M_i 之后，不继续接着进行所述明文块数据 M_{i+1} 的加密处理时，用于存储被反馈的模块输出块数据 T_i；选择器 54，当明文块数据 M_{i+1} 继续接着明文块数据 M_i 进行加密时，用于选择由所述反馈回路的反馈线 65 所反馈的模块输出块数据 T_i 并通过反馈回路提供至加密模块 51，当所述明文块数据 M_{i+1} 不是继续接着明文块数据 M_i 进行加密，而是接着明文 N 的某一明文块数据进行加密时，用于选择所述存储器所存储 55 的模块输出块数据 T_i 并通过反馈回路提供至加密模块 51。

图 17 是图 16 的 OFB 模式加密装置的操作说明图。

在图 17，图 2CBC 模式的操作变为 OFB 模式的操作，其他的操作与图 2 的操作相同。

图 18 是 CFB 模式的加密装置示意图。

与图 47 相比，其特征是设置了存储器 55。存储器 55，存储从“异”逻辑电路 58 输出的密文块数据 C_i。

而且，“异”逻辑电路 58 和使用加密键 K 的加密模块 51 构成了加密单元 52。

图 18，是对构成明文 M 的明文块数据 M_i（i＝1，2，3，……）和构成明文 N 的明文块数据 N_j（j＝1，2，3，……）进行加密的加密装置，其特征是包括：中断处理机构，用于在明文 M 的加密处理过程中接收在明文 M 的加密处理结束之前的明文 N 的加密要求；加密单元 52，用于对明文块数据 M_i 进行加密处理并输出密文块数据 C_i；反馈回路 65、66，用于将加密模块所输出的密文块数据 C_i 通过反馈线 65 反馈给加密处理；存储器 55，与反馈回路的反馈线 65 并行设置，当由于接收所述明文 N 的加密要求，开始明文 N 的某一明文块数据的加密处理，而紧接在明文块数据 M_i 之后，不继续接着进行所述明文块数据 M_{i+1} 的加密处理时，用于存储被反馈的密文块数据 C_i；选择器 54，当明文块数据 M_{i+1} 继续接着明文块数据 M_i 进行加

密时，用于选择由所述反馈回路的反馈线 65 所反馈的密文块数据 C_i 并通过反馈回路提供至加密单元 52，当所述明文块数据 M_{i+1} 不是继续接着明文块数据 M_i 进行加密，而是接着明文 N 的某一明文块数据进行加密时，用于选择所述存储器所存储 55 的密文块数据 C_i 并通过反馈回路提供至加密单元 52。

图 19 是图 18 的 CFB 模式加密装置的操作说明图。

在图 19，图 2CBC 模式的操作变为 CFB 模式的操作，其他的操作与图 2 的操作相同。

图 20 是 CBC 模式的解密装置示意图。

与图 44 相比，其特征是设置了存储器 75。

存储器 75，由暂存器 76 和转换器 77 构成。

而且，“异”逻辑电路 78 和使用键 K 的解密模块 71 构成了解密单元 72。

另外，暂存器 111 可以设置在选择器 74 的内部。

图 20 所示的解密装置，用于对构成密文 C 的密文块数据 C_i（i＝1，2，3，……）和构成密文 D 的密文块数据 N_j（j＝1，2，3，……）进行解密，具有在密文 C 的解密处理过程中的任一时间接收密文 D 的解密要求的中断处理机构。

而且，图 20 所示的解密装置，还具有解密模块 71，用于将密文块数据 C_i 的经过解密处理的数据作为模块输出块数据 T_i 进行输出；反馈回路 85、111、82、86，用于将为解密密文块数据 C_{i+1} 的密文块数据 C_i 通过反馈线 85、111、82 反馈到解密单元 72；存储器 71，与反馈回路的反馈线 85、111、82 并行设置，当由于接收所述密文 D 的解密要求，开始密文 D 的某一密文块数据的解密处理，而紧接在密文块数据 C_i 之后，不继续接着进行所述密文块数据 C_{i+1} 的解密处理时，用于存储被反馈的块数据。

而且，图 20 所示的解密装置，还具有选择器 74，当密文块数据 C_{i+1} 接着密文块数据 C_i 继续进行解密时，用于选择由所述反馈回路的反馈线 85、111、82 所反馈的密文块数据 C_i 并通过反馈回路提供至加密单元 72，当所述密文块数据 C_{i+1} 不是接着密文块数据 C_i 继续进行解密，而是接着密文 D 的某一密文块数据进行解密时，用于选择所述存储器所存储的密文块数据 C_i 并通过反馈回路提供至加密单元

72。

另外，在所述图 20 的说明中，虽然使用了［反馈线］、［反馈回路］的用词，但不是［将本身的输出变为本身的输入］的［反馈］的意思。在这里，［反馈］的意思，是当对密文块数据 C_i 进行解密之后，为对密文块数据 C_{i+1} 进行解密，而再提供密文块数据 C_i 的意思。

图 21 是图 20 解密装置的操作顺序示意图。

当使用加密键（也称为解密键）K_1，对密文块数据 C_1 进行解密的过程中发生中断 IT 时，密文块数据 C_1 存储在存储器 75 的暂存器 76 中。其后，使用加密键（也称为解密键）K_2，对密文块数据 D_1 进行解密，得到明文块数据 N_1。然后，读出存储在存储器 75 的暂存器 76 中的密文块数据 C_1，进行密文块数据 C_2 的解密，从而得到明文块数据 M_2。选择器 74 的操作，与图 4 所述内容相同。同时，转换器 77 的操作，与图 5 所示内容相同。

图 22 是 OFB 模式的解密装置示意图。

图 22，是对构成密文 C 的密文块数据 C_i（i = 1，2，3，……）和构成密文 D 的密文块数据 D_j（j = 1，2，3，……）进行解密的解密装置，其特征在于：包括中断处理机构，用于在密文 C 的解密处理过程中的任一时间接收密文 D 的解密要求；解密模块 71，用于将经过解密处理的数据作为模块输出块数据 T_i 进行输出；反馈回路 85、86，用于将从解密模块 71 输出的模块输出块数据 T_i 通过反馈线 85 反馈到解密模块 71；存储器 75，与反馈回路的反馈线 85 并行设置，当由于接收所述密文 D 的解密要求，开始密文 D 的某一密文块数据的解密处理，而紧接在密文块数据 C_i 之后，不继续接着进行所述密文块数据 C_{i+1} 的解密处理时，用于存储被反馈的模块输出块数据 T_i；选择器 74，当密文块数据 C_{i+1} 接着密文块数据 C_i 继续进行解密时，用于选择由所述反馈回路的反馈线 85 所反馈的模块输出块数据 T_i 并通过反馈回路提供至解密模块 71，当所述密文块数据 C_{i+1} 不是接着密文块数据 C_i 继续进行解密，而是接着密文 D 的某一密文块数据进行解密时，用于选择所述存储器所存储 75 的模块输出块数据 T_i 并通过反馈回路提供至解密模块 71。

图 23 是图 22OFB 模式加密装置的操作说明图。

在图 23，图 21CBC 模式的操作变为 OFB 模式的操作，其他的操作与图 21 的操作相同。

图 24 是 CFB 模式的解密装置示意图。

而且，“异”逻辑电路 78 和使用键 K 的解密模块 71 构成了解密单元 72。

另外，暂存器 111 可以设置在选择器 74 的内部。

图 24，是对构成密文 C 的密文块数据 C_i（i＝1，2，3，……）和构成密文 D 的密文块数据 D_j（j＝1，2，3，……）进行解密的解密装置，其特征在于包括：中断处理机构，用于在密文 C 的解密处理过程中的任一时间接收密文 D 的解密要求；解密模块 71，用于将密文块数据 C_i 的经过解密处理的数据作为模块输出块数据 T_i 进行输出；反馈回路 85、111、82、86，用于将为解密密文块数据 C_{i+1} 的密文块数据 C_i 通过反馈线 85、111、82 反馈到解密单元 72；存储器 75，与反馈回路的反馈线 85、111、82 并行设置，当由于接收所述密文 D 的解密要求，开始密文 D 的某一密文块数据的解密处理，而紧接在密文块数据 C_i 之后，不继续接着进行所述密文块数据 C_{i+1} 的解密处理时，用于存储被反馈的密文块数据 C_i；选择器 74，当密文块数据 C_{i+1} 接着密文块数据 C_i 继续进行解密时，用于选择由所述反馈回路的反馈线 85、111、82 所反馈的密文块数据 C_i 并通过反馈回路提供至解密模块 71，当所述密文块数据 C_{i+1} 不是接着密文块数据 C_i 继续进行解密，而是接着密文 D 的某一密文块数据进行解密时，用于选择所述存储器所存储 75 的密文块数据 C_i 并通过反馈回路提供至解密模块 71。

另外，在所述图 24 的说明中，［反馈线］、［反馈回路］的用词虽然被使用，但不是［将本身的输出变为本身的输入］的［反馈］的意思。在这里，［反馈］的意思，是当对密文块数据 C_i 进行解密之后，为对密文块数据 C_{i+1} 进行解密，而再提供密文块数据 C_i 的意思。

图 25 是图 24 的 CFB 模式加密装置的操作说明图。

在图 25，图 21CBC 模式的操作变为 CFB 模式的操作，其他的操作与图 21 的操作相同。

图 26 是图 1 所示的 CFB 模式加密装置的改进例示意图。

图 26 的加密装置，增加了选择器 154 和存储器 155。图 1 的情况，表示了键 K_1 在中断 IT 解除时由外部提供的情况，在这里，对保存并再利用从外部一次提供的键 K_1 的情况进行说明。

存储器 155，由暂存器 156 和转换器 157 构成。转换器 157，对是将加密键 K 输入至暂存器 156 还是忽略进行转换。此转换，例如，通过中断 IT 来进行。当中断 IT 发生时，则转换器 157 连接 E，而当中断 IT 解除时，则转换器 157 连接 F。暂存器 156，对经过 E 而来的键 K 进行输入并存储。存储在暂存器 156 中的键 K 输出至选择器 154。选择器 154，选择 A、C2 个输入中的 1 个输入。这些选择，如后述那样依据中断 IT。

图 27 是图 26 所示加密装置的操作顺序示意图。

当该加密装置接通电源时，选择器 54 和选择器 154 的输入设定为 A，转换器 57 和转换器 157 连接 E。接着，如果有明文 N 的加密要求时，则发生中断 IT，并且到明文 N 的加密要求解除为止，中断 IT 一直维持在发生（ON）状态。另外，明文 M 使用键 K_1 加密，明文 N 使用键 K_2 加密。键 K_1 或键 K_2 被提供给加密模块 51。

在时刻 T0，键 K_1 作为键 KI 被从外部提供。选择器 154，由于连接 A，所以将键 KI 作为键 K 输出给加密模块 51。而且，由于转换器 157 连接 E，键 K_1 被存储于暂存器 156。于是，开始明文块数据 M_1 的加密处理。在时刻 T0，当明文块数据 M_1 的加密开始后，一旦从选择器 54 的输入 A 输入初始值 IV，则选择器 54 转换到 B。接着，在明文块数据 M_1 使用键 K_1 进行加密过程中的时刻 X，发生了明文块数据 N_1 要求加密的中断 IT。到时刻 T1 为止，密文块数据 C_1 被一直存储在存储器 55。接着，由于中断 IT 的发生，在时刻 T1，键 K_2 作为键 KI 被从外部提供给加密模块 51。选择器 154，由于连接 A，所以将键 KI 作为键 K 输出给加密模块 51。同时，在时刻 T1，选择器 54 设定输入为 A。同时，在时刻 T1，转换器 57 和转换器 157 连接到 F。所以，键 K_2 不在暂存器 156 存储。在时刻 T1 之后，使用键 K_2 对明文块数据 N_1 进行加密，并输出密文块数据 D_1。在时刻 Y，明文块数据 N_1 的加密处理结束，中断 IT 被解除。由于该中断 IT 的解除，在时刻 T2，选择器 54 的输入转换到 C，转换器 57 连接到 E。所以，键 K_1 作为键 KI 从暂存器 156 输出至选择器 154，从选择器 154 键 K_1 作为键 K 提供给

加密模块 51。另外，由于选择器 54 转换到 C，存储在存储器 55 的密文块数据 C_1 为了明文块数据 M_2 的加密而被输入，通过使用键 K_1 的加密模块 51 对明文块数据 M_2 进行加密，并输出密文块数据 C_2。在时刻 T3 之前，当选择器 54 的输入转换到 B，并对明文块数据 M_3 进行加密时，从反馈回路的反馈线 65 所反馈的密文块数据 C_2 被输入，通过使用键 K_1 的加密模块 51 明文块数据 M_3 被加密，并输出密文块数据 C_3。

另外，在时刻 T3 之前，选择器 154 的输入转换到 A。

对选择器 154 的操作处理进行说明。

当接通电源时，输入设定为 A。而且，即使中断 IT 的发生被确认，输入也一直设定为 A。到中断 IT 解除为止，选择器 154，一直以输入为 A 的状态操作。选择器 154，当探测到中断 IT 的解除时，输入设定为 C。通过将该输入设定为 C，存储在存储器 55 中的键 K_1 作为键 K 被输入给加密模块 51。当根据该 C 的键输入开始加密时，则选择器 154 设定输入为 A。

这样，基于中断 IT 的发生，可转换选择器 154。

接着，对转换器 157 的中断处理操作进行说明。

当接通电源，而且，其后最初的明文 M 加密处理时，转换器 157 连接 E。明文 M 的键 K_1 被存储于暂存器 156。接着，在时刻 X，中断 IT 发生时，在时刻 T_1 转换器 157 离开 E 连接 F，忽略明文 N 的键 K_2。接着，在时刻 Y，探测到中断 IT 的解除时，在时刻 T2，转换器 157 离开 F 连接 E。由此，从中断 IT 的发生到解除，转换器 157 将一直忽略明文 N 的键 K_2。所以，在存储器 155 的暂存器 156 中，明文 M 的键 K_1 将一直被储存。

图 28，表示针对图 20 所示的解密装置，存储并再利用键 K_1 情况的结构。

图 28，针对图 20 增加了选择器 174 和存储器 175。选择器 174 和存储器 175 的操作，与图 26 所示的选择器 154 和存储器 155 相同。

存储器 55 和存储器 155，是在中断 IT 发生时存储加密装置状态的存储器的实例。如此，通过存储器 55 和存储器 155 存储加密处理的状态，即使在某数据的加密处理过程当中进行了其他数据的加密，也还可以再恢复到某数据的加密处理。即通过使用存储器 55 所

存储的数据和存储器 155 所存储键 K，可以使加密装置恢复到与加密中断时完全相同的状态，从而能继续中断了的加密处理。

这里，存储器 155 和存储器 175，可以是与图 6、图 8 所示的存储器 55 相同的结构。而且，虽未图示，但针对图 16、图 18、图 22、图 24，可以增加如图 26、图 28 所示的结构存储键 K_1。

另外，图 26 的存储器 55 和存储器 155，由于进行同一操作，所以可以统一成 1 个存储器。而且，图 28 的存储器 75 和存储器 175，也由于进行同一操作，所以可以统一成 1 个存储器。

如以上所述，本实施方式的解密装置，用于对由 1 个以上块数据 C_i（i = 1，2，3，……，m）所构成的第 1 处理数据（密文 C）和由 1 个以上块数据 D_j（j = 1，2，3，……，n）所构成的第 2 处理数据（密文 D）进行解密，其特征为：具有存储解密处理状态的存储器 75，在第 1 处理数据的所有块数据（$C_1 \sim C_m$）解密处理结束之前开始第 2 处理数据的最初块数据 D_1 解密处理的同时，当第 2 处理数据的最初块数据 D_1 的解密处理开始时，将第 1 处理数据的解密处理状态存储于所述存储器，当重新开始第 1 处理数据的解密处理时，将解密装置的解密处理状态恢复至存储器 75 所存储的第 1 处理数据的解密处理状态之后，再开始第 1 处理数据的解密处理。

并且，所述加密装置，其特征还在于：在第 2 处理数据的所有块数据（$D_1 \sim D_n$）解密处理结束之前再开始第 1 处理数据的解密处理的同时，所述存储器 74，在重新开始第 1 处理数据的解密处理时，存储第 2 处理数据的解密处理状态，当重新开始第 2 处理数据的解密处理时，将解密装置的解密处理状态恢复至存储器所存储的第 2 处理数据的解密处理状态之后，再开始第 2 处理数据的解密处理。

在这里，加密处理的状态，例如，

在图 1 的 CBC 模式中，是密文块数据 C_i（以及键 K_1）；

在图 16 的 OFB 模式中，是模块输出数据 T_i（以及键 K_1）；

在图 18 的 CFB 模式中，是密文块数据 C_i（以及键 K_1），

同时，解密处理的状态，例如，

在图 20 的 CBC 模式中，是密文块数据 C_i（以及键 K_1）；

在图 22 的 OFB 模式中，是模块输出数据 T_i（以及键 K_1）；

在图 24 的 CFB 模式中，是密文块数据 C_i（以及键 K_1）。

在所述的说明中，虽然对 3 个模式情况的加密装置和解密装置进行了说明，但所述的 3 个模式只是一例，也可以是这些模式的改进，或是，这些模式的变形。特别是，成为特征之处，是在加密、解密前面的块数据而生成的块数据 C_i 或 M_i 或 T_i 作为反馈数据被用于接着的块数据 M_{i+1} 或 C_{i+1} 的加密、解密处理的加密、解密方法中，设置存储加密、解密状态的存储器 55，在其他数据的加密、解密处理之后利用块数据 C_i 或 M_i 或 T_i 可以重新恢复原状态。由此，不用特别顾及加密模式、解密模式。

另外，也可以不用中断 IT，而用定时询问方式或取得令牌方式等的其他机构接收加密要求，进行 2 个以上加密、解密处理的交互并行处理。

而且，虽然表示了使用加密键 K 的加密、解密处理的情况，但不使用加密键 K 的加密、解密处理也可以。

实施方式 2

在本实施方式中，对加密装置进行保密处理和数据完整性保证处理的情况进行说明。

所谓数据的保密处理，是指对数据进行加密，而即使数据被偷听或被盗也不使意思内容泄露。并且，所谓数据完整性保证，是指保证数据没有被他人置换。当传送数据时，希望在数据保密处理基础上保证数据的完整性进行传送。数据的保密处理，通过对数据加密来进行。数据完整性的保证处理，通过在数据最后附加认证码（MAC: Message Authentication Code），由验证其认证码而发现篡改来进行。

图 29，表示通过 OFB 模式的加密部 100 进行保密处理，通过 CBC 模式的认证码生成部 200 生成认证码（MAC）的情况。

图 29 的加密装置，其通过加密模块 51 把由 1 个以上的明文块数据组成的明文加密成密文，并针对密文生成为保证密文完整性的认证码，其特征在于：包括

加密部 100，具有通过加密模块 51 在对明文块数据进行加密后，将加密模块 51 输出的模块输出块数据 T_i 反馈至加密模块 51 的第 1 反馈回路 65，并用于输入明文块数据，而且通过第 1 反馈回路 65 反馈模块输出块数据 T_i 进行加密处理，输出密文块数据 C_i；

认证码生成部 200，具有用于反馈认证码演算中间结果 T_i 的第 2 反馈回路 66，每当从加密部 100 输出密文块数据 C_i 时，用于输入密文块数据 C_i，进行认证码演算处理，并通过第 2 反馈回路 66 反馈认证码演算中间结果 T_i，从而生成为保证密文完整性的认证码 P。

图 30 是图 29 所示加密装置的操作顺序示意图。

明文块数据 M_1，首先被加密成密文块数据 C_1。接着，明文块数据 M_2 被输入，并加密成密文块数据 C_2。在加密该明文块数据 M_2 的同时，输入密文块数据 C_1，开始认证码的演算。在时刻 T1 与 T2 之间进行明文块数据 M_2 的加密和基于密文块数据 C_1 的认证码演算。并且，在时刻 T2 与 T3 之间进行明文块数据 M_3 的加密和基于密文块数据 C_2 的认证码演算。在时刻 T3，进行基于密文块数据 C_3 的认证码演算，并输出认证码 P。

图 29 的特征，是从“异”逻辑电路 58 输出的密文块数据 C_i 通过反馈线 69 输入“异”逻辑电路 59。基于反馈线 69 通过结合 OFB 模式和 CBC 模式，如图 30 所示，由流水处理来进行保密处理和完整性认证处理。图 52 所示的情况，是到时刻 T6 花费了处理时间，而图 30 所示的情况，是到时刻 T4 就结束处理从而实现了高速处理。

图 31 是图 29 所示加密装置的操作流程图。

在 S51，设块数据计数 i 为 1。S52 是加密部 100 的操作，加密部 100，输入明文块数据 M_i 并加密明文块数据 M_i，生成密文块数据 C_i 并输出密文块数据 C_i。S53 是认证码生成部 200 的操作，输入密文块数据 C_i 加密密文块数据 C_i，演算认证码。S54，判断块数据计数 i 是否是表示最后的块数据 n，如果不是最后的块数据，则在 S55，增加块数据计数 i，再返回 S52 的处理。即重复加密部 100 和认证码生成部 200 的处理。在 S54，如果是最后块数据的处理结束了的情况，则之前在 S53 刚被演算的认证码为最终认证码，所以在 S56，将该认证码附加到密文块数据 C_i 的最后。如图 31 所示，由于加密部 100 每生成密文块数据 C_i 时，认证码生成部 200 都输入密文块数据 C_i 并演算认证码，所以流水处理变为可能，从而实现高速处理。

图 32，合并了图 29 所示的加密部 100 和认证码生成部 200。即兼用加密部 100 和认证码生成部 200 的加密模块 51，同时，兼用加密部 100 和认证码生成部 200 的“异”逻辑电路 58 和 59。还兼用加

密部 100 的反馈线 65 和认证码生成部 200 的反馈线 66。

第 1 选择器 61，在保密处理开始时选择初始值 IV。第 2 选择器 62，在完整性保证处理开始时选择初始值 IV。第 3 选择器 63，交互选择保密处理和完整性保证处理。第 3 选择器 63 通过设输入为 E，可进行保密处理。而且，第 3 选择器 63 通过设输入为 F，可进行完整性保证处理。

存储器 93，存储从使用加密键 K 的加密模块 51 输出的模块输出数据 T_i。存储器 93，由输入转换器 96、输出转换器 97、第 1 暂存器 98 和第 2 暂存器 99 构成。输入转换器 96 和输出转换器 97，同步于第 3 选择器 63 的转换，每当第 3 选择器 63 转换时输入转换器 96 及输出转换器 97 也转换。

图 33 是图 32 所示加密装置的操作顺序示意图。

在时刻 T0 和 T1 之间进行明文块数据 M_1 的保密处理。在保密处理过程中所生成的模块输出数据存储于第 1 暂存器 98。在时刻 T1 和 T2 之间进行基于密文块数据 C_1 的认证码演算。由完整性保证处理所生成的认证码演算中间结果存储于第 2 暂存器 99。接着，在时刻 T2 和 T3 之间，基于第 1 暂存器 98 所存储的模块输出数据和明文块数据 M_2 进行明文块数据 M_2 的保密处理。接着，在时刻 T3 和 T4 之间，第 2 暂存器 99 所存储的认证码演算中间结果和密文块数据 C_2 被输入，进行认证码演算。通过重复这种处理，完成保密处理和完整性认证处理，输出密文和认证码 P。图 33 所示的情况，是到时刻 T6 结束处理，虽然没有谋求时间的缩短，但如图 32 所示，由于兼用了使用加密键 K 的加密模块 51、“异”逻辑电路 58 和反馈线 67、68（反馈回路），所以可以缩小电路规模。

图 34 是具有 OFB 模式解密部 300 和 CBC 模式认证码生成部 400 的解密装置示意图。

该认证码生成部 400 与认证码生成部 200 的结构相同。

图 34 的解密装置，用于将由 1 个以上密文块数据所组成的密文解密成明文，并针对密文生成为确认密文完整性的认证码，其特征在于：包括

解密部 300，具有在通过解密模块 71 对密文块数据 C_i 进行解密后，反馈所生成的模块输出块数据 T_i 的第 1 反馈回路 65，并用于输

入密文块数据 C_i，而且通过第 1 反馈回路 65 反馈模块输出块数据 T_i 进行解密处理，输出明文块数据 M_i；

认证码生成部 400，具有反馈认证码演算中间结果 T_i 的第 2 反馈回路 66，并用于输入与输入到解密部 300 的密文块数据 C_i 相同的密文块数据，进行认证码演算处理输出认证码演算中间结果 T_i，并通过第 2 反馈回路 66 反馈认证码演算中间结果 T_i，从而生成为确认密文完整性的认证码 Q。

密文块数据 C_i，在输入至解密部 300 的“异”逻辑电路 78 的同时，通过反馈线 69 输入至认证码生成部 400。基于这样的结构，解密部 300 和认证码生成部 400 同时并行地进行处理，处理速度得到提高。

图 35，将图 34 所示解密装置的解密部 300 和认证码生成部 400 一体化。

图 35 表示兼用使用加密键 K 的解密模块 71 和反馈线 87、88（反馈回路）的情况。

第 1 选择器 81，在解密处理开始时选择初始值 IV。第 2 选择器 82，在完整性保证处理开始时选择初始值 IV。第 3 选择器 83，交互选择解密处理和完整性保证处理。第 3 选择器 83 通过设输入为 E，可进行解密处理。而且，第 3 选择器 83 通过设输入为 F，可进行完整性保证处理。

存储器 93，存储从使用加密键 K 的加密模块 51 输出的模块输出数据 T_i。存储器 93，由输入转换器 96、输出转换器 97、第 1 暂存器 98 和第 2 暂存器 99 构成。输入转换器 96 和输出转换器 97，同步于第 3 选择器 83 的转换，每当第 3 选择器 83 转换时输入转换器 96 及输出转换器 97 也转换。

图 36 是图 35 所示解密装置的操作顺序示意图。

在时刻 T0 和 T1 之间进行密文块数据 C_1 的解密处理和将密文块数据 C_1 存储于暂存器 111。在解密处理过程中所生成的模块输出数据存储于第 1 暂存器 98。在时刻 T1 和 T2 之间进行基于暂存器 111 所存储的密文块数据 C_1 的认证码演算。由完整性保证处理所生成的认证码演算中间结果存储于第 2 暂存器 99。接着，在时刻 T2 和 T3 之间，密文块数据 C_2 存储于暂存器 111，基于第 1 暂存器 98 所存储的

模块输出数据和密文块数据 C_2 进行密文块数据 C_2 的解密处理。接着，在时刻 T3 和 T4 之间，第 2 暂存器 99 所存储的认证码演算中间结果和暂存器 111 所存储的密文块数据 C_2 被输入，进行认证码演算。通过重复这种处理，输出明文和认证码 Q。该认证码 Q，与认证码 P 相比较，如果认证码 Q 与认证码 P 一致，则数据的完整性被认证。至此，解密处理和完整性认证处理结束。

图 37 将图 290FB 模式的加密部 100 作为了 CBC 模式的加密部 100。

图 37 的加密装置，将由 1 个以上的明文块数据组成的明文加密成密文，并针对密文生成为保证密文完整性的认证码，其特征在于：包括

加密部 100，具有通过加密单元 52 在对明文块数据进行加密后，反馈加密模块 51 输出的密文块数据 C_i 的第 1 反馈回路 65，并用于输入明文块数据 M_i，而且通过第 1 反馈回路 65 反馈密文块数据 C_i 进行加密处理，输出密文块数据 C_i；

认证码生成部 400，具有用于反馈认证码演算中间结果 T_i 的第 2 反馈回路 66，每当从加密部 100 输出密文块数据 C_i 时，用于输入密文块数据 C_i，进行认证码演算处理，并通过第 2 反馈回路 66 反馈认证码演算中间结果 T_i，从而生成为保证密文完整性的认证码 P。

图 38 将图 340FB 模式的解密部 300 作为了 CBC 模式的解密部 300。

图 38 的解密装置，用于将由 1 个以上密文块数据所组成的密文解密成明文，并针对密文生成为确认密文完整性的认证码，其特征在于：包括

解密部 300，具有反馈密文块数据 C_i 的第 1 反馈回路 85、82，并用于输入密文块数据 C_i，而且通过第 1 反馈回路 85、82 反馈密文块数据 C_i 进行解密处理，输出明文块数据 M_i；

认证码生成部 400，具有反馈认证码演算中间结果 T_i 的第 2 反馈回路 66，并用于输入与输入到解密部 300 的密文块数据 C_i 相同的密文块数据 C_i，进行认证码演算处理输出认证码演算中间结果 T_i，并通过第 2 反馈回路反馈认证码演算中间结果 T_i，从而生成为确认密文完整性的认证码 Q。

如以上所述，图 29、图 37 所表示的加密装置，其特征在于：具有输入数据进行加密，并输出密数据的加密部，和输入加密部所输出的密数据并生成为保证密文完整性的认证码的认证码生成部，认证码生成部在基于加密部的数据加密结束之前开始生成认证码。

同时，图 34、图 38 所表示的解密装置，其特征在于：具有输入数据进行解密，并输出解密数据的解密部，和输入解密部所输入的数据并生成为保证密文完整性的认证码的认证码生成部，认证码生成部在基于解密部的数据解密结束之前开始生成认证码。

另外，虽未图示，也可以使用 OFB 模式的加密部 100 或解密部 300。

另外，虽未图示，也可以使用 OFB 模式或 CFB 模式的认证码生成部 200。

图 39 是加密模块 51 或解密模块 71 的结构图。

加密模块 51 具有键调度部 511 和随机数据发生部 512。键调度部 511 输入 1 个键 K 进而生成 n 个扩展键 $ExtK_1$～$ExtK_n$。随机数据发生部 512 通过函数 F 和 XOR 电路发生随机数。函数 F，输入扩展键并进行非线形数据变换。

在所述加密装置的加密模块 51 中，可以使用例如

（1） DES（Data Encryption Standard），或

（2）MISTY，国际公开号 WO97／9705（美国专利申请号 08／83640）所公开的块密码算法，或

（3）KASUMI，以所述块密码算法 MISTY 为基础的 64 位块密码，作为下时代携带电话用国际标准密码（IMT2000）而被决定采用的块密码算法（详细内容参照 http: ／／www. 3gpp. org／About _ 3GPP ／3gpp. htm），或

（4）Camellia，日本专利申请号 2000－64614（申请日 2000 年 3 月 9 日）所记载的块密码算法

等的块密码算法。而且，在所述解密装置的解密模块 71 中，也可以使用 DES、MISTY、KASUMI 或 Camellia 等的块密码算法。

图 40 是所述加密装置或解密装置的装饰形式示意图。

图 40 表示在 FPGA 或 IC 或 LSI 中所实现的所述加密装置及解密装置。即所述加密装置及解密装置可以由硬件来实现。而且，虽未

图示，也可以通过印制电路板来实现。

图 41 表示由软件实现所述加密装置及解密装置的情况。

所述加密装置，可由加密程序 47 来实现。加密程序 47 存储在 ROM（Read Only Memory）42（记录媒体的一例）。加密程序 47 也可以记录在 RAM（Random Access Memory）或软盘或固定磁盘等的其他记录媒体上。而且，加密程序 47 也可以由计算机服务器上下载。加密程序 47 作为子程序运行。加密程序 47，被从 RAM45 所存储的应用程序 46 通过子程序调用函数而调出执行。或是加密程序 47，也可以通过中断控制部 43 所接收的中断的发生来启动。存储器 55 可以是 RAM45 的一部分。应用程序 46、加密程序 47，都是由 CPU41 来执行的程序。

图 42 表示应用程序 46 调用加密程序 47 的机构。

应用程序 46，以键 K、初始值 IV、明文 M 和密文 C 为参数调用加密程序 47。加密程序 47，输入键 K、初始值 IV 和明文 M，返回密文 C。当加密程序 47 与解密程序合一时，以键 K、初始值 IV、密文 C 和明文 M 为参数调用加密程序 47。

而且，虽未图示，加密程序 47 也可以通过数字信号处理器、和由该数字信号处理器所读取并执行的程序来实现。即可以通过硬件和软件的组合来实现加密程序 47。

图 40、图 41、图 42，虽然主要说明了加密装置的情况，但解密装置也可以用同样的方式来实现。

图 40 及图 41 所示的加密装置及解密装置可以安装进电子设备。例如，可以安装进个人电脑、传真机、携带电话、摄象机、数字照相机、电视摄象机等的所有电子设备。特别是本实施方式特征的发挥在加密、解密多个信道的数据时很有效。或是在多个用户的数据随机到达并进行解密时，或是针对多个用户的数据随机发生，并对每个数据进行实时加密时有效。即与加密、解密数据的数量相比加密、解密装置的数量少时，所述实施方式的加密装置、解密装置非常有效。例如，对于必须支持大量客户机的服务器、必须配送大量携带电话数据的基站或线路控制器等，所述加密装置和解密装置都非常有效。

另外，可以不是加密处理彼此之间以及解密处理彼此之间的并行

处理，而是加密处理和解密处理的并行处理。

另外，虽然表示了 OFB 模式的加密部（或解密部）和 CBC 模式的认证码生成部的组合情况，但 OFB 模式、CBC 模式、CFB 模式、这些模式的改进模式、以及其他模式的任何模式的组合也都可以。

另外，虽然表示了认证码生成部使用加密键 K 进行加密的情况，但认证码生成部也可以进行数据的搅乱、演算以及其他的数据处理。

如以上所述，根据本发明理想的实施方式，在明文 M 的加密过程中可以开始明文 N 的加密。并且，在密文 C 的解密过程中可以开始其他密文 D 的解密。

而且，根据本发明理想的实施方式，通过附加优先权可以根据优先权对加密、解密的数据进行高速处理。

而且，根据本发明理想的实施方式，通过保密处理和完整性保证处理的并行处理可以实现高速处理。并且，保密处理和完整性保证处理可以组合至 1 个硬件来实现。

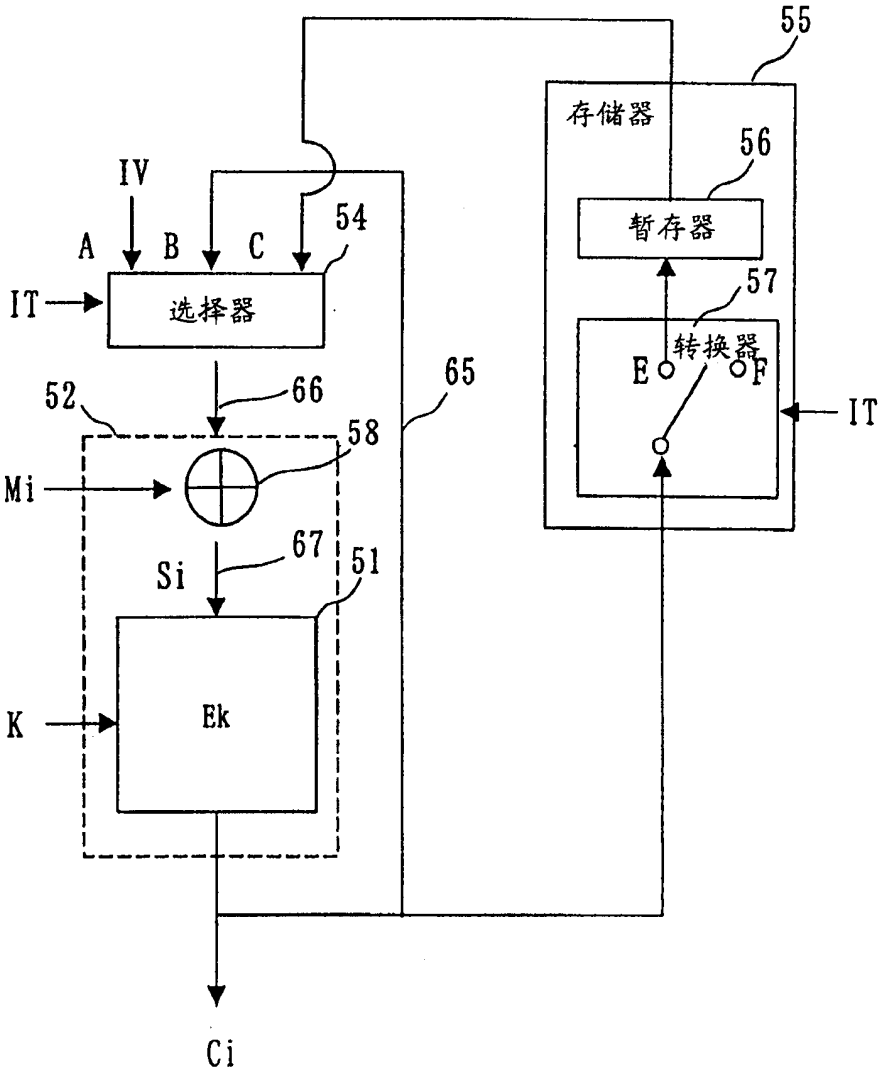

55
存储器
56
暂存器
57
转换器
E
F
IT
IV
A
B
C
54
IT
选择器
65
52
66
58
Mi
67
Si
51
K
Ek
Ci

图 1

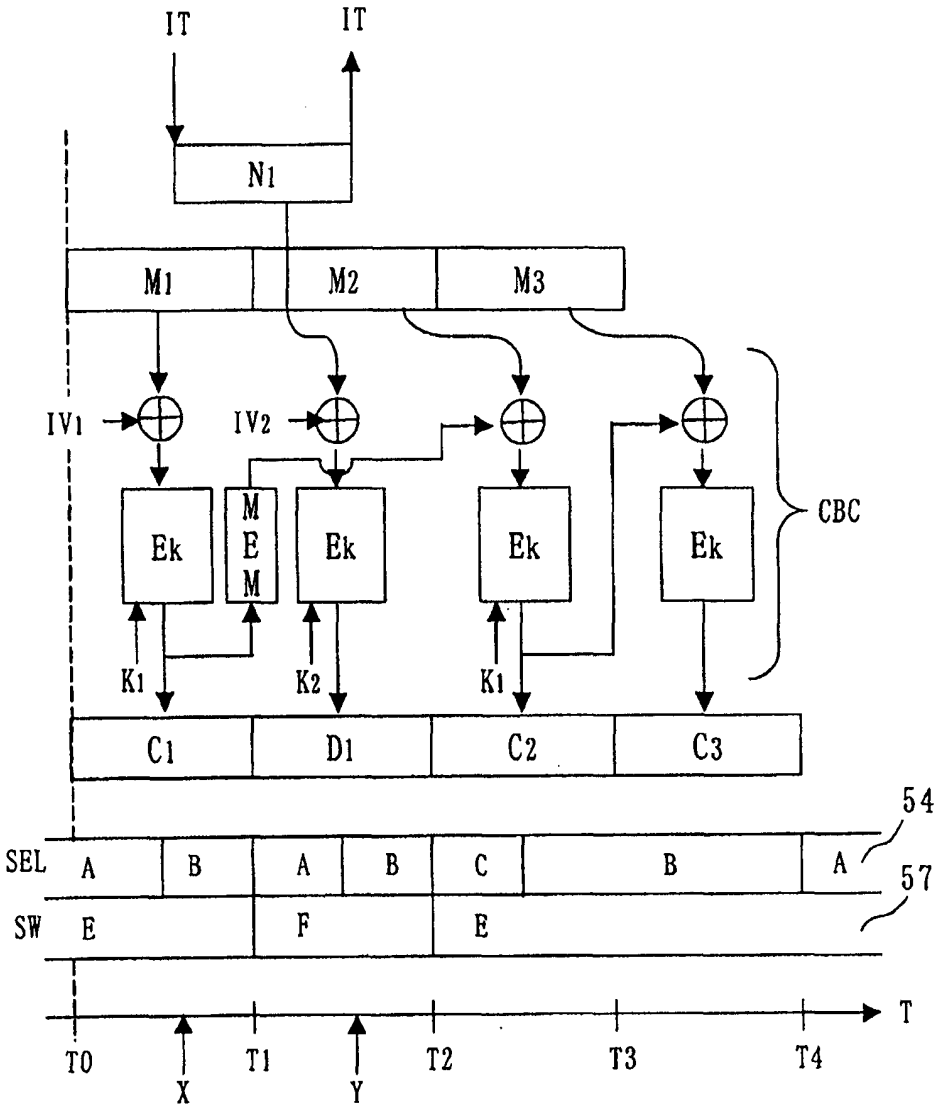

IT
IT
N1
M1
M2
M3
IV1
IV2
Ek
MEM
Ek
Ek
Ek
CBC
K1
K2
K1
C1
D1
C2
C3
54
SEL
A
B
A
B
C
B
A
57
SW
E
F
E
T
T0
X
T1
Y
T2
T3
T4

图 2

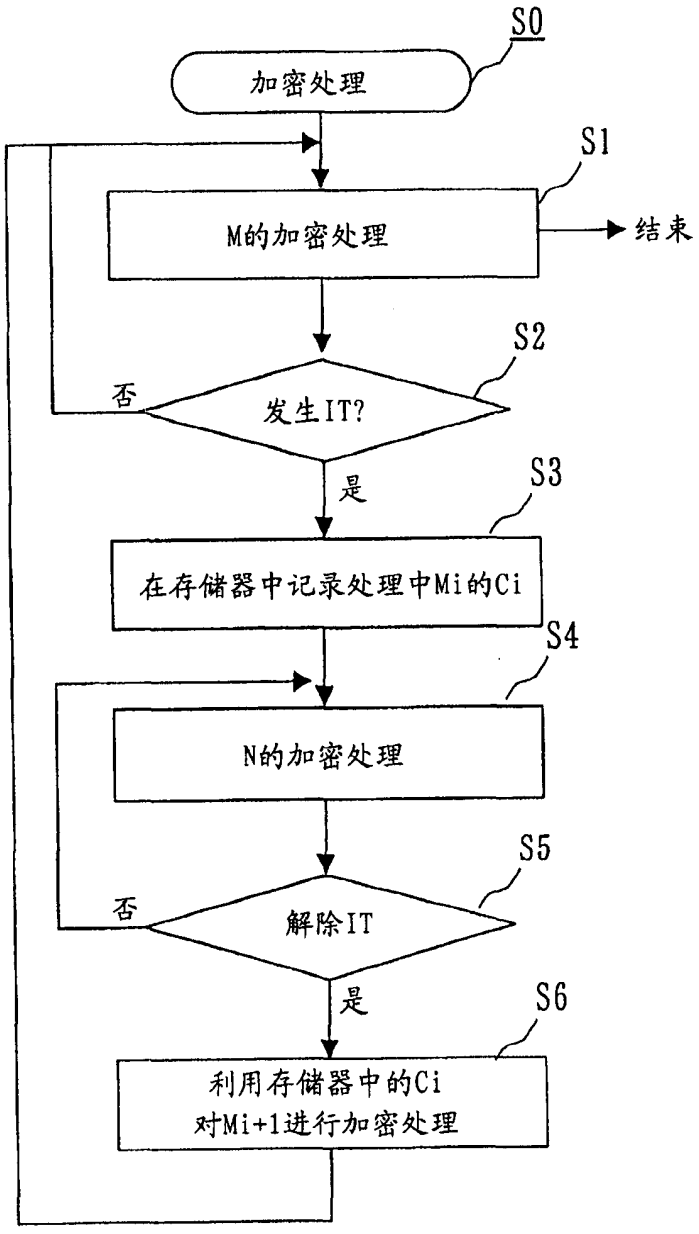

S0
加密处理
S1
M的加密处理
结束
S2
否
发生IT?
是
S3
在存储器中记录处理中Mi的Ci
S4
N的加密处理
S5
否
解除IT
是
S6
利用存储器中的Ci
对Mi+1进行加密处理

图 3

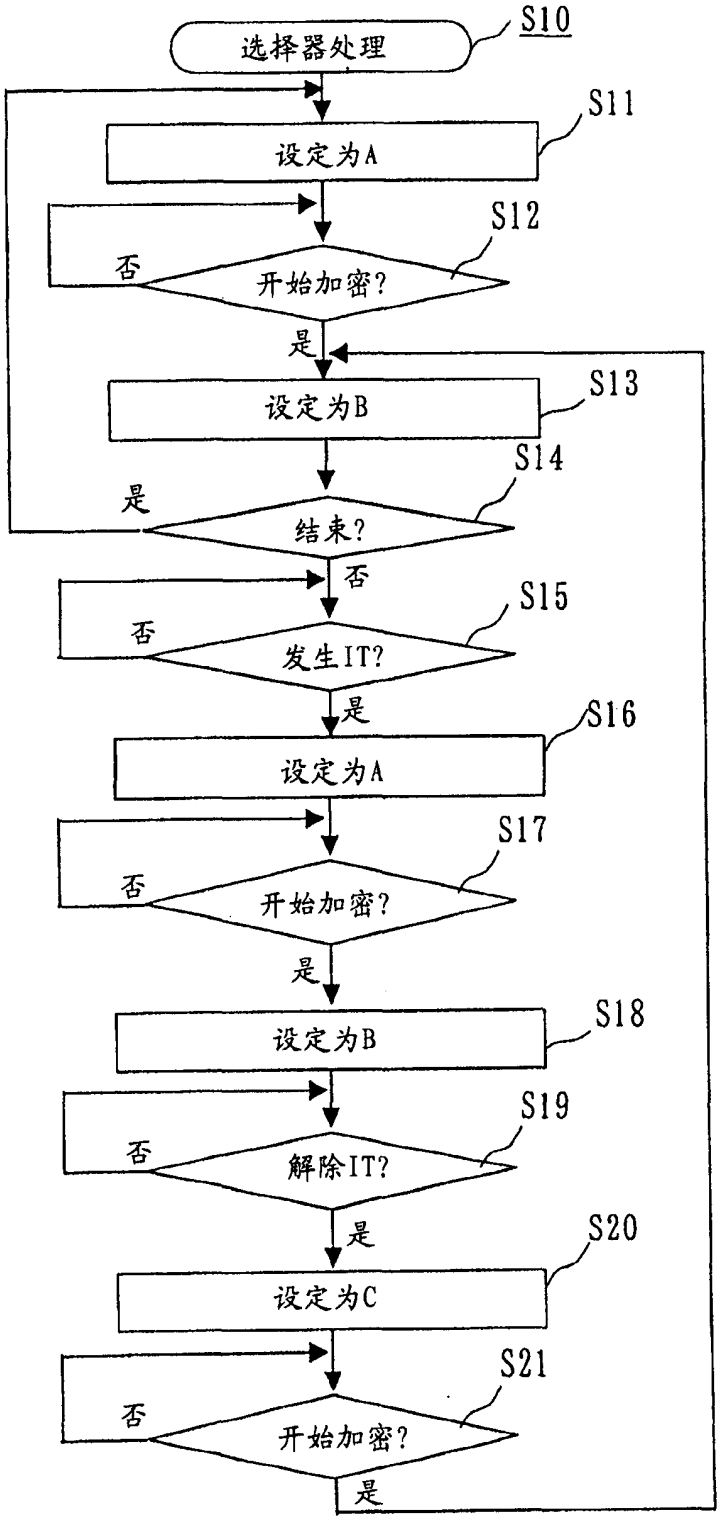

选择器处理
S10
设定为A
S11
开始加密?
S12
否
是
设定为B
S13
结束?
S14
是
否
发生IT?
S15
否
是
设定为A
S16
开始加密?
S17
否
是
设定为B
S18
解除IT?
S19
否
是
设定为C
S20
开始加密?
S21
否
是

图 4

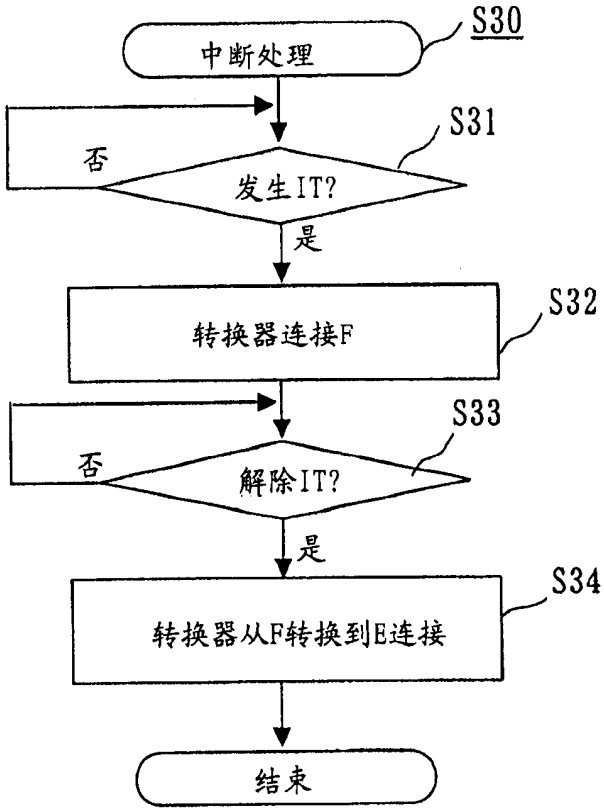

S30
中断处理
S31
否
发生IT?
是
S32
转换器连接F
S33
否
解除IT?
是
S34
转换器从F转换到E连接
结束

图 5

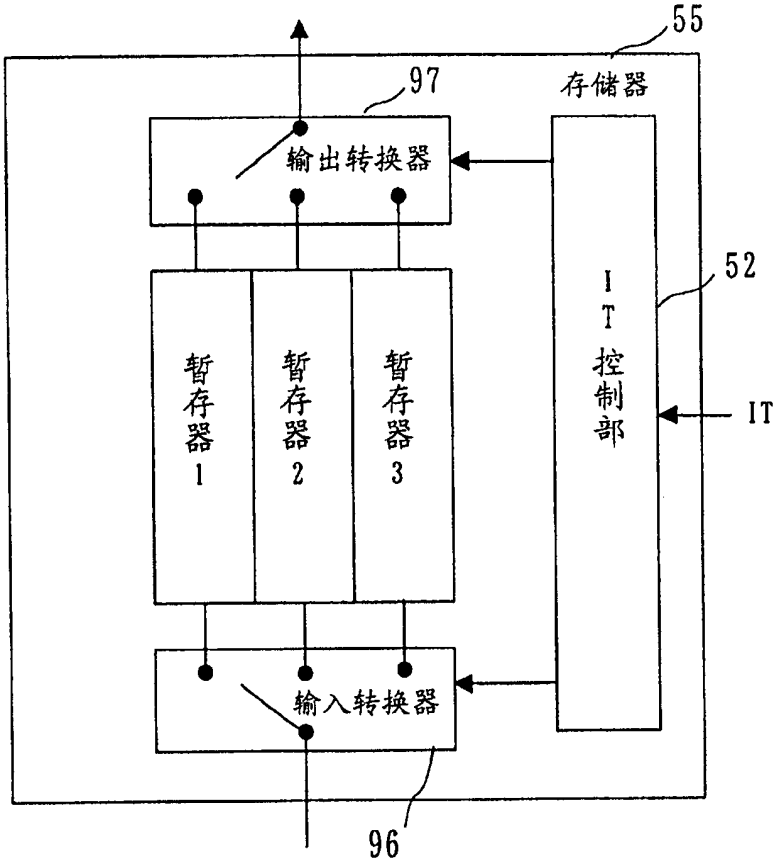


图 6

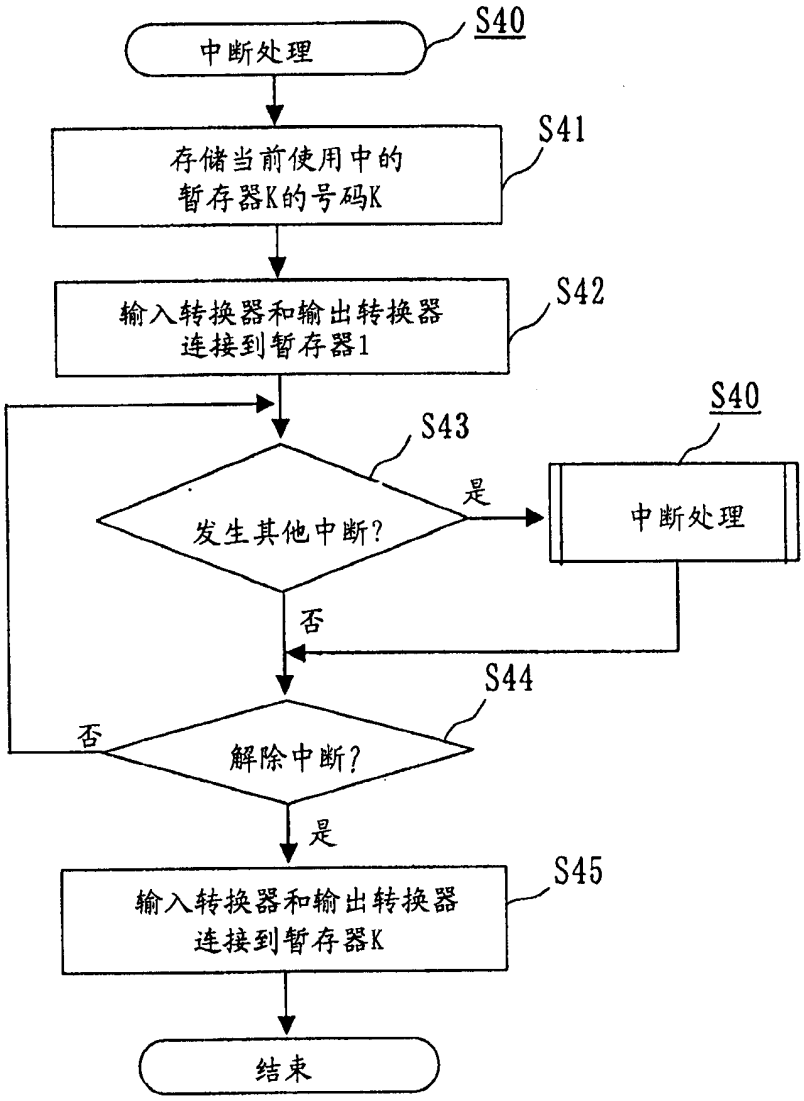

S40
中断处理
S41
存储当前使用中的
暂存器K的号码K
S42
输入转换器和输出转换器
连接到暂存器1
S43
发生其他中断?
是
S40
中断处理
否
S44
解除中断?
否
是
S45
输入转换器和输出转换器
连接到暂存器K
结束

图 7

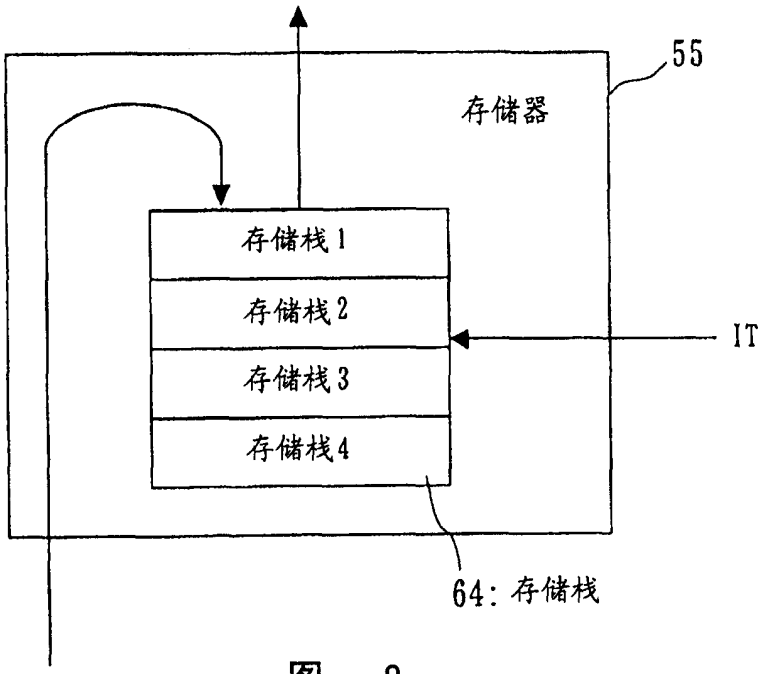

55
存储器
存储栈 1
存储栈 2
存储栈 3
存储栈 4
IT
64: 存储栈

图 8

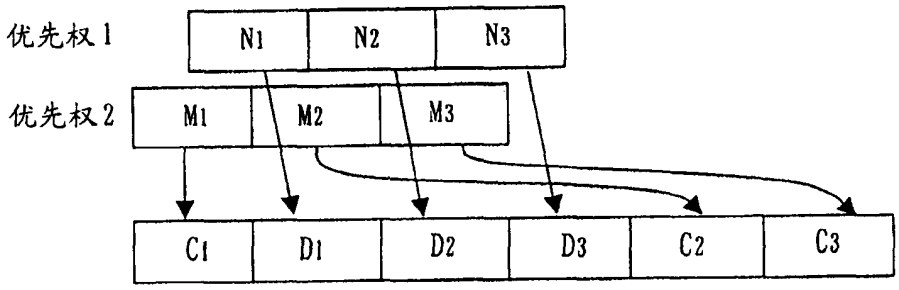

优先权 1
优先权 2
N1
N2
N3
M1
M2
M3
C1
D1
D2
D3
C2
C3

图 9

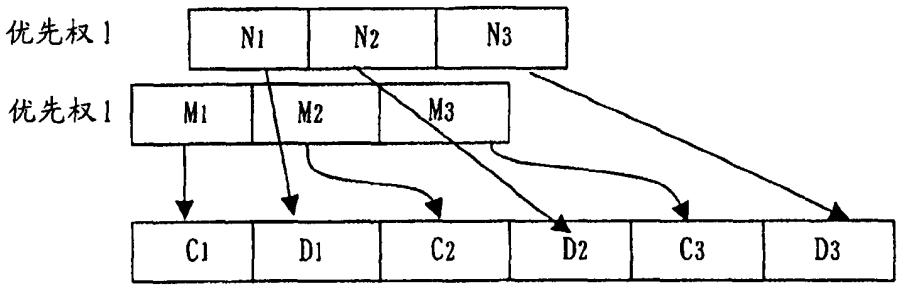

优先权 1
N1
N2
N3
优先权 1
M1
M2
M3
C1
D1
C2
D2
C3
D3

图 10

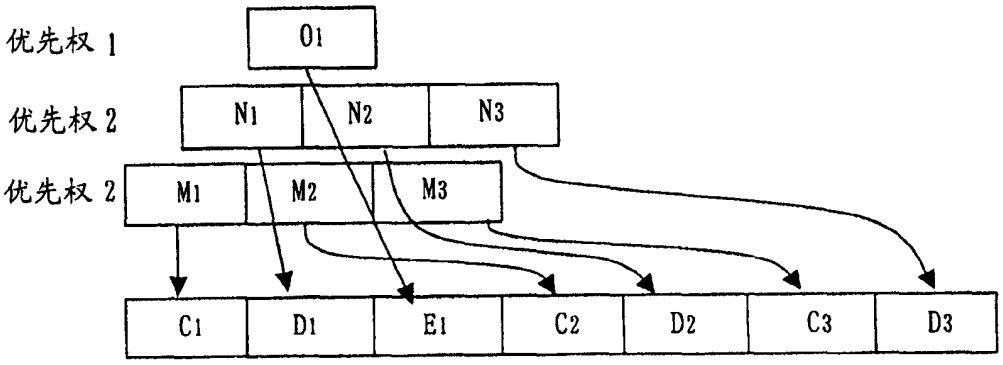

优先权 1
O1
优先权 2
N1
N2
N3
优先权 2
M1
M2
M3
C1
D1
E1
C2
D2
C3
D3

图 11

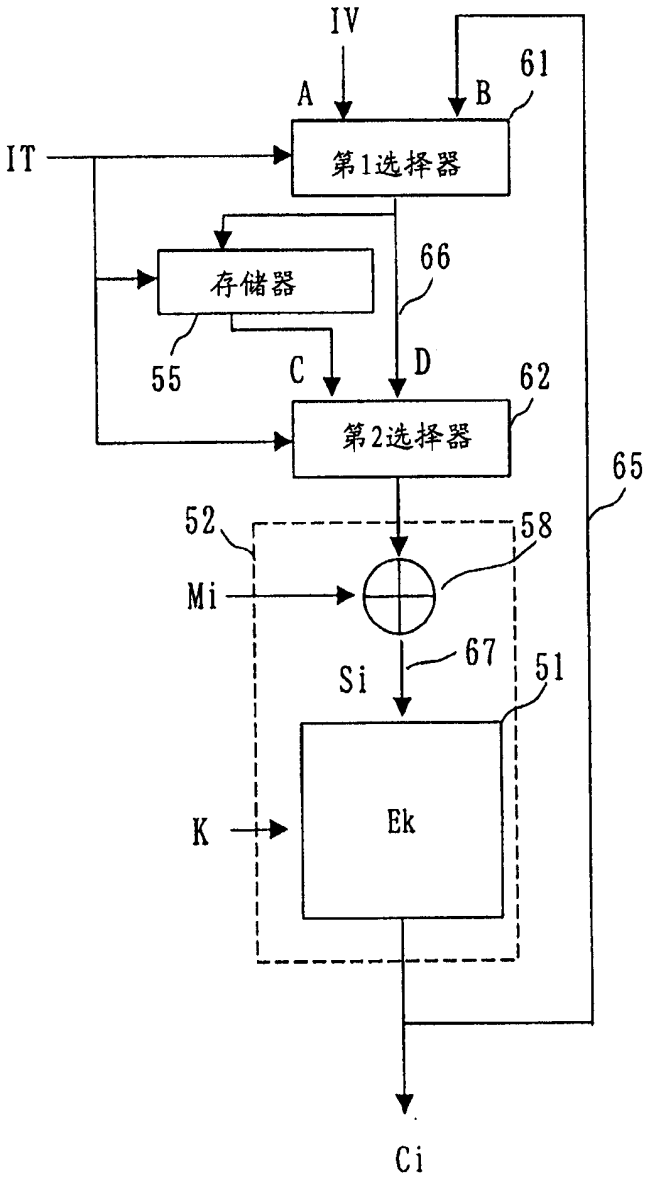


图 12

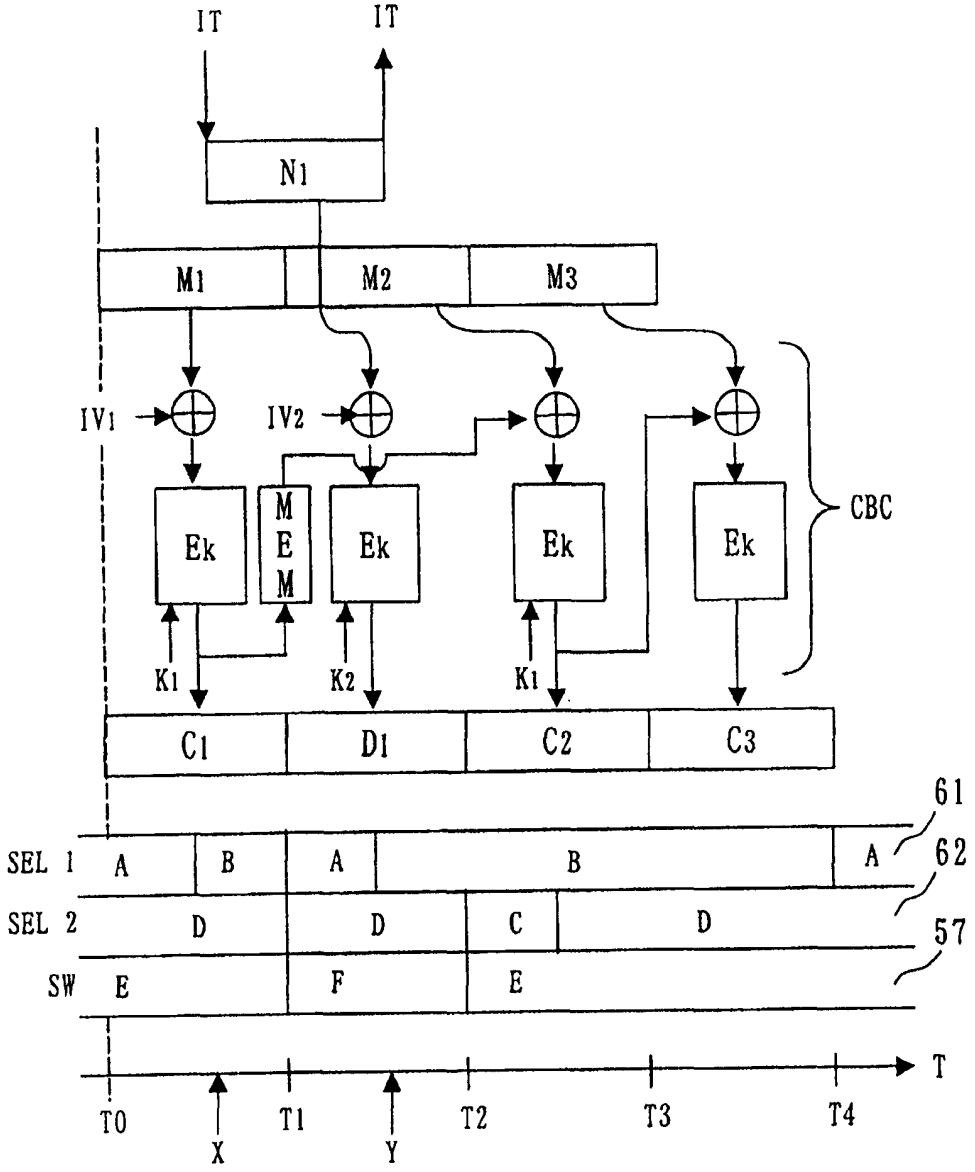

IT
IT
N1
M1
M2
M3
IV1
IV2
Ek
MEM
Ek
Ek
Ek
CBC
K1
K2
K1
C1
D1
C2
C3
61
62
57
SEL 1
SEL 2
SW
A
B
A
B
A
D
D
C
D
E
F
E
T
T0
T1
T2
T3
T4
X
Y

图 13

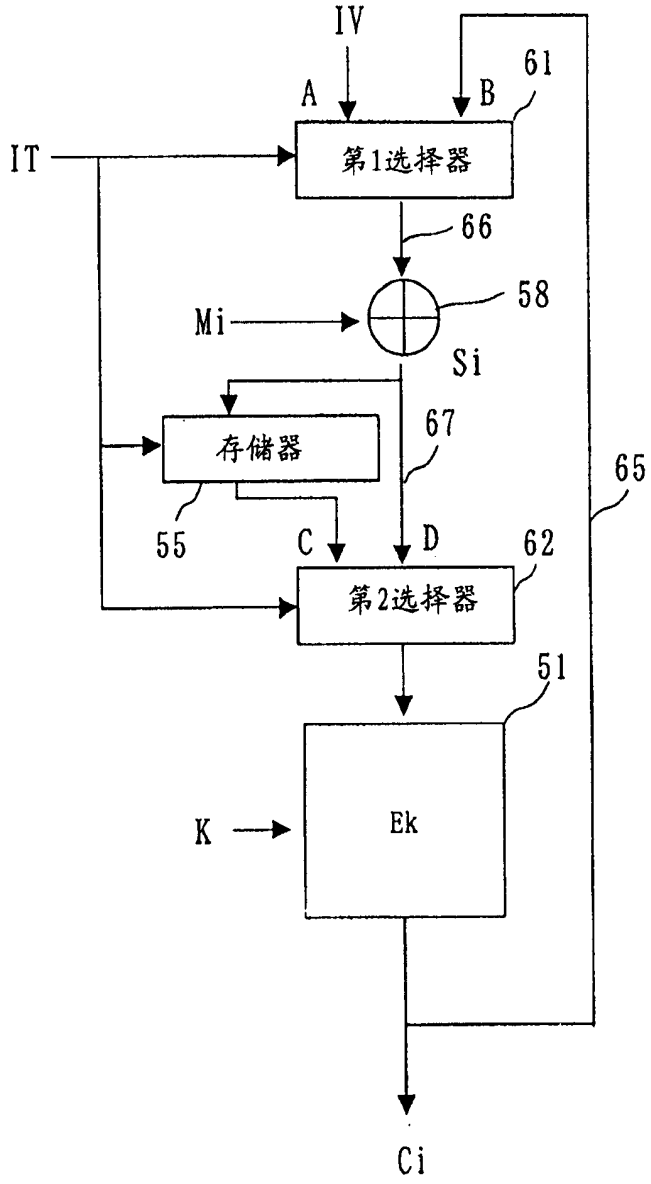


图 14

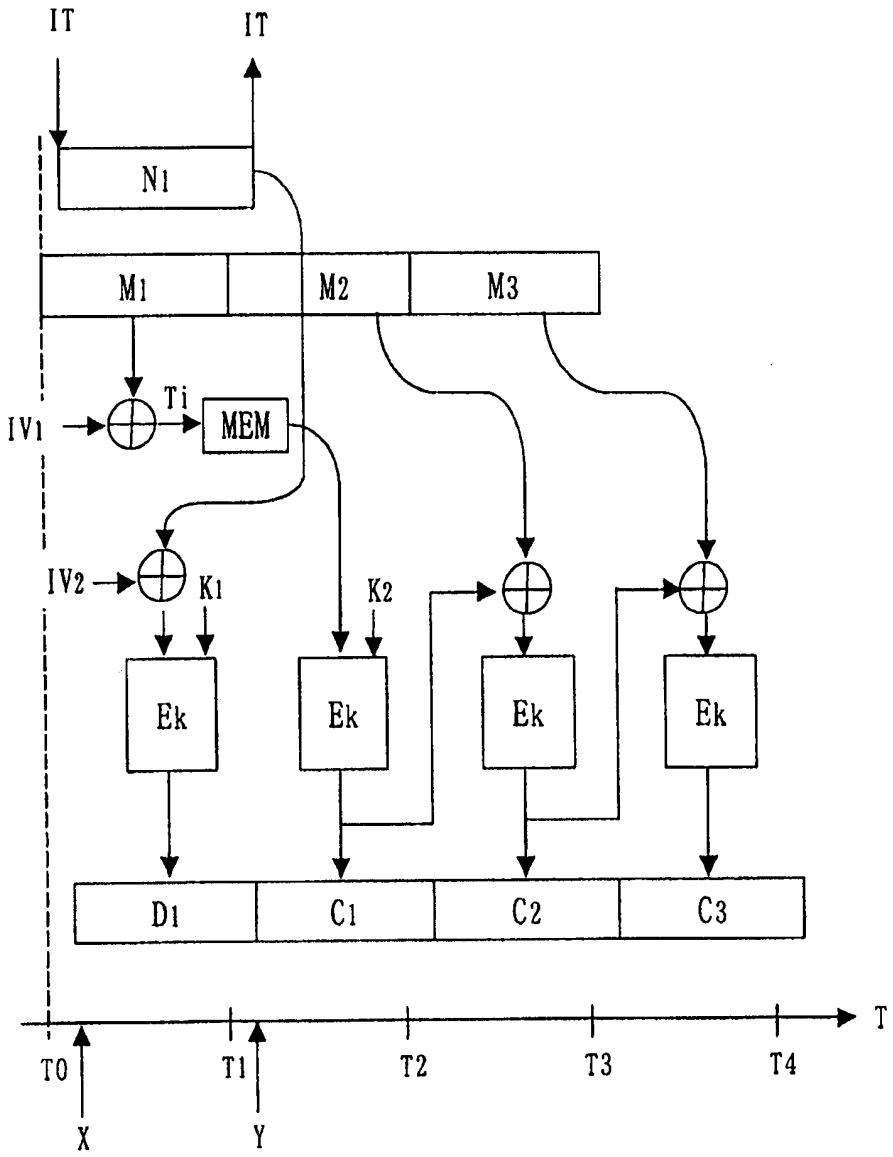

IT
IT
N1
M1
M2
M3
Ti
IV1
MEM
IV2
K1
K2
Ek
Ek
Ek
Ek
D1
C1
C2
C3
T
T0
T1
T2
T3
T4
X
Y

图 15

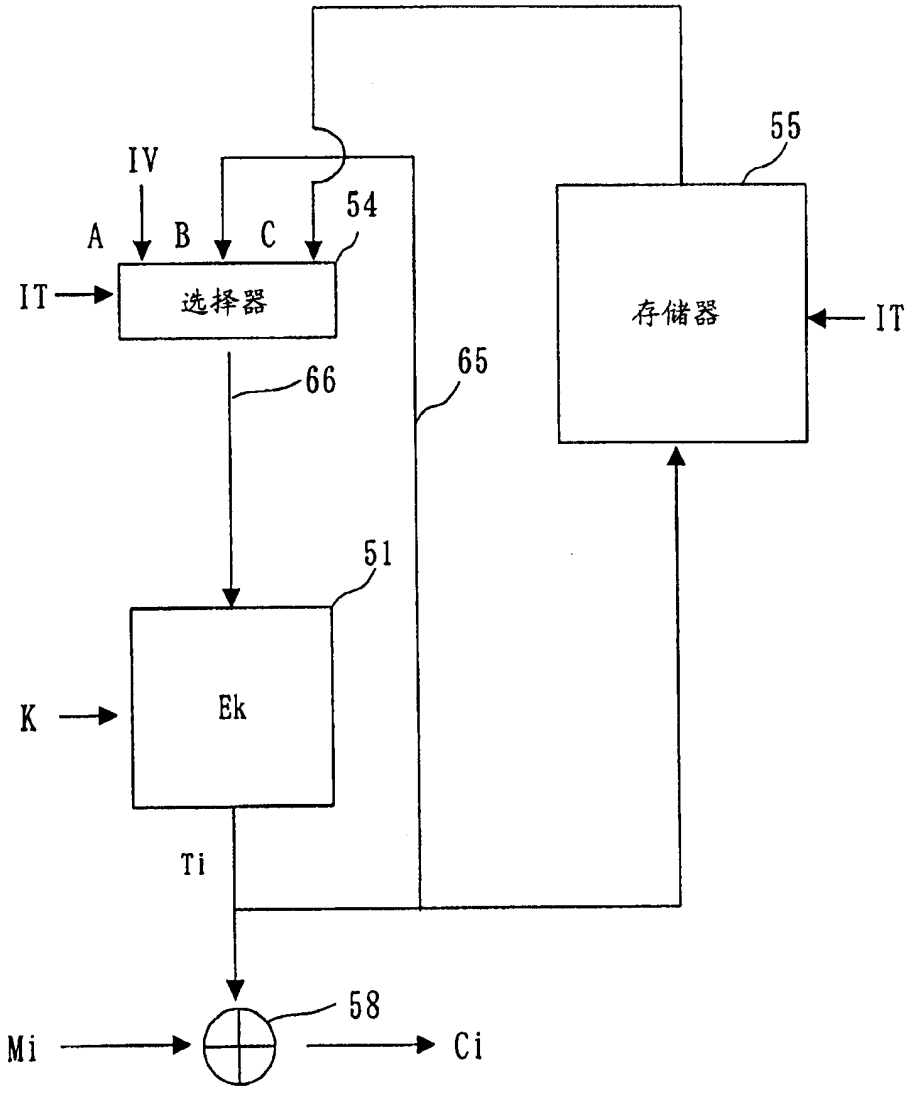


图 16

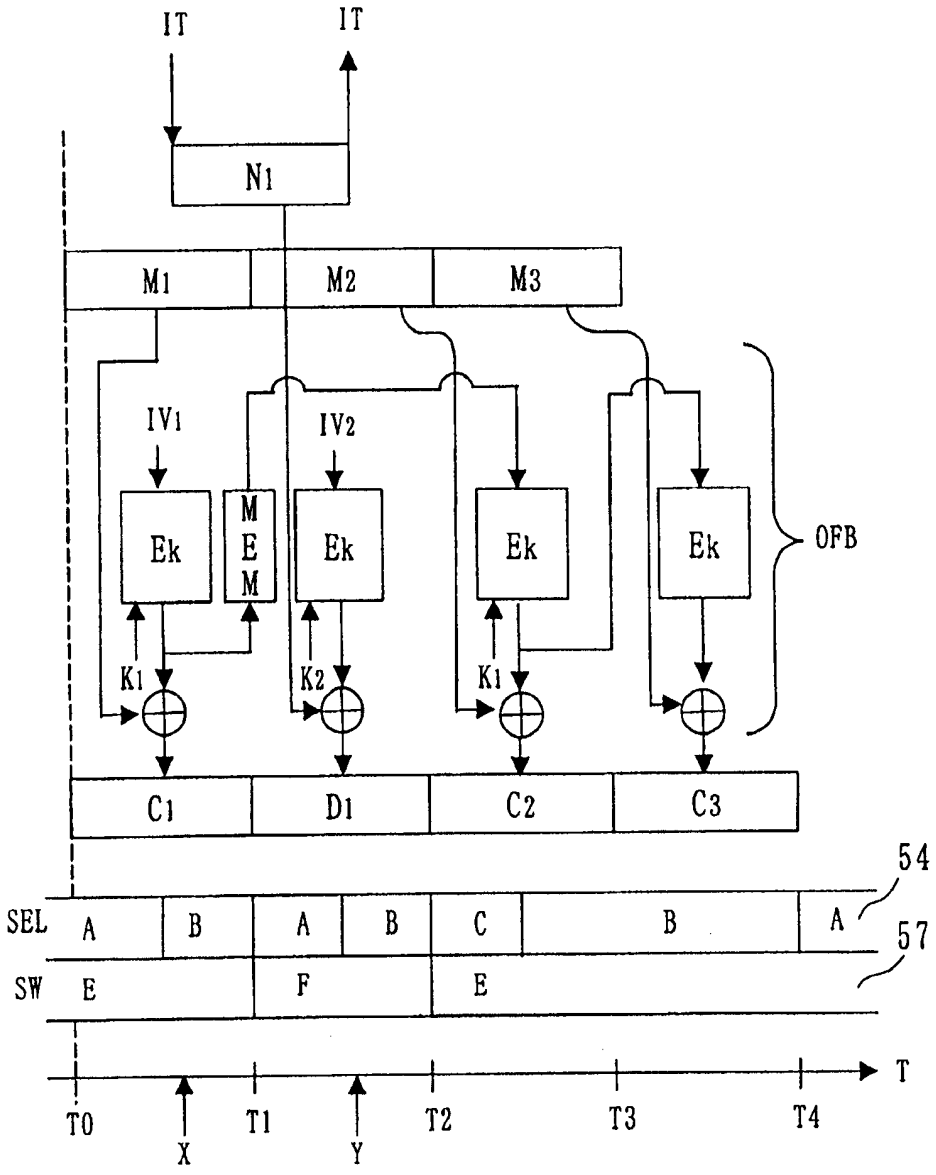

IT
IT
N1
M1
M2
M3
IV1
IV2
Ek
MEM
Ek
Ek
Ek
OFB
K1
K2
K1
C1
D1
C2
C3
54
SEL
A
B
A
B
C
B
A
57
SW
E
F
E
T
T0
X
T1
Y
T2
T3
T4

图 17

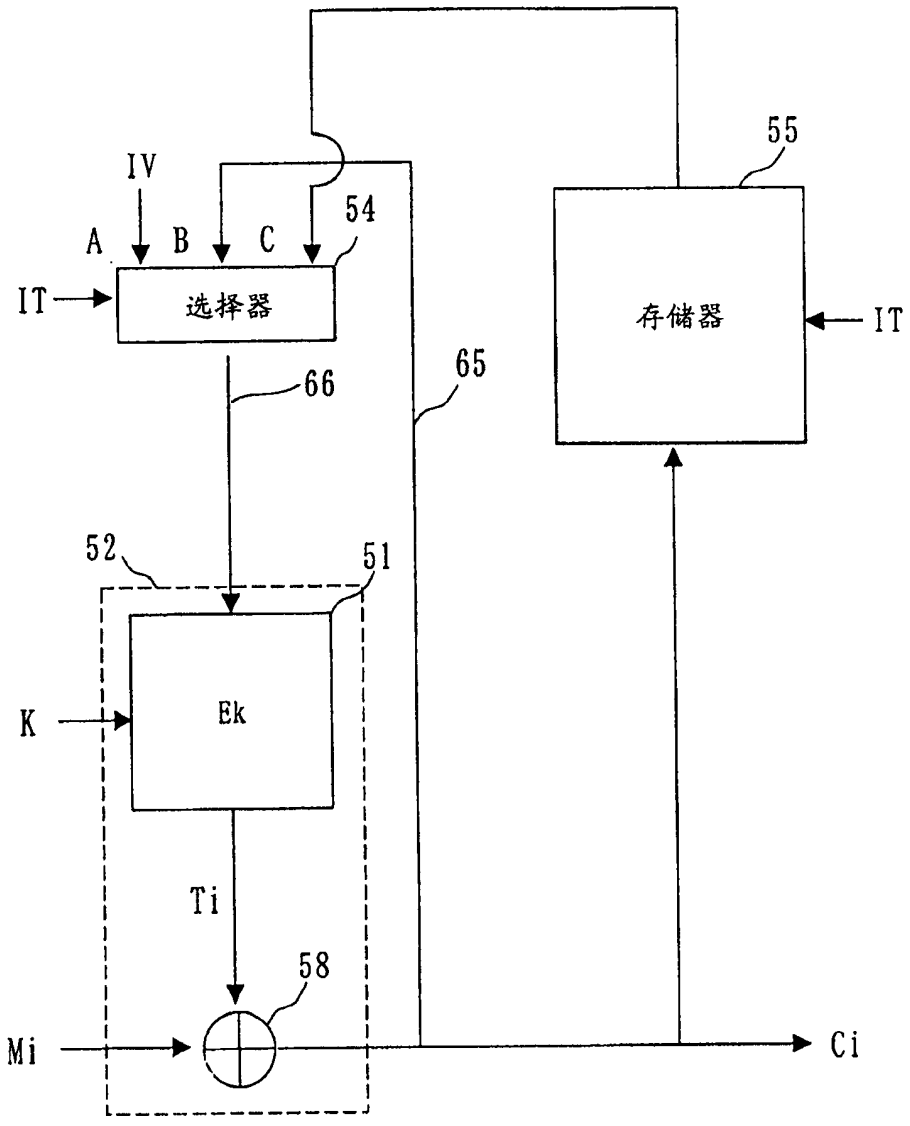


图 18

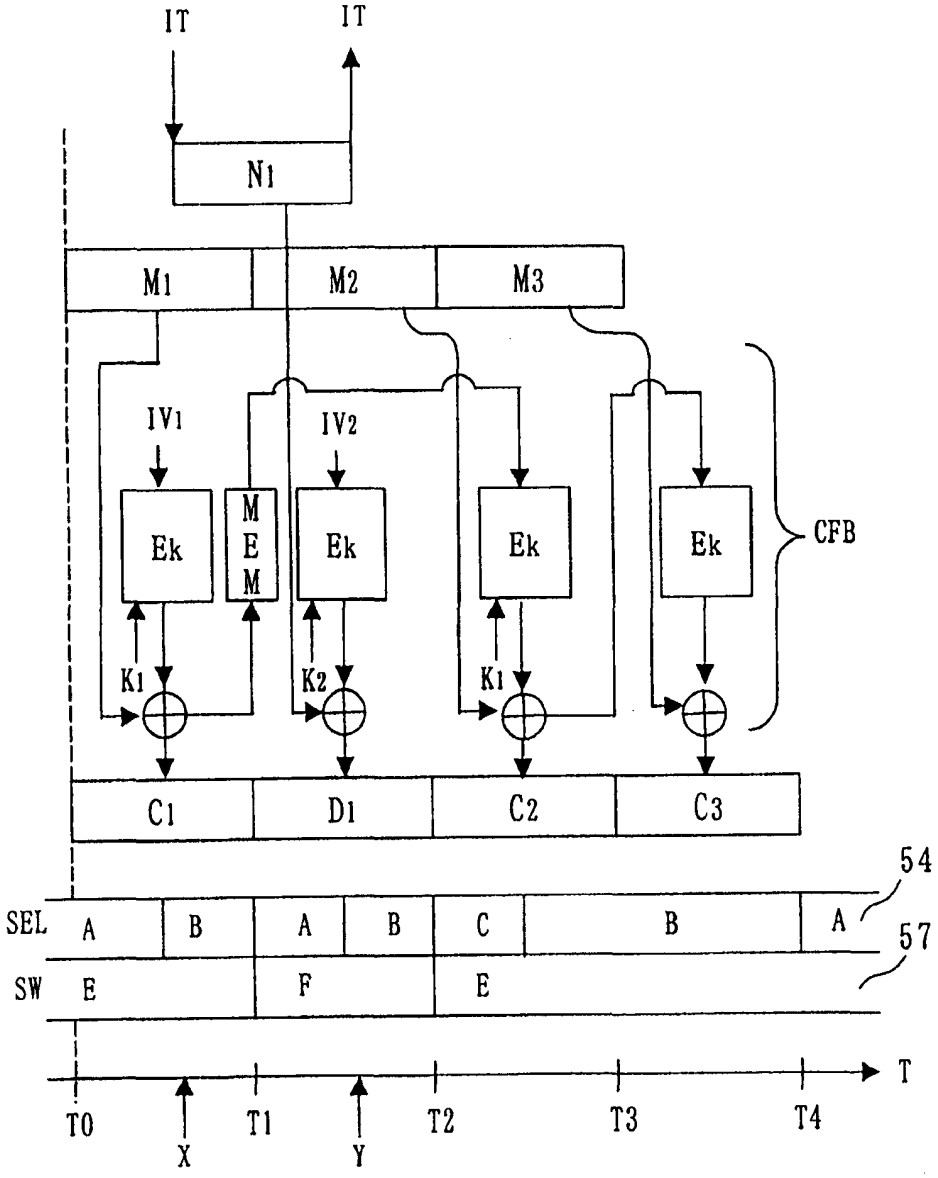

IT
IT
N1
M1
M2
M3
IV1
IV2
Ek
MEM
Ek
Ek
Ek
CFB
K1
K2
K1
C1
D1
C2
C3
54
SEL
A
B
A
B
C
B
A
57
SW
E
F
E
T
T0
X
T1
Y
T2
T3
T4

图 19

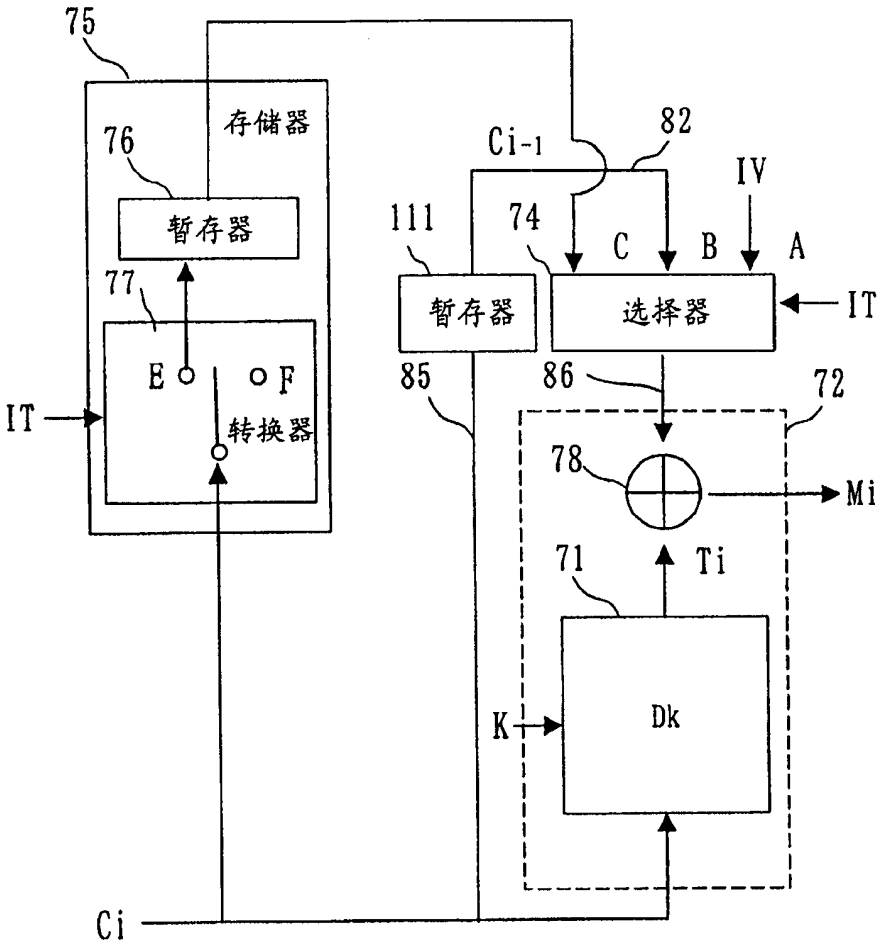

75
存储器
76
暂存器
77
E
F
转换器
IT
Ci
Ci-1
82
IV
111
74
C
B
A
暂存器
选择器
IT
85
86
72
78
Mi
71
Ti
K
Dk

图 20

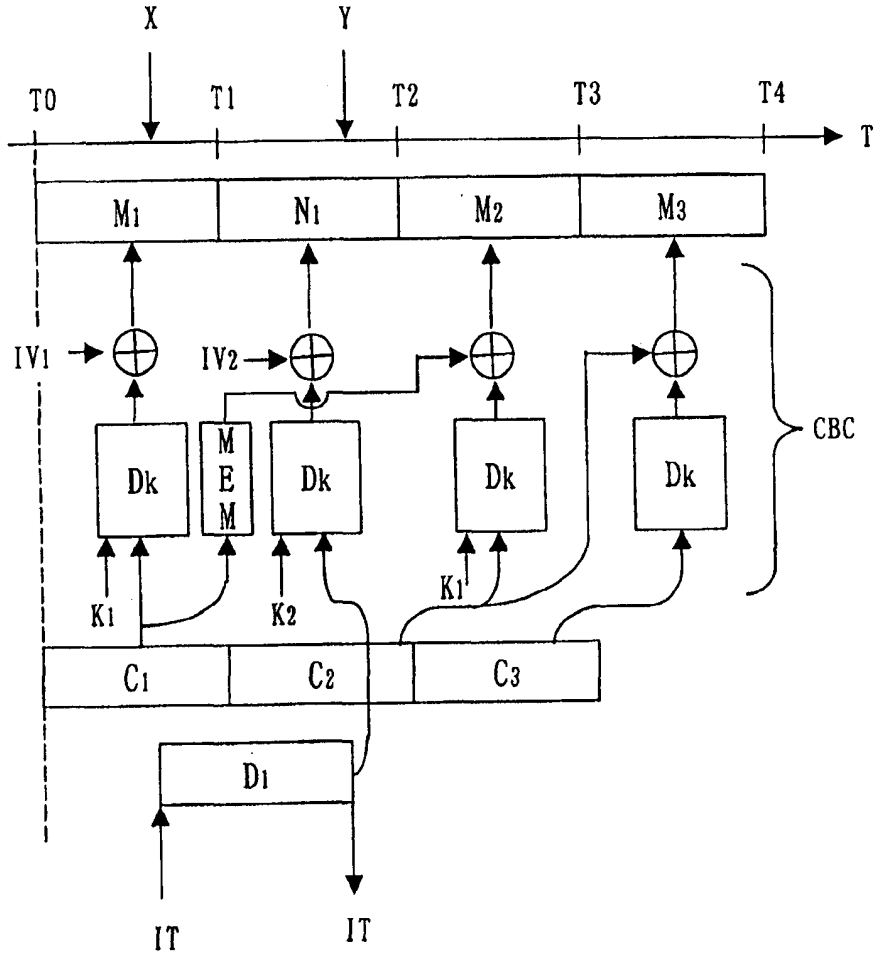

X
Y
T0
T1
T2
T3
T4
T
M1
N1
M2
M3
IV1
IV2
Dk
MEM
Dk
Dk
Dk
CBC
K1
K2
K1'
C1
C2
C3
D1
IT
IT

图 21

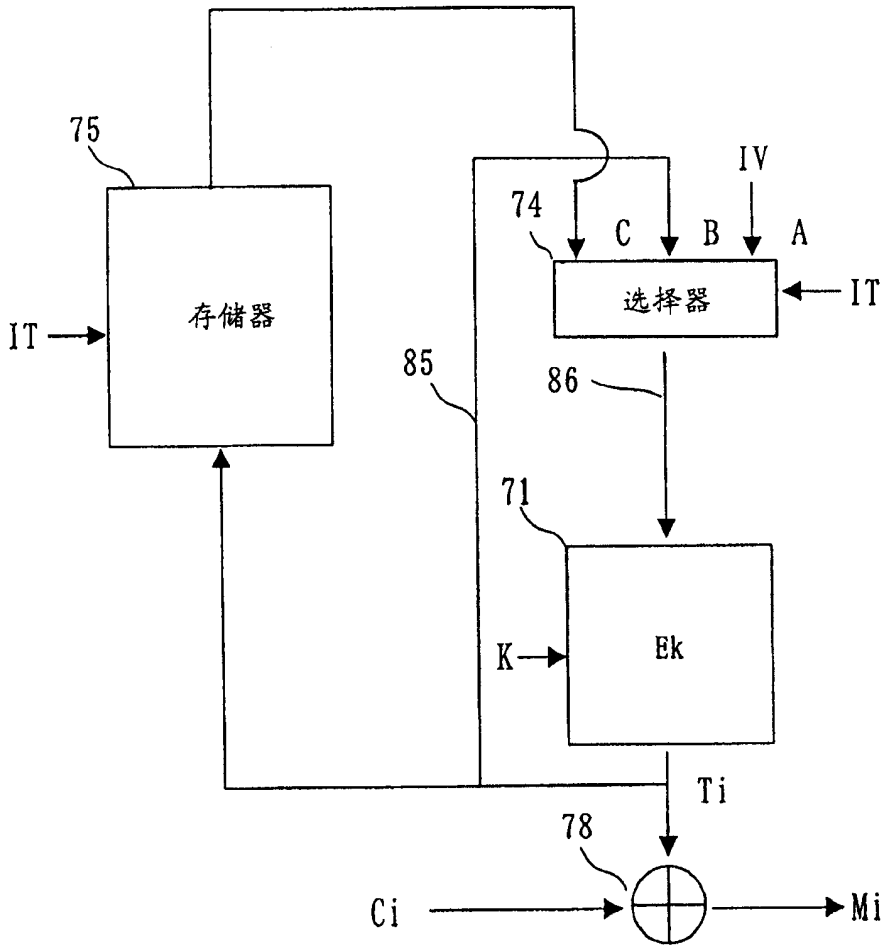


图 22

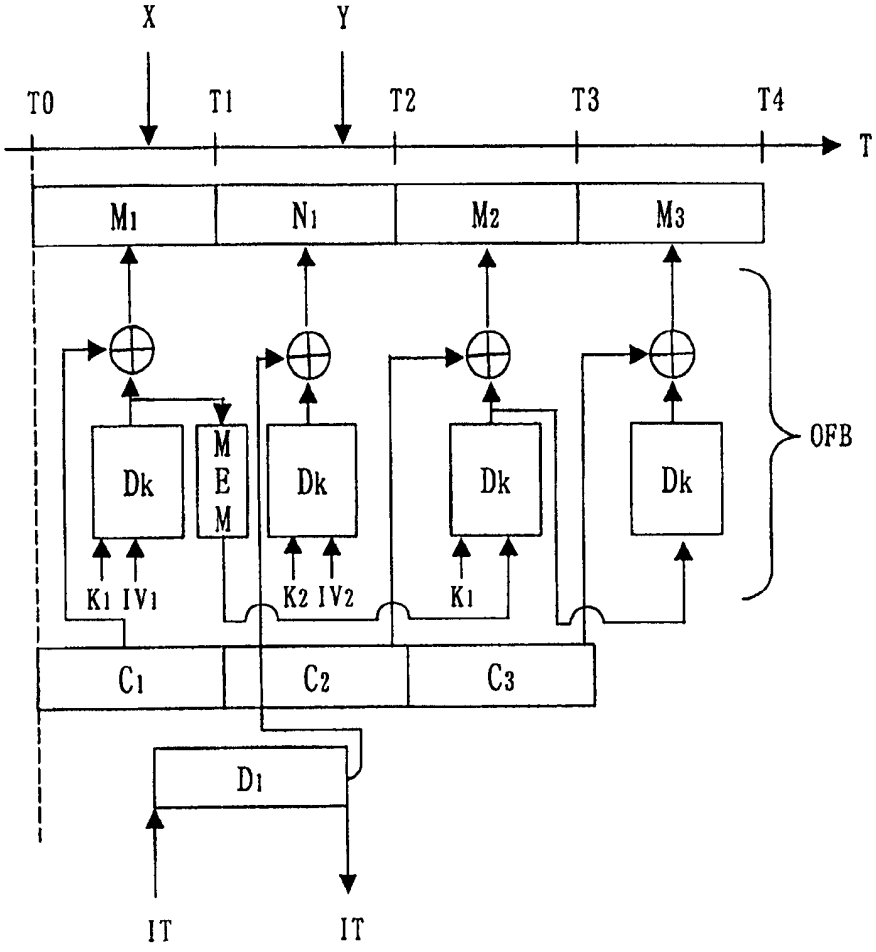

X
Y
T0
T1
T2
T3
T4
T
M1
N1
M2
M3
Dk
MEM
Dk
Dk
Dk
OFB
K1 IV1
K2 IV2
K1
C1
C2
C3
D1
IT
IT

图 23

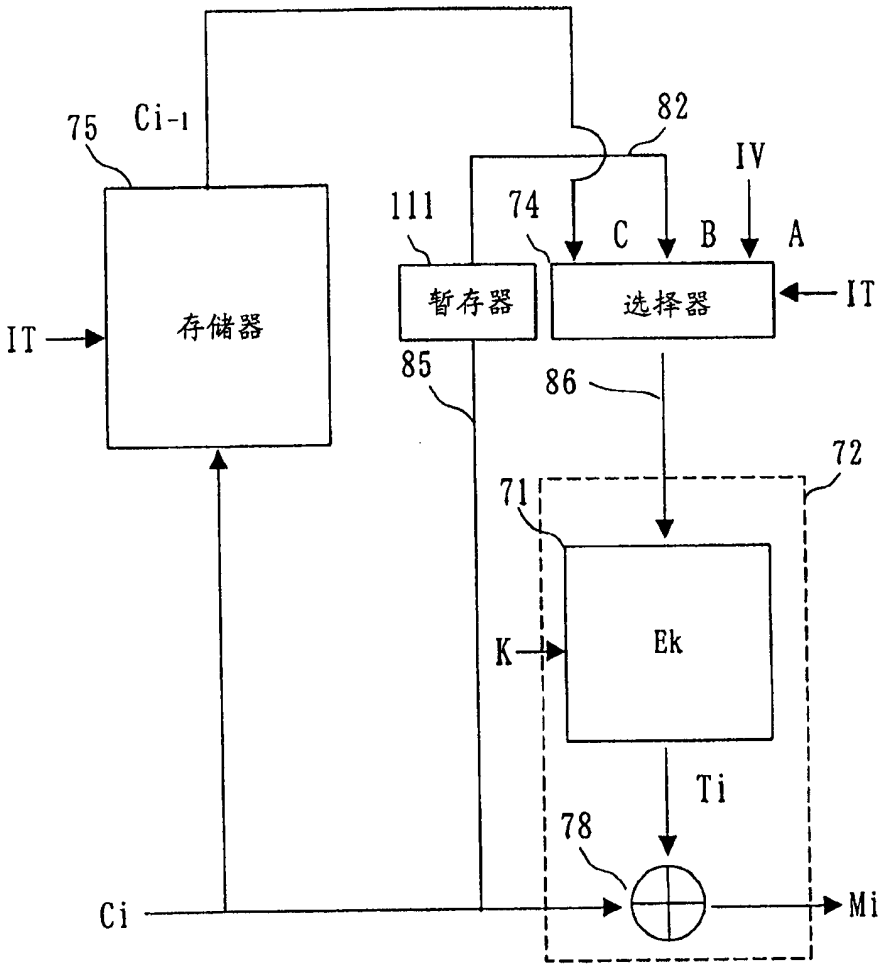


图 24

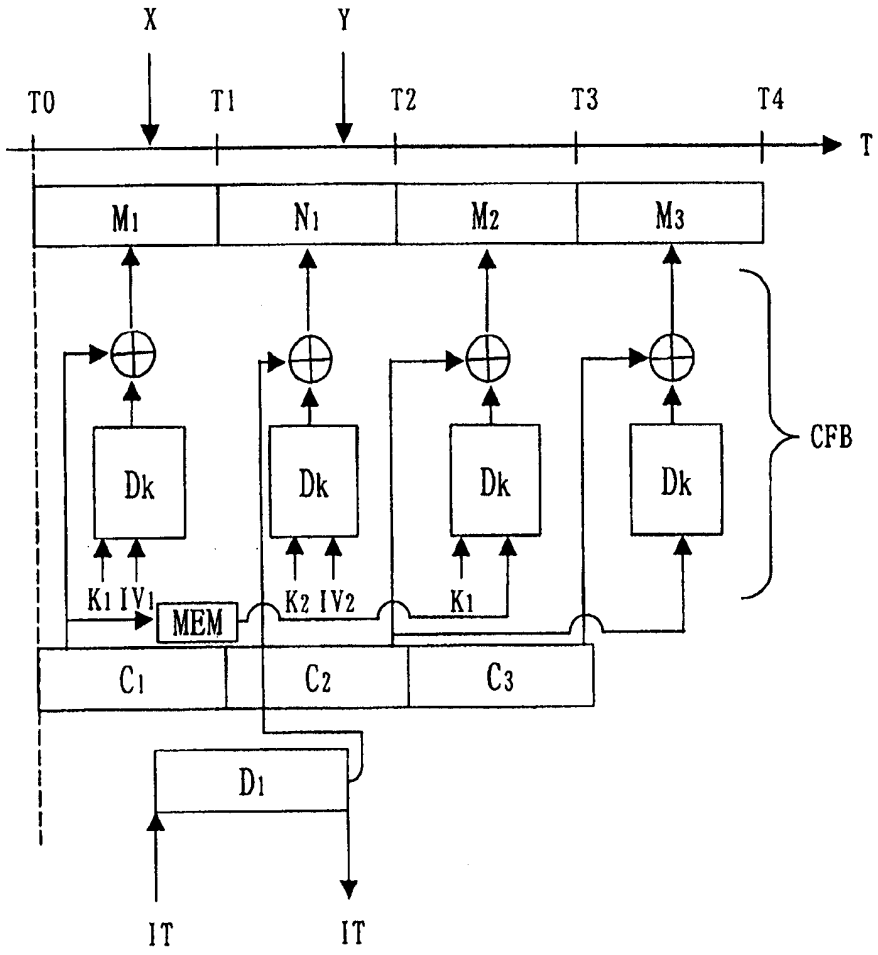

X
Y
T0
T1
T2
T3
T4
T
M1
N1
M2
M3
Dk
Dk
Dk
Dk
CFB
K1 IV1
MEM
K2 IV2
K1
C1
C2
C3
D1
IT
IT

图 25

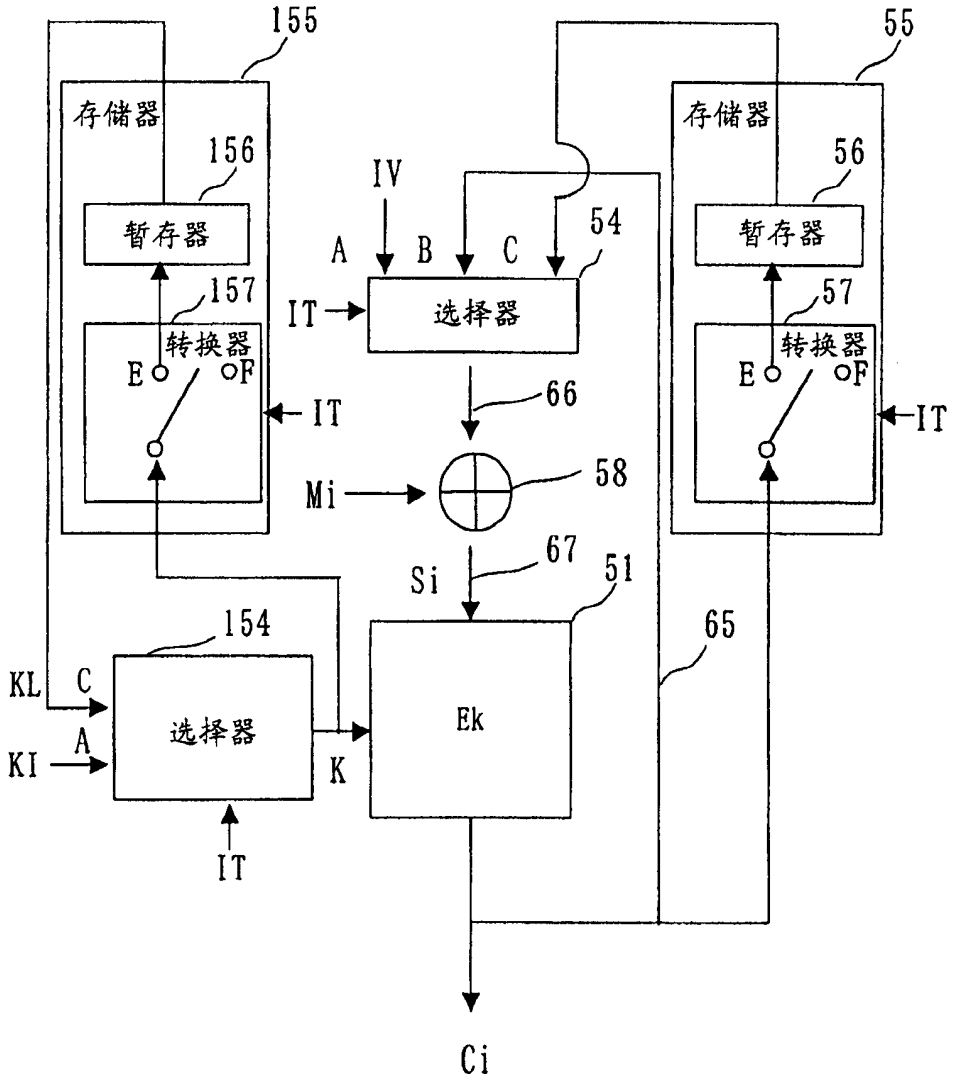

155
存储器
156
暂存器
157
转换器
E
F
IT
IV
A
B
C
54
IT
选择器
66
Mi
58
Si
67
51
Ek
65
55
存储器
56
暂存器
57
转换器
E
F
IT
154
KL
C
KI
A
选择器
K
IT
Ci

图 26

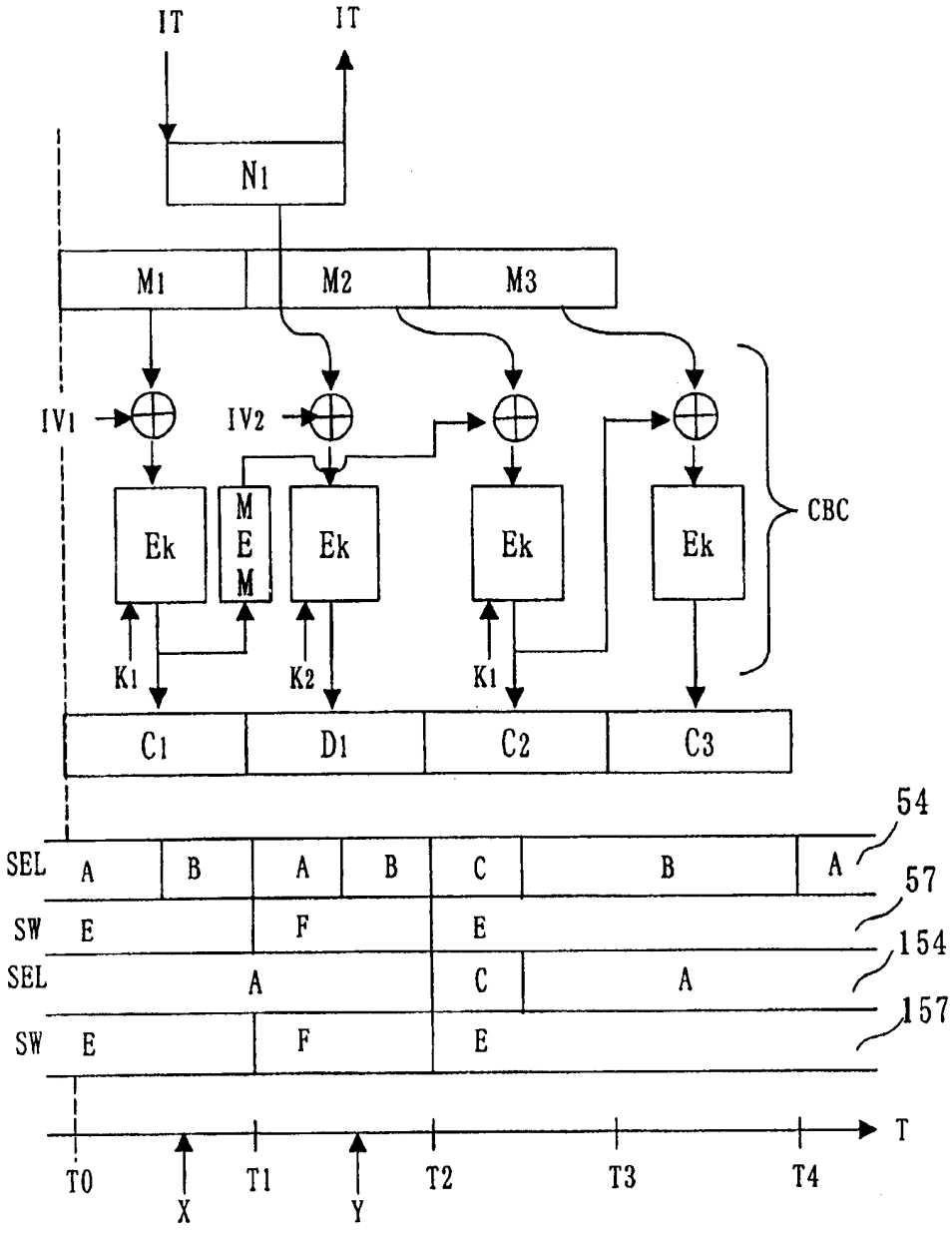

IT
IT
N1
M1
M2
M3
IV1
IV2
Ek
MEM
Ek
Ek
Ek
CBC
K1
K2
K1
C1
D1
C2
C3
54
SEL
A
B
A
B
C
B
A
57
SW
E
F
E
154
SEL
A
C
A
157
SW
E
F
E
T
T0
X
T1
Y
T2
T3
T4

图 27

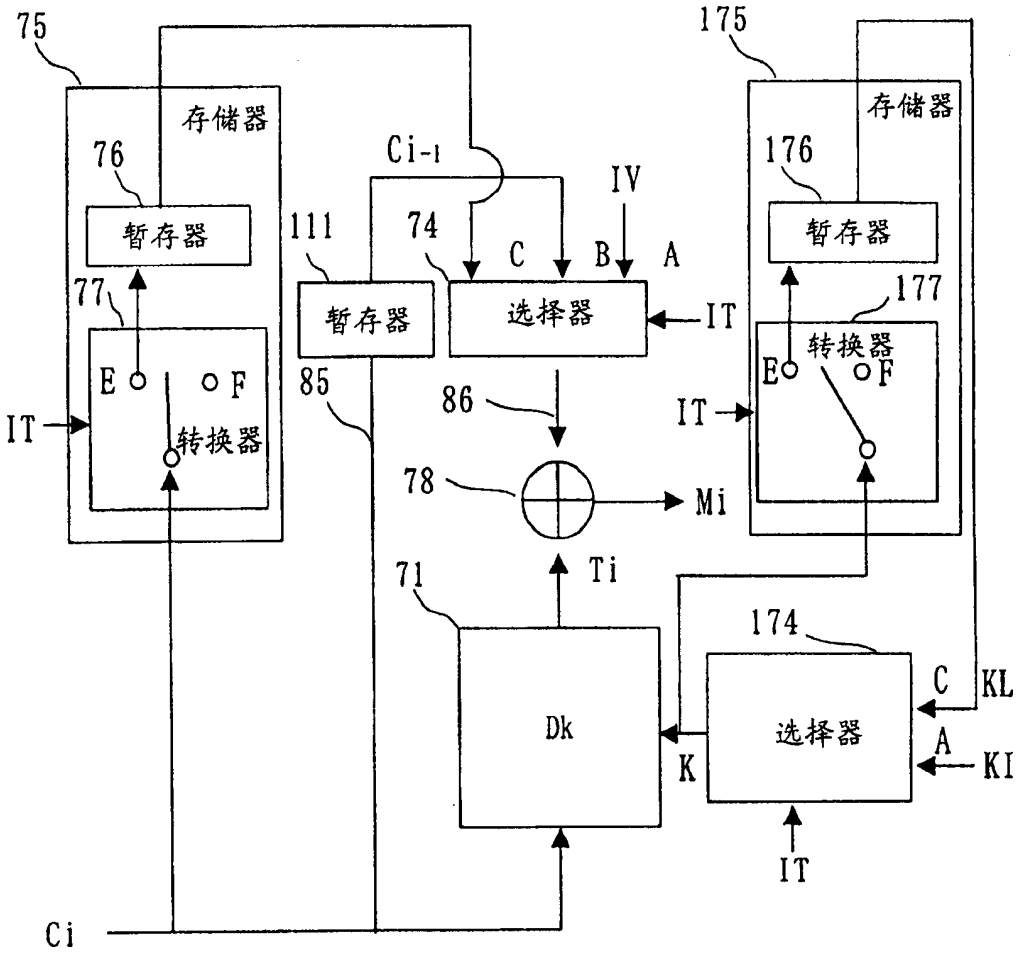

75
存储器
76
暂存器
77
E
F
转换器
IT
Ci-1
111
暂存器
74
C
B
A
IV
选择器
IT
85
86
78
Mi
Ti
71
Dk
K
Ci
175
存储器
176
暂存器
177
转换器
E
F
IT
174
选择器
C
KL
A
KI
IT

图 28

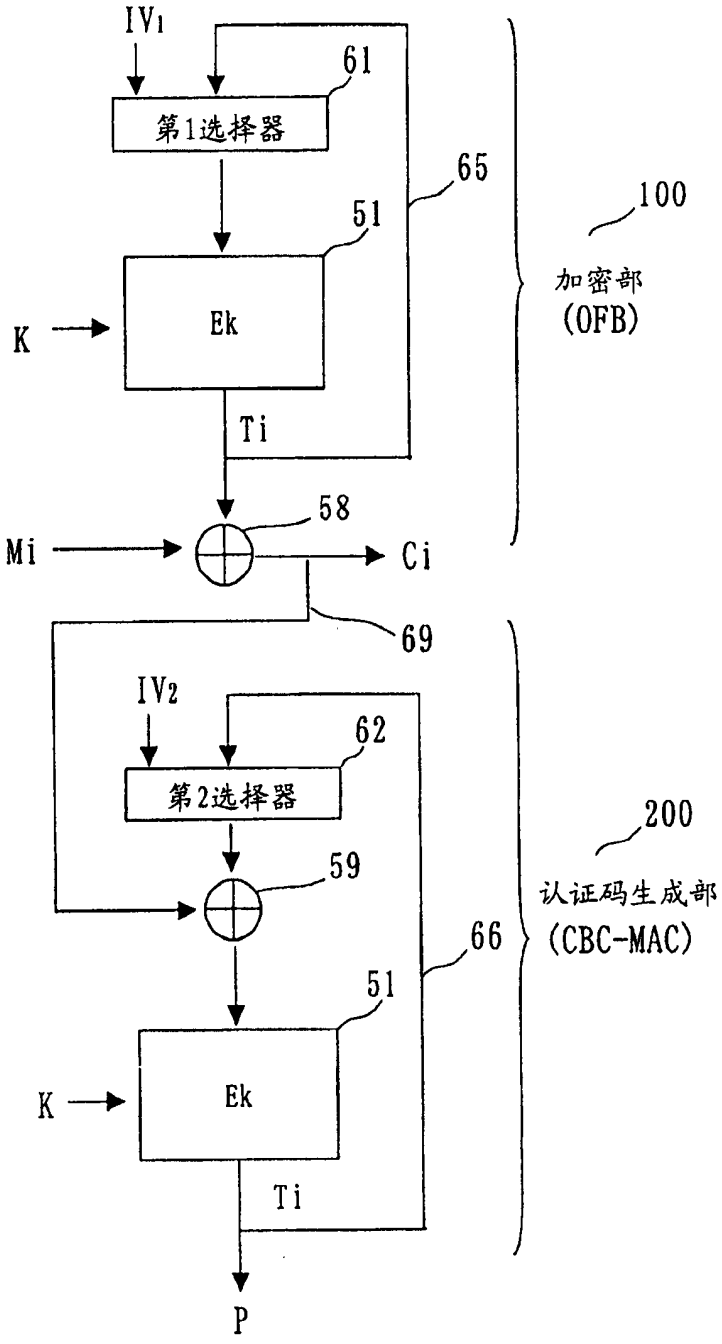

IV1
61
第1选择器
65
51
100
加密部
(OFB)
K
Ek
Ti
58
Mi
Ci
69
IV2
62
第2选择器
200
59
认证码生成部
(CBC-MAC)
66
51
K
Ek
Ti
P

图 29

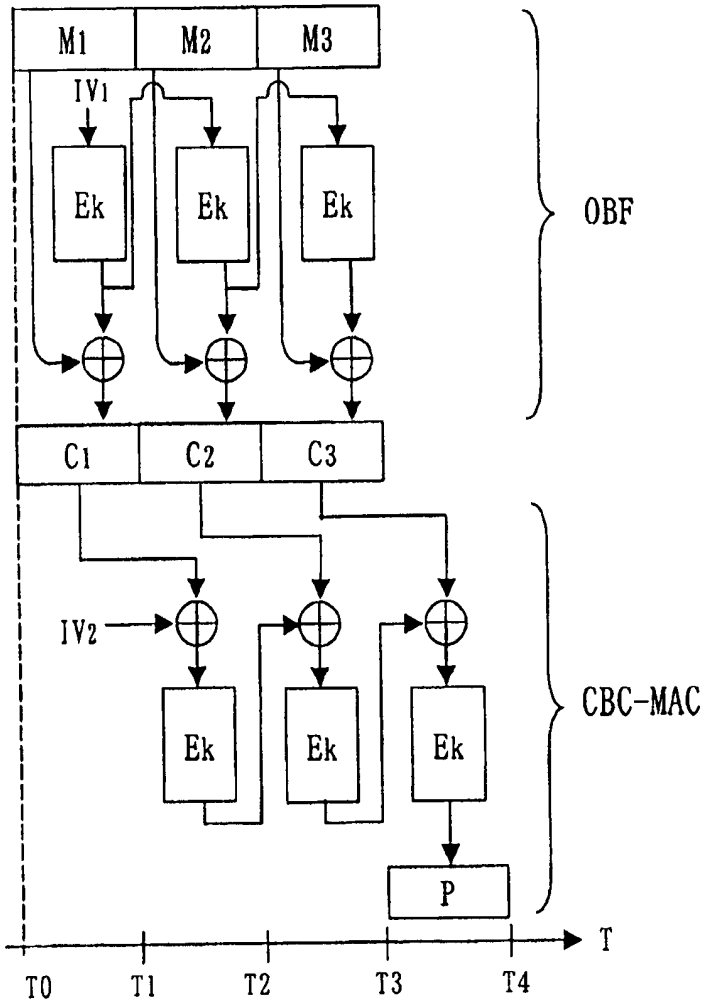

M1
M2
M3
IV1
Ek
Ek
Ek
OBF
C1
C2
C3
IV2
Ek
Ek
Ek
CBC-MAC
P
T
T0
T1
T2
T3
T4

图 30

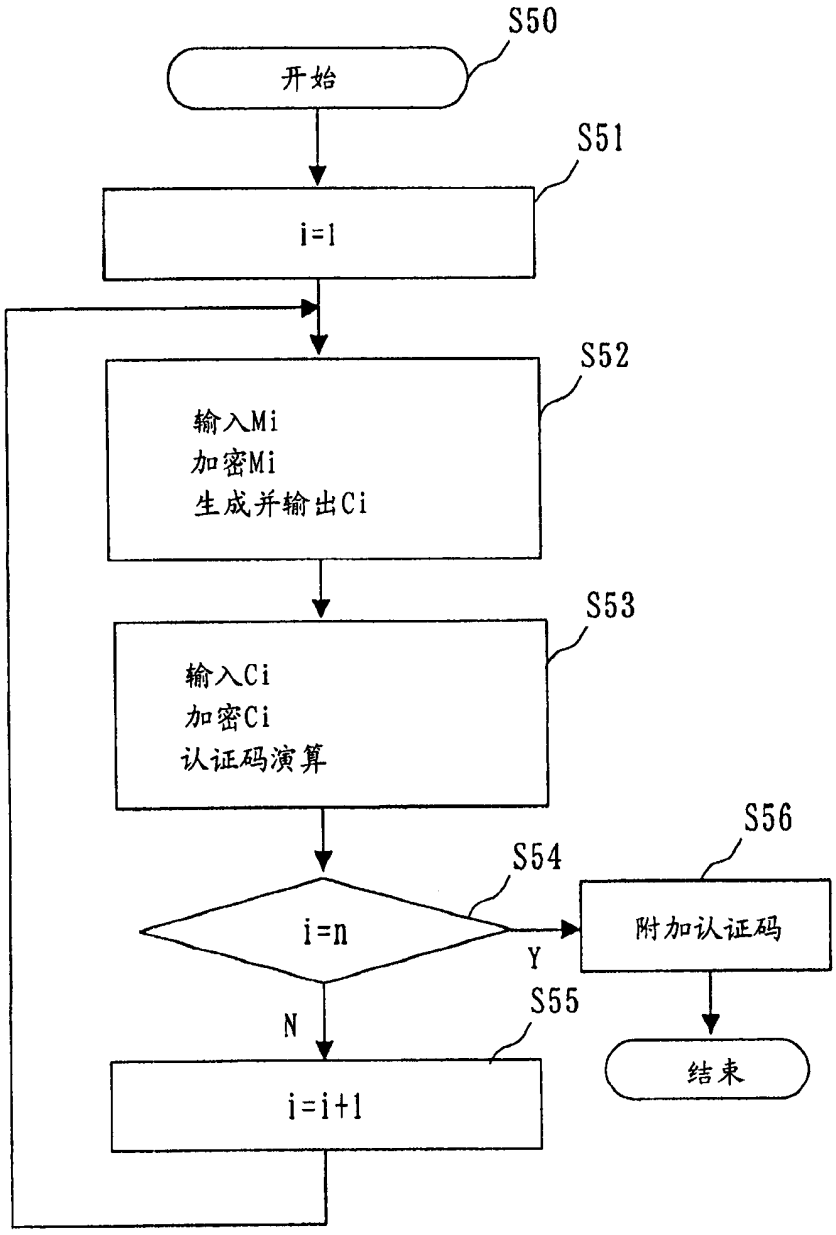

S50
开始
S51
i=1
S52
输入Mi
加密Mi
生成并输出Ci
S53
输入Ci
加密Ci
认证码演算
S54
i=n
Y
N
S55
i=i+1
S56
附加认证码
结束

图 31

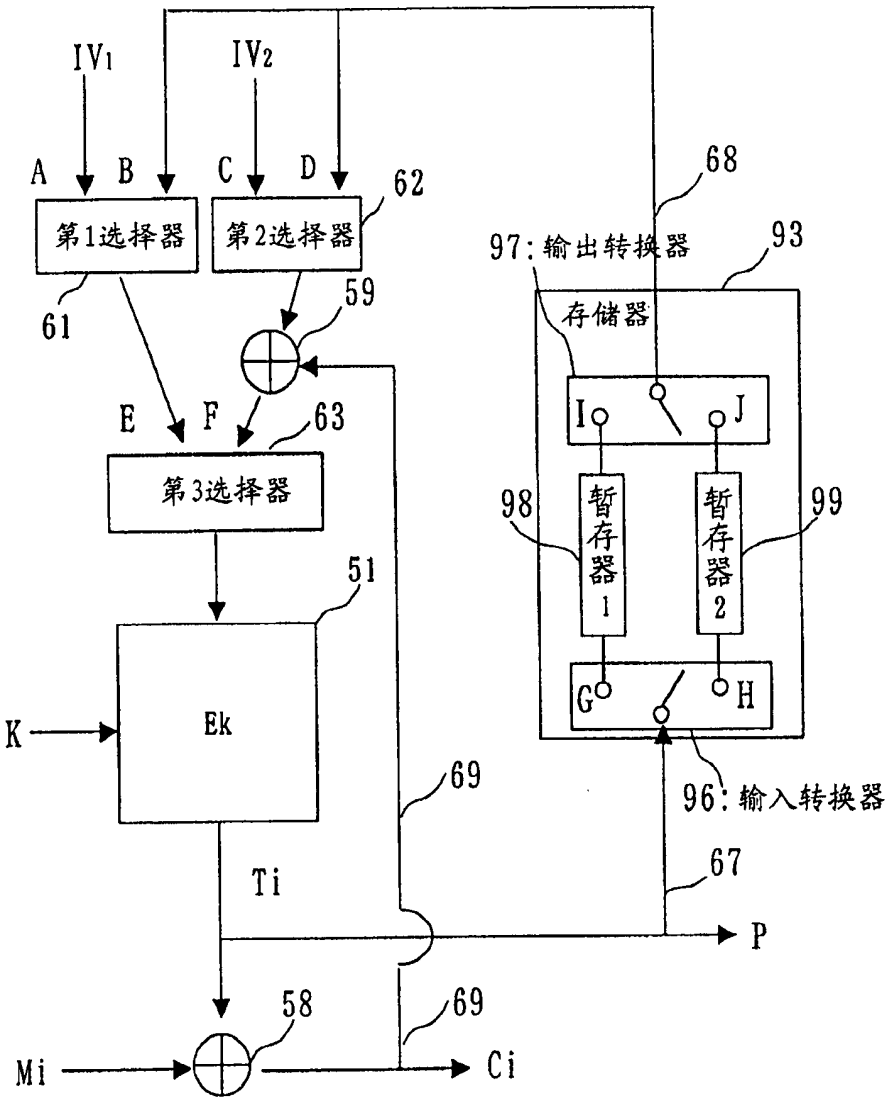

IV1
IV2
A
B
C
D
第1选择器
第2选择器
62
61
59
E
F
63
第3选择器
51
Ek
K
Ti
69
58
Mi
Ci
P
68
97:输出转换器
93
存储器
I
J
98
暂存器1
暂存器2
99
G
H
96:输入转换器
67

图 32

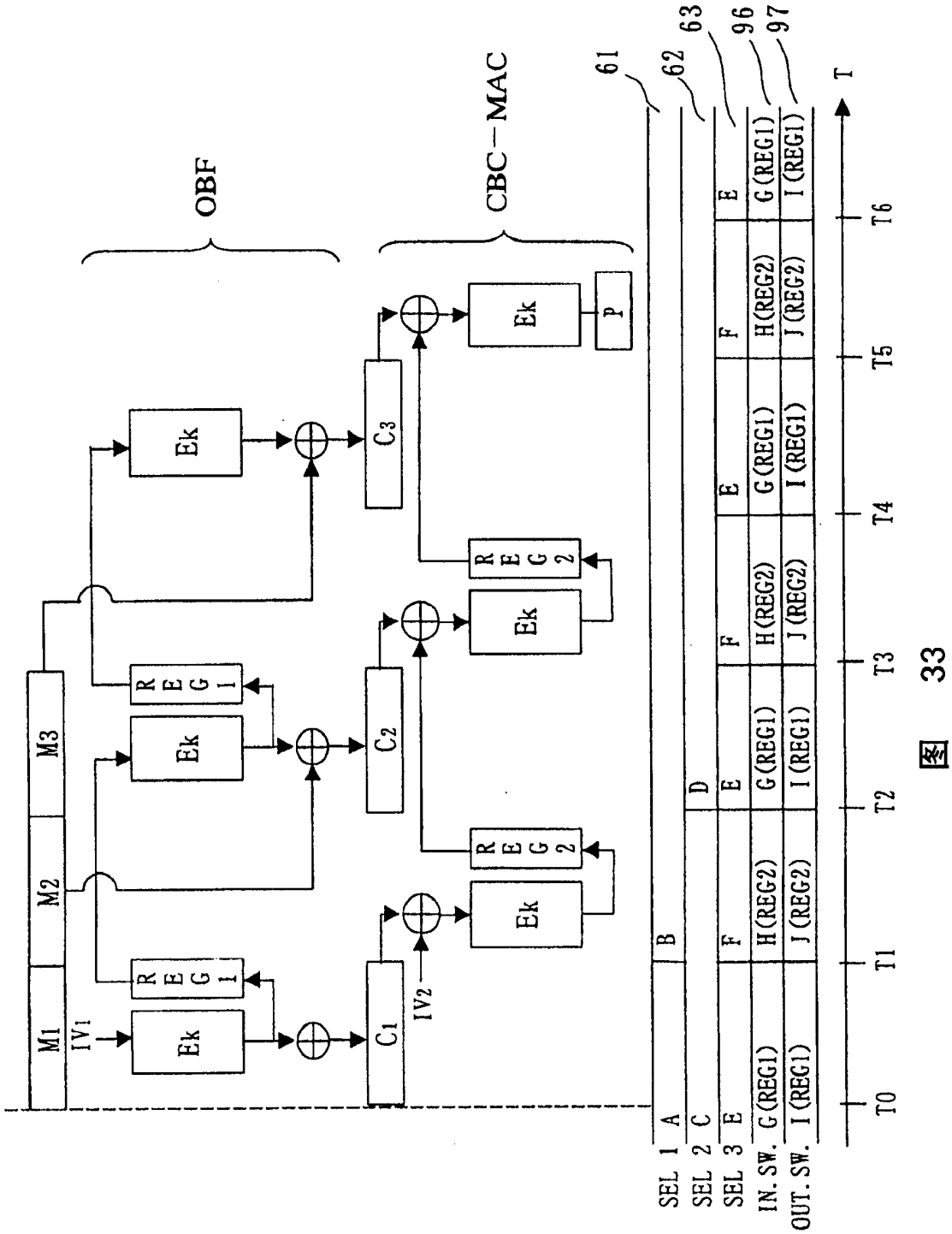

OBF
CBC－MAC
M1
M2
M3
IV1
IV2
Ek
REG1
REG2
C1
C2
C3
P
61
62
63
96
97
SEL 1 A B
SEL 2 C D
SEL 3 E F E F E
IN.SW. G(REG1) H(REG2) G(REG1) H(REG2) G(REG1)
OUT.SW. I(REG1) J(REG2) I(REG1) J(REG2) I(REG1)
T0 T1 T2 T3 T4 T5 T6 T

图 33

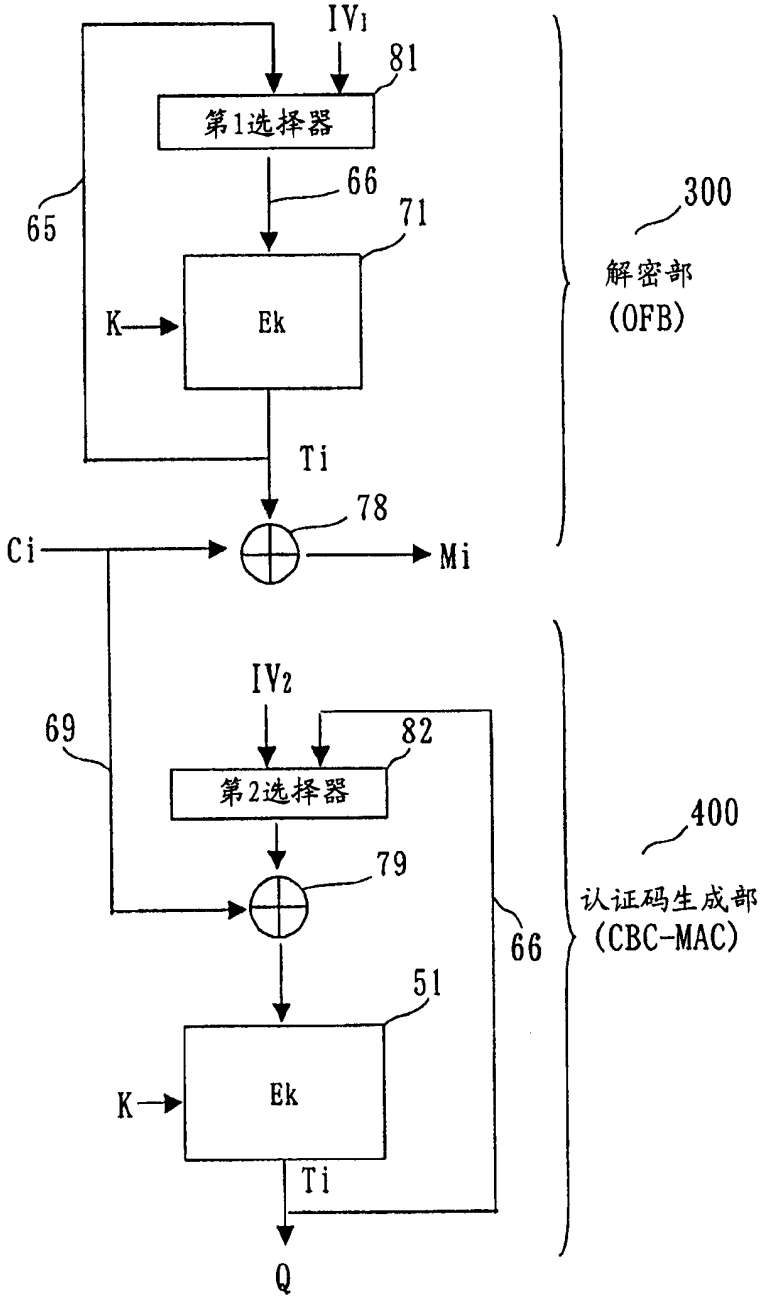

IV1
81
第1选择器
66
65
71
300
K
Ek
解密部
(OFB)
Ti
78
Ci
Mi
IV2
69
82
第2选择器
400
79
66
认证码生成部
(CBC-MAC)
51
K
Ek
Ti
Q

图 34

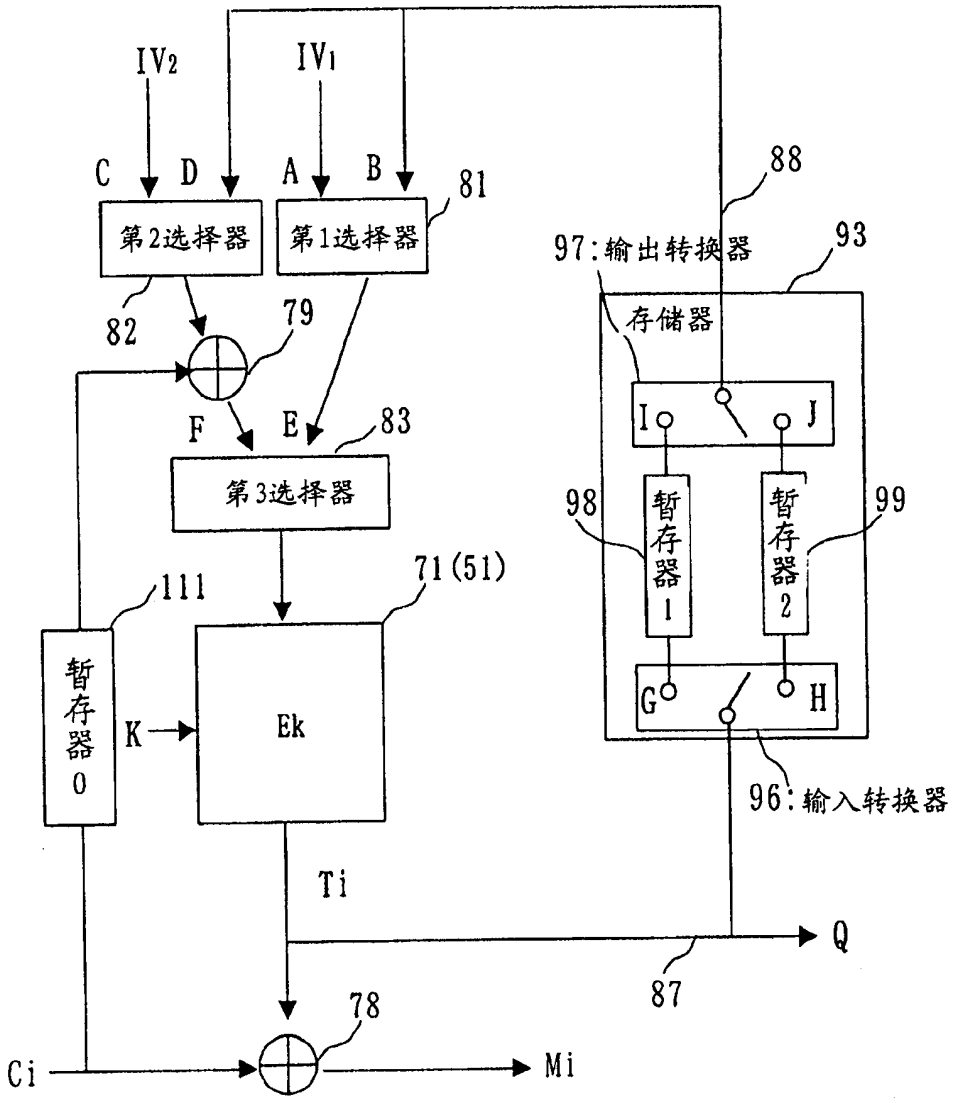

IV2
IV1
C
D
A
B
81
第2选择器
第1选择器
82
79
F
E
83
第3选择器
71(51)
111
暂存器0
K
Ek
Ti
78
Ci
Mi
88
97:输出转换器
93
存储器
I
J
98
暂存器1
暂存器2
99
G
H
96:输入转换器
Q
87

图 35

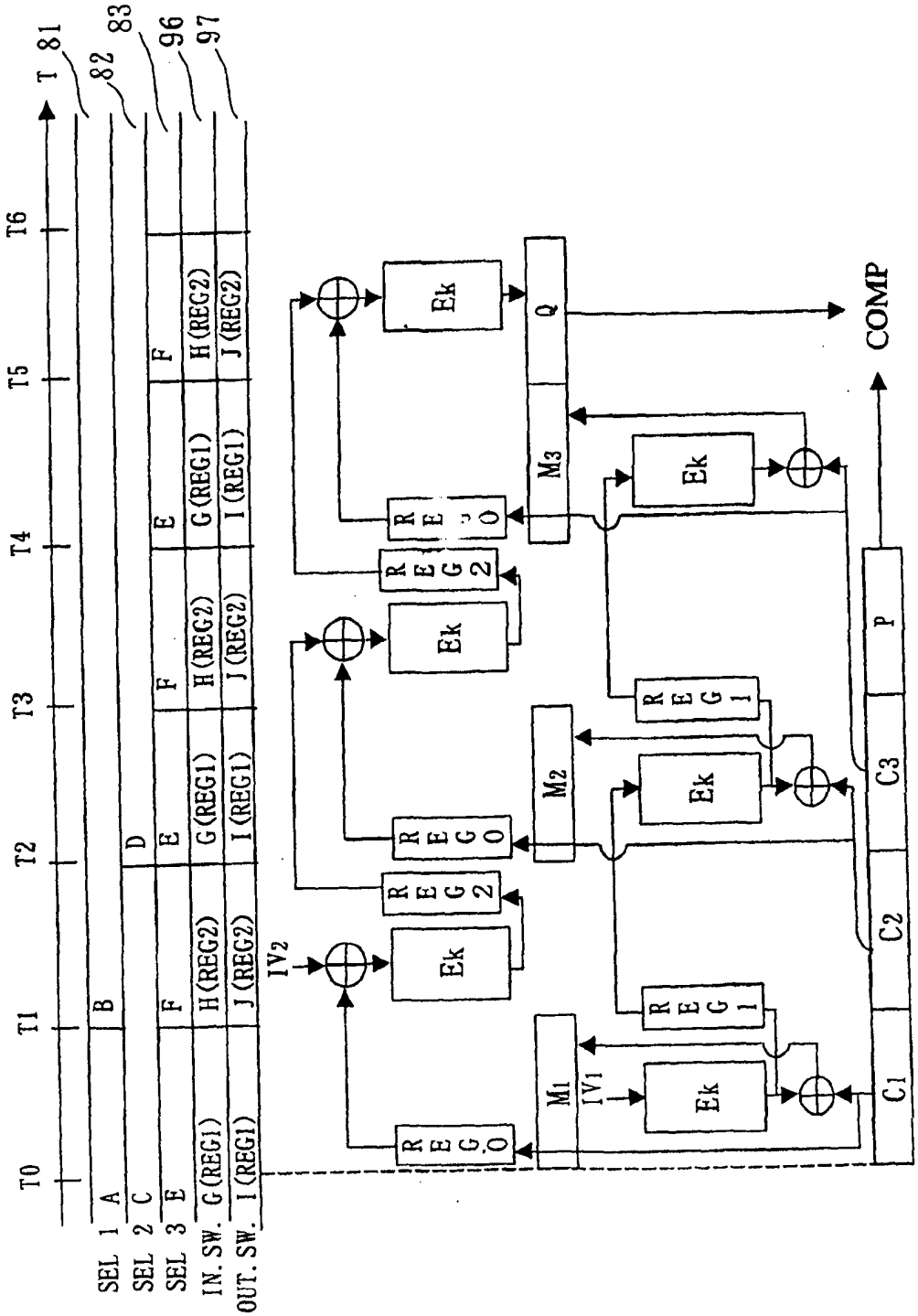

T 81
82
83
96
97
T0
T1
T2
T3
T4
T5
T6
SEL 1 A B
SEL 2 C D
SEL 3 E E F F E F
IN. SW. G(REG1) H(REG2) G(REG1) H(REG2) G(REG1) H(REG2)
OUT. SW. I(REG1) J(REG2) I(REG1) J(REG2) I(REG1) J(REG2)
IV2
IV1
Ek
REG 0
REG 1
REG 2
M1
M2
M3
Q
C1
C2
C3
P
COMP

图 36

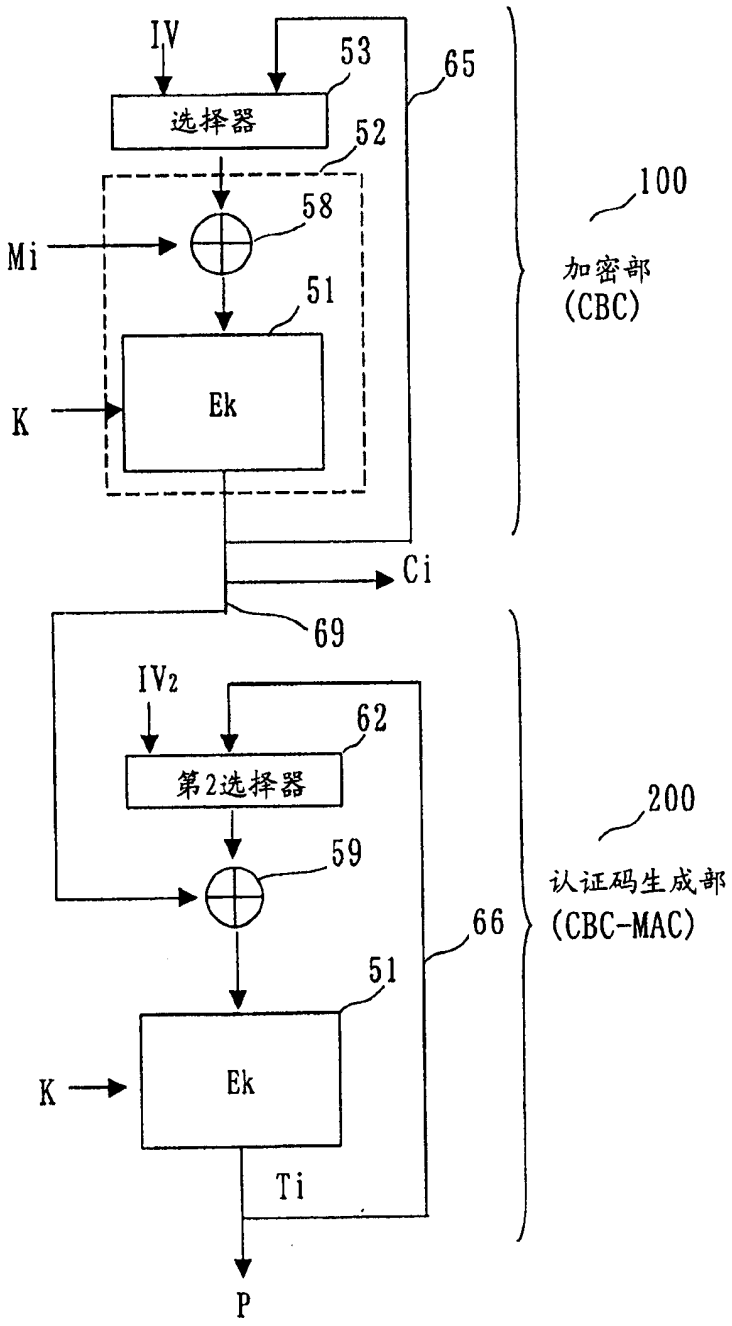

IV
53
65
选择器
52
100
58
Mi
51
加密部
(CBC)
K
Ek
Ci
69
IV2
62
第2选择器
200
59
认证码生成部
(CBC-MAC)
66
51
K
Ek
Ti
P

图 37

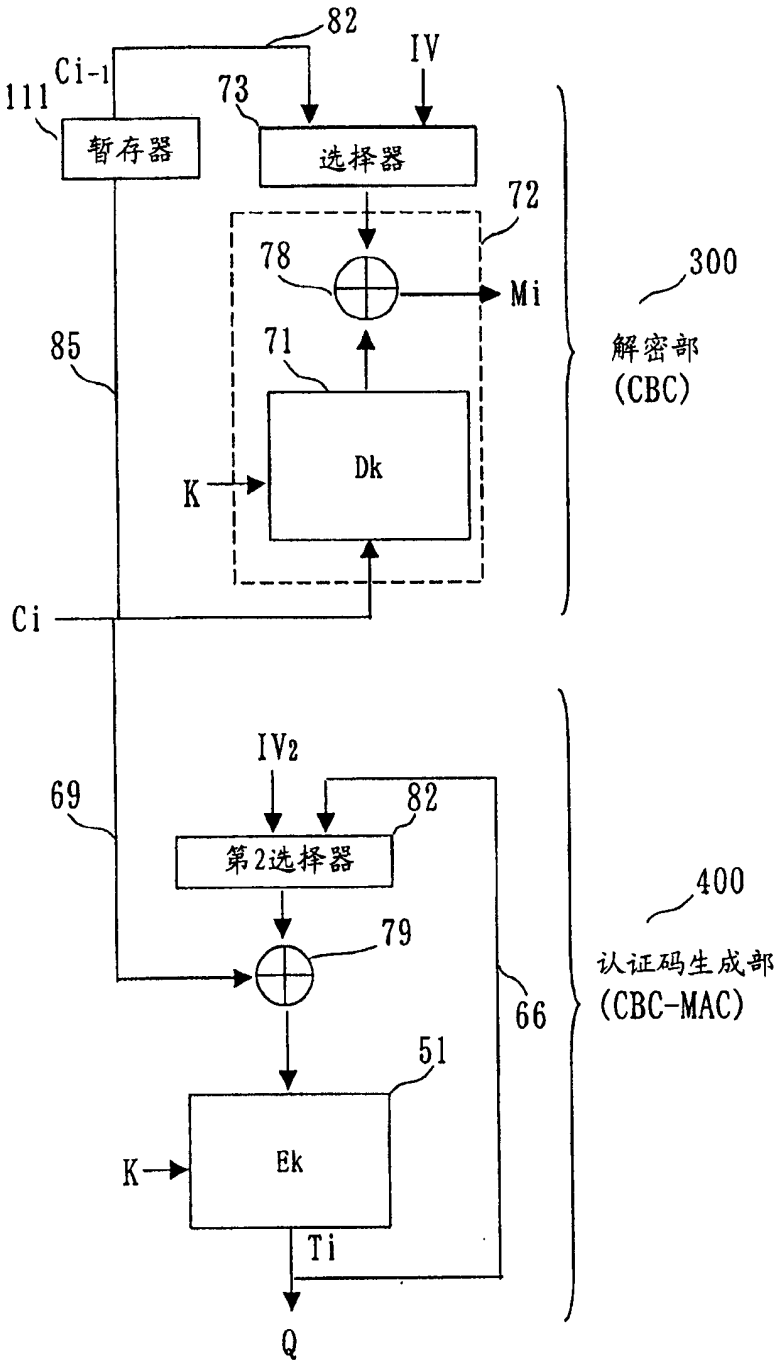

82
IV
Ci-1
111
73
暂存器
选择器
72
78
Mi
300
解密部
(CBC)
85
71
Dk
K
Ci
IV2
69
82
第2选择器
400
79
认证码生成部
(CBC-MAC)
66
51
Ek
K
Ti
Q

图 38

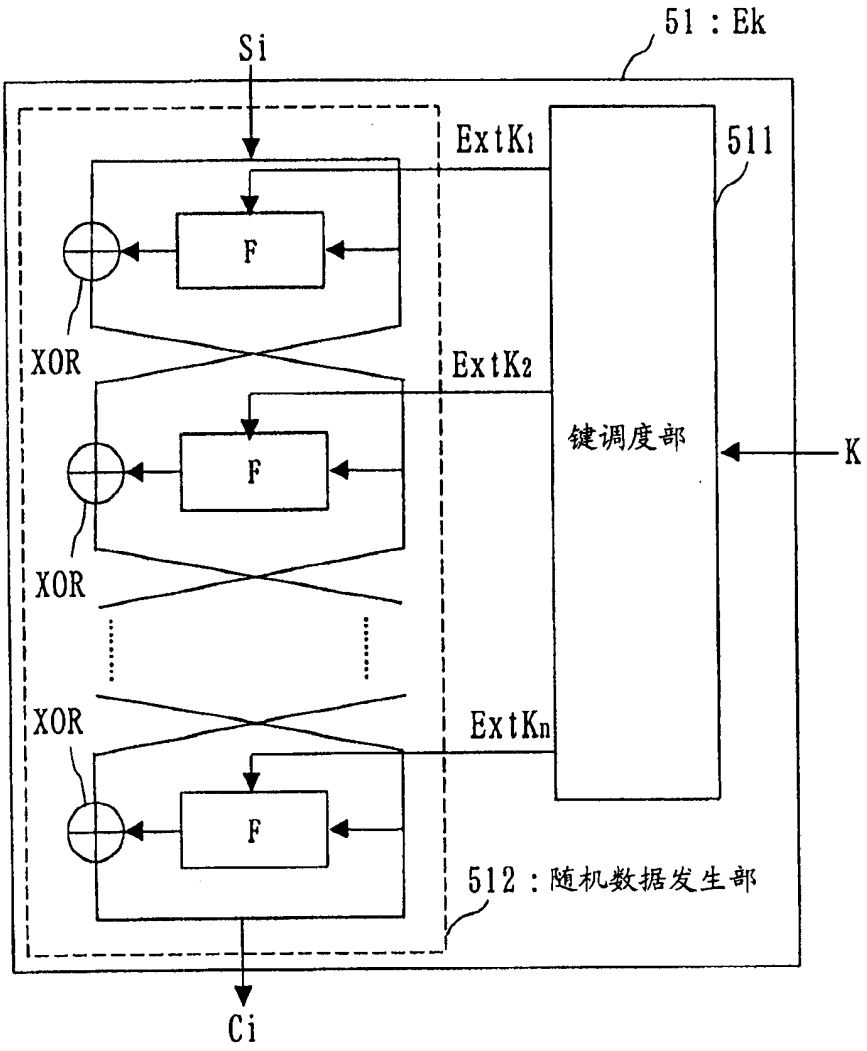

51 : Ek
Si
ExtK1
511
F
XOR
ExtK2
键调度部
K
F
XOR
XOR
ExtKn
F
512 : 随机数据发生部
Ci

图 39

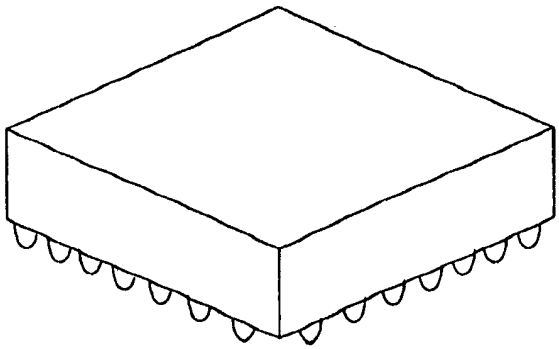


图 40

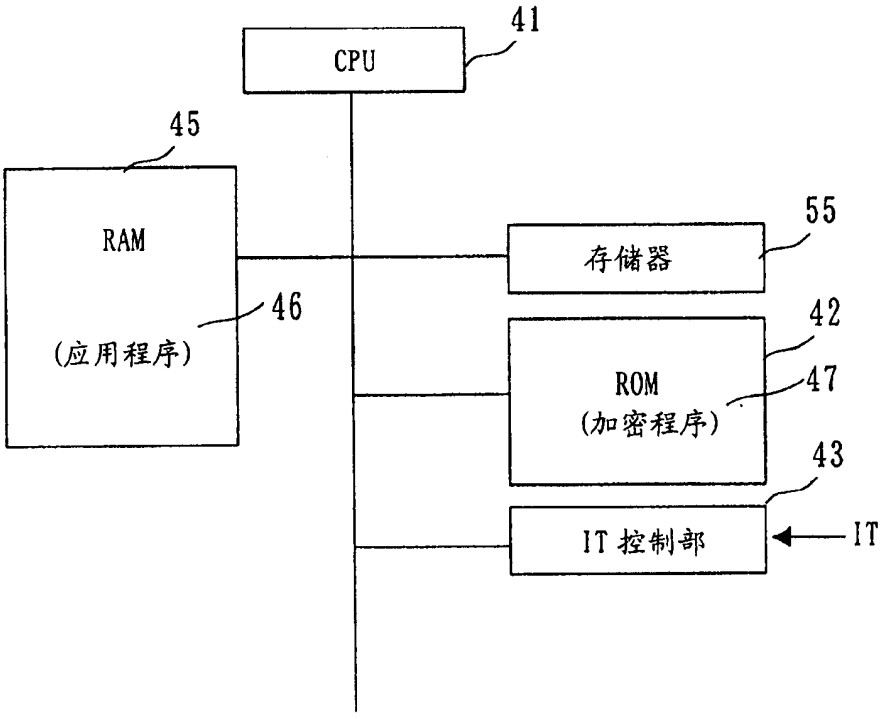


图 41

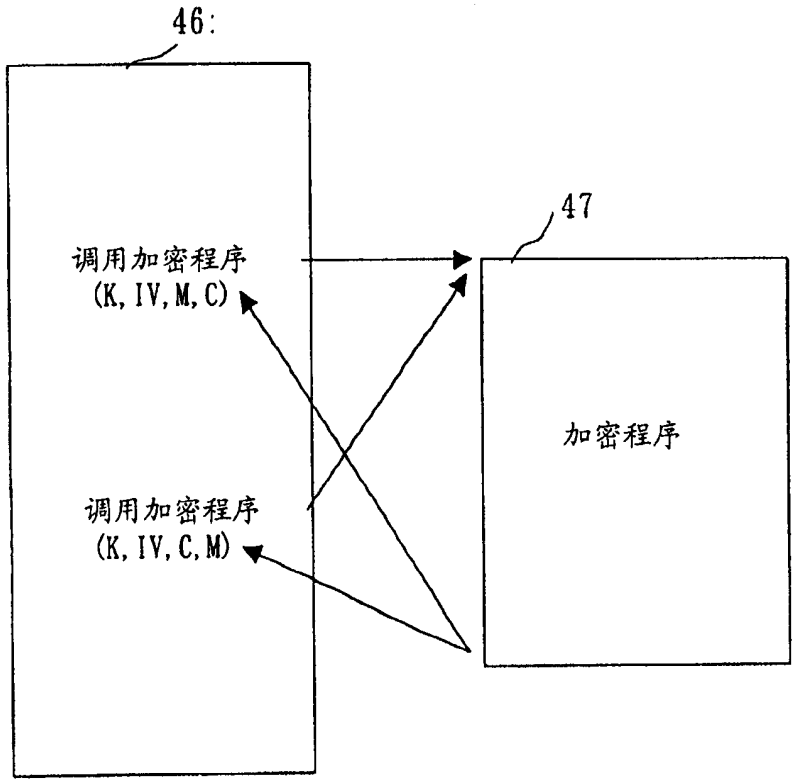


图 42

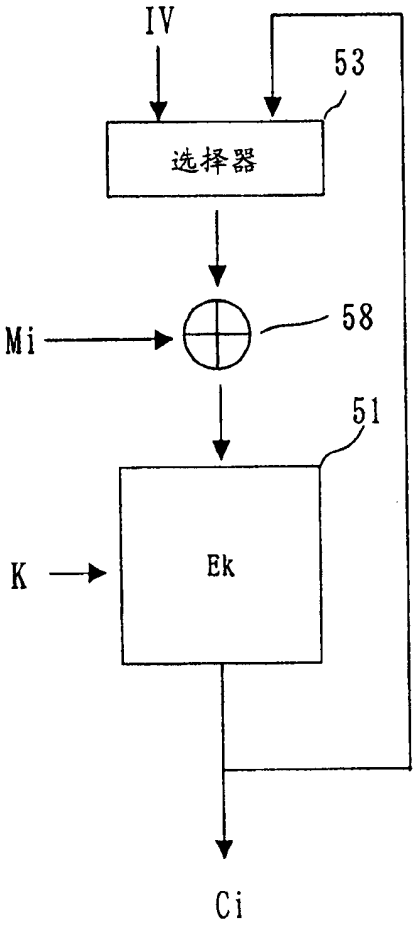


图 43

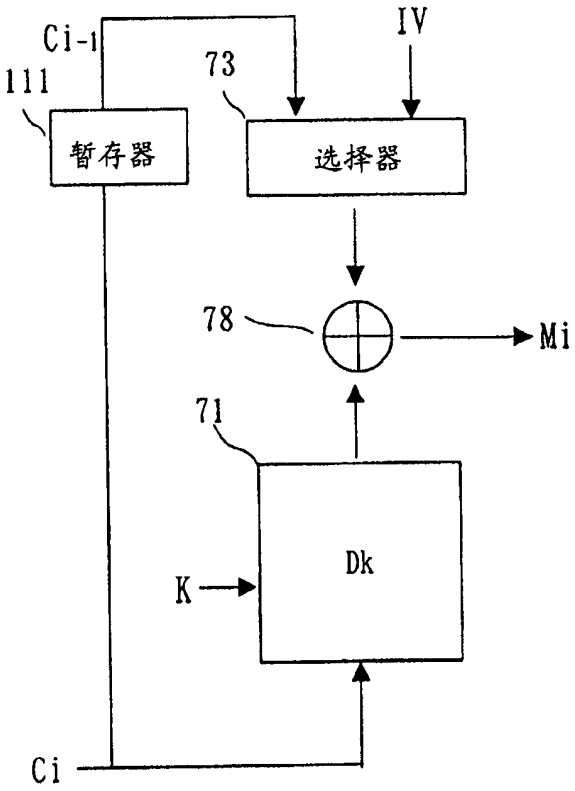


图 44

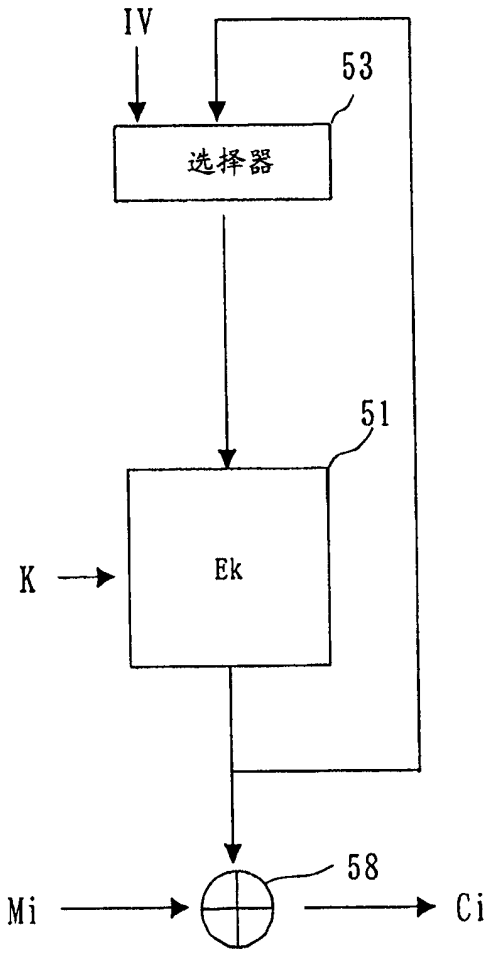


图 45

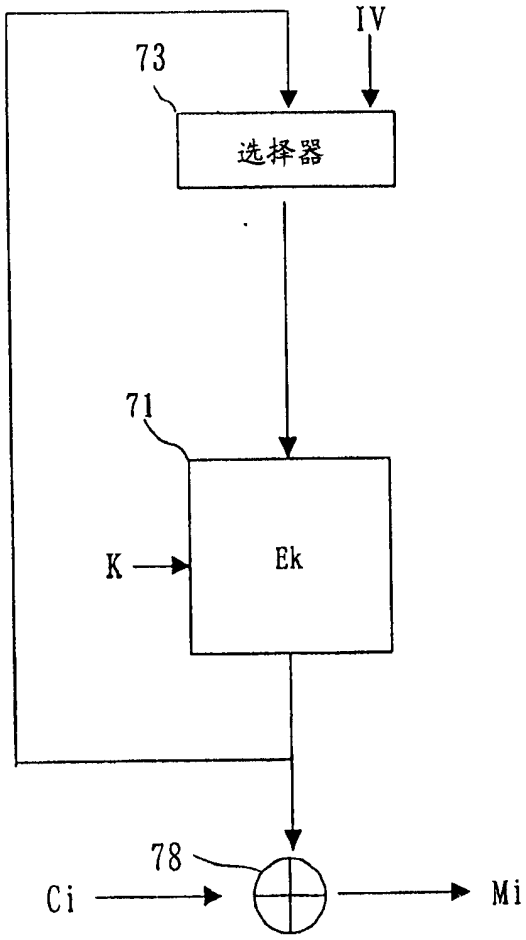


图 46

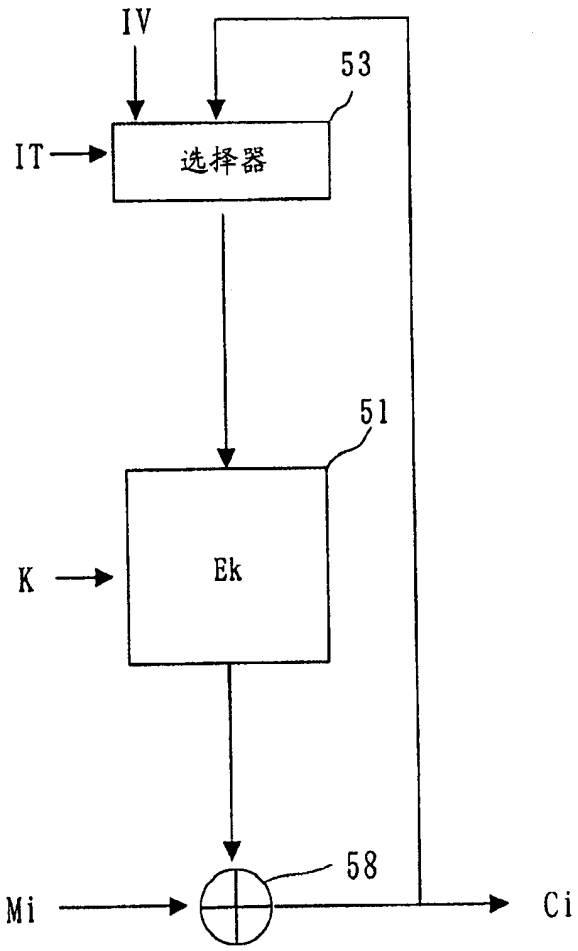


图 47

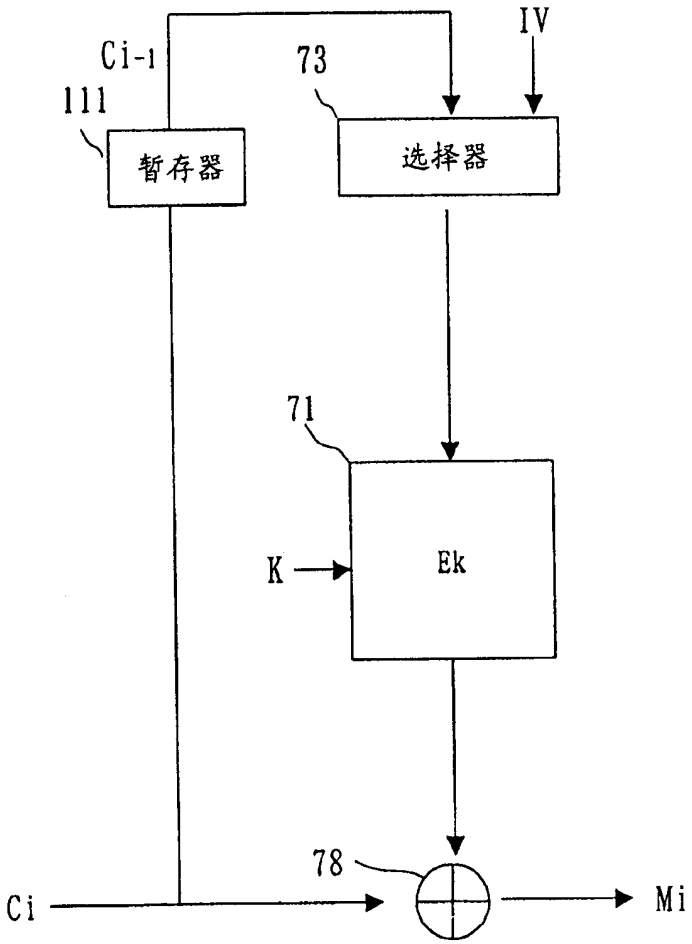


图 48

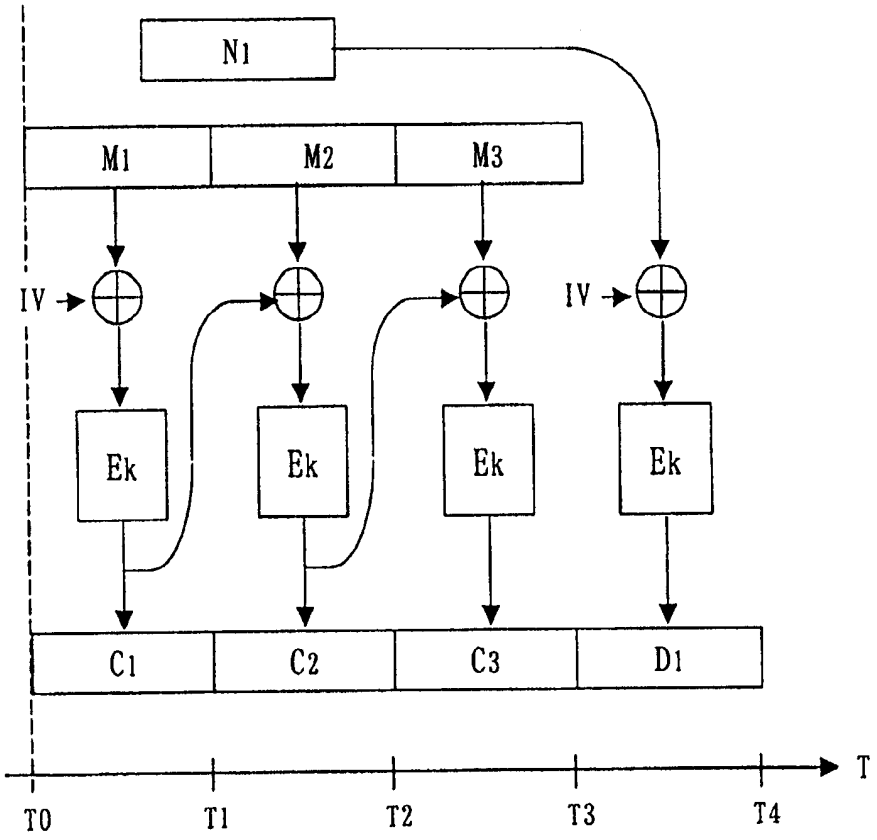


图 49

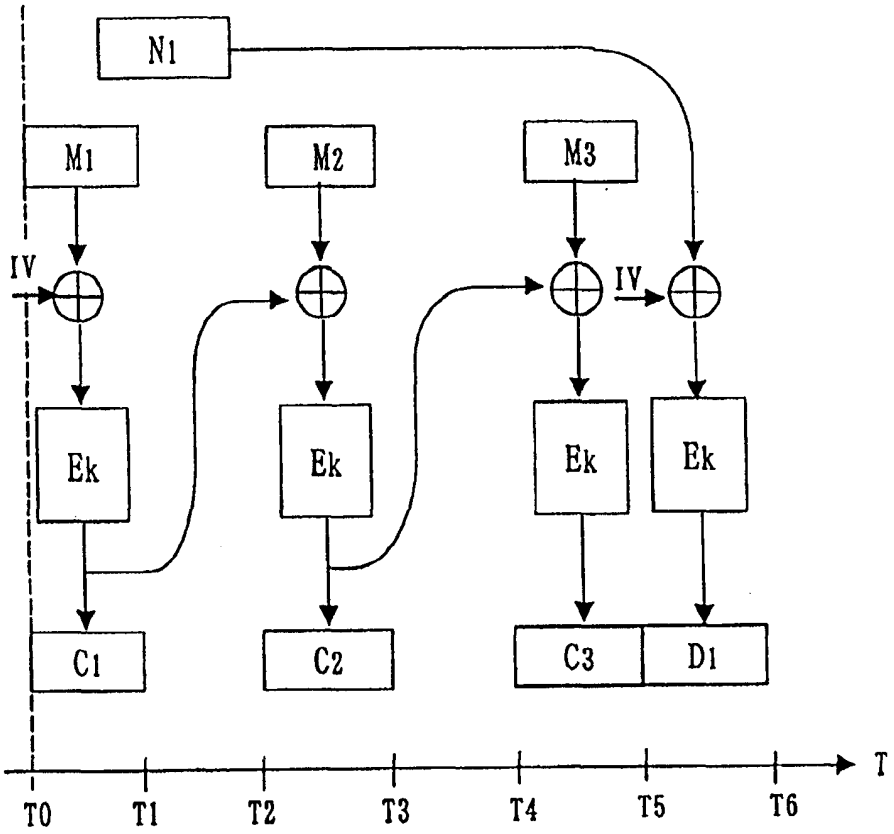


图 50

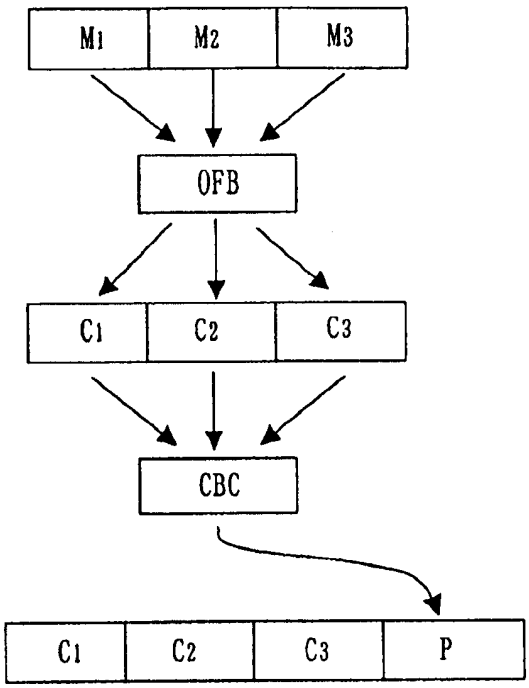


图 51

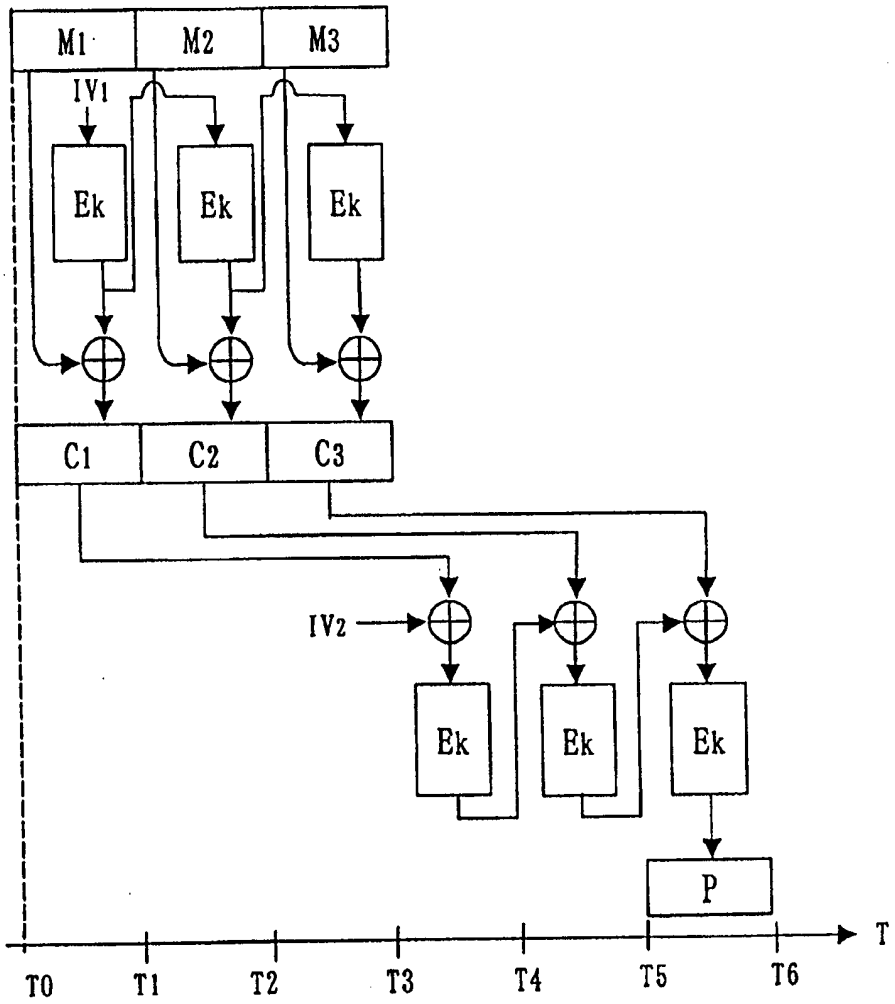


图 52