[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/32
G07F 19/00 G07F 7/10

[12] 发明专利说明书

[21] ZL 专利号 01812340.6

[45] 授权公告日 2005 年 3 月 9 日

[11] 授权公告号 CN 1192545C

[22] 申请日 2001.7.4 [21] 申请号 01812340.6
[30] 优先权
[32] 2000. 7. 5 [33] FR [31] 00/08773
[86] 国际申请 PCT/FR2001/002143 2001.7.4
[87] 国际公布 WO2002/003338 法 2002.1.10
[85] 进入国家阶段日期 2003.1.6
[71] 专利权人 瓦利迪公司
地址 法国伊泽尔省
[72] 发明人 J-C·屈埃诺 G·斯格罗
审查员 尹海霞

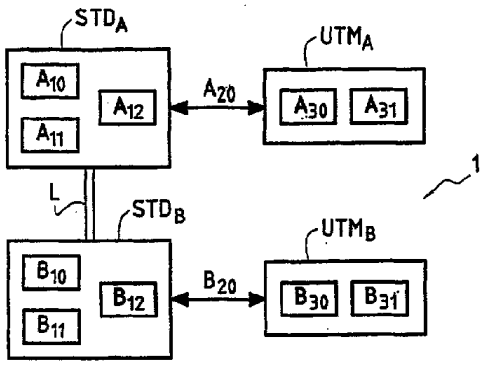
[74] 专利代理机构 北京纪凯知识产权代理有限公司
代理人 程 伟 戈 泊

权利要求书 8 页 说明书 15 页 附图 6 页

[54] 发明名称 限制变换构成尤其预付款标记的数据可能性的方法和系统

[57] 摘要

本发明涉及一种用于限制变换数据可能性的方法和系统，所述变换 Tx 数据为 Ty 数据是以 A 型变换功能产生的，同时变换 Ty 数据为 Tx 数据是以与 A 型变换功能反相的 B 型变换功能产生的，该数据尤其是被用于构成例如预付款标记。本发明其特征在于：该系统包括至少一个 A 型处理系统(STD_A)，至少一个 B 型数据处理系统(STD_B)，至少一个，至少曾经在该系统(STD_A)和该系统(STD_B)之间的链路，至少一个至少包括 A 型变换功能的 A 型处理和存储单元(UTM_A)，至少一个包括 B 型变换功能而不包括 A 型变换功能的 B 型处理和存储单元(UTM_B)。



ISSN1008-4274

1. 一种经由至少一个处理和存储单元限制变换Tx型数据为Ty型数据的可能性和变换Ty型数据为Tx型数据的可能性的方法，Tx型数据变换为Ty型数据被使用A型变换功能(F_A)执行，同时Ty型数据变换为Tx型数据被使用B型变换功能(F_B)执行，该B型变换功能与A型变换功能是反相的，上述各型数据尤其被用于构成例如，预付款标记， 以及被在至少一个数据处理系统上执行，所述方法包括：

使用一个A型数据处理系统(STD_A)和一个B型数据处理系统(STD_B)，

至少一次，建立至少一个在A型数据处理系统(STD_A)和B型数据处理系统(STD_B)之间的链路(L)，以便将至少Ty型数据从A型数据处理系统(STD_A)传送到B型数据处理系统(STD_B)，和/或将至少Tx型数据从B型数据处理系统(STD_B)传送到A型数据处理系统(STD_A)，

在A型定制阶段期间，产生至少一个包括至少A型变换功能(F_A)的A型处理和存储单元(UTM_A)，

在A型变换阶段期间：

对于一个拥有至少一个A型处理和存储单元(UTM_A)的用户，能够：

从A型数据处理系统(STD_A)传送至少一块Tx型数据给A型处理和存储单元(UTM_A)，

在A型处理和存储单元(UTM_A)中使用A型变换功能(F_A)变换每块Tx型数据为一块Ty型数据，

从A型处理和存储单元(UTM_A)传送每块Ty型数据给A型数据处理系统(STD_A)，

对于不拥有任何A型处理和存储单元(UTM_A)的用户，不能使用A型变换功能(F_A)变换Tx型数据块为Ty型数据块，

在B型定制阶段期间，产生至少一个包括B型变换功能(F_B)而不包括A型变换功能(F_A)的B型处理和存储单元(UTM_B)，

以及在B型变换阶段期间：

对于拥有B型处理和存储单元(UTM_B)而不拥有A型处理和存储单元(UTM_A)的用户，

能够：

从B型数据处理系统(STD_B)传送至少一块Ty型数据给B型处理和存储单元(UTM_B)，

在B型处理和存储单元(UTM_B)中使用B型变换功能(F_B)变换每块Ty型数据为一块Tx型数据，

从B型处理和存储单元(UTM_B)传送每块Tx型数据给B型数据处理系统(STD_B)，

不能使用A型变换功能(F_A)变换一块Tx型数据为一块Ty型数据。

2. 根据权利要求1的方法，包括： 在A型定制阶段期间，产生一个还包括与A型变换功能(F_A)反相的B型变换功能(F_B)的A型处理和存储单元(UTM_A)。

3. 根据权利要求1的方法，包括：

在A型处理和存储单元(UTM_A)中作为A型变换功能(F_A)，分别：

使用密钥加密功能(CS)，以及用作密钥加密功能(CS)的密钥的Kcs型秘密信息单元(Ics)，

或使用公共密匙加密功能(CPU)，以及用作公共密匙加密功能(CPU)的密钥的Kcpu型秘密信息单元(Icpu)，

或使用专用密匙加密功能(CPR)，以及用作专用密匙加密功能(CPR)的密钥的Kcpr型秘密信息单元(Icpr)；

以及在B型处理和存储单元(UTM_B)中作为B型变换功能(F_B)，分别：

使用与密钥加密功能(CS)反相的密钥反相加密功能(CSI)，以及用作密钥反相加密功能(CSI)的密钥的Kcsi型秘密信息单元(Icsi)，

或使用与公共密匙加密功能(CPU)反相的专用密钥解密功能(CPUI)，以及用作专用密钥解密功能(CPUI)的密钥的Kcpui型秘密信息单元(Icpui)，

或使用与专用密匙加密功能(CPR)反相的公用密钥解密功能(CPRI)，以及用作公用密钥解密功能(CPRI)的密钥的Kcpri型秘密信息

单元(Icpri)。

4. 根据权利要求2的方法，包括：

在A型处理和存储单元(UTM_A)中作为A型变换功能(F_A)，分别：

使用密钥加密功能(CS)，以及用作密钥加密功能(CS)的密钥的Kcs型秘密信息单元(Ics)，

或使用公共密匙加密功能(CPU)，以及用作公共密匙加密功能(CPU)的密钥的Kcpu型秘密信息单元(Icpu)，

或使用专用密匙加密功能(CPR)，以及用作专用密匙加密功能(CPR)的密钥的Kcpr型秘密信息单元(Icpr)；

以及在B型处理和存储(UTM_B)中作为B型变换功能(F_B)，分别：

使用与密钥加密功能(CS)反相的密钥反相加密功能(CSI)，以及用作密钥反相加密功能(CSI)的密钥的Kcsi型秘密信息单元(Icsi)，

或使用与公共密匙加密功能(CPU)反相的专用密钥解密功能(CPUI)，以及用作专用密钥解密功能(CPUI)的密钥的Kcpui型秘密信息单元(Icpui)，

或使用与专用密匙加密功能(CPR)反相的公用密钥解密功能(CPRI)，以及用作公用密钥解密功能(CPRI)的密钥的Kcpri型秘密信息单元(Icpri)。

5. 根据权利要求3的方法，包括：

作为A型变换功能(F_A)，与密钥加密功能(CS)相结合，与公共密匙加密功能(CPU)相结合，或者与专用密钥加密功能(CPR)相结合使用一个附加变换功能(Fad),

以及作为B型变换功能(F_B)，与密钥反相的加密功能(CSI)相结合，与专用密匙解密功能(CPUI)相结合，或者与公用密钥解密功能(CPRI)相结合使用一个附加反相的变换功能(Fadi)。

6. 根据权利要求4的方法，包括：

作为A型变换功能(F_A)，与密钥加密功能(CS)相结合，与公共密匙加密功能(CPU)相结合，或者与专用密钥加密功能(CPR)相结合使用一

个附加变换功能(Fad),

以及作为B型变换功能(F_B)，与密钥反相的加密功能(CSI)相结合，与专用密匙解密功能(CPUI)相结合，或者与公用密钥解密功能(CPRI)相结合使用一个附加反相的变换功能(Fadi)。

7. 根据权利要求1、2、3或4的方法，包括：

作为A型处理和存储单元(UTM_A)和/或B型处理和存储单元(UTM_B)使用处理和存储单元(UTM)，该处理和存储单元(UTM)包括每个为执行A型变换功能(F_A)和B型变换功能(F_B)所必需的算法装置(110，120)，

禁止：

在B型定制阶段期间，在每个B型处理和存储单元(UTM_B)中，执行A型变换功能(F_A)的可能性，

或者，在A型定制阶段期间，在每个A型处理和存储单元(UTM_A)中，执行B型变换功能(F_B)的可能性。

8. 根据权利要求3的方法，包括： 产生一个主要的秘密信息(SP)，从中确定一对Kcs型(Ics)和Kcsi型(Icsi)，或者Kcpu型(Icpu)和Kcpui型(Icpui)，或者Kcpr型(I_{CPR})和Kcpri型(I_{CPRI})的秘密信息单元。

9. 根据权利要求5的方法，包括： 产生一个主要的秘密信息(SP)，从中确定一对Kcs型(Ics)和Kcsi型(Icsi)，或者Kcpu型(Icpu)和Kcpui型(Icpui)，或者Kcpr型(I_{CPR})和Kcpri型(I_{CPRI})的秘密信息单元，以及用于附加变换功能(Fad)的参数(Pad)，和用于附加的反变换功能(Fadi)的参数(Padi)。

10. 根据权利要求6的方法，包括： 产生一个主要的秘密信息(SP)，从中确定一对Kcs型(Ics)和Kcsi型(Icsi)，或者Kcpu型(Icpu)和Kcpui型(Icpui)，或者Kcpr型(I_{CPR})和Kcpri型(I_{CPRI})的秘密信息单元，以及用于附加变换功能(Fad)的参数(Pad)，和用于附加的反变换功能(Fadi)的参数(Padi)。

11. 根据权利要求8、9或10的方法，包括： 使用一种方法共用秘

密信息（S1、S2、...、Sn)去产生该主要的秘密信息(SP)。

12. 根据权利要求8、9或者10的方法，包括：

使用该主要的秘密信息(SP)去产生一对Kcs型(Ics)和Kcsi型(Icsi)，或者Kcpu型(Icpu)和Kcpui型(icpui)，或者Kcpr型(I_{CPR})和Kcpri型(I_{CPRI})秘密信息单元的至少一个单元，或者用于附加变换功能(Fad)的参数(Pad)，和用于附加的反变换功能(Fadi)的参数(Padi)，

在A型定制阶段期间，通过将以下传送给处理和存储单元(UTM_A)而定制每个处理和存储单元(UTM_A)：

该Kcs型秘密信息单元(Ics)或者该Kcpu型秘密信息单元(Icpu)或者该KcpR型秘密信息单元(I_{CPR})，或者用于附加变换功能(Fad)的参数(Pad)去使其执行A型变换功能(Fa)，

或者该Kcsi型秘密信息单元(Icsi)或者该Kcpui型秘密信息单元(Icpui)或者该Kcpri型秘密信息单元(I_{CPRI})，或者用于附加的反变换功能(Fadi)的参数(Padi)去使处理和存储单元(UTM_A)执行B型变换功能(F_B)，

在B型定制阶段期间，通过将以下传送给B型处理和存储单元(UTM_B)而定制每个B型处理和存储单元(UTM_B)：该Kcsi型秘密信息单元(Icsi)或者该Kcpui型秘密信息单元(Icpui)或者该Kcpri型秘密信息单元(I_{CPRI})，或者用于附加的反变换功能(Fadi)的参数(Padi)去使B型处理和存储单元(UTM_B)执行B型变换功能(F_B)。

13. 根据权利要求1的方法，包括：

在A型变换阶段期间：

定义一个开始设置(E_d)，它的组成部分是Tx型数据块，

使用包含在A型处理和存储单元(UTM_A)中的A型变换功能(F_A)变换该开始设置(E_d)的所有的组成部分，以便获得一个目标设置(E_A)，它的组成部分是Ty型数据块，

从A型数据处理系统(STD_A)将以下内容经由链路(L)传送到B型数据处理系统(STD_B)：

信息(I)，能够表示该开始设置(E_d)，

和目标设置(E_A)的至少一个组成部分；

以及在B型变换阶段期间，对于目标设置(E_A)的至少一个组成部分，从A型数据处理系统(STD_A)将以下内容传送到B型数据处理系统(STD_B)：

使用包含在B型处理和存储单元(UTM_B)中的B型变换功能(F_B)变换目标设置(E_A)的至少一个组成部分，

并且使用能够表示该开始设置(E_d)的信息(I)，验证对应于开始设置(E_d)的一个由B型变换功能(F_B)变换的组成部分。

14. 根据权利要求13的方法，包括： 使用该目标设置(E_A)的每个组成部分去构成一个预付款标记(j)。

15. 一种限制变换Tx型数据为Ty型数据的可能性，以及变换Ty型数据为Tx型数据的可能性的系统， Tx型数据变换为Ty型数据被使用A型变换功能(F_A)执行，而Ty型数据变换为Tx型数据被使用B型变换功能(F_B)执行，该B型变换功能与A型变换功能是反相的， 该数据尤其是被用于构成例如预付款标记，所述系统特征在于包括：

至少一个A型数据处理系统(STD_A)，

至少一个B型数据处理系统(STD_B)，

至少一次，建立至少一个在A型数据处理系统(STD_A)和B型数据处理系统(STD_B)之间的链路(L)，以便将至少Ty型数据从A型数据处理系统(STD_A)传送到B型数据处理系统(STD_B)，和/或将至少Tx型数据从B型数据处理系统(STD_B)传送到A型数据处理系统(STD_A)，

至少一个包括至少A型变换功能(F_A)的A型处理和存储单元(UTM_A)，

定义至少一块用于要变换为一块Ty型数据的Tx型数据的装置，

从A型数据处理系统(STD_A)传送至少一块Tx型数据到A型处理和存储单元(UTM_A)的装置，

在A型处理和存储单元(UTM_A)中，使用A型变换功能(F_A)变换每块Tx型数据为一块Ty型数据的装置，

从A型处理和存储单元(UTM_A)传送每块Ty型数据到A型数据处理系统(STD_A)的装置，

至少一个包括B型变换功能(F_B)而不包括A型变换功能(F_A)的B型

处理和存储单元(UTM_B)，以达到不能使用A型变换功能(F_A)变换一块Tx型数据为一块Ty型数据的目的，

定义至少一块用于要变换为一块Tx型数据的Ty型数据的装置，

从B型数据处理系统(STD_B)传送至少一块Ty型数据给B型处理和存储单元(UTM_B)的装置，

在B型处理和存储单元(UTM_B)中，使用B型变换功能(F_B)变换每块Ty型数据为一块Tx型数据的装置，

以及从B型处理和存储单元(UTM_B)传送每块Tx型数据给B型数据处理系统(STD_B)的装置。

16. 根据权利要求15的系统，其特征在于： 该A型处理和存储单元(UTM_A)还包括与A型变换功能(F_A)反相的B型变换功能(F_B)。

17. 根据权利要求15或者16的系统，其特征在于：

该A型处理和存储单元(UTM_A)包括作为A型变换功能(F_A)使用的密钥加密功能(CS)，以及对于所述功能用作密钥的Kcs型秘密信息单元(Ics)，

以及该B型处理和存储单元(UTM_B)或者和该A型处理和存储单元(UTM_A)作为B型变换功能(F_B)包括：

一个与密钥加密功能(CS)反相的密钥反相加密功能(CSI)，

以及一个对于密钥反相加密功能(CSI)用作密钥的Kcsi型秘密信息单元(Icsi)。

18. 用于定制在按照权利要求15的一个系统中使用的处理和存储单元(UTM)的装置，其特征在于它包括自定义装置用于定制：

至少一个包括A型变换功能(F_A)而不包括B型变换功能(F_B)的A型处理和存储单元(UTM_A)，

和/或至少一个包括B型变换功能(F_B)而不包括A型变换功能(F_A)的B型处理和存储单元(UTM_B)。

19. 用于定制在按照权利要求16的一个系统中使用的处理和存储单元(UTM)的装置，其特征在于它包括自定义装置用于定制：

至少一个包括A型变换功能(F_A)而不包括B型变换功能(F_B)的A型处理和存储单元(UTM_A)，

和/或至少一个包括B型变换功能(F_B)而不包括A型变换功能(F_A)的B型处理和存储单元(UTM_B)。

20. 根据权利要求18或19的装置，其特征在于，它包括用于执行A型变换功能(F_A)和B型变换功能(F_B)的每个可能性的处理和存储单元(UTM)的禁止装置，该禁止装置用于禁止：

在每个B型处理和存储单元(UTM_B)中，使用A型变换功能(F_A)，

或者在每个A型处理和存储单元(UTM_A)中，使用B型变换功能(F_B)。

限制变换构成尤其预付款标记的数据可能性的方法和系统

技术领域

本发明的主题涉及适用于经由至少一个处理和存储单元，限制变换Tx型数据为Ty型数据的可能性，和限制变换Ty型数据为Tx型数据的可能性的专门的装置领域， Tx型数据变换为Ty型数据被使用A型变换功能执行，同时Ty型数据变换为Tx型数据被使用B型变换功能执行，B型变换功能与A型变换功能是反相的。

背景技术

本发明的主题在产生和使用用于构成预付款标记，诸如预缴款卡的数据的领域中发现特别的有益但是非独家的应用。

在技术状态中，对于某些应用出现需要归因于至少三个种类的个人或者用户对于数据不同的变换性能。 第一个用户种类能够使用A型变换功能变换Tx型数据为Ty型数据。 第二个用户种类能够使用A型变换功能反相的B型变换功能变换Ty型数据为Tx型数据，但是不能使用A型变换功能变换Tx型数据为Ty型数据。 第三个用户种类既不能使用A型变换功能变换Tx型数据为Ty型数据，也不能使用A型变换功能反相的B型变换功能变换Ty型数据为Tx型数据。

例如，这样需要分类现有用于构成预付款标记的数据为三个用户种类。 因此，第一个用户种类能够从已知的、相应于每个拥有资源消费信用客户的初始标识符产生防止窜改的预付款标记标识符。 第二个用户种类能够从预付款标记标识符恢复该已知的初始标识符，因此该客户以影响他的资源耗费为目的给他。 第三个用户种类既不能产生预付款标记标识符，也不能确定对应于标记标识符的该客户。

对于执行这样一个过程在先前的领域已知的方法是，使用公用的密钥、专用密钥编密码系统施加两次。 第一个用户种类具有一个公用密钥#_1和一个专用密钥#_2。 第二个用户种类具有一个公用密钥#_2和一个专用密钥#_1。

第一个用户种类能够变换Tx型数据Dx为Ty型数据dy。 为此，该

数据Dx被使用该公用密钥#_1加密以获得中间数据，该中间数据被使用该专用密钥#_2解密以形成数据Dy。

第二个用户种类能够变换Ty型数据Dy为Tx型数据Dx。 该数据Dy被使用该公用密钥#_2加密以获得中间数据，该中间数据被使用该专用密钥#_1解密以构成该数据Dx。 但是，第二个用户种类不能变换数据Dx为数据Dy，因为其不具有该专用密钥#_2。

第三个用户种类既不能变换数据Dx为数据Dy，也不能变换数据Dy为数据Dx。

这些方法的执行限制变换数据的可能性，需要建立公用密钥确认基础结构。 这样的基础结构是相对复杂和昂贵的。

发明内容

本发明的主题旨在通过提出一种能够限制用于三个用户种类数据的可能性的方法，及通过实施简单和廉价的装置改善先前的技术的缺点。

为了达到这样的目的，本发明的主题涉及一种经由至少一个处理和存储单元限制变换Tx型数据为Ty型数据的可能性，和变换Ty型数据为Tx型数据的可能性的方法，变换Tx型数据为Ty型数据被使用A型变换功能执行， 同时，变换Ty型数据为Tx型数据被使用与A型变换功能反相的B型变换功能执行，该数据尤其是被用于构成例如预付款标记，以及被在至少一个数据处理系统上执行。

按照本发明，该方法包括：

使用一个A型数据处理系统和一个B型数据处理系统，

至少一次建立至少一个在A型数据处理系统和B型数据处理系统之间的链路，以便将至少Ty型数据从A型数据处理系统(STDA 传送到B型数据处理系统(STDB)，和/或将至少Tx型数据从B型数据处理系统(STDB)传送到A型数据处理系统(STDA)，

在A型定制阶段期间，产生至少一个包括至少A型变换功能的A型处理和存储单元，

在A型变换阶段期间：

对于一个拥有至少一个A型处理和存储单元的用户，能够：

从A型数据处理系统传送至少一块Tx型数据给A型处理和存储单元，

在A型处理和存储单元中使用A型变换功能变换每块Tx型数据为一块Ty型数据，

从A型处理和存储单元传送每块Ty型数据给A型数据处理系统，

对于不拥有任何A型处理和存储单元的用户，不能使用A型变换功能变换Tx型数据块为Ty型数据块，

在B型定制阶段期间，产生至少一个包括B型变换功能而不包括A型变换功能的B型处理和存储单元，

以及在B型变换阶段期间：

对于拥有B型处理和存储单元并不拥有A型处理和存储单元的用户，

能够：

从B型数据处理系统传送至少一块Ty型数据给B型处理和存储单元，

在B型处理和存储单元中使用B型变换功能变换每块Ty型数据为一块Tx型数据，

从B型处理和存储单元传送每块Tx型数据给B型数据处理系统，

不能使用A型变换功能变换一块Tx型数据为一块Ty型数据。

附图说明

从下面参考附加的示意图进行的说明中展现各种各样的其他的特征，该附加的示意图作为非限制性的例子示出本发明主题的实施例和实施。

图1是一个功能方框图，举例说明能够实施本发明的技术装置。

图2是一个示意图，举例说明按照本发明的主题实施的数据变换。

图3是一个示意图，示出执行变换功能的地点。

图4是一个示意图，举例说明按照本发明的主题区分的用户类别。

图5是一个示意图，举例说明使用公知的密钥加密方法执行变换功能。

图6和7是举例说明使用公知的公用密钥、专用密钥加密方法的二

个变换功能实施例的示意图。

图8是一个示意图，举例说明除了已知的加密功能之外，实施一个附加的变换功能。

图9是一个示意图，举例说明一个实施定制处理和存储单元装置的例子。

图10是一个示意图，举例说明信息产生的原理。

图11是一个示意图，举例说明在定制阶段期间，朝着处理和存储单元的方向产生和传送信息。

图12和13分别是原理和应用的示意图，举例说明一个允许产生和使用预付款标记的本发明主题应用的例子。

具体实施方式

图1举例说明一个限制数据变换的可能性的系统1的实施例。 该系统1包括一个A型数据处理系统STD_A。 一般而言，这样的一个A型数据处理系统STD_A至少包括一个能够执行实施软件A_{11}的处理器A_{10}。 概括地说，该A型数据处理系统STD_A可以是一个计算机，一个服务器，或者例如是不同的机器、设备，固定或者移动的产品，或者载体的一部分。 该A型数据处理系统STD_A使用传送装置A_{12}通过链路A_{20}连接到一个A型处理和存储单元UTM_A。

在余下的说明书中，为了简单化起见，该A型数据处理系统STD_A将称为系统STD_A，并且该A型处理和存储单元UTM_A将称为单元UTM_A。

在该系统STD_A和该单元UTM_A之间的链路A_{20}可以以任何可能的方式实现，例如，一个串行链路，一个USB总线，一个无线电链路，一个光链路，一个网络链路，或者一个直接到系统STD_A的电路的电连接等等。 应该注意到，与系统STD_A的处理器相比较，该单元UTM_A可能也许实际上位于相同的集成电路之内。 在这种情况下，相对于该系统STD_A的处理器和是在该集成电路之内的链路A_{20}，该单元UTM_A可以被认为是共同的处理器。

该单元UTM_A包括传送装置A_{30}和处理和存储装置A_{31}。 必须考虑，该传送装置A_{12}和A_{30}存在软件和/或硬件特性，并且能够提供和优化在

该系统STD_A和该单元UTM_A之间的数据传输。 所述传送装置A_{12}、A_{30}适合于允许具有一个由其支配的实施软件A_{11}，最好是，与使用的链路A_{20}的类型无关。 所述传送装置A_{12}、A_{30}不是本发明主题的一部分，并且更确切地说作为该领域为大家所熟知的常识不做描述。

所述单元UTM_A能够：

使用该传送装置A_{30}：

接受由系统STD_A提供的数据，

返回数据给系统STD_A，

使用该处理和存储装置A_{31}：

或者以秘密方式存储数据，并且即使该单元UTM_A被关掉，保留至少一部分所述数据，

以及对于数据执行算法处理，部分或者所有的所述处理也许是秘密的。

作为非限制的例子，所述单元UTM_A可以由接通该系统STD_A的USB总线的材料，或者最好是由码片卡构成，并且其接口通常称作连接至该系统STD_A的读卡器。

在该情况下，该单元UTM_A由码片卡和其接口构成，该传送装置A_{30}被分成二个部分，一个在该接口上，以及另一个在该码片卡上。 在这个实施例中，由于包含在该码片卡中的该处理和存储装置A_{31}被丢失，缺少该码片卡被认为是相当于缺少该单元UTM_A。

该系统1还包括一个B型数据处理系统STD_B。 一般而言，这样的一个B型数据处理系统STD_B至少包括一个能够执行实施软件B_{11}的处理器B_{10}。 概括地说，该B型数据处理系统STD_B可以是一个计算机，一个服务器，或者例如是不同的机器、设备，固定或者移动的产品，或者载体的一部分。 该B型数据处理系统STD_B使用传送工具B_{12}通过链路B_{20}连接到一个B型处理和存储单元UTM_B。

在余下的说明书中，为了简单化起见，该B型数据处理系统STD_B将称为系统STD_B，并且该B型处理和存储单元UTM_B将称为单元UTM_B。

在该系统STD_B和该单元UTM_B之间的链路B_{20}可以以任何可能的方式实现，例如，一个串行链路，一个USB总线，一个无线电链路，一个光链路，一个网络链路，或者一个直接到系统STD_B的电路的电连接

等等。 应该注意到，与系统STD_B的处理器相比较，该单元UTM_B可能也许完全地位于相同的集成电路之内。 在这种情况下，相对于是集成电路内在的系统STD_B和链路B_{20}的处理器，该单元UTM_B可以被认为是共同的处理器。

该单元UTM_B包括传送装置B_{30}和处理和存储装置B_{31}。 必须考虑，该传送装置B_{12}和B_{30}具有软件和/或硬件本质性质，并且能够提供和优化在系统STD_B和单元UTM_B之间的数据传输。 所述传送工具B_{12}、B_{30}适合于允许具有一个由其支配的实施软件B_{11}，最好是，与使用的链路B_{20}的类型无关。 所述传送工具B_{12}、B_{30}不是本发明主题的一部分，并且更确切地说作为该领域为大家所熟知的常识不做描述。

所述单元UTM_B能够：

使用该传送工具B_{30}：

接受由系统STD_B提供的数据，

返回数据给系统STD_B，

使用该处理和存储装置B_{31}：

可能以秘密方式去存储数据，并且即使该单元UTM_B被关掉，保留至少一部分所述数据，

以及对于数据，被可能秘密处理的所述过程的部分或者所有的去执行算法处理。

作为非限制的例子，所述单元UTM_B可以由接通该系统STD_B的USB总线的材料，或者最好是由码片卡和其接口，通常为连接至该系统STD_B的电话卡读取器构成。

在该情况下，该单元UTM_B由码片卡和其接口构成，该传送装置B_{30}被分成二个部分，一个在该接口上，以及另一个在该码片卡上。 在这个实施例中，由于包含在该码片卡中的该处理和存储装置B_{31}被丢失，缺少该码片卡被认为是相当于缺少该单元UTM_B。

按照本发明的系统1至少曾经还包括至少一个在系统STD_A和该系统STD_B之间的链路L。 所述链路L构成一个信息传输通道，并且可以以所有公知的方法实现。 所述链路L可以由一个计算机网络和/或由传输信息（个人投送，邮政投送等等）的材料提供。 取决于应用，该链路L可以从系统STD_A发送信息给系统STD_B，从系统STD_B给系统STD_A，

或者以双向发送信息。 作为非限制的例子，通过在系统STD_A和系统STD_B之间的所述链路L的传送可以采用下列不同种类的信道： 从系统STD_A传输文件存储器，然后在一个实体载体上打印，然后传送所述实体的载体，然后在计算机上键盘操作数据，然后末了经由计算机网络传送到系统STD_B。

图2举例说明由按照本发明的过程执行的该数据变换。 定义了二种数据类型，即，Tx型和Ty型。 每一个所述Tx和Ty型是计算机数据的类型，例如8位字符，32位整数，64位整数512位整数，64位浮点。 在一个优选的变种实施例中，64位整数型被用作数据类型Tx和数据类型Ty。

本发明使用一个A型变换功能F_A和一个B型变换功能F_B。 该A型变换功能F_A是拥有作为设置Tx型开始和作为设置Ty型末端的一一对应。该B型变换功能F_B是拥有作为设置Ty型开始和作为设置Tx型末端的一一对应。 A型变换功能F_A和B型变换功能F_B是彼此相反的。 为了简单化起见，在余下的说明书中，A型变换功能F_A将称为功能F_A，以及B型变换功能F_B将称为功能F_B。

因此，该功能F_A变换一块Tx型数据Dx为一块Ty型数据Dy，即$Dy = F_A(Dx)$，同时该功能F_B变换一块Ty型数据Dy '为一块Tx型数据Dx '，即$Dx' = F_B(Dy')$。

由于该二种功能F_A和F_B是彼此相反的：

通过先后施加该二种功能F_A、F_B给一块数据Dx，人们再次找到这块数据Dx，即$Dx = F_B(F_A(dx))$，

通过先后施加该二种功能F_B、F_A给一块数据Dy '，人们再次找到这块数据Dy '，即$Dy' = F_B(F_A, (Dy'))$。

图3举例说明该功能F_A和F_B被执行的地点。 为的是实施本发明，该功能F_A和F_B必须保持机密。 为此目的，该功能F_A被仅在单元UTM_A内部执行，并且该功能F_B被仅在单元UTM_B内部，并且也许在单元UTM_A内部执行。 因此，在该单元UTM_A中，一块Tx型数据Dx被功能F_A变换为一块Ty型数据Dy，并且也许一块Ty型数据Dy '被功能F_B变换为一块Tx型数据Dx '。 此外，在该单元UTM_B中，一块Ty型数据Dy '被功能F_B变换为一块Tx型数据Dx '。

图4取决于单元UTM_A和/或UTM_B的属地，使通过本发明的主题区分的三个人或者用户的类别C1、C2、C3明确。

第一个类别C1的每个用户能够使用功能F_A变换一块Tx型数据为一块Ty型数据，并且也许使用功能F_B变换一块Ty型数据为一块Tx型数据。因此，第一个类别C1的每个用户可以使用单元UTM_A以及也许单元UTM_B。

第二个类别C2的每个用户能够使用功能F_B变换一块Ty型数据为一块Tx型数据。但是，第二个类别C2的每个用户不能使用功能F_A变换一块Tx型数据为一块Ty型数据。第二个类别C2的每个用户可以使用单元UTM_B，但是不能使用单元UTM_A。

第三个类别C3的每个用户既不具有单元UTM_A，又不具有单元UTM_B。所述第三个类别C3中没有用户能够使用功能F_A变换一块Tx型数据为一块Ty型数据，或者使用功能F_B变换一块Ty型数据为一块Tx型数据。

当然，只是在它们是不重要，并且很难推断观测数据进入和出自单元UTM_A和/或UTM_B的时候，该功能F_A和F_B是重要的。

图5举例说明使用公知的秘密键加密方法的功能F_A和F_B的第一个变种实施例。按照这个变种，该功能F_A被以密钥加密功能CS的形式执行，该密钥加密功能CS使用一个秘密信息单元Ics作为秘密关键码。

该密钥加密功能CS是一个标准的加密功能，例如DES、反相的DES、三重DES或者IDEA。该秘密信息单元Ics是一个用于该选择的加密功能的密钥。因而，该秘密信息单元Ics属于Kcs类型，即，属于用于所述功能的密钥的设置。例如，当该选择的密钥加密功能CS是DES的时候，所述Kcs类型秘密信息单元Ics是56位整数。

换句话说，使用该功能F_A变换一块Tx类型数据Dx为一块Ty类型数据Dy相当于使用密钥加密功能CS，使用该Kcs类型秘密信息单元Ics作为秘密关键码加密这块数据Dx。

类似地，功能F_A的反相的该功能F_B也以使用秘密信息单元Icsi作为秘密关键码，称作反相的密钥加密功能CSI的形式执行。

该秘密关键码反相的加密功能CSI是一个标准的加密功能，例如DES、反相的DES、三重DES或者IDEA。

该秘密信息单元Icsi是一个用于该选择的加密功能的密钥。 因而，该秘密信息单元Icsi属于Kcsi类型，即，属于用于所述功能的密钥的设置。

换句话说，使用该功能F_B变换一块Ty类型数据Dy '为一块Tx类型数据Dx '相当于使用秘密关键码反相的加密功能CSI，使用该KCSI类型秘密信息单元ICSI作为秘密关键码加密这块数据Dy。

使用该秘密关键码Icsi的该秘密关键码反相的加密功能CSI是使用该秘密关键码Ics的该密钥加密功能CS的反相。 例如，在该密钥加密功能CS是由功能DES执行的情况下，该秘密关键码反相的加密功能CSI必须由反相的DBS功能执行，同时该Kcs类型秘密信息单元Ics和Kcsi类型秘密信息单元Icsi必须是同样的。

图6和7举例说明使用公知的公共密钥、专用密钥加密方法，该功能F_A和F_B的第二个变种的实施例。

图6举例说明第一个实施例，其中该功能F_A是以公共密匙加密功能CPU作为公共密钥使用秘密信息单元icpu的形式执行的。

该公共密匙加密功能CPU是一个标准的加密功能，例如RSA。 该秘密信息单元icpu是一个用于该选择的加密功能的密钥。 因而，该公众秘密信息单元Icpu属于Kcpu类型，即，属于用于所述功能的公用密钥类。 例如，当该选择的公共密匙加密功能CPU是RSA的时候，所述Kcpu类型秘密信息单元icpu可以是由一个“模块”和一个“公开指数”形成的。

换句话说，使用该功能F_A变换一块Tx类型数据Dx为一块Ty类型数据Dy相当于使用公共密匙加密功能CPU，使用该KCPU类型秘密信息单元ICPU作为公共密钥加密这块数据Dx。

类似地，功能F_A的反相的该功能F_B以专用密钥解密功能CPUI，使用秘密信息单元icpui作为专用密钥的形式对其部分执行。

该专用密钥解密功能CPUI是一个标准功能，例如RSA。

该秘密信息单元icpui是一个用于该选择的解密功能的密钥。 因而，该秘密信息单元icpui属于kcpui类型，即，属于用于所述功能的专用密钥类。

换句话说，使用该功能F_B变换一块Ty类型数据Dy '为一块Tx类型

数据Dx '相当于使用专用密钥解密功能CPUI，使用该Kcpui类型秘密信息单元icpui作为专用密钥解密这块数据Dy '。

使用专用密钥icpui的该专用密钥解密功能CPUI是与使用公共密钥Icpu的该公共密匙加密功能CPU反相的。 例如，在该公共密匙加密功能CPU是由RSA加密功能执行的情况下，该专用密钥解密功能CPUI必须由该RSA解密功能执行，同时该Kcpu类型秘密信息单元icpu和该Kcpui类型秘密信息单元icpui必须分别是一个RSA公共密钥和其相关的专用密钥。

图7举例说明第二个实施例，其中该功能F_A被以专用密钥加密功能CPR，使用秘密信息单元I_{CPR}作为专用密钥的形式执行。

该专用密钥加密功能CPR是一个标准加密功能，例如RSA。 该秘密信息单元I_{CPR}是一个用于该选择的加密功能的密钥。 因而，该秘密信息单元I_{CPR}属于kcpr类型，即，属于用于所述功能的专用密钥类。 例如，当该选择的专用密钥加密功能CPR是RSA的时候，所述KcpR类型秘密信息单元I_{CPR}可以是由一个“模块”和一个“专用指数”形成的。

换句话说，使用该功能F_A变换一块Tx类型数据Dx为一块Ty类型数据Dy相当于使用专用密钥加密功能CPR，使用该KCPR类型秘密信息单元I_{CPR}作为专用密钥加密这块数据Dx。

类似地，功能F_A反相的该功能F_B以公共密钥解密功能CPRI，使用秘密信息单元I_{CPRI}作为公共密钥的形式对于其部分执行。

该公共密钥解密功能CPRI是一个标准功能，例如RSA。

该秘密信息单元I_{CPRI}是一个用于该选择的解密功能的密钥。因而，该秘密信息单元I_{CPRI}属于Kcpri类型，即，属于用于所述功能的公用密钥类。

换句话说，使用该功能F_B变换一块Ty类型数据Dy '为一块Tx类型数据Dx '相当于使用该公共密钥解密功能CPRI，使用该Kcpri类型秘密信息单元I_{CPRI}作为公共密钥解密这块数据Dy '。

使用公共密钥I_{CPRI}的该公共密钥解密功能CPRI是与使用专用密钥I_{CPR}的该专用密钥加密功能CPR反相的。 例如，在该专用密匙加密功能CPR是由RSA加密功能执行的情况下，该公共密钥解密功能CPRI必须由该RSA解密功能执行，同时该KcpR类型秘密信息单元I_{CPR}和该

KCPRI类型秘密信息单元I_{CPRI}必须分别是一个RSA专用密钥和其相关的公共密钥。

在相对于图6和7描述的二个例子中，该术语“加密功能”和“解密功能”被用于涉及二个彼此相反的加密术操作。 为了清楚起见，第一个功能被称作加密功能，以及第二个功能被称作解密功能。 其选择是任意的，甚至第一个功能不妨被称作解密功能，以及第二个功能不妨被称作加密功能。

图8是一个示意图，举例说明除了如在图5至7举例说明的公知的加密功能之外，执行一个附加变换功能。 当然，一个附加变换功能Fad与密钥加密功能CS或者与公共密匙加密功能CPU或者与专用密钥加密功能CPR相结合，可以被用作功能F_A。 所述附加变换功能Fad可以以任何方式与先前和/或以后的密钥加密功能CS，公共密匙加密功能CPU或者专用密钥加密功能CPR组合。 当然，所述附加变换功能Fad还可以由至少一个加密功能形成。

类似地，该功能F_B可以由一个称作反相Fadi的附加变换功能形成，其与该密钥反相加密功能CSI或者与该专用密钥解密功能CPUl或者与该公共密钥解密功能CPRI结合。

除在图5至8举例说明的任何一个变换功能的实施例之外，必须考虑本发明的主题包括一个处理和存储单元的定制阶段，在此期间该变换功能被插入在处理和存储单元中。

图9举例说明以分别获得单元UTM_A和单元UTM_B为目的，一个用于处理和存储单元UTM的定制装置100a和100B的执行例子。

在一个优选的实施例中，必须考虑每个处理和存储单元UTM包括为执行功能F_A所必需的算法装置110，以及为执行功能F_B所必需的算法装置120。 在使用密钥加密功能CS的情况下，该算法装置110对应于例如能够执行DES功能的装置。 在这种情况下，该算法装置120对应于能够执行反相的DES功能的装置。

在B型定制阶段期间，以获得一个单元UTM_B为目的，该定制装置100B经由任何类型的数据处理系统执行，包括去定制至少一个处理和存储单元UTM的装置。为此，使用该算法装置120以便获得单元UTM_B，单元UTM_B能够执行功能F_B。 但是，该定制装置100B也必须：

或者禁止为执行该功能F_A所必需的该算法装置110，

或者不加载给该处理和存储单元UTM能够执行功能F_A的该定制信息，并且或者防止其稍后加载。

因此，获得一个包括功能F_B而不包括功能F_A的单元UTM_B。

类似地，在一个A型定制阶段期间，以获得一个包括功能F_A或者和功能F_B的单元UTM_A为目的，使用该定制装置100A经由任何类型数据处理系统执行定制至少一个处理和存储单元UTM。 在该单元UTM_A不包括功能F_B的情况下，如在上面解释的，该算法装置120被禁止或者不加载该定制信息。

当然，该定制装置100A和100B可以经由相同的数据处理系统执行。 此外，可以使用为执行二个变换功能的仅一个所必需的仅包括该算法装置的处理和存储单元UTM。 在那种情况下，显而易见不需要禁止反相的功能。

该定制装置100A和100B也被用于提供产生由功能F_A和F_B使用的秘密信息，并且或者提供产生用于在图5至8举例说明的例子中描述的附加功能Fad、Fadi的附加参数。

图10是信息产生的一般原理清楚。 按照所述附图，一个主要的秘密信息SP（principal secret）是由算法Dp使用的，能够确定一对秘密信息单元Kcs型Ics和Kcsi型Icsi，或者Kcpu型Icpu和Kcpui型icpui，或者Kcpr型I_{CPR}和Kcpri型I_{CPRI}的一个，或者用于附加变换功能Fad的参数Pad和用于附加的反变换功能Fadi的参数Padi。

为了增加安全性，该主要的秘密信息SP可以使用一个秘密信息重建算法Dps，可以便利地从共用的秘密信息S1、S2、...、Sn来确定。

在产生该信息之后，其可以被考虑进入定制单元UTM_A和UTM_B。因此，如更确切地说从附图11显现出来的，在A型定制阶段期间，以获得一个单元UTM_A为目的，使用该定制装置100A去传送给处理和存储单元UTM：

该Kcs型秘密信息单元Ics或者该Kcpu型秘密信息单元icpu或者该KcpR型秘密信息单元I_{CPR}，或者用于附加变换功能Fad的该参数Pad去使单元UTM_A执行该功能F_A，

或者该Kcsi型秘密信息单元Icsi或者该Kcpui型秘密信息单元Icpui

或者该Kcpri型秘密信息单元I_{CPRI}，或者用于附加的反变换功能Fadi的该参数Padi去使该单元UTM_A执行该功能F_B。

类似地，在B型定制阶段期间，以获得一个单元UTM_B为目的，使用该定制装置100B去传送给处理和存储单元UTM，该Kcsi型秘密信息单元Icsi或者该Kcpri型秘密信息单元icpui或者该Kcpri型秘密信息单元I_{CPRI}，或者用于附加的反变换功能Fadi的该参数Padi去使该单元UTM_B执行该功能F_B。

本发明的主题旨在能够限制变换Tx型数据为Ty型数据的可能性，以及变换Ty型数据为Tx型数据的可能性。 为此，本发明的主题旨在放置最初用户类别C1的配置，至少一个单元UTM_A使用功能F_A能够变换一块Tx型数据为一块Ty型。 选择性地，所述单元UTM_A包括使用功能F_B可能变换一块Ty型数据为一块Tx型数据。

第二个用户类别C2具有至少一个单元UTM_B，能够使用该功能F_B提供变换Ty型数据为Tx型数据。 但是，所述第二个类别C2中没有用户使用该功能F_A能够执行变换Tx型数据为Ty型数据。因此出现可能性去限制在不同类别的用户之间变换数据的可能性。

在二个用户类别C1和C2能够变换数据，不能访问表示其变换的秘密信息的情况下，本发明的主题尤其是有用的。 这样的目的是通过在USB总线或者码片卡上使用，诸如材料密钥的处理和存储单元达到的。对于执行归因于另一个类别用户变换的用户类别唯一的可能性是去获得属于另一个类别的单元。

图12和13分别是原理和应用的示意图，举例说明一个能够产生和使用用于构成预付款标记的数据的本发明主题应用的例子。

更确切地说，如在图12出现的，定义一个开始装置E_d，其组成部分是Tx型数据块。在举例说明的例子中，该开始装置E_d包括五个部件，即：3、4、5、6、7。 该开始装置E_d的每个部件对应于一个客户的标识符，该客户拥有资源消费信用，例如一个查看信用的网页。 在A型变换阶段期间，该开始装置E_d的所有部件被使用包括在单元UTM_A中的功能F_A变换，以便获得一个目标装置E_A，其组成部分是Ty型数据块。在举例说明的例子中，该组成部分3、4、5、6、7被分别变换为12850、85503、23072、70331、45082。 因此，通过在单元UTM_A中执行的变

换获得的数据在该开始装置E_d的组成部分上给出无指示。

更确切地说，如在图13出现的，属于第一个类别C1的每个用户具有一个单元UTM_A，并且因此可以从在举例说明的例子中已知的起始标识符，即：3、4、5、6、7分别获得预付款标记标识符12580、85503、23072、70331、45082。 这样的预付款标记标识符例如可以被打印在标记j上，该标记j可以由任何适当的载体构成，诸如塑料卡或者赠券。所述预付款标记标识符最好是被遮盖，以证明对应于所述标记该资源停用。

此外，能够表示该开始装置E_d的信息I被经由链路L1发射给至少一个属于第二个类别C2的用户的系统STD_B。 在目前的情况下，该开始装置E_d由连续的整数组成，能够表示开始装置E_d的信息I例如可以是最小的组成部分的值和该装置组成部分的数目，即一对(3,5)。

在举例说明的例子中，一个标记j被发送给第三个类别C3的用户，因此其变为一个拥有资源消费信用的客户。 这些传输被任何适当的装置执行，诸如邮政投送或者个人投送(链路L2的一部分)。 还记得所述第三个类别C3的每个用户既不具有单元UTM_A，又不具有单元UTM_B。

在已经暴露他的预付款标记的标识符之后，即在举例说明的例子中的85503，第三个类别C3的用户经由链路L2的另一部分发送该暴露的标识符和一个用于资源Res耗费的请求Rq给第二个类别C2的用户。 还记得第二个类别C2的每个用户具有一个连接到系统STD_B的单元UTM_B。 由第三个类别C3的用户发射给系统STD_B的标识符被转送到单元UTM_B，以便以恢复该起始标识符为目的，使用包含在单元UTM_B中的功能F_B提供其变换。 在举例说明的例子中，因此，该单元UTM_B传送给系统STD_B已知的起始标识符，即4，对应于该预付款标记85503。

该系统STD_B使用信息I去验证该变换的成分，即4，在举例说明的例子中其属于开始装置E_d。 该验证能够保证该预付款标记没有被干预或者虚构。 因此，如果该标识符未被认出(N)，该请求Rq被拒绝，以致于一个否定答复Rp被发送给第三个类别C3的用户。如果该请求被接受(O)，该标识符被在一个资源阵列T中用作一个标志。 所述阵列T表示对于拥有对应于该标识符4的预付款标记的客户保持信用(举例说明的例子中为96)的数量。然后验证该剩余的信用对于进行的请求是足够

的。 在否定的情况(N)下，一个否定答复Rp被发送给第三个类别C3的用户。 在该信用是足够(O)的情况下，通过减去请求的资源的成本该阵列被更新，并且一个包括请求的资源Res的确定的回复Rp被制定，然后送给第三个类别C3的用户。

在先前的例子中，注意到：

在系统STD_A和STD_B之间存在几个链路，称作L1，L2，

第一个类别C1对应于个人的用户能够发行预付款标记，

第二个类别C2对应于服务提供者的用户希望去负担对资源Res访问，

第三个类别C3拥有至少一个预付款标记的用户，对应于或者访问负担资源的客户，

第三个类别C3不拥有预付款标记的用户，可以不是客户，因此不不能访问负担资源，

在描述的优选的例子中，本发明旨在限制变换用来构成预付款标记数据的可能性。 当然，本发明的主题可以被实施去限制变换不同的种类数据的可能性，例如，电子邮件消息，因特网页面等等。

本发明不局限于描述和表示的例子，例如在其框架内可以产生各种各样的修改。

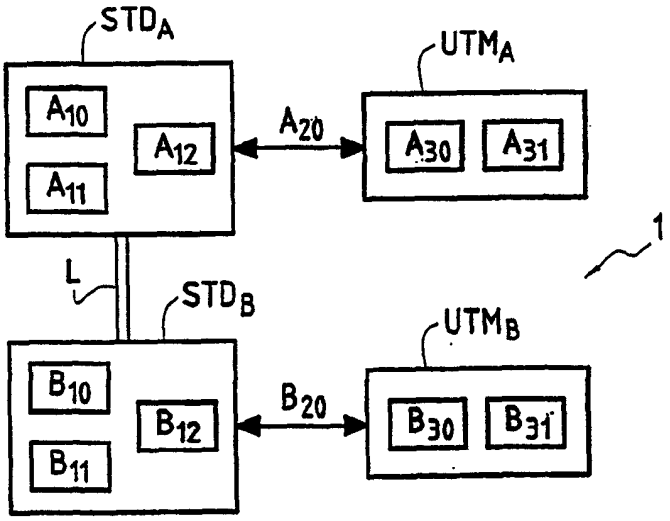

STDA
UTMA
A10
A11
A12
A20
A30
A31
L
STDB
UTMB
B10
B11
B12
B20
B30
B31
1

图1

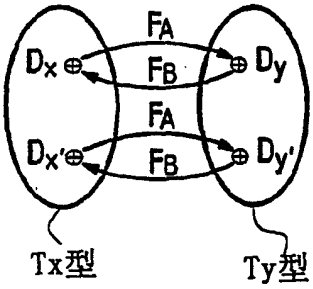

FA
FB
Dx
Dy
Dx'
Dy'
Tx型
Ty型

图2

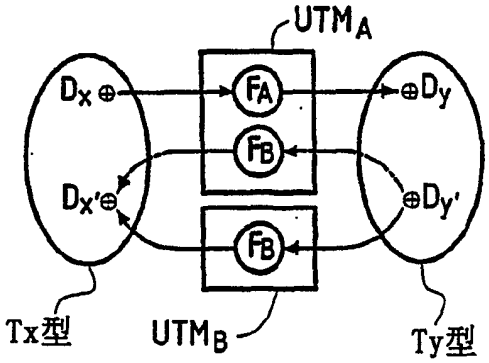

UTMA
Dx
Dy
Dx'
Dy'
FA
FB
FB
Tx型
UTMB
Ty型

图3

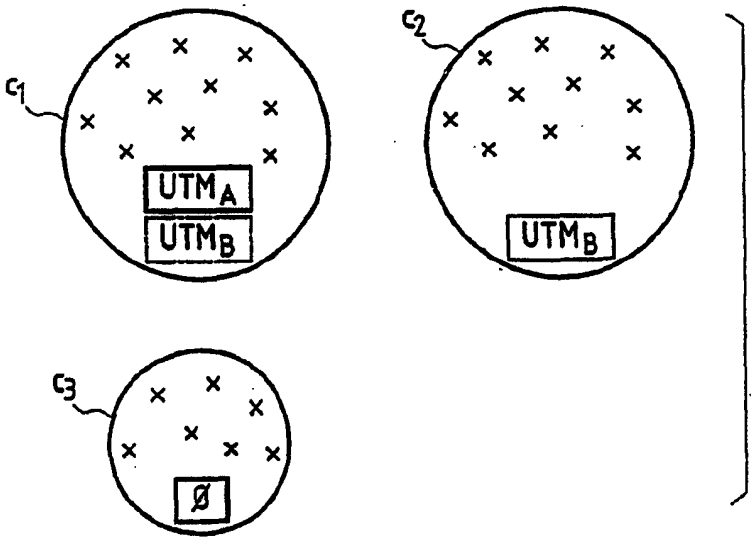

C1
UTMA
UTMB
C2
UTMB
C3
Ø

图4

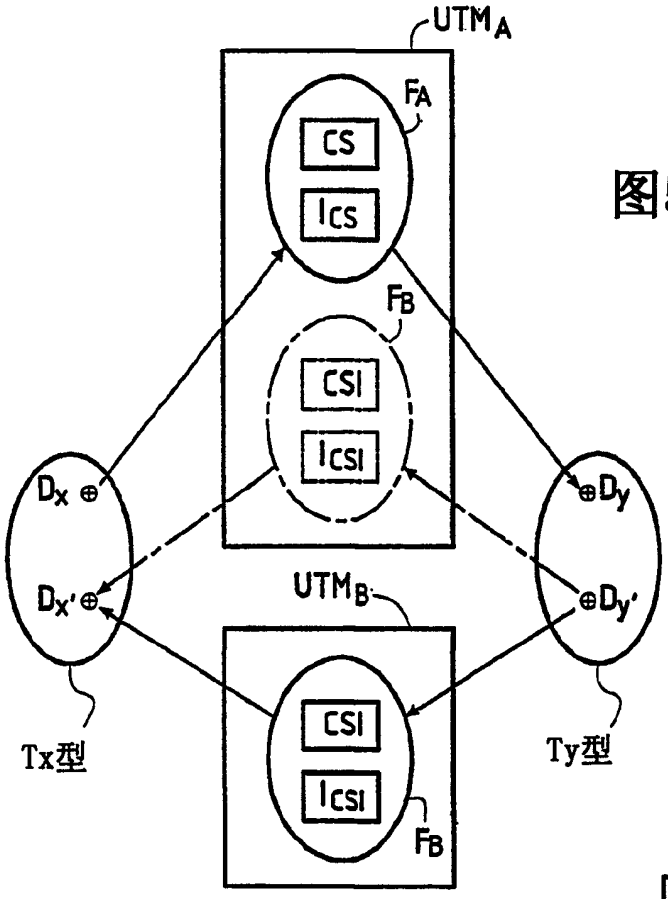
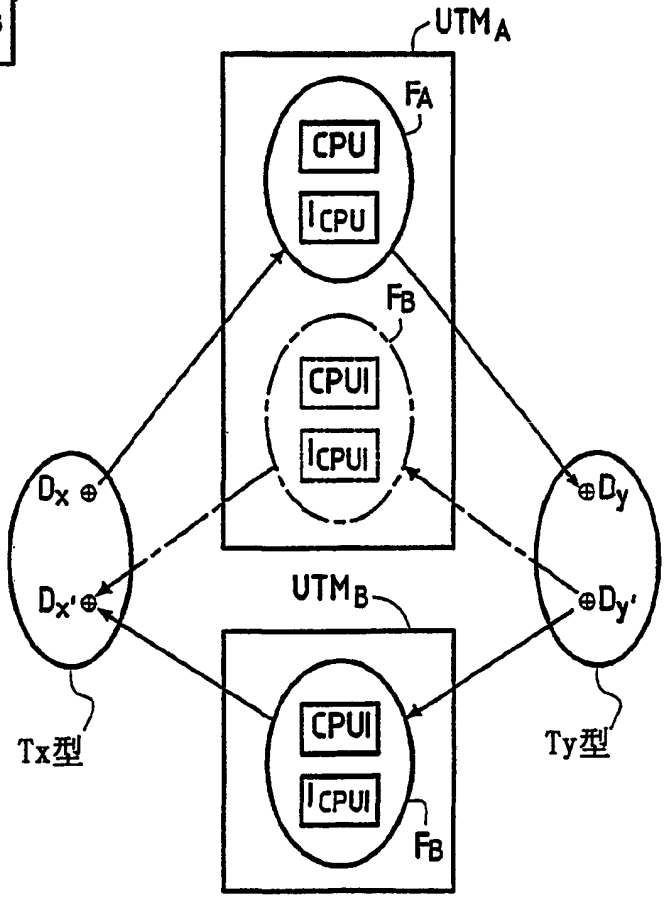

UTM A
FA
CS
ICS
FB
CSI
ICSI
Dx ⊕
⊕Dy
Dx'⊕
⊕Dy'
UTM B
CSI
ICSI
FB
Tx型
Ty型

图5

图6


UTM A
FA
CPU
ICPU
FB
CPUI
ICPUI
Dx ⊕
⊕Dy
Dx'⊕
⊕Dy'
UTM B
CPUI
ICPUI
FB
Tx型
Ty型

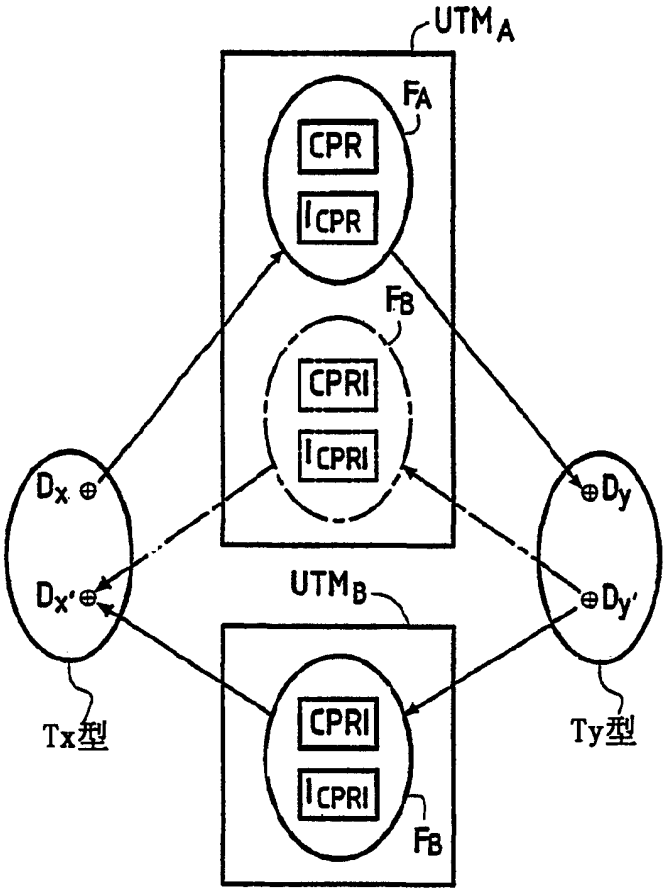

UTM A
FA
CPR
ICPR
FB
CPRI
ICPRI
Dx
Dx'
Dy
Dy'
UTM B
CPRI
ICPRI
FB
Tx型
Ty型

图7

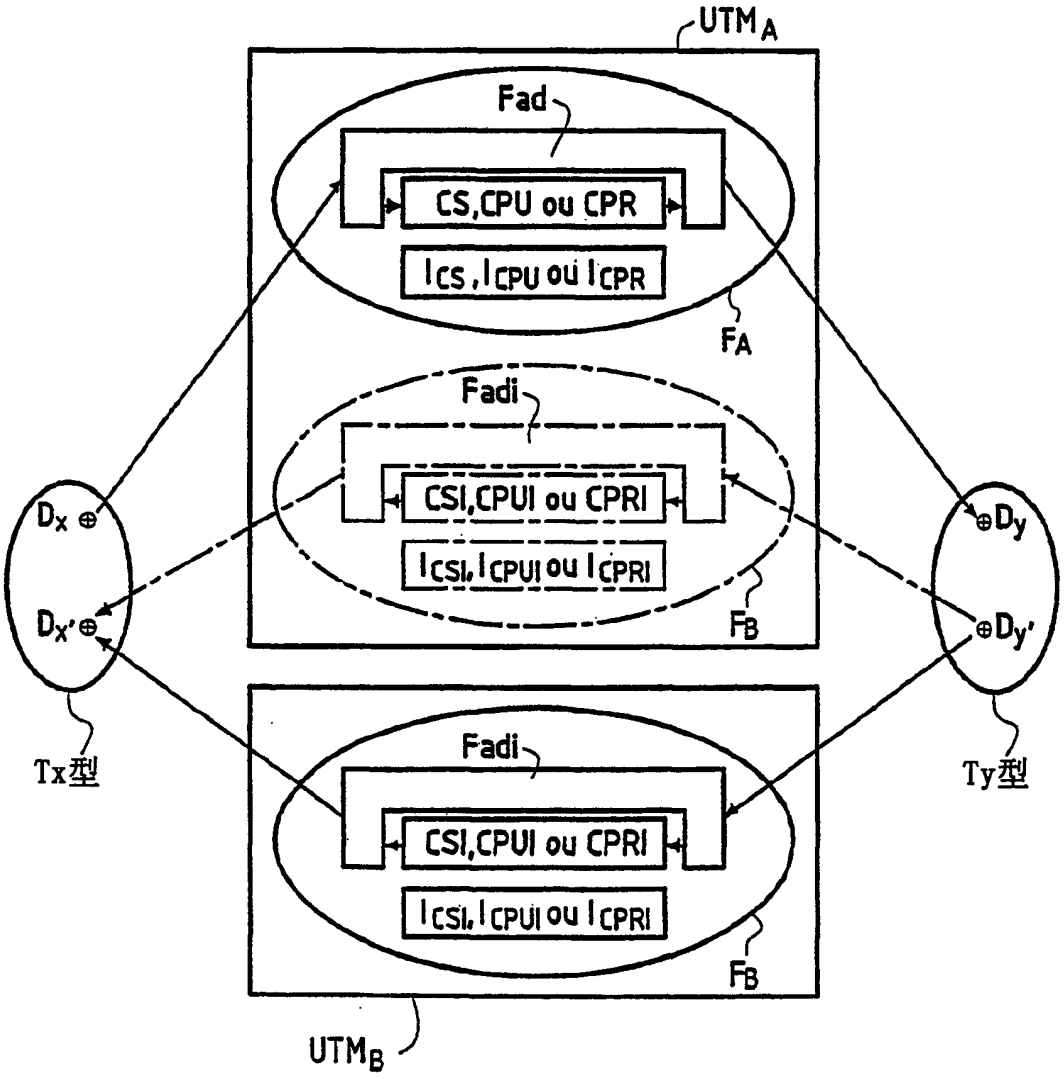
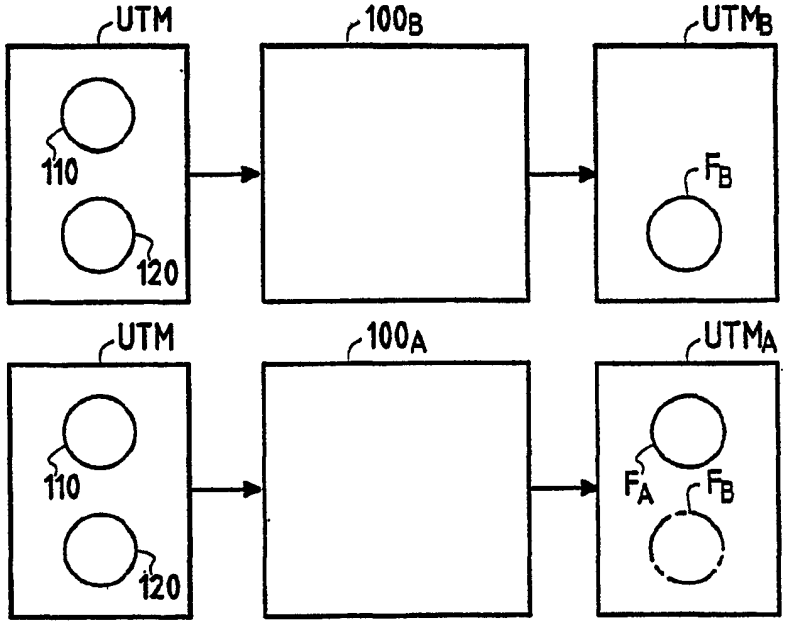

UTM A
Fad
CS,CPU ou CPR
ICS , ICPU ou ICPR
FA
Fadi
CSI,CPUI ou CPRI
ICSI, ICPUI ou ICPRI
FB
Dx ⊕
Dx' ⊕
⊕Dy
⊕Dy'
Tx型
Ty型
Fadi
CSI,CPUI ou CPRI
ICSI, ICPUI ou ICPRI
FB
UTM B

图8

图9


UTM
100B
UTMB
110
120
FB
UTM
100A
UTMA
110
120
FA
FB

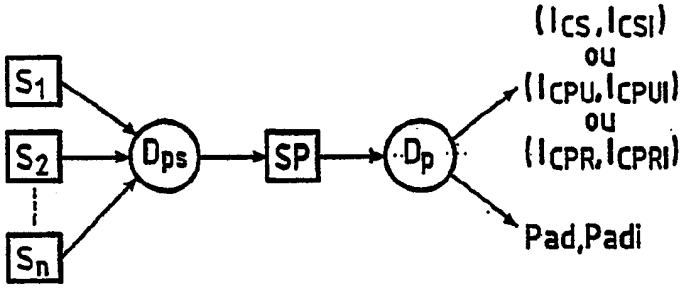

S1
S2
Sn
Dps
SP
Dp
(ICS,ICSI)
ou
(ICPU,ICPUI)
ou
(ICPR,ICPRI)
Pad,Padi

图10

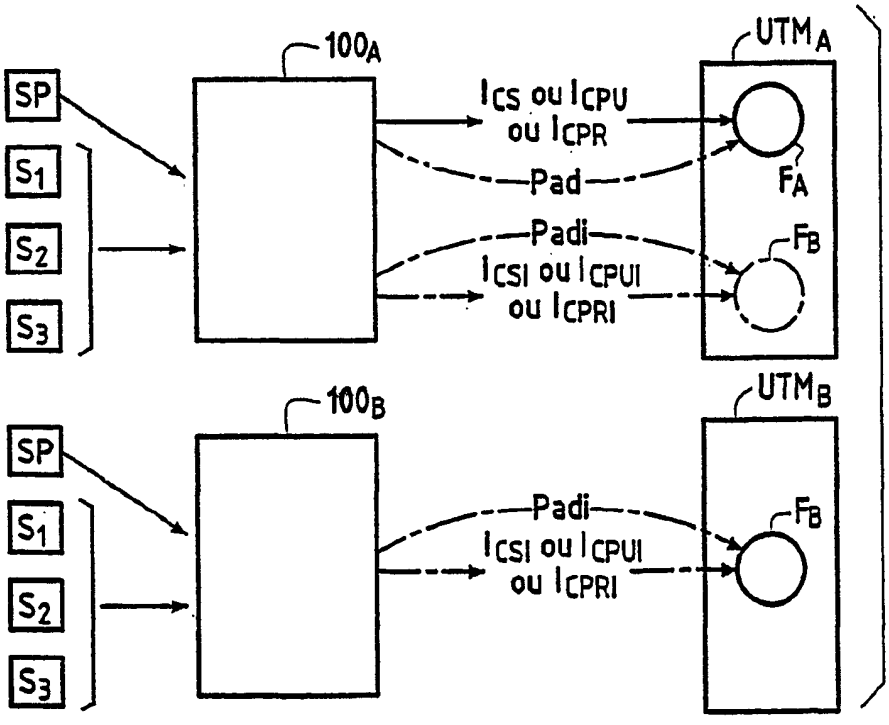

100A
UTMA
SP
S1
S2
S3
ICS ou ICPU
ou ICPR
Pad
FA
Padi
FB
ICSI ou ICPUI
ou ICPRI
100B
UTMB
SP
S1
S2
S3
Padi
FB
ICSI ou ICPUI
ou ICPRI

图11

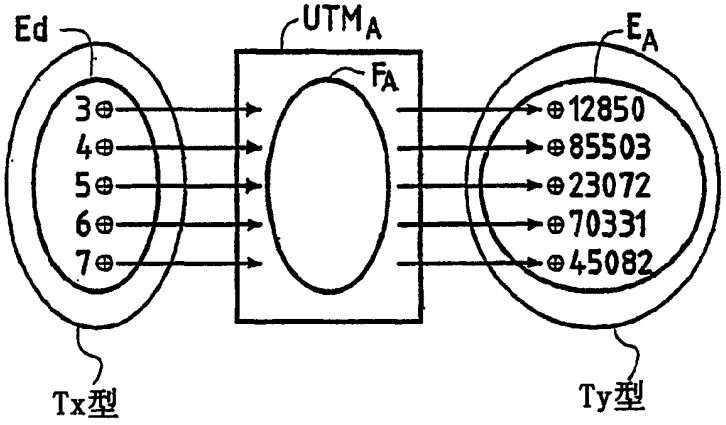

Ed
UTM A
E A
F A
3⊕
4⊕
5⊕
6⊕
7⊕
⊕12850
⊕85503
⊕23072
⊕70331
⊕45082
Tx型
Ty型

图12

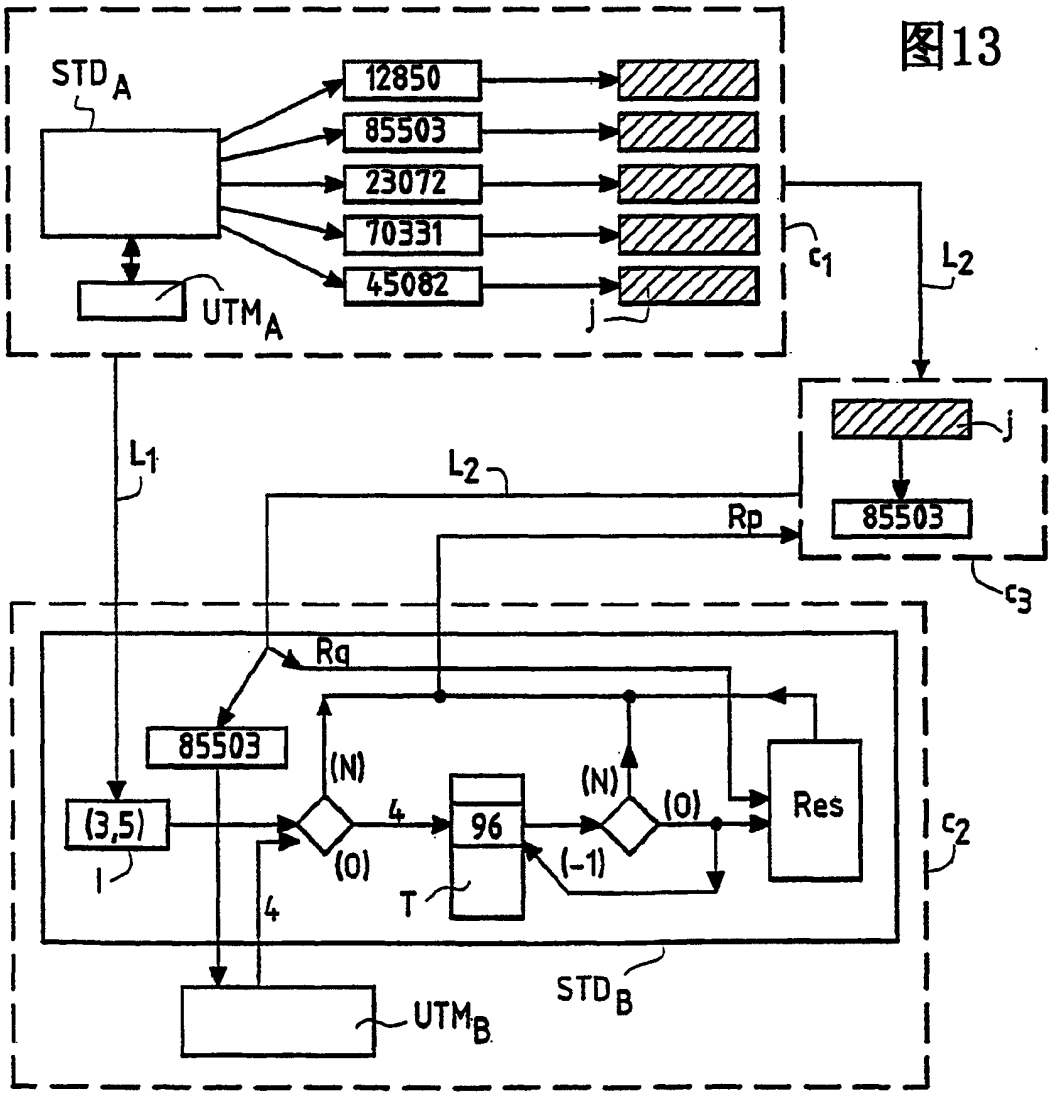

STD A
12850
85503
23072
70331
45082
UTM A
j
c1
L2
L1
L2
j
85503
Rp
c3
Rq
85503
(N)
(3,5)
1
4
(0)
96
T
(N)
(0)
(-1)
Res
c2
4
STD B
UTM B

图13